SOPHOS

GUIDA ALLA INCIDENT RESPONSE

Come realizzare un piano strategico di risposta agli attacchi informatici

"Prima di ogni altra cosa, la preparazione è la chiave del successo".

Alexander Graham Bell

Qual è il modo migliore per impedire che un attacco informatico diventi un vero e proprio caso di violazione? Prepararsi in anticipo.

Dopo una violazione, spesso le organizzazioni si rendono conto che avrebbero potuto evitare tutti i costi, i problemi e i disagi subiti, se solo avessero avuto un piano strategico di risposta.

Questa guida è stata compilata per aiutarvi a definire il quadro strutturale più efficace per la vostra strategia di Incident Response, ovvero la risposta agli incidenti di cybersecurity, al fine di incrementare la vostra capacità di sventare gli attacchi. Le raccomandazioni fornite in questa guida si basano sulle competenze maturate sul campo dai team Sophos Managed Threat Response e Sophos Rapid Response, che vantano decine di migliaia di ore di esperienza pratica nel contrastare gli attacchi informatici.

Piano strategico di risposta agli incidenti di cybersecurity

Un piano strategico di risposta agli incidenti di sicurezza è composto da 10 passaggi.

Quadro strutturale di un piano strategico di risposta agli incidenti di sicurezza

1. Stabilire quali membri del personale occorre coinvolgere

La responsabilità di una pianificazione adeguata non deve ricadere solamente sul team di IT security. È infatti molto probabile che un incidente colpisca quasi tutti i reparti dell'organizzazione, specialmente se l'attacco diventa una vera e propria violazione su vasta scala. Per coordinare adeguatamente la risposta, occorre prima identificare chi deve svolgere un ruolo attivo. Spesso si tratta di esponenti dei team di senior management, sicurezza, assistenza tecnica, ufficio legale e pubbliche relazioni.

Le persone da coinvolgere nelle attività di risposta e negli esercizi di pianificazione dell'organizzazione devono essere identificate in anticipo. Inoltre, occorre definire un metodo di comunicazione efficace per garantire una risposta rapida, tenendo presente la possibilità che i canali di comunicazione abituali (ovvero la posta elettronica dell'organizzazione) potrebbero essere stati compromessi dall'incidente.

2. Identificare le risorse critiche

Per determinare l'impatto e l'estensione di un attacco, l'organizzazione deve prima identificarne le risorse più importanti. La mappatura delle risorse da proteggere con la massima priorità non aiuta solamente a definire la strategia di sicurezza, ma semplifica anche la definizione dell'impatto e dell'estensione di un attacco. Inoltre, identificando queste risorse in anticipo, il team di risposta agli incidenti potrà focalizzarsi sulle risorse critiche quando si verifica un attacco, riducendo così il livello di disservizio per l'organizzazione.

3. Eseguire simulazioni

Come avviene per molte altre discipline, anche per la risposta agli incidenti di sicurezza i risultati si ottengono con la pratica. Sebbene sia difficile replicare completamente l'intensità e la pressione sul personale di un potenziale caso di violazione, le prove pratiche aiutano a garantire una risposta più coordinata ed efficace quando dovessero verificarsi incidenti reali. È importante non solo eseguire simulazioni (spesso nell'ambito di un'esercitazione avviata da un red team), ma anche altre prove che riguardano i membri del personale (precedentemente identificati) da coinvolgere in caso di attacco.

Le simulazioni devono mettere alla prova le strategie di riposta dell'organizzazione in diversi potenziali scenari di attacco. Ogni scenario può anche coinvolgere altri membri del personale che non fanno parte del team tecnico. L'organizzazione deve definire in anticipo chi informare quando viene rilevato un attacco, anche se dovesse essere stato neutralizzato.

