

- Le registrazioni dei log degli amministratori devono essere conservate per un congruo periodo, non inferiore a sei mesi, in conformità alla normativa in materia di protezione dei dati personali (Privacy) e dei principi di sicurezza.
- Tracciare le operazioni critiche eseguite a livello applicativo.
- Eseguire un regolare backup dei file di log e analizzarli regolarmente per verificare la presenza di attività sospette.

#### Protezione log

##### Minaccia

- Abuso di privilegi da parte dell'utente.
- Negazione dei servizi (ad es. da errori hardware/software non rilevati in maniera tempestiva o corretta per carenze di monitoraggio nei sistemi ICT).
- Accesso non autorizzato alle informazioni.
- Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, ecc.).
- Violazione di leggi, di regolamenti, di obblighi contrattuali.

##### Contromisure

Controllare che le informazioni contenute nei file di log siano protette da manomissioni e accessi non autorizzati e che non ci siano problemi operativi con le logging facilities. In particolare, occorre verificare che non vi sia:

- alterazione delle informazioni tracciate nel file di log;
- discordanza fra il periodo di conservazione dei log e quanto indicato dalle policy di retention o specifiche disposizioni legali;
- fallimento delle operazioni di registrazione degli eventi causato da un raggiungimento della dimensione massima del file di log;
- sovrascrittura delle informazioni precedentemente tracciate causata da un raggiungimento della dimensione massima del file di log, nel caso in cui la scrittura dei log sia effettuata in modo ciclico sempre sullo stesso file.

#### Registrazione degli accessi logici da parte degli amministratori di sistema

##### Minaccia

- Abuso di privilegi da parte dell'utente;
- Cancellazione dei log di accountability e/o ripudio di operazioni effettuate.

##### Contromisure

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) al sistema/piattaforma da parte degli amministratori di sistema. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate.

Si tenga presente che il controllo e la registrazione possono essere aggirati da un account condiviso (questo vale sia per gli account amministrativi che per gli account utente / applicativi / di servizio): pertanto gli account amministrativi non devono essere condivisi.

In generale, anche per gli account utente non privilegiati e per gli account usati dagli applicativi per l'esecuzione dei servizi in uno specifico contesto (es. account httpd per un server web in ambito UNIX), devono essere nominativi / specifici per l'utente o l'applicativo e non condivisi.

### 5.1.7 Procedure

#### Change management

##### Gestione dei cambiamenti

##### Minaccia

- Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, ecc.).
- Accesso non autorizzato alle informazioni.
- Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione.