Incident Response: dal Processo alle Procedure

Author : Andrea Boggio

Date : 3 ottobre 2018

Premessa

In un precedente articolo dal titolo "**Security Operations Center: il cuore della protezione dell'Informazione**[1]", focalizzato sulle strutture dedicate alla gestione operativa della cyber-security, ho fatto riferimento a processi tipici di un Security Operations Center (SOC). L'assenza di standard di riferimento e di rigide nomenclature promuove una certa libertà di definire i contorni, spesso liquidi e incerti, di entità operative tra loro simili (da cui la frequente interscambiabilità di acronimi quali SOC[2], CERT[3], CSIRT e IRT[4], la cui origine, spesso, non è relativa al contesto ICT[5]): tali entità sono le protagoniste assolute dei processi di *Incident Management*.

Alcune definizioni

Evento

Un evento è un episodio osservabile in un sistema o in una rete. Gli eventi comprendono un utente che si collega a un file condiviso o che invia un messaggio di posta elettronica, un server che riceve una richiesta per una pagina web, un firewall che impedisce un tentativo di connessione. Eventi avversi hanno una conseguenza negativa, quali ad esempio i crash di sistema, i *packet flood***[6]**, l'utilizzo non autorizzato dei privilegi di sistema, l'accesso non autorizzato a dati sensibili e l'esecuzione di codice malevolo finalizzato a distrugge i dati o a prenderli in ostaggio.

Incidente di sicurezza

Un incidente di sicurezza è una violazione o una minaccia imminente di violazione delle politiche di sicurezza e di utilizzo lecito degli strumenti tecnologici. Esempi di incidenti sono:

- un attaccante comanda a una *botnet***[7]** di inviare un elevato volume di richieste di connessione a un web server, causandone il blocco;
- gli utenti sono indotti ad aprire un file di report trimestrale inviato tramite posta

elettronica che, in realtà, incorpora codice malevolo;
- un attaccante ottiene dati sensibili e minaccia di renderli pubblici se l'organizzazione non pagherà una certa somma di denaro;
- un utente fornisce o espone informazioni sensibili verso altri tramite servizi di *file sharing* [8]*peer-to-peer***[9]**.

Incident Management

L'*Incident Management* è la capacità di gestire in modo efficace eventi avversi inaspettati con l'obiettivo di minimizzarne gli impatti e mantenere o ripristinare le normali operazioni all'interno di limiti temporali definiti. Una capacità sostenibile di *Incident Management* richiede l'allocazione di risorse umane e materiali a supporto delle operazioni di business per assicurare la continuità del minimo delle operazioni e contenere le violazioni di sicurezza secondo la strategia di gestione del rischio adottata dall'organizzazione. L'*Incident Management* riguarda tutte le azioni prese prima (inclusi test e pianificazione), durante e dopo il verificarsi di un incidente di sicurezza delle informazioni. Le azioni intraprese dovrebbero essere finalizzate a mitigare l'impatto di un incidente con i seguenti obiettivi:

- fornire uno strumento efficace per indirizzare la situazione in modo tale che l'impatto dell'incidente sia minimo per l'organizzazione;
- fornire al management le informazioni sufficienti per decidere un corso di azione appropriato;
- mantenere o ripristinare la continuità dei servizi dell'organizzazione;
- fornire una difesa contro gli attacchi;
- fornire deterrenza tramite l'utilizzo di tecnologia, investigazione e azioni successive.

Incident Response

L'*Incident Response* è parte del processo di *Incident Management* e può essere definito come la "capacità operativa dell'*Incident Management* che identifica, prepara e risponde agli incidenti per controllare e limitare i danni; fornire capacità investigative e mantenere, recuperare e ripristinare le normali operazioni in accordo ai livelli di servizio (SLA) previsti".

