

Administrateur informatique : règles d'or pour sécuriser vos accès à distance

Lorsque des circonstances inattendues bouleversent les habitudes sociétales comme c'est le cas en ce moment, l'option du télétravail semble être un excellent compromis pour l'activité des entreprises. Toutefois, l'urgence de vouloir déployer au plus vite une organisation de travail à distance peut engendrer des vulnérabilités en matière de cybersécurité. Les cybercriminels l'ont bien compris et profitent précisément de la situation pour commettre leurs forfaits.

☐ Renforcez votre politique de sécurité des mots de passe

C'est le moment de durcir les règles appliquées aux mots de passe. Exigez de très longs mots (voire même mieux : des phrases en guise de mot de passe), imposez des modifications régulières et verrouillez les comptes après la saisie erronée d'un certain nombre de mots de passe. Expliquez aux employés qu'ils ne peuvent pas réutiliser leurs mots de passe professionnels pour leurs comptes personnels.

☐ Instaurez une solution d'authentification multifacteur (MFA)

Également appelée "double authentification" (2FA), il s'agit de la meilleure méthode de défense contre les cybercriminels utilisant toutes sortes de techniques coercitives. Celles-ci peuvent aller du vol d'identifiants de connexion (achetés sur le dark web) à la pulvérisation de mots de passe, tout ceci dans l'optique de se faire passer, ensuite, pour des employés en se connectant au réseau de l'entreprise. Si vous utilisez une messagerie électronique basée sur un réseau ou un cloud, des logiciels de productivité ou d'autres applications, activez la fonction MFA, si celle-ci est disponible. Dans le cas où vos employés auraient besoin d'accéder au réseau interne de l'entreprise, il vous faudra également mettre en place une solution MFA.

☐ Mettez en place une solution VPN pour l'accès au réseau de l'entreprise

Le VPN a pour objectif de chiffrer le trafic de l'entreprise lorsque celui-ci traverse l'Internet dit "public" et empêche donc de potentiels malfaiteurs de mettre la main sur d'éventuelles données. Une connexion VPN possède aussi l'avantage de permettre à l'équipe informatique d'étendre les mesures de sécurité du réseau interne aux appareils distants. Si vous utilisez déjà un service de ce type pour vos employés, assurez-vous d'avoir suffisamment de licences et de capacités pour accueillir de nouveaux utilisateurs.

☐ Utilisez une solution de bureau virtuel, si cela vous est possible

Ce type de solution permet à l'employé d'accéder à une machine virtuelle qui se trouve dans le cloud ou dans votre centre de données et de la contrôler à distance. Sa configuration peut être identique à celle d'un système de bureau classique. Son avantage réside dans le fait que les données ou fichiers sensibles n'existent que sur la machine virtuelle et n'ont pas besoin d'être stockés sur le système domestique de l'employé.

☐ Faites une note aux employés les alertant sur les menaces liées au Wi-Fi et à leur réseau !

Vous n'avez que très peu de pouvoir sur le réseau domestique de chaque employé et les appareils qui y sont connectés. Alors, comme il vaut mieux prévenir que guérir, voici quelques conseils à leur distiller : dans un premier temps, suggérez-leur de désactiver tout partage de fichiers sur le système qu'ils utilisent pour travailler. Puis, dites-leur de vérifier leur routeur personnel ou leur point d'accès Wi-Fi : ils doivent être sécurisés par un accès protégé (WPA2). Enfin, rappelez à vos employés l'importance de ne jamais se connecter sur un Wi-Fi non sécurisé ou ouvert et donc sans clé de sécurité.



☐ Investissez dans une sécurité endpoint complète pour les salariés à distance

Il est difficile d'évaluer la pertinence de l'antivirus de chaque ordinateur domestique et si celui-ci sera en mesure de protéger correctement les données de l'entreprise en cas de télétravail. Une solution complète et robuste avec plusieurs couches de sécurité (notamment un pare-feu personnel, une protection contre les sites malveillants et les malwares localisés sur des disques amovibles ou clés USB) s'avère la meilleure garantie contre toutes sortes de menaces. Notre suite de sécurité endpoint destinée aux entreprises, entièrement administrable à distance par votre service informatique, sera votre meilleure alliée !

☐ Installez le chiffrement pour les employés en contact avec des fichiers sensibles

Dans le cas où vos employés auraient besoin de télécharger des fichiers professionnels sur leurs appareils domestiques, nous vous conseillons de leur fournir une solution de chiffrement. Il est impératif de leur demander de stocker leurs documents personnels séparément de ceux qui concernent l'entreprise, puis de conserver ces derniers dans un dossier, à part, chiffré. En complément, installez une politique pour que les employés enregistrent les documents révisés dans l'espace de données de l'entreprise, de manière à ce que vous n'ayez pas à vous soucier de la sauvegarde à distance.

☐ Formez les employés à se déconnecter

Qu'ils prennent leur pause déjeuner, terminent leur journée de travail ou simplement qu'ils quittent la pièce plus de 5 minutes, formez vos employés à se déconnecter systématiquement du réseau de l'entreprise. Ce principe de base vaut d'ailleurs pour toute connexion

en dehors de chez vous. C'est d'autant plus essentiel si l'ordinateur est partagé ou si d'autres personnes peuvent y avoir accès à la maison.

☐ Faites l'apologie des mises à jour et des correctifs

Indiquez aux salariés distants d'activer les mises à jour automatiques de l'ensemble de leurs appareils de manière à ce que ceux-ci soient en conformité avec les mesures de sécurité. Vérifiez également que votre environnement interne soit aussi à jour, en particulier tout ce qui a trait aux éléments de sécurité critiques potentiellement non corrigés car utilisés 24h/24 et 7j/7. Soyez également particulièrement vigilants concernant les machines domestiques fonctionnant sous Windows 7 qui n'est plus mis à jour. Il serait peut-être préférable en attendant, de simplement bloquer l'accès jusqu'à ce qu'une mise à niveau soit disponible pour cette version.

☐ Réalisez des formations en cybersécurité pour les employés

Vous pouvez déployer tous les efforts et toutes les technologies possibles, un critère reste déterminant pour une cyber-hygiène d'entreprise fiable : vos employés. D'autant qu'actuellement, les arnaques en tout genre fleurissent un peu partout pour piéger les salariés en télétravail : de fausses notifications de l'entreprise pour réclamer des identifiants de connexion, des demandes fictives provenant du patron pour soutirer des paiements ou des transferts d'argent en sont de parfaits exemples. D'où l'importance d'éveiller les salariés et de leur fournir les connaissances nécessaires : des employés vigilants auront bien moins tendance à se laisser piéger par de tels abus. Un programme d'entraînement régulier, surtout en ce moment avec le télétravail, leur permettra de ne pas baisser la garde.

Les clés du succès

Des logiciels de productivité sur le cloud aux outils de discussion, de conférence et de collaboration en ligne, en passant par d'autres technologies d'accès à distance sont autant de moyens d'aider les employés en télétravail à rester aussi productifs qu'au bureau, sinon plus ! Lorsqu'ils décident d'apporter leurs documents et outils professionnels à domicile, assurez-vous de leur transmettre les mesures de cyber-hygiène adaptées à leur situation.

Pour plus d'informations sur les solutions de sécurité ESET, rendez-vous sur notre [PAGE WEB](#) dédiée !

