Misure minime di sicurezza ICT per le pubbliche amministrazioni

Premessa

Con la Circolare nr. 2/2017 del 18 aprile 2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni", l'AgID ha individuato un elenco di misure, raggruppate per classi di controlli, utili ai fini della riduzione e prevenzione dei rischi derivanti da attacchi ai sistemi informatici, che possono pregiudicare l'integrità dei dati trattati e la continuità operativa dell'amministrazione medesima.

Ogni classe di controllo si compone di una serie di misure classificate in base ai seguenti livelli di sicurezza:
- M: minimo
- S: standard
- A: avanzato

Le misure definite "minime", sono da considerarsi obbligatorie per qualsiasi tipo di amministrazione.

Nella tabella successiva è riportato, per ogni classe di controlli, l'elenco delle misure "minime" di sicurezza.

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI	
1.1.1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4
1.3.1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.
1.4.1	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.
ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI	
2.1.1	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'installazione di software non compreso nell'elenco.
2.3.1	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	
3.1.1	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.
3.2.1	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di

	sistemi usati dall'organizzazione.
3.2.2	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.
3.3.1	Le immagini d'installazione devono essere memorizzate offline.
3.4.1	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).
ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	
4.1.1	Ad ogni modifica significativa della configurazione 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.
4.4.1	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.
4.5.1	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.
4.5.2	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.
4.7.1	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.
4.8.1	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).
4.8.2	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	
5.1.1	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.
5.1.2	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.
5.2.1	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.
5.3.1	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.

5.7.1	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).
5.7.3	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).
5.7.4	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).
5.10.1	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.
5.10.2	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.
5.10.3	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.
5.11.1	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.
5.11.2	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.
ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE	
8.1.1	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.
8.1.2	Installare su tutti i dispositivi firewall ed IPS personali.
8.1.3	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.
8.7.1	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.
8.7.2	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.
8.7.3	Disattivare l'apertura automatica dei messaggi di posta elettronica.
8.7.4	Disattivare l'anteprima automatica dei contenuti dei file.
8.8.1	Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.
8.9.1	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.
8.9.2	Filtrare il contenuto del traffico web.
8.9.3	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	
10.1.1	Effettuare almeno settimanalmente una copia di sicurezza, quanto meno delle informazioni strettamente necessarie per il completo ripristino del sistema.
10.3.1	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.
10.4.1	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	
13.1.1	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.
13.8.1	Bloccare il traffico da e verso url presenti in una blacklist.

Adempimenti

Entro la data del 31/12/2017, l'amministrazione deve attuare le misure che ritiene più idonee e dare evidenza dell'attuazione e della modalità di implementazione, mediante la redazione del "Modulo di di implementazione delle misure minime di sicurezza" (allegato 2 alla suddetta circolare).

L'attuazione delle suindicate misure ricade sul responsabile per la transizione digitale (figura prevista dall'art.17 del D.Lgs.82/2005, Codice dell'Amministrazione Digitale) o, in sua assenza,sul dirigente allo scopo designato.

Sul modulo di implementazione, per ogni misura adottata, occorre riportare una descrizione sintetica delle modalità di attuazione.

Nel modello proposto da Argo, all'interno dell'applicativo Privacy Web, per ogni misura sono previsti diversi stati:
- implementata;
- in corso da implementazione (nel caso la misura non abbia ancora piena efficacia);
- da implementare (nel caso l'adozione della misura rientri nei piani di miglioramento dell'organizzazione);
- non applicabile (nel caso non sussistano le condizioni per dare attuazione alla misura);
- non implementata.

Per le misure minime previste dalle linee guida AgID, lo stato di ogni singola misura è preimpostato a "implementata" e nelle modalità di implementazione, viene descritta una possibile modalità di attuazione, eventualmente modificabile dall'utente qualora non corrisponda al sistema implementato dall'organizzazione.

L'utente può naturalmente procedere alla compilazione anche delle misure di livello superiore, qualora siano state realizzate o se ne preveda l'attuazione nel breve-medio periodo.

Il modulo compilato va firmato digitalmente dal responsabile per la transizione e dal rappresentante legale dell'amministrazione, quindi, marcato temporalmente o protocollato e conservato a norma.

E' da evidenziare che la circolare non prevede sanzioni per la mancata compilazione del modulo, ma è chiaro che la finalità del documento è quella di dimostrare l'attenzione dell'amministrazione sul tema della sicurezza informatica e della protezione dei dati.

Aggiornamento del modulo

Il modulo "certifica" lo stato di attuazione delle misure di sicurezza dell'amministrazione, pertanto va aggiornato ad ogni variazione dello stato e delle modalità di implementazione delle misure.

Cosa fare in caso di incidente informatico

Al verificarsi di un grave incidente informatico, tale per cui si registra la perdita o sottrazione di dati personali, l'amministrazione deve segnalare l'incidente al CERT-PA, inviando anche il modulo di implementazione.

Suggerimenti per l'implementazione delle misure e la compilazione del modulo

Oltre al responsabile per la transizione, le figure da coinvolgere nell'implementazione delle misure e nella redazione del modulo sono sicuramente gli amministratori di sistema e gli installatori\manutentori della rete e dei dispositivi informatici.
E', inoltre, necessario adeguare le lettere di nomina dei responsabili esterni al trattamento e degli amministratori, includendo le istruzioni necessarie all'implementazione delle misure minime.
Nel caso di servizi "cloud" si consiglia, infine, di acquisire da parte del fornitore del servizio una informativa o dichiarazione che attesti la rispondenza dei servizi alle misure minime di sicurezza.

Applicativo Argo Privacy Web, previsto l'aggiornamento per l'adempimento

Vi comunichiamo che le funzionalità di gestione e stampa del modulo di implementazione delle misure minime richieste dall'AgID saranno rilasciate con la versione 1.8.0 dell'applicativo.

Con la versione 2.0 è, invece, prevista una profonda revisione dell'applicativo per adeguarlo ai requisiti richiesti dal nuovo Regolamento Europeo in materia di protezione dati (Regolamento UE 2016/679), la cui applicazione è prevista per il 25 Maggio 2018.

Staff Assistenza Argo