Una *capability* di *Incident Response* dovrebbe includere:

- creazione di una **policy** e di un **piano** di *Incident Response*;
- sviluppo delle **procedure** per garantire il trattamento dell'incidente e il reporting;
- definizione delle linee guida per comunicare con entità esterne all'organizzazione;
- scelta di una struttura di team e un modello di staffing;
- stabilire relazioni e linee di comunicazione tra l'*Incident Response Team* (*IRT*) e altri gruppi, sia interni (dipartimento legale) sia esterni (ad esempio, forze dell'ordine);
- determinare quali servizi dovrebbe erogare l'IRT;
- dedicare appropriate risorse e addestrare il team.

Gli attacchi compromettono frequentemente dati personali e di business e rispondere velocemente ed efficacemente alle violazioni di sicurezza è diventato un fattore critico; il

concetto di incidente di sicurezza informatica è ormai ampiamente noto. Avere una *capability* di *Incident Response* permette di gestire gli incidenti in modo sistematico in maniera tale che siano prese tempestivamente le decisioni appropriate. Una *capability* del genere permette anche di migliorarsi nel tempo e di gestire nel migliore dei modi anche le problematiche di natura legale che possono presentarsi durante le fasi di un incidente.

Contesto operativo

Gli incidenti possono verificarsi in molti modi diversi e non è possibile creare istruzioni universalmente valide per trattare in maniera appropriata ogni incidente. Ci sono diverse tipologie di incidenti basate su **vettori di attacco** comuni, ma si tratta di categorie utili a definire procedure di trattamento specifiche: diversi tipi di incidenti hanno bisogno di diverse strategie di risposta.

I segnali di un incidente ricadono in due categorie: **precursori** e **indicatori**. Un **precursore** è un segnale di un incidente che potrebbe accadere nel futuro, mentre un **indicatore** è un segnale di un incidente che potrebbe già essere accaduto o potrebbe addirittura essere in corso.

Esempio di **precursori** sono:

- log di applicazioni e sistemi che rilevano l'utilizzo di attività di *Information Gathering* e *Vulnerability Scanning*;
- l'annuncio della disponibilità di *exploit***[10]** software per sfruttare vulnerabilità tecnologiche effettivamente esistenti all'interno dell'organizzazione;
- minacce provenienti dall'esterno, quali, ad esempio, attacchi informatici o azioni dimostrative effettuate da gruppi di Hacktivist come Anonymous in concomitanza con la data del 5 novembre[11].

Esempi di **indicatori** sono:

- un sensore IDS o una qualsiasi sonda di sicurezza che rileva attività anomale o attacchi veri e propri generando il relativo allarme;
- software *antivirus* e *antimalware* che rileva *endpoint* infettati da codice malevolo e produce il relativo allarme;
- evidenza di manomissioni, tramite analisi del file di log, alle configurazioni di sistemi, applicazioni, database, sistemi di storage o apparati di rete e sicurezza;
- diversi tentativi di autenticazione falliti da parte di sistemi remoti e sconosciuti;
- aumento esponenziale del traffico di rete sia sulle direttrici esterne (compromissione massiva di sistemi interni che, facendo parte di una o più *botnet* e obbedendo alle istruzioni impartite da un Centro di Comando e Controllo remoto, tentano di partecipare ad attacchi DDoS[12] verso indirizzi IP pubblici su Internet) sia su quelle interne (ricezione di un attacco DDoS proveniente dall'esterno).

Policy

La policy che governa la risposta agli incidenti è peculiare per ogni organizzazione, ma molte sono caratterizzate da tratti comuni: oltre alle dichiarazioni di alto livello e all'ambito di applicazione, la policy definisce:

- concetti e nomenclature delle entità coinvolte;
- struttura organizzativa, ruoli, responsabilità, livelli di autorizzazione e punti di escalation;
- requisiti di gestione degli incidenti in termini di comunicazione esterna e *Information Sharing*;
- definizione della gravità (*severity*) degli incidenti;
- indicatori di performance e tipologia di report.

