SOPHOS
Cybersecurity delivered.

Quattro suggerimenti chiave sull'Incident Response

Per sapere in anticipo come reagire in caso di cyberattacco

L'Incident Response può essere un'attività molto intensa ed estenuante. Sebbene niente possa alleviare completamente lo stress di un attacco, questi quattro suggerimenti chiave che sono stati identificati dai nostri esperti di Incident Response, possono aiutare il tuo team a ottimizzare la strategia di difesa dell'organizzazione.

Questo documento mette in evidenza i principali consigli e suggerimenti che tutti dovrebbero prendere in considerazione per poter rispondere adeguatamente agli incidenti di sicurezza. Le indicazioni fornite si basano sull'esperienza maturata sul campo dai team Sophos Managed Detection and Response e Sophos Rapid Response, che collettivamente sono intervenuti in migliaia di incidenti di cybersecurity.

Suggerimento numero 1: reagire il più rapidamente possibile

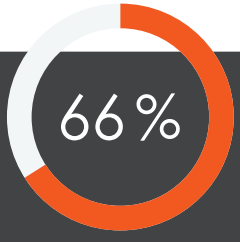
Quando un'organizzazione si trova sotto attacco, ogni secondo è importante.

I team potrebbero non reagire tempestivamente e i motivi possono essere diversi. Quello più comune è non comprendere la gravità della situazione, che risulta inevitabilmente nel non capire l'urgenza con cui è richiesto un intervento.

Di solito gli attacchi si verificano nei momenti meno opportuni: giorni festivi, fine settimana e ore notturne. Poiché nella maggior parte dei casi i team di Incident Response sono a corto di personale, l'attitudine che ne deriva è, comprensibilmente, quella del "ci penso domani". Purtroppo, però, domani potrebbe essere troppo tardi per poter attutire l'impatto dell'attacco.

I team oberati di lavoro sono anche quelli con la maggiore probabilità di reagire in maniera più lenta agli indicatori di attacco, poiché soffrono di quello che viene definito "affaticamento da allarme", ovvero la presenza di troppe interferenze per notare questi segnali. Anche quando un caso viene inizialmente aperto, potrebbe non ricevere la giusta priorità, a causa di una potenziale mancanza di visibilità e contesto. Tutte queste operazioni richiedono tempo, e il tempo non è dalla parte di chi, nel processo di Incident Response, deve difendersi.

Anche in situazioni nelle quali i team di sicurezza dovessero rilevare l'attacco in corso ed essere consci della necessità di intervenire immediatamente, potrebbero mancare le competenze tecniche per decidere come procedere, e anche questo fattore potrebbe rallentare la risposta. Il modo migliore per impedire che si verifichino queste situazioni è pianificare in anticipo cosa fare in caso di incidente.



L'anno scorso, quasi due terzi delle organizzazioni hanno subito attacchi ransomware e i pirati informatici sono riusciti a cifrare i file nel 65% dei casi[1].

Suggerimento numero 2: non cantare vittoria troppo presto

Nell'Incident Response non basta eliminare i sintomi. È importante curare anche la malattia di fondo.

Quando viene rilevata una minaccia, la prima azione da compiere deve essere valutare l'attacco immediato, il che potrebbe includere la rimozione di un file eseguibile o un trojan di Internet banking, oppure il blocco delle attività di esfiltrazione dei dati. Tuttavia, dopo aver bloccato l'attacco iniziale, spesso i team non si rendono conto di non averne risolto la causa originaria.

Aver rimosso il malware e cancellato l'avviso non significa aver espulso il cybercriminale dall'ambiente informatico. È anche possibile che l'attacco rilevato sia stato semplicemente un "giro di prova" del pirata informatico, che desiderava scoprire quali fossero le difese da affrontare. Se il cybercriminale è ancora in grado di accedere ai sistemi, è molto probabile che colpisca di nuovo, ma questa volta in maniera devastante.

I team di Incident Response devono accertarsi di risolvere la causa originaria dell'incidente appena attenuato. Il pirata informatico ha ancora la possibilità di accedere all'ambiente? Sta pianificando un secondo attacco? I team di Incident Response che sono intervenuti su migliaia di attacchi sanno quando e dove approfondire le indagini. Cercano tracce di altre attività degli hacker passate, presenti o future, che potrebbero avere un impatto sulla rete. Una volta identificate, neutralizzano anche quelle.

