Security Information & Incident Response

ING. CHRISTIAN FUSCIELLO

Security Incident Response

«*Uno o più eventi di sicurezza informatica inaspettati o non voluti, che hanno significativa probabilità di compromettere le attività aziendali e minacciare la sicurezza delle informazioni*»

Al verificarsi di un evento di questo tipo bisogna essere in grado di verificare rapidamente se si tratta di un incidente informatico e nel caso mettere in atto una serie di metodiche per poter reagire efficacemente alla minaccia rilevata attraverso le cosiddette attività di Incident Response tra cui l'utilizzo di tecniche di Informatica Forense.

Security Incident Response

Incidenti relativi alla sicurezza informatica potrebbero includere attività come:

- Tentativi (falliti o di successo) per ottenere l'accesso non autorizzato ad un sistema o ai suoi dati (Es. *Mossack Fonseca – Panama Papers*)
- Interruzione di servizi (per attacchi DoS o per malfunzionamenti *Es. Google Drive*)
- Uso non autorizzato di un sistema per il trattamento o la conservazione dei dati
- Modifiche al sistema hardware, firmware o le caratteristiche del software senza conoscenza, istruzione, o il consenso del proprietario.

Incident Response

E’ quindi spesso utile dotarsi di un piano di Incident Response delineando come ridurre al minimo la durata ed i danni causati da un incidente, individuando i soggetti interessati ed i partecipanti, semplificando l'analisi forense, accelerando i tempi di recupero.

Il piano deve identificare e descrivere ruoli e responsabilità dei membri del team di Incident Response che sono responsabili per la verifica del piano e della sua attuazione. Il piano dovrebbe anche specificare gli strumenti, le tecnologie e le risorse fisiche che devono essere disponibili per recuperare le informazioni violate.

Incident Response

Secondo il SANS Institute, ci sono sei fasi fondamentali di un piano di risposta:

1. Preparazione: Preparare gli utenti ed il personale IT per gestire potenziali incidenti
2. Identificazione: Determinare se un evento è davvero un incidente di sicurezza
3. Contenimento: limitare i danni dell'incidente, isolando i sistemi interessati per prevenire ulteriori danni

Incident Response

4. Eradicazione: Trovare la causa principale dell'incidente, eliminando sistemi interessati dall'ambiente di produzione

5. Recupero: Permettere ai sistemi interessati di tornare nell'ambiente di produzione, garantendo che non siano rimaste delle minacce

6. Lezioni apprese: Completamento documentazione incidente, effettuare analisi per apprendere le cause, fare esperienza dell'incidente e migliorare i futuri sforzi di risposta

Incident Response - CSIRT

Uno dei layer che molte organizzazioni includono nella loro ottica strategica di sicurezza è la creazione di un Computer Security Incident Response Team detto CSIRT.

Le motivazioni della creazione di queste squadre possono essere riassunte in:

- un aumento generale del numero di incidenti di sicurezza informatica che sono stati segnalati
- un aumento generale del numero e del tipo di organizzazioni minacciate da incidenti di sicurezza informatica

Incident Response - CSIRT

- una consapevolezza più mirata da parte delle organizzazioni sulla necessità di politiche e pratiche di sicurezza come parte delle loro strategie globali di gestione del rischio
- nuove leggi e regolamenti che hanno un impatto su come le organizzazioni sono tenute a proteggere le informazioni
- la presa di coscienza che i sistemi e gli amministratori di rete da soli non possono proteggere i sistemi organizzativi e gli asset.

Incident Response – Security Policy

La Policy sulla Sicurezza Informatica è un documento nel quale sono contenute tutte le disposizioni, comportamenti e misure organizzative richieste ai dipendenti e/o collaboratori aziendali per contrastare i rischi informatici.

Tale regolamento è da consegnare al momento dell'assunzione ad ogni dipendente e da reinviare ogni anno, a cura del Responsabile del Trattamento dei dati, tramite email con i necessari aggiornamenti e da far firmare ai CONSULENTI o COLLABORATORI che accedono alla Rete Aziendale.

Incident Response - Security Policy

Per comprendere l'importanza di avere una Policy sulla Sicurezza Informatica in Azienda è sufficiente considerare questi dati :

- Diverse ricerche effettuate a livello internazionale hanno rivelato che, in mancanza di regole e/o strumenti tecnologici di filtraggio, una percentuale tra il 30% e il 40% del tempo impiegato on line dal dipendente viene utilizzato per fini diversi da quelli aziendali.
- Una recente indagine evidenzia che il 25,1% dei lavoratori dipendenti dichiara di navigare per fini personali dal posto di lavoro da 10 a 30 minuti al giorno, il 22,4% da 30 minuti ad 1 ora, l'11,9% da 1 ora a 2 e ben il 12,6% oltre 2 ore. Solo il 27% dichiara di navigare meno di 10 minuti al giorno.