Piano

Il piano di risposta all'incidente deve fornire gli elementi per implementare la *capability* richiesta. Ogni organizzazione dovrebbe avere un piano per soddisfare i propri requisiti unici e specifici, correlati alla missione dell'organizzazione stessa, alle sue dimensioni, strutture e funzioni. Il piano dovrebbe comprendere i seguenti elementi:

- missione, strategie e obiettivi;
- approccio organizzativo e approvazione da parte del senior management;
- modalità di comunicazione da parte dell'IRT;
- metriche di misurazione dell'efficacia della risposta agli incidenti.

Procedure

Le procedure dovrebbero prendere le mosse dalla **Policy** e dal **Piano**. Le procedure operative standard delineano specifici processi tecnici, *checklist* e moduli utilizzati dall'IRT. Le procedure devono fornire il giusto livello di dettaglio recependo al proprio interno le priorità dettate dai requisiti dell'organizzazione. L'utilizzo di procedure standard dovrebbe anche minimizzare gli errori, soprattutto quelli derivanti dalla gestione degli incidenti da parte degli operatori del team in situazioni di forte stress.

Il Processo di *Incident Response*

Il processo di *Incident Response* definito dal NIST[13] consta di diverse fasi:

- **Preparation** (Preparazione): in questa fase rientra ogni azione propedeutica e continuativa finalizzata a creare le condizioni migliori per gestire l'incidente in maniera appropriata. Ogni elemento utile dovrebbe essere ricondotto a questa fase, sia esso di natura logistica, hardware, software, di comunicazione e di processo (*Risk Assessment* periodici, gestione delle configurazioni, *facility* quali *War Room*);
- **Detection & Analysis** (Rilevamento e Analisi): in considerazione dell'eterogeneità e del dinamismo intrinseco dei vettori d'attacco (interni, esterni, tecnologici, di processo, umani) è possibile isolare, per ogni tipologia di attacco, precursori e indicatori. Tali elementi sono di natura tecnologica (log, apparati di sicurezza specializzati, SIEM, flussi di traffico di rete), informativa (reperimento delle notizie di vulnerabilità, *Information*

Sharing con strutture preposte) e umana (segnalazioni provenienti da personale interno o da organizzazioni esterne). Precursori e indicatori determinano la capacità di rilevare potenziali incidenti definendo contestualmente il perimetro di visibilità e il margine operativo effettivo. La componente di analisi, immediatamente successiva, è particolarmente complessa e si scompone in ulteriori attività specializzate (*profiling*, comprensione dei comportamenti “normali”, definizione di *baseline* di riferimento, correlazione degli eventi di sicurezza, mantenimento di una base di conoscenza aggiornata e facilmente fruibile, capacità di raccolta e filtraggio di grandi quantità di dati). Il risultato della fase di analisi è costituito dalla documentazione completa dell’incidente, descritto negli attributi fondamentali di categoria di impatto sulle funzioni organizzative (*severity* alta, media o bassa), sulla dimensione di sicurezza dell’informazione interessata (Privacy Breach, perdita di riservatezza, integrità, disponibilità) e nella stima di risorse necessarie al superamento del problema. In questo modo è possibile assegnare la corretta priorità all’incidente indirizzando, di conseguenza, gli sforzi operativi;

