Ottimizzare denaro, tempo, risorse

Negli ultimi tempi, uno dei cambiamenti più evidenti che ha interessato lo scenario della sicurezza informatica è stato il ricorso ad elevati livelli di automazione nell'analisi del traffico di dati alla ricerca di malware, incursioni da parte di criminali informatici e altri vettori di attacco. Nel settore dell'IT Security, alcuni vendor hanno abbandonato la pura analisi in profondità dei pacchetti di dati – a causa dell'eccessivo carico del processore derivante da un controllo in tempo reale – per adottare il principio di verifica delle credenziali di autenticazione dell'utente su un dato indirizzo IP e di quali applicazioni sono in esecuzione.

Quest'approccio si discosta dal tradizionale ricorso alla tecnologia IDS/IPS, che richiede un'analisi euristica per monitorare le applicazioni dell'utente, prima di consentire o rifiutarne l'accesso all'indirizzo IP. Questo è un elemento interessante, dal momento che per migliorare la protezione delle reti aziendali dalla crescente ondata di minacce multi-vettoriali e ibride, è necessario uno sforzo comune per migliorare le performance dei sistemi e dei software di sicurezza IT, oltre che dell'architettura che li supporta.

A nostro parere, vi è una chiara e stringente necessità di definire metodi misurabili per il controllo della sicurezza, insieme al monitoraggio automatizzato e al reporting degli incidenti. In particolare, i nostri studi sulle Tecniche di Evasione Avanzate (AET), che i cyber criminali sempre più utilizzano per diffondere il malware, evidenziano come le organizzazioni debbano sviluppare un insieme ben progettato di azioni di risposta agli incidenti.

Ritengo anche che l'adozione di quest'approccio da parte delle aziende possa aiutarle a ridurre i costi marginali legati alla sicurezza – limitando anche i danni che un'assenza di sistemi di difesa può causare – oltre ai costi fissi, contribuendo così ad una diminuzione dei valori Capex e Opex. Questo metodo automatizzato per il monitoraggio dell'utente e delle applicazioni in esecuzione si rivela essenziale per fronteggiare il crescente volume di traffico che scorre attraverso la Porta 80, lo standard normalmente assegnato al traffico internet.

Se si consente il passaggio del traffico dati dalla porta 80 – come solitamente accade in tutte le organizzazioni – automaticamente si approva il passaggio di pseudo traffico che transita insieme alle pagine Web regolari. Ma se il processo di analisi in profondità del pacchetto dati divora letteralmente risorse, quali sono le alternative che può adottare l'IT Security Manager assieme al suo team? Crediamo che la soluzione risieda nel monitorare solo le applicazioni attive sulle macchine da ispezionare.

Insieme all'analisi del flusso di dati, questo metodo facilita notevolmente il livello di automazione nel processo di ispezione richiesto per quantificare il rischio generato dal passaggio di un certo segmento di codice all'interno dell'infrastruttura di rete. Quest'approccio può essere straordinariamente utile nel difendersi dal problema crescente delle minacce di sicurezza che affligge i vendor di IT Security che, con il rilevamento di decine di migliaia di nuove tipologie di malware alla settimana, costringono a focalizzare l'attenzione solo sulle ultime minacce scoperte. Ciò significa che se un criminale particolarmente capace riutilizza un malware già noto modificando la metodologia con cui questo attacco viene veicolato, esiste il rischio che i tradizionali sistemi di protezione non siano in grado di rilevare la nuova minaccia modificata nel momento in cui viene lanciato il primo nuovo attacco.

La situazione si aggrava se consideriamo che non è raro che un PC aziendale manchi di patch o di aggiornamenti del sistema operativo, vanificando in tal modo l'efficacia dei sistemi di protezione da alcuni vettori di attacco. Intervenire con patch dopo che l'attacco è stato sferrato non è sufficiente per eliminare il problema. I tradizionali sistemi di sicurezza IPS (Intrusion Prevention System) sono progettati per operare su due livelli: innanzitutto per bloccare vettori di attacco conosciuti, e in secondo luogo per lanciare un allarme nel momento in cui viene rilevata un'intrusione.

Pensiamo alle minacce veicolate tramite AET: non solo riescono ad eludere le soluzioni IPS, ma lo fanno agendo in maniera silente e impercettibile. I vendor IPS dovrebbero mostrare maggiore attenzione a questa tipologia di attacchi, prendendo la decisione di utilizzare alcuni dei cicli di CPU disponibili per analizzare ancora più a fondo i pacchetti di dati che transitano nei sistemi di rete. L'altra faccia della medaglia è che quest'approccio genera un aumento dei costi per gigabyte di dati analizzati, ma d'altronde se un criminale è in grado di eludere le difese di un'organizzazione, perché possedere quei sistemi di protezione?

Riuscire a sviluppare una strategia di sicurezza IT economicamente efficiente significa ottimizzare le risorse già esistenti e utilizzare il denaro risparmiato per investire in un sistema di sicurezza IT multi-livello. Ma prima di percorrere questa strada, è necessario condurre un'analisi completa del rischio e una classificazione dei dati della propria organizzazione e solo quando questi due processi sono completi l'IT Security Manager può iniziare a pianificare le fasi di un processo di protezione multi-livello.

Queste fasi dovrebbero essere riviste alla luce della necessità di effettuare un'analisi dei costi, utilizzando indicatori KPI (Key Performance Indicator), per presentare i valori di Capex e Opex in un formato che può essere paragonato a quelli generati dalle più tradizionali architetture IT. Si tratta di un aspetto importante per una moderna pianificazione dei sistemi di sicurezza a protezione di una rete aziendale, spesso sottovalutato dai professionisti IT che non considerano le valutazioni economiche tra le loro competenze, con il rischio che decisioni riguardanti l'infrastruttura IT vengano prese dal reparto finanziario. Si manifesta pertanto la necessità di lavorare in team collaborando allo sviluppo di strategie di sicurezza IT più efficienti. La pianificazione è fondamentale quando si tratta di affrontare un crescente flusso di attacchi ibridi da parte di hacker e di cyber criminali alla piattaforma IT aziendale per meglio difendersi dagli attacchi basati sulle AET in grado di eludere i sistemi di sicurezza esistenti.