I più comuni scenari per la risposta agli incidenti includono:

- **Rilevamento di active adversary nella rete:** in questo tipo di scenario è essenziale che il team di Incident Response riesca a comprendere come l'hacker sia riuscito a infiltrarsi nell'ambiente informatico dell'organizzazione, identificando quali strumenti e tecniche abbia utilizzato, le risorse colpite e se abbia stabilito la persistenza. Queste informazioni aiuteranno a definire l'approccio più adeguato da adottare per neutralizzare l'attacco.

  Sebbene la soluzione più ovvia possa sembrare l'espulsione immediata dell'intruso, alcuni team di sicurezza preferiscono attendere e osservarne le azioni, per raccogliere dati essenziali al fine di scoprirne gli obiettivi e i metodi che utilizza per raggiungerli.

- **Violazione dei dati avvenuta:** se viene rilevata una violazione dei dati, il team di Incident Response deve essere in grado di determinare quali dati sono stati esfiltrati e come. Successivamente, dovrà delineare una strategia di risposta adeguata, che includa anche considerazioni in termini di impatto sulla conformità e sulle politiche di regolamentazione; occorrerà inoltre stabilire se sia necessario contattare i clienti e potenzialmente le forze dell'ordine.

- **Attacco ransomware avvenuto:** se vengono cifrati dati e sistemi critici, il team di Incident Response deve seguire una strategia che preveda il recupero tempestivo delle informazioni sottratte. Tale strategia deve includere un processo di ripristino dei sistemi dai backup. Per impedire che l'attacco si ripeta quando si è nuovamente operativi, il team deve indagare e assicurarsi che il cybercriminale non abbia più accesso ai sistemi. Inoltre, l'organizzazione deve considerare se, in situazioni estreme, sarebbe disposta a pagare una somma di denaro per recuperare i dati e in tal caso quale sarebbe il limite massimo di tale somma.

- **Compromissione di sistemi critici:** la compromissione di un sistema ad alta priorità potrebbe impedire all'organizzazione di svolgere le normali attività lavorative. Oltre a tutti i passaggi necessari per un piano strategico di risposta agli incidenti di sicurezza, l'organizzazione deve anche considerare se definire o meno un piano per eventi imprevisti che limiti il disservizio in tali eventualità.

4. Implementare strumenti di protezione

Il modo migliore per affrontare un incidente è prevenirlo. Verificare che l'organizzazione possa fare affidamento su adeguate tecnologie di protezione per endpoint, rete, server, cloud, dispositivi mobili ed e-mail.

5. Garantire massima visibilità

Senza un adeguato livello di visibilità su quello che succede durante un attacco, l'organizzazione farà fatica a implementare una risposta adeguata. Prima che si verifichi un attacco, i team dei reparti tecnici e di sicurezza devono accertarsi di poterne comprendere l'impatto e l'estensione, e questo include anche la necessità di identificare i punti di ingresso e i punti di persistenza dei cybercriminali. Un'adeguata visibilità include la raccolta di dati di log, con una particolare focalizzazione sulle informazioni relative a endpoint e rete. Siccome molti attacchi vengono rilevati solamente dopo diversi giorni o settimane, è importante avere accesso a dati storici, risalenti a giorni o settimane (talvolta persino mesi) precedenti, per poter svolgere le indagini. Inoltre, occorre eseguire regolarmente il backup di questi dati, per potervi accedere durante un incidente attivo.

6. Implementare il controllo dell'accesso ai sistemi

Gli hacker possono approfittare di una strategia di controllo dell'accesso inadeguata per aggirare le difese dell'organizzazione e ottenere privilegi più elevati. Occorre verificare regolarmente che siano implementati adeguati controlli dell'accesso ai sistemi. Questi controlli includono, a titolo esemplificativo, l'autenticazione a fattori multipli, la limitazione dei privilegi di amministrazione a meno account possibili (seguendo il principio dell'assegnazione di meno privilegi), la modifica delle password predefinite e la riduzione del numero di punti di accesso da monitorare.

7. Investire in strumenti di indagine

Oltre a garantire la visibilità, l'organizzazione deve investire anche in strumenti in grado di fornire il giusto contesto durante un'indagine.