- **Containment Eradication & Recovery** (Contenimento, Sradicamento e Ripristino): il contenimento è la fase che fornisce il tempo necessario alla definizione della migliore strategia possibile. Tali strategie sono variabili in funzione di diversi fattori ed è possibile svilupparne diverse in base alla categoria di attacco: contenere un attacco in corso tramite il vettore della posta elettronica è diverso da contenere un attacco DDoS o un’estrazione indebita di dati sensibili. In questa fase è necessario collezionare ogni evidenza possibile dell’incidente tramite opportuni strumenti e tecnologie finalizzate a salvaguardare l’integrità dei dati raccolti, identificando la sorgente dell’attacco e monitorandone l’attività. Dopo che un incidente è stato contenuto è necessario procedere all’eventuale sradicamento di alcune componenti dell’incidente stesso (codice malevolo, account compromessi) e al ripristino delle normali operazioni. Tale ripristino può coinvolgere attività sistemistiche (*backup&restore*, installazione da zero di sistemi e applicazioni, installazione di patch critiche) e di sicurezza (revisione delle policy dei firewall, modifiche nella produzione di log). Per gli incidenti su larga scala, è bene ricordarlo, la fase di *Recovery* può durare mesi;
- **Post-Incident Activity** (Attività post incidente): questa fase riguarda l’apprendimento e il miglioramento. Ogni incidente gestito rappresenta un’occasione di crescita e dovrebbe essere affrontato collettivamente dal gruppo di lavoro tramite incontri (*Lesson Learned*) finalizzati ad analizzare, commentare ed eventualmente correggere i comportamenti attuati. Ci sono diversi indicatori significativi a questo proposito: numero di incidenti gestiti in un dato lasso di tempo, tempo speso per risolvere ogni singolo incidente, rivisitazione della documentazione di ogni incidente.

