Les 3 impératifs d'une stratégie d'accès réseau zero-trust

Les modèles traditionnels de sécurités reposent sur l'hypothèse que tout ce qui se trouve à l'intérieur du périmètre réseau est de confiance. Pour autant, une confiance attribuée automatiquement à tous les dispositifs et utilisateurs met l'entreprise en péril : il suffit les uns ou les autres soient compromis, intentionnellement ou non. C'est la raison pour laquelle de nombreux responsables de la sécurité se tournent vers une approche Zero-Trust Access (ZTA), ou accès à vérification systématique, pour identifier, authentifier et surveiller les utilisateurs et les appareils, sur et hors du réseau.

L'innovation digitale favorise les gains de productivité, mais de nouveaux risques émergent. Les assaillants, les logiciels malveillants et les appareils infectés qui contournent la sécurité en périphérie de réseau ont souvent libre accès à l'intérieur de ce réseau.

Pour ces raisons, les entreprises ne doivent plus faire confiance aux utilisateurs ou aux dispositifs réseau. Elles doivent intégrer le principe que chaque appareil sur le réseau est potentiellement infecté et que tout utilisateur est susceptible de mettre en péril des ressources critiques, intentionnellement ou fortuitement. Une stratégie d'accès zero-trust au réseau remet en cause cette notion de confiance a priori qui s'applique aux réseaux ouverts, pour privilégier un framework zero-trust, basé sur des contrôles d'accès strictes et systèmatiques au réseau.

L'univers des menaces s'élargit compte tenu d'une connectivité, d'une collaboration et de dispositifs omniprésents. Dans ce contexte, une approche globale pour des accès zero-trust permet de comprendre et contrôler chaque dispositif et chaque utilisateur présent sur votre réseau.

Une stratégie ZTA porte sur la connectivité du réseau et se décline en trois fonctions essentielles.

1. Connaître tous les dispositifs présents sur le réseau

La prolifération des applications et des dispositifs élargit le périmètre réseau, créant d'innombrables environnements edge devant être gérés et protégés. Les équipes de sécurité, souvent submergées, peinent à gérer ce parc d'appareils, constitué d'objets connectés ou de dispositifs personnels BYOD notamment.

L'adoption d'une stratégie ZTA s'initie par l'identification de tous les appareils sur le réseau, qu'il s'agisse du téléphone ou de l'ordinateur portable d'un utilisateur, d'un serveur réseau, d'une imprimante ou d'un dispositif IoT headless (sans interface graphique) tel qu'un contrôleur CVC ou un lecteur de badge de sécurité. Avec cette visibilité, les équipes de sécurité connaissent chaque type d'appareil, sa fonction et son utilité au sein du réseau. De là, les équipes peuvent mettre en place un contrôle d'accès spécifique à chaque profil de dispositif. En aval de ce contrôle d'accès, une approche ZTA assure le contrôle et la prise en charge continus des dispositifs, pour détecter et prendre en charge tout dispositif posant problème, et prévenir toute infection potentielle d'autres systèmes présents sur le réseau.

2. Connaître tous les utilisateurs qui accèdent au réseau

L'identité des utilisateurs est essentielle pour élaborer une politique ZTA efficace. Les entreprises doivent connaître chaque utilisateur qui tente d'accéder à son réseau. S'agit-il d'un collaborateur, d'un sous-traitant, d'un invité ou d'un fournisseur ? Connaître l'identité d'un utilisateur nécessite une connexion de sa part mais aussi une authentification multifactorielle, les mots de passe étant souvent faibles et piratés. Des certificats doivent ensuite être utilisés pour faire respecter l'identité, avec la possibilité d'utiliser un contrôle d'accès basé sur les rôles (RBAC) pour attribuer des droits d'accès et des services spécifiques à l'utilisateur.

Une fois l'identité de l'utilisateur établie, les règles d'accès sont déterminées selon son rôle dans l'entreprise. Une politique d'accès minimal est utilisée pour accorder l'accès aux ressources nécessaires à un rôle ou à un poste, l'accès aux autres ressources n'étant fourni qu'en fonction des besoins.

Au fur et à mesure que le modèle zero-trust est adopté, les équipes de sécurité peuvent activer des fonctions qui permettent aux utilisateurs, quelle que soit leur localisation, d'accéder au réseau. La possibilité d'accueillir tous les utilisateurs via un accès réseau basé sur le rôle renforce la sécurité réseau, au profit de l'ensemble de l'entreprise et des tiers (partenaires, fournisseurs, sous-traitants) avec lesquels elle travaille.

3. Protéger les ressources sur et hors du réseau

Selon un récent rapport, 63 % des entreprises ne sont pas en mesure de surveiller les terminaux hors réseau, et plus de la moitié d'entre elles ne peuvent pas déterminer le niveau de conformité de ces terminaux. [1] L'un des principaux responsables de cette carence est le développement de la mobilité sur le lieu de travail, associée à une place accrue du télétravail.

Avec une stratégie ZTA, les entreprises sont outillées pour protéger les dispositifs hors du réseau, grâce à une meilleure visibilité sur les terminaux. L'analyse des vulnérabilités, des règles de patching pertinentes et le filtrage Web sont les piliers du ZTA. En outre, une approche ZTA sécurise les accès distants aux ressources du réseau, via une connexion par réseau privé virtuel (VPN). Ainsi, les équipes de sécurité voient, contrôlent et protègent chaque ressource présente sur et hors du réseau.

Étapes suivantes

Un framework ZTA identifie, segmente et contrôle en permanence tous les appareils et sécurise les ressources internes des entreprises : les données, les applications et les éléments de propriété intellectuelle restent protégées tandis que les opérations de réseau et de sécurité sont globalement simplifiées.

Une stratégie ZTA pour vos dispositifs vous permet de :

- Identifier, de profiler et d'analyser tous les dispositifs, à la recherche de vulnérabilités ;
- Établir et d'assurer un contrôle permanent du réseau ;
- Automatiser la réponse aux menaces et l'orchestration du réseau.

Une stratégie ZTA pour vos utilisateurs vous permet de :

- Établir leur identité grâce à une connexion, une authentification à facteurs multiples et un certificat ;
- Fournir des informations basées sur les rôles et sur l'authentification, pour définir et mettre en œuvre les privilèges d'accès ;
- Renforcer la sécurité accrue et simplifier l'expérience des utilisateurs, grâce à une authentification single signe-on (SSO).

[1] « The Cost of Insecure Endpoints, » Ponemon Institute, 2019.

FORTINET

www.fortinet.fr

décembre 7, 2020 11:16 AM

696154-0-1-FR