Alcune delle risorse più frequentemente utilizzate per la risposta agli incidenti di sicurezza includono strumenti di Endpoint Detection and Response (EDR, rilevamento e risposta alle minacce endpoint) o di Extended Detection and Response (XDR, rilevamento e risposta estesi), che consentono di rilevare proattivamente gli indicatori di compromissione (IoC) e gli indicatori di attacco (IoA) all'interno del proprio ambiente. Gli strumenti EDR aiutano gli analisti a identificare le risorse che sono state compromesse e di conseguenza a determinare l'impatto e l'estensione di un attacco. Più sono i dati raccolti (da endpoint e altri sistemi), maggiore sarà il contesto disponibile durante le indagini. Questa visibilità estesa permetterà ai team non solo di definire le risorse attaccate dai cybercriminali, ma anche come sono riusciti a infiltrarsi nell'ambiente informatico dell'organizzazione e se sono ancora in grado di accedervi.

Oltre agli strumenti EDR, i team di sicurezza avanzata potrebbero implementare anche una soluzione SOAR (Security Orchestration, Automation and Response, ovvero orchestrazione, automazione e risposta), per ottimizzare i flussi di lavoro per la risposta.

8. Determinare azioni di risposta

Rilevare un attacco è solamente parte del processo. Per poter rispondere in maniera adeguata a un attacco, i team dei reparti tecnici e di sicurezza devono accertarsi di avere la capacità di eseguire una vasta gamma di azioni di correzione per interrompere e neutralizzare un attacco. Le azioni di risposta includono anche, ma non solo, le seguenti:

- Isolamento degli host colpiti
- Blocco di file, processi e programmi dannosi
- Blocco delle attività di comando e controllo (C2) e delle operazioni provenienti da siti web dannosi
- Blocco degli account compromessi e dell'accesso per gli hacker
- Rimozione di artefatti e strumenti degli hacker
- Chiusura dei punti di ingresso e delle aree di persistenza utilizzati dai cybercriminali (sia all'interno dei sistemi, sia in sistemi di terze parti)

- Ottimizzazione delle configurazioni (policy per le minacce, implementazione di una soluzione di protezione endpoint ed EDR sui dispositivi non protetti, modifica delle esclusioni, ecc.)
- Ripristino delle risorse colpite, con backup off-line

9. Condurre attività di formazione e sensibilizzazione

Sebbene non esista un programma di formazione che possa essere efficace al 100% contro una tipologia specifica di cybercriminale, l'uso di programmi educativi (ad es. di sensibilizzazione sul phishing) aiuta a ridurre il rischio e a limitare il numero di avvisi per i team di sicurezza. Gli strumenti di simulazione di attacchi di phishing offrono un modo sicuro per aiutare i dipendenti a capire cosa significhi essere colpiti da un tentativo di phishing e potenzialmente caderne vittima. Questi strumenti permettono di iscrivere a un corso di formazione i dipendenti che non superano le prove e consentono di identificare i gruppi di utenti più a rischio, che potrebbero richiedere ulteriore training.

10. Usufruire di un servizio di sicurezza gestito

Molte organizzazioni non dispongono delle risorse necessarie per rispondere autonomamente a un incidente di sicurezza. Per essere rapida ed efficace, la risposta agli incidenti richiede tecnici esperti in ambito di sicurezza. Per garantire una risposta adeguata, un'opzione potrebbe essere affidarsi a una risorsa esterna, come ad esempio un fornitore di servizi di Managed Detection and Response (MDR, rilevamento e risposta gestiti).

L'MDR offre un servizio gestito in grado di garantire individuazione proattiva delle minacce, indagine e risposta agli incidenti 24/7. I servizi MDR non aiutano solamente l'organizzazione a rispondere agli incidenti prima che diventino veri e propri casi di violazione, ma contribuiscono anche a prevenire gli incidenti, diminuendo la probabilità che si verifichino. I servizi MDR stanno diventando sempre più diffusi: secondo Gartner*, entro il 2025 il 50% delle organizzazioni utilizzerà servizi MDR (una percentuale in aumento, rispetto a meno del 5% nel 2019).

