Red Hat

Gettare le basi della sicurezza con automazione e approccio Zero Trust

Come adottare un approccio Zero Trust

Sommario

Introduzione

Come l'attività di un'organizzazione non si ferma dopo l'orario di chiusura, così anche quella di criminali informatici e di altri utenti malintenzionati, sempre alla ricerca dell'occasione giusta per sottrarre dati o causare danni alle aziende, ai partner o ai clienti.

Oggi il numero di minacce alla sicurezza informatica è talmente elevato che i team operativi, di sicurezza e IT devono essere sempre in uno stato di massima allerta. Queste minacce interessano tutte le aziende a prescindere dalla dimensione e possono arrivare a costare miliardi di dollari. Secondo un report di IBM il costo medio per una violazione dei dati causata da un attacco informatico è in aumento. Ha infatti raggiunto i 4,24 milioni di USD nel 2021, contro i 3,86 milioni di USD del 2020.[1]

Le minacce non provengono solo da elementi esterni all'organizzazione. Il "2021 Data Breach Investigations Report" di Verizon ha mostrato infatti che il 30% delle violazioni coinvolgeva l'accesso da parte di dipendenti a sistemi che non rientravano nel loro ruolo e grado di autorizzazione.[2]

L'aumento del numero e della gravità degli attacchi è dovuto a diversi fattori, tra cui i rapidi cambiamenti dell'infrastruttura di rete, la migrazione verso soluzioni basate sul cloud e la proliferazione di modelli di lavoro da remoto o di smart working a partire dal 2020.

L'evoluzione dell'ambiente di lavoro, con dipendenti che accedono ai sistemi sensibili da dispositivi aziendali ma anche da dispositivi personali e che per farlo si servono di reti internet pubbliche o domestiche, ha ampliato le superfici di attacco. Inoltre, il fatto che sempre più persone lavorino con colleghi che non hanno mai incontrato di persona ha favorito la diffusione e l'affinamento degli attacchi di phishing e spear phishing.

La migrazione verso soluzioni basate sul cloud offre moltissimi vantaggi, dal risparmio sui costi alla riduzione drastica dello storage fisico necessario per i documenti. Ma questi vantaggi si accompagnano anche a tutta una serie di costi per la gestione della sicurezza di utenti, applicazioni e infrastruttura per centinaia di migliaia di utenti distribuiti tra i sistemi on premise esistenti e quelli basati sul cloud.

La combinazione di lavoro da remoto e migrazione al cloud hanno reso obsoleto il tradizionale approccio alla sicurezza basato su ambienti controllati e VPN. Oltre al fatto che i dipendenti si connettono con più dispositivi a più sistemi, anche l'avvento dell'IoT e dell'edge computing ha creato nuovi potenziali vettori di attacco per i criminali informatici.

Inoltre, le organizzazioni hanno moltiplicato i team che si occupano della gestione dei diversi sistemi di sicurezza e reti. I team InfoSec, SysOps, NetOps e altri lavorano simultaneamente, e spesso in autonomia gli uni dagli altri, per applicare i criteri di sicurezza e rispondere alle minacce. Purtroppo, il fatto che molto spesso questi team operino separatamente, utilizzino sistemi diversi e non condividano processi comuni mina la loro capacità di rispondere in maniera coordinata alle minacce. E quando si tratta di minacce alla sicurezza, il tempo è tutto.

1 "Cost of a data breach report 2021", IBM, consultato il 16 giugno 2022.
2 "2022 Data Breach Investigations Report", Verizon, consultato il 16 giugno 2022.

Vuoi saperne di più sull'approccio Zero Trust? Continua a leggere.

Conosci già l'architettura Zero Trust ma vuoi scoprire come automatizzarla? Vai alla sezione **La scalabilità dell'architettura Zero Trust con l'automazione**.

Un altro problema che espone le organizzazioni al rischio di attacchi informatici è la mancanza di integrazione tra le soluzioni che permettono il funzionamento dell'infrastruttura e quelle di sicurezza. E una comunicazione poco efficiente fra i team che gestiscono questi due tipi di soluzioni si ripercuote sulla capacità di risolvere gli incidenti di sicurezza, che sarà più lenta e poco puntuale.

I rischi per la sicurezza informatica sono aspetti che non si possono più trascurare. Infatti, le organizzazioni e i fornitori si sono adattati per conformarsi a normative quali il California Consumer Privacy Act (CCPA) e il Regolamento generale sulla protezione dei dati (GDPR). Nel 2021 il governo degli Stati Uniti ha riconosciuto l'aumento delle minacce alla sicurezza informatica con l'introduzione dell'Executive Order on Improving the Nation's Cybersecurity.

