

LES RÉSEAUX ZERO TRUST ONT LE VENT EN POUPE

Les infrastructures d'impression et de numérisation sont souvent négligées dans les modèles de sécurité Zero Trust et les prestataires de services compétents sont impliqués bien trop tardivement. Cette négligence peut s'avérer très risquée.

L'essor massif des modèles de travail hybrides nous a montré à la fois les perspectives prometteuses et les pièges de notre monde numérique et connecté. À titre d'exemple, la proportion croissante de personnes travaillant à domicile entraîne une multiplication exponentielle des risques de cyberattaques, car de plus en plus d'appareils se connectent au réseau de l'entreprise depuis plusieurs endroits différents et via des services de cloud publics.

«Never trust, always verify»

Dans ce contexte, les architectures de réseau Zero Trust gagnent en importance. Tandis qu'un réseau traditionnel repose sur la notion de confiance inhérente, le modèle Zero Trust exige que l'ensemble des utilisateur-trice-s, appareils et applications, qui se trouvent à l'intérieur comme l'extérieur du réseau de l'entreprise, fassent systématiquement l'objet d'une authentification, d'une autorisation et d'une surveillance selon le principe «never trust, always verify» avant de pouvoir accéder aux réseaux et aux données.

Imprimantes multifonctions: trop souvent négligées dans les environnements Zero Trust

Les imprimantes, les imprimantes multifonctions (MFP) ainsi que les solutions logicielles correspondantes ne sont pas prioritaires dans le développement d'une stratégie de réseau Zero Trust. Cette négligence peut avoir des conséquences désastreuses, car les MFP disposent aujourd'hui d'innombrables fonctions, services et paramètres de sécurité, dont beaucoup sont inconnus ou utilisés à mauvais escient, ce qui entraîne des risques inutilisés. Pour les pirates informatiques, les MFP constituent donc un moyen d'attaque pratique: elles peuvent être utilisées pour propager des logiciels malveillants sur l'ensemble du réseau et dérober des informations protégées, ou même servir de point d'entrée (Entry Point) pour explorer le réseau et collecter des informations en vue d'une attaque de plus grande envergure. Les entreprises doivent donc combiner sécurité des réseaux, des données et des points de terminaison pour l'environnement de numérisation et d'impression: c'est la clé d'une architecture Zero Trust.

Faire appel au bon partenaire de service

Les entreprises qui offrent à leur personnel un poste de travail moderne tout en optimisant la gestion



des risques grâce à l'approche Zero Trust doivent, à un stade précoce, faire appel à des partenaires de service spécialisés dans l'infrastructure d'entrée et de sortie. Il convient d'avoir recours à des solutions basées sur le cloud ainsi qu'à une approche cohérente couvrant les appareils, les logiciels, les processus et les utilisateur-trice-s. Les facteurs suivants doivent notamment être pris en compte:

- **Identification et protection des identités:** l'approche Zero Trust commence par l'identification des identités et la protection des points de terminaison. Les terminaux à usage collectif tels que les MFP et les imprimantes doivent en particulier être authentifiés et faire l'objet de certificats. De plus, les ports et protocoles inutilisés par lesquels ils sont accessibles doivent être désactivés.
- **Protection de réseaux:** une microsegmentation du réseau permet de garantir que les utilisateur-trice-s ont uniquement accès aux ressources du réseau qui sont absolument nécessaires à leur travail. En ce qui concerne le travail hors site, il est nécessaire de séparer hermétiquement les applications de l'entreprise à usage professionnel des réseaux domestiques locaux et privés des collaborateur-trice-s, car leur sécurité ne peut tout simplement pas être garantie.
- **Surveillance et optimisation continues:** toutes les identités doivent être surveillées et optimisées en permanence afin de respecter les politiques de sécurité de l'entreprise et faire preuve de résilience face aux menaces actuelles. Les modifications non intentionnelles ou non autorisées doivent être détectées immédiatement. De plus, les firmwares, les logiciels et les applications doivent être régulièrement mis à jour afin de combler les failles connues et de se protéger au mieux contre les attaques Zero Day.