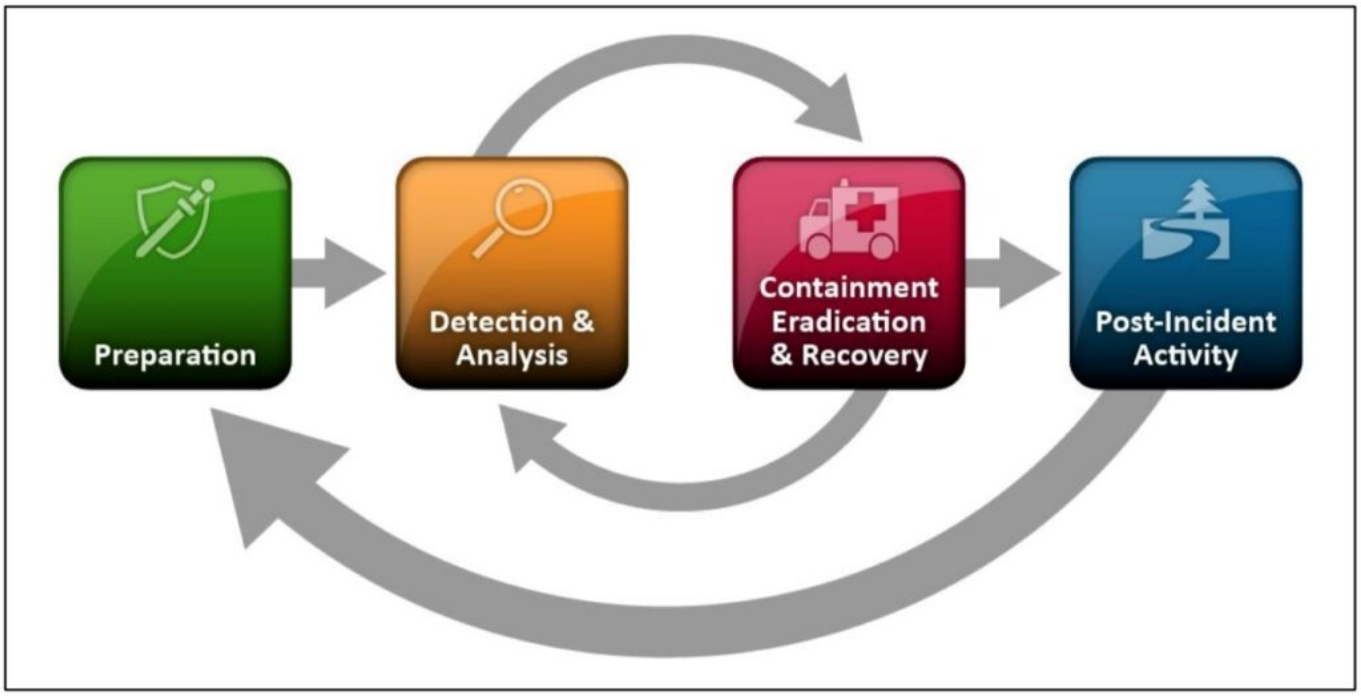

Figura 1 - Ciclo di vita dell'Incident Response - NIST

Incident Report

L'*Incident Report* dovrebbe incorporare tutte le informazioni salienti relative all'incidente e alle operazioni attuate per la sua gestione. Alcuni elementi fondamentali sono di seguito elencati:

- Informazioni di contatto relative a chi ha gestito e prodotto il report dell'incidente
- Nome
- Ruolo
- Unità organizzativa
- Indirizzo e-mail
- Numero di telefono
- Ubicazione (indirizzo, numero di stanza)
- Dettagli dell'incidente
- Riferimenti temporali: quando è iniziato l'incidente, quando è stato rilevato, quando è stato risolto o chiuso, quando è stato fatto il report
- Ubicazione fisica (città, stato)
- Stato corrente dell'incidente (in corso, chiuso)
- Sorgente/causa dell'incidente (reti, sistemi, applicazioni, dati), inclusi i nomi dei sistemi, gli indirizzi IP e i ruoli
- Descrizione dell'incidente (come è stato rilevato, cosa è accaduto)
- Descrizione delle risorse coinvolte (reti, sistemi, applicazioni, dati), inclusi i nomi dei sistemi, gli indirizzi IP e i ruoli
- Se si tratta di informazioni note, categoria dell'incidente, vettori di attacco associati,

indicatori (schemi di traffico anomalo, chiavi di registro Microsoft)
- Fattori usati per assegnare la priorità (impatto sulle funzionalità, sull'informazione, capacità di recupero)
- Fattori di mitigazione (ad esempio, furto di un portatile contenente dati sensibili ma equipaggiato con soluzioni di full disk encryption)
- Azioni di risposta effettuate (spegnimento di un server, disconnessione dalla rete, etc)
- Altre organizzazioni contattate (ad esempio, il produttore del software)
- Commenti generali

Raccomandazioni

Le raccomandazioni finali del NIST, applicabili in ogni scenario in cui è necessario gestire in maniera appropriata un incidente di sicurezza, sono di natura generale e quindi adottabili e adattabili all'interno di contesti eterogenei. Tali raccomandazioni, di seguito elencate, sono un utile punto di riferimento:

- acquisire strumenti e risorse che potrebbero essere utili durante il trattamento dell'incidente;
- prevenire l'accadimento degli incidenti assicurando che reti, sistemi e applicazioni si trovino in uno stato di sufficiente sicurezza;
- identificare precursori e indicatori tramite gli allarmi generati dalle varie tipologie di dispositivi e software di sicurezza;
- stabilire meccanismi per ricevere comunicazione, dall'esterno, di incidenti di sicurezza generati dalla propria organizzazione;
- richiedere un livello di *logging* e audit minimo su tutti i sistemi e un livello superiore per tutti i sistemi critici;
- profilare reti e sistemi per rilevare eventuali discostamenti dalle *baseline* di riferimento;
- comprendere il normale comportamento di reti, sistemi e applicazioni;
- creare una politica di conservazione dei log (*log retention*);
- effettuare la correlazione degli eventi;
- mantenere sincronizzati tutti gli orologi interni dei sistemi;
- mantenere viva e utilizzare una base di conoscenza condivisa interna al gruppo IRT;
- iniziare a registrare ogni informazione non appena si presenta un concreto sospetto di incidente;
- tutelare e proteggere i dati relativi all'incidente;
- assegnare le giuste priorità al trattamento degli incidenti sulla base di fattori rilevanti;
- stabilire strategie e procedure per contenere gli incidenti;
- seguire procedure predefinite per raccogliere e gestire le evidenze;
- catturare i dati volatili dei sistemi come ulteriori evidenze;
- ottenere *snapshot* complete dei sistemi, non solamente backup dei *file system*;
- condurre riunioni di *Lesson Learned* dopo gli incidenti più significativi.