Per affrontare queste minacce occorre adottare un approccio orientato alla sicurezza per ciò che concerne le policy, le reti e le applicazioni. Molte organizzazioni sembrano vedere nell'approccio Zero Trust la soluzione, compreso il governo federale degli Stati Uniti che prevede di implementare un'architettura Zero Trust per le sue reti.

Ma l'adozione di un'architettura Zero Trust non è che l'inizio, soprattutto quando si parla di organizzazioni di grandi dimensioni con diverse sedi e un insieme di sistemi on premise, cloud ed edge. Per la scalabilità dell'architettura Zero Trust, occorre disporre di un livello di automazione adeguato ai contesti enterprise. In questo ebook scoprirai perché Red Hat® Ansible® Automation Platform è la soluzione giusta per la tua organizzazione.

L'approccio Zero Trust è la soluzione?

Gli approcci alla sicurezza tradizionali erano progettati per sistemi a cui i dipendenti accedevano da un luogo fisico. Con l'evoluzione delle opzioni di accesso a distanza, ovvero la transizione da connessioni remote a connessioni ad alta velocità sempre attive, la regolazione degli accessi dall'esterno è passata alle reti private virtuali (VPN). Ma se è vero che le reti VPN forniscono un'autenticazione sicura, è anche vero che espongono le risorse e i sistemi a più utenti di quanti avrebbero effettivamente bisogno di accedervi, e questo crea potenziali rischi per la sicurezza.

Oggi le classiche autorizzazioni basate sull'utente e le reti VPN non sono più in grado di fornire un livello di sicurezza adeguato per le complicatissime architetture di soluzioni on premise, cloud e ibride da cui dipendono le organizzazioni moderne. Occorreva un nuovo modello che ripensasse in toto l'approccio alla sicurezza. Questo nuovo approccio ha preso il nome di architettura Zero Trust.

Riconosciuto come modello per la sicurezza nel 2010, l'approccio Zero Trust parte dal presupposto che gli attacchi possono venire sia dall'esterno che dall'interno della rete. In base a questo principio, nel modello Zero Trust ogni interazione viene considerata non affidabile di default.

Invece di autorizzare l'accesso solo in base a posizione, ruolo o utente, nel framework Zero Trust è necessaria la verifica dell'utente, del dispositivo e dell'applicazione perché l'interazione si possa considerare affidabile. L'adozione di un'architettura Zero Trust richiede un approccio completamente nuovo alla sicurezza dove gli architetti di sistema sono chiamati ad autenticare utenti o dispositivi ad ogni transazione e ad autorizzare solo l'accesso ai dati e ai sistemi strettamente necessari in base al concetto di privilegio minimo.

Autenticare ogni transazione

Il principio cardine dell'architettura Zero Trust è trattare ogni interazione, proveniente dall'interno o dall'esterno della rete, come una potenziale minaccia. Questo significa che prima di poter procedere con l'interazione, occorre autenticare i suoi componenti. Ciascuna architettura Zero Trust richiederà la convalida di specifici componenti, ma quelli di base sono:

- **Utente.** Convalidare che l'utente che sta tentando l'accesso a una rete, applicazione o sistema basato sul cloud disponga del livello di autorizzazione adeguato.
- **Applicazione.** Verificare che l'utente disponga del livello di autorizzazione adeguato per accedere ai dati e all'applicazione.
- **Dispositivo.** Confermare che l'utente che sta tentando l'accesso a una risorse utilizzi un dispositivo autorizzato ad accedere alla rete e all'applicazione.
- **Stato.** Controllare che il dispositivo utilizzato disponga degli aggiornamenti, delle patch e della crittografia necessari per accedere in tutta sicurezza alla rete e all'applicazione.

L'approccio Zero Trust sta prendendo piede anche nel settore pubblico, ad esempio il governo federale degli Stati Uniti prevede di implementarlo per le sue reti. Come illustrato nell'Executive Order on Improving the Nation's Cybersecurity del 2021, il governo degli Stati Uniti intende intraprendere diverse iniziative che vanno dall'adozione di soluzioni basate sul cloud all'introduzione di un'architettura Zero Trust per tutta l'infrastruttura governativa.

Se le agenzie governative eseguono l'upgrade dell'infrastruttura e dei livelli di sicurezza verso un modello Zero Trust, anche i loro fornitori dovranno giocoforza conformarsi ai nuovi standard.

