Télétravail et défis informatiques

Mais le télétravail pose un certain nombre de défis en matière de sécurité informatique. Voici lesquels, ainsi que quelques clés pour les appréhender.

Licence VPN

D'une manière générale, les travailleurs à domicile qui accèdent aux ressources du réseau d'entreprise le font via un VPN. Cela garantit que, quel que soit leur type de connexion depuis un endroit éloigné du réseau d'entreprise, ils peuvent travailler sous les différentes protections et politiques qui s'y appliquent.
Les VPN sont généralement attribués sous forme de licence par utilisateur, et si les organisations disposent souvent d'un certain nombre de licences, la plupart n'en ont pas assez pour mettre un grand nombre de nouveaux travailleurs à domicile en ligne dans un court laps de temps. Pour que le VPN fonctionne et pour qu'il puisse assurer une bonne sécurité des applications d'entreprises, il faut qu'il soit configuré correctement ainsi que les serveurs sur lesquels il tourne.

Il est conseillé de se renseigner auprès de ses partenaires informatiques qui sont en relations étroites avec les principaux fournisseurs de VPN, notamment Cisco et Palo Alto, et qui peuvent avoir accès à des options tarifaires préférentielles mises en place pour aider les entreprises à relever le défi soulevé par l'épidémie de coronavirus.

Contrôler l'utilisation des applications cloud

Certains utilisateurs sont en mesure de travailler en utilisant uniquement des applications cloud. Pour ces derniers, l'accès VPN au réseau de l'entreprise peut se révéler inutile.

Toutefois, ces utilisateurs, qui accèdent aux applications cloud sans se connecter au réseau, ne seront pas régis par les politiques de l'entreprise et ne bénéficieront pas des protections mises en place sur celui-ci. Cela présente bien sûr des risques en termes de sécurité.
Par exemple, lorsqu'un utilisateur transmet ses identifiants de connexion de manière non sécurisée, ou lorsqu'il accède à un site web compromis, il peut permettre l'installation de logiciels malveillants sur son appareil : une mise en danger évidente pour lui-même et son équipement, mais également pour les actifs de l'entreprise.

Pour faire face à ce défi, deux approches peuvent être adoptées. Un portail d'authentification unique sécurisée (SSO) permet aux utilisateurs de se connecter une fois, puis de s'authentifier sur les applications cloud lorsqu'ils en ont besoin. Ceux-ci étant connectés par le portail SSO, le département informatique peut appliquer les politiques de l'entreprise, par exemple en contrôlant les applications cloud auxquelles chaque utilisateur peut accéder. Le SSO peut être rapidement opérationnel, configuré et lancé en seulement deux ou trois heures.

Parallèlement, des outils de filtrage du web, tels que Cisco Umbrella par exemple, peuvent gérer l'accès aux sites web de l'entreprise à chaque fois qu'un ordinateur portable de l'entreprise est utilisé pour accéder à l'internet, où que ce soit dans le monde.

Protéger le terminal

Lorsque l'entreprise fournit aux employés leurs ordinateurs pour le travail à distance, il est important que les machines soient correctement sécurisées, cryptées et configurées pour un usage domestique. Plusieurs logiciels permettant une protection des données sensibles sur les différents Endpoints des utilisateurs existent. Votre fournisseur de services est le plus à même de vous conseiller sur la bonne stratégie à suivre et la meilleure façon de les déployer.

Les tests de pénétration sont utiles à cet égard, car ils permettent de déceler les faiblesses des ordinateurs portables standard et d'identifier les domaines dans lesquels la sécurité des appareils peut être améliorée.

Former les utilisateurs

Aucune protection technologique ne sera utile si les utilisateurs n'adoptent pas des mesures de travail sûres et sécurisées. Les nouveaux venus dans le monde du télétravail auront tout particulièrement besoin d'être informés à ce sujet.

Des formations ou des conseils de bonnes pratiques sont disponibles auprès de plusieurs fournisseurs et peuvent être mis en place en quelques heures, pour des personnes spécifiques ou plus largement pour l'ensemble du personnel, en fournissant des instructions sur les habitudes de travail sûres telles que la sécurité des ordinateurs portables et la prévention des points d'accès Wi-Fi publics non sécurisés.