Comment et pourquoi sécuriser son poste de travail ?

Technologie : *Les changements d'habitudes de travail des salariés n'ont pas échappé aux pirates, dont les attaques redoublent. Le développement du travail à distance oblige les entreprises à repenser leur sécurité et aussi à sensibiliser aux menaces.*

Par APM | Modifié le jeudi 01 avril 2021 à 08:00

Les crises ont souvent du bon pour les pirates. Le premier confinement de 2020 a ainsi déclenché une vague d'attaques visant notamment à exploiter l'isolement des salariés et la Covid. Les menaces prennent en particulier la forme de sites et d'e-mails de phishing, mais aussi de ransomwares. En conséquence, les entreprises ont dû continuer d'investir dans la

sécurité informatique. En 2020, 45 % des entreprises françaises sondées par IDC ont même augmenté leurs dépenses. Pour 46 %, la priorité est de se protéger contre les attaques ciblées.

Cela passe, entre autres, par un renforcement de la sécurisation des terminaux mobiles, qui fait un bond dans la hiérarchie des priorités. Elle se classe désormais en seconde place, à 38 %, contre un sixième rang un an plus tôt. Dans les deux ans à venir, les entreprises se concentreront en outre, à 57 %, sur la sécurité des accès aux applications et pour 48 % sur la protection des comptes à privilèges. Une conséquence directe de l'explosion du télétravail, une pratique amenée à se pérenniser. Mais comment concrètement se prémunir contre ces menaces ?

Des règles d'hygiène IT et des solutions technologiques

TPE et PME ne disposent pas toujours, voire rarement, des compétences internes en cybersécurité. Différents organismes proposent cependant des guides pour les aider à adopter des règles d'hygiène informatique. C'est le cas par exemple de l'Etat, au travers du site Cybermalveillance.gouv.fr, qui livre une série de recommandations à destination des télétravailleurs, mais aussi de leurs employeurs. L'objectif est de couvrir ainsi la sécurité des terminaux, mais aussi des ressources de l'entreprise. Et ces préconisations présentent un atout certain pour les TPE/PME en manque de trésorerie : elles sont peu coûteuses, voire gratuites dans leur mise en œuvre.

Voici les principales recommandations de sécurité à destination des télétravailleurs :

1. Ne mélangez pas usages personnel et professionnel sur le même ordinateur, plus encore si votre employeur vous fournit un terminal. Attention notamment aux sites que vous visitez et aux applications que vous installez. L'activité professionnelle expose en principe à des risques moindres. En séparant ces deux usages, vous réduisez les risques de sécurité, même si un salarié peut recevoir un e-mail de phishing ou un ransomware sur son adresse pro.
2. Installez les mises à jour de sécurité sur vos terminaux. Dans le cas d'un PC professionnel, il est d'ailleurs recommandé de configurer les mises à jour en mode automatique. Cela évitera les interventions des télétravailleurs, et donc les oublis éventuels.
3. Installez et activez un antivirus, voire la protection en temps réel. Ces applications de sécurité doivent en outre être à jour afin de détecter les dernières menaces identifiées par les éditeurs. Il peut être recommandé de procéder à une analyse complète pour s'assurer qu'aucun programme malveillant n'est déjà présent sur le poste. En cas de doute, ne vous connectez pas au réseau de l'entreprise afin d'éviter toute propagation.
4. Sécurisez vos comptes. La compromission des mots de passe menace directement l'entreprise et ses infrastructures et applicatifs. L'utilisation de mots de passe fort, via notamment un générateur de mot de passe, constitue une bonne pratique en l'absence d'authentification forte.
5. Protégez votre accès réseau, notamment Wi-Fi. Une faille dans la protection de l'accès internet peut constituer une porte d'accès au réseau professionnel et aux ressources

stockées sur le terminal. Le Wi-Fi doit donc être sécurisé grâce à une clé robuste et le chiffrement (WPA2) activé.
6. Sauvegardez vos données : face aux attaques, mais aussi aux défaillances logicielles et matérielles, la sauvegarde permet de se prémunir contre une perte de données. Des systèmes comme Windows 10 proposent une sauvegarde automatique dans le cloud. Les données professionnelles peuvent aussi être enregistrées sur un disque externe, un espace de stockage géré par l'employeur ou un service cloud d'entreprise.

L'entreprise chef d'orchestre de la cybersécurité

La responsabilité de la sécurité informatique ne peut cependant pas être totalement déléguée aux collaborateurs de l'entreprise. Les employeurs doivent, eux aussi, participer à la cybersécurité. Comment ?

1. En fournissant autant que possible des terminaux professionnels aux salariés. Ceux-ci seront administrés et sécurisés par l'entreprise. Les ordinateurs personnels ne peuvent garantir un même niveau de sécurité car ils ne sont pas supervisés.
2. En maîtrisant les accès depuis l'extérieur : seuls les accès réellement indispensables doivent être ouverts. Ils doivent néanmoins être contrôlés grâce à du filtrage réseau et un pare-feu. Les accès distants des collaborateurs doivent en outre être sécurisés grâce à une connexion VPN. CyberMalveillance préconise de plus l'application de la double authentification sur ces accès VPN, afin de se protéger des usurpations d'identité.
3. En appliquant une politique de mot de passe à l'échelle de l'entreprise, voire en leur substituant de l'authentification multifacteur pour la connexion aux actifs sensibles ou pour les personnels les plus critiques. Cela comprend notamment les membres du service informatique.
4. En sauvegardant les données. Les sauvegardes, qui doivent être réalisées et testées régulièrement, seront sans doute la seule solution pour rétablir l'activité en cas d'infection par un ransomware. La CNIL recommande de plus le stockage des données des utilisateurs sur un espace de stockage régulièrement sauvegardé accessible via le réseau plutôt qu'une sauvegarde sur les postes de travail.
5. En supervisant et conservant les logs. Tous les équipements d'infrastructure génèrent des données d'activités, des logs. Cette journalisation permettra, en cas d'attaque, d'identifier la cause et les remèdes à apporter. La supervision des accès et systèmes sensibles alertera quant à elle sur une activité anormale, indice possible d'une attaque.
6. En sensibilisant les collaborateurs. Ces derniers ne sont pas des experts des menaces et de la cybersécurité. Ils doivent donc être informés des risques et des moyens de s'en prémunir. L'entreprise doit aussi pouvoir leur apporter une réponse rapide en cas de doute ou d'infection par un malware.