SOPHOS

Guida Alla Incident Response di Sophos

Indice dei contenuti

Introduzione

Questo documento è stato sviluppato per fornire una panoramica completa delle best practice di incident response. Aiuta a orientare la valutazione delle minacce informatiche da un punto di vista sia tecnico che organizzativo. Lo scopo di questa guida è assistere le aziende nello sviluppo di processi di incident response efficaci.

Destinata tanto ai professionisti di cybersecurity che operano in ruoli tecnici e organizzativi, quanto a chi muove i primi passi nel campo della sicurezza informatica, questa guida offre un'introduzione all'incident response. Ti preghiamo di notare che la guida non fornisce indicazioni esaurienti sui quadri normativi e legali di gestione della sicurezza delle informazioni. Deve essere utilizzata come risorsa supplementare, per accompagnare le linee guida per la divulgazione e la risposta in caso di violazione dei dati applicabili in modo specifico alla tua organizzazione. In aggiunta, consigliamo di considerare il ruolo delle cyberassicurazioni come caso distinto, in quanto le polizze potrebbero contenere linee guida che divergono dalle raccomandazioni indicate in questa guida all'incident response.

Un'efficace strategia di preparazione agli incidenti informatici offre alle organizzazioni protocolli e procedure già consolidati, su cui fare affidamento per accelerare i tempi di risposta, classificazione e contenimento dei rischi. L'obiettivo di questo documento è fornire linee guida per i processi di incident response durante la fase di preparazione di un ciclo di gestione delle violazioni informatiche. Queste strategie possono, in ultima analisi, ridurre l'impatto finanziario e operativo sulle organizzazioni, accelerando il contenimento degli incidenti informatici.

Consigliamo ai professionisti di cybersecurity di integrare questi concetti e metodi investigativi nei propri piani e processi di incident response, adattandoli alle esigenze dell'organizzazione. La guida può essere letta dall'inizio alla fine, oppure in maniera selettiva, dedicando maggiore attenzione al o ai capitoli che riflettono maggiormente le esigenze del lettore. Sebbene non offra un piano dettagliato e definitivo per la gestione degli incidenti informatici, è realizzata per aiutare i team di sicurezza a preparare e implementare i propri processi interni.

Le fasi di gestione degli incidenti descritte in questa guida riflettono il framework di incident response consigliato da SANS, che è composto da sei fasi diverse. Questo framework è progettato per mettere in evidenza ogni fase del ciclo di gestione degli incidenti e offre ai professionisti di sicurezza un valido aiuto per la preparazione di una strategia efficace di risposta agli incidenti. Non deve tuttavia essere considerato come un manuale strategico. Gli incidenti di cybersecurity sono dinamici e sebbene i framework forniscano la struttura necessaria per pianificare un approccio generale, la valutazione di professionisti di sicurezza e dipendenti qualificati in ambito informatico resta un elemento fondamentale per affrontare questi tipi di incidenti.

Preparazione

La prima fase del ciclo di incident response è quella di preparazione. L'impegno investito e le attività svolte durante questa fase avranno un impatto significativo sull'efficacia e sull'esito delle fasi successive. Di conseguenza, la fase di preparazione non è solamente essenziale, ma anche dinamica, in quanto deve essere rivista e aggiornata regolarmente. La fase di preparazione include sia elementi non strettamente tecnici, come processi e procedure, sia aspetti puramente tecnici, quali la protezione avanzata dei sistemi, la raccolta di dati di telemetria e la formazione. Dedicando la giusta quantità di tempo e risorse alla preparazione, le organizzazioni possono gettare basi solide per strutturare una strategia di incident response efficace e flessibile.

Processi e procedure

Processi e procedure ben documentati sono elementi essenziali per instaurare dinamiche efficienti in un team di incident response. Definendo queste linee guida e diffondendole tra il personale selezionato per il processo di gestione degli incidenti, puoi garantire l'integrità delle informazioni e l'allineamento degli obiettivi per tutte le persone direttamente interessate. Se descritti chiaramente, i processi e le procedure contribuiscono a mantenere un approccio coerente nell'intero team, facilitando le comunicazioni e aiutando a snellire e coordinare la risposta agli incidenti informatici.

Piano di gestione degli incidenti

Per essere efficace, un piano di gestione degli incidenti deve stabilire procedure ben definite per rispondere agli incidenti e deve includere le informazioni necessarie per tutte le parti coinvolte. Nel tuo piano di gestione degli incidenti, ti consigliamo di includere i seguenti elementi, che ti aiuteranno a implementare un approccio all'incident response a 360 gradi:

- **Definisci quali sono le persone interessate:** identifica le principali persone interessate e assegna ruoli specifici per il processo di gestione dell'incidente, ad esempio responsabili di incident management, personale IT supplementare, team di organizzazione e leadership, nonché terze parti esterne quali provider di servizi IT, forze dell'ordine e vendor di soluzioni di incident response.
- **Classificazione e livelli di gravità degli incidenti:** definisci i criteri necessari per la classificazione degli incidenti, basandoli su fattori quali impatto potenziale, sistemi coinvolti e tipo di minaccia. Stabilisci i livelli di gravità, per assegnare le giuste priorità e orientare l'incident response.
- **Procedure di escalation:** sviluppa procedure di escalation trasparenti per gli incidenti che richiedono capacità o poteri decisionali che superano quelli dei responsabili dell'incident response iniziali. È possibile coinvolgere l'alta dirigenza o esperti esterni, a seconda delle esigenze.
- **Comunicazioni:** assicurati che venga implementato un sistema di comunicazione efficace durante eventuali crisi, utilizzando modelli di incident response predefiniti per team interni, clienti e partner. Puoi anche includere best practice per il disaster recovery e piani di continuità aziendale per valutare i canali di comunicazione da utilizzare come failover per le e-mail, la messaggistica istantanea e le videoconferenze.
- **Inventario delle risorse:** mantieni un inventario aggiornato delle risorse, per monitorare e gestire tutti gli hardware e i software utilizzati dall'organizzazione. Queste informazioni sono fondamentali per determinare l'estensione e l'impatto di una minaccia, nonché per coordinarne la risposta.
- **Tempistiche di incident response:** definisci le tempistiche di ogni fase del processo di incident response, indicando le scadenze per le varie fasi, al fine di garantire una risposta tempestiva e organizzata.
- **Documentazione e reportistica sull'incidente:** stabilisci uno standard per come devono essere documentati tutti gli aspetti di un incidente, incluse le azioni effettuate, le decisioni prese e i risultati ottenuti. Questa documentazione sarà cruciale per l'analisi post-incidente e per potenziali inchieste legali o regolamentari.
- **Studi di revisione post-azione e miglioramento costante:** implementa un processo che preveda studi di revisione delle azioni svolte in seguito a un incidente, al fine di valutare l'efficacia della strategia di risposta e di identificare gli ambiti da migliorare. Utilizza queste informazioni per aggiornare e ottimizzare il piano di gestione degli incidenti, in base alle esigenze emerse.

Integrando questi elementi nel tuo piano di gestione degli incidenti, aumenterai il grado di preparazione della tua organizzazione, incrementando l'efficacia e l'efficienza delle attività di gestione e risposta agli incidenti di cybersecurity.

Documentazione legale

Durante la fase di preparazione, le aziende devono considerare le responsabilità legali legate alla divulgazione, alle normative in materia di gestione degli incidenti e ad altri aspetti della cybersecurity. I paragrafi che seguono indicano alcune delle considerazioni legali più comuni, tuttavia consigliamo alle organizzazioni di condurre un'analisi completa di tutti i requisiti normativi applicabili ai propri settori di attività e alle aree geografiche in cui operano. Identifica i responsabili individuali della reportistica e della conformità legale all'interno dell'organizzazione e includili in qualità di persone interessate nel piano di incident response, assegnando ruoli ben definiti.

- **Responsabilità legali e normative di divulgazione:** alcune organizzazioni potrebbero essere legalmente vincolate o sollecitate a divulgare i dettagli degli incidenti, a seconda del loro stato o settore di attività.
  - Organizzazioni nel settore delle infrastrutture critiche
  - Enti governativi
  - Società ad azionariato diffuso
- **Privacy dei dati:** attieniti alle leggi in termini di protezione dei dati, che prescrivono la divulgazione responsabile dell'incidente alle agenzie di informazioni incaricate e ai clienti o singoli individui coinvolti, i cui dati potrebbero essere stati compromessi.
- **Conservazione e distruzione dei dati:** applica policy e procedure per la conservazione, l'archiviazione e la distruzione sicura dei dati raccolti durante le attività di incident response, in conformità con le leggi e i regolamenti applicabili.
- **Accordi e contratti con terze parti:** revisiona accordi e contratti stipulati con vendor, fornitori e partner, per capirne gli obblighi in termini di incident response e per comprenderne i requisiti di notifica in caso di incidente o violazione.
- **Tutela della proprietà intellettuale (PI):** gestisci tutti gli aspetti legali della protezione della proprietà intellettuale della tua organizzazione, inclusi segreti commerciali, brevetti, copyright e marchi registrati, sia durante che dopo un incidente informatico.
- **Trasferimento transfrontaliero di dati e segnalazione:** se la tua organizzazione opera a livello internazionale, considera le implicazioni e i requisiti legali del trasferimento e della segnalazione dei dati in più giurisdizioni.
- **Diritti e doveri dei dipendenti:** definisci i diritti e i doveri legali dei dipendenti nel contesto degli incidenti di cybersecurity, inclusi gli obblighi di segnalare gli incidenti e di proteggere le informazioni di natura sensibile.
- **Documentazione sulla polizza assicurativa:** acquisisci un'ottima comprensione del processo e dei requisiti necessari per chiedere un indennizzo cyberassicurativo.
  - Rivedi termini e condizioni della polizza, per stabilire quali sono le inclusioni e le esclusioni.
  - Consulta i detentori interni della polizza, per capire cos'è incluso nella copertura assicurativa.

