SICUREZZA AZIENDALE ALLA PORTATA DI PICCOLE E MEDIE IMPRESE

PANORAMICA

La maggior parte delle aziende dipende da protocolli di email e web per scopi commerciali. Di conseguenza, la maggior parte degli attacchi informatici inizia con questi protocolli. Una protezione efficace rileva e previene sia gli attacchi di base noti che gli attacchi avanzati sconosciuti. Le tecnologie FireEye di maggiore successo individuano e fermano con accuratezza gli attacchi avanzati multifase e multivettoriali. Dotano i team di sicurezza di strumenti efficaci che consentono l'efficienza operativa attraverso l'emissione di un numero significativamente inferiore di falsi positivi. Si tratta di soluzioni preziose che sono pensate per un accesso e un uso facile da parte delle aziende, che in questo modo possono concentrarsi a far crescere il business.

FireEye è all'avanguardia nella tecnologia di rilevamento degli attacchi sconosciuti avanzati, ma inizialmente era utilizzata solo dalle grandi aziende. Tuttavia, gli aggressori informatici prendono di mira le aziende di tutte le dimensioni. Le piccole e medie imprese (PMI) sono consapevoli di non essere immuni e che la protezione avanzata delle minacce è fondamentale per il loro quadro di sicurezza.

LE SFIDE DELLA SICUREZZA

Le piccole e medie imprese si trovano ad affrontare molte sfide di sicurezza, in parte a causa della natura dinamica del panorama delle minacce informatiche e in parte a causa di come PMI tentano di rendere operativa la gestione della sicurezza all'interno dell'azienda.

Le sfide legate al panorama delle minacce derivano in genere da una mancanza di visibilità di sicurezza in tutta l'azienda. Le tecnologie legacy perimetrali di rilevamento e prevenzione che si basano sulle firme di attacco fanno fatica a identificare le minacce di oggi. Gli aggressori sfruttano le tecniche per cambiare la firma rivelatrice del malware in modo che appaia una sola volta in ogni data azienda. In molti casi, il malware non è nemmeno coinvolto negli attacchi.

Le sfide legate alle operazioni di sicurezza ruotano intorno al fatto che le PMI ricevono spesso troppi avvisi di sicurezza che richiedono un intervento dalle risorse umane di cui non dispongono. Molti avvisi sono falsi positivi e il tempo degli analisti viene sprecato indagando problemi non correlati alla protezione. Troppi falsi positivi possono anche nascondere veri positivi che richiedono un'interazione immediata per ridurne l'impatto.

Ci sono ulteriori complicazioni. Per studiare gli avvisi, le PMI devono assumere personale con adeguate competenze di sicurezza. Nella maggior parte delle aziende, le risorse di sicurezza fanno parte del reparto IT, il che crea conflitti di interesse. Le PMI che applicano un approccio a più livelli di difesa in profondità possono trovarsi a utilizzare molteplici strumenti tecnologici di sicurezza che sono spesso mal gestiti, gestiti dai fornitori di servizi di sicurezza o non gestiti affatto. Nella migliore delle ipotesi, questo può causare costi eccessivi e, nel peggiore dei casi, può presentare una significativa esposizione al rischio. Queste sfide sono tutte collegate: le PMI devono controllare i costi impiegando personale molto limitato per gestire molti strumenti di sicurezza che generano troppi avvisi.

LA SOLUZIONE

La soluzione FireEye combina Network Security Essentials (NXE) e Email Threat Prevention Cloud (ETP) per proteggere le aziende dalle minacce basate su email e web.[1] Questi due vettori rappresentano il 90% degli attacchi informatici. La soluzione aiuta le imprese a ottimizzare il budget per la sicurezza, individuando problemi di sicurezza gravi, senza la distrazione dei falsi positivi che appesantiscono inutilmente la portata e la tempestività della risposta agli incidenti.

Al centro di queste tecnologie FireEye c'è il potente motore FireEye Multi-Vector Virtual Execution™ (MVX). Si tratta di una tecnologia che individua gli attacchi multifase e le minacce combinate che colpiscono più vettori, compreso il web e le email, che prese isolatamente potrebbero non sembrare pericolose.

