FORTINET

Strategie che riducono la complessità e semplificano le operazioni di sicurezza

Sommario

FORTINET

Panoramica preliminare

Due dei numeri che sono cresciuti più rapidamente nel campo della sicurezza informatica negli ultimi anni sono la varietà di minacce e il numero di strumenti di sicurezza specifici progettati per affrontarle. Gli architetti della sicurezza si trovano ad affrontare una complessità crescente che rende difficili le operazioni di sicurezza. Tuttavia, tre strategie riducono sostanzialmente tale complessità: 1) centralizzare e attribuire una priorità alle minacce, 2) semplificare l'audit e la compliance e 3) automatizzare per velocizzare la risposta, tre strategie chiave che migliorano sostanzialmente le operazioni di sicurezza e l'approccio alla sicurezza di un'organizzazione.

Fino al 40% del nuovo malware rilevato in un determinato giorno è zero-day o precedentemente sconosciuto.[1]

In un'azienda media vengono utilizzati 75 diversi strumenti di sicurezza.[2]

Oggi nel mondo sono scoperti quasi 3 milioni di posti nel campo della sicurezza.[3]

Introduzione: troppi dati utili sulla sicurezza

Per i professionisti della sicurezza, i numeri sono scoraggianti: con l'aumento del volume e della sofisticatezza delle minacce informatiche, le organizzazioni non hanno a disposizione abbastanza specialisti del campo per affrontarle.

Il problema non è che i team incaricati della sicurezza non dispongono di strumenti di sicurezza informatica o di dati preziosi provenienti da tali strumenti per agire. Sono invece troppi: troppi registri da correlare, troppe console da gestire e troppe segnalazioni da analizzare. Non sorprende che il 79% dei team incaricati della sicurezza si dichiari sopraffatto dal volume delle segnalazioni.[4]

L'insegnamento è che gli architetti della sicurezza devono prendere in considerazione diverse strategie per ridurre la complessità e semplificare le operazioni di sicurezza.

01 Centralizzare la visibilità e attribuire una priorità alle minacce

Il monitoraggio della sicurezza deve essere centralizzato. I team hanno bisogno di un approccio alla sicurezza che fornisca una visibilità unica attraverso un portale appositamente studiato, oppure la capacità di integrare le soluzioni di sicurezza con un strumento di visibilità di loro scelta tra quelli più diffusi.

La soluzione deve fornire una panoramica delle anomalie in tutta l'azienda digitale estesa, compresi gli ambienti on-premises, cloud, IoT (Internet-of-Things) e OT (Operational Technology). Un approccio alla gestione dei registri e della sicurezza di tipo analitico mette in correlazione i dati provenienti da più dispositivi e combatte l'affaticamento dovuto all'eccessivo numero di segnalazioni fornendo una visione critica delle minacce e individua dove è necessaria una risposta immediata, consentendo di agire tempestivamente.

La soluzione deve anche consentire la distribuzione zero-touch delle configurazioni di sicurezza in tutta l'azienda, riducendo al minimo gli errori umani e le configurazioni errate, e deve assicurare un'ampia visibilità degli indicatori di compromissione (IOC) ai team incaricati della sicurezza e delle operazioni, utilizzando l'apprendimento automatico (ML) per stabilire le linee comportamentali di base, rilevare le anomalie e consentire l'identificazione degli IOC, oltre a ricevere nuovi aggiornamenti degli IOC estrapolati da analisi automatizzate e umane di altri ambienti in tutto il mondo, forniti da un feed di threat intelligence.

Avere la threat intelligence in un unico feed è importante e di fatto pone l'accento sui rischi per la sicurezza. Ad esempio, in due recenti violazioni globali, i team hanno trascurato gli avvertimenti a causa di un eccesso di segnalazioni.[5]

02 Semplificare l’audit e la compliance

Quando le aziende sono troppo lente ad attuare misure di sicurezza critiche per proteggere i propri dati, intervengono le autorità federali, statali e locali. A livello globale, le normative sulla sicurezza informatica si moltiplicano e diventano sempre più rigide.[6] Il regolamento generale sulla protezione dei dati dell’Unione europea (GDPR), che prevede sanzioni e multe severe, è il più corposo mai visto finora.[7] E con l’imminente entrata in vigore del California Consumer Privacy Act (CCPA), le preoccupazioni sulla privacy dei dati non faranno che aumentare per gli architetti della sicurezza.[8]

I team incaricati della sicurezza devono cercare una soluzione analitica che fornisca strumenti per mappare le operazioni secondo le best practice del settore, che si basano sugli standard di sicurezza di organizzazioni quali il National Institute of Standards and Technology (NIST) e il Center for Internet Security (CIS). La soluzione deve anche generare rapporti che aiutino a dimostrare la compliance a normative come il Payment Card Industry Data Security Standard (PCI DSS).

