Requisiti minimi agid

Inventario dei dispositivi autorizzati e non autorizzati

```
  • Implementare un inventario delle risorse attive correlato a quello ABSC
1.4
  • 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.
```

Inventario dei software autorizzati e non autorizzati

```
  • 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.
  • Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza
di software non autorizzato.
```

Proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server

```
  • Utilizzare configurazioni sicure standard per la protezione dei sistemi
operativi.
  • Definire ed impiegare una configurazione standard per workstation,
server e altri tipi di sistemi usati dall'organizzazione.
  • Eventuali sistemi in esercizio che vengano compromessi devono essere
ripristinati utilizzando la configurazione standard.
  • Le immagini d'installazione devono essere memorizzate offline.
  • 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).
```

Valutazione e correzione continua della vulnerabilità

```
  • 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.
  • 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 sia 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 (e.g. 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.

Uso appropriato dei privilegi di amministratore

• 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 (e.g. 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, debbono essere nominative e riconducibili ad una sola persona.
• 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.
• 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.

Difese contro i malware

• 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).

Copie di sicurezza

- 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.

Protezione dei dati

- 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.