Ostacoli all'adozione dell'architettura Zero Trust

Con l'aumento delle minacce e dei vettori di attacco, adottare un'architettura Zero Trust in tutta l'organizzazione è ormai indispensabile. Ma, nonostante i numerosi vantaggi di questo approccio rispetto alla sicurezza tradizionale, l'implementazione di un modello Zero Trust in un'infrastruttura esistente può presentare alcune difficoltà.

In primo luogo, l'infrastruttura esistente è in genere una commistione di soluzioni di più provider. Per quanto la maggior parte dei fornitori si impegni ad adottare i principi dell'architettura Zero Trust, non tutti i sistemi garantiscono l'interoperabilità con i sistemi di altri fornitori. I problemi di interoperabilità rischiano di ostacolare non solo il lavoro dei team interni (SysOps, NetOps, ecc.), che si trovano in difficoltà se le soluzioni non operano in sinergia, ma possono addirittura arrivare a compromettere il rilevamento della minacce.

In secondo luogo, l'approccio Zero Trust richiede un cambiamento radicale nel modo in cui i dirigenti considerano e trattano la sicurezza. Passare da un approccio "castle-and-moat" (a fortezza) ad uno "deny-by-default" (blocca di default) significa che i dirigenti devono lavorare per far sì che tutta l'organizzazione si adegui ai principi e alle procedure dell'architettura Zero Trust anche se sembrano rallentare il lavoro. Senza l'impegno di tutta l'azienda, si rischia di tornare ben presto a pratiche obsolete o addirittura di creare uno "shadow IT" che elude i processi, le policy e l'architettura Zero Trust.

Come creare una base solida per la sicurezza con l'architettura Zero Trust

Gli approcci alla sicurezza tradizionali come le VPN con token fisici o digitali erano progettati per offrire percorsi sicuri per l'accesso da remoto a una rete on premise. Definito anche modello di sicurezza della rete "castle-and-moat", questo approccio si concentrava unicamente sul creare un punto di accesso a tutte le risorse dall'altra parte.

Nella sicurezza fisica, questo tipo di soluzione corrisponderebbe all'utilizzo di una chiave elettronica per accedere a un edificio o ad aree riservate dell'edificio. L'organizzazione potrebbe avere l'impressione di garantire la sicurezza fisica autorizzando l'accesso dei dipendenti all'edificio o a specifici settori dell'edificio tramite sistemi di sicurezza basata sui ruoli. Ma questo tipo di sicurezza fisica è facilmente raggirabile con semplici escamotage di ingegneria sociale: ad esempio un utente malintenzionato potrebbe fingersi un fattorino e ottenere l'autorizzazione ad accedere all'edificio dagli addetti alla sicurezza.

L'approccio Zero Trust deve essere alla base di tutto

L'approccio Zero Trust parte dal presupposto che la sicurezza debba diventare un elemento fondamentale di qualunque progetto aziendale, dallo sviluppo di un nuovo prodotto all'implementazione di una nuova infrastruttura. Invece di creare un modello di sicurezza focalizzato sull'accesso alla rete, l'architettura Zero Trust applica le procedure di sicurezza ad ogni interazione che avviene in azienda.

Come adottare un'architettura Zero Trust

Per adottare un'architettura Zero Trust non si parte dalla scelta dei fornitori o delle piattaforme di sicurezza. Il primo passo consiste nel porsi una domanda all'apparenza molto semplice ma che ha conseguenze enormi per la scelta della strategia da utilizzare: che tipo di dati, applicazioni o sistemi sto cercando di proteggere?

- **Costruisci un inventario.**Stabilire il tipo di risorse da proteggere dà modo alle organizzazioni di avere una base di riferimento per la creazione di regole e policy per l'implementazione del modello Zero Trust da applicare a rete, utenti, applicazioni e carichi di lavoro. Grazie a questa base di riferimento, i team SysOps, NetOps e InfoSec possono rendersi conto di quali strumenti di analisi saranno necessari per rilevare, identificare e rispondere agli incidenti di sicurezza.
- **Stabilisci processi e policy.** Una volta stabilito il tipo di risorse da proteggere, i team interni possono collaborare alla creazione di processi e policy Zero Trust che permettano ai dipendenti di lavorare in tutta sicurezza.
- **Testa. Adatta. Distribuisci.** Non sempre le idee teoricamente perfette si rivelano tali una volta implementate. Analizzando i processi e le policy in azione, i team di sicurezza, di rete e operativi possono rendersi conto dei problemi e apportare le dovute correzioni per garantire il funzionamento ottimale dell'architettura Zero Trust.

Stabilire il tipo di risorse da proteggere è il primo passo necessario per la scalabilità dell'architettura Zero Trust con l'automazione.

