REGOLAMENTO DEL PROCESSO DI
Log Management

Procedura emessa il 27/09/2022

Owner della procedura: IT Operation Security & Governance

Indice

1 OBIETTIVO DEL DOCUMENTO

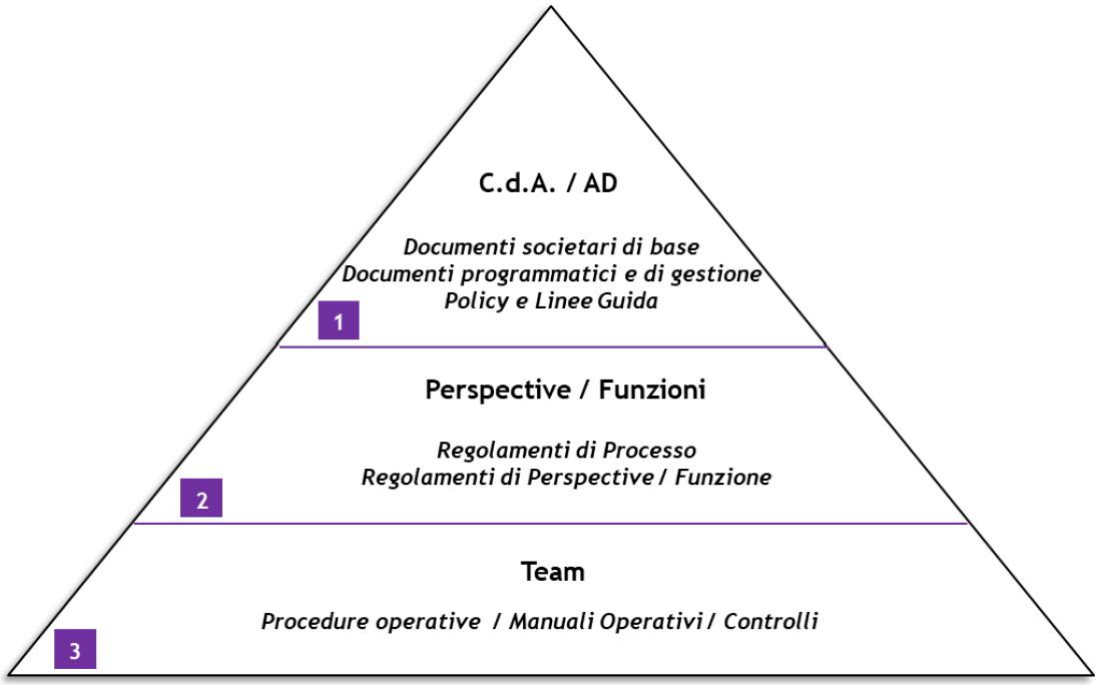
Il *Logging* è il processo mediante il quale i sistemi, i database, le applicazioni o i dispositivi di rete tengono traccia degli eventi di sicurezza (come accessi, logoff, ecc.) generati dagli utenti, dai servizi e dai processi, memorizzando le informazioni all'interno di un file protetto, di una tabella di database, o altri sistemi. Tale meccanismo consente il monitoraggio di determinate attività all'interno del sistema.

L'attività di monitoraggio permette di analizzare gli eventi di sicurezza che si sono verificati al fine di identificare le fonti da cui scaturiscono i problemi, che potranno così essere indirizzati e corretti.

Obiettivo del documento è, quindi, di regolamentare la gestione dei Log all'interno dell'organizzazione con riferimento a tutte le fasi di generazione, trasmissione, archiviazione, analisi e cancellazione e più in dettaglio:

- descrivere le categorie in cui sono raggruppati i Log, con particolare riferimento alla loro fonte, al loro contenuto, alla loro localizzazione, al periodo di retention e alle regole di accesso;
- indicare le regole di sicurezza che dovranno essere osservate per la protezione dei log sui sistemi, in memoria ed in transito;
- descrivere il processo di gestione dei Log suddiviso nelle fasi di: generazione, elaborazione, conservazione, analisi e cancellazione;
- descrivere l'attività di controllo legata all'analisi dei Log.

Con riferimento alla "Policy di Gruppo sulle modalità di redazione, approvazione, diffusione ed aggiornamento della Normativa Interna", il presente documento si colloca al secondo livello della piramide documentale richiamata nello schema seguente.