A volte vengono impiegati anche servizi DFIR (Data Forensic Incident Response, ovvero risposta agli incidenti con indagine approfondita dei dati), che raccolgono le prove necessarie per cause legali o per gestire eventuali sinistri assicurativi.

Riepilogo

Quando un attacco di cybersecurity colpisce i sistemi di un'organizzazione, le tempistiche di risposta sono un fattore cruciale. Un piano strategico di risposta ben strutturato e comprensibile, nonché semplice da implementare per tutte le persone coinvolte, riduce drasticamente l'impatto di un attacco sull'organizzazione.

Sophos vi può aiutare, ecco come

Servizio Sophos Managed Threat Response (MTR)

Sophos Managed Threat Response (MTR) offre un servizio completamente gestito con opzioni di ricerca, rilevamento e risposta alle minacce, disponibile 24h su 24 e 7gg su 7 e gestito direttamente dal nostro team di esperti. Andando ben oltre la semplice notifica di attacchi o comportamenti sospetti, il team Sophos MTR intraprende azioni mirate per conto degli utenti, in modo da neutralizzare persino le minacce più sofisticate e complesse.

Il team Sophos MTR, composto da esperti di threat hunting e risposta alle minacce:

- Intercetta e conferma proattivamente la presenza di potenziali minacce e incidenti
- Utilizza tutte le informazioni disponibili per determinare il raggio di azione e la gravità delle minacce
- Applica il giusto contesto imprenditoriale per le minacce confermate
- Avvia azioni volte a fermare, contenere e neutralizzare le minacce in remoto
- Offre consigli pratici per risolvere alla radice il problema degli incidenti ricorrenti

Per saperne di più, visitate www.sophos.com/mtr

Servizio Sophos Rapid Response

Sophos Rapid Response è un servizio fornito da un team di esperti di Incident Response, in grado di garantire assistenza tempestiva per identificare e neutralizzare le minacce attive presenti nei sistemi dell'organizzazione. L'attivazione richiede poche ore e nella maggior parte dei casi la valutazione avviene entro 48 ore. Il servizio è disponibile sia per i clienti Sophos che per i sistemi che non includono soluzioni Sophos.

Sophos Rapid Response è composto da un team che interviene da remoto e include esperti in materia di risposta agli incidenti di sicurezza, threat hunting e analisi delle minacce in grado di:

- Intervenire rapidamente per valutare, contenere e neutralizzare le minacce attive
- Espellere gli intrusi dalla vostra struttura informatica, per impedire che arrechino ulteriori danni alle risorse
- Monitorare costantemente e rispondere agli incidenti 24/7 per potenziare la protezione
- Offrire consigli su azioni preventive in tempo reale, per agire sulla causa originaria di un attacco
- Fornire un riepilogo dettagliato della minaccia dopo la risoluzione dell'incidente, con una descrizione delle indagini svolte

Per maggiori informazioni, visitate www.sophos.com/rapidresponse

Sophos Intercept X Advanced with EDR

Sophos Intercept X Advanced with EDR aiuta a garantire la regolare esecuzione delle attività di threat hunting e l'integrità delle IT operation nell'intero ambiente informatico. Sophos EDR permette ai vostri team di formulare domande dettagliate per identificare minacce, active adversary e potenziali vulnerabilità informatiche; sarà quindi possibile intervenire tempestivamente per bloccarli, intraprendendo le dovute azioni. Potrete rilevare anche gli hacker che si nascondono inosservati all'interno della vostra rete in attesa di distribuire ransomware.

Per scoprire di più e per una prova gratuita, visitate www.sophos.com/edr

* Gartner, Market Guide for Managed Detection and Response Services, 26 agosto 2020, analisti: Toby Bussa, Kelly Kavanagh, Pete Shoard, John Collins, Craig Lawson, Mitchell Schneider

Vendite per Italia:
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it

20-10-09 WPIT (DD)

SOPHOS