architettura zero trust

Gli approcci tradizionali alla sicurezza informatica comportano il trasferimento di dati sensibili dentro i data center protetti da accessi e firewall. Il presupposto era che tutti all’interno dell’organizzazione fossero controllati e affidabili: nome utente e password bastavano e proteggere.
Questo approccio tradizionale è simile al fossato intorno al castello. Tuttavia, questo approccio non si adatta alle moderne minacce alla sicurezza informatica.

L'approccio ZERO TRUST, invece, evolve questo tradizionale approccio alla sicurezza informatica e, oltre alla segmentazione della rete, mira a verificare (anche più volte) ciascun utente, dispositivo e applicazione che tentano l’accesso.

L’architettura ZERO TRUST è un approccio innovativo ma soprattutto efficace contro il moderno ed evoluto cyber-crime. Il modello ZERO TRUST, ZeroTrust architecture (o ZeroTrust framework), è stato creato nel 2010 da John Kindervag, che all'epoca era il principale analista di Forrester Research Inc.

La cybersecurity innovativa con approccio ZERO TRUST informatica è fondamentale perché i dipartimenti IT, oggi, vedono quadruplicare le tipologie di attacco, devono difendere una attack surface molto più ampia e diffusa del vecchio “perimetro di rete”, devono proteggere i dipendenti in smart-working con dispositivi personali che non hanno la medesima cyber-posture ed igiene dei dispositivi aziendali.
ZTNA (architettura ZERO TRUST) protegge le tradizionali tecnologie VPN per l'accesso alle applicazioni e rimuove la fiducia "di default" per consentire a dipendenti e partner di connettersi e collaborare. Gartner definisce lo ZTNA come prodotti e servizi che creano un confine logico di accesso basato su identità e contesto, che comprende un utente aziendale e un'applicazione aziendale.

Il Dott. Daniel Rozenek di TEKAPP ci racconta: "Sia vendor che system integrator, vedendo il grande interesse intorno allo ZERO TRUST stanno cominciando a inquadrare tutti i prodotti che vendono da anni come prodotti "zero trust ".

Il consiglio classico che possiamo dare alle organizzazioni che intendono perseguire la sicurezza ad approccio ZERO TRUST informatica è di implementare soluzioni ZTNA (ad esempio la innovativa soluzione Made in Israel ZERO NETWORKS) la un passo alla volta e scegliendo gli asset e risorse più critiche da proteggere prima.

Per maggiori dettagli, controlla zero trust informatica.

Fonte: https://www.techtarget.com/searchsecurity/definition/zero-trust-model-zero-trust-network