Inoltre, i responsabili della sicurezza devono considerare un approccio analitico che risponda a tre importanti domande legate alla supervisione:

1. La rete è configurata correttamente? È possibile identificare i problemi di configurazione prima che provochino un incidente?
2. Qual è l'approccio assunto in generale nei confronti della sicurezza? La risposta dovrebbe riassumersi in un unico parametro, un punteggio che nel tempo risulta utile per dimostrare l'impatto degli investimenti nella sicurezza e riferire le tendenze generali alla direzione esecutiva e al consiglio di amministrazione.
3. Cos'è la prova della compliance? Una soluzione può far risparmiare centinaia di ore di analisi manuale se è in grado di analizzare e segnalare le modifiche intervenute nella topologia della rete. Deve semplificare l'identificazione e il ripristino dei dispositivi ad alto rischio e non conformi e fornire piani di azione e rapporti sullo stato di avanzamento sia al livello tecnico che gestionale.

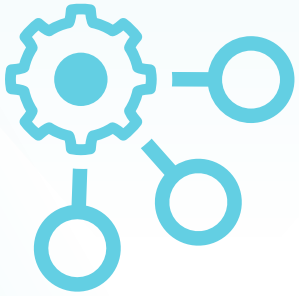
Le risposte a queste domande possono essere sintetizzate in un punteggio di rischio oggettivo, che deve includere raffronti con benchmark accettati e organizzazioni di pari livello, oltre a consigli attuabili su come ottenere una migliore strategia di gestione del rischio.[9] Il corrispondente punteggio di valutazione della sicurezza consente agli architetti della sicurezza di stabilire gli elementi indispensabili della sicurezza con le relative priorità, consentendo nel contempo ai team incaricati delle operazioni di sicurezza di assegnare le risorse in base alla tolleranza al rischio e alle vulnerabilità identificate. Inoltre, i team incaricati delle operazioni di sicurezza può utilizzare un storico facilmente accessibile di problemi di sicurezza e attività di attenuazione da sfruttare per gestire in modo proattivo il rischio.[10]

"I parametri relativi al rischio tecnologico monitorano il raggiungimento degli obiettivi e dei traguardi quantificando l'attuazione, l'efficienza e l'efficacia dei controlli di sicurezza, analizzando l'adeguatezza delle attività del programma di sicurezza delle informazioni e identificando le possibili azioni di miglioramento."[11]

03 Automatizzare per velocizzare la risposta

I team dei NOC (Network Operations Center) e dei SOC (Security Operations Center) condividono gli stessi obiettivi di garantire la disponibilità e la protezione dei servizi, ma hanno prospettive e strumenti diversi. Per aiutarli a collaborare, gli architetti della sicurezza devono considerare un approccio alla sicurezza e alla gestione dei registri basato sull'analisi, che fornisca una visione consolidata delle operazioni e della sicurezza. Ciò consente al personale dei NOC e dei SOC di allinearsi tra loro e vedere i dati dei NOC e dei SOC in maniera integrata e correlata. Il rilevamento delle minacce basato sull'analisi identifica le minacce attribuendovi un rischio alto, medio o basso. Inoltre, per indagare più velocemente una minaccia, è necessario che una vista cronologia dell'incidente mostri gli eventi contestualizzati.

Questa soluzione può inoltre integrarsi con le soluzioni di gestione delle informazioni di sicurezza e degli eventi (SIEM) e gestione dei servizi IT (ITSM), automatizzando il processo di approvazione del flusso di lavoro tra i team incaricati della sicurezza e della rete per le risposte agli eventi e/o le raccomandazioni relative a impostazioni e policy. Gli incidenti di sicurezza vengono automaticamente passati a una soluzione ITSM, e gli analisti scelgono da un catalogo di risposte, che può essere compilato automaticamente da una postazione centrale. Queste capacità diminuiscono i tempi di risposta da giorni a minuti e consentono al personale, numericamente limitato, di concentrarsi sul processo decisionale a livello di esperti anziché sul monitoraggio e sul routing delle informazioni.[12]