Un esempio di procedura

Partendo dalle fasi del ciclo di vita dell'*Incident Response* individuate dal NIST, in Tabella 1 è

rappresentata sinteticamente una possibile procedura di risposta ad un attacco DDoS:

Fase	Azioni
Preparation	• Definizione della lista dei contatti e delle procedure interne di comunicazione • Definizione del supporto specialistico e dell'Internet Service Provider che eroga il servizio di connettività • Configurazioni di rete e dell'infrastruttura
Detection & Analysis	• Rivelamento e allarme • Analisi dell'attacco • Identificazione delle motivazioni • Attivazione delle azioni di mitigazione
Containment, Eradication and Recovery	• Modifiche alle configurazioni di rete • Controllo dell'andamento del traffico legittimo • Gestione della banda e della priorità assegnata a specifici protocolli di comunicazione • Blocco del traffico malevolo • Scrubbing del traffico • Sinkholing • Verifica del ritorno allo stato di normalità del traffico • Ripristino della configurazione standard
Post-Incident Activity	• Analisi dell'incidente e divulgazione dell'informazione • Eventuali contatti con le forze dell'ordine

Tabella 1 - Procedura di Incident Response a un attacco DDoS

Conclusioni

La risposta agli incidenti informatici di sicurezza è storicamente caratterizzata da un approccio reattivo, ma la dinamica evolutiva delle tecnologie di sicurezza di nuova generazione (*Machine Learning, Artificial Intelligence, Big Data*) permette di prefigurare con notevole accuratezza possibili scenari tramite l'utilizzo di analisi predittive e di altre tecniche statistiche. La crescente automazione in determinate aree tecnologiche di sicurezza (antivirus, firewall, gestione delle patch e dei sistemi di autenticazione) non riesce però a essere del tutto efficace nella risposta agli incidenti perché, come evidenziato da Bruce Schneier[16], questa appartiene ad un dominio caratterizzato da eccessiva incertezza. In questo senso un modello di orchestrazione della sicurezza basato sugli umani – che rappresenti l'unione di persone, processi e tecnologia - può essere incredibilmente potente. Lo sviluppo di un autentico approccio proattivo rappresenta una possibilità nuova e importante per le attività di *Incident Response* ma, come sempre, le innovazioni dirompenti nel mondo delle macchine devono essere conoscibili, gestibili e governate da esseri umani.

Note

- [1] https://www.ictsecuritymagazine.com/articoli/security-operations-center-il-cuore-della-protezione-dellinformazione/
- [2] https://en.wikipedia.org/wiki/Security_operations_center
- [3] https://en.wikipedia.org/wiki/Computer_emergency_response_team
- [4] https://en.wikipedia.org/wiki/Incident_response_team
- [5] https://en.wikipedia.org/wiki/Information_and_communications_technology
- [6] https://en.wikipedia.org/wiki/Flooding_(computer_networking)
- [7] https://en.wikipedia.org/wiki/Botnet
- [8] https://en.wikipedia.org/wiki/File_sharing
- [9] https://en.wikipedia.org/wiki/Peer-to-peer
- [10] https://en.wikipedia.org/wiki/Exploit_(computer_security)
- [11] https://knowyourmeme.com/memes/events/fifth-of-november
- [12] https://en.wikipedia.org/wiki/Denial-of-service_attack
- [13] https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
- [14] https://en.wikipedia.org/wiki/DDoS_mitigation
- [15] https://www.fastweb.it/internet/che-cos-e-e-come-funziona-il-sinkholing/
- [16] https://www.schneier.com/blog/archives/2017/03/security_orches.html

Articolo a cura di **Andrea Boggio**