Travail à distance : six étapes pour le sécuriser à grande échelle

1 – VPN et sécurité des terminaux (endpoints)

Tous les utilisateurs doivent disposer d'un ordinateur portable chargé de toutes les applications essentielles dont ils ont besoin pour faire leur travail. En outre, cet ordinateur portable doit comporter un client préconfiguré pour assurer la connectivité VPN avec le siège de l'entreprise.

2 – Authentification multifactorielle

L'authentification multifactorielle permet d'empêcher les cybercriminels d'utiliser des mots de passe volés pour accéder aux ressources du réseau. Pour permettre un accès plus sûr, chaque utilisateur doit également disposer d'un jeton d'authentification sécurisé. Ces jetons peuvent être un dispositif physique (comme un porte-clés) ou logiciel (comme une application téléphonique), et sont utilisés lors d'une connexion VPN ou d'une connexion au réseau pour fournir une couche supplémentaire de validation d'identité.

Étapes 3 et 4 – Aide aux télétravailleurs avec des exigences avancées

Certains des télétravailleurs ont besoin d'un accès avancé aux ressources du réseau pour faire leur travail. Les administrateurs de systèmes, les techniciens d'assistance, le personnel d'urgence et les équipes de direction doivent souvent accéder à des informations extrêmement sensibles et confidentielles et les traiter, ou bien travailler dans des environnements informatiques multiples et parallèles.

3 – Connectivité persistante

Des points d'accès sans fil préconfigurés permettent une connectivité sécurisée entre le site distant d'un utilisateur et le réseau de l'entreprise via un tunnel fiable et sécurisé. Pour une connexion plus sûre, un point d'accès sans fil peut être associé à un pare-feu de nouvelle génération basé sur le bureau pour permettre des connexions persistantes, un contrôle d'admission avancé et un éventail complet de services de sécurité avancés, y compris la prévention des pertes de données.

4- Téléphonie sécurisée

Ces utilisateurs ont également besoin d'une solution de téléphonie prenant en charge la voix sur IP (VoIP) pour assurer des communications sécurisées. Il existe des modèles de clients physiques et logiciels qui permettent aux utilisateurs de passer ou de recevoir des appels, d'accéder à la messagerie vocale, de consulter l'historique des appels et de faire des recherches dans le répertoire de l'organisation.

Étapes 5 et 6 – Création d'une tête de réseau sécurisée et évolutive

L'autre moitié de l'équation consiste à faire en sorte que la tête de réseau puisse s'adapter au volume soudain de télétravailleurs ayant besoin d'un accès à distance aux ressources du réseau tout en garantissant que l'accès au réseau est correctement sécurisé.

5 – Authentification de l'utilisateur et du dispositif

Un service d'authentification central connecté à l'annuaire actif du réseau, LDAP et Radius, permet aux télétravailleurs de se connecter en toute sécurité aux services du réseau à grande échelle.

Cette solution doit également prendre en charge les services d'authentification unique, la gestion des certificats et la gestion des invités.

6 – Sécurité périmétrique avancée

Une solution NGFW permet de mettre fin aux connexions VPN en toute sécurité, d'assurer une protection avancée contre les menaces – y compris l'analyse des logiciels malveillants et autres contenus suspects dans un environnement « sandboxed » avant qu'ils n'atteignent leur destination, et une inspection performante du trafic en clair et chiffré pour éliminer les logiciels et le trafic malveillants.

L'évolutivité de cette fonction est particulièrement importante, car l'inspection des données cryptées est extrêmement gourmande en ressources processeur. Sans processeurs de sécurité avancés conçus pour inspecter de gros volumes de trafic crypté, les solutions NGFW peuvent rapidement devenir un goulot d'étranglement qui peut avoir un impact sur la productivité des télétravailleurs.