Sette consigli per ottimizzare il piano di Incident Response

Negli ultimi anni i team IT e di sicurezza hanno dovuto affrontare una moltitudine di situazioni ed eventi. Adozione massiccia del cloud, attacchi sempre più aggressivi e sofisticati, passaggio al lavoro da remoto e altri fattori contribuiscono a far sì che un piano di Incident Response (IR) definito solo qualche anno fa oggi non sia più adeguato. Nessuna organizzazione desidera essere solamente reattiva quando si verifica un incidente di sicurezza e un approccio proattivo con un solido piano di IR aiuta a rispondere in modo rapido ed efficace, con l'opportunità di ripristinare l'operatività il più rapidamente possibile.

Molte aziende dispongono già di un piano di IR, ma per quanto approfondito sia, l'evoluzione del panorama delle minacce informatiche – per non parlare di altre circostanze mutevoli dell'organizzazione – richiede modifiche e miglioramenti periodici.

Ad esempio, il recente Incident Response Report 2022 di Unit 42 ha rilevato che la compromissione della posta elettronica aziendale e gli attacchi ransomware stanno dilagando, costituendo complessivamente il 70% dei casi gestiti dal team di Unit 42. Sebbene gli attori delle minacce si dedichino da anni a questi tipi di schemi per monetizzare le loro attività, le specifiche si evolvono. I gruppi ransomware, ad esempio, si impegnano più spesso in ulteriori livelli di estorsione per spingere le organizzazioni a pagare. Inoltre, stanno creando versioni facilmente accessibili del loro malware per consentire a malintenzionati con inferiori competenze tecniche di partecipare alle loro attività pericolose. Rivedendo

continuamente i piani di IR esistenti, un’azienda potrà essere all’avanguardia quando i cybercriminali cambieranno le proprie tattiche.

I tre principali vettori di accesso per gli attori delle minacce sono il phishing, lo sfruttamento delle vulnerabilità del software e gli attacchi brute force alle credenziali. Per questo motivo, è fondamentale rivedere i piani di IR esistenti per concentrarsi sulle tipologie di attacco più diffuse.

Ecco sette best practice che potranno ottimizzare un piano di IR, rafforzando al contempo la postura di sicurezza complessiva di ogni organizzazione.

1. Stabilire comunicazioni regolari sul piano di IR

Quando si verifica un incidente di sicurezza, è probabile si debba affrontare uno dei giorni peggiori della propria carriera: in una violazione dei dati o attacco ransomware, ci si affannerà per capire cosa sia stato danneggiato o rubato, fermare gli attori della minaccia e mantenere le normali operazioni aziendali. Tuttavia, non sapere da dove iniziare può aggravare il danno. Quando arriva il momento di mettere in atto o avviare il piano, ogni individuo coinvolto deve sapere esattamente cosa fare. Per garantire che tutti siano sulla stessa lunghezza d’onda, è fondamentale utilizzare una comunicazione chiara e promuovere la consapevolezza di ruoli e responsabilità di ciascun membro del team di IR. Durante un incidente, tutti sono pronti a intervenire, ma per far sì che le cose si svolgano senza intoppi, ognuno deve sapere quali attività siano in realtà eseguite da altri e chi sia il punto di contatto critico per ogni flusso di lavoro.
È anche importante mantenere un atteggiamento positivo. La risposta agli incidenti di sicurezza può diventare frenetica e spesso si commettono errori. Riconoscere positivamente i risultati ottenuti dal team aiuterà a mantenere elevata la

motivazione.

2. Non trascurare il valore di un manuale di IR

Molte organizzazioni dichiarano di avere un piano di risposta agli incidenti, ma troppo spesso non sanno come utilizzarlo. Un manuale specifico di incident response per le minacce è fondamentale per l'efficacia del piano. Non è necessario che sia pubblicato formalmente, ma dovrebbe almeno consistere in un documento facilmente accessibile e in grado di fornire una guida durante il caos di risposta. Un problema comune durante cyberattacchi e altri incidenti è che i gruppi sanno quali siano le loro responsabilità, ma non sono sicuri di come portarle a termine. Il manuale dovrebbe fornire indicazioni pratiche sulle azioni da intraprendere per risolvere determinate situazioni e può essere considerato come un insieme di procedure operative standard di IR. Ad esempio, durante il contenimento di un incidente ransomware, il team di IR riconoscerà probabilmente la necessità di cambiare le password, ma potrebbe non essere sicuro della portata di tale compito. Il manuale dovrebbe delineare quali password aggiornare: amministrative, individuali, account di servizio, globali e così via. Fornirà inoltre una lista di controllo di tutte le altre azioni necessarie e dei responsabili.