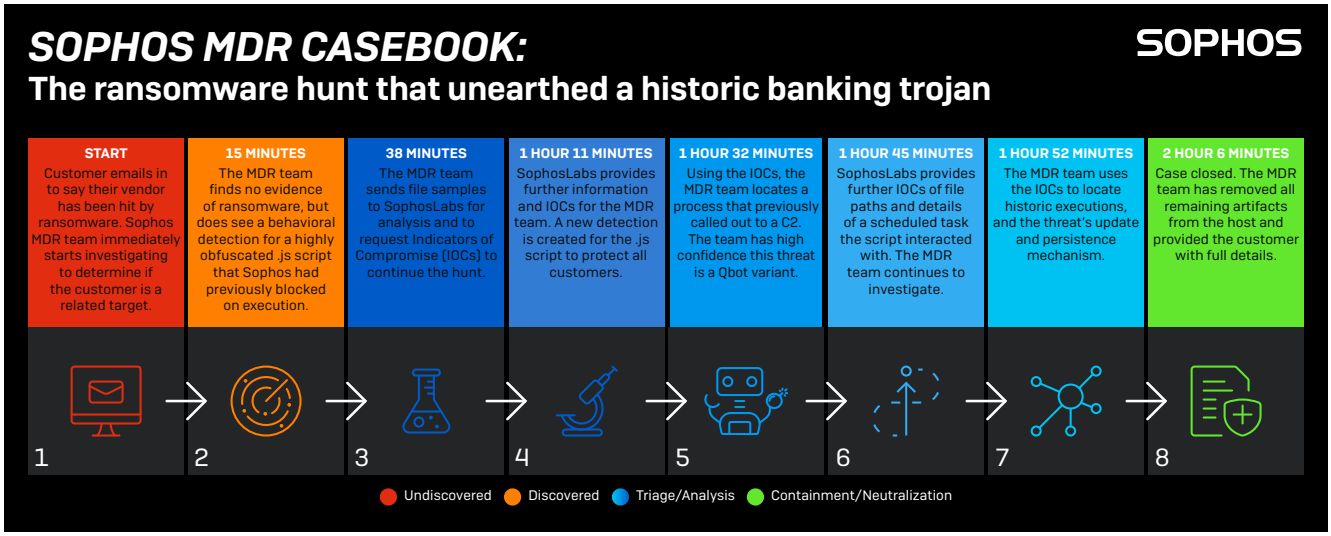
Ad esempio, in un caso in particolare gli specialisti di Incident Response di Sophos sono stati in grado di sventare un attacco che era in corso da nove giorni, e hanno osservato tre tentativi diversi di attacco ransomware ai danni dell'organizzazione.

Poiché la vittima non era ancora cliente Sophos MDR, a entrare in azione per primo è stato il team Sophos Rapid Response.

Nella prima ondata dell'attacco (che è stata bloccata dalla soluzione di Endpoint Protection dell'organizzazione) i cybercriminali hanno infettato 700 computer con il ransomware Maze, esigendo un riscatto pari a 15 milioni di $. Non appena notato l'attacco in corso, il team di sicurezza della vittima ha deciso di avvalersi delle competenze avanzate di Incident Response del team Sophos Managed Detection and Response (MDR).

Gli esperti di Incident Response di Sophos hanno rapidamente identificato l'account di amministrazione compromesso, rilevato e rimosso diversi file malevoli e bloccato le comunicazioni C2 (comando e controllo) dei cybercriminali. Il team Sophos MDR è stato in grado di proteggere l'organizzazione da altre due ondate di attacchi da parte di questi pirati informatici. Se i cybercriminali fossero riusciti nel loro intento e la vittima avesse pagato il riscatto, sarebbe potuta essere una delle somme più elevate versate fino a oggi come conseguenza di un attacco ransomware.

In un altro esempio, il team Sophos MDR ha risposto a una potenziale minaccia di ransomware, per poi rendersi rapidamente conto che non era presente alcuna traccia di ransomware. A questo punto alcuni team avrebbero potuto chiudere il caso e passare ad altre attività. Tuttavia, il team Sophos MDR ha proseguito con le indagini, che hanno portato alla luce la presenza di un trojan di internet banking ormai leggendario. Fortunatamente per questo cliente, la minaccia non era più attiva, ma questo esempio dimostra l'importanza dell'andare oltre i sintomi iniziali, per determinare la causa originaria nella sua completezza, in quanto potrebbe essere un semplice indizio di un attacco più esteso.



Suggerimento numero 3: la visibilità completa è essenziale

Quando occorre proteggere un'organizzazione da un attacco, non esiste ostacolo più grande del doversi muovere alla cieca. È importante avere a disposizione dati di alta qualità, per poter identificare in maniera accurata i potenziali indicatori di attacco e stabilire quale sia stata la causa originaria.

La strategia più efficace prevede la raccolta di dati per osservare i segnali, la capacità di riconoscere tali segnali nonostante le interferenze e l'identificazione di quelli che devono essere gestiti con maggiore priorità.

