AGID: Le misure minime di sicurezza ICT per la PA

Cosa sono e come implementarle nel contesto accademico

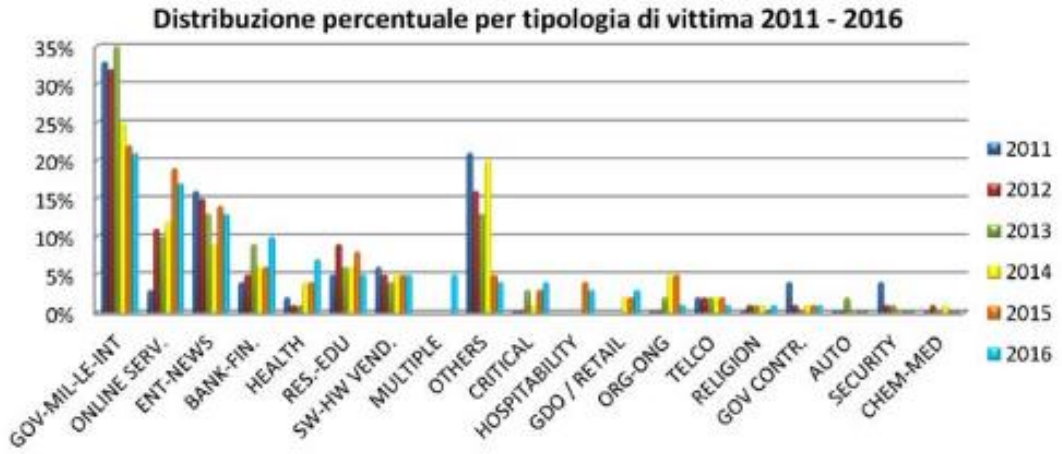
SAPIENZA
UNIVERSITÀ DI ROMA

Giuseppe Arrabito
Centro Infosapienza
giuseppe.arrabito@uniroma1.it

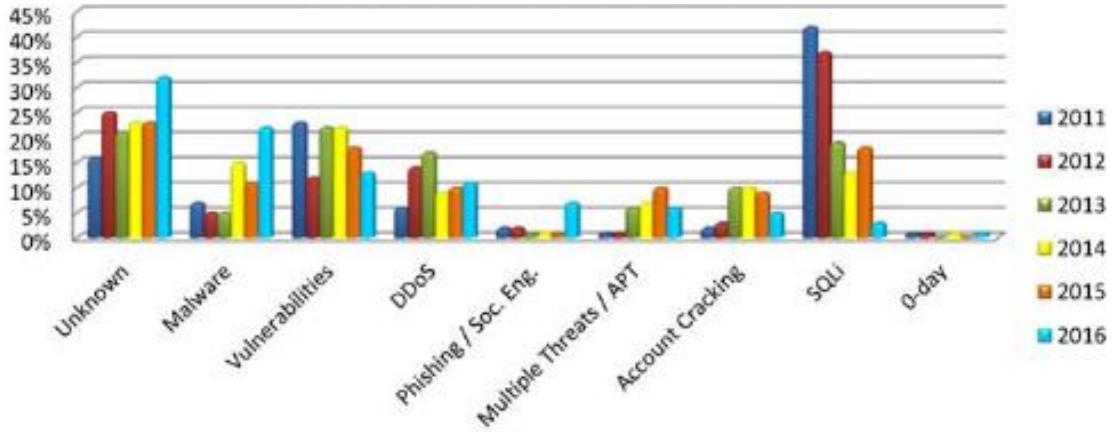
Francesco Ficarola
Centro Infosapienza
francesco.ficarola@uniroma1.it

Lo scenario attuale

2016 l'anno peggiore di sempre in termini di evoluzione delle minacce "cyber"



