| | |
|---|---|
| | sistema senza perdita di informazione o interruzione di servizi, procedendo tempestivamente alla sostituzione del disco guasto.<br><br>Ciò si applica sia ai dischi locali al sistema, sia a quelli disponibili in rete attraverso sistemi di Storage Area Networks. |

### 5.2.2 Hardening

| **Hardening del sistema** | |
|---|---|
| **Minaccia** | - Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, interfacce amministrative, ecc.).<br>- Accesso non autorizzato alle informazioni.<br>- Furto di credenziali di autenticazione (ad es. con tecniche di brute-force o password crackers).<br>- Negazione dei servizi.<br>- Cancellazione o furto di informazioni.<br>- Attacchi all'integrità dei sistemi (BIOS, software di base, configurazioni).<br>- Attacchi all'integrità delle informazioni<br>- Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione.<br>- Violazione di leggi, di regolamenti, di obblighi contrattuali. |
| **Contromisure** | Consolidare la sicurezza di base del sistema implementando dei meccanismi di protezione atti a contrastare in maniera più efficace eventuali attacchi e limitarne la capacità di azione. I principali interventi da intraprendere sono:<br>- attivare una password a protezione del BIOS in modo da prevenire alterazioni alla configurazione di avvio del sistema;<br>- impedire l'uso di password vuote;<br>- configurare il sistema affinché obblighi all'uso di password "robuste" (es. almeno una maiuscola, una minuscola, un numero e un carattere speciale, e almeno 8 caratteri di lunghezza);<br>- cambiare le password di default delle utenze di sistema e di quelle applicative in uso;<br>- disabilitare le utenze di sistema e quelle applicative predefinite e non utilizzate;<br>- installare gli aggiornamenti di sicurezza più recenti sia durante la fase di installazione iniziale, prima di iniziare ad utilizzare il sistema, sia regolarmente e periodicamente, quando il sistema è in uso;<br>- disattivare o rimuovere le funzionalità non utilizzate, inclusi protocolli di comunicazione, servizi, software, interfacce di rete, interfacce hardware (es. porte seriali e parallele, cd-rom se non usati, porte usb se non permesse, ecc.);<br>- assicurarsi che i permessi d'accesso (lettura, scrittura, modifica, etc.) al file system siano concessi secondo la profilatura degli utenti accreditati, evitando la presenza di condivisioni accessibili indiscriminatamente da tutti gli utenti dell'organizzazione, o senza autenticazione, o scrivibili da chiunque;<br>- bloccare tutte le porte di comunicazione non utilizzate sul firewall di rete e su quelli degli host server (se presenti). |

| **Hardening del sistema** | |
|---|---|
| **Minaccia** | - Negazione dei servizi (es. fault per buffer overflows).<br>- Attacchi all'integrità dei sistemi (BIOS, software di base, configurazioni). |
| **Contromisure** | - Rendere certe pagine di memoria, come quelle contenenti stack e heap, non eseguibili. In generale, utilizzare un meccanismo di Data Execution Prevention (DEP) o l'opzione kernel ExecShield per limitare attacchi di iniezione di codice. |

| | |
|---|---|
| | - Utilizzare meccanismi di address space layout randomization (ASLR) o l'opzione del kernel per il Randomized Virtual Memory Region Placement, nelle modalità più restrittive supportata da ciascun sistema operativo. |

