Voici comment ça marche avec Zero Trust

La mise en œuvre d'une stratégie Zero Trust rigoureuse nécessite davantage que des outils de sécurité ponctuels et insuffisamment intégrés. Une approche complète est nécessaire, qui englobe tous les aspects de Zero Trust, comme les utilisateurs, les applications et l'ensemble de l'infrastructure.

Pour la majorité des entreprises, les jours où les collaborateurs ne travaillaient qu'au sein du réseau bien sécurisé de l'entreprise sont désormais comptés. Les formes de travail hybrides, les infrastructures dispersées, la multitude d'applications et de services cloud utilisés, l'intégration de l'IoT ainsi que les différents appareils mobiles, en partie personnels, offrent aux cybercriminels une surface d'attaque fortement élargie en dehors du périmètre réseau traditionnel. Ce défi ne peut être relevé qu'en renonçant à la confiance implicite lors de chaque accès aux ressources de l'entreprise et en vérifiant en permanence chaque interaction numérique à toutes les étapes ¬– en bref, dans le monde du travail actuel marqué par le numérique, une approche Zero Trust est la stratégie de cybersécurité à adopter.

Zero Trust dans toute l'entreprise
Pour mettre en œuvre une stratégie Zero Trust, certaines entreprises utilisent différentes solutions ponctuelles mal intégrées entre elles, telles que protection des endpoints, l'accès à distance (VPN), l'authentification multifactorielle et la prévention des pertes de donnée, souvent de différents fabricants. Ces différentes mesures de sécurité doivent être testées, implémentées et corrigées individuellement, ce qui est coûteux. Parallèlement, les ressources humaines et financières manquent pour faire face au paysage très dynamique des menaces. Tout cela rend difficile la mise en œuvre d'une stratégie Zero Trust à l'échelle de l'entreprise. Une solution applicable à l'échelle de l'entreprise et couvrant tous les aspects de la cybersécurité et du Zero Trust est donc préférable. C'est précisément sur ce point que Palo Alto Networks se penche depuis plus de dix ans et est parvenu à trois conclusions:

1. Prise en compte de l'ensemble
Utilisateurs, systèmes, réseau, applications, données: Zero Trust ne doit pas se limiter à une seule technologie, mais doit englober l'ensemble de l'écosystème utilisé pour sécuriser l'entreprise.

2. Procédure par étape
La mise en place d'une entreprise Zero Trust complète n'est pas triviale – mais on peut commencer par des mesures simples qui peuvent déjà être mises en œuvre avec les outils de sécurité existants.

3. Avantages pour le business
Outre les aspects techniques, l'approche Zero Trust offre d'autres avantages qui peuvent être communiqués de manière simple et compréhensible.

Pour les utilisateurs, les applications et l'infrastructure

Zero Trust élimine la confiance implicite dans toute l'entreprise et vérifie chaque transaction numérique tout au long du processus, tant pour les utilisateurs que pour les applications et toute l'infrastructure. La première étape consiste à mettre en place des contrôles stricts pour authentifier l'identité des utilisateurs et assurer le respect des politiques out en limitant les droits d'accès au strict nécessaire.

Les applications et les microservices ainsi que l'ensemble du trafic de données ne sont en principe pas non plus dignes de confiance et doivent également être vérifiés en permanence pendant toute leur durée de vie. Il en va de même pour l'infrastructure complète, des routeurs et des commutateurs aux ressources utilisées dans la chaîne d'approvisionnement, en passant par les appareils des utilisateurs et les ressources cloud et IoT.

Grâce à son approche de plateforme, Palo Alto Networks fournit un portefeuille de sécurité complet pour la mise en œuvre d'une stratégie Zero Trust. Avec des solutions telles que des pare-feux de nouvelle génération, des services de sécurité depuis et vers le cloud, une excellente protection des endpoints et des produits Secure Access Service Edge, le fabricant offre une plateforme entièrement intégrée pour tout voir, tout vérifier et tout sécuriser. Le portefeuille est complété par des services de sécurité complets et un solide réseau de partenaires disposant d'un savoir-faire d'experts.

BOLL
IT Security Distribution

BOLL Engineering SA
En Budron H15,
1052 Le Mont-sur-Lausanne

Tél. 021 533 01 60
vente@boll.ch
www.boll.ch