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

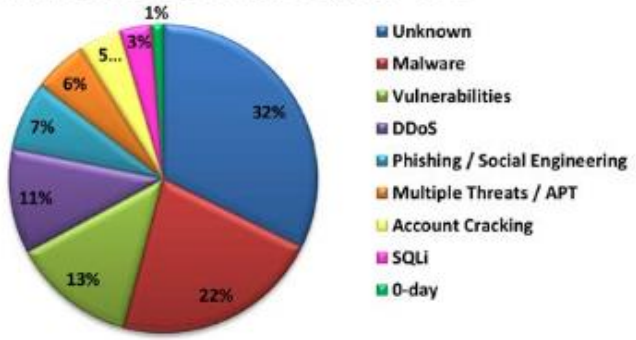


© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

Lo scenario attuale: le vittime illustri

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	-	-

Tipologia e distribuzione delle tecniche d'attacco - 2016



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

Attacchi rilevati per l'Ateneo

- Casi di ransomware/cryptolocker
- Furti di credenziali
- Spam
- Phishing e truffe on line
- Wi-Fi Rogue Access point
- Attacchi a forza bruta sulle form di autenticazione: il caso www.uniroma1.it
- Attacchi ai siti web istituzionali di dipartimenti e facoltà
- PC appartenenti a reti botnet
- Attacchi DDOS

Gestione incidenti

#EyePyramid

Infezione di un malware del tipo Remote Control adibito a compromettere i sistemi delle vittime ed esflitrare un gran quantitativo di informazioni riservate.

- Supporto congiunto CIS ed Infosapienza
- Analisi e verifica dell'infezione
- Nessun caso riscontrato sui dispostivi dell'Amm. Centrale

#WannaCry

Infezione virale di un malware del tipo ransomware che ha colpito circa 99 paesi con più di 200.000 infezioni.

- Attivazione del team Infosapienza
- Analisi del worm e successive contromisure
- Emanazione di linee guida preventive e correttive
- Nessun caso riscontrato nell'amministrazione Centrale
- 6 casi isolati all'interno di strutture dipartimentali

I possibili rischi per l'Ateneo

- Rischio di perdita di disponibilità, integrità e confidenzialità delle informazioni e dei dati: violazioni informatiche
- Rischio di sanzioni amministrative e penali: perdite economiche
- Rischio reputazionale: danno all'immagine
- Perdita di fiducia degli utenti nell'utilizzo delle tecnologie informatiche e nell'innovazione digitale: possibile calo di nuove iscrizioni

IL DANNO DI IMMAGINE

«…consiste nella considerazione e nella credibilità di cui il soggetto gode nella società e ne costituisce il primo driver di valore….»
[Corradini, Nardelli 2013]

Il quadro normativo per la PA

Con l'avvenuta pubblicazione in Gazzetta Ufficiale (Serie Generale n.103 del 5-5-2017) della Circolare 18 aprile 2017, n. 2/2017, recante «**Misure minime di sicurezza ICT per le pubbliche amministrazioni**. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)», le Misure minime sono ora divenute di obbligatoria adozione per tutte le Amministrazioni. **Scadenza 31/12/2017**

AGID Misure minime di sicurezza

Il **regolamento generale sulla protezione dei dati** (GDPR, *General Data Protection Regulation-Regolamento UE 2016/679)* è un Regolamento con il quale la Commissione europea intende rafforzare e unificare la protezione dei dati personali entro i confini dell'Unione europea). **Applicabile dal 24/05/2018**

GDPR

Il nuovo CAD. Con la pubblicazione sulla Gazzetta Ufficiale n. 214 del **13 settembre 2016**, il decreto legislativo 26 agosto 2016, n. 179 recante *Modifiche ed integrazioni al Codice dell'amministrazione digitale, in materia di riorganizzazione delle amministrazioni pubbliche*, entra in vigore oggi, 14 settembre 2016

Codice Amministrazione Digitale

DPCM 17 febbraio 2017
Decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017
Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali (pubblicato sulla GU n. 87 del 13/4/2017)

Strategia nazionale e piano di cybersecurity

Inquadramento generale

CIRCOLARE 17 marzo 2017, n. 1/2017
Misure minime di sicurezza ICT per le pubbliche amministrazioni. (*GU Serie Generale n.79 del 04-04-2017)*

CIRCOLARE 18 marzo 2017, n. 2/2017
Misure minime di sicurezza ICT per le pubbliche amministrazioni. *(GU Serie Generale n.103 del 05-05-2017)*

