Come adottare lo Zero Trust Identity secondo Saviynt



Le organizzazioni aziendali, di diverse dimensioni, si stanno confrontando in merito al concetto di Zero Trust. I team di sicurezza vedono questo approccio come un catalizzatore per cambiare radicalmente il modo in cui implementare la sicurezza. I CISO la vedono come una soluzione efficace a livello aziendale per guidare il processo decisionale ai massimi livelli di leadership.

Zero Trust non è solamente una tecnologia che può essere acquistata. Per abbracciare completamente questo nuovo "mantra", occorre ridefinire l'intero approccio all'identità e alla sicurezza per proteggere il personale, l'infrastruttura IT e le risorse sensibili. Lo Zero Trust è il passaggio dalla fiducia implicita a una rivalutazione continua del rischio. Per questo motivo le organizzazioni devono comprendere che questo nuovo paradigma è guidato dall'identità e richiede uno spostamento dell'attenzione dal livello di sicurezza della rete al livello di identità. Questo approccio ha tre pilastri fondamentali:

1. Un cambio di mentalità
2. Un approccio strategico e non limitato alla soluzione puntuale
3. Una nuova architettura basata sull'identità

L'ascesa dello Zero Trust

La digital transformation ha portato molte aziende a migrare al cloud per sfruttare i suoi vantaggi di scalabilità, efficienza e riduzione dei costi. Nonostante i numerosi aspetti positivi, questo cambiamento ha ampliato il tradizionale perimetro di lavoro e il relativo panorama delle

minacce.

Nel 2020 gli attacchi esterni agli account cloud sono aumentati del 630% mentre quelli interni all'azienda rappresentano oltre il 30% di tutte le violazioni. Questi dati dimostrano chiaramente come un approccio basato sulla tradizionale fiducia possa risultare estremamente pericoloso anche verso i dipendenti più fidati. Oggi, non è più sufficiente proteggere unicamente il tradizionale perimetro di rete aziendale ma è necessario delineare un'area attraverso l'implementazione di soluzioni di Identity. Questo nuovo modello di sicurezza consiste nel fornire il giusto accesso a persone e dispositivi IT, ottimizzando i controlli in base ai profili di rischio delle entità che accedono alle varie risorse.

Cosa si intende per Zero Trust Identity?

Ogni volta che si effettua un accesso, lo Zero Trust Identity prevede una verifica continua del rischio e dell'affidabilità dell'utente, attraverso informazioni contestuali sull'identità per informare e ottimizzare le policy di accesso. In aggiunta la soluzione deve supportare anche il principio del privilegio minimo e la concessione dell'accesso a specifiche identità, per le giuste motivazioni, in un periodo di tempo ben definito e limitatamente per lo svolgimento di una puntuale attività. Quindi le aziende come possono implementare la Zero Trust Identity? La risposta sta nella comprensione e nell'applicazione dei tre aspetti chiave dello Zero Trust: mentalità, strategia e architettura.

Lo Zero Trust è una mentalità

Nel nostro mondo digitale dominato da dati, cloud, dispositivi mobili e IoT, qualsiasi organizzazione è diventata un'azienda tecnologica. Realizzare e riconoscere questo richiede un cambiamento di mentalità. Occorre rapportarsi al mondo attraverso una lente diversa. Questo vale sia per le grandi

imprese globali che per le piccole imprese. È necessario accettare che la tecnologia è al centro di ogni attività. Indipendentemente dal fatto che le aziende ospitino il proprio hardware o si affidino a soluzioni SaaS, quasi tutte le funzioni aziendali principali, dalle risorse umane alla contabilità e alle vendite, si basano sulla tecnologia. Ecco perché sia le risorse organizzative che i dati sensibili esistono in ogni angolo dei sistemi IT. Queste risorse non solo devono essere messe in sicurezza, ma anche monitorate in modo aggressivo e attivamente protette.

Il cambio di paradigma dello Zero Trust Identity

Lo Zero Trust richiede l'abbandono delle convinzioni che limitano l'applicazione di security checks solo ad azioni provenienti dall'esterno, classificando di default come sicure le identità e le risorse interne. Il nuovo presupposto deve essere che ogni identità e richiesta di accesso sia sospetta e debba essere convalidata. Il passaggio a questa mentalità fa avanzare l'organizzazione da una posizione reattiva sulla sicurezza a una proattiva.

L'integrazione della formazione sulla sicurezza e il cambiamento di mentalità rappresentano i due pezzi del puzzle di un solido programma di sicurezza. Comprendendo che anche un dipendente ben intenzionato può esporre un'azienda alle minacce, la formazione sulla consapevolezza della sicurezza deve diventare una priorità. Prepararli a diventare una linea di difesa è fondamentale. Lo Zero Trust Identity aggiunge livelli di sicurezza, estendendosi oltre il semplice controllo degli accessi verso il monitoraggio e la gestione continua. È necessario che l'azienda riconosca che tutti gli accessi concessi comportano un certo livello di rischio. Per questo è indispensabile adottate pratiche per migliorare la capacità di valutare i diritti di accesso, il loro livello di rischio e assumere politiche di riparazione e ripristino. Questo livello

di preparazione è reso possibile dal monitoraggio continuo delle risorse e dall'utilizzo degli accessi. La visibilità approfondita, l'automazione e l'applicazione del machine learning (ML) accelerano le revisioni degli accessi e i tempi di risposta agli incidenti. Identificando rapidamente le risorse compromesse, le organizzazioni possono adottare misure proattive per bloccare l'accesso, restringere l'ambito di un attacco e ridurne l'impatto.