| **Hardening del protocollo TCP/IP** | |
|---|---|
| **Minaccia** | Negazione dei servizi (Denial of Service). |
| **Contromisure** | - Disabilitare l'IP forwarding al fine di impedire che il server in esame possa essere utilizzato come "testa di ponte" per attacchi verso ulteriori sistemi nella rete interna.<br>- Disabilitare il source routing, inibendo la possibilità ad un utente malintenzionato di specificare le rotte da percorrere in fase di connessione verso un sistema.<br>- Abilitare i log per i pacchetti di rete ricevuti aventi un indirizzo di origine non-routable (privo di una rotta in tabella di routing). Questa contromisura aiuta ad individuare attacchi basati sull'IP spoofing.<br>- Abilitare i TCP SYN cookies per la gestione efficiente dell'handshake TCP SYN/ACK, in presenza di attacchi DOS specifici.<br>- Disattivare la funzione di risposta alle richieste ICMP via broadcast.<br>- Filtrare i pacchetti IP in modo che siano consentite solo le richieste ICMP provenienti da indirizzi IP appartenenti al piano d'indirizzamento aziendale.<br>- Attivare la funzione di Quality of Service (QoS) e limitare, con valori idonei, l'ampiezza della banda di rete destinata al protocollo ICMP, ad esempio mediante tecniche di Committed Access Rate (CAR). |

| **Hardening del sistema** | |
|---|---|
| **Minaccia** | Accesso non autorizzato alle informazioni (es. da Memory dump attack). |
| **Contromisure** | Sui sistemi operativi server è necessario, se possibile tecnicamente e se consentito dalle regole del supporto tecnico dei fornitori, disabilitare la generazione dei dump di memoria di sistema ("core dump").<br>Laddove ciò non fosse possibile, è necessario configurare i sistemi in modo che i dump contengano la minor quantità possibile di informazioni sensibili.<br>In ogni caso, i dump di memoria possono essere inviati ai fornitori solo in presenza di un accordo di riservatezza e con modalità di trasmissione atte a garantirne la riservatezza. |

| **Hardening del sistema** | |
|---|---|
| **Minaccia** | - Compromissione delle comunicazioni. (es. Cache poisoning)<br>- Falsificazione di identità.<br>- Furto di credenziali di autenticazione.<br>- Negazione dei servizi.<br>- Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (da Malware). |
| **Contromisure** | - Assicurarsi di utilizzare versioni di software DNS più recenti ed installare tutte le patch di sicurezza disponibili;<br>- Rimuovere dal server DNS qualsiasi altro servizio e software non necessari al suo funzionamento;<br>- Proteggere i server DNS con un firewall perimetrale;<br>- Configurare i server DNS in modo tale da fare il meno affidamento possibile nei rapporti di fiducia con altri server DNS;<br>- Configurare il DNS server in modo tale da limitare query ricorsive, memorizzare solo i dati relativi a domini richiesti e limitare la risposta al fine di fornire |

| | |
|---|---|
| | informazioni inerenti al solo dominio richiesto. Assicurarsi che non ci siano servizi attivi sul DNS che non sono utilizzati;<br>- Utilizzare DNSSEC;<br>- Utilizzare ARP e tabelle IP statiche sul server DNS;<br>- Utilizzare comunicazioni crittografate con SSH per accedere al server DNS. |

| **Hardening del sistema** | |
|---|---|
| **Minaccia** | - Perdita di riservatezza delle informazioni sulla rete e sui sistemi.<br>- Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (attacchi da Malware). |
| **Contromisure** | Configurare i sistemi operativi, in particolare quelli che ospitano il software di rete (ad esempio il firewall) o esposti sulla rete, per impedire il footprinting disabilitando i protocolli e le porte inutilizzate che possono rivelare informazioni sul sistema, sui servizi installati, sulle versioni utilizzate, sul posizionamento dei sistemi e sulla logistica degli uffici, ecc. |