> *La direttiva del 1 agosto 2015 del Presidente del Consiglio dei ministri impone l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici. Al fine di agevolare tale processo, individua nell'Agenzia per l'Italia digitale l'organismo che dovrà rendere prontamente disponibili gli indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori partner del nostro Paese e dalle organizzazioni internazionali di cui l'Italia è parte.*

Art. 1. ***Scopo***
Obiettivo della presente circolare è indicare alle pubbliche amministrazioni le misure minime per la sicurezza ICT che debbono essere adottate al fi ne di contrastare le minacce più comuni e frequenti cui sono soggetti i loro sistemi informativi. Le misure minime di cui al comma precedente sono contenute nell'allegato 1, che costituisce parte integrante della presente circolare.

Art. 2. ***Amministrazioni destinatarie***
Destinatari della presente circolare sono i soggetti di cui all'art. 2, comma 2 del C.A.D.

Art. 3. ***Attuazione delle misure minime***
Il responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie di cui all'art.17 del C.A.D., ovvero, in sua assenza, il dirigente allo scopo designato, ha la responsabilità della attuazione delle misure minime di cui all'art. 1.

Art. 4. ***Modulo di implementazione delle MMS-PA***
Le modalità con cui ciascuna misura è implementata presso l'amministrazione debbono essere sinteticamente riportate nel modulo di implementazione di cui all'allegato 2, anch'esso parte integrante della presente circolare. Il modulo di implementazione dovrà essere fi rmato digitalmente con marcatura temporale dal soggetto di cui all'art. 3 e dal responsabile legale della struttura. Dopo la sottoscrizione esso deve essere conservato e, in caso di incidente informatico, trasmesso al CERT-PA insieme con la segnalazione dell'incidente stesso.

Inquadramento generale

Obiettivo della presente circolare è indicare alle pubbliche amministrazioni **le misure minime per la sicurezza ICT che debbono essere adottare al fine di contrastare le minacce più comuni** e frequenti cui sono soggetti i loro sistemi informativi.

Ai sensi dell'art. 3 della Circolare citata, "**il responsabile dei sistemi informativi** di cui all'art. 10 del decreto legislativo 12 febbraio 1993, n. 39, ovvero, in sua assenza, il **dirigente allo scopo designato**, ha la responsabilità della attuazione delle misure minime di cui all'art. 1".

Obbligo per le pubbliche amministrazioni, in ossequio a quanto previsto al successivo art. 5 della Circolare, entro il **31 dicembre 2017** dovranno attuare gli adempimenti necessari ed uniformarsi.

Inquadramento generale

- Le misure minime di sicurezza ICT per le pubbliche amministrazioni costituiscono una parte integrante delle linee guida per la sicurezza ICT delle pubbliche amministrazioni.

- Sono state emesse in attuazione alla direttiva del 1 agosto 2015 del Presidente del Consiglio dei ministri che impone l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici e costituiscono un'anticipazione urgente della regolamentazione completa in corso di emanazione.

- Consistono in un insieme ordinato e ragionato di "controlli", ossia azioni puntuali di natura tecnica ed organizzativa, predisposto da AgID per fornire alle pubbliche amministrazioni dei criteri di riferimento per stabilire se il livello di protezione offerto da un'infrastruttura risponda alle esigenze operative, individuando anche gli interventi idonei per il suo adeguamento

Le misure minime di sicurezza - AGID

- Tali misure, il cui rispetto è richiesto a tutte le PA, prevedono **tre livelli di attuazione: minimo, standard e alto**

- Fra le misure minime è previsto anche che le pubbliche amministrazioni accedano sistematicamente a **servizi di early warning** che consentano loro di rimanere aggiornate sulle nuove vulnerabilità di sicurezza. A tal proposito il CERT-PA fornisce servizi proattivi ed informativi a tutte le amministrazioni accreditate.

