À l'ère du télétravail, six axes pour assurer la continuité des activités métiers

Christophe AUBERGER
Directeur technique - FORTINET

Les entreprises font plus que jamais appel au télétravail, une tendance commune à nombre de secteurs d'activité. Si ce travail à distance présente des avantages concrets à court terme, les dirigeants d'entreprises doivent aussi miser sur ce télétravail et sur les technologies associées pour créer de nouvelles opportunités et évoluer à plus long terme. Le télétravail n'est pas perçu comme le moteur d'un changement radical dans la façon de concevoir les architectures de sécurité des réseaux corporate, mais plutôt comme une évolution continue susceptible de faire avancer les entreprises et leurs professionnels de la sécurité. Ainsi, les décisions de sécurité dans l'optique d'accompagner le télétravail pourraient bien contribuer à la résilience contre les futures cyberattaques.

Tirer parti des technologies existantes pour encourager le télétravail

Voici 6 axes sur lesquels les dirigeants d'entreprise sont invités à se pencher pour accompagner leurs collaborateurs, sécuriser leur activité corporate et favoriser un travail hors du traditionnel siège social d'entreprise, sans pour autant devoir investir dans de nouveaux sites.

1. Assurer la confidentialité de la connectivité

Les télétravailleurs peuvent se connecter à distance à leur entreprise via un logiciel de VPN (réseau privé virtuel). Ce logiciel, installé sur le PC de chaque collaborateur, assure la confidentialité des connexions vers les applications et données distantes des entreprises, contribuant ainsi à la protection des ressources.

2. Privilégier l'authentification à facteurs multiples

Si les télétravailleurs connaissent certaines carences au niveau des fonctions de sécurité, l'authentification à facteurs multiples (ou MFA pour Multi-Factor Authentication) s'impose pour protéger les données. Le MFA peut se déployer en associant un élément en possession de l'utilisateur (un jeton ou un smartphone) avec un élément connu par cet utilisateur (un mot de passe par exemple). Cette approche active un niveau supplémentaire de sécurité qui valide l'identité d'un collaborateur lors de sa connexion.

3. Tirer parti des points d'accès sans fil et des pare-feux

Les entreprises qui souhaitent améliorer leurs stratégies de télétravail sont invitées à tirer parti de points d'accès sans fil et de pare-feux simples à déployer sur les sites distants. Préconfigurées avant d'être expédiées, ces solutions s'installent automatiquement sur site, assurant ainsi la continuité des activités et un support pour les travailleurs distants qui ont besoin de performances et de fonctionnalités supplémentaires.

4. Renforcer l'agilité des chemins de communication

Les bureaux centralisés offrent généralement des liens de communication sécurisés au niveau de leur siège social pour accueillir les nombreux utilisateurs qui y travaillent. Avec un SD-WAN, les entreprises peuvent choisir avec agilité et sécurité le meilleur chemin de communication pour leurs utilisateurs, et ce, à tout moment. Cette stratégie accompagne l'évolution des modes de communication des télétravailleurs, ces derniers étant toujours plus nombreux.

5. Tirer le meilleur parti du cloud

Les équipes qui n'ont plus accès aux ordinateurs fixes de leur siège social peuvent déployer des applications dans le cloud, similaires à celles installées sur leur PC au bureau. L'ajout de solutions de cybersécurité, pour notamment prendre en charge les connexions SSL sécurisées de n'importe quel navigateur vers le cloud, permet aux utilisateurs d'accéder en toute sécurité à ces applications et aux données associées stockées dans le cloud, et ce, sans alimenter la complexité au niveau des utilisateurs ou de l'équipe de sécurité.

6. Améliorer ses compétences en toute autonomie

Un des avantages du télétravail est d'offrir davantage de temps supplémentaire aux collaborateurs, ces derniers n'ayant plus à se déplacer chaque jour au bureau. Comment tirer parti de ce temps ? Pourquoi ne pas en profiter pour renforcer ses compétences ? Il est par exemple possible de se former en ligne à la cybersécurité afin de garder une longueur d'avance sur les menaces. En réaffectant ce gain de temps qu'on ne gaspille plus dans des déplacements parfois interminables, les dirigeants tout comme les collaborateurs peuvent développer un savoir-faire pouvant se révéler particulièrement utile dans le futur.

Perspectives

En mettant l'accent sur ces six points, les entreprises vont pouvoir définir un modèle de télétravail efficace et sécurisé. Ces évolutions associent les infrastructures du cœur de réseau avec des solutions de connectivité tierces pour étendre la périphérie de réseau au-delà du bureau de travail classique. En optant pour une stratégie de cybersécurité pertinente couvrant la périphérie, le cœur de réseau et le cloud, les entreprises assurent la continuité de leurs activités sur leurs sites distants tout en jetant les bases des méthodes de travail et des architectures à venir.