3. Stabilire una cadenza regolare per la revisione dell'igiene generale della sicurezza

Un solido piano di IR incoraggia abitudini sane. Regolari revisioni dell'igiene della sicurezza renderanno la risposta più efficiente e contribuiranno soprattutto a ridurre il rischio di incidenti. Questi controlli dovrebbero includere: modifica delle password, aggiornamento e/o la rotazione delle chiavi, revisione dei livelli di accesso e verifica della

presenza di account di ex dipendenti o creati da un attore pericoloso.

4. Aggiornare il piano di IR seguendo l’evoluzione tecnologica interna.

La creazione di un piano di IR non è un compito banale, e soprattutto il piano deve essere valutato e verificato regolarmente. Questo è particolarmente importante nel panorama attuale, in cui la tecnologia e i relativi sistemi informativi avanzano e cambiano rapidamente. Possono verificarsi anche altri mutamenti, ad esempio delle attività aziendali, del personale e dei ruoli. Il piano di IR deve essere quindi adattato per tenere il passo della tecnologia – ad esempio, se alcuni dati o workload sono stati spostati nel cloud, l’organizzazione potrà essere esposta a nuove minacce. Sarà necessario adattare e aggiornare il piano di IR per affrontare quelle specifiche del cloud.

5. Valutare in modo proattivo il proprio piano IR

Una valutazione proattiva del piano IR è imperativa per non scoprire eventuali falle troppo tardi e i responsabili della messa in atto del piano potranno farlo più facilmente dopo un’ampia pratica. Le fasi proattive possono includere esercitazioni di IR, penetration test, esercitazioni tabletop e purple teaming, ed è fondamentale che tutti i principali stakeholder partecipino effettivamente alla valutazione del piano.

6. Pianificare un budget Zero-Day

Anche il miglior piano può fallire se non c’è un budget per eseguirlo. È fondamentale accantonarne uno per affrontare i

costi in caso di incidente zero-day. Un’organizzazione può avere un’assicurazione che copre un attacco informatico, ma ci sarà bisogno di capitale per coprire costi accessori o inaspettati. È importante, inoltre, che i responsabili siano consapevoli di come utilizzare il budget, per evitare di prendere decisioni durante un incidente o di subire limitazioni della capacità di risposta.
Ad esempio, in caso di incidente, potrebbe essere necessario acquistare nuovi computer o componenti hardware per mantenere le operazioni o investire in software per contenere un attacco. Si tratta di una discussione da intraprendere già in fase di pianificazione, in modo da evitare incertezze o perdite di tempo sotto pressione.

7. La formazione sulla risposta agli incidenti deve essere una priorità

Con le numerose attività di business quotidiane, può accadere di lasciare che la formazione sulla risposta agli incidenti passi in secondo piano, portando a strategie e risposte poco convincenti nei momenti più importanti. Tutte le organizzazioni, a prescindere dalle dimensioni, dovrebbero fare della formazione sull’incident response una priorità. La formazione dovrebbe essere inserita nel piano di gestione dell’IR e programmata di conseguenza, includendo l’analisi di vari scenari ed esercitazioni delle azioni di risposta, in modo che tutti sappiano di cosa sono responsabili e prevedere anche la condivisione delle conoscenze tra i membri del team di IR per evitare un singolo punto di guasto, in cui solo una persona possiede conoscenze specifiche su software, hardware o sistemi chiave.

La formazione deve essere continua e seguire l’integrazione di nuove tecnologie (ad esempio, endpoint e strumenti di rilevamento o risposta) nell’ambiente. Con così tanti rischi, è fondamentale che la risposta agli incidenti sia tempestiva

ed efficace. Un robusto piano di IR, che includa preparazione, formazione e test, farà sì che, sebbene le probabilità di un incidente di sicurezza siano elevate, un’azienda sia in grado di affrontare la sfida e gestire l’incidente con successo.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/sette-consigli-per-ottimizzare-il-piano-di-incident-response/