Playbook di incident response

I playbook di incident response sono manuali strategici che offrono linee guida dettagliate sulle azioni da intraprendere quando vengono identificate minacce specifiche. Le strategie devono essere sviluppate utilizzando un approccio basato sui rischi, considerando la probabilità e il potenziale impatto di vari scenari di attacco. Per lo sviluppo dei playbook di incident response, consigliamo di considerare i seguenti fattori:

- **Devono essere personalizzati per l'organizzazione:** assicurati che i tuoi playbook siano realizzati su misura, in modo da riflettere l'ambiente, le risorse e le capacità specifiche dell'organizzazione. Dovrai considerare, tra gli altri aspetti, anche le dimensioni, il settore di attività e i rischi che riguardano in modo particolare la tua organizzazione.

- **Minacce e scenari specifici:** per le organizzazioni con pratiche ben rodate, è consigliabile sviluppare playbook destinati ad affrontare minacce specifiche, ad esempio alcuni tipi di malware o di attacchi mirati. Tuttavia, alle organizzazioni con risorse limitate consigliamo piuttosto di realizzare playbook universali, da utilizzare in vari scenari diversi e che siano applicabili a un'ampia selezione di minacce.
- **Istruzioni chiare e concise:** i playbook devono offrire istruzioni chiare e concise per ogni fase del processo di risposta. In questo modo, i responsabili dell'incident response potranno capire e svolgere rapidamente le azioni necessarie durante un incidente.
- **Ruoli e responsabilità:** definisci chiaramente i ruoli e le responsabilità di ogni membro del team coinvolto nel processo di risposta. Con questa strategia, tutte le persone coinvolte sapranno esattamente cosa devono fare e saranno in grado di collaborare in maniera efficace.
- **Comunicazioni ed escalation:** includi linee guida per le comunicazioni e l'escalation in caso di incidente, ad esempio quando inviarne notifica al management e quando richiedere assistenza esterna.
- **Integrazione con un piano di gestione degli incidenti:** assicurati che i tuoi playbook siano in linea con il piano generale di gestione degli incidenti e che ne facilitino l'implementazione. Questo accorgimento aiuta a mantenere un approccio coerente e omogeneo per tutte le attività di incident response.
- Aggiornamenti e revisioni a cadenza regolare: i playbook devono essere rivisti e aggiornati regolarmente, per garantirne la pertinenza e l'efficacia contro minacce in continua evoluzione, in ambienti organizzativi che possono cambiare frequentemente.

Integrando questi elementi nei tuoi playbook di incident response, la tua organizzazione potrà rispondere con maggiore preparazione ed efficacia a un ampio ventaglio di incidenti di cybersecurity, riducendone il potenziale impatto.

Backup

I backup sono essenziali per garantire la continuità operativa e per ridurre l'impatto della perdita dei dati in caso di incidenti, errori nei sistemi o attacchi informatici. Per implementare una strategia di backup efficace, occorre creare e verificare i backup regolarmente, scegliendo opzioni di archiviazione diverse per incrementare la disponibilità dei dati in base alla situazione. Per lo sviluppo della tua strategia di backup, consigliamo di considerare i seguenti fattori:

- **Frequenza dei backup:** stabilisci un'adeguata frequenza di creazione dei backup, tenendo in considerazione quali livelli di rischio e di criticità dei dati possano essere accettabili. L'esecuzione regolare di backup aiuta a ridurre l'impatto di una potenziale perdita dei dati.
- **Tipi di backup:** utilizza una combinazione tra backup completi, incrementali e differenziali.
- **Opzioni di archiviazione:** opta per più opzioni di archiviazione, includendo backup sui sistemi locali, nel cloud e off-line. Potrai così garantire la disponibilità dei dati e mitigare il rischio di perdita dei dati derivata da un Single Point of Failure.
- **Prioritizzazione dei dati business-critical:** concentrati sull'esecuzione dei backup dei dati e dei sistemi business-critical, ovvero quelli essenziali per garantire la continuità operativa e per sostenere i principali processi dell'azienda.
- **Cifratura dei backup:** cifra i backup per proteggere i dati di natura sensibile e per prevenire l'accesso non autorizzato durante l'archiviazione e la trasmissione delle informazioni.
- **Verifica dei backup:** verifica regolarmente i tuoi backup, per accertarti che siano affidabili e che, all'occorrenza, possano essere utilizzati per il ripristino. La verifica può includere controlli del processo di ripristino e dell'integrità dei dati contenuti nei backup.
- **Policy di conservazione dei dati:** applica policy di conservazione dei dati per gestire l'archiviazione e l'eliminazione dei backup in conformità con i requisiti legali, normativi e aziendali.
- **Pianificazione del ripristino di emergenza:** integra la tua strategia di backup nel piano generale di ripristino di emergenza della tua organizzazione, per garantire una risposta efficace e coordinata agli eventi di perdita dei dati.

Integrando questi fattori nella tua strategia per i backup, la tua organizzazione potrà riprendersi da un eventuale incidente con maggiore preparazione.

Protezione avanzata dei sistemi e della rete

Per implementare la protezione avanzata dei sistemi e della rete, occorre ridurre la superficie di attacco, limitando quanto più possibile funzionalità, accessi ai sistemi e connessioni di rete che non siano strettamente essenziali. Applicando pratiche efficaci di protezione avanzata, la tua organizzazione può ridurre la probabilità che un attacco vada a segno. Per sviluppare la tua strategia di protezione avanzata dei sistemi e della rete, considera i seguenti fattori:

Patch

- **Programma di gestione delle patch:** stabilisci un programma in grado di garantire l'applicazione regolare e tempestiva delle patch alle risorse presenti nella rete, sfruttando strumenti automatici o semiautomatici.
- **Documentazione:** mantieni un elenco di patch applicate ed eventuali esclusioni indispensabili.
- **Prioritizzazione:** assegna alle patch la giusta priorità, in base a un'analisi del rischio. Concentrati principalmente su come risolvere le vulnerabilità dal maggiore impatto potenziale sulla tua organizzazione.

Configurazione

- **Controlli di conformità della sicurezza:** esegui regolarmente controlli interni ed esterni per verificare l'efficacia della configurazione e delle impostazioni dei tuoi strumenti di sicurezza, identificando e risolvendo eventuali errori di configurazione o esclusioni non indispensabili.
- **Controllo delle applicazioni:** implementa elenchi di autorizzazione o blocco, per limitare il numero e le versioni delle applicazioni in grado di eseguirsi sugli host. Con questa strategia, potrai ridurre il rischio di exploit di software non autorizzati o vulnerabili.
- **Controllo degli accessi alla rete:** configura strumenti di rete che siano in grado di limitare gli IP e l'accesso alle porte, in modo da autorizzare solo gli host interni ed esterni essenziali. Potrai così diminuire il rischio di accesso non autorizzato e di esfiltrazione dei dati.
- **Principio del privilegio minimo:** assicurati che gli utenti all'interno della tua organizzazione abbiano diritti di accesso limitati al minimo indispensabile per svolgere le proprie mansioni lavorative. In questo modo ridurrai il rischio di accesso non autorizzato e compromissione dei dati.

Protezione della rete

- **Segmentazione della rete:** dividi la rete in segmenti più piccoli e isolati, per limitare il potenziale impatto di una violazione di sicurezza e per ostacolare gli hacker che cercano di muoversi lateralmente all'interno della tua rete.
- **Configurazione del firewall:** configura i firewall in modo da bloccare tutto in traffico in entrata e in uscita che non sia strettamente indispensabile. Per mantenere un profilo di sicurezza ottimale, non dimenticare di rivedere e aggiornare frequentemente anche le regole.
- **Sistemi di rilevamento e prevenzione delle intrusioni (Intrusion Detection and Prevention System, IDPS):** applica IDPS per monitorare il traffico e individuare segnali di attività dannosa. Questo ti permetterà di intraprendere una risposta adeguata.

Monitoraggio e telemetria

Il monitoraggio e la telemetria sono componenti indispensabili per una strategia efficace di incident response: offrono infatti dati importantissimi sull'ambiente di un'organizzazione e permettono di rilevare tempestivamente potenziali minacce. Approfondendo la conoscenza del tuo ambiente e implementando livelli adeguati di rilevamento e protezione, puoi potenziare le capacità di risposta agli incidenti della tua organizzazione.

