



Fastweb Digital Academy

CIBERSICUREZZA: MINACCE E CONTROMISURE

Docente
Guglielmo Bondioni

PRINCIPALI MINACCE INFORMATICHE UE

1. Ransomware
2. Malware
3. Cryptojacking e cryptomining occulto
4. Attacchi e-mail
5. Violazioni e fughe di dati
6. Attacchi DoS/DDoS
7. Disinformazione
8. Minacce non malevole (accidentali)
9. Minacce alle catene di approvvigionamento

CONTRASTO ALLE MINACCE INFORMATICHE

Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015

L'**Agenzia per l'Italia Digitale** emana le:

Misure minime di sicurezza ICT
per le pubbliche amministrazioni

MISURE MINIME DI SICUREZZA ICT PER LE PA

Circolare AgID 18 aprile 2017, n. 2/2017

5-5-2017

GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA

Serie generale - n. 103

CIRCOLARI

AGENZIA PER L'ITALIA DIGITALE

CIRCOLARE 18 aprile 2017, n. 2/2017.

Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)».

MISURE MINIME DI SICUREZZA ICT PER LE PA

Articolate in **8 gruppi di controlli**.

I controlli sono mutuati dai "critical security controls" (CSC) del Center for Internet Security (CIS).

Le misure sono **obbligatorie** per le pubbliche amministrazioni.

I controlli sono suddivisi in **3 livelli**:

- Minimo: controlli obbligatori per tutte le P.A.
- Standard: il livello che tutte le P.A. dovrebbero ottenere
- Alto: l'obiettivo a cui le P.A. devono tendere

MISURE MINIME AGID PER LE PA

Codice	Titolo
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

MISURE MINIME AGID PER LE PA

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."

MISURE MINIME AGID PER LE PA

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."

MISURE MINIME AGID PER LE PA

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

"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."

MISURE MINIME AGID PER LE PA

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."

MISURE MINIME AGID PER LE PA

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."

MISURE MINIME AGID PER LE PA

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."

MISURE MINIME AGID PER LE PA

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."

MISURE MINIME AGID PER LE PA

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

"Processi interni, strumenti e sistemi necessari per evitare l'effiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti."

MISURE AGID NON SOLO PER LE PA

Le "misure minime" AgID sono valide per qualsiasi organizzazione

Sono necessarie per avere il governo:

- dei sistemi informatici
- dei dati
- dell'operato delle persone su sistemi e dati

Sono **misure organizzative** prima che tecniche.

