WHITE PAPER

Prepararsi all'imprevedibile: perché servono competenze e strumenti specializzati per una risposta efficace agli incidenti

Sintesi preliminare

La superficie di attacco digitale si sta espandendo ad un ritmo astronomico. Ci sono "bordi" perimetrali ovunque, che offrono ai cybercriminali opzioni di accesso quasi infinite alle reti aziendali. Inoltre, il panorama delle minacce continua a evolversi con attacchi sempre più sofisticati e tecniche elusive. La realtà oggi è che non è possibile per le organizzazioni fermare ogni minaccia prima che entri nella rete.

Quando un'organizzazione scopre un incidente, deve reagire immediatamente per ridurre al minimo i danni. Comprendere la natura, la portata e i rischi posti dall'incidente per poter rispondere correttamente richiede strumenti specializzati, competenze e processi ripetibili. Le organizzazioni hanno bisogno di personale specializzato per un'attenuazione efficace delle minacce.

Quasi l'80% delle organizzazioni adotta le innovazioni digitali più rapidamente della sua capacità di proteggerle dagli attacchi.[1]

"Il tempo è denaro e la lentezza nell'individuare e contenere una violazione può essere costosa... Oggi ci vogliono complessivamente 279 giorni per individuare e contenere una violazione, prima erano 266. Una risposta rapida può consentire un risparmio enorme in termini di costi. Le aziende in grado di individuare e contenere una violazione in non più di 200 giorni hanno speso in media 1,2 milioni di dollari in meno."[3]

Le violazioni sono inevitabili e l'immediatezza della risposta è fondamentale

La rete aziendale, le filiali, gli utenti e i dispositivi remoti, come anche le risorse in cloud, sono tutti vettori, e gli autori delle minacce stanno trovando nuovi modi per attaccarli. "I confini tra ciò che è all'interno del firewall e ciò che è all'esterno diventano sempre più indistinti, per cui la superficie di attacco di un'organizzazione, tutto ciò che l'organizzazione deve preoccuparsi di difendere, ora inizia all'interno della rete aziendale e si estende, attraverso Internet, anche nelle case dei dipendenti."[2]

L'improvviso e diffuso passaggio al telelavoro ha ampliato molto rapidamente la superficie di attacco dell'azienda. È un compito impossibile proteggere ogni dispositivo presente in rete. Molti di questi dispositivi forse non sono neanche noti ai team IT, ma sono comunque un potenziale punto di ingresso per gli aggressori.

Inoltre, gli attacchi continuano ad accelerare in termini di velocità e sofisticatezza. Ad esempio, l'automazione del malware e le tecniche di elusione rendono non solo difficile fermarlo, ma lo aiutano anche a diffondersi molto rapidamente. Vi sono stati anche attacchi più mirati, in particolare attacchi ransomware. Gli avversari si concedono il tempo di una ricognizione più lunga per prendere di mira una vittima specifica restando nell'ambiente per settimane, mappandolo e aggirando i controlli di sicurezza. Più a lungo restano in agguato, più danni fanno. Questa tempo dà loro l'opportunità non solo di scaricare il loro "pacco", il ransomware, ma anche di trovare il modo di estrarre dati dell'azienda e tenerli in ostaggio.

Anche nei casi in cui non si tratta di ransomware, quanto più a lungo un aggressore trascorre all'interno di una rete, tanto maggiore è l'accesso che può ottenere a dispositivi, dati e account. Questo aumenta l'impatto della violazione e fa aumentare il tempo necessario per rimuoverli e il loro accesso, facendo aumentare anche i costi per porvi rimedio.

Le organizzazioni si stanno rendendo conto che non possono sfuggire alle violazioni, ma possono attenuarle. Mettere in atto un piano di risposta (IR) **prima che** si verifichi un incidente è la chiave di ogni strategia di sicurezza informatica.

Cos'è la risposta agli incidenti?

La risposta agli incidenti è il processo di rilevamento, indagine e gestione delle ripercussioni di un incidente o una violazione della sicurezza. L'obiettivo è quello di limitare l'entità dei danni (costi e reputazione) causati dall'attacco e ridurre i tempi di ripristino.

Tale processo, però, richiede team specializzati, strumenti giusti e processi ripetibili.

Capacità di risposta agli incidenti

La maggior parte delle organizzazioni e delle aziende di medie dimensioni dispone di personale che si occupa almeno del funzionamento quotidiano degli strumenti di sicurezza. Tuttavia, questi strumenti sono tipicamente focalizzati sulla prevenzione delle minacce, e i team sono incaricati della distribuzione, della configurazione e della gestione continua del set di strumenti. Inoltre, questi compiti di amministrazione della sicurezza sono spesso solo una delle tante aree di responsabilità condivise dal team. Questi operatori hanno generalmente bisogno di un'ampia gamma di conoscenze informatiche e prodotti di sicurezza, ma hanno una disponibilità di tempo o un'esperienza limitata per quanto concerne la risposta agli incidenti.

Viceversa, quando un'organizzazione si trova nel bel mezzo di una violazione, è necessario un insieme completamente diverso di competenze materia di emergenza e conoscenze a livello di sicurezza informatica. Ad esempio:

- Autenticazione e controllo degli accessi
- Vulnerabilità della sicurezza
- Progettazione dei protocolli
- Analisi dei codici dannosi
- TTP degli avversari
- Difetti a livello di realizzazione
- Punti deboli della configurazione
- Analisi dei registri, tra cui sistema operativo (Windows e Linux, Apple) e rete (firewall, proxy, SIEM, PCAP)
- Indagini digitali

In sintesi, hanno bisogno di capire gli strumenti e le modalità dell'autore dell'attacco informatico, più che le tecnologie e il funzionamento della difesa all'attacco. E, dato che il panorama delle minacce informatiche è in rapida evoluzione, per farlo devono anche essere appassionati delle loro responsabilità e mantenersi aggiornati con le più recenti tattiche, tecniche e procedure utilizzate dagli aggressori.

