Travailler à distance en sécurité : Dix pratiques de base en Cybersécurité pour la finance inclusive, pendant le CoVid-19, et au-delà...

Introduction

La pandémie de CoVid-19 a soudainement conduit de **nombreuses personnes à travailler depuis leur domicile, pour beaucoup pour la première fois, et pour une durée inconnue**. Si le travail à distance à l'avantage de permettre la continuité des activités, il se peut que les infrastructures, les processus, les politiques et la préparation des employés ne soient pas au niveau nécessaire pour faire face à la tendance à de **cyber risques de plus en plus fréquents et graves**.

Le secteur financier est l'une des principales cibles des hackers au niveau mondial. Les pirates sont souvent organisés en réseaux criminels internationaux ; ils disposent de compétences et d'outils avancés et **recherchent de l'argent**. Les institutions d'inclusion financière avec leurs réseaux d'agents importants et des services numériques émergents ont des défenses plus faibles que les grandes institutions. Les **employés et les agents,** qui utilisent les équipements de l'entreprise ou leurs appareils personnels (PC, tablette et Smartphone) depuis une multitude de lieux pour accéder au système bancaire central (CBS), à la gestion des services financiers numériques et à d'autres applications métier critiques, sont d'**excellents vecteurs d'intrusion**.

La **récente recrudescence d'attaques avec de nombreuses escroqueries liées au Covid dans le monde entier** ([1]) ne doit pas masquer le fait que l'inclusion financière doit faire face à un **défi de cyber sécurité de longue durée** avec la prolifération de nombreuses techniques qui peuvent être mélangées : attaques de phishing, documents malveillants, sites web frauduleux, usurpation d'identité d'entités gouvernementales et d'organisations internationales, Ransomware, ingénierie sociale, vente de faux masques, faux dons caritatifs... Si certains incidents peuvent avoir des conséquences limitées aux données ou aux finances des employés, beaucoup peuvent **mettre en danger les institutions elles-mêmes et la protection des clients : pertes financières, vol de données, interruption d'activité, atteinte à la réputation.**

Un comportement exceptionnel des employés sera la première ligne de défense ; ce document vise à partager des pratiques de base de la Cybersécurité faciles et peu coûteuses à mettre en œuvre et qui devraient être **appliquées de manière cohérente pour tous vos appareils.**

1. Sauvegarde régulière

- **Faites une sauvegarde hebdomadaire** de vos documents pour vous protéger contre la perte ou la dissimulation de votre appareil, ainsi que contre la corruption ou le cryptage par un logiciel malveillant.
- La sauvegarde doit inclure **tous vos documents professionnels**, y compris les courriels, les contacts, les photos
- Sauvegarde sur les serveurs de l'entreprise, service de sauvegarde en ligne, disque dur USB ou clé USB.
- Débranchez les supports de sauvegarde mobiles après utilisation et rangez-les séparément de l'appareil dans un endroit sûr.

[1] +667% en quelques semaines, source Barracuda Networks, 26 mars 2020

2. Renforcez vos mots de passe

- **Modifier les mots de passe par défaut** ("0000", "admin", "1234", "password") de tous vos appareils, y compris le code PIN des téléphones portables
- Utilisez des **mots de passe longs et complexes**, de préférence les mots de passe sécurisés recommandés. Les paraphrases sont des alternatives faciles à mémoriser, par exemple "Il est temps de boire ton café, Jean" deviendra "Iet2btc,J".
- **Ne communiquez jamais vos mots de passe à** quiconque, que ce soit par téléphone, par courriel, par le formulaire d'un site web ou par un Post It sur votre écran.
- **Changez régulièrement** les mots de passe
- Utiliser deux facteurs ou l'authentification biométrique chaque fois que cela est possible

✓ **ASTUCE** Le logiciel de gestion des mots de passe Free Password vous aidera dans cette tâche essentielle.

3. Utiliser un logiciel authentique, mis à jour avec la dernière version disponible

- **Vérifiez la version installée** pour chaque appareil (ordinateur portable, tablette, smart phone). Si une version récente n'est pas disponible pour votre appareil, comme c'est souvent le cas pour les anciens Smartphones Android, cessez d'utiliser cet appareil à des fins professionnelles.
- **Utiliser des logiciels authentiques** : les logiciels copiés illégalement sont souvent téléchargés à partir de sites web compromis. Ne téléchargez les logiciels que sur les sites officiels d'éditeurs réputés.
- **Mise à jour systématique vers la dernière version**. Les mises à jour contenant des correctifs de sécurité doivent être installées immédiatement. Vérifiez que "mise à jour automatique" est sélectionnée dans la configuration de votre système.

✓ **ASTUCE** Il existe des équivalents **Open Source** fiables et complets pour la plupart des logiciels, y compris les suites bureautiques (par exemple LibreOffice).

4. Éviter les attaques de phishing

- **Les courriels de phishing** contiennent des **liens vers des sites web compromis ou des documents malveillants** qui activeront des logiciels malveillants si vous cliquez ou les ouvrez, et finiront par voler vos identifiants. Ces courriels présentent généralement les caractéristiques suivantes :
    - **Usurpation d'identité** : le courrier électronique semble avoir été envoyé par une partie de confiance (une banque, un opérateur de réseau, des services gouvernementaux, des organisations caritatives, un transporteur express), tant au niveau de l'adresse électronique de l'expéditeur que de la conception du courrier (logos d'entreprises, texte)
    - **Sens** de **l'urgence :** vous inciter à activer le contenu ("vous avez reçu un prix ou un don", "votre compte est sur le point d'être suspendu", "ventes spéciales", "vérifiez vos données bancaires", "facture urgente", "envoyez de l'argent en urgence à"...).
- **À la réception d'un courrier électronique provenant d'un expéditeur inhabituel ou d'un contenu suspect,** n'ouvrez pas le document joint ou cliquez sur le lien et **supprimez le courrier** immédiatement. En cas de doute
    - **Vérifiez l'adresse de l'expéditeur** : placez le curseur sur le nom de l'expéditeur et l'adresse complète s'affichera (peut varier d'un client de messagerie à l'autre). L'adresse peut être celle d'une personne réelle qui a été compromise, ou une adresse créée dans un but précis, par exemple @paypalinvoice
    - **Vérifiez le contenu** avec votre moteur de recherche, les escroqueries ont souvent été partagées par des cyber-experts, vérifiez l'orthographe.
    - Si le courrier semble être légitime, ne cliquez pas sur le lien mais connectez-vous via votre navigateur en entrant l'adresse complète, par exemple : www.paypal.com.