2 AMBITO DI APPLICAZIONE

Il presente documento si applica a Flowe S.p.A. Società Benefit.

3 AGGIORNAMENTO DEL DOCUMENTO

L'aggiornamento del documento è a cura di *IT Operation Security & Governance* che dovrà provvedere a revisionarlo con cadenza almeno annuale o qualora si verifichi un cambiamento sostanziale, che possa influire in modo diretto o indiretto sul processo qui descritto.

4 STRUMENTI A SUPPORTO DEL PROCESSO

Gli strumenti a supporto del processo di gestione dei log sono i seguenti:

- ***Microsoft Sentinel***: soluzione di analisi della sicurezza e intelligence che raccoglie i dati su scala cloud per utenti, dispositivi, applicazioni e infrastruttura (in locale e in cloud), rileva minacce riducendo i falsi positivi, analizza le minacce attraverso l'intelligenza artificiale e risponde rapidamente agli eventi imprevisti.
- ***Microsoft Azure Monitor***: piattaforma di raccolta e analisi per il monitoraggio dei dati di telemetria, collezionati da diverse origini locali e di Azure come applicazioni Web, infrastruttura e rete. La piattaforma valuta il livello delle prestazioni ed identifica ed effettua una diagnostica proattiva dei problemi e degli eventi legati alle risorse da cui dipendono.
- ***Microsoft Azure Application Insight***: è una funzione di Microsoft Azure Monitor che fornisce una gestione delle prestazioni delle applicazioni estendibili e il monitoraggio delle applicazioni web live. L'applicazione consente di rilevare le anomalie nelle prestazioni e di migliorarle, nonché di diagnosticare i problemi.

5 ATTORI, RUOLI E RESPONSABILITA'

Il modello organizzativo adottato dalla Società per la gestione dei Log prevede il coinvolgimento di *IT Operation Security & Governance e* di Organization & Business Continuity, che si impegnano, per quanto di competenza, ad applicare rigorosamente i principi contenuti nel presente documento.

Vengono indicati di seguito i ruoli e le responsabilità dei principali attori coinvolti nel processo di gestione dei log.

5.1 *IT OPERATION SECURITY & GOVERNANCE*

IT Operation Security & Governance ha la responsabilità di:

- Definire la quantità e qualità delle informazioni da raccogliere in relazione ai log rispetto anche alla memoria di archiviazione prevista;
- Stabilire le misure da implementare per l'accesso, la trasmissione e la conservazione

sicura dei log;

- Definire le dashboard utili ai fini del monitoraggio dei log;
- Definire degli alert con delle soglie per intervenire proattivamente all'analisi di eventi anomali;
- Monitorare continuamente lo stato dei sistemi informativi tramite l'ausilio dei log definiti;
- Supportare la funzione di Sicurezza Logica nell'eseguire controlli periodici su determinati tipi di Log (E.g. log degli amministratori di sistema).

5.2 ORGANIZATION & BUSINESS CONTINUITY

Organization & Business Continuity ha la responsabilità di effettuare le attività di verifica periodica circa l'adeguatezza sulle attività delle utenze privilegiate tramite l'ausilio dei log tracciati.

6 TIPOLOGIE DI LOG

I Log che vengono raccolti da Microsoft Azure Monitor possono essere generati da molti asset quali server, software di sicurezza, database e applicazioni IT ospitati in Azure o in locale. Pertanto, a seconda della sorgente, è possibile raggruppare i file di log nelle seguenti macro-categorie:

