INCIDENT RESPONSE PASSO PER PASSO CON HWG SABABA



HWG Sababa

Il SOC di HWG Sababa

Monitoraggio 24×7, rilevamento e risposta agli incidenti, intelligence e threat hunting

Team di oltre 70 cybersecurity analyst certificati organizzati su 3 livelli

Milioni di eventi di sicurezza analizzati ogni mese, 3500 casi investigati e 500 incidenti risolti

100+ progetti di Incident Response negli ultimi 4 anni

Di fronte alla proliferazione delle minacce informatiche - con un **incremento degli attacchi del 12%**[1] nel 2023 e un **dwell time ridotto a soli 8 giorni**[2] - le aziende subiscono la crescente pressione di dover rispondere rapidamente alle emergenze cyber. Tali emergenze presentano loro una serie di sfide uniche, tra cui la **rapida escalation degli incidenti**, la **complessità dell'identificare e del neutralizzare le minacce**, l'imperativo di **ridurre al minimo i tempi di inattività** o le **interruzioni operative**, nonché il rischio di **ingenti perdite finanziarie**. Inoltre, la natura mutevole delle minacce richiede una conoscenza approfondita dei vettori di attacco emergenti e di misure di sicurezza proattive, che spesso va oltre le capacità dei team interni.

Oltre alle sfide tecniche, le aziende devono saper gestire la **componente umana degli incidenti**, che può avere un impatto significativo sull'efficacia della risposta e sulla resilienza dell'intera struttura organizzativa. Infatti, il rapido svolgersi degli attacchi e le potenziali conseguenze di una violazione possono aumentare il **livello di stress, la tensione e lo stato di incertezza**, compromettendo il processo decisionale ed accrescendo la sensazione di estrema urgenza.



Questo scenario rispecchia l'esperienza vissuta da una **grande multinazionale**, con numerosi **uffici commerciali** e **stabilimenti produttivi** dislocati in **3 continenti**, e un organico che supera i **5.000 dipendenti**. Ritrovatasi nel caos di un attacco informatico, l'azienda ha dovuto affrontare grossi ostacoli. **Con perdite giornaliere stimate di 3 milioni di euro**, la capacità di fornire servizi ad una **clientela globale di oltre 700 imprese** è stata seriamente compromessa. L'operatività aziendale ha subito una brusca interruzione, impattando per alcuni giorni la quasi totalità dei reparti.

Di fronte alla minaccia incombente sulla sua stimata reputazione e alla carenza di competenze interne per gestire la crisi in modo efficace, **l'azienda si è rivolta ad HWG Sababa per ricevere supporto. Dalla formulazione ed attuazione di una strategia articolata di crisis management** - compresi i protocolli di comunicazione e le procedure di Incident Response - **all'implementazione di soluzioni tecniche** per limitare i danni, **senza tralasciare il lato umano dell'emergenza**, HWG Sababa ha garantito una risposta coordinata ed efficace. Il loro coinvolgimento è stato fondamentale per consentire all'organizzazione di gestire le difficoltà con fiducia e resilienza.

HWG Sababa

[1]Rapporto Clusit 2024

[2]2023 Active Adversary Report for Tech Leaders

Alla scoperta della violazione

L'episodio ha avuto inizio quando i sistemi hanno manifestato un riavvio inaspettato delle loro macchine virtuali. Poiché la disfunzione si è protratta, il reparto IT interno ha avuto contezza della criticità della situazione, decidendo di contattare HWG Sababa per richiedere assistenza.

In prima battuta, HWG Sababa ha inviato **due specialisti del Defence Center** per affiancare l'azienda nella gestione dell'incidente. Insieme, hanno avviato un'**indagine forense,** con l'obiettivo di scoprire le origini e la dinamica dell'attacco. Nel giro di poco tempo, è emersa un'informazione importante: gli attaccanti hanno effettuato accesso alla rete **tramite canale VPN**, senza ricorrere ad alcuna tattica di brute-force. Sfruttando un'**utenza di servizio compromessa**, hanno infatti ottenuto accesso all'infrastruttura, ponendo le basi per le loro attività illecite.