Identificare i segnali

Avere visibilità limitata su un ambiente è un metodo infallibile per fare in modo che gli attaccanti possano agire indisturbati. Nel corso degli anni, sono stati introdotti sul mercato molti strumenti di big data, progettati per cercare di risolvere questa sfida in particolare. Alcuni utilizzano dati basati sugli eventi, ad es. eventi di log, altri sfruttano dati basati sulle minacce, mentre altri ancora adottano un approccio ibrido. In ogni caso, l'obiettivo rimane identico: raccogliere una quantità sufficiente di dati per generare informazioni approfondite e significative, al fine di indagare sugli attacchi che sarebbero passati inosservati e implementare una strategia di risposta adeguata.

La raccolta di dati di qualità elevata, provenienti da fonti diverse, garantisce una visibilità totale sugli strumenti, sulle procedure e sulle tattiche di un cybercriminale. Senza questa possibilità, è probabile che venga osservata solamente una parte dell'attacco.

Ridurre le interferenze

Temendo di non avere abbastanza dati per poter delineare il profilo completo di un attacco, alcune organizzazioni (e gli strumenti di sicurezza che utilizzano) raccolgono tutte le informazioni possibili. Tuttavia, questa strategia complica ulteriormente la ricerca del proverbiale ago nel pagliaio: non fa altro che aggiungere più paglia del dovuto. La conseguenza non è solamente un incremento dei costi implicati dalla raccolta e dalla memorizzazione dei dati, ma anche la creazione di moltissime informazioni non necessarie, che portano all'affaticamento da allarme e a un inutile dispendio di tempo, passato a gestire falsi positivi.

Applicare il giusto contesto

Un detto molto diffuso tra i professionisti in materia di rilevamento e risposta alle minacce dice: "Il contenuto è il re, ma il contesto è la regina". Ambedue sono componenti indispensabili per un programma di Incident Response efficace. L'applicazione di metadati significativi associati ai segnali consente agli analisti di stabilire se tali segnali siano pericolosi o innocui.

Uno dei componenti essenziali di una strategia efficace per il rilevamento e la risposta alle minacce è l'assegnazione delle giuste priorità ai segnali più importanti. Il modo migliore per identificare gli avvisi più significativi è utilizzare una combinazione tra il contesto fornito dagli strumenti di sicurezza (ad es. le soluzioni di protezione endpoint e di risposta alle minacce), l'intelligenza artificiale, i dati di intelligence sulle minacce e l'esperienza di operatori umani.

Il contesto aiuta a determinare l'origine di un segnale, la fase attuale di attacco, gli eventi correlati e il potenziale impatto sull'organizzazione.

Suggerimento numero 4: chiedere aiuto è normale

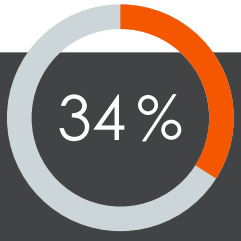
Nessuna organizzazione vuole avere a che fare con un tentativo di violazione. Tuttavia, quando bisogna rispondere a un incidente, l'esperienza è un fattore insostituibile. Questo significa che gli esperti informatici e i team di sicurezza, spesso già alle prese con intense attività di Incident Response, vengono molto frequentemente messi in situazioni che vanno oltre le loro capacità. Sovente, si tratta di casi che hanno un forte impatto sull'organizzazione.

Al giorno d'oggi, uno dei principali problemi affrontati dal settore della cybersecurity è la mancanza di personale dotato di competenze tecniche adeguate per indagare sugli incidenti e implementare una strategia di risposta efficace. Il problema è talmente diffuso tra le organizzazioni che, secondo una ricerca condotta da ESG[2], "il 34% sostiene che la sfida principale è la mancanza di risorse umane dotate delle giuste competenze e in grado di analizzare un incidente di cybersecurity che colpisce un endpoint, per determinarne la causa originaria e identificare la catena di attacco".

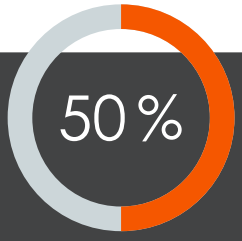
Questo dilemma ha dato origine a una nuova alternativa: i servizi di sicurezza gestiti. Nello specifico, i servizi di rilevamento e risposta gestiti (MDR - Managed Detection and Response). I servizi MDR sono operazioni di sicurezza affidate in outsourcing a un team di specialisti esterno, che svolge la funzione di un'estensione del team di sicurezza del cliente. Questi servizi offrono la combinazione ottimale tra: indagini supervisionate da esseri umani, threat hunting, monitoraggio in tempo reale, risposta agli incidenti e uno stack di tecnologie progettate per raccogliere e analizzare dati di intelligence. Secondo Gartner, "entro il 2025 il 50% delle organizzazioni utilizzerà servizi MDR"[3]; questa tendenza indica che le organizzazioni sono consce del fatto che avranno bisogno di assistenza per implementare un programma completo di Incident Response e operazioni di sicurezza.

