



La délocalisation croissante des ressources et des identités en dehors du réseau de l'entreprise exige des contrôles plus stricts. Les stratégies de sécurité traditionnelles comme le «Trusted Network» ne sont plus suffisantes pour contrecarrer les méthodes d'attaque avancées.

Pourquoi les entreprises ont-elles besoin de Zero Trust?

De plus en plus de ressources et d'identités sortent du réseau de l'entreprise (BYOD, télétravail, mobile et cloud) et de plus en plus d'utilisateurs internes et externes ont accès aux ressources de l'entreprise. Des instructions, des méthodes et des applications sont requises pour un contrôle rigoureux et vérifiable des utilisateurs et des autorisations. Des méthodes d'attaque avancées permettent en outre une usurpation d'identité comme l'hameçonnage et le vol de données d'accès. La stratégie de sécurité «Trusted Network» n'est donc plus suffisante pour protéger adéquatement le réseau de l'entreprise. Zero Trust propose une série de

concepts et d'idées visant à réduire au minimum l'incertitude quant à la mise en application de décisions d'accès précises, suivant le principe du moindre privilège et à la demande, dans les systèmes et services d'information. Le but est de réduire les coûts occasionnés par les incidents de sécurité et d'empêcher d'éventuelles atteintes à la réputation. Notre équipe Security Consulting conseille votre entreprise au sujet de la gestion et de la mise en œuvre des concepts Zero Trust pour protéger encore mieux votre infrastructure et votre activité. Grâce à la méthode standardisée que nous utilisons pour introduire une architecture Zero Trust, nous vous menons à la maturité nécessaire à votre propre rythme.

Les avantages d'une consultation Zero Trust pour vous

Élaboration de la roadmap et du plan de migration

Nos expertes et experts élaborent une roadmap et un plan de migration avec des projets Zero Trust stratégiques.



Sécurité accrue – hausse de la résilience

Une mise en œuvre systématique des concepts Zero Trust permet de parer, de limiter ou d'identifier plus tôt les attaques.



Sensibilisation à la conformité et aux exigences réglementaires

Soutien au développement de la gouvernance pour réaliser les projets Zero Trust.



Évaluations de la maturité

La maturité culturelle et technique de votre entreprise est évaluée et le degré de maturité nécessaire déterminé.



Approche consultative utilisée pour introduire une architecture Zero Trust





Facts & Figures

Évaluation et ateliers

- Ateliers clients – détermination du degré de maturité nécessaire
 - Évaluations de la maturité et évaluations techniques
 - Identification des données, ressources, applis et services les plus importants et les plus précieux
 - Identification des principaux risques et du champ d'application réglementaire
 - Identification de solutions d'identité et de réseau pour les utilisateurs finaux et les DC
 - Roadmap avec des projets Zero Trust stratégiques
 - Élaboration d'une roadmap avec des projets Zero Trust stratégiques
 - Plan de migration vers l'architecture de référence Zero Trust
-

Sensibilisation

- Sensibilisation culturelle: répercussions de Zero Trust sur la culture d'entreprise existante
 - État de préparation pour l'introduction d'un cadre de sécurité Zero Trust sur base des ressources critiques, des risques clés, des technologies existantes et des aspects culturels
 - Conception/mise en œuvre de campagnes de sensibilisation dans le domaine de la sécurité de l'information:
 - Organisation de formations de sensibilisation à la sécurité
 - Planification et mise en œuvre de campagnes de sensibilisation à l'hameçonnage
-

Soutien organisationnel et par projet

- Soutien au développement de la gouvernance pour réaliser les projets Zero Trust et l'adoption de Zero Trust (Zero Trust Journey) dans son ensemble
 - Développement de la sécurité organisationnelle à l'aide des besoins commerciaux
-

Vous trouverez de plus amples informations et les données de contact de nos experts sous swisscom.ch/security-consulting