Le capacità degli attaccanti penetrati all'interno della rete hanno permesso di raggiungere un obiettivo primario: il **Domain Controller**. Preso possesso di questo centro nevralgico, tramite attività mirate di enumeration, hanno scoperto **altri account non correttamente configurati**, alcuni dei quali con privilegi molto elevati. Con queste armi a disposizione, hanno potuto agire e rilasciare **un'ondata di malware**, tra cui Mimikatz, eludendo il rilevamento da parte dell'antivirus aziendale. Parallelamente a quest'attività di attacco volta alla disruption dei sistemi, hanno orchestrato **un'esfiltrazione di dati verso un indirizzo IP russo**. Completate le attività di esfiltrazione e la preparazione degli strumenti di disruption, hanno proceduto poi all'avvio di un'**attività di criptazione sia sulle macchine host che sull'ambiente virtuale.**

Le fasi di gestione e risposta all'incidente



- **Lockdown e segregazione dell'Infrastruttura.**

In seguito all'immediato coinvolgimento di HWG Sababa nell'incidente, sono state impartite rapidamente le direttive di contenimento dell'emergenza. Ciò ha comportato il **lockdown completo dell'infrastruttura on-premise e in cloud**, disabilitando l'accesso a Internet, nonché la **segregazione est-ovest dell'infrastruttura** stessa al fine di creare dei sottoinsiemi isolati. Questo approccio ha facilitato lo svolgimento delle operazioni di analisi, contenimento e ripristino senza compromettere i servizi non impattati e che potevano essere riavviati rapidamente.

• Validazione dell'Active Directory.

Dopo le misure di contenimento iniziali, è stata avviata un'**attenta validazione dell'ambiente Active Directory**. Ogni singolo utente è stato esaminato al fine di garantire l'assenza di **amministratori non autorizzati** creati dagli attaccanti. Questo processo di verifica ha consentito **la riattivazione delle funzionalità di posta elettronica dopo solo un giorno dalla chiamata di emergenza**.

• EDR e Compromise Assessment.

Parallelamente all'indagine in loco, gli esperti di HWG Sababa hanno provveduto a **fornire e distribuire rapidamente licenze EDR di ultima generazione**, in sostituzione del meno efficace antivirus. In stretta collaborazione con l'organizzazione, hanno installato con successo **oltre 3.000 licenze su server fisici e virtuali nel giro di una settimana**, con l'obiettivo di bonificare l'infrastruttura e migliorare la copertura contro potenziali re-infezioni. Progettata per bloccare eventuali infezioni future prima che possano propagarsi, questa soluzione si è rivelata fondamentale per consolidare le difese dell'azienda.

Nel frattempo, attraverso il **Compromise Assessment**, il Defence Center di HWG Sababa ha analizzato da remoto quelle **macchine che mostravano evidenti segni di compromissione per valutarne lo stato di salute**. Questa misura proattiva mirava ad identificare le macchine compromesse che necessitavano di un ripristino del backup, laddove possibile, e, al contempo, ad individuare quelle ritenute sicure per essere reintegrate nella produzione.

• Ripristino dei servizi principali.

Sulla base delle informazioni ricavate dal Compromise Assessment e dalle licenze EDR installate, gli specialisti di HWG Sababa hanno iniziato a definire delle **linee guida per il ripristino dei servizi**. La priorità è stata data ai servizi core, seguendo un ordine strutturato di importanza, con un'attenzione particolare a quei task che potevano **essere eseguiti rapidamente e produrre benefici immediati**. Partendo dai sistemi ERP aziendali, uno di essi è stato ripristinato in 3 giorni, mentre l'altro in 5.

• Competenza on-site.

Alla fine della prima settimana, uno specialista di sistemi virtualizzati si è recato presso la sede del cliente. Dotato di hardware e vaste competenze, ha attrezzato un' **infrastruttura virtuale ad hoc per la ricostruzione e bonifica delle macchine compromesse**. Inoltre, a metà della seconda settimana, un altro esperto di HWG Sababa è stato inviato in loco per guidare il processo di **ricostruzione e ripristino della rete**, rispettando rigorosamente i più recenti principi di cybersecurity.