Per le organizzazioni che non utilizzano un servizio MDR e si trovano ad affrontare un attacco attivo, i servizi specializzati di Incident Response sono un'ottima opzione. Gli esperti di Incident Response entrano in azione quando i team di sicurezza interni sono oberati di lavoro e hanno bisogno di assistenza esterna per valutare l'attacco e assicurarsi che il pericolo sia stato neutralizzato.

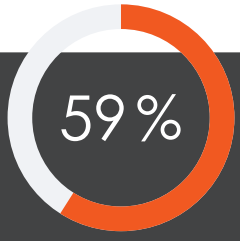
Anche le organizzazioni che hanno a disposizione un team di esperti di analisi di sicurezza possono trarre ampio beneficio dalla collaborazione con un servizio di Incident Response in grado di colmare eventuali lacune di disponibilità del personale (ovvero notti, fine settimana e ferie) e di offrire le competenze specializzate necessarie per rispondere agli incidenti.



Secondo le ricerche svolte dagli analisti di ESG, per il 34% delle organizzazioni la sfida principale è la mancanza di "risorse umane dotate delle giuste competenze e in grado di analizzare un incidente di cybersecurity che colpisce un endpoint, per determinarne la causa originaria e identificare la catena di attacco"[2].



Entro il 2025 il 50% delle organizzazioni utilizzerà servizi MDR (una percentuale in aumento, rispetto a meno del 5% nel 2019)[3].



In un sondaggio condotto nel 2022 a cui hanno partecipato 5.600 responsabili IT, il 59% degli intervistati dichiara di avere osservato un aumento nella complessità degli attacchi che hanno colpito la propria organizzazione l'anno scorso[4].

Sophos ti può aiutare, ecco come

Sophos Managed Detection and Response (MDR)

Hai dei dubbi sulla capacità della tua organizzazione di rispondere a un incidente potenzialmente critico? Se la risposta è sì, il servizio Sophos Managed Detection and Response (MDR) è un'opzione che merita di essere considerata.

Sophos MDR offre un servizio completamente gestito con opzioni di intercettazione, rilevamento e risposta alle minacce 24h su 24 e 7gg su 7, a cura del nostro team di esperti. Andando ben oltre la semplice notifica di attacchi o comportamenti sospetti, il team Sophos MDR intraprende azioni mirate per conto degli utenti, in modo da neutralizzare persino le minacce più sofisticate e complesse. Se un incidente dovesse verificarsi comunque, il team MDR intraprenderà azioni correttive da remoto, fermando, contenendo e neutralizzando la minaccia. Inoltre, questo team di esperti di IT security operation offrirà anche consigli pratici per intervenire sulle cause originarie degli incidenti ricorrenti.

Per saperne di più, visita www.sophos.it/mdr

Servizio Sophos Rapid Response

Se la tua organizzazione si trova ad affrontare un attacco e ha bisogno di assistenza immediata per l'Incident Response, Sophos può aiutarti.

Sophos Rapid Response è un servizio fornito da un team di esperti in ambito di risposta agli incidenti, 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.

Il team Sophos Rapid Response è composto da esperti di Incident Response che entrano rapidamente in azione per valutare, contenere e neutralizzare le minacce attive. Gli intrusi vengono espulsi dal vostro ambiente informatico, per impedire che rechino ulteriori danni alle risorse.

Per maggiori informazioni, visitawww.sophos.com/rapidresponse

Sophos XDR

Sophos XDR è l'unica soluzione XDR nel settore in grado di sincronizzare la protezione nativa di endpoint, server, firewall, e-mail, cloud e M365. Fornisce una prospettiva olistica dell'ambiente dell'organizzazione, con i set di dati più completi e con analisi approfondite, per offrire opzioni di rilevamento, indagine e risposta alle minacce sia per interi team SOC dedicati che per singoli amministratori IT.

Per scoprire di più e per una prova gratuita, visita www.sophos.it/xdr

[1] La Vera Storia Del Ransomware 2022 - Basato su un sondaggio indipendente e agnostico rispetto ai vendor che ha coinvolto 5.600 professionisti IT in 31 paesi: https://www.sophos.com/it-it/whitepaper/state-of-ransomware
[2] https://www.esg-global.com/blog/soapa-discussion-on-edr-and-xdr-with-jon-oltsik-and-dave-gruber-video-part-1
[3] 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
[4] La Vera Storia Del Ransomware 2022 - Basato su un sondaggio indipendente e agnostico rispetto ai vendor che ha coinvolto 5.600 professionisti IT in 31 paesi: https://www.sophos.com/it-it/whitepaper/state-of-ransomware

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

22-08-08 WPIT (PC)

SOPHOS