Il tuo ambiente

La comprensione del tuo ambiente costituisce la base su cui puoi strutturare strutturare una strategia efficace di monitoraggio e telemetria. Questo approccio include:

- Inventario delle risorse: mantieni un elenco aggiornato di endpoint e server, indicandone il livello di protezione con le piattaforme di sicurezza applicabili.
- Topologia della rete: acquisisci una chiara comprensione della tua rete, inclusi i punti di ingresso/uscita, la segmentazione, i punti di controllo e preferibilmente un diagramma aggiornato dell'architettura.

Livelli di rilevamento e protezione

L'applicazione di più livelli di rilevamento e protezione è fondamentale per una strategia di sicurezza a 360 gradi. Considera le seguenti origini di telemetria e assicurati di sincronizzare i timestamp per tutte le origini (il fuso orario standard consigliato è UTC):

- **Dispositivi perimetrali:** firewall, Intrusion Prevention System (IPS), Intrusion Detection System (IDS), VPN e proxy.
- **Protezione endpoint:** antivirus (AV), antivirus next-gen (NGAV), Endpoint/Extended Detection and Response (EDR/XDR).
- **Compilazione centralizzata di log:** strumenti SIEM (gestione delle informazioni e degli eventi di sicurezza), server Syslog e archiviazione dei dati sul cloud.
- **Autenticazione:** servizi di autenticazione a più fattori e servizi IAM (gestione delle identità e degli accessi).
- **Intelligence sulle minacce:** intelligence strategica di correlazione e brand monitoring, che segnala un'eventuale esposizione esterna.

Strumenti e tecniche di monitoraggio

Implementare i giusti strumenti e tecniche di monitoraggio è di importanza vitale per identificare e rispondere agli incidenti con la massima efficacia. Considera i seguenti approcci:

- **Monitoraggio costante:** applica la combinazione tra monitoraggio in tempo reale e periodico, per mantenere visibilità completa sul tuo ambiente.
- **Rilevamento delle anomalie:** approfitta degli algoritmi avanzati di analisi e di machine learning per identificare pattern e comportamenti insoliti che potrebbero indicare la presenza di una potenziale minaccia.
- **Correlazione dei log:** aggrega e metti in correlazione i dati di log raccolti da più origini, per identificare pattern e tendenze che potrebbero indicare che è in corso un attacco.
- **Prioritizzazione degli avvisi:** sviluppa un processo che assegni la giusta priorità agli avvisi, in base a fattori quali criticità, impatto potenziale e livello di minaccia.

Concentrandoti sul tuo ambiente, applicando livelli efficaci di rilevamento e protezione e implementando validi strumenti e tecniche di monitoraggio, puoi migliorare significativamente le capacità della tua organizzazione di identificare e rispondere agli incidenti di sicurezza in maniera tempestiva e mirata.

Comunicazioni

Una strategia di comunicazione efficace è fondamentale durante l'incident response, in quanto permette la coordinazione e collaborazione immediata tra tutte le persone interessate. Questa sezione descrive le considerazioni più importanti per le comunicazioni interne ed esterne nel contesto dell'incident response, valutando anche l'impatto dei requisiti legali.

Comunicazioni interne

- **Strategia di comunicazione:** definisci una strategia di comunicazione completa, che descriva in maniera dettagliata i percorsi di escalation, i canali di comunicazione e le principali persone di riferimento. La strategia deve essere rivista e aggiornata periodicamente, per garantirne l'efficacia in caso di incidente.
- **Team di incident response:** crea un team di incident response e nomina un responsabile del team che coordini le attività di risposta. Assicurati che i membri del team comprendano i propri ruoli e responsabilità, e mantieni canali di comunicazione aperti per l'intera la durata dell'incidente.
- **Proteggi i canali di comunicazione:** utilizza canali di comunicazione sicuri e affidabili, per impedire l'accesso non autorizzato alle informazioni di natura sensibile. Considera l'adozione di applicazioni di messaggistica crittografate, l'invio di messaggi e-mail sicuri oppure l'uso di piattaforme di comunicazione dedicate.
- **Modelli di risposta:** crea un catalogo di modelli di risposta predefiniti che possano essere applicati a vari scenari diversi. In questo modo garantirai comunicazioni più rapide e coerenti. Questi modelli devono essere accessibili, personalizzabili e allineati con le linee guida per la comunicazione dell'intera organizzazione.
- **Aggiornamenti per le persone interessate:** invia aggiornamenti regolari alle persone interessante durante l'intero processo di gestione degli incidenti. Manda report sulla situazione, sulle azioni intraprese e sugli esiti attesi. Questo livello di trasparenza può aiutare a preservare la fiducia pubblica nelle capacità dell'organizzazione di gestire l'incidente.

Comunicazioni esterne

- **Strategia per le notifiche:** sviluppa una strategia di comunicazione per le notifiche a clienti, vendor, partner e forze dell'ordine, da applicare in caso di violazioni di sicurezza o di altri incidenti che potrebbero coinvolgerli. La strategia deve definire i criteri per l'invio delle notifiche, i canali da utilizzare e i responsabili della gestione delle comunicazioni.
- **Conformità legale e normativa:** assicurati che le comunicazioni esterne rispettino i requisiti legali e normativi, incluse le leggi sulla protezione dei dati, le linee guida sulla divulgazione responsabile e le normative applicabili al proprio settore di attività. Rivolgiti a consulenti legali che possano confermare che tali comunicazioni siano conformi a tutti gli obblighi applicabili.
- **Portavoce designato:** nomina un portavoce designato o un team di pubbliche relazioni che gestisca le inchieste dei media e le dichiarazioni pubbliche, per garantire un messaggio coerente e accurato. Questa persona o questo team deve avere esperienza nell'ambito delle comunicazioni di crisi e nell'interazione con i mass media.
- **Preparazione per le comunicazioni esterne:** prepara modelli di comunicazioni per i vari scenari possibili, in modo da permettere la notifica chiara e rapida dell'incidente a terze parti esterne. Personalizza questi modelli in modo da soddisfare le esigenze specifiche delle varie persone interessate, ad esempio clienti, partner ed enti normativi.
- **Collaborazione con altri reparti:** collabora a stretto contatto con il team legale, di pubbliche relazioni e altri reparti interessati, per assicurarti che le comunicazioni esterne soddisfino requisiti quali la conformità alle normative, la protezione della reputazione dell'organizzazione e la trasparenza con le parti coinvolte.

Implementando queste strategie di comunicazione, la tua organizzazione può avviare una risposta coordinata ed efficace agli incidenti di cybersecurity, preservando, in ultima analisi, la fiducia pubblica nelle capacità dell'organizzazione di gestire dell'incidente.

Formazione e sensibilizzazione sulla sicurezza

Sensibilizzare i dipendenti in materia di minacce e best practice di cybersecurity è fondamentale per preservare il profilo di sicurezza di un'organizzazione. In questa sezione scopriremo quali sono i componenti fondamentali di un programma completo di formazione e sensibilizzazione sulla sicurezza; parleremo inoltre dei contenuti e della frequenza dei corsi, nonché delle esercitazioni e delle simulazioni di attacco.

Programmi di sensibilizzazione sulla sicurezza

- **Obiettivi del programma:** definisci obiettivi chiari per il tuo programma di sensibilizzazione sulla sicurezza, concentrandoti principalmente sulle conoscenze da acquisire e sui comportamenti da adottare per proteggere le risorse e le informazioni dell'azienda.
- **Formazione mirata:** sviluppa risorse di formazione personalizzate per i vari ruoli e reparti all'interno dell'organizzazione, tenendone in considerazione le diverse responsabilità e il livello di accesso alle informazioni di natura sensibile.
- **Aggiornamenti costanti:** aggiorna regolarmente il programma di sensibilizzazione sulla sicurezza, in modo da riflettere le evoluzioni del panorama delle minacce e da integrare le nuove tendenze e regole di best practice.
- **Metriche e valutazioni:** monitora e misura l'efficacia del programma di sensibilizzazione sulla sicurezza con indicatori chiave di prestazione (KPI) quali il livello di coinvolgimento dei dipendenti, i tassi di comportamento dei corsi di formazione e il miglioramento dei comportamenti di sicurezza.

Contenuti e frequenza dei corsi di formazione

- **Sviluppo dei contenuti:** crea contenuti di formazione utili e interessanti, che includano un'ampia selezione di argomenti quali la gestione delle password, la sensibilizzazione sul phishing, il social engineering e la navigazione sicura on-line.
- **Erogazione dei corsi:** offri formati diversi di formazione, inclusi corsi on-line, workshop in presenza e webinar interattivi, per rispondere a varie preferenze e tempistiche di apprendimento.
- **Frequenza:** pianifica sessioni di formazione regolari nel corso dell'anno, con una frequenza minima consigliata di una volta ogni tre mesi. Puoi anche fornire sessioni di formazione on-demand in seguito a un incidente o all'insorgere di nuove minacce.

- **Apprendimento continuo:** promuovi una cultura di apprendimento continuo, offrendo ai dipendenti accesso a risorse aggiuntive come articoli, video e podcast, per aiutarli a incrementare le conoscenze in ambito di cybersecurity.

