La zona grigia che affligge la cyber security

Date : 20 ottobre 2017

Di fronte all'odierno panorama caratterizzato da minacce di livello avanzato, da tempo la best-practice prevede una difesa stratificata e profonda. La prima linea di tale difesa (a parte solide attività di formazione e di manutenzione dei sistemi) solitamente è perimetrale: antivirus, firewall di ultima generazione e sistemi antintrusione (Intrusion Prevention Systems, IPS). Gli altri strati di difesa possono prevedere sistemi per la gestione degli eventi e delle informazioni sulla sicurezza (Security Information and Event Management, SIEM) oltre a soluzioni per la prevenzione della perdita di dati (Data Loss Prevention, DLP) e le innovative soluzioni di risposta e rilevazione degli endpoint (Endpoint Detection and Response, EDR).

Tuttavia, tutti questi strati lasciano una zona grigia: dopo che il malintenzionato si è introdotto nel perimetro, ma prima che abbia compromesso i sistemi chiave e trafugato i dati. Attualmente è difficile notare, tenere traccia e contrastare rapidamente malware avanzati e attacchi mirati presenti proprio in queste fasi. Occorre dunque una visibilità in tempo reale delle possibili attività di minaccia dopo l'exploit iniziale, mentre l'infiltrato valuta la rete, cerca i punti deboli e si prepara ad appropriarsi dei dati.

La zona grigia odierna

Il problema risiede nel fatto che le difese perimetrali forniscono un'allerta per le minacce note, ma non hanno visibilità sulla ricognizione dell'avversario o i movimenti laterali e soprattutto non sono in grado di capire quali altri sistemi potrebbero essere compromessi. Ciò è dovuto ai sistemi di prevenzione della perdita di dati e di risposta e rilevamento degli endpoint, che avvertono in caso di accessi sospetti e/o di furti di asset critici. Purtroppo, tali sistemi non sono concepiti per individuare e tantomeno tenere traccia di comportamenti minacciosi che si presentano in rete.

Sebbene offrano una maggiore visibilità, i sistemi SIEM sono sviluppati per fungere da strutture difensive che reagiscono a indicatori noti; soluzioni non ottimali, dunque, al momento di individuare in maniera proattiva movimenti laterali sospetti oppure attività correlate a malware nuovi/ignoti. Riuscire a filtrare e assegnare una priorità agli effettivi indicatori di compromissione (Indicators of Compromise, IoC) tra l'immensa mole di allerte può rivelarsi un compito arduo. Come se non bastasse, ottenere un'immagine completa di un'intera attività di attacco che

interessa la rete è difficile e richiede tempi lunghi.

Le minacce più pericolose da affrontare al giorno d'oggi non sono i semplici malware ma le campagne di attacco orchestrate da soggetti umani. La componente malware è comunque sviluppata per operare furtivamente eludendo, inosservata, gli strati di sicurezza. Questi strumenti riscuotono successo: numerose violazioni restano ignote finché un soggetto terzo non avverte la vittima.

Migliore visibilità dopo l'exploit

Ciò che occorre realmente è una visibilità immediata e flessibile delle tecniche di attacco, dopo le manovre iniziali (siano essere rilevate o meno) e prima che dati e sistemi vengano ulteriormente compromessi: l'avanscoperta interna, il movimento laterale, le comunicazioni esterne, le credenziali soggette a escalation o rubate. Grazie a una migliore visibilità dopo l'exploit le aziende possono:

- Attivarsi proattivamente nella ricerca di attacchi di matrice umana; indagare se le minacce in atto possano annidarsi nella rete. Considerando che la rapidità è essenziale, i team IT sono in grado di collegare meglio le allerte, i sistemi e i comportamenti;
- Ottimizzare le operazioni dei SOC esistenti e gli investimenti in strumenti di sicurezza aggiornati, ad esempio con un'individuazione più rapida dei falsi positivi e l'assegnazione delle priorità alle minacce reali;
- Arrestare completamente le infiltrazioni e ostacolare gli attacchi. Tenere traccia dei movimenti laterali degli antagonisti, dei sistemi che hanno toccato o dei payload lanciati, oltre a eliminare tutte le componenti dell'attacco prima che possano provocare danni.

L'automazione al servizio delle capacità umane

L'entità, la quantità di dati e la velocità della minaccia impongono il massimo livello di automazione possibile nella visibilità successiva all'attacco. Tuttavia, gli attacchi più complessi sono ideati da soggetti umani e, come già noto, nessuna macchina analitica riesce a superare la mente umana quanto a complessità e sofisticazione. L'automazione non è mai in grado di sostituirsi agli addetti umani alla difesa che combattono in prima linea, ma è senz'altro un utile strumento che li coadiuva e ne potenzia le capacità.

Man mano che si ampliano le conoscenze sul comportamento di attacco e sui processi per individuarli l'automazione diventa sempre più utile e imprescindibile. Si tratta di uno strumento in rapida evoluzione, che può però già essere suddiviso in tre categorie.

- Automazione di flussi di lavoro: automazione del flusso quotidiano del SOC in cui i diversi processi, talvolta anche le comunicazioni manuali al telefono e le e-mail, e l'uso di fogli elettronici sono integrati e automatizzati. Si tratta di un processo simile a quello avvenuto negli anni '90 del secolo scorso con l'automazione degli help desk informatici.
- Analisi automatizzata: integrazione di intelligence delle minacce più attenta al contesto

per un’analisi che fa leva sull’automazione. Dalla ricerca basata sul contesto all’individuazione più veloce dei falsi positivi grazie alla correlazione automatica dei dati provenienti dai vari sistemi. Popolazione automatica delle indagini SOC con intelligence sulle minacce contestuali: insieme alla visualizzazione degli specifici indicatori l’utente, l’IP di destinazione (con i dati relativi alla reputazione) e la porta in uso. In questi casi l’automazione riesce a ridurre le operazioni manuali oltre a rendere possibile una valutazione più veloce ed efficace delle allerta.

- Risposta automatica alle minacce: contromisure automatiche presso endpoint e reti volte a rispondere alle minacce prima che i dati vengano sottratti. Sviluppo di playbook per la sicurezza e contromisure “immediate”, ad esempio un attacco malware confermato si traduce nella quarantena per l’host e nel blocco dell’IP nel firewall.

Ma la vera battaglia contro le campagne di attacco avanzate si combatte dopo che è già avvenuta la violazione. È dunque essenziale disporre della visibilità in tempo reale delle tecniche di attacco adottate. La visibilità successiva all’exploit ostacola gli avversari nel tentativo di celarsi e agevola chi subisce l’attacco nelle attività di difesa. È dunque ora che le organizzazioni si sbarazzino della zona grigia che affligge la cyber security dei propri sistemi.

A cura di: ***Ivan Straniero****, Regional Manager, Southern & Eastern Europe di Arbor Networks*