NetEye

SYSTEM MANAGEMENT E MONITORAGGIO IN AMBIENTI CLOUD

Rilevare gli attacchi alla rete in ambienti ibridi

PATRICK ZAMBELLI, NetEye Product Manager in Würth Phoenix

System Management e monitoraggio in ambiente Cloud

Rilevare gli attacchi alla rete in ambiente Cloud

Cloud, IOT e mobilità stanno cambiando radicalmente il modo in cui i clienti e le reti aziendali devono essere protetti. I precedenti approcci di sicurezza non sono più sufficienti a garantire l'integrità dei dati. Un monitoraggio dei flussi di dati nella rete è indispensabile per un rilevamento tempestivo. Questo perché gli attacchi di qualsiasi tipo lasciano tracce nel traffico di rete che possono essere rilevate e rintracciate con opportuni approcci di monitoraggio. L'intelligenza artificiale, in particolare, fornirà agli amministratori un importante aiuto.

La trasformazione digitale sta creando una nuova economia. E allo stesso tempo è anche una sfida importante per i reparti che si occupano di sicurezza informativa all'interno delle aziende. I processi, i prodotti e i servizi digitali devono prima di tutto essere sicuri. Si tratta di proteggere i dati di cui l'azienda ha bisogno per poter vendere i propri prodotti e servizi. La sicurezza informatica diventa quindi la sicurezza dei dati. Da qualche tempo l'attenzione si è spostata verso nuovi orizzonti per proteggere i dati e i sistemi che li raccolgono. I client sono infatti il bersaglio preferito per attacchi cibernetici di ogni tipo: sono molto più difficili da proteggere rispetto ai server a causa del gran numero di applicazioni installate e sono molto più frammentari con sistemi operativi quali Windows, Apple, Android e altri di nicchia.

Patrick Zambelli
NetEye Product Manager in Würth Phoenix

NetEye
WÜRTHPHOENIX

Würth Phoenix S.r.l.
Via Kravogl, 4
39100 Bolzano
Italia

+39 0471 56 41 11

info@wuerth-phoenix.com
www.wuerth-phoenix.com/neteye

25 miliardi di dispositivi IoT entro il 2021

L'elevata complessità ed eterogeneità del mondo degli endpoint è spesso ulteriormente rafforzata dall'Internet of Things (IoT) e dalla comunicazione machine-to-machine (M2M): secondo i ricercatori di mercato di Gartner, entro il 2021 circa 25 miliardi di dispositivi IoT saranno in uso in tutto il mondo. E sono principalmente client che devono essere gestiti come parte della sicurezza degli endpoint. Un sondaggio condotto da Gartner nel 2020 mostra quanto ciò sia necessario: secondo il sondaggio, negli ultimi tre anni quasi il 20 per cento delle imprese è già stato vittima di un attacco agli IoT.

Eterogeneità come sfida principale

Questa eterogeneità è una sfida per garantire la sicurezza degli endpoint. Lo scopo delle soluzioni di monitoraggio è quindi quello di limitare i client e gli altri dispositivi attivi nella rete in modo tale che non possano causare danni. Ma per gestire l'accesso, le politiche e la protezione da malware in tutte le reti, i servizi, gli endpoint e le soluzioni stesse devono essere estremamente ampie e complesse. Ed è chiaro che oggi i responsabili della sicurezza non si fidano delle soluzioni di controllo degli endpoint per fornire una protezione completa: un sondaggio condotto da circa 600 esperti di sicurezza dal provider americano Minerva Labs ha mostrato che tre quarti degli intervistati ritengono che la loro strategia di monitoraggio possa difendere solo il 70% degli attacchi malware.
Per ridurre un po' la complessità del controllo degli endpoint, spostare l'attenzione aiuta. Invece di concentrarsi strettamente sul punto finale da proteggere, la comunicazione degli endpoint sulla rete dovrebbe essere esaminata più attentamente. Dopo tutto, ogni attacco, ogni falla e persino ogni errore umano lascia tracce nel traffico dati. La parola chiave è "rilevamento di anomalie": qualsiasi attività in una rete che non segue gli

NetEye
WÜRTHPHOENIX

Würth Phoenix S.r.l.
Via Kravogl, 4
39100 Bolzano
Italia

+39 0471 56 41 11

info@wuerth-phoenix.com
www.wuerth-phoenix.com/neteye

schemi abituali si rivela un'anomalia. E questo può essere sempre rilevato tramite il monitoraggio della rete. Un'anomalia tipica può essere, ad esempio, quella che un utente effettua il login alle tre del mattino e non inizia a lavorare prima delle otto. O picchi improvvisi nel traffico dati di un client.

