Veille Zero Trust

Le modèle « Zero Trust » ou « zéro confiance » est une approche de sécurité informatique qui part du principe simple : on ne fait confiance à personne par défaut. Contrairement à l'ancienne stratégie qui protégeait uniquement les frontières du réseau, le Zero Trust considère que tout accès, qu'il vienne de l'extérieur ou de l'intérieur, doit être vérifié. Chaque utilisateur, chaque appareil et chaque demande d'accès est contrôlé en continu : on vérifie l'identité de l'utilisateur, la sécurité de l'appareil utilisé et le contexte de connexion. Seuls les accès strictement nécessaires sont accordés (principe du moindre privilège).

De plus en plus d'organisations adoptent ce modèle dans leurs infrastructures informatiques modernes. Par exemple, avec l'essor du télétravail, un employé qui se connecte depuis chez lui doit passer par un système Zero Trust qui vérifie en permanence ses accès : mot de passe + code envoyé sur son téléphone, vérification que son ordinateur est à jour et limitation de ses accès aux seules applications dont il a besoin. De même, dans le cloud où les données d'entreprise sont hébergées hors site, le Zero Trust impose des contrôles forts pour chaque connexion, même depuis le réseau interne de l'entreprise. Les accès aux applications sensibles sont ainsi strictement gérés, et les grandes entreprises ou administrations adoptent progressivement ces principes pour sécuriser leurs réseaux étendus.

Ce modèle présente de nombreux avantages : il renforce la protection des données et des ressources en empêchant la propagation d'une attaque dans tout le système informatique. Il est adapté au monde actuel, marqué par le nomadisme des utilisateurs, la diversité des appareils et la migration vers le cloud, car il ne dépend pas d'un lieu ou d'un « périmètre » fixe. En outre, le Zero Trust améliore la traçabilité des accès et oblige les entreprises à mieux gérer les utilisateurs et le parc informatique. Toutefois, cette approche a aussi ses défis. Sa mise en place peut être complexe et coûteuse : elle exige de mettre à jour les systèmes, d'ajouter des dispositifs de sécurité supplémentaires (par exemple l'authentification en deux étapes : mot de passe + code) et de gérer finement les identités et les droits d'accès. Ce changement demande du temps et une adaptation des équipes. Il ne s'agit pas d'une solution miracle, mais d'une évolution de la sécurité qui répond aux nouveaux risques. Avec la multiplication des attaques et la fin des frontières physiques dans les réseaux, Zero Trust devient une tendance forte en cybersécurité, car il offre un cadre plus robuste pour protéger les entreprises des menaces d'aujourd'hui.

Sources: ANSSI - DarkReading - NIST

Cybersecurity: Politique Zero Trust