L’ultimo miglio

Nel giro di tre settimane, l'azienda ha recuperato la propria stabilità, con un **ripristino graduale del 75%-80% dei servizi critici**. Tuttavia, il recupero dell'ultimo 20% ha rappresentato la sfida più difficile, richiedendo un ulteriore grande impegno ai reparti IT per via dei livelli di energia in calo. Nonostante i significativi progressi compiuti, è proprio in questa fase che solitamente si manifestano gli ostacoli più imprevedibili, allontanando nuovamente il traguardo.

“Durante tutto l’affiancamento, con il CIO e CISO, abbiamo gestito difficoltà tecniche e discusso scelte operative che sono proprie solo del contesto di Incident Response. Raramente si è preparati a questo contesto. L’Incident Response va sempre considerato come un momento totale di Crisi dove la sfida più grande è affrontare, gestire e superare i continui momenti di incertezza di risoluzione, mantenendo salda la lucidità. La nostra esperienza nella gestione degli incidenti e le figure messe a disposizione hanno permesso al CIO, al CISO e ai team IT di fronteggiare e rispondere all’impatto senza perder di vista l’obbiettivo finale o esser vittime della stanchezza. Tutto questo è stato molto apprezzato”,
ha spiegato **Raffaele Fazio, Head of Defence Center di HWG Sababa.**

La gestione di una crisi informatica infatti non richiede soltanto soluzioni tecniche, ma anche **un'attenzione costante al fattore umano**. Confrontarsi con queste emergenze può essere molto stressante, ma avere al proprio fianco un partner fidato di cybersecurity conferisce maggiore tranquillità nell’affrontare la sfida. In questo caso, HWG Sababa ha svolto un ruolo chiave nell'**offrire una guida chiara, rispondere alle domande e fornire un supporto continuo** alle persone e agli stakeholder che avrebbero potuto sentirsi sopraffatti o incerti su come districarsi nel percorso di recovery, soprattutto durante l'ultimo miglio.

“Dopo aver risolto l'incidente, il nostro impegno è proseguito. Abbiamo mantenuto la nostra piena dedizione nel supportare l’azienda a rafforzare la propria postura di cybersecurity, mitigare i rischi futuri e salvaguardarsi da episodi simili. Grazie ad un’attenta pianificazione e ad una stretta collaborazione, stiamo lavorando per costruire una strategia di difesa proattiva”,
ha proseguito **Raffaele Fazio, Head of Defence Center di HWG Sababa.**

Lesson Learned

1 Preparare in anticipo un piano di Incident Response

Le conclusioni tratte da questa esperienza sottolineano la necessità assoluta per le aziende di **sviluppare e implementare in modo proattivo piani completi di Incident Response**. Questo infatti assicura una risposta unificata ed efficiente durante le emergenze cyber, dove ogni ora che passa rappresenta un'opportunità preziosa per aggirare le difficoltà e mitigare gli impatti finanziari, reputazionali e operativi.

2 Rivedere e aggiornare regolarmente le proprie strategie



Ma non è tutto: è fondamentale che le organizzazioni **rivedano e aggiornino regolarmente le loro strategie** sulla base di insight acquisiti da incidenti concreti. Questo approccio proattivo garantisce che le aziende siano flessibili e adattabili di fronte alla continua evoluzione delle minacce informatiche. Traendo insegnamento da esperienze passate e adattando di conseguenza le proprie tattiche, le organizzazioni possono rafforzare la propria resilienza e la propria preparazione per mitigare efficacemente i rischi futuri.

3 Prioritizzare una formazione continua

In ultimo, è fondamentale **prioritizzare una formazione continua per garantire la preparazione del personale a tutti i livelli**. Simulazioni regolari di emergenze cyber aiutano a convalidare le procedure di risposta, ad identificare le lacune e a migliorare il coordinamento tra le parti interessate. Promuovendo un approccio proattivo, le organizzazioni possono **rafforzare la loro capacità di rispondere efficacemente agli incidenti informatici**, riducendo al minimo l'impatto sulle loro attività e sulle loro risorse.

Preparati proattivamente ad eventuali incidenti di cybersecurity.

Contattaci per costruire un piano di Incident Response su misura: **contacts@hwgsababa.com**

HWG Sababa

Follow us on:

HWG Sababa

www.hwgsababa.com