10 astuces pour protéger les travailleurs à distance des cybermenaces

Devolutions

LES ENTREPRISES DOIVENT S'ADAPTER LE PLUS RAPIDEMENT POSSIBLE

Auparavant, les travailleurs à distance - qu'on appelait généralement des télétravailleurs – étaient des exceptions qui suscitaient l'envie chez ceux qui devaient effectuer chaque jour un trajet interminable vers le bureau où ils s'enfermaient de 9 h à 17 h dans un cubicule sans fenêtres.

La situation est radicalement différente aujourd'hui en raison de la pandémie du COVID-19. Les entreprises doivent s'adapter le plus rapidement possible afin de survivre à cette période d'instabilité et de volatilité. Maintenant, les travailleurs à distance ne sont plus seulement une pièce du casse-tête de la main-d'œuvre, ils sont devenus la pièce maîtresse.

Alors que les entreprises prennent tous les moyens pour s'en sortir, les pirates informatiques en profitent pour subtiliser des données. En conséquence, les entreprises et les travailleurs à distance doivent jouer un rôle actif dans la réduction des failles de sécurité et des cybermenaces.

Voici donc 10 astuces qui aident à protéger les travailleurs à distance et qui tiendront les pirates informatiques… à distance!

1. Utiliser des points d'accès WiFi mobiles et/ou des RPV

Les travailleurs à distance adorent les réseaux WiFi publics, car ils sont disponibles presque partout ces jours-ci : cabinets de médecins, aéroports, restaurants, etc. Malheureusement, les pirates informatiques apprécient également les réseaux sans fil publics, parce qu'ils peuvent facilement espionner, hameçonner et usurper des identités.

Pour gérer ce risque, vous pouvez fournir aux travailleurs à distance des points d'accès WiFi mobiles. Si cela est trop coûteux, les travailleurs à distance devraient au moins utiliser un bon réseau privé virtuel (RPV). Bien que les RPV ne soient pas infaillibles, ils sont beaucoup plus sécuritaires que les accès sans fil publics ordinaires. Pour en savoir plus, lisez l'article « Devriez-vous utiliser un RPV? »

2. Segmenter le réseau domestique

De nombreux travailleurs à distance croient à tort que leur réseau domestique est sécurisé, alors qu'il peut être tout aussi vulnérable qu'un réseau WiFi public. L'utilisation d'un RPV (comme indiqué ci-dessus) permet de réduire les risques, mais les travailleurs à distance devraient aller encore plus loin en segmentant leur réseau domestique et en l'isolant derrière un pare-feu de niveau professionnel.

3. Utiliser l'authentification à deux facteurs

L'authentification à deux facteurs est une couche de sécurité supplémentaire qui oblige les travailleurs à distance à vérifier leur identité en fournissant leurs identifiants de connexion, ainsi que d'autres informations qui peuvent être :

- Quelque chose qu'ils savent, comme la réponse à une question secrète, un NIP ou un mot de passe.
- Quelque chose qu'ils ont, comme un téléphone intelligent, un jeton ou une carte de crédit.
- Ce qu'ils sont, par exemple leur empreinte digitale, leur voix ou leurs yeux.

L'idée est que, même si les identifiants de connexion d'un travailleur à distance sont volés, il est peu probable (bien que ce ne soit pas impossible) que les pirates informatiques soient en mesure de fournir les informations supplémentaires et d'accéder à un appareil, une application, un réseau ou un système. Nous recommandons d'ailleurs d'utiliser Devolutions Authenticator, qui prend en charge les textos, les notifications poussées et les courriels.

4. Utiliser un gestionnaire de mots de passe robuste

Pour renforcer la sécurité, les travailleurs à distance (ainsi que les travailleurs internes) doivent utiliser un gestionnaire de mots de passe robuste, tels que Devolutions Password Server ou Devolutions Password Hub, qui offre des fonctionnalités comme la rotation des mots de passe, un générateur de mots de passe puissant, des contrôles automatiques des mots de passe exposés lors de piratages (« pwned ») et des alertes par courriels en temps réel en cas de tentatives d'accès non autorisé. Rappelez-vous : la grande majorité des violations de données sont causées par des informations d'identification volées ou faibles.