La scalabilità dell'architettura Zero Trust con l'automazione

Scopri di più sull'automazione della sicurezza con Ansible e a che punto sei nel tuo percorso di automazione della sicurezza in questo webinar.

L'architettura Zero Trust richiede che le risorse, inclusi dispositivi, dati e applicazioni, siano protette allo stesso modo ovunque. Ad esempio, se si trasferisce un carico di lavoro da un datacenter on premise a un cloud pubblico o privato, l'approccio Zero Trust richiede che vengano applicate le stesse regole di gestione della sicurezza. Con un'architettura Zero Trust le regole sono slegate dal carico di lavoro così che il codice non cambi.

Nelle organizzazioni di grandi dimensioni o in quelle in rapida crescita, l'introduzione di pratiche di automazione può semplificare l'applicazione di policy, regole e processi su larga scala via via che si aggiungono nuovi strumenti o infrastrutture. Prima parlare di Red Hat® Ansible® Automation Platform, riportiamo di seguito i cinque vantaggi dell'automazione delle architetture Zero Trust.

I vantaggi dell'automazione

- **Sapere di essere protetti.** Stabilire il tipo di risorse da proteggere è un passaggio fondamentale per l'estensione dell'architettura Zero Trust a tutti i dispositivi, le reti e le applicazioni aziendali. L'automazione aiuta le aziende a tenere traccia e registrare le risorse distribuite in diverse ubicazioni e nel cloud.
- **Conformità continua.** L'uso di bot o di altri strumenti di automazione da parte dei criminali informatici ha reso necessaria l'adozione di sistemi di sicurezza che monitorino costantemente l'ambiente alla ricerca di potenziali minacce. L'automazione dell'architettura Zero Trust assicura che le policy vengano applicate sempre, 24 ore su 24, 365 giorni l'anno.
- **Riduzione dei rischi.** I team InfoSec possono adottare le policy e le regole ma mano che si verificano gli incidenti di sicurezza. Questi processi si possono codificare come flussi di lavoro ed eseguire in maniera automatizzata, il che riduce il rischio di commettere errori durante l'implementazione.
- **Maggiore reattività.** Maggiore è il tempo impiegato per risolvere un rischio per la sicurezza, maggiore sarà la possibilità che si verifichino violazioni o attacchi informatici. Automatizzare l'architettura Zero Trust permette di reagire tempestivamente, che l'azienda conti 1000 o 100.000 utenti, creando azioni automatizzare che si possono eseguire on demand o tramite l'automazione guidata dagli eventi.
- **Prototipazione rapida.** L'automazione consente di creare prototipi, testarli e implementare i cambiamenti al framework di sicurezza, a prescindere dal livello di complessità del framework.

L'automazione dell'architettura Zero Trust va oltre la sicurezza

Estendere l'approccio Zero Trust oltre la rete e la sicurezza permette alle organizzazioni di mettere davvero la sicurezza al centro di ogni progetto e sistema. L'automazione di questi processi aumenta ancora di più il valore dell'approccio Zero Trust perché garantisce l'applicazione e la verifica di processi e policy e riduce così il rischio di attacchi informatici o altre violazioni.

Conformità e sicurezza coerenti

L'automazione agevola l'applicazione delle regole di sicurezza e conformità perché permette di gestire le configurazioni, il deployment delle applicazioni e controlli di conformità che alimentano i processi di sviluppo. Le organizzazioni possono automatizzare attività quali il provisioning, la configurazione, il deployment delle applicazioni, ecc.

L'automazione non serve solo per la protezione di applicazioni e componenti. Si può anche utilizzare per le attività di manutenzione dei componenti e per svolgere regolari controlli e verifiche di conformità. L'applicazione continua ed end to end della sicurezza è indispensabile per il ciclo di vita di integrazione e deployment continui (CI/CD) dell'azienda.

Sicurezza dei software olistica

I principi Zero Trust si possono applicare anche ai software e ai sistemi di un'organizzazione. Spesso i diversi team e reparti hanno bisogno di utilizzare applicazioni, hardware e soluzioni che non offrono l'interoperabilità integrata. L'automazione agevola l'integrazione tra i sistemi di fornitori diversi perché permette la creazione di flussi di lavoro automatizzati con cui orchestrare l'interoperabilità in maniera efficiente e sicura.

Le soluzioni principali di un'azienda, che siano sviluppate internamente o da terze parti, possono contenere componenti open source, che se non vengono monitorati potrebbero rappresentare un vettore di attacco per i criminali informatici. Gli stessi processi di automazione sviluppati per la gestione dell'interoperabilità si possono utilizzare per garantire che le applicazioni siano sempre in uno stato di sicurezza ottimale.