Strumenti di risposta agli incidenti

Analogamente, questi team hanno bisogno un diverso set di strumenti. Se da un lato i controlli di sicurezza orientati alla prevenzione effettuati quotidianamente possono segnalare un incidente in corso, dall'altro l'attacco sarebbe già stato fermato se questi controlli fossero stati in grado di inquadrarlo incontrovertibilmente come tale.

Ad esempio, un firewall di nuova generazione può bloccare le minacce note e attribuire a ulteriori minacce un rischio medio, ma, in ragione del modo in cui è progettato, lascerà comunque passare un attacco a rischio medio. Inoltre, l'attribuzione di un rischio medio non rappresenta di norma una classificazione definitiva e richiede pertanto un approfondimento, altrimenti all'evento sarebbe stata attribuito un rischio più elevato.

Per quanto riguarda gli endpoint, una piattaforma di protezione degli endpoint (Endpoint Protection Platform, EPP) può bloccare molti malware noti o attività del sistema dannose, ma può anche segnalare comportamenti sospetti sulla base di scansione euristica che consente ancora di eseguire sulla macchina. Anche in questo caso, sono necessarie ulteriori indagini.

Le organizzazioni devono prepararsi a tali situazioni e fornire ai team specializzati strumenti specifici di rilevamento e analisi, nonché threat intelligence e capacità di ricerca.

Strumenti di rilevamento. Gli strumenti di rilevamento devono identificare minacce e indicatori atomici come gli indirizzi IP, nonché indicatori calcolati da URL e domini come gli hash dei file e le firme dettagliate, ma soprattutto devono identificare i comportamenti.

Strumenti di analisi. Una volta che qualcosa viene rilevato, è necessario il giusto set di strumenti per automatizzare l'analisi di file eventualmente presenti su disco o malware senza file presenti in memoria. L'estrazione di tali informazioni e l'esecuzione di analisi automatizzate e umane sono necessarie per poter determinare in modo tempestivo ed efficace ciò che il malware sta effettivamente facendo.

Threat intelligence. Una volta scoperti indicatori di compromissione (CIO), la threat intelligence può arricchire le informazioni per contestualizzarle.

Capacità di ricerca. La capacità di ricerca permette all'organizzazione di raccogliere tutte le informazioni estrapolate dalla fase di analisi per fare in modo che l'esatta portata della violazione o dell'incidente di sicurezza sia compresa.

Nonostante la rapida proliferazione di nuove minacce informatiche, il 77% dei dirigenti aziendali ha ammesso di non avere un piano formale di risposta agli incidenti informatici (CSIRP) che sia applicato in modo coerente nella propria organizzazione.[5]

Processo di risposta agli incidenti

Tutte le azioni di risposta devono avvenire molto più velocemente (e con maggiore precisione) rispetto alle operazioni standard. Data l'urgenza della risposta agli incidenti, anche il personale più esperto e dotato di strumenti adeguati trova utile un processo ben definito che è completamente diverso dalla norma. Consideriamo che:

- Le patch escono ogni mese, il martedì, ma le organizzazioni impiegano ancora 30 giorni o più per distribuirli.
- Gli aggiornamenti del software vengono rilasciati più volte all'anno, ma le organizzazioni spesso rimangono indietro di una o più versioni.

E l'elenco dei processi operativi standard potrebbe proseguire con tempi di risposta variegati, il che in molti casi va bene. Non è così per la risposta agli incidenti. Come ha osservato il NIST nella sua Computer Security Incident Handling Guide del 2012, "La disponibilità in tempo reale è la soluzione migliore nel caso della risposta agli incidenti, perché quanto più a lungo dura un incidente, tanto maggiore è il potenziale di danni e perdite."[4] Da allora non è cambiato molto. Di conseguenza, non appena un incidente viene segnalato, tutta una serie di attività, molte con esiti incerti e iter variabili, deve iniziare e procedere il più rapidamente possibile. Per questo sono assolutamente indispensabili processi ben definiti per ogni potenziale situazione.

Due approcci ai team di risposta agli incidenti

Vista l'attuale rapida espansione della superficie di attacco e la crescente sofisticatezza degli attacchi, le aziende non possono sfuggire a ogni minaccia. Per ridurre al minimo i danni derivanti dalle violazioni è necessario una risposta rapida e risoluta agli incidenti. È molto importante disporre dei dispositivi di risposta e degli strumenti giusti, ma anche di azioni documentate. I team di risposta possono essere interni o esterni. Per decidere quale sia l'approccio migliore per la propria organizzazione, può essere di supporto la nostra checklist "Le 5 considerazioni principali per decidere se esternalizzare la risposta agli incidenti o creare un team interno".

[1] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture Security and Ponemon Institute, 2019.

[2] Lucian Constantin, "Enterprise internet attack surface is growing, report shows," CSO, 11 giugno 2020.

[3] Dan Swinhoe, "What is the cost of a data breach?" CSO, 8 maggio 2020.

[4] Paul Cichonski, et al, "Computer Security Incident Handling Guide, Special Publication 800-61 Revision 2," NIST, agosto 2012.

[5] Conner Forrest, "Report: 77% of companies don't have a consistent cybersecurity response plan," TechRepublic, 14 marzo 2018.

novembre 19, 2020 12:17 PM

750405-0-1-IT