- **Log di gestione/controllo**: offrono informazioni dettagliate sulle operazioni CREATE, UPDATE e DELETE di Azure Resource Manager. In particolare, rientrano in questa categoria i Log attività di Azure che permettono di determinare "*cosa, chi e quando*" per le operazioni di scrittura eseguite sulle risorse nella sottoscrizione e forniscono aggiornamenti sugli eventi di integrità dei servizi.
- **Log del piano dati**: offrono informazioni sugli eventi generati durante l'utilizzo di una risorsa di Azure registrati dai componenti dei sistemi operativi di host, di server, di stazioni di lavoro e di device di rete. All'interno di questa categoria rientrano il registro eventi di sistema di Windows, il log di sicurezza, il log applicazioni di una macchina virtuale e i log di diagnostica configurati tramite Microsoft Azure Monitor, che contengono informazioni relative ai cambiamenti del dispositivo, ai drivers del dispositivo, alle modifiche di sistema, alle operazioni eseguite dagli utenti sul sistema, all'avvio/arresto di un servizio e altre informazioni relative al sistema operativo
- **Log sugli eventi elaborati**: offrono informazioni sugli eventi o avvisi generati dai software di sicurezza, come software antivirus, firewall e sistemi di rilevamento e prevenzione delle intrusioni. In particolare, rientrano in questa categoria gli avvisi di *Microsoft Defender for Cloud* che forniscono informazioni per identificare gli eventi di sicurezza, rilevare attacchi informatici e analizzare i risultati degli incidenti di sicurezza, fornendo avvisi di sicurezza concisi.
- **Log dei database**: si tratta dei registri generati dai database e contengono i record di qualsiasi utente che tenta di accedervi e le modifiche effettuate al loro interno (inserimento, aggiornamento, eliminazione di record). Questi registri possono essere utilizzati per determinare quali attività sono state avviate sui database e se hanno avuto successo o meno.

- **Log di rilevazione degli accessi delle utenze privilegiate**: si tratta dei registri che contengono informazioni relative all'accesso ai sistemi informatici e agli archivi elettronici da parte delle utenze privilegiate. Questi registri dovrebbero garantire la completezza, l'inalterabilità e l'integrità degli accessi delle utenze privilegiate sul sistema operativo, sui database e sulle applicazioni.

Per quanto riguarda l'App Flowe, la raccolta dei seguenti log viene realizzata tramite lo strumento Azure Application Insight:

- **Log applicativi**: offrono informazioni sulla disponibilità, le prestazioni e l'utilizzo delle applicazioni Web, indipendentemente dal fatto che siano ospitate in Azure o in locale, al fine di monitorare il loro corretto funzionamento e tenere traccia di flussi di metriche live, richieste, tempi di risposta ed eventi come le operazioni eseguite dall'utente nell'utilizzo dell'applicazione/servizio, le informazioni sull'account, e le telemetrie delle componenti applicative.

7 EVENTI DI SICUREZZA REGISTRATI

Di seguito verranno indicati, a titolo esemplificativo, una serie di eventi che vengono registrati a fini di analisi:

- Tentativi di autenticazione falliti o di successo: forniscono informazioni relative a possibili tentativi di accesso non autorizzato alle informazioni o ai sistemi;
- Modifiche effettuate a impostazioni di configurazione, sistemi o processi: forniscono informazioni relative a possibili fenomeni di accesso non autorizzato o abuso di privilegi da parte dell'utente;
- Reimpostazione multipla della password da parte dell'utente: forniscono informazioni rispetto a possibili attacchi di brute force;
- Errori o alert di sistema o di applicazione: forniscono informazioni per verificare le prestazioni attraverso il rilevamento di modelli insoliti nelle metriche o anomalie degli errori, come ad esempio un incremento anomalo della frequenza di richieste non riuscite nell'app Web.
- Alert ricevuti dai controlli di sicurezza come firewall o antimalware: forniscono informazioni relative ad eventuali tentativi di intromissione registrati dal firewall o eventi di sicurezza registrati dall'antimalware;
- Presenza di e-mail contenenti URL malevoli: forniscono informazioni rispetto alla possibile presenza di minacce;
- Rapidi spostamenti tra gli host attraverso i quali gli utenti si connettono: forniscono informazioni rispetto a possibili attività sospette di lateral movement.
- Anomalie connessioni RDP: forniscono informazioni rispetto a possibili intromissioni attraverso remote desktop.
- Attivazione del redirect o del forewarding automatico delle mail.

8 FASI DEL PROCESSO DI LOG MANAGEMENT

Il processo di gestione dei log si suddivide nelle fasi descritte di seguito:

- Generazione ed elaborazione dei log
- Conservazione ed accesso dei log
- Analisi dei log
- Cancellazione dei log

8.1 GENERAZIONE ED ELABORAZIONE DEI LOG

La corretta generazione dei log è un passaggio fondamentale. Pertanto, *IT Operation Security & Governance* è chiamata a stabilire un compromesso tra lo spazio di archiviazione disponibile e la quantità di informazioni contenute nei registri. *IT Operation Security & Governance* identifica il contenuto dei log in base al tipo di sistema operativo/ database/ applicazione e sulla base delle esigenze aziendali (ad es. criticità del sistema, tipo di dati trattati, finalità del sistema, architettura del sistema, ecc.) o delle normative interne esistenti.