✓ **ASTUCE** Votre équipe informatique peut vous apporter un **soutien supplémentaire pour les vérifications** et vous indiquer **quoi faire au cas où vous auriez activé par inadvertance un contenu malveillant**.

5. Navigation web sécurisée

- **Évitez les sites ou les applications qui n'ont pas une réputation établie** ; ils sont souvent compromis (jeux, paris, copies de logiciels, téléchargement de musique ou de vidéos, contenus illégaux ou pour adultes).
- Soyez extrêmement **vigilant lorsque vous utilisez des applications de paiement et bancaires,** fixez des limites de crédit peu élevées.
- Évitez les sites web utilisant les protocoles non sécurisés http (https est sécurisé).
- Prenez soin des informations personnelles, professionnelles et de l'identité numérique, y compris les adresses électroniques.

6. Sécurisez votre accès Wi-Fi

- Définissez un **mot de passe fort** pour remplacer le mot de passe par défaut de votre routeur Wi-Fi.
- Activez un **protocole fort (WPA2)** et désactivez le Wi-Fi Protected Setup (WPS).
- Créez un **compte d'invité** pour les invités, les enfants, etc. avec des droits d'accès limités. Ne partagez jamais vos identifiants.
- **Désactivez l'accès à distance au** routeur.
- En voyage : évitez d'utiliser les réseaux Wi-Fi publics, à moins que votre organisation ne fournisse un VPN (Virtual Private Network) pour crypter les communications, utilisez plutôt les hot spots mobiles 3G/4G.

7. Prenez soin de tous vos appareils et données

- **Installez un antivirus et activez les mises à jour automatiques**. Un antivirus ne vous protégera pas de tout, mais c'est une bonne base.
- **Ne laissez jamais un appareil sans surveillance à la** maison, au bureau ou lorsque vous voyagez.
- Veillez à ce que les sessions soient automatiquement clôturées après quelques minutes d'inactivité.
- **N'utilisez pas de clé USB** pour partager des données, mais plutôt un transfert de fichiers sécurisé en ligne.
- **Protégez votre lieu de travail** : vérifiez si quelqu'un ne regarde pas par-dessus votre épaule, n'utilisez jamais les ordinateurs publics.

✓ **ASTUCE** : il existe d'excellents antivirus gratuits.

8. Séparez strictement les utilisations professionnelles et personnelles

- **Les appareils de l'entreprise** doivent être **réservés aux activités professionnelles** et ne doivent pas être utilisés par des membres de la famille.
- **N'installez aucun autre logiciel que ceux prescrits par votre équipe informatique.**
- **Fermer les applications ou le navigateur après utilisation, en** particulier l'accès aux applications professionnelles critiques

9. Vous n'êtes pas seul

- **Contactez votre équipe informatique** pour obtenir de l'aide sur la configuration de vos appareils et l'accès au réseau, pour tout problème ou activité suspecte, ou si vous avez fait une erreur.
- En cas d'incident, **contactez les autorités de Police**.

Du côté de l'entreprise

10. Veillez à mettre en œuvre rapidement les mesures de cyber sécurité de base pour le travail à domicile sécurisé

- **La sensibilisation** est un élément clé de la sécurité des systèmes d'information
- Fournir un **point de contact et un soutien technique aux** employés (accès, sauvegarde, antivirus, logiciels autorisés...)
- Configuration de l'**accès à distance par VPN**
- Mettre en place **un partage de fichiers central avec un fournisseur de services en ligne,** avec une structure de dossiers appropriée, un nommage des documents et des paramètres d'accès
- **Vérifier et limiter les droits d'accès pour** tous les employés, y compris l'équipe informatique
- **Appliquer des correctifs de sécurité** pour corriger les vulnérabilités connues
- **Surveiller de** près les **systèmes et les réseaux pour détecter les** comportements anormaux

À propos de nous :

Suricate Solutions est une **entreprise pionnière en matière de Cybersécurité pour l'inclusion financière,** basée au Luxembourg et au Sénégal, où elle gère le premier centre opérationnel de Cybersécurité pour l'inclusion financière. Elle est la filiale pour l'Afrique d'un des principaux acteurs européens.

Comme les pirates ont aujourd'hui virtuellement accès à n'importe quel système, Suricate s'intéresse tout particulièrement à la sécurité opérationnelle, c'est-à-dire à la capacité de **détecter, de corriger et de récupérer les incidents de Cybersécurité,** et donc de favoriser la cyber-résistance. Un certain nombre de services sont adaptés à l'inclusion financière**, par exemple la supervision de la sécurité, l'analyse des vulnérabilités, les tests de pénétration, les campagnes de sensibilisation, les audits, le conseil et un "diagnostic flash de la Cybersécurité"** pour évaluer la maturité de l'organisation et identifier les actions prioritaires.

Contact : jlperrier (at) suricatesolutions (dot) com