Zero Trust Identity come strategia

Il passaggio a una strategia Zero Trust richiede l'adozione dell'Identità come nuovo perimetro di sicurezza. Parte del motivo per cui Zero Trust è efficace è che non presuppone più che tutto ciò che si trova dietro il firewall sia sicuro. Al contrario, parte dal presupposto che si sia già verificato un certo livello di compromissione e che sia necessaria una verifica prima di concedere l'accesso. Uno dei miglioramenti chiave del passaggio a una strategia di Zero Trust Identity è l'accelerazione della trasformazione e dell'agilità del business. Le soluzioni di identità sono una delle componenti essenziali per raggiungere questi obiettivi, grazie alla loro efficacia, indipendentemente da dove si trovano le risorse o da dove si accede. Ciò consente alle organizzazioni di ridurre la dipendenza dalle applicazioni legacy precedenti e di riprogettare in modo sicuro gli ambienti IT utilizzando linguaggi e design più recenti che possono trarre vantaggio dal cloud computing. Questi cambiamenti fondamentali richiedono un investimento significativo nel programma di sicurezza, inclusa un'enfasi aggiuntiva sull'implementazione di soluzioni basate sull'identità. Velocità e agilità, tuttavia, sono solo una parte dell'equazione. Le aziende devono comunque garantire che i propri dati siano protetti e soddisfino i requisiti di conformità e governance organizzativa. Lo Zero Trust Identity è un importante fattore abilitante nella gestione dei privilegi minimi attraverso politiche di sicurezza dinamiche che consentono

l’autenticazione e l’autorizzazione appropriate per qualsiasi risorsa digitale, fattore fondamentale per le risorse privilegiate.

Zero Trust Identity come architettura

Zero Trust Identity è un componente essenziale di un’architettura che richiede la progettazione del modello di sicurezza a più livelli per affrontare le sfide di un ecosistema IT in continua espansione. Le organizzazioni sono passate all’utilizzo di applicazioni moderne che utilizzano microservizi e DevSecOps integrato per sfruttare tutti i vantaggi del cloud. E sebbene queste tecnologie contribuiscano all’accelerazione, sono intrinsecamente rischiose data la mancanza di visibilità e l’impossibilità di controllare l’accesso. Poiché risiedono al di fuori dei tradizionali confini dell’organizzazione, l’approccio alla sicurezza deve includere un’architettura che si adatti per affrontare questi rischi. Il refactoring dell’architettura su queste basi richiede una moderna soluzione di identità che protegga le risorse cloud, integrando contemporaneamente gli strumenti di sicurezza e conformità esistenti in tutto l’ecosistema IT. In questo modo, il processo di verifica per Zero Trust può tenere conto in modo efficace delle politiche nuove ed esistenti.

L’architettura Zero Trust Identity sfrutta visibilità, rischi e informazioni sulle minacce per guidare il processo decisionale. Un’altra componente essenziale, consente l’interoperabilità tra le soluzioni di sicurezza che scambiano informazioni. L’utilizzo di un approccio aperto e basato su standard consente alle tecnologie di sicurezza di scambiare informazioni sui rischi, quasi in tempo reale per migliorare la visibilità. Con una maggiore visibilità, le organizzazioni ottengono valutazioni dinamiche e accurate del proprio ambiente spostando i controlli di accesso più vicini agli endpoint e ai dati effettivi. Dati di valutazione più accurati e tempestivi consentono un processo decisionale migliore e più

rapido.

Come intraprendere questo nuovo viaggio

L’utilizzo dell’identità per guidare l’approccio Zero Trust è più della semplice tendenza alla sicurezza informatica del momento. Aiuta l’azienda a evolvere la propria posizione di sicurezza e conformità in risposta sia al panorama delle minacce in evoluzione che alla sua crescita. Il viaggio verso lo Zero Trust richiede un cambiamento di mentalità organizzativa e il passaggio da soluzioni puntuali e circoscritte ad una strategia di sicurezza coerente. Questa strategia deve essere progettata con l’identità come fondamento per integrare tutti i livelli in tutto l’ecosistema.

L’approccio Zero Trust non è una destinazione. È un viaggio.

Per ulteriori informazioni consultare www.saviynt.com

A cura di **Alberto Dossena**, *Regional Sales Director per Italia, Svizzera, Grecia, Croazia e Ungheria di Saviynt*

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/come-adottare-lo-zero-trust-identity-secondo-saviynt/