Automazione della conformità

L'automazione è utile anche per ridurre l'errore umano in tutte quelle attività relative alla conformità. Pensiamo ad esempio a un'organizzazione che si occupi di processare le transazioni con carta di credito. Sono necessari numerosi processi e controlli hardware e software per verificare la conformità agli standard PCI DSS (Payment Card Industry Data Security Standard). Oltre al fatto che per questi controlli occorre che i diversi sistemi forniscano rapidamente dati accurati. Invece di avere un dipendente o un team che monitora manualmente i processi, si può sfruttare l'automazione. In questo modo si riduce l'errore umano e si liberano i team che potranno dedicarsi a progetti strategici.

L'automazione dell'architettura Zero Trust con Red Hat Ansible Automation Platform

Per saperne di più sui vantaggi dell'automazione, leggi Red Hat Ansible Automation Platform: guida introduttiva.

Perché un'architettura Zero Trust operi al meglio occorre che l'organizzazione disponga di una visibilità chiara su tutte le transazioni che avvengono nei suoi ambienti. Red Hat Ansible Automation Platform offre funzionalità che agevolano l'adozione dell'approccio Zero Trust e altre funzionalità di automazione. La piattaforma garantisce un ROI rapido perché riduce gli ostacoli all'introduzione di processi automatizzati in tutti i settori aziendali, sicurezza, rete, applicazioni, cloud ed edge computing.

Zero Trust	**Automazione dell'architettura Zero Trust con Red Hat Ansible Automation Platform**
Il modello Zero Trust si basa sull'approccio "deny-by-default".	Red Hat Ansible Automation Platform permette agli amministratori di controllare gli accessi assegnando agli utenti autorizzazioni, privilegi e ruoli. Inoltre, consente di automatizzare la crittografia (crittografia mTLS, audit trail, e controlli dell'inventario).
Il modello Zero Trust sfrutta le policy di autorizzazione per limitare l'accesso ad applicazioni e risorse.	Red Hat Insights for Ansible Automation Platform aiuta le organizzazioni a monitorare e identificare potenziali criticità e rischi che richiedono l'attenzione dei team SysOps o NetOps.
Il modello Zero Trust garantisce che le risorse dispongano delle ultime patch prima di autorizzare l'accesso.	Red Hat Ansible Automation Platform garantisce che tutte le risorse applicative di tutta l'infrastruttura aziendale dispongano degli ultimi aggiornamenti e patch di sicurezza.

Red Hat Ansible Automation Platform è il tessuto connettivo che centralizza su un'unica piattaforma le diverse tecnologie aziendali che altrimenti risulterebbero disorganiche e sconnesse tra loro. La piattaforma mette a disposizione oltre 100 Red Hat Certified Content Collections, che dispongono del supporto di Red Hat e dei suoi partner e permettono di automatizzare in maniera facile e veloce tutti i componenti dell'infrastruttura, siano essi on premise, cloud o ibridi.

Inizia il tuo percorso di automazione dell'architettura Zero Trust

Red Hat Consulting può aiutare le aziende nel percorso di adozione dell'automazione e dell'approccio Zero Trust. Esegui una breve autovalutazione o contatta il team di Red Hat Consulting.

Scopri di più sull'automazione dell'IT e comincia la prova gratuita.

Informazioni su Red Hat

Red Hat è leader mondiale nella fornitura di soluzioni software open source. Con un approccio che si avvale della collaborazione delle community, distribuisce tecnologie come Kubernetes, container, Linux e cloud ibrido caratterizzate da affidabilità e prestazioni elevate. Red Hat consente di sviluppare applicazioni cloud native, integrare applicazioni IT nuove ed esistenti, e automatizzare e gestire ambienti complessi. Considerata un partner affidabile dalle aziende della classifica Fortune 500, Red Hat fornisce pluripremiati servizi di consulenza, formazione e assistenza, che portano i vantaggi dell'innovazione open source in qualsiasi settore. Red Hat è l'elemento catalizzatore in una rete globale di aziende, partner e community, e permette alle organizzazioni di crescere, evolversi e prepararsi a un futuro digitale.

ITALIA
it.redhat.com
italy@redhat.com

EUROPA, MEDIO ORIENTE, E AFRICA (EMEA)
00800 7334 2835
it.redhat.com
europe@redhat.com

facebook.com/RedHatItaly
twitter.com/RedHatItaly
linkedin.com/company/red-hat

it.redhat.com
F32053