Area 5 - LA PA NELLA TRASFORMAZIONE DIGITALE

Modulo 4 – Il Piano triennale per l'informatica nella PA

Lezione 5.4.4 – Misure minime di sicurezza ICT per la PA

Introduzione

Ciao e benvenuto/a a questa lezione dedicata alle Misure minime di sicurezza che ogni PA deve adottare nel campo delle tecnologie dell'informazione e della comunicazione (ICT).

Dopo aver visto brevemente il contesto normativo di riferimento, analizzeremo insieme le Linee guida stilate dall'AgID (Agenzia per l'Italia Digitale) in materia. Iniziamo!

I rischi legati alla digitalizzazione della PA

La progressiva digitalizzazione della Pubblica Amministrazione offre innumerevoli vantaggi ma comporta anche un crescente aumento dei rischi che un ambiente informatico implica.

Per questo diventa sempre più necessario per le Pubbliche Amministrazioni adottare misure di sicurezza adeguate che proteggano dati e processi.

A questo proposito AgID ha individuato le Misure minime di sicurezza ICT di riferimento per le Pubbliche Amministrazioni con l'obiettivo di contrastare le minacce informatiche più frequenti. Tali Misure sono state pubblicate in Gazzetta Ufficiale con Circolare del 18 aprile 2017, n. 2/2017. Tutte le Pubbliche Amministrazioni si sono dovute adeguare ad esse entro il 31 dicembre 2017 e i Dirigenti che non hanno provveduto alla loro adozione sono sanzionabili per legge.

Non si tratta tuttavia di una norma statica: AgID si impegna ad aggiornarle tutte le volte che si renderà necessario, in funzione dell'evoluzione della minaccia cibernetica, al fine di mantenere la Pubblica Amministrazione a un livello adeguato di protezione.

Cosa sono le Misure minime di sicurezza ICT

Le Misure minime di sicurezza ICT per le Pubbliche Amministrazioni emanate dall'AgID consistono in un supporto metodologico che elenca un insieme ordinato e ragionato di "controlli" di natura tecnologica, organizzativa e procedurale. Tali controlli aiutano le Pubbliche Amministrazioni a verificare il proprio stato di protezione responsabilizzandosi sulla sicurezza cibernetica e avviando un percorso autonomo di monitoraggio e miglioramento. Questo aspetto è particolarmente significativo per le Amministrazione più piccole che hanno meno possibilità di avvalersi di professionalità specifiche.

Le Misure minime forniscono alle Pubbliche Amministrazioni un elenco di azioni puntuali che costituiscono un riferimento operativo per valutare e innalzare il livello della sicurezza informatica. Esse stabiliscono inoltre una base comune di misure irrinunciabili e omogenee.

La modularità delle Misure di sicurezza

Quest'ultimo concetto è molto importante. AgID infatti ha modulato le Misure di sicurezza fornendo un minimo comune denominatore ma tenendo anche conto delle enormi differenze di dimensioni, mandato, tipologie di informazioni gestite, esposizione al rischio, complessità strutturali, eterogeneità dei servizi erogati e risorse economiche che caratterizzano le oltre 20.000 Amministrazioni Pubbliche italiane.

In questo modo ogni Amministrazione ha implementato un livello di sicurezza informatica basilare e adatto alle effettive esigenze della specifica realtà locale. Le Amministrazioni più piccole non sono state costrette a introdurre misure esagerate per la propria organizzazione, con conseguente inutile dispendio di risorse, mentre le Amministrazioni più complesse si avvalgono di una protezione più elevata commisurata all'esposizione a rischi maggiori.

I tre livelli di attuazione delle Misure di sicurezza

I livelli di attuazione progressiva individuati da AgID sono tre:

1. Minimo, ovvero quello al quale ogni Pubblica Amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme;
2. Standard, cioè il livello, superiore a quello minimo, che ogni Amministrazione deve considerare come base di riferimento in termini di sicurezza. Questo rappresenta la maggior parte delle realtà della PA italiana;
3. Avanzato, il quale deve essere adottato dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visto come obiettivo di miglioramento da parte di tutte le altre organizzazioni.

Fra le misure minime è previsto inoltre che le Pubbliche Amministrazioni accedano a servizi di early warning per rimanere aggiornate sulle nuove vulnerabilità di sicurezza.

Il SAN20 come modello di ispirazione

Le Misure minime di sicurezza ICT per le Pubbliche Amministrazioni si ispirano all'insieme di controlli noto come SAN20, pubblicato dal Center for Internet Security come CCSC «CIS Critical Security Controls for Effective Cyber Defense» nella versione 6.0 di ottobre 2015. Il SAN20 è un elenco composto da 20 controlli, denominati Critical Security Control (CSC), ordinato sulla base dell'impatto sulla sicurezza dei sistemi. La scelta di prenderlo a riferimento trova giustificazione, oltre che nella larga diffusione ed utilizzo pratico, dal fatto che esso nasce con una particolare sensibilità per i costi di vario genere che l'implementazione di una misura di sicurezza richiede, correlata ai benefici che per contro è in grado di offrire.

