Una breve storia dello zero trust: dalla teoria alla Casa Bianca

Le organizzazioni stanno adottando lo zero trust per soddisfare le esigenze del business moderno. Per comprendere realmente quanto sia rivoluzionaria questa architettura, le organizzazioni devono considerare l'evoluzione dello zero trust e il modo in cui questo approccio ha trasformato radicalmente idee ormai datate sulle reti e la sicurezza aziendale.

1987

La costruzione dei confini del perimetro di rete

Gli ingegneri della Digital Equipment Corporation (DEC) pubblicano il primo documento sulla tecnologia dei firewall, inaugurando un periodo lungo decenni di sicurezza della rete basata sul modello a castello e fossato.

1990

Separazione elementare con la segmentazione della rete

Hanno inizio i primi tentativi di segmentare la rete utilizzando VLAN o sottoreti; si tratta di un approccio estremamente limitato senza autenticazione, con restrizioni minime e poche funzionalità interne di sicurezza. Le restrizioni implementate possono essere bypassate senza difficoltà.

2001

Viene aggiunto il controllo degli accessi alla rete

L'IEEE Standards Association pubblica il protocollo 802.1X per il controllo degli accessi alla rete (NAC, Network Access Control). A seguito dell'adozione delle WLAN, questa soluzione consente connessioni di rete autenticate e offre un accesso a livello di rete (LAN/VLAN), ma è complessa e difficile da distribuire su larga scala.

2004

Il concetto di zero trust fa capolino

Nasce il Jericho Forum. Il forum riconosce il progressivo abbandono della rete aziendale da parte di utenti e app, e introduce i primi concetti relativi allo zero trust attraverso il principio della deperimetralizzazione.

2010

Nasce lo zero trust

L'analista John Kindervag presenta il "modello zero trust" in un documento per Forrester Research. Sposta l'autenticazione e la sicurezza inline e suggerisce la segmentazione delle sessioni. Sebbene il focus sia ancora sull'accesso alla rete, in questo modello il perimetro si sposta all'interno della rete.

2014

Google definisce il suo modello

L'iniziativa BeyondCorp di Google reinventa l'architettura di sicurezza dopo l'attacco Operazione Aurora, e porta alla distribuzione dello zero trust a livello aziendale.

2016

Zscaler sposta lo zero trust sul cloud

Zscaler introduce la prima soluzione zero trust fornita sul cloud, consentendo alle organizzazioni di eliminare la superficie di attacco esterna e di ridurre al minimo il movimento laterale potenziale e semplificando radicalmente la distribuzione dello zero trust.

2019

Gartner entra in scena

Gartner introduce il concetto di SASE (Secure Access Service Edge) e rivitalizza il concetto di zero trust, ridefinendolo come ZTNA (Zero Trust Network Access).

2020

Il NIST definisce il framework standard dello zero trust

Il NIST pubblica l'SP 800-207 come framework unificato per la creazione di un'architettura zero trust (ZTA), e introduce il primo vero cambiamento rispetto alla definizione di zero trust nel contesto della rete.

2021

Gartner definisce un percorso sicuro

Gartner definisce i componenti di sicurezza del SASE come una nuova categoria di mercato, nota come Security Service Edge (SSE).

2022

Il governo degli Stati Uniti impone lo zero trust

L'Office of Management and Budget impone l'adozione dei principi dello zero trust a tutte le agenzie entro il 2024.

Approfondisci la storia dello zero trust e il suo futuro.

Leggi il white paper

zscaler | Experience your world, secured.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.it