Incident Response - Security Policy

- Un'indagine interna dell'Internal Revenue Service, l'ente che negli Stati Uniti si occupa delle entrate fiscali, ha rivelato che la navigazione o l'utilizzo di e-mail da parte dei lavoratori per scopi personali rappresentava il 51% del totale del tempo dedicato ad attività on line.
- Più del 70% di tutto il traffico generato dai siti VIETATI AI MINORI viene generato durante l'orario d'ufficio.
- Il 32,6% dei lavoratori che accedono ad Internet durante l'orario di lavoro dichiarano di farlo senza nessuna specifica finalità.
- Il 23% dei dipendenti in europa ha ammesso di aver acquistato un servizio cloud esterno e di utilizzarlo in azienda per archiviare i propri dati insieme a quelli aziendali, in modo non autorizzato.

Incident Response - Security Policy

Gli incidenti di sicurezza provocati accidentalmente da personale interno all'azienda sono in aumento. E possono avere un impatto ben più negativo degli attacchi perpetrati in malafede.

La sicurezza è responsabilità di tutti, non solo degli addetti ai lavori !

Non è più sufficiente garantire una connessione cifrata (VPN) con l'azienda e una protezione da virus e malware, ma è necessario affrontare temi come le garanzie di riservatezza, dentro e fuori l'azienda, mantenere il controllo del livello di sicurezza di applicazioni e dati ospitati su un cloud pubblico o tutelare l'azienda nel caso di utilizzo di strumenti non pensati per la propria utenza (tablet e smartphones).

Incident Response - Security Policy

La policy sulla sicurezza informatica predispone tutte le azioni corrette da compiere per:

A. l'utilizzo del personal computer
B. l'utilizzo della rete
C. la gestione delle password
D. l'utilizzo pc portatili, telefoni fissi, cellulari, fax e fotocopiatrici
E. l'utilizzo della posta elettronica
F. l'uso della rete internet e dei relativi servizi
G. la protezione antivirus e malware

Incident Response – Computer Forensics

A seguito di un incidente vengono spesso impiegate tecniche di analisi forense utili per poter preservare, tramite opportune operazioni la «prova» ovvero i dati contenuti in un determinato dispositivo di memoria. Tali operazioni consistono in primis nell'acquisizione del contenuto del dispositivo con copie bit a bit ottenute nella maggioranza dei casi spegnendo il sistema che li ospita.

Inoltre servono strumenti ad esempio di «write blocking» ed altri tali da poter preservare le informazioni estratte ed essere utilizzate in sede di giudizio.

Incident Response – Computer Forensics

Questo processo richiede altresì personale molto specializzato e presente durante tutte le fasi, oltre al tempo necessario per l'effettuazione dell'indagine. Spegnendo poi la macchina si perdono dati importanti (dati in memoria, processi attivi, connessioni attive etc..).

Tutto questo richiede quindi un dispendio tempo, di risorse e soprattutto di macchine che possono essere analizzate.

Incident Response – Remote Forensics

L'analisi forense remota è stata proposta come soluzione per ridurre il tempo di risposta. Molteplici operazioni semplici possono essere eseguite utilizzando le potenzialità del sistema operativo, come ad esempio l'analisi dei file condivisi su una risorsa di dominio o con dei tool di amministrazione remota (*psexec*, *sleuthkit*).

Tutto questo può essere ottenuto installando un client su ogni macchina, che permette ad un investigatore di collegarsi ed effettuare un'analisi sul sistema.

Incident Response – GRR Rapid Response

GRR nasce come il desiderio di implementare un tool open source che possa scalare migliaia di macchine, possa accedere in modo raw ai dati del disco e della memoria, possa essere gestito tramite interfaccia web e supportare le maggiori piattaforme.

GRR è una piattaforma scalabile, ha tutta una serie di strumenti per facilitare l'analisi forense, spostandosi dal trattare un sistema alla volta ad un modello di analisi forense continua.

Incident Response – GRR Rapid Response

Diversi software per il controllo da remoto necessitano di una connessione di rete stabile; per superare il fatto che non tutti i computer possano essere simultaneamente connessi oppure che parte di loro possano essere fuori sede come i notebook, le modalità di comunicazione di GRR sono molto diverse agli standard finora utilizzati. GRR comunica con i client tramite messaggi, le richieste (quelle inviate dal server ai client) e le risposte (viceversa). Spesso una singola richiesta prevede molteplici messaggi di risposta.

Incident Response – Conclusioni

La Security Incident Response non è un'opzione. Non importa quanto bene sia protetta un'organizzazione, e nonostante il personale qualificato, l'utilizzo di tecnologia appropriata e procedure collaudate il fatto è che non c'è niente a rischio zero.

È impossibile prevedere in modo accurato e coerente, il tipo, la frequenza o la gravità degli attacchi soprattutto con l’evolversi tecnologico.

Security Information & Incident Response

Grazie per l'attenzione!

Ing. Christian Fusciello