| **Hardening del sistema** | |
|---|---|
| **Minaccia** | Negazione dei servizi. |
| **Contromisure** | - Configurare le applicazioni, i servizi e il sistema operativo tenendo sempre presente le possibili esposizioni ad attacchi DoS.<br>- Ad es. è opportuno utilizzare estesamente architetture di tipo "stateless" o "RESTful" perché l'esaurimento delle risorse di sistema creando un numero elevato di false sessioni su sistemi che memorizzano lo stato di ciascuna di esse è una tecnica di attacco molto diffusa.<br>- Assicurarsi che i criteri di blocco dell'account predisposti non possano essere sfruttati per bloccare service accounts ben noti (quindi il blocco di un account in caso di ripetuti tentativi di accesso deve essere temporaneo, e tra un tentativo e l'altro deve essere imposto un ritardo dell'ordine dei secondi).<br>- Assicurarsi che il sistema sia in grado di gestire alti volumi di traffico e che le soglie massime per le risorse siano opportunamente impostate per gestire carichi anormalmente elevati. A tale scopo è necessario effettuare periodicamente il monitoraggio del carico sull'applicazione in condizioni realistiche per verificare il corretto dimensionamento del sistema in termini di risorse quali memoria RAM e CPU, numero di sessioni concorrenti gestite e tempi di connessione e di risposta effettivi in presenza di picchi di carico. |

| **Hardening del sistema** | |
|---|---|
| **Minaccia** | - Negazione dei servizi (es. fault per buffer overflows).<br>- Attacchi all'integrità dei sistemi. |
| **Contromisure** | Disabilitare tutti i protocolli e i servizi legacy non sicuri, quali ad es. Telnet, FTP, r-commands, SNMP v1, ecc. |

| **Hardening del sistema** | |
|---|---|
| **Minaccia** | - Negazione dei servizi (es. fault per buffer overflows).<br>- Attacchi all'integrità dei sistemi (software e configurazioni).<br>- Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.).<br>- Uso non autorizzato di privilegi. |
| **Contromisure** | Assicurarsi che la variabile d'ambiente PATH (usata su UNIX e Windows per accedere |

| | |
|---|---|
| | alle utilità di sistema da una finestra di terminale interattivo), non contenga percorsi sospetti né percorsi scrivibili da chiunque, ma solo quelli standard previsti dallo specifico sistema operativo. In particolare il PATH non deve mai contenere il percorso "." che rappresenta la directory corrente.<br>Su UNIX e Linux in particolare, l'utenza di root deve avere la variabile di ambiente PATH definita ad esempio come *PATH="/usr/bin:/usr/sbin:/sbin"*. |

| **Disabilitazione delle interfacce di rete inutilizzate** | |
|---|---|
| **Minaccia** | - Negazione dei servizi (es. fault per buffer overflows).<br>- Attacchi all'integrità dei sistemi.<br>- Accesso non autorizzato ai sistemi. |
| **Contromisure** | Disabilitare le interfacce wireless non necessarie al corretto funzionamento del server. Ciò include le interfacce WiFi, Bluetooth e di altri protocolli wireless, ivi compresi quelli proprietari usati da mouse e tastiere wireless, su sistemi server e su Workstation critiche.<br>Per quanto riguarda tastiere e mouse wireless sulle postazioni desktop (non server) è preferibile usare dispositivi bluetooth che consentano di utilizzare l'autenticazione e la crittografia della comunicazione. |

| **Anti-spam** | |
|---|---|
| **Minaccia** | - Negazione dei servizi (es. fault per buffer overflows).<br>- Abuso di risorse. |
| **Contromisure** | Sui sistemi Linux e UNIX in genere, i Mail Transfer Agents o MTA (ad es. Sendmail e Postfix) sono usati per ricevere email in entrata e trasferire I messaggi all'utente o al mail server di destinazione.<br>Se il sistema non è un mail server o un SMTP relay, l'MTA deve essere configurato per processare solo le mail generate localmente al sistema (ad es. da applicative che generano un errore e inviano un messaggio a root per scopi di diagnostica). |