- Le misure minime di sicurezza ICT- che costituiscono parte integrante del più ampio disegno delle Regole Tecniche per la sicurezza informatica della Pubblica Amministrazione di futura emanazione

MMS-PA: ABSC (Agid Basic Security Controls)

- I controlli individuati da AgID sono basati sui 20 CIS Critical Security Control (CCSC) pubblicati dal Center for Internet Security (CIS) noti anche come «SANS 20»
- I CCSC sono largamente diffusi ed utilizzati, e pongono una particolare attenzione ai costi che l'implementazione di una misura minima richiede rispetto ai benefici che è in grado di offrire
- Le MMS-PA pongono l'accento sugli **aspetti di prevenzione** piuttosto che su quelli di risposta e ripristino

I CONTROLLI : ABSC

AgID Basic Security Control(s) (ABSC) sono un estratto di 5 dei 20 Critical Security Check (CSC) del SANS Institute

Tipologia	Descrizione
ABSC1 (CSC1)	INVENTARIO DEI DISPOSITIVI AUTORIZZATI
ABSC2 (CSC2)	INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI
ABSC3 (CSC3)	PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER
ABSC4 (CSC4)	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ
ABSC5 (CSC5)	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE
ABSC8 (CSC8)	DIFESE CONTRO I MALWARE
ABSC10 (CSC10)	COPIE DI SICUREZZA
ABSC13 (CSC13)	PROTEZIONE DEI DATI

I controlli: ABSC1

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

ABSC_ID #			Descrizione	FNSC	Min	Std.	Alto
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	ID.AM-1	X	X	X
		2	Implementare ABSC 1.1.1 attraverso uno strumento automatico	ID.AM-1		X	X
		3	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	ID.AM-1			X
		4	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	ID.AM-1			X
	2	1	Implementare il "logging" delle operazione del server DHCP.	ID.AM-1		X	X
		2	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	ID.AM-1		X	X
	3	1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1	X	X	X
		2	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1		X	X
	4	1	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	ID.AM-1	X	X	X
		2	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	ID.AM-1		X	X
		3	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	ID.AM-1			X

ABSC	ID #		Descrizione	FNSC	Min.	Std.	Alto
1	5	1	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	ID.AM-1			X
	6	1	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	ID.AM-1			X

ABSC1: Le modalità di implementazione

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4		M
		2	Implementare ABSC 1.1.1 attraverso uno strumento automatico		S
		3	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.		A
		4	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.		A
	2	1	Implementare il "logging" delle operazione del server DHCP.		S
		2	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.		S
	3	1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.		M
		2	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.		S

Le misure minime di sicurezza: le criticità per le Università

- Pubblicazione e periodo di applicabilità
- Criticità legate al contesto accademico
- Sostenibilità delle contromisure: budget di previsione già redatti
- Gruppo di lavoro CODAU per consultazione con AGID
- Dubbi riguardanti alcune definizioni (risorse attive, dispositivi informatici, etc)
- Applicabilità e sostenibilità interna
- Mancanza di un processo di verifica di quanto dichiarato
- Obbligo normativo: configura l'inadempienza di atti di ufficio.

Il processo interno dell'Ateneo

- Circolare del DG recanti indirizzi e modalità operative
- Incontri con i referenti informatici (5/10)
- Definizione di procedure interne
- Definizione di aree omogenee per l'Ateneo e relative responsabilità
- Ruolo e attività dei referenti informatici
- Ruolo e attività dei responsabili di laboratorio
- Ruoli e responsabilità del RAD e dei Direttori di Dipartimento
- Ogni struttura produrrà un documento per le aree individuate da consegnare il 15.12.2017 a CINFO

Cronoprogramma

Attività	ottobre	novembre	dicembre
Formazione referenti informatici	5 ott		
Attività interne alla struttura	5 ott	5 nov	
Formazione RAD		10 nov	
Follow up ai referenti		14 nov	
Consegna ad InfoSapienza delle MMS delle strutture per			Entro il 15/12/17
Firma del Rettore			Entro il 31/12/17

GRAZIE A TUTTI

PER L'ATTENZIONE

Giuseppe Arrabito
Centro Infosapienza
giuseppe.arrabito@uniroma1.it

Francesco Ficarola
Centro Infosapienza
francesco.ficarola@uniroma1.it