Una strategia Zero-trust Network Access ha 3 esigenze

I modelli di sicurezza tradizionali operano partendo dal presupposto che tutto ciò che si trova all'interno della rete delle organizzazioni deve essere affidabile. Tuttavia, estendere automaticamente la fiducia a qualsiasi dispositivo o utente mette a rischio l'organizzazione quando, intenzionalmente o meno, uno o l'altro viene compromesso. Questo è il motivo per il quale molti responsabili della sicurezza si stanno orientando verso un approccio Zero-Trust Access (ZTA) per identificare, autenticare e monitorare utenti e dispositivi, sia all'interno che all'esterno della rete.

L'innovazione digitale sta migliorando notevolmente la produttività, ma allo stesso tempo sta creando nuovi rischi per la sicurezza informatica. Gli aggressori, il malware e i dispositivi infetti che eludono i punti di controllo della sicurezza lungo il perimetro spesso hanno libero accesso all'interno della rete.

Per questi motivi, le organizzazioni non possono più fidarsi degli utenti o dei dispositivi all'interno o all'esterno della rete. I responsabili della sicurezza devono presumere che ogni dispositivo della rete sia potenzialmente infetto e che ogni utente sia in grado di compromettere le risorse critiche, intenzionalmente o meno. Una strategia ZTA trasforma il paradigma fondamentale delle reti aperte costruite intorno alla fiducia intrinseca in una struttura a fiducia zero attraverso l'adozione di rigorosi controlli di accesso alla rete.

Una strategia ZTA si concentra sulla connettività di rete e ha tre funzioni essenziali.

1. COSA: conoscere ogni dispositivo presente in rete

La proliferazione di applicazioni e dispositivi sta espandendo il perimetro, creando una geometria variabile che deve essere gestita e protetta. Il personale IT, sopraffatto, fatica a gestire i numerosissimi dispositivi, siano essi provenienti da iniziative IoT (Internet-of-Things), policy BYOD (Bring Your Own-Device) o qualsiasi altra area dell'ambiente aziendale.

Il primo passo dell'adozione di una strategia ZTA è quello di scoprire e identificare tutti i dispositivi in rete, che si tratti di telefoni o laptop di utenti finali, server di rete, stampanti o dispositivi IoT headless come controller HVAC o lettori di badge di sicurezza. Con questa visibilità, i team incaricati della sicurezza possono quindi conoscere ogni tipo di dispositivo, funzione e scopo che ha all'interno della rete. Partendo da tali informazioni, i team

Con l'aumento della connettività, della collaborazione e dei dispositivi, il panorama delle minacce si sta espandendo. Ciò richiede un approccio ZTA globale, in grado di comprendere e controllare tutti e tutto in rete.

possono impostare controlli adeguati dell'accesso di tali dispositivi. Dopodiché, una volta istituito il controllo adeguato, un approccio ZTA include anche una continua attività di monitoraggio e risposta dei dispositivi, che aiuta a identificare e correggere i dispositivi problematici in modo che non possano infettare altri dispositivi o sistemi in rete.

2. CHI: conoscere ogni utente che accede alla rete

L'identità dell'utente è fondamentale per lo sviluppo di una politica ZTA efficace. Le organizzazioni devono conoscere ogni utente che sta tentando di accedere alla rete. Sono dipendenti? Un appaltatore? Un ospite? Un vendor? Per stabilire l'identità dell'utente è necessario effettuare il login e l'autenticazione a più fattori; le password sono deboli e spesso sottratte. Dopodiché vanno utilizzati i certificati per affermare l'identità, certificati che possono essere legati al controllo dell'accesso basato sul ruolo (RBAC) per abbinare un utente autenticato a specifici diritti di accesso e servizi.

Una volta stabilita l'identità, le policy di accesso sono determinate dal ruolo dell'utente all'interno dell'organizzazione. Una "politica di accesso minimo" può essere utilizzata per garantire l'accesso alle risorse necessarie per un ruolo o un compito, con accesso a risorse aggiuntive fornito solo in base alle necessità.

Con l'adozione sempre più diffusa del modello ZTA, i responsabili della sicurezza possono iniziare a introdurre i giusti controlli per garantire ovunque agli utenti un accesso corretto accesso alla rete. La possibilità di far accedere tutti gli utenti con una formula basata sul ruolo garantisce una robusta sicurezza di rete che va a beneficio dell'intera organizzazione e delle diverse entità (partner, fornitori, appaltatori) con cui l'organizzazione collabora.

3. DENTRO e FUORI: sapere come proteggere le risorse all'interno e all'esterno della rete

Secondo un recente rapporto, il 63% delle aziende non è in grado di monitorare gli endpoint all'esterno della rete e oltre la metà non è in grado di determinare lo stato di compliance dei dispositivi endpoint.[1] Uno dei principali responsabili di questa sfida è la maggiore mobilità dei lavoratori, unita a una maggiore enfasi posta sul telelavoro.

Con una strategia ZTA, le organizzazioni possono affrontare la sfida di proteggere i dispositivi all'esterno della rete migliorando la visibilità degli endpoint. La scansione delle vulnerabilità, le robuste policy di patch e il web filtering sono tutti elementi critici di una strategia "zero fiducia". Inoltre, un approccio ZTA può consentire un accesso remoto sicuro alle risorse di rete tramite la connettività VPN. Ciò consente ai team incaricati della sicurezza di vedere, controllare e proteggere ogni risorsa, sia che si trovi all'interno della rete sia che si trovi all'esterno.

Considerazioni conclusive

Un vero e proprio framework ZTA identifica, segmenta e monitora continuamente tutti i dispositivi, consentendo alle organizzazioni di garantire che le risorse interne rimangano sicure, che i dati, le applicazioni e la proprietà intellettuale rimangano protetti e che le operazioni di rete e sicurezza siano complessivamente semplificate.

Una strategia ZTA per i dispositivi consente di:

- Identificare, profilare ed eseguire la scansione di tutti i dispositivi per individuare le vulnerabilità
- Stabilire e garantire un costante controllo della rete
- Mantenere la risposta automatica e l'orchestrazione della rete

Una strategia ZTA per gli utenti consente di:

- Stabilire l'identità attraverso login, autenticazione a più fattori e certificato
- Fornire informazioni basate sul ruolo dalla fonte di autenticazione per l'accesso privilegiato
- Fornire maggiore sicurezza e ridurre l'affaticamento dell'utente finale attraverso un'autenticazione SSO

[1] "The Cost of Insecure Endpoints," Ponemon Institute, 2019.

FORTINET

www.fortinet.com

dicembre 1, 2020 12:26 PM

696154-0-1-IT