Esercitazioni e simulazioni di attacco

- **Scenari realistici:** realizza esercitazioni e simulazioni di attacco basate su situazioni realistiche, in cui i dipendenti si potrebbero trovare mentre svolgono il loro lavoro. Questi scenari possono aiutare i dipendenti a comprendere meglio il potenziale impatto di una violazione di sicurezza e a mettere in pratica le proprie capacità di risposta.
- **Collaborazione interfunzionale:** coinvolgi più dipartimenti nelle esercitazioni e nelle simulazioni, promuovendo la collaborazione e la comunicazione tra i vari team, favorendone così la condivisione delle competenze.
- **Valutazione e feedback:** Svolgi una valutazione accurata della performance dei dipendenti durante le esercitazioni e le simulazioni di attacco. Fornisci feedback costruttivo e identifica gli ambiti da migliorare.
- **Lezioni importanti apprese:** condividi con l'intera organizzazione le lezioni importanti apprese durante le esercitazioni e le simulazioni, consolidando i principali concetti e regole di best practice.

Adottando un valido programma di formazione e sensibilizzazione sulla sicurezza, le organizzazioni possono fornire ai dipendenti tutte le conoscenze e le competenze necessarie per identificare e rispondere alle minacce di cybersecurity. Tutto questo può, in ultima analisi, contribuire alla riduzione del rischio che gli attacchi vadano a segno.

Team di incident response

Un team di incident response efficace è di importanza vitale per avviare una risposta coordinata e tempestiva agli incidenti di sicurezza. In questa sezione osserveremo i vari ruoli e responsabilità, analizzando come sono composti i team e valutando l'importanza dell'assistenza e dell'esperienza di un team esterno di incident response.

Ruoli e responsabilità

- **Incident response manager:** supervisiona il processo di incident response, coordina le attività del team e assicura una comunicazione efficace tra i membri del personale interno e le persone interessate all'esterno dell'organizzazione.
- **Analisti di sicurezza:** svolgono indagini e analizzano gli incidenti di sicurezza, mettendo a disposizione le proprie competenze tecniche per aiutare a identificare la causa originaria, l'estensione e l'impatto dell'incidente.
- **Analisti forensi:** svolgono attività di analisi digitale forense, che includono la raccolta, l'analisi e la conservazione di prove, per favorire le indagini e i procedimenti legali.
- **IT Operations:** questo team offre assistenza durante le attività di contenimento, estirpazione delle minacce e ripristino dei sistemi. Gestisce l'infrastruttura informatica e implementa i cambiamenti necessari per prevenire incidenti futuri.
- **Reparto legale e di rispetto della conformità:** offre consulenza sui requisiti legali e normativi associati all'incident response, per garantire l'adeguata divulgazione e segnalazione dei fatti.
- **Pubbliche relazioni e comunicazioni:** questo team gestisce le comunicazioni interne ed esterne, creando messaggi adeguati da inviare a tutte le parti interessate, ad esempio dipendenti, clienti, partner ed enti normativi.

Composizione del team di incident response

- **Rappresentazione interfunzionale:** crea un team composto da membri con background diversi, per rappresentare i vari reparti, inclusi IT, Sicurezza, Legale, HR e Comunicazioni. In questo modo coprirai i vari aspetti della natura interdisciplinare dell'incident response.
- **Esperienza e competenze:** assicurati che i membri del team abbiano l'esperienza e le competenze adatte per svolgere i ruoli a loro assegnati, offrendo opportunità continue di formazione e sviluppo.
- **Disponibilità e rotazione del personale:** crea un team che sia disponibile 24/7, applicando un sistema di disponibilità a rotazione o turni dedicati per garantire il monitoraggio ininterrotto.

Supporto e competenze esterni

- **Vendor di terze parti:** rivolgiti a esperti esterni, ad esempio consulenti di cybersecurity o Managed Security Service Provider (MSSP), per estendere le capacità del tuo team interno e approfittare delle conoscenze di tecnici specializzati in ambiti quali analisi forensi digitali o intelligence sulle minacce.
- **Consulenza legale:** cerca consulenza legale esterna, rivolgendoti a professionisti specializzati nelle leggi sulla cybersecurity e sulla privacy dei dati. Questi esperti dovranno offrire consulenza sui requisiti di conformità e divulgazione e dovranno rappresentare l'organizzazione in caso di procedimenti legali correlati a un incidente di sicurezza.
- **Forze dell'ordine e agenzie di regolamentazione:** stabilisci un dialogo costante con le forze dell'ordine e gli enti normativi pertinenti, in modo da agevolare la collaborazione e la condivisione di informazioni durante le indagini sugli incidenti.
- **Collaborazione nel settore:** partecipa ai forum e ai gruppi di discussione dedicati al settore della cybersecurity, condividendo dati di intelligence sulle minacce e best practice di sicurezza con altre organizzazioni, per affrontare in maniera adeguata le tendenze e le minacce emergenti.

Creando un team di incident response a tutto tondo e sfruttando assistenza ed esperti esterni, le organizzazioni possono gestire con maggiore efficacia gli incidenti di cybersecurity, riducendone il potenziale impatto.

Identificazione

La fase di identificazione è determinante per rilevare la presenza di un intruso all'interno di un sistema o di una rete. Monitorare continuamente i dati di telemetria della rete è pertanto fondamentale per ridurre i tempi che intercorrono tra l'intrusione e l'identificazione. Più rapidamente reagisce un team, minore sarà l'impatto dell'attacco sulla riservatezza, sull'integrità e sulla disponibilità di dati, sistemi e reti. Le soluzioni di Managed Detection and Response (MDR) possono essere un valido aiuto durante questo processo, in quanto offrono capacità di rilevamento e risposta alle minacce a cura di esperti.

Elementi principali dell'identificazione

- **Telemetria della rete e del dispositivo:** come indicato nella sezione dedicata alla telemetria, il monitoraggio completo di diverse origini potenziali è fondamentale per il rilevamento e la risposta alle minacce in tempo reale. Utilizzando una soluzione MDR, questo processo può diventare ancora più efficiente.
- **Comunicazioni esterne:** collaborare con le forze dell'ordine e con altre origini esterne per raccogliere e analizzare i dati di intelligence sulle minacce permette di identificare più rapidamente le potenziali intrusioni.
- **Intelligence sulle minacce:** il monitoraggio del dark web e dei siti web clandestini per identificare potenziali compromissioni dei sistemi aziendali in vendita su mercati illeciti aiuta a ottimizzare ulteriormente il rilevamento.
- **Segnalazione da parte degli utenti:** invita gli utenti a segnalare le e-mail o i link sospetti e a rispondere rapidamente alle minacce potenziali, per garantire che i responsabili della gestione degli incidenti ricevano immediatamente tutti i dati contestuali importanti.

Occorre inoltre stabilire processi efficaci per classificare il livello di gravità di un incidente, in base ai seguenti criteri:

- **Affidabilità:** questo criterio si riferisce all'attendibilità dell'origine (ad es. IPS, FW, AV, XDR).
- **Criticità:** considera l'importanza del sistema coinvolto.
- **Pericolosità:** valuta il comportamento sospetto, che fornisce indizi che possono a loro volta portare all'identificazione di una violazione precedentemente inosservata.
- **Tipo di incidente:** utilizza framework come la Cyber Kill Chain e MITRE ATT&CK per classificare gli incidenti.
- **Timestamp:** garantisci la sincronizzazione dei timestamp utilizzando UTC, NTP e altri standard comuni di normalizzazione dei dati.

Tipi di incidenti

NIST classifica gli incidenti in due categorie:

- **Precursore:** per questo tipo di incidente occorre rilevare indicatori di tentativi di ricognizione, ad esempio attività volte a identificare porte aperte e vulnerabilità dei software. In questo contesto, le soluzioni MDR possono risultare particolarmente utili. È necessario identificare gli exploit noti delle vulnerabilità nel codice remoto presenti nell'infrastruttura dell'organizzazione.
- **Indicatore:** il rilevamento di questo tipo di incidente implica l'identificazione di vari incidenti che rappresentano segnali importanti, come avvisi di malware, modifiche ai file o ad Active Directory oppure comportamenti insoliti degli utenti (ad esempio l'accesso tramite RDP a orari anomali). Successivamente, occorre avviare un'incident response adeguata. Le soluzioni MDR possono fornire assistenza supplementare per i processi di rilevamento e risposta a questi tipi di incidenti.

Adottando una strategia di monitoraggio a 360 gradi che sfrutti le notifiche e i dati di intelligence sulle minacce provenienti da origini esterne, che inviti gli utenti a segnalare gli eventi insoliti e che utilizzi criteri ben definiti per la classificazione degli incidenti, le organizzazioni possono migliorare il proprio profilo di sicurezza complessivo. Inoltre, l'integrazione di soluzioni MDR può offrire assistenza supplementare per il rilevamento e la risposta a questi tipi di incidenti. Per essere efficace, la fase di identificazione non deve limitarsi a ridurre l'impatto degli incidenti di sicurezza, ma deve anche promuovere una cultura di sicurezza proattiva all'interno dell'organizzazione. Questa strategia contribuisce, in ultima analisi, a favorire la continuità aziendale e la protezione delle risorse più importanti.

File, directory, processi potenzialmente sospetti e persistenza

Capire e identificare file, directory, processi potenzialmente sospetti e meccanismi di persistenza può aiutare le organizzazioni a rilevare tempestivamente gli incidenti.

