N-able indica agli MSP le tre fasi per gestire un attacco informatico

Gli **MSP** sono uno dei **principali bersagli degli attacchi informatici.** A dirlo è **Dave MacKinnon, Chief Security Officer di N-able: "***Non è una questione di "se", ma di "quando" l'attacco potrebbe verificarsi e il fattore di differenziazione per la maggior parte degli MSP e dei loro clienti è* ***quanto velocemente si riesce ad attuare un piano di risposta e recovery".***

Il successo di un MSP attento alla sicurezza che desidera proteggere le proprie risorse digitali e la propria reputazione aziendale dipende dalla sicurezza dei suoi clienti e dall'efficacia delle misure di sicurezza adottate. Capire **dove risiede la responsabilità nel caso di un attacco informatico** – contro l'MSP o i suoi clienti – è fondamentale per **identificare la portata del problema, contenerlo e risolverlo**. Individuare l'**origine dell'attacco** consente di migliorare il livello di sicurezza di tutte le parti

coinvolte.
Una recente ricerca di Gartner mostra che oltre il 90% dei dipendenti ha ammesso di aver attuato una serie di azioni non sicure durante le attività lavorative con la consapevolezza di poter esporre la propria azienda ai rischi.
L'e-book di Gartner rileva che entro il 2025, il 60% delle aziende prenderà in esame l'analisi del rischio informatico come fattore significativo nelle trattative con parti terze per evitare la compromissione di informazioni, sistemi e infrastrutture. Se a ciò si aggiunge che gli attacchi informatici di oggi sono sempre più sofisticati, gli MSP, e i CISO in generale, devono necessariamente essere proattivi e pronti nell'avere un piano di risposta e recovery.
Come la maggior parte dei processi di pianificazione, nella gestione di un attacco informatico c'è un "Prima", un "Durante "e un "Dopo". Ne parla MacKinnon.

Prima dell'attacco

- Promuovere e mantenere una cultura aziendale orientata alla sicurezza e basata su un approccio Zero Trust
- Valutare costantemente le abitudini di sicurezza informatica dei propri clienti e assicurarsi che le policy e le patch di sicurezza siano aggiornate. Adottare misure per ridurre al minimo i rischi con l'automazione, la gestione delle identità, le policy, i sistemi e le procedure. Aggiornare regolarmente i propri sistemi e i software dei clienti per prevenire gli attacchi informatici.
- Stabilire le best practice e gli standard di sicurezza per la propria azienda e i propri clienti e valutarli regolarmente.
- Creare un piano di backup e di Disaster Recovery as a Service (DRaaS) e riesaminarlo almeno una volta al trimestre, tenendo presente che il ripristino istantaneo non è sempre l'opzione migliore o disponibile per un recupero e un ripristino sicuri.

- Contemporaneamente, sviluppare un piano di risposta agli incidenti che delinei le misure da adottare in caso di attacco. Dovrebbe includere misure per isolare i sistemi infetti, informare le parti interessate e ripristinare le operazioni aziendali. Questo piano deve essere collegato al piano di disaster receovery. Identificare il piano di comunicazione di crisi e l'albero delle chiamate (compresi i legali, l'assicurazione, le principali parti interessate, i coach per gli stati di crisi, l'ecosistema dei partner e i dipendenti).
- Stampare una copia cartacea del proprio piano (nel caso in cui non sia possibile accedervi durante un attacco) e creare una sintesi di una sola pagina con i punti più importanti.
- Incoraggiare i propri clienti a eseguire esercitazioni per la loro azienda e per i clienti per l'esecuzione di un piano di ripristino d'emergenza: testare le procedure e individuare le lacune. L'obiettivo di queste esercitazioni è il miglioramento continuo.
- Promuovere la resilienza alle minacce informatiche in modo da poter rispondere a una violazione riuscendo al contempo a portare avanti le attività quotidiane.

Durante l'attacco

- Identificare il tipo di attacco.
- Mettere in atto il piano di risposta agli incidenti, determinare la gravità del problema e iniziare ad attivare il team di risposta agli incidenti.
- Contenere l'incidente in base al proprio piano di risposta agli incidenti. Ciò può comportare l'isolamento di un endpoint, la disconnessione della rete interessata da Internet, la disabilitazione dell'accesso remoto o la modifica di tutte le password.
- Valutare l'esposizione dei dati. Determinare se questo problema costituisce una violazione della sicurezza.

- Stabilire se è necessario coinvolgere il proprio agente di assicurazione informatica, un consulente legale o addirittura le autorità.
- Avviare il piano di comunicazione di crisi.
- Eseguire il piano di backup e disaster recovery, che comprenda anche la strategia di resilienza informatica.

Dopo l'attacco

- Valutare i danni.
- Eseguire il debrief con il team di risposta agli incidenti.
- Comunicare con clienti, stakeholder, investitori, partner e dipendenti.
- Imparare dall'esperienza e condividerla.
- Ampliare le misure di protezione per garantire che la causa scatenante non si verifichi nuovamente.
- Ampliare le misure di rilevamento per garantire il rilevamento delle variazioni dell'attacco nell'ambiente aziendale.
- Istituire un nuovo piano di prevenzione basato su quanto appreso.
- Verificare le aree che non hanno funzionato bene durante le esercitazioni.

MacKinnon conclude: *"Per preservare il successo e la reputazione della propria azienda e dei clienti, è indispensabile una* ***pianificazione, prevenzione, monitoraggio, rilevamento e ripristino dei processi.*** *Adottando le misure sopra elencate, gli MSP potranno meglio proteggere il loro team e i loro clienti dagli attacchi informatici e consentire loro una ripresa più rapida e in sicurezza".*