| **Hardening del sistema** | |
|---|---|
| **Minaccia** | - Accesso non autorizzato alle informazioni - Cold boot attack<br>- Accesso non autorizzato ai sistemi |
| **Contromisure** | - Utilizzare meccanismi di crittografia dei dischi di sistema (es. BitLocker);<br>- Assicurarsi che tutti i dischi crittografati siano smontati (protetti) quando il computer è in una posizione in cui può essere rubato. Tipicamente ciò non è possibile con il disco su cui il sistema operativo è in esecuzione;<br>- Impiegare un meccanismo di autenticazione a due fattori per l'avvio del sistema, ad esempio un PIN di pre-avvio o un dispositivo USB rimovibile contenente una chiave di avvio;<br>- Assicurarsi che il computer abbia completato la procedura di arresto prima di lasciarlo incustodito;<br>- Sui sistemi UNIX inserire un controllo di autenticazione per accedere in single user mode e disabilitare il boot interattivo (che consente di presentare un prompt interattivo di amministratore senza autenticazione);<br>- Quando è previsto che il Sistema Operativo passi in modalità di sospensione a seguito di un periodo di inutilizzo, configurarlo invece per l'arresto completo;<br>- Applicare le patch per kernel Linux quali TRESOR e Loop-Amnesia che modificano il |

| | |
|---|---|
| | kernel del sistema operativo in modo tale da utilizzare i registri della CPU (nel caso TRESOR registri di debug x86 e, in caso di Loop-Amnesia, i registri di profilazione AMD64 o EMT64) per memorizzare le chiavi di crittografia, piuttosto che memorizzarle in RAM;<br>- Seguire l'approccio denominato "frozen cache" conosciuto anche come "cache as RAM", con il quale si disattiva la cache L1 della CPU per poterla utilizzare come supporto di memorizzazione delle chiavi di crittografia. Ovviamente questo approccio è oneroso dal punto di vista delle performance, ma si può ovviare a ciò utilizzando CPU multicore in cui tale cache viene disattivata per un solo core; Impiegare hardware in cui i moduli di memoria RAM sono saldati o incollati nel socket della scheda madre. |

| **Inibizione dei terminali non in uso** | |
|---|---|
| **Minaccia** | Accesso non autorizzato ad informazioni, causato dal personale utente per inadeguati meccanismi, strumenti, procedure o abilità tecniche atti a prevenire l'accesso non autorizzato al sistema. |
| **Contromisure** | Tutti gli utenti devono essere sensibilizzati sui requisiti e sulle procedure di sicurezza per proteggere le apparecchiature incustodite.<br>Le postazioni di lavoro e i sistemi informativi di qualsiasi tipo dotati di un terminale video e una tastiera, devono essere configurati in modo da bloccare la sessione di login e richiedere la password utente quando il sistema viene lasciato incustodito o inattivo per oltre 5 minuti.<br>Ciò si applica specialmente ai sistemi server, anche se posizionati in data center o in zone ad accesso ristretto. |

| **Limitazione del tempo di connessione** | |
|---|---|
| **Minaccia** | - Accesso non autorizzato ad informazioni.<br>- Abuso di privilegi. |
| **Contromisure** | Sui sistemi più critici, laddove sia prevista una durata massima per lo svolgimento di determinati compiti, o quando l'uso di tali sistemi sia consentito solamente in certi orari, alla scadenza temporale prevista deve essere effettuato un logout automatico. |

| **Limitazione dell'uso delle utility/servizi di sistema** | |
|---|---|
| **Minaccia** | - Accesso non autorizzato ad informazioni.<br>- Abuso di privilegi.<br>- Errori di amministrazione dei sistemi.<br>- Uso non autorizzato di privilegi. |
| **Contromisure** | Limitare l'uso delle utility/servizi di sistema attraverso:<br>- sistemi di identificazione e autenticazione per l'uso delle utility/servizi;<br>- separazione delle utility di sistema dalle applicazioni;<br>- autorizzazione all'uso delle utility/servizi solo per chi ne ha la reale necessità (compreso l'orologio di sistema);<br>- tracciamento di ogni operazione privilegiata svolta con l'uso delle utility/servizi;<br>- rimozione di tutte le utility/servizi non strettamente necessarie (in particolare i servizi di RAS o dial-up, gestione remota, ecc.);<br>- disabilitazione di tutte le porte non necessarie;<br>- rimozione di tutti gli strumenti di sviluppo (compilatori e interpreti) su sistemi destinati ad ambienti di test, collaudo, certificazione e produzione. |