- **File e directory:** la presenza di file e directory insoliti o inattesi può indicare che è in corso un incidente di sicurezza. Alcuni esempi includono:
  - File con estensioni o nomi poco comuni
  - File in percorsi inattesi
  - Directory contenenti dati di natura sensibile che dovrebbero essere inaccessibili
- **Processi:** i processi sospetti potrebbero essere indicatori di attività pericolose in un sistema. Alcuni esempi includono:
  - Processi che presentano un utilizzo elevato della CPU o della memoria
  - Processi che si eseguono da percorsi insoliti
  - Processi che cercano di accedere a dati o risorse sensibili
- **Persistenza:** spesso i cybercriminali stabiliscono meccanismi di persistenza per mantenere l'accesso ai sistemi che sono riusciti a violare. Alcuni esempi di tecniche di persistenza includono:
  - Attività pianificate oppure operazioni cron che eseguono script dannosi
  - Malware che si reinstalla dopo la rimozione o il riavvio
  - Chiavi di registro o elementi di avvio che attivano processi dannosi
- **Accesso con credenziali:** le credenziali ottenute in maniera illecita possono portare a un'ulteriore compromissione dei sistemi e dei dati di natura sensibile. Alcuni esempi includono:
  - Attacchi di tipo brute force contro gli account degli utenti
  - Campagne di phishing che cercano di prelevare le credenziali dei dipendenti
  - Dump delle credenziali dei sistemi compromessi
- **Ulteriori infiltrazioni/accessi:** gli autori degli attacchi potrebbero cercare di infiltrarsi nell'ambiente di un'organizzazione anche in altri modi, per estendere le proprie capacità di accesso e di controllo. Alcuni esempi includono:
  - Compromissione degli account di utenti con privilegi elevati
  - Exploit di vulnerabilità a cui non sono state applicate patch nei sistemi o nelle applicazioni
  - Movimenti laterali all'interno della rete per accedere ad altre risorse

Riconoscendo questi tipi di incidenti e come si possono manifestare, le organizzazioni hanno la possibilità di identificare con maggiore certezza le potenziali minacce e avviare pertanto un'azione di risposta adeguata. Accertarsi che tutti gli utenti siano consapevoli dei vari tipi di incidenti è fondamentale affinché un'organizzazione possa rilevare e mitigare tempestivamente gli attacchi di sicurezza.

Analisi forensi

Le analisi forensi sono un aspetto cruciale del processo di incident response, in quanto aiutano le organizzazioni a identificare la causa originaria di un incidente, nonché a comprenderne l'impatto e a raccogliere prove destinate ad ampliare le indagini o a essere presentate durante i ricorsi legali. Di seguito vengono indicati alcuni degli elementi principali delle analisi forensi:

Strumenti e tecniche di analisi forense

Sono disponibili vari strumenti e tecniche di analisi forense per aiutare i ricercatori a svolgere l'analisi dei sistemi e delle reti durante il processo di incident response. Questi strumenti possono assistere in fase di raccolta, analisi e conservazione dei dati. Alcuni esempi di strumenti e tecniche di analisi forense includono:

- Strumenti di creazione e clonazione di immagini dei dischi, per preservare lo stato di un sistema compromesso
- Strumenti di analisi della memoria, per indagare sui dati volatili e identificare i processi dannosi
- Strumenti di analisi del traffico di rete, per valutare le attività della rete e individuare potenziali indicatori di compromissione
- Strumenti di analisi dei log, per permettere la revisione dei log di sistema e delle applicazioni, alla ricerca di tracce di attività sospetta

Raccolta e conservazione delle prove

Un'adeguata raccolta e conservazione delle prove è fondamentale per le analisi forensi, in quanto permette di garantire l'integrità dei dati e di preservarne l'ammissibilità durante i procedimenti legali. Alcune best practice per la raccolta e la conservazione delle prove includono:

- Documentare ogni fase del processo di raccolta di prove, inclusi gli strumenti e le tecniche utilizzati.
- Creare una cronologia dettagliata degli eventi correlati all'incidente.
- Utilizzare write blocker e altri strumenti di analisi forense per impedire l'alterazione delle prove durante la raccolta.
- Proteggere i dati raccolti in container antimanomissione o in supporti di archiviazione cifrati.
- Garantire che i dati raccolti vengano conservati in un ambiente sicuro e controllato.

Catena di custodia

L'implementazione di una catena di custodia adeguata è essenziale per preservare l'integrità delle prove e per garantirne l'ammissibilità nelle procedure legali. Il termine "catena di custodia" definisce la documentazione e il monitoraggio della gestione, della conservazione e del trasferimento delle prove durante le indagini. Per garantire una catena di custodia adeguata, le organizzazioni devono:

- Registrare i dettagli di ogni persona fisica che maneggia le prove, inclusi nome, ruolo e informazioni di contatto.
- Documentare data, ora e luogo ogni volta che le prove vengono trasferite o maneggiate.
- Registrare tutte le azioni svolte sulle prove, ad esempio: copia, analisi o archiviazione.
- Assicurarsi che le prove vengano sempre conservate e trasportate in maniera sicura, utilizzando sigilli antimanomissione o supporti di archiviazione cifrati.

Integrando le analisi forensi nel processo di incident response, le organizzazioni possono ottenere informazioni molto utili sulla natura e sull'estensione degli incidenti di sicurezza. Possono inoltre raccogliere prove di importanza cruciale e facilitare ulteriori indagini o ricorsi legali. Capire e implementare strumenti, tecniche e pratiche forensi adeguate è essenziale per svolgere analisi approfondite ed efficaci.

Esfiltrazione Dei Dati

Il termine "esfiltrazione dei dati" viene utilizzato per definire il trasferimento non autorizzato di informazioni o dati di natura sensibile dai sistemi o dalla rete di un'organizzazione a un luogo esterno, solitamente controllato da un hacker. Rilevare e prevenire l'esfiltrazione dei dati è di vitale importanza per ridurre l'impatto delle violazioni dei dati e per proteggere le risorse di maggior valore. Per affrontare il problema dell'esfiltrazione dei dati in maniera efficace, le organizzazioni devono considerare i seguenti aspetti:

- **Monitoraggio e avvisi:** implementa un sistema completo di monitoraggio, in modo da rilevare i trasferimenti di dati o i pattern di traffico insoliti, come i trasferimenti di un numero elevato di file, le comunicazioni con indirizzi IP sospetti oppure la presenza di tentativi multipli di accesso non riusciti. Assicurati di applicare meccanismi di avviso adeguati, in modo da informare il personale competente in caso di potenziali incidenti di esfiltrazione dei dati.
- **Soluzioni DLP (Data Loss Prevention):** implementa soluzioni DLP per identificare e impedire l'invio di dati sensibili all'esterno della rete della tua organizzazione. Le soluzioni DLP aiutano a rilevare e bloccare il trasferimento non autorizzato delle informazioni di natura sensibile, in base a criteri e regole predefiniti.
- **Cifratura:** cifra i dati sensibili sia quando sono inattivi, sia quando si trovano in transito, per diminuire il valore dei dati agli occhi di un cybercriminale, in caso di esfiltrazione.
- **Corsi di formazione e sensibilizzazione dei dipendenti:** educa i dipendenti a riconoscere i rischi derivati dall'esfiltrazione dei dati e a comprendere l'importanza di attenersi alle policy di sicurezza, evitando ad esempio di condividere informazioni sensibili su canali non protetti o con personale non autorizzato.

Conferma e prioritizzazione

Una volta identificato un potenziale incidente di sicurezza, è essenziale confermare che si tratti di un incidente e assegnare priorità alle varie attività di risposta, in base alla gravità e al potenziale impatto sull'organizzazione. La conferma e la prioritizzazione prevedono i seguenti passaggi:

- **Conferma dell'incidente:** verifica che l'incidente identificato sia un evento di sicurezza a tutti gli effetti e non un falso positivo. Per farlo, puoi analizzare i dati disponibili, metterli in correlazione con dati di intelligence sulle minacce note e controllare il contesto dell'evento.
- **Assegnazione di priorità all'incidente:** valuta il potenziale impatto dell'incidente sulle risorse, sulle operazioni e sulla reputazione dell'organizzazione. Considera fattori quali il tipo di dati o i sistemi coinvolti, l'estensione della violazione e le potenziali conseguenze dell'incidente.
- **Livelli di gravità:** assegna un livello di gravità all'incidente, basandoti sulla valutazione delle priorità. I livelli di gravità possono essere definiti utilizzando una scala preimpostata (ad esempio livello basso, medio, alto o critico) e devono aiutare il team di incident response a definire l'urgenza dell'intervento e a stabilire quali risorse dedicare alla risposta.
- **Piano di risposta:** in base al livello di gravità e alla natura dell'incidente, seleziona il giusto piano di risposta dal playbook di incident response dell'organizzazione. Questo piano deve definire i passaggi necessari per contenere l'incidente, svolgere indagini e applicare azioni correttive. Deve inoltre indicare tutte le procedure di comunicazione e segnalazione necessarie.

Identificando, confermando e attribuendo la giusta priorità agli incidenti di sicurezza, le organizzazioni possono garantire un processo di assegnazione efficiente delle proprie risorse. In questo modo, le attività di risposta saranno concentrate sugli incidenti più critici, riducendo l'impatto complessivo sull'organizzazione.

