

**Area Sistemi, tecnologie e sicurezza informatica**

**MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI**

(*Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015*)

26 APRILE 2016

**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** | **Min.** |
| 1 | 1 | 1 | Implementare un inventario delle risorse attive correlato a quello ABSC 1.4 | X |
| 3 | 1 | Aggiornare l’inventario quando nuovi dispositivi approvati vengono collegati in rete. | 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. | X |

**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*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ABSC\_ID #** | | |  | **Min.** |
| 2 |  | 1 | Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di si- stema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l’istallazione di software non compreso nell’elenco. | X |
| 3 | 1 | Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autoriz- zato. | X |

**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 vul- nerabilità di servizi e configurazioni.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ABSC\_ID #** | | |  | **Min.** |
| 3 | 1 | 1 | Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi. | X |
| 2 | 1 | Definire ed impiegare una configurazione standard per workstation, server e altri tipi di si- stemi usati dall’organizzazione. | X |
| 2 | Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzan- do la configurazione standard. | X |
| 3 | 1 | Le immagini d’installazione devono essere memorizzate offline. | X |
| 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). | X |

**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.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ABSC\_ID #** | | |  | **Min.** |
| *4* | *4* | *1* | Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente ag- giornati con tutte le più rilevanti vulnerabilità di sicurezza. | X |
| *5* | *1* | Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema opera- tivo sia per le applicazioni. | X |
| *2* | Assicurare l’aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità. | X |
| 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 ra- gionevole rischio. | X |
| *8* | *1* | Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabi- lità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.). | X |
| *2* | Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al ri- schio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche. | X |

**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.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ABSC\_ID #** | | |  | **Min.** |
| *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. | X |
| *2* | Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato. | X |
| *2* | *1* | Mantenere l’inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata. | X |
| *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. | X |
| *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). | X |
| *3* | Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging). | X |
| *4* | Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history). | X |
| *10* | *1* | Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministra- tori, alle quali debbono corrispondere credenziali diverse. | X |
| *2* | Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconduci- bili ad una sola persona. | X |
| *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. | X |
| *11* | *1* | Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza. | X |
| *2* | Se per l’autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette. | X |

**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.*

|  |  |  |
| --- | --- | --- |
| **ABSC\_ID #** |  | **Min.** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 8 | *1* | *1* | Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloc- care l’esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico. | X |
| *2* | Installare su tutti i dispositivi firewall ed IPS personali. | X |
| *3* | *1* | Limitare l’uso di dispositivi esterni a quelli necessari per le attività aziendali. | X |
|  | *7* | *1* | Disattivare l’esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili. | X |
| *2* | Disattivare l’esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file. | X |
| *3* | Disattivare l’apertura automatica dei messaggi di posta elettronica. | X |
| *4* | Disattivare l’anteprima automatica dei contenuti dei file. | X |
| *8* | *1* | Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione. | X |
| *9* | *1* | Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destina- tario, prevedendo anche l’impiego di strumenti antispam. | X |
| *2* | Filtrare il contenuto del traffico web. | X |
| *3* | Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente ne- cessaria per l’organizzazione ed è potenzialmente pericolosa  (e.g. .cab). | X |

**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.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ABSC\_ID #** | | | **Descrizione** | **Min.** |
| 10 | *1* | *1* | Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni stretta- mente necessarie per il completo ripristino del sistema. | X |
| *3* | *1* | Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante ade- guata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud. | X |
| *4* | *1* | Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente ac- cessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza. | X |

**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*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ABSC\_ID #** | | | **Descrizione** | **Min.** |
| 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. | X |
| *8* | *1* | Bloccare il traffico da e verso url presenti in una blacklist. | X |