AGID: Le misure minime di sicurezza ICT per la PA

Documento di sintesi della Circolare AGID

SAPIENZA
UNIVERSITÀ DI ROMA

Obiettivi

- Indirizzare l’esigenza delle Amministrazioni fornendo loro, in particolare a quelle meno preparate, un riferimento operativo direttamente utilizzabile (checklist) nell’attesa della pubblicazione di documenti di indirizzo di più ampio respiro (linee guida, norme tecniche)

- Stabilire una baseline comune di misure tecniche ed organizzative irrinunciabili

- Fornire alle Amministrazioni uno strumento per poter verificare lo stato corrente di attuazione delle misure di protezione contro le minacce informatiche, e poter tracciare un percorso di miglioramento

- Responsabilizzare le Amministrazioni sulla necessità di migliorare e mantenere adeguato il proprio livello di protezione cibernetica ponendo il compito (e la relativa responsabilità) direttamente in capo al dirigente competente

Struttura: le famiglie di controlli

ABSC 1 (CSC 1): inventario dei dispositivi autorizzati e non autorizzati

ABSC 2 (CSC 2): inventario dei software autorizzati e non autorizzati

ABSC 3 (CSC 3): proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server

ABSC 4 (CSC 4): valutazione e correzione continua della vulnerabilità

ABSC 5 (CSC 5): uso appropriato dei privilegi di amministratore

ABSC 8 (CSC 8): difese contro i malware

ABSC 10 (CSC 10): copie di sicurezza

ABSC 13 (CSC 13): protezione dei dati

I livelli di applicazione

MINIMO

È quello al quale ogni pubblica amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme.

STANDARD

Può essere assunto come base di riferimento nella maggior parte dei casi

ALTO

Deve essere adottato dalle organizzazioni maggiormente esposte a rischi per la criticità delle informazioni trattate o dei servizi erogati ma anche come un obiettivo da parte di tutte le altre organizzazioni per aumentare la sicurezza

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

Inventario delle risorse

Logging

Autenticazione di rete

ABSC 2 (CSC 2)
Inventario dei software autorizzati e non autorizzati

Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione

- **Inventario dei software autorizzati**
- **Whitelist delle applicazioni autorizzate**
- **Individuazione di software non autorizzato**
- **Isolamento delle reti (air-gap)**

ABSC 3 (CSC 3)
Proteggere le configurazioni di hardware e software sui dispositivi

Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.

- **Configurazioni standard**
- **Accesso amministrativo da connessioni protette**
- **Verifica dell’integrità dei file critici**
- **Gestione delle configurazioni**

ABSC 4 (CSC 4)
Valutazione e correzione continua della vulnerabilità

Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.

- **Verifica delle vulnerabilità**
- **Aggiornamento dei sistemi**

ABSC 5 (CSC 5)
Uso appropriato dei privilegi di amministratore

Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.

- **Limitazione dei privilegi delle utenze amministrative**
- **Inventario delle utenze amministrative**
- **Gestione delle credenziali delle utenze amministrative**

ABSC 8 (CSC 8)
Difese contro i malware

Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.

- **Sistemi di protezione (antivirus, firewall, IPS)**
- **Uso dei dispositivi esterni**
- **Controllo dei contenuti Web, email**

ABSC 10 (CSC 10)
Copie di sicurezza

Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.

- **Backup e verifica del restore**
- **Protezione delle copie di backup**

ABSC 13 (CSC 13):
Protezione dei dati

Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti Uso della crittografia

- **Limitazioni sull'uso di dispositivi removibili**
- **Controlli sulle connessioni di rete/Internet**

ABSC 4 (CSC 4):
Valutazione e correzione continua della vulnerabilità

Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.

- **Verifica delle vulnerabilità**
- **Aggiornamento dei sistemi**

ABSC 4 (CSC 4):
Valutazione e correzione continua della vulnerabilità

Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.

- **Verifica delle vulnerabilità**
- **Aggiornamento dei sistemi**