La correlazione degli URL dannosi con le e-mail di spear-phishing è fondamentale per individuare una salva d'apertura di più attacchi multivettoriali. Il motore Cloud MVX ha la capacità di approfondire questi legami e consente alle aziende di vedere la correlazione tra i due eventi e quindi blocca automaticamente le fasi successive dell'attacco, come il tentativo degli aggressori di provare a trasferire i dati rubati sul web. Inoltre, individua e blocca gli attacchi successivi che sfruttano tattiche, tecniche e procedure (*Tactics, Tools and Procedures*, TTP) simili.

Grazie a un elevato livello di automazione, efficienza ed efficacia, questa soluzione consente alle aziende di ottimizzare nel complesso l'approccio alla sicurezza e semplificare l'applicazione e la gestione quotidiana della sicurezza della rete e delle email.

Network Security Essentials

Network Security Essentials è una soluzione economica plug-and-play per la sicurezza della rete che può essere implementata in meno di 60 minuti per ridurre al minimo il rischio di costose violazioni.

Oltre al motore brevettato e senza firma Cloud MVX, Network Security Essentials include la tecnologia Intelligence-Driven Analysis che identifica e blocca le minacce note e sconosciute. La tecnologia Intelligence-Driven Analysis è una raccolta di motori contestuali basati su regole, che rilevano e bloccano le attività dannose grazie alle ultime informazioni basate su macchina, aggressore e vittima. Un sistema di prevenzione delle intrusioni (*Intrusion Prevention System*, IPS) rileva gli attacchi comuni con firma convenzionale e garantisce la protezione dal riskware per bloccare spyware e adware. Al contrario dei firewall convenzionali o di nuova generazione, delle soluzioni antivirus (AV) o solo IPS, Network Security Essentials rileva con maggiore precisione gli attacchi zero-day sia noti che sconosciuti, generando al contempo un numero ridotto di falsi positivi, consentendo ai team di sicurezza di concentrarsi sugli avvisi importanti.

Opzioni di distribuzione flessibili

Network Security Essentials richiede un'appliance virtuale o fisica in loco che può essere distribuita sia in modalità in linea che in solo monitoraggio. Network Smart Node, l'appliance in loco, può essere distribuita in una serie di posizioni, dal perimetro di rete principale alle sedi remote, in pratica ovunque ci sia un accesso diretto a Internet. L'immagine della macchina virtuale scaricabile (Figura 1) è preferita perché è conveniente e rapida da implementare. I Network Smart Nodes utilizzano la tecnologia Intelligence-Driven Analysis e il rilevamento IPS basato su firma per identificare e proteggere da attività sospette. Utilizzano una connessione crittografata per inviare oggetti sospetti che richiedono ulteriori analisi al servizio Cloud MVX nel cloud privato FireEye. Il servizio Network Smart Node e Cloud MVX è disponibile anche come appliance hardware integrata (Figura 2). FireEye consiglia l'opzione 50 Mbps per le piccole imprese e 100 Mbps per le medie imprese.

Sicurezza email: Email Threat Protection Cloud

L'email viene spesso utilizzata per avviare le principali violazioni. Email Threat Protection (ETP) è una soluzione cloud-based Software-as-a-Service (SaaS) che analizza le email alla ricerca di segnali di spear phishing nonché i commodity virus e le minacce spam. ETP usa la tecnologia brevettata Cloud MVX per prevenire attivamente gli attacchi email avanzati. Fornisce anche una protezione anti-spam e antivirus in linea. ETP è in grado di proteggere sia le caselle in locale che quelle su cloud con distribuzione in linea o solo monitoraggio.

Informazioni sulle minacce

Le informazioni sulle minacce cloud-based di FireEye accompagnano gli avvisi della soluzione FireEye. Le informazioni, aggiornate ogni 60 minuti, comprendono le informazioni sui nuovi profili di malware, gli exploit sulla vulnerabilità, le informazioni su avversari e vittime e le minacce rilevate. Integra il motore Cloud MVX con analisi cloud-enabled e tecnologie di apprendimento automatico per rilevare le minacce avanzate. Pertanto, gli avvisi sugli attacchi FireEye possono comprendere importanti informazioni contestualizzate, come la possibile identità degli autori delle minacce, i motivi più probabili e i dettagli del malware, per aiutare i professionisti della sicurezza a rilevare e bloccare attacchi zero-day altamente mirati e il malware noto.