Gli 8 ABSC

Sulla base del SAN20 AgID ha definito 8 Basic Security Control(s) (ABSC) validi per la Pubblica Amministrazione italiana.

I primi 5 ABSC corrispondono esattamente ai primi 5 CSC, i quali sono considerati indispensabili per assicurare il minimo livello di protezione nella maggior parte delle situazioni. Il CSC è stato però concepito essenzialmente nell'ottica di prevenire e contrastare gli attacchi cibernetici, ragione per la quale non viene data particolare rilevanza agli eventi di sicurezza dovuti a casualità quali guasti ed eventi naturali. Per questo ai controlli delle prime 5 classi AgID ha aggiunto il CSC8 relativo alle difese contro i malware, il CSC10 relativo alle copie di sicurezza e il CSC13 riferito alla protezione dei dati rilevanti contro i rischi di esfiltrazione.

Gli 8 ABSC per la Pubblica Amministrazione sono dunque:

- 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;

Ognuno di questi 8 ABSC è suddiviso a sua volta, come dicevamo, nei livelli Minimo, Standard e Avanzato.

Vediamoli insieme uno ad uno soffermandoci brevemente sulle Misure minime indispensabili per qualsiasi Pubblica Amministrazione indicate direttamente dall'AgID nelle tabelle di riferimento.

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

L'ABSC 1 (CSC 1) prevede la gestione attiva di 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.

Le Misure minime di sicurezza impongono alle Pubbliche Amministrazioni di:

- implementare un inventario delle risorse attive;
- aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete;
- gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.

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

L'ABSC 2 (CSC 2) prevede che siano gestiti attivamente (inventariati, tracciati e corretti) 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.

Le Misure minime che le Pubbliche Amministrazioni devono adottare sono:

- stilare un elenco di software autorizzati (e relative versioni) necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'istallazione di software non compresi nell'elenco;
- eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.

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

L'ABSC 3 (CSC 3) prevede di 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 rigorosa, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.

Le Misure minime di sicurezza sono:

- utilizzare configurazioni sicure standard per la protezione dei sistemi operativi;
- definire e impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione;
- ripristinare utilizzando la configurazione standard eventuali sistemi in esercizio che vengano compromessi;
- memorizzare offline le immagini d'installazione;

- eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (su protocolli intrinsecamente sicuri, ovvero su canali sicuri).

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

L'ABSC 4 (CSC 4) implica 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.

Per questo controllo AgID individua queste Misure minime:

- ad ogni modifica significativa della configurazione è necessario eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche;
- assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza;
- installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni;
- assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità;
- verificare che le vulnerabilità emerse dalle scansioni siano state risolte per mezzo di patch o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio;
- definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (come server esposti, server interni, PdL, portatili, etc.);
- attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.

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

L'ABSC 5 (CSC 5) definisce regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.

Le Misure minime relative a questo controllo sono:

- limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi;
- utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato;
- mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata;
- prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso;
- quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (ad esempio di almeno 14 caratteri);
- assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging);

- impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history);
- assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse;
- tutte le utenze, in particolare quelle amministrative, devono essere nominative e riconducibili ad una sola persona;
- le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, devono essere utilizzate solo per le situazioni di emergenza e le relative credenziali devono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso;
- conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza;
- se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.

ABSC 8 (CSC 8) - difese contro i malware

L'ABSC 8 (CSC 8) prevede di 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.

L'AgID stabilisce come Misure minime di sicurezza le seguenti azioni:

- installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico;
- installare su tutti i dispositivi firewall ed IPS personali;
- limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali;
- disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili;
- disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file;
- disattivare l'apertura automatica dei messaggi di posta elettronica;
- disattivare l'anteprima automatica dei contenuti dei file;
- eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione;
- filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam;
- filtrare il contenuto del traffico web;
- bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).

ABSC 10 (CSC 10) - copie di sicurezza

L'ABSC 10 (CSC 10) riguarda le procedure e gli strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.

Le Misure minime relative sono:

- effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema;

- assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud;
- assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.

ABSC 13 (CSC 13) - protezione dei dati

Infine, l'ABSC 13 (CSC 13) riguarda i processi interni, gli strumenti e i sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti.

Le Misure minime cui le Pubbliche Amministrazioni devono adempiere sono:

- effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica;
- bloccare il traffico da e verso URL presenti in una blacklist.

Conclusioni

Con l'ABSC 13 siamo arrivati alla fine di questo video. Abbiamo visto insieme cosa sono le Misure minime di sicurezza ICT stabilite dall'AgID, la loro modularità e i loro livelli di adozione. Abbiamo poi analizzato gli 8 ABSC in cui le Misure minime si dettagliano. La sicurezza informatica è un aspetto che diviene sempre più fondamentale per la Pubblica Amministrazione, in parallelo con la sua progressiva digitalizzazione. Ti invito quindi a studiarlo con particolare attenzione!

Grazie per la tua presenza e a presto.