Le informazioni che devono essere contenute nel registro sono le seguenti:

- Che tipo di evento si è verificato (ID evento)
- Quando e a che ora si è verificato l'evento (data e ora)
- Dove si è verificato l'evento (indirizzo IP di destinazione)
- Qual è l'evento registrato (descrizione dell'evento)
- La fonte dell'evento (indirizzo IP di origine)
- L'esito dell'evento (successo o fallimento)
- Identità di qualsiasi utente/soggetto associato all'evento (ID utente/ID processo)
- Nomi dei file coinvolti e regole di controllo degli accessi o di controllo dei flussi predisposte

Una volta generati, i log vengono trasmessi al server di gestione centralizzato di Microsoft Azure Monitor e vengono spediti al Microsoft Azure Sentinel (l'utilizzo dei tools citati è regolamentato dal contratto di servizi con Microsoft).

8.2 CONSERVAZIONE ED ACCESSO DEI LOG

I log vengono raccolti ed archiviati in maniera automatica all'interno del cloud.

Il periodo di archiviazione previsto per i log è di massimo 2 anni, scaduto il quale vengono cancellati automaticamente.

L'accesso ai log dev'essere effettuato nel rispetto delle normative vigenti e della privacy, evitando qualsiasi forma di monitoraggio remoto del dipendente. Il trattamento dei log contenenti dati personali è consentito esclusivamente al personale autorizzato ed ogni operazione di accesso viene opportunamente tracciata.

8.3 ANALISI DEI LOG

I log devono consentire l'analisi di eventi attraverso l'individuazione di correlazioni tra due o più voci di registro. L'infrastruttura di Microsoft Azure Monitor consente la generazione in maniera automatica di alert sulla base dei quali è possibile effettuare ulteriori approfondimenti da parte del personale specializzato di *IT Operation Security & Governance* che procederà alle analisi e indirizzerà l'evento nella maniera più opportuna.

Organization & Business Continuity dovrà provvedere al monitoraggio periodico dei log tracciati al fine di verificare l'adeguatezza e la coerenza delle attività effettuate tramite le utenze privilegiate.

I log devono essere estratti in un formato che consenta la visualizzazione a fini di audit. Se i log fossero prodotti in un formato non compatibile, dovranno essere adottati strumenti per convertirli in formato standard (es. Txt, csv, ecc.).

8.4 CANCELLAZIONE DEI LOG

La cancellazione dei log dev'essere effettuata ogniqualvolta tali dati non siano più necessari per lo scopo per il quale sono stati generati.

La cancellazione dei log può avvenire in maniera automatica grazie alle funzionalità di data retention messe a disposizione dalla piattaforma cloud Microsoft Azure (l'utilizzo della piattaforma è regolamentato dal contratto di servizi con Microsoft). Ogni operazione di cancellazione dei log viene tracciata.

9 NORMATIVA

Nel presente capitolo si richiama il contesto normativo di riferimento per le attività in esame. L'elenco fornito non si ritiene esaustivo e viene riportato principalmente allo scopo di richiamare l'attenzione sui principali riferimenti, della normativa generale ed interna aziendale, sui quali si fonda la presente procedura.

Normativa interna:

- Policy di Sicurezza di Flowe

Normativa esterna:

- Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 e successivi aggiornamenti;
- EBA/GL/2017/05 "Orientamenti sulla valutazione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) a norma del processo di revisione e valutazione prudenziale (SREP)" e successivi aggiornamenti; Banca d'Italia Circolare n. 285 del 17 dicembre 2013 – Disposizioni di vigilanza per le Banche e successivi aggiornamenti;
- EBA/GL/2019/02 - Orientamenti in materia di esternalizzazione e successivi aggiornamenti;

- Provvedimento Della Banca d'Italia de 23 luglio 2019, Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica e successivi aggiornamenti;

- Direttiva (UE) 2015/2366 PSD2 – (Payment Services Directive 2) e successivi aggiornamenti;