Il punto di vista dell'utente

Il rilevamento di anomalie provenienti da un client può essere effettuato tramite i consueti strumenti di System Management. Il punto di vista dell'utente gioca un ruolo importante in questo contesto. Quando il monitoraggio avviene su client - è chiamato Real User Experience (RUE) - le latenze o altre metriche vengono misurate proprio lato client. Di solito questo viene fatto simulando azioni tipiche dell'utente, come ad esempio una richiesta sui sistemi gestionali come SAP. Il monitoraggio della rete è una parte essenziale. In questo contesto sono disponibili sul mercato diversi strumenti per la misurazione delle prestazioni lato client, come il progetto open source Alyvix, attivamente supportato da Würth Phoenix. Con questo approccio, i dati sul comportamento del client vengono raccolti e valutati in un sistema di monitoraggio centrale. Il monitoraggio lato del client ha anche il vantaggio che il traffico sospetto può essere facilmente assegnato a un endpoint. Uno strumento di monitoraggio della rete viene invece utilizzato per monitorare il traffico di dati dal client ai server e ad altri componenti. Qui lo strumento open source ntopng ha dato prova ad esempio nella difesa contro gli attacchi di ransomware: in modalità passiva, l'amministratore riceve un avviso se un endpoint tenta di accedere a host sospetti o bloccati. Le liste nere sono state aggiornate automaticamente su ntopgn per diversi mesi. In modalità online, ntopng può forzare l'uso di server DNS definiti per bloccare l'accesso del client a fonti sospette anche in questo modo. Tutti gli strumenti di monitoraggio della rete offrono le stesse o simili possibilità di analizzare il traffico e di bloccarlo se necessario.

NetEye
WÜRTHPHOENIX

Würth Phoenix S.r.l.
Via Kravogl, 4
39100 Bolzano
Italia

+39 0471 56 41 11

info@wuerth-phoenix.com
www.wuerth-phoenix.com/neteye

Real User Experience

Il monitoraggio della rete e la RUE forniscono un quadro completo di ciò che i client eseguono in rete. Analizzando il traffico di rete, è possibile prevenire molte azioni potenzialmente dannose degli endpoint senza richiedere l'accesso diretto al dispositivo finale. Il grande vantaggio di questo approccio senza agenti è che il sistema operativo e le prestazioni hardware del client sono irrilevanti. Ciò significa che è possibile controllare endpoint sconosciuti che altrimenti non sarebbero rilevabili nel monitoraggio. Inoltre, questo metodo funziona anche per i client per i quali non esiste una soluzione di sicurezza convenzionale. Ciò è particolarmente importante per le aziende che pianificano e realizzano ampie attività di IoT. Questo perché molti dei sensori e degli attuatori non consentono l'installazione di ulteriori soluzioni di sicurezza e le risorse hardware non sono dimensionate per questo.

Endpoint security

Tuttavia, gli strumenti a sé stanti hanno un'utilità limitata per il rilevamento delle anomalie. Questo perché, oltre al puro monitoraggio delle metriche, deve esserci anche un'istanza che aggreghi e analizzi questi dati e fornisca agli amministratori gli opportuni avvertimenti. Inoltre, le norme come la ISO 27001, stabiliscono che i file di registro devono essere analizzati per gli eventi rilevanti per la sicurezza e che la gestione dell'inventario debba essere gestito. Ciò significa che una gestione completa del sistema IT è in realtà indispensabile anche per la sicurezza degli endpoint. Una soluzione per la gestione centrale dovrebbe essere disponibile in ogni azienda. Con IoT e il cloud, tuttavia, si devono porre nuovi requisiti anche alle soluzioni di monitoraggio. In termini di endpoint sicuri, è necessario monitorare sia i servizi cloud che i dispositivi IoT in modo consolidato e non permettere lo sviluppo di un silo tecnologico. Questo perché il monitoraggio con il minor

NetEye
WÜRTHPHOENIX

Würth Phoenix S.r.l.
Via Kravogl, 4
39100 Bolzano
Italia

+39 0471 56 41 11

info@wuerth-phoenix.com
www.wuerth-phoenix.com/neteye

numero possibile di falsi positivi e, peggio ancora, di falsi negativi richiede che tutti i sistemi e i componenti siano riuniti il più possibile durante il monitoraggio. Solo in questo modo è possibile ottenere informazioni significative.

Con l'Intelligenza artificiale per una maggiore sicurezza

Con la crescente diffusione dell'intelligenza artificiale, anche il rilevamento di anomalie nel traffico dati migliorerà notevolmente. Il rilevamento delle anomalie come riconoscimento di pattern può già essere automatizzato abbastanza bene in combinazione con il machine learning. Si cerca di mappare funzionalmente l'ingresso X dato in base al valore Y, cioè Y=f(X). Così, il rilevamento di anomalie nella rete si presta al machine learning.
L' intelligenza artificiale tenta di rilevare i pattern dagli andamenti del traffico di rete e ne deriva la funzione di mappatura. L'obiettivo è trovare la funzione che produce il minor numero di falsi positivi o falsi negativi. Il machine learning è già stato implementato in diverse aziende e le prime soluzioni di questo genere come NetEye di Würth Phoenix sono già state collaudate.

Conclusione

Oggi è estremamente importante stabilire la sicurezza degli endpoint direttamente sul client stesso per proteggere i dati e le informazioni da un uso improprio. Ma questo approccio sta raggiungendo sempre più i suoi limiti. La crescente eterogeneità contribuisce a far sì che a medio termine una parte considerevole di tutti gli endpoint non possa più essere controllata in modo efficace. Concentrandosi sul traffico dati in rete, è possibile introdurre un ulteriore livello di sicurezza. I dati, che vengono consolidati a livello centrale nel monitoraggio, forniscono un quadro significativo della sicurezza anche lato client. Inoltre, tecniche di machine learning stano facendo rapidi progressi in questo settore, consentendoci di reagire ancora più rapidamente - idealmente anche in modo predittivo - alle minacce degli endpoint.

NetEye
WÜRTHPHOENIX

Würth Phoenix S.r.l.
Via Kravogl, 4
39100 Bolzano
Italia

+39 0471 56 41 11

info@wuerth-phoenix.com
www.wuerth-phoenix.com/neteye