Estirpazione

L'estirpazione è il processo di rimozione di ogni traccia della minaccia o dell'autore dell'attacco dall'ambiente informatico. Spesso include più fasi, volte a identificare, documentare e rimuovere qualsiasi attività degli hacker, modifica del sistema, malware ed esecuzione di elementi dannosi su computer e rete. Poiché la maggior parte degli attacchi informatici utilizza più metodi di infiltrazione e attacchi di tipo "hands-on-keyboard", è fondamentale identificare eventuali irregolarità che potrebbero eludere il rilevamento da parte delle scansioni. Durante il processo di estirpazione di una minaccia, è essenziale considerare tutti i potenziali effetti che potrebbero derivarne.

Per l'estirpazione, è possibile scegliere tra due strategie principali: la ricompilazione e ricreazione dell'immagine del computer, oppure la rimozione mirata. Entrambi gli approcci presentano punti di forza e debolezze, per cui spesso vengono svolti contemporaneamente per ottenere maggiore efficacia.

Ricompilazione o ricreazione dell'immagine del computer

Il metodo più efficace per estirpare le minacce dalle risorse compromesse è ricompilare o ricreare le immagini degli host, effettuando un completo ripristino a uno stato precedente e integro. Questo processo risulta più semplice quando le organizzazioni applicano immagini software standard sugli host e hanno accesso all'immagine master per il ripristino. L'immagine master deve essere creata prima dell'implementazione nel sistema di produzione, per garantire che non sia stata compromessa.

Per i server di importanza critica (come i sistemi di ERP, i server di posta e i file server), il ripristino da un'immagine master precedente non è una pratica comune, a causa dei potenziali rischi di perdita dei dati e dei costi che ne risulterebbero. Le organizzazioni possono invece eseguire il ripristino da un file di backup pulito (ad es. server di backup, backup su nastro, cloud o altri supporti). Questo processo richiede la verifica della disponibilità e dell'integrità dei file di backup, nonché la selezione di uno stato di ripristino non infettato. Per applicare la migliore strategia di ricompilazione e ricreazione delle immagini, le organizzazioni devono svolgere indagini a livello di rete sugli indicatori di compromissione e sulle tattiche, tecniche e procedure (TTP) degli hacker, concentrandosi in particolar modo sui computer più vulnerabili.

Rimozione mirata

La strategia di rimozione mirata ha l'obiettivo di identificare tutti i singoli malware e artefatti dannosi, nonché di determinare le modifiche del sistema più significative che sono state effettuate dagli antagonisti informatici, per poi rimuovere i malware o ripristinare i sistemi interessati al loro stato pre-compromissione. Questo approccio è necessario per i computer che supportano i sistemi di produzione, i sistemi di controllo industriale o altre funzionalità business-critical, per i quali eventuali perdite dei dati o periodi di inattività sarebbero devastanti.

La rimozione mirata viene spesso messa in atto con una combinazione tra gli strumenti di sicurezza e l'intervento di esperti di incident response in grado di individuare proattivamente le minacce basandosi sugli indicatori di compromissione e sui dati di intelligence sulle minacce osservati, nonché grazie all'esperienza che hanno maturato in ambito di TTP degli hacker. Le organizzazioni possono utilizzare la rimozione mirata per ottenere una comprensione più approfondita dell'attacco, ricavandone lezioni importanti da implementare nella propria strategia di miglioramento a lungo termine, al fine di ridurre il rischio di attacchi informatici in futuro.

Se, ad esempio, un cybercriminale riesce a compromettere un host sfruttando vulnerabilità esistenti, errori di configurazione o una violazione avvenuta in passato ma rimasta inattiva, l'estirpazione deve anche includere l'attenuazione di tali vulnerabilità. Sarà così possibile impedire che l'host venga utilizzato come vettore per la reinfezione o per un nuovo attacco. Una root cause analysis può aiutare le organizzazioni a identificare tutte le azioni svolte da un hacker prima che l'impatto dell'attacco diventasse evidente, individuando il paziente zero al fine di prevenire attacchi futuri.

Consigliamo alle aziende di continuare a documentare i risultati delle indagini e di utilizzare framework come MITRE ATT&CK per concettualizzare la struttura di un attacco. Questo approccio strutturato facilita il processo di identificazione della causa originaria di un incidente e permette alle organizzazioni di migliorare il proprio profilo di sicurezza complessivo.

Ripristino

L'obiettivo della fase di ripristino è riportare, con un approccio a fasi, i computer e i sistemi colpiti dall'attacco a uno stato operativo normale, restituendo all'organizzazione la stessa funzionalità pre-incidente. La strategia di ripristino dipende dall'incidente subito, in quanto in alcuni casi la risposta adottata può prevedere il semplice isolamento di alcuni computer, con impatto operativo minimo sull'organizzazione. Tuttavia, gli attacchi estesi come il ransomware possono colpire una grande quantità di computer, causando tempi di inattività e ripercussioni devastanti sulle capacità operative. I piani di ripristino devono pertanto essere personalizzati in base all'attacco.

- Un singolo host infettato da un'e-mail di phishing con un payload che è stato rilevato e rimosso dalla protezione endpoint potrebbe richiedere semplicemente l'isolamento del computer interessato per l'intera durata delle indagini, fino a quando gli analisti di sicurezza non siano certi di avere rimosso completamente la minaccia. Questo scenario implica complessivamente un impatto operativo minimo.
- Il rilevamento tempestivo di una botnet che ha infettato due computer degli utenti nella rete sui quali sono stati installati meccanismi di persistenza potrebbe richiedere l'isolamento immediato e la ricompilazione dei computer colpiti. Una situazione simile potrebbe implicare tempi di inattività per i dipendenti, ma un impatto operativo minimo sull'azienda.
- Un attacco ransomware in cui è coinvolta l'intera rete, caratterizzato da diverse settimane di persistenza nei sistemi e con causa originaria identificata richiederà non solo l'isolamento degli endpoint, ma anche di e-mail, VPN, account Active Directory e altri servizi. In questo caso i responsabili dell'incident response dovranno applicare misure di contenimento adeguate fino a quando l'identificazione dei metodi di infiltrazione utilizzati, l'applicazione delle patch e la ricreazione delle immagini dei computer non riportino l'attacco sotto controllo. Le potenziali strategie da adottare in questi casi possono includere la creazione di una rete alternativa "pulita", ricompilata senza i computer infettati, nella quale vengono reintegrati i computer uno per uno. La decisione di reintegrare i computer isolati deve essere presa solo se il rischio di reinfiltrazione e reinfezione è basso. I responsabili dell'incident response dovranno quantificare il rischio e comunicarlo al management, in modo che possano essere concordati approcci e tempistiche adeguati in base alle esigenze dell'azienda.

Un approccio prudente

Il ripristino dei computer è un'attività che richiede estrema concentrazione e una particolare attenzione ai dettagli critici del sistema, in quanto un eccesso di certezza nel ritenere che una minaccia sia stata rimossa, sommato allo stress della gestione dell'incidente, può essere deleterio. È fondamentale rimanere vigili e prestare attenzione a quanto segue:

- Integrità complessiva dei sistemi di tutti i computer interessati, man mano che vengono reintegrati nella rete. Occorre quindi verificare l'integrità dei dati e la stabilità del sistema.
- Applicazione di patch alle vulnerabilità di sicurezza, in particolar modo dopo aver ripristinato un computer da una versione precedente che potrebbe essere soggetta allo stesso attacco.
- Verifica dell'adeguata applicazione di criteri e controlli di sicurezza per ogni singolo computer:
  - L'agent di sicurezza deve essere installato su tutti i computer reintegrati nella rete.

Analisi Post-Incidente E Lezioni Importanti Apprese

Una volta riprese le normali attività operative in seguito a un incidente di cybersecurity, è fondamentale svolgere un'analisi post-incidente e identificare le lezioni importanti apprese. Questo processo aiuterà la tua organizzazione a valutare l'efficacia della strategia di incident response, a identificare eventuali ambiti da migliorare e ad apportare modifiche al piano di incident response. In questo modo, potrai prepararti in maniera più efficace ad affrontare eventuali incidenti futuri e sarai in grado di ridurre il rischio di violazioni simili.

Analisi post-incidente

Valutazione dell'efficacia della strategia di incident response

Per valutare l'efficacia della strategia di incident response della tua organizzazione, analizza le azioni intraprese dal team di incident response, misurandone i risultati. Considera i seguenti aspetti:

- Tempo necessario per rilevare, contenere e rimediare ai danni dell'incidente
- Comunicazione e coordinazione interna tra i membri del team ed esterna con terze parti (ad es. forze dell'ordine, vendor)
- Idoneità delle strategie di contenimento, estirpazione e ripristino
- Precisione e utilità delle informazioni fornite dagli strumenti di monitoraggio e rilevamento

Identificazione degli ambiti da migliorare

Una volta valutata l'efficacia della strategia di incident response, occorre identificare gli ambiti nei quali la tua organizzazione può migliorare processi e procedure. Alcuni dei più comuni ambiti da migliorare possono includere:

- Programmi di formazione e sensibilizzazione del personale
- Capacità di rilevamento e monitoraggio dell'incidente
- Aggiornamento del piano di incident response
- Controlli tecnici e misure di sicurezza
- Ruoli e responsabilità dei team di incident response
- Comunicazione esterna e collaborazione con le parti interessate

Implementazione di modifiche e aggiornamenti del piano di incident response

Una volta identificati gli ambiti da migliorare, è fondamentale implementare le giuste modifiche al piano di incident response della tua organizzazione. Assicurati di:

- Aggiornare il piano aggiungendo nuove procedure, linee guida o misure tecniche, secondo necessità.
- Comunicare le modifiche a tutte le parti coinvolte, inclusi dipendenti, management e persone interessate esterne all'organizzazione.
- Organizzare corsi di formazione ed esercitazioni a intervalli regolari, per verificare che il piano sia stato compreso da tutti e che possa essere implementato in maniera efficace.
- Monitorare e valutare l'efficacia delle modifiche nel tempo, introducendo ulteriori ottimizzazioni a seconda delle esigenze.