L’automazione dei processi di sicurezza non solo riduce il rischio di un’organizzazione diminuendo i tempi di risposta da giorni o settimane a minuti, ma può anche migliorare l’efficienza operativa.[13]

Conclusione: il rischio informatico definisce la nostra epoca

Un'azienda può avere miliardi di dollari di attrezzature presso diverse strutture nel mondo, disperse e ben protette fisicamente. Ma oggi, nell'era digitale, le operazioni globali possono essere paralizzate silenziosamente e in pochi minuti da un attacco informatico, mettendo a rischio la sicurezza dei dipendenti, i ricavi e le relazioni con i clienti, oltre che la fiducia nel marchio e la sua reputazione costruita in decenni di duro lavoro. Ad esempio, il malware NotPetya ha bloccato per giorni le operazioni di migliaia di aziende in tutto il mondo, tra cui una società di spedizioni globale e una società farmaceutica globale. Le perdite a livello mondiale sono state stimate in 10 miliardi di dollari.[14]

Di fronte a queste minacce avanzate, gli architetti della sicurezza devono valutare le modifiche da apportare all'architettura per poter rispondere agli incidenti e gestire gli eventi. Le organizzazioni operano con circa una probabilità su tre che si verifichi una violazione nei prossimi 24 mesi.[15] Ma il verificarsi di una violazione non deve necessariamente avere un impatto negativo. Come osserva un sottoscrittore di una compagnia assicurativa specializzata in rischi, "Una violazione di per sé non è un disastro, ma una cattiva gestione lo è."[16]

Ed è qui che un architetto della sicurezza può fare la differenza, riducendo al minimo il tempo necessario per il rilevamento di una violazione e la sua correzione. Un approccio alla sicurezza e alla gestione dei registri basato sull'analisi è un elemento chiave per raggiungere tale obiettivo. Può infatti stabilire la priorità dei rischi, velocizzare le indagini e fornire risposte più rapide in caso di violazione. In particolare, è fondamentale la capacità di unificare e correlare i dati provenienti da diverse soluzioni di sicurezza e automatizzare i flussi di lavoro per il ripristino.

In un anno in 65 paesi:[17]

2.216
violazioni di dati segnalate

53.000
incidenti di sicurezza informatica segnalati

Il costo medio di una violazione è di 3,86 milioni di dollari, ma le organizzazioni con una completa automazione della sicurezza possono ridurlo di 1,55 milioni di dollari.[18]

[1] Secondo dati interni di FortiGuard Labs.

[2] Kacy Zurkus, "Defense in depth: Stop spending, start consolidating," CSO, 14 marzo 2016.

[3] "Cybersecurity Skills Shortage Soars, Nearing 3 Million," (ISC)², 18 ottobre 2018.

[4] Greg Masters, "Crying wolf: Combatting cybersecurity alert fatigue," SC Magazine, 9 giugno 2017.

[5] Ibid.

[6] Jadzia Pierce, "Privacy and Cybersecurity: A Global Year-End Review," Inside Privacy, 21 dicembre 2018.

[7] Juliette Rizkallah, "The Cybersecurity Regulatory Crackdown," Forbes, 25 agosto 2017.

[8] Mary K. Pratt, "State data privacy laws, regulations changing CISO priorities," TechTarget, aprile 2019.

[9] "Proactive, Actionable Risk Management with the Fortinet Security Rating Service," Fortinet, 5 aprile 2019.

[10] "Bridging the NOC-SOC Divide: Understanding the Key Architectural Requirements for Integration," Fortinet, 23 agosto 2018.

[11] Mukul Pareek, "Standardized Scoring for Security and Risk Metrics," ISACA Journal, 2017.

[12] "Purpose-built Integrated NOC-SOC Management and Analytics," 11 settembre 2018.

[13] Marina Martin, "How Inefficiency Negatively Impacts Your Business," Dummies.com, consultato il 21 giugno 2019.

[14] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," WIRED, 22 agosto 2018.

[15] "2018 Cost of a Data Breach Study," Ponemon Institute, consultato il 18 ottobre 2018.

[16] "Phrases to help us think about cyberattacks…" The Cyber Rescue Alliance, consultato il 25 aprile 2019.

[17] Gil Press, "60 Cybersecurity Predictions For 2019," Forbes, 3 dicembre 2018.

[18] "2018 Cost of a Data Breach Study," Ponemon Institute, consultato il 18 ottobre 2018.

www.fortinet.com

402438-0-0-IT

novembre 19, 2020 12:11 PM

eb-cybersecurity-architect-fortianalyzer_IT