Sécuriser le télétravail dans les institutions publiques

Christophe AUBERGER
Directeur technique
FORTINET

Dans le cadre de la crise que nous traversons, les gouvernements du monde entier se sont concentrés sur la gestion de la transition globale de leurs technologies de l'information à destination de collaborateurs travaillant soudainement tous à distance. La continuité des opérations et la continuité du gouvernement (COOP/COG) sont devenues plus urgentes. Jusqu'alors ils s'étaient surtout attachés à identifier les employés considérés comme "essentiels" ou " critiques pour la mission " et qui devaient continuer à se rendre sur leur lieu de travail habituel ou sur un autre site officiel.

Les gouvernements doivent maintenant trouver le moyen d'assurer la pleine action de leurs équipes pendant une période prolongée, la plupart de ces employés étant souvent à domicile, pour assurer la continuité des opérations gouvernementales.

D'un point de vue informatique, ce défi se décompose en trois éléments :

- Tout d'abord, la sécurité du point d'accès d'un travailleur à distance. Il peut s'agir d'un réseau domestique auquel sont attachés des dispositifs personnels connectés vulnérables. Les membres de la famille qui utilisent des applications, les médias sociaux et les consoles de jeux, introduisent potentiellement des menaces dans le réseau. L'ensemble de cet environnement d'exploitation échappe au contrôle de l'organisation et donne un nouveau sens à l'expression " risque d'initié ". Alors comment isoler l'appareil du travailleur à distance ou, du moins, garantir l'intégrité des données et des opérations gouvernementales sur cet appareil ?

- La sécurité de la transmission ensuite - il s'agit de s'assurer que les données gouvernementales sont cryptées lorsqu'elles circulent sur Internet.

- Enfin, le HQS ou bureau principal. Les réseaux de presque tous ces environnements ont été conçus pour le cas où les employés travaillent à l'intérieur du périmètre du réseau. A-t-il la capacité d'absorber le nombre de connexions nécessaires à leur déplacement vers des sites distants ? Peut-il gérer ces connexions avec un temps de latence acceptable, afin que les utilisateurs ne soient pas frustrés par la lenteur des performances du réseau ? Peut-il garantir que ces connexions sont sécurisées et uniquement accessibles aux utilisateurs autorisés ?

La bande passante est aussi un élément important. Certaines applications nécessitent-elles des niveaux de bande passante inhabituellement élevés ? Quelle peut être l'efficacité de la solution mise en place lorsque les télétravailleurs ont des difficultés à se connecter ? Et même s'ils ont accès, il est important de reconnaître que non seulement les vitesses varient

considérablement, mais que d'autres ressources connectées à un réseau domestique - comme les enfants qui suivent un enseignement à distance - peuvent consommer la bande passante disponible.

Ainsi, l'informatique dématérialisée devient une option particulièrement attrayante. Pour les fonctionnaires, les TIC 3.0 permettent une connexion directe aux ressources basées sur le cloud - plutôt que de devoir faire transiter le trafic par l'agence d'origine - et permettent également l'utilisation de plateformes SaaS (Software as a Service).

En gardant ces considérations à l'esprit, les éléments clés pour un accès à distance sécurisé par un fonctionnaire devraient inclure :

- Un réseau privé virtuel (VPN) dont les points d'extrémité sont l'appareil de l'utilisateur distant et le bureau parent (ou le cloud).
- L'authentification multifactorielle pour garantir que seul l'employé distant autorisé peut accéder au réseau ou aux données de l'employeur.
- La sécurité des points d'extrémité (endpoints) fournie par l'employeur pour garantir la sécurité de l'informatique, des données et des réseaux du gouvernement, même lorsque l'employé travaille à partir d'un réseau domestique vulnérable ou compromis.
- La prévention des pertes de données (DLP) qui fournit un filet de sécurité contre l'exposition par inadvertance de données sensibles, même lorsque les employés travaillent avec des distractions potentielles ou sous des facteurs de stress extraordinaires.
- Le contrôle de la gestion des dispositifs pour répondre aux besoins des organisations qui veulent autoriser - ou peuvent même exiger - des opérations BYOD de la part de leurs employés.

Il existe des solutions commerciales éprouvées qui tiennent compte de tous ces facteurs. Idéalement, du point de vue des frais généraux informatiques, la plupart de ces solutions devraient fonctionner comme un seul système intégré, avec un seul point de gestion. Les organisations qui ont été confrontées à la nécessité d'agir rapidement pour soutenir les populations de travailleurs éloignés ne devraient pas avoir à réinventer la roue, que ce soit en termes de technologies ou de meilleures pratiques requises pour leur adoption.