Conducendo un'analisi post-incidente accurata e identificando le lezioni importanti apprese, la tua organizzazione potrà migliorare il proprio profilo di cybersecurity e prepararsi meglio ad affrontare eventuali incidenti in futuro. Ricorda che l'incident response è un processo continuo e che la revisione e l'aggiornamento costante del piano ti aiuterà a garantire la resilienza della tua organizzazione, permettendole di contrastare minacce informatiche sempre più evolute.

Lezioni importanti apprese

Le lezioni importanti apprese dipenderanno dalla tipologia dell'incidente e da come è stato gestito. Rappresentano gli ambiti da migliorare che sono stati identificati. Quella delle lezioni importanti apprese è una fase essenziale, che tuttavia viene spesso trascurata quando l'organizzazione esce dallo stato di emergenza, i dirigenti non sono più coinvolti direttamente e la normalità operativa viene ripristinata. È proprio per questo motivo che è fondamentale avviare la fase delle lezioni importanti apprese subito dopo la fase di ripristino, coinvolgendo direttamente il management per capire ogni singolo dettaglio dell'incidente e per concordare i miglioramenti da implementare al fine di attenuare i rischi futuri.

Negli scenari più comuni, potrebbe prevedere un rapporto sull'incidente che includa un riepilogo da condividere con tutte le persone interessate all'interno dell'azienda e che deve risultare comprensibile anche dal personale non tecnico. Questo rapporto

deve essere collaborativo, con commenti e modifiche da parte di più persone interessate; la sua compilazione deve concludersi con il consenso di tutte le parti sulla versione finale del report, con dettagli sugli aspetti tecnici e sulle lezioni importanti apprese.

Alcuni dei potenziali ambiti da migliorare vengono indicati di seguito. Tuttavia, dato l'ampio spettro di possibilità, si tratta di un elenco tutt'altro che specifico e completo.

Best practice per la sicurezza consigliate:

- Rimuovi le autorizzazioni di software, applicazioni e hardware obsoleti all'interno dell'ambiente informatico aziendale, al fine di ridurre il rischio di exploit.
- Stabilisci un processo efficace di gestione delle patch per software e hardware; il processo deve essere in linea con le esigenze dell'organizzazione e deve prevedere l'aggiornamento regolare delle patch.
- Installa agent di protezione endpoint basata sul cloud in tutti i computer presenti nell'ambiente aziendale, in modo da consentire il rilevamento e la neutralizzazione delle minacce.
- Implementa l'autenticazione a più fattori (Multi-Factor Authentication, MFA) per VPN, RDP e altri servizi che richiedono autenticazione. Questo accorgimento permette di incrementare il livello di sicurezza.
- Salvaguarda l'infrastruttura informatica implementando meccanismi automatici per i principali controlli di sicurezza, proteggendo così i servizi connessi a internet dall'accesso non autorizzato.
- Migliora la gestione delle credenziali implementando requisiti obbligatori di complessità, utilizzando sistemi di gestione delle password ed eseguendo la rotazione regolare delle credenziali.
- Implementa protocolli di autenticazione della posta elettronica quali DMARC, DKIM e SPF, per proteggere i sistemi dalle e-mail di phishing e dai tentativi di spoofing.

Configurazione della rete:

- Implementa il controllo degli accessi alla rete (Network Access Control, NAC), per aggiungere un ulteriore livello di sicurezza e per proteggerti dalle minacce e dai dispositivi non autorizzati.
- Segrega le reti utilizzando VLAN per difendere i sistemi di importanza critica e i dati di natura sensibile; è anche consigliabile isolare le piattaforme e i servizi connessi a internet con una DMZ.

Protezione avanzata:

- Implementa il blocco geografico degli IP sui firewall, per prevenire il traffico di rete indesiderato in base all'origine geografica.
- Utilizza soluzioni di controllo delle applicazioni come AppLocker, per impedire che applicazioni e file non autorizzati vengano installati o eseguiti nell'ambiente aziendale.
- Incrementa il livello di protezione dei controller di dominio, valutando e rimuovendo i servizi superflui, i software non supportati e i protocolli obsoleti che potrebbero presentare rischi di sicurezza.

Gestione proattiva e precauzioni di sicurezza:

- **Controllo delle infrastrutture:** svolgi controlli regolari delle configurazioni delle porte per tutte le infrastrutture connesse a internet all'interno dell'organizzazione. Assicurati che vengano autorizzati solamente i protocolli strettamente necessari e che le porte per i flussi di rete siano configurate correttamente.
  - Per esempio: eth0 è connessa a internet, eth1 è raggiungibile solo internamente.
- **Verifica del controllo del web:** rivedi regolarmente le configurazioni del traffico web sui server proxy e su piattaforme simili per il flusso del traffico web. Applica controlli di sicurezza più severi ovunque possibile, attenendoti al principio del privilegio minimo. Implementa un criterio predefinito di negazione o blocco. Alcuni esempi:
  - Blocco dei tipi di file che presentano rischi evitabili per l'organizzazione.
  - Valutazione dei criteri predefiniti di classificazione per gli URL e i domini senza una categoria.
  - Esportazione dei dati statistici, per identificare anomalie, pattern o eventi sospetti e dannosi ricorrenti.

- Verifica dell'aggiornamento dei gruppi e dei criteri di sicurezza, in linea con il principio del controllo degli accessi in base al ruolo (Role-Based Access Control, RBAC).

- **Controllo dell'account:** esegui controlli regolari alla ricerca degli account di amministratori (o ruoli equivalenti) non standard e non approvati nell'organizzazione, allo scopo di rimuoverli.
- **Registri eventi Windows:** configura i registri eventi Windows in modo che conservino dati quali l'aumento delle dimensioni dei registri eventi Windows principali attraverso i criteri di gruppo, oppure la creazione di nuovi registri di eventi una volta raggiunti i limiti. I registri eventi Windows offrono informazioni forensi molto importanti.
- **Piano di incident response:** sviluppa, implementa, metti alla prova e mantieni un piano di risposta agli incidenti di cybersecurity per l'organizzazione. Rivedi e sottoponi regolarmente a test questo piano, aggiornandone e ottimizzandone i contenuti secondo necessità.
- **Gestione delle risorse hardware e software:** implementa la gestione delle risorse hardware e software nell'intera organizzazione. Integra valutazioni basate su priorità/criticità nella soluzione di gestione delle risorse, per identificare rapidamente gli asset più importanti. Conserva un inventario aggiornato di risorse hardware e software, per poter identificare potenziali rischi e per consentire la formulazione di piani strategici di risposta a tali rischi.
- **Topologia della rete:** compila e aggiorna regolarmente un diagramma di alto livello della topologia della rete dell'organizzazione, in modo da fornire un quadro di riferimento per la revisione delle configurazioni e dei tipi di infrastrutture esistenti. Questa risorsa può essere molto utile durante la formulazione di piani strategici per le modifiche e le implementazioni sulla rete. Durante un attacco informatico, un diagramma della topologia della rete può aiutare i responsabili dell'incident response a capire la struttura organizzativa della rete, consentendo così di eseguire azioni di incident response più mirate e tempestive.

Integrità dei dati

Backup:

- Proteggi i dati di backup implementando varie soluzioni di backup diverse, conservando i dati di backup in percorsi di rete completamente segregati o in tipi di supporti multimediali indipendenti dalla struttura aziendale. Consigliamo anche di gestire gli accessi con controlli di sicurezza adeguati.
  - Inizia dall'impostazione di soluzioni di ridondanza dei backup, facendo riferimento alla regola 3-2-1 e applicando una cifratura adeguatamente sicura ai dati di backup inattivi: crea 3 copie dei dati, archivia i dati su almeno 2 tipi di supporti multimediali, conserva almeno 1 copia dei dati all'esterno della struttura.

Cifratura:

- Applica la cifratura completa del disco a computer, dispositivi mobili e unità USB, per difendere i dati dall'accesso non autorizzato in caso di furto o smarrimento di un dispositivo.
- Proteggi i dati inattivi all'interno dell'organizzazione applicando la crittografia at-rest (Data At Rest Encryption, DARE), attribuendo maggiore priorità ai dati più sensibili. Assicurati di implementare meccanismi di cifratura adeguati per i dati di rete in transito, ad esempio utilizzando la versione più recente di TLS (Transport Layer Security) per le comunicazioni cifrate. TLS richiede certificati digitali e impedisce ai server di eseguire il downgrade delle suite di cifratura per sfruttare tipi di browser non supportati.