[1] Verizon 2015 Data Breach Investigations Report

CONFIGURAZIONI DI ESEMPIO

I fattori da considerare quando si assembla una soluzione includono: il numero di caselle di email da monitorare, il volume di traffico di rete che attraversa il sistema, l'ambiente virtualizzato o fisico, l'adozione di servizi cloud-delivered e il livello di consapevolezza della sicurezza degli alti dirigenti e del consiglio di amministrazione. FireEye e i suoi partner possono aiutarti a scegliere o progettare una soluzione che soddisfi le tue esigenze, sulla base di queste configurazioni di esempio.

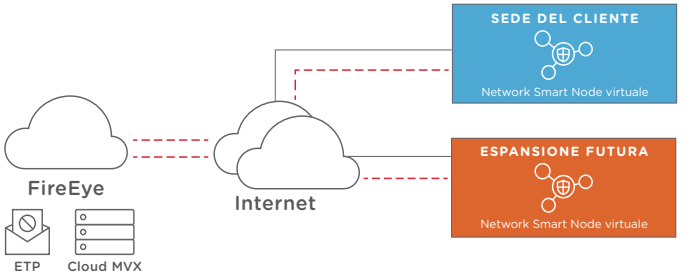

FIGURA 1. ETP CLOUD E CLOUD MVX CON APPLIANCE VIRTUALI

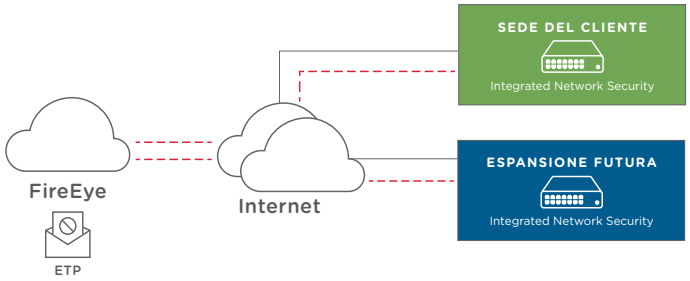

FIGURA 2. ETP CLOUD E APPLIANCE FISICHE INTEGRATED NETWORK SECURITY

	PICCOLA 1	PICCOLA 2	MEDIA 1	MEDIA 2
TIPO DI DISTRIBUZIONE	**VIRTUALE/CLOUD**	**APPLIANCE FISICA**	**VIRTUALE/CLOUD**	**APPLIANCE FISICA**
Numero di dipendenti	200-250	200-250	450-550	450-550
Traffico di rete	50 Mbit/s	50 Mbit/s	100 Mbit/s	100 Mbit/s
Soluzione di esempio proposta	ETP 200-250 posti NX1500 virtuale Cloud MVX	ETP 200-250 posti 2500NXE1 integrato	ETP 450-550 posti NX2500 virtuale Cloud MVX	ETP 450-550 posti 2500NXE2 integrato

PROSSIME TAPPE

Le PMI sono il bersaglio prediletto o un'opportunità per gli autori di attacchi avanzati perché spesso adottano misure di sicurezza deboli, dovute in larga misura alle scarse risorse e a una consapevolezza insufficiente. Per far crescere l'azienda e ridurre i rischi, è fondamentale mantenere un livello essenziale di sicurezza. E per questo è necessaria la fiducia nello stato di sicurezza, nonché nel programma, negli strumenti e nei processi di sicurezza.

Per saperne di più su FireEye, visita:
www.FireEye.com

A PROPOSITO DI FIREEYE, INC.

FireEye® è leader nella sicurezza come servizio basato sulle informazioni. Fungendo da estensione semplice e scalabile delle operazioni di sicurezza del cliente, FireEye offre un'unica piattaforma che fonde tecnologie di sicurezza innovative, informazioni sulle minacce a livello nazionale e i servizi di consulenza Mandiant®, rinomati in tutto il mondo. L'azienda ha oltre 5.000 clienti in 67 Paesi, tra cui più di 940 dei Forbes Global 2000.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com