5. Installer une solution de sécurité des terminaux

Les solutions de sécurité des terminaux sont une ligne de défense essentielle pour empêcher les pirates informatiques de lancer des attaques contre des appareils pour, ultimement, attaquer des réseaux et des systèmes. Les principaux outils de sécurité des terminaux incluent :

- Pare-feu de réseau (sur les terminaux et les réseaux domestiques)
- Logiciel antivirus
- Logiciel de mise à jour (plus ci-dessous)

Si certaines entreprises ont intérêt à laisser leurs experts TI qui travaillent à distance décider du moment de la mise à jour de leurs logiciels, la bonne pratique à adopter pour les autres utilisateurs consiste à placer des périphériques distants sur une image standard et à activer les mises à jour automatiques pour toutes les applications et tous les programmes, en particulier les logiciels de sécurité.

6. Utiliser un bloqueur de données USB

Si les travailleurs à distance doivent charger leur appareil et que la seule option est une station de chargement USB publique, ils doivent toujours utiliser un bloqueur de données USB. Cela permet aux câbles d'alimentation de se connecter (et la charge de s'effectuer), sans exposer les câbles de données à l'intérieur de l'appareil, ce qui empêche l'échange de données et la protection contre les logiciels malveillants.

7. Utiliser une solution d'accès à distance sécuritaire

En télétravail, il est important que les professionnels des TI aient sécuritairement accès en tout temps aux ressources clés de l'entreprise. Qu'ils doivent mettre à jour les machines du parc informatique ou qu'ils doivent assister les utilisateurs à distance, l'idéal est d'utiliser une solution d'accès à distance complète et rapide à déployer. Wayk Now fait partie de ces solutions abordables, puisqu'elle offre une édition gratuite pour une utilisation personnelle et commerciale.

Si l'entreprise recherche des fonctionnalités avancées, comme l'accès sans surveillance, le lancement de plusieurs sessions en simultané, l'exécution de scripts à distance et l'enregistrement de sessions, l'édition Enterprise répond à leurs besoins et est offerte sous forme d'abonnement à un prix concurrentiel.

Les utilisateurs professionnels pourront également se doter gratuitement de Wayk Den, un serveur centralisé et auto-hébergé sur les serveurs de l'entreprise, pour gérer toutes les machines du parc informatique. Ils peuvent consulter le tableau de bord pour savoir quelles machines sont connectées, des pistes d'audit à des fins de conformité et bien plus. En raison de la COVID-19, un nombre illimité de licences Wayk Now Enterprise est inclus avec toute installation sur site d'un Wayk Den privé pendant six mois.

Différentes solutions d'accès à distance existent, alors voici un aperçu de ce qu'il y a sur le marché.

8. Fournir de la formation continue sur la cybersécurité

Tous les employés ont besoin d'une formation continue en cybersécurité, mais c'est encore plus vrai pour les travailleurs à distance qui peuvent parfois laisser tomber leurs gardes, car on ne leur rappelle pas constamment de suivre les bonnes pratiques (ou pour dire les choses plus clairement, ils ne sont pas trop inquiets de faire face à la colère de l'équipe TI, parce qu'ils ne sont pas au bureau). La formation continue en cybersécurité devrait inclure les aspects suivants :

- Comment reconnaître et éviter les escroqueries en ligne

- Comment choisir des mots de passe et des phrases secrètes forts
- Comment protéger les données à la maison

De plus, les travailleurs à distance doivent être mis en garde contre le partage excessif sur les médias sociaux – les fameux check-ins dans les applications quand ils arrivent dans des hôtels ou des aéroports par exemple – parce que les pirates se servent de ces informations pour traquer leurs victimes. Les travailleurs à distance doivent également garder leurs appareils avec eux et ne jamais les laisser sans surveillance, même pendant quelques secondes. Lorsque vous quittez votre domicile, les appareils doivent toujours être verrouillés et non pas laissés à la vue de cambrioleurs.

9. Passer au stockage en nuage

Stocker des données dans le nuage n'est pas simplement plus pratique pour les travailleurs à distance, il améliore également la protection contre les menaces (comme les rançongiciels). De plus, si un appareil est volé, l'accès aux données en nuage peut être contrôlé en modifiant les mots de passe ou en le verrouillant. Pour en savoir plus, lisez l'article : « **Robust IT Security Comes to the Cloud** ».

10. Utiliser des protecteurs d'écran

Cette technique est peut-être très low tech comparée à certains autres outils de cette liste, mais les protecteurs d'écran sont un moyen très efficace pour empêcher « l'espionnage au-dessus de l'épaule » et le vol des données. Chaque travailleur à distance devrait en avoir un.