Investimenti in ambito di cybersecurity

Approfitta delle lezioni importanti apprese dagli incidenti di sicurezza e usale a supporto delle richieste di una quantità maggiore di fondi e budget da destinare al potenziamento del profilo di sicurezza dell'organizzazione.

- Investi in corsi di sensibilizzazione e formazione del personale. Poiché spesso il vettore iniziale di attacco sono proprio gli esseri umani, ti consigliamo di investire in questi ambiti:

- Corsi di formazione e sensibilizzazione sul phishing o soluzioni volte a educare gli utenti finali, mettendoli alla prova con test sulle più comuni tecniche di phishing. Integra questa formazione nell'azienda come esercitazione continua, per mezzo di implementazioni pianificate o simulazioni di attacco automatizzate. Queste soluzioni forniscono inoltre al team IT la reportistica necessaria per identificare le vittime più frequenti e offrono ulteriore consulenza.
- Sviluppo delle competenze del personale in materia di IT security, in particolar modo nell'ambito di analisi di sicurezza, threat hunting e incident response.

Servizi di cybersecurity gestiti

- Affidati a un team di professionisti di cybersecurity, specializzati nelle analisi di sicurezza, nel threat hunting, nell'incident response, nella progettazione di strumenti di rilevamento e sicurezza ecc. L'implementazione di un Security Operation Center permette alle aziende di monitorare le minacce e intraprendere azioni di risposta 24/7.
- Investi in una soluzione di cybersecurity gestita come Sophos Managed Detection and Response (MDR). I servizi MDR sono Security Operations Center (SOC) in outsourcing, composti da un team di specialisti che svolge la funzione di un'estensione del personale di sicurezza del cliente.

Investimenti negli strumenti di sicurezza

- Sophos XDR (Extended Detection and Response) è una soluzione che archivia e permette di eseguire query su informazioni critiche raccolte da endpoint, server, firewall, e-mail e altri prodotti compatibili con XDR, semplificando così i flussi di lavoro del processo di rilevamento e risposta alle minacce.
- Le tecnologie SIEM (Security Information and Event Management) offrono opzioni di rilevamento delle minacce, rispetto della conformità e gestione degli incidenti, in quanto agiscono raccogliendo eventi e informazioni da varie origini di dati, inserendole in un archivio centrale di dati sulle minacce.
- Potrebbe essere consigliabile investire in ulteriori soluzioni, a seconda delle lezioni importanti apprese. I prodotti devono contribuire al miglioramento del profilo di sicurezza, un requisito che verrà misurato in base alla capacità di queste soluzioni di colmare le lacune negli ambiti di protezione/filtro, rilevamento e monitoraggio. Questi strumenti possono includere antivirus, sistemi di prevenzione/rilevamento delle intrusioni (IPS/IDS), firewall ecc.

Focalizzandosi su questi comuni ambiti da migliorare, la tua organizzazione può ottimizzare significativamente il profilo di sicurezza, incrementando allo stesso tempo la protezione contro eventuali incidenti informatici futuri. Ricorda che il processo di apprendimento di lezioni importanti è continuo e che la revisione e l'aggiornamento costante delle tue best practice di sicurezza ti aiuterà a garantire la resilienza della tua organizzazione, permettendole di affrontare minacce informatiche sempre più evolute.

Segnalazione degli incidenti

Dopo un incidente di cybersecurity, è fondamentale comunicare alle persone interessate i vari dettagli, i risultati delle indagini e le azioni di correzione intraprese. Segnalare l'incidente internamente, alle autorità normative e alle forze dell'ordine è essenziale per mantenere la trasparenza, assicurare il rispetto della conformità e facilitare le indagini.

Segnalazione interna

Per promuovere una cultura di miglioramento e apprendimento continuo, le organizzazioni devono definire un chiaro processo di segnalazione interna. Questo processo deve includere:

- La documentazione dell'incidente, descrivendo la cronologia degli eventi, i sistemi coinvolti e la natura dell'attacco.
- Un riepilogo dell'impatto dell'incidente sulle operazioni, sulla situazione finanziaria e sulla reputazione dell'organizzazione.
- Una definizione delle azioni intraprese per contenere ed estirpare la minaccia, nonché per riprendere le normali attività operative dopo l'incidente.
- L'identificazione delle lezioni importanti apprese e delle raccomandazioni da seguire in futuro per migliorare il profilo di sicurezza dell'organizzazione.
- L'invio del report sull'incidente alle parti interessate, ad esempio il Senior Management, i team IT e i dipendenti o i reparti coinvolti.

Segnalazione alle autorità normative

A seconda della giurisdizione e del settore di attività, le organizzazioni potrebbero essere tenute a segnalare gli incidenti di cybersecurity alle autorità normative. La conformità a questi requisiti è fondamentale per evitare multe e sanzioni, nonché per prevenire eventuali danni alla reputazione dell'organizzazione. Quando segnalano un incidente alle autorità normative, le organizzazioni devono:

- Determinare quai sono le autorità competenti da informare. La decisione viene presa a seconda della natura dell'incidente, del settore di attività dell'organizzazione e del paese in cui ha sede.
- Rivedere i requisiti di reportistica applicabili, incluse le informazioni necessarie e le tempistiche per la segnalazione.
- Preparare un report dettagliato, attenendosi al formato richiesto e ai contenuti specificati dalle autorità normative.
- Inviare il proprio report, rispettando le tempistiche specificate e mantenendo un canale di comunicazione aperto con le autorità normative per l'intera durata delle indagini e del processo di risoluzione.

Segnalazione alle forze dell'ordine

In caso di attività criminale o di attacchi informatici estremamente gravi, è consigliabile che le organizzazioni segnalino l'incidente alle forze dell'ordine. I report inviati possono favorire le indagini e potenzialmente aiutare ad arrestare gli autori dell'attacco. Quando segnalano un incidente alle forze dell'ordine, le organizzazioni devono:

- Identificare le forze dell'ordine competenti, ad esempio polizia locale, autorità nazionali per la cybersicurezza, enti specializzati (ad esempio l'FBI).
- Raccogliere prove pertinenti, inclusi log, immagini del sistema e acquisizioni del traffico di rete, preservando la catena di custodia e attenendosi ai requisiti legali applicabili.
- Preparare un report dettagliato sull'incidente, che includa informazioni sulla natura dell'attacco, sui sistemi e sui dati coinvolti, oltre a una cronologia degli eventi e a tutto ciò che si sa sull'autore o sugli autori dell'attacco.
- Cooperare con le forze dell'ordine per l'intera durata delle indagini, fornendo ulteriori dati e assistenza, se richiesto.

Seguendo queste linee guida per la segnalazione degli incidenti, le organizzazioni possono garantire trasparenza e conformità ai requisiti normativi. Inoltre, possono svolgere un ruolo importante nell'impegno collettivo di lotta al cybercrimine.

Conclusione

In conclusione, questa guida alla pianificazione dell'incident response fornisce un quadro a 360 gradi che aiuta le organizzazioni a prepararsi in maniera efficace ad affrontare e a gestire gli attacchi di cybersecurity, nonché a riprendere le normali attività operative dopo un incidente. Adottando un approccio gestionale proattivo e le dovute precauzioni di sicurezza allo scopo di salvaguardare l'integrità dei dati, le organizzazioni possono incrementare notevolmente la propria resilienza in seguito a un attacco informatico. Consigliamo inoltre di investire in strumenti di sicurezza e corsi di formazione per il personale, definendo procedure trasparenti per la segnalazione degli incidenti.

Una pianificazione efficace dell'incident response non aiuta solo le organizzazioni a limitare i danni causati dai cyberattacchi, ma contribuisce anche a promuovere una cultura di miglioramento e apprendimento costante a livello organico. Il panorama delle minacce informatiche continuerà a evolversi, per cui le organizzazioni devono rivedere e aggiornare i propri piani di incident response a cadenza regolare, per rimanere sempre un passo avanti rispetto alle minacce e alle vulnerabilità emergenti.

Attenendosi diligentemente ai consigli forniti in questa guida, le organizzazioni potranno affrontare le minacce con maggiore preparazione, rilevando e contenendo gli incidenti di cybersecurity, nonché intraprendendo azioni correttive. Saranno inoltre in grado di proteggere risorse e dati critici, rispettare la conformità ai requisiti normativi e preservare la propria reputazione in un mondo in cui la connessione al web gioca un ruolo sempre più importante.

Per maggiori informazioni sul servizio Sophos Incident Response,

Sei stato colpito da un cyberattacco?

Chiamaci in qualsiasi momento per parlare con i nostri esperti di Incident Response.

Australia: +61 272084454

Austria: +43 73265575520

Canada: +1 7785897255

Francia: +33 186539880

Germania: +49 61171186766

Italia: +39 0294752897

Paesi Bassi: +31 162708600

Svezia: +46 858400610

Svizzera: +41 445152286

Regno Unito: +44 1235635329

Stati Uniti: +1 4087461064

E-mail: RapidResponse@Sophos.com

I nostri esperti di incident response risponderanno alla tua richiesta il prima possibile.

2023-09-01 (IRG-MP)

SOPHOS