



La crescente delocalizzazione di risorse e identità al di fuori della rete aziendale richiede controlli più severi. Tradizionali strategie di sicurezza come il «Trusted Network» non bastano più per contrastare le avanzate tipologie degli attacchi.

Perché le aziende hanno bisogno di Zero Trust?

Sempre più risorse e identità abbandonano la rete aziendale (BYOD, home office, mobile & cloud) e un numero sempre maggiore di utenti interni ed esterni ha accesso alle risorse aziendali. Questo richiede istruzioni, metodi e applicazioni per un controllo rigoroso e verificabile degli utenti e delle autorizzazioni. Metodi di attacco avanzati permettono altresì furti d'identità come phishing e furti dei dati di accesso. La strategia di sicurezza «Trusted Network» non è quindi più sufficiente per proteggere a tutto campo la rete aziendale. Zero Trust offre una serie di concetti e idee per ridurre

al massimo l'insicurezza quando si mettono in atto precise decisioni di accesso con i privilegi minimi per ogni richiesta nei sistemi e servizi d'informazione. La finalità è quella di abbassare i costi causati da eventi critici per la sicurezza ed evitare possibili danni alla reputazione. Il nostro Security Consulting Team offre consulenza alla vostra impresa per l'uso e l'attuazione delle strategie Zero Trust ai fini di una protezione ancora più ampia della vostra infrastruttura e del vostro business. Con la nostra procedura standardizzata per l'introduzione dell'architettura Zero Trust, vi guideremo al vostro passo verso il necessario livello di maturità.

I vantaggi di una consulenza Zero Trust

Creazione della roadmap e del piano di migrazione

I nostri esperti e le nostre esperte elaboreranno per voi una roadmap e un piano di migrazione con strategici progetti Zero Trust.



Maggiore sicurezza – Aumento della resilienza

L'attuazione coerente di strategie Zero Trust consente di bloccare, delimitare o riconoscere prima gli attacchi.



Consapevolezza della compliance e requisiti normativi

Supporto nell'ottimizzazione della governance per la gestione di progetti Zero Trust.



Valutazione della maturità

Viene accertata la maturità culturale e tecnica della vostra impresa con la determinazione del necessario grado di maturità.



Approccio di consultazione per l'introduzione dell'architettura Zero Trust





Facts & Figures

Valutazione e workshop

- Workshop per i clienti – determinazione del necessario grado di maturità
 - Valutazioni della maturità e valutazioni tecniche
 - Identificazione dei più importanti e preziosi dati, risorse, app e servizi
 - Identificazione dei principali rischi e del campo di applicazione a livello normativo
 - Identificazione di soluzioni relative all'identità e alla rete per utenti finali e DC
 - Roadmap con strategici progetti Zero Trust
 - Elaborazione di una roadmap con strategici progetti Zero Trust
 - Piano di migrazione all'architettura di riferimento Zero Trust
-

Consapevolezza

- Consapevolezza culturale: ripercussioni di Zero Trust sulla cultura aziendale esistente
 - Disponibilità all'introduzione di un modello di sicurezza Zero Trust sulla base di risorse critiche, rischi chiave, tecnologie esistenti e aspetti culturali
 - Ideazione / implementazione di campagne di sensibilizzazione nel campo della sicurezza dell'informazione:
 - effettuazione di corsi di formazione sulla security awareness
 - pianificazione e implementazione di campagne di phishing
-

Supporto relativo al progetto e a livello organizzativo

- Supporto nell'ottimizzazione della governance per la gestione di progetti Zero Trust nonché della completa adozione Zero Trust (Zero Trust Journey)
 - Ottimizzazione dell'organizzazione di sicurezza in base alle esigenze aziendali
-

Per maggiori informazioni e per contattare i nostri esperti si prega di consultare [swisscom.ch/security-consulting](https://www.swisscom.ch/security-consulting)

Le informazioni contenute in questo documento non rappresentano un'offerta vincolante. Con riserva di modifiche in qualsiasi momento.

Swisscom (svizzera) SA Enterprise Customers, casella postale,
CH-3050 Berna, tel. 0800 800 900, www.swisscom.ch/enterprise