Grzesinski
Thomas

10/10/2023
Mr Fenetre

TP2– Mise en place des bonnes pratiques BYOD

Nouvelle politique pour l'entreprise.

Suite à la récente crise sanitaire, nous serons donc obligé de procédé à un autre type de mode de production qui est le télétravail. Vous pourrez procédé a ce genre de méthode de travaille une fois, par semaine si vous le souhaitez pour protéger vous et votre entourage.

Mais vous serez donc obligatoirement obligé de suivre ces outils mis en place pour garantir la sécurité des données de vous et de votre entreprise.

Vous devez donc pour protéger votre informatique à distance grâce a ses outils suivants :

-**Avoir un ordinateur qui sert que pour l'entreprise** et rien d'autres

- **Utilisez** des logiciel **antivirus** et **anti-malware**

Exemple : **Malwarebytes**

- Assurez-vous que le **système d'exploitation et les logiciels sont toujours à jour avec les derniers correctifs de sécurité**

-**Activez le pare-feu intégré** à votre système d'exploitation ou utilisez un pare-feu tiers comme ZoneAlarm

-**Activez une 2FA** sur les comptes et les applications sensibles pour une sécurité accrue

-**Utilisez un gestionnaire de mots de passe** pour stocker et générer des mots de passe forts

-**Activez le chiffrement de disque complet** sur votre ordinateur pour protéger les données en cas de perte ou de vol

Exemples: **BitLocker** (Windows), **FileVault**(macOS), **VeraCrypt** (multiplateforme)

-**Soyez vigilant envers les courriels suspect** et ne cliquez pas sur des liens pour des pièces jointes non vérifiés

-**Utilisez des Solutions de sécurité de messagerie** si disponibles

-Installez des exetensions anti-pishing danq votre navigateur pour identifier les sites Web malveillants

Exemples : **Netcraft Extension, Avast Online Security**

-**Effectuez régulièrement des sauvegardes** de vos données sur un support externe ou dans le cloud.

Exemples Dropbox, Google Drive, OneDrive

-**Utilisez des outils de suppression sécuriséee** pour effacer définitivement les données sensibles

Exemples : BleachBit (multiplateforme)

-**Évitez de vous connecter à des réseaux Wi-Fi publics non sécurisés** lorsque vous travaillez à distance

-Utilisez des extensions de navigateur pour renforcer la confidentialité en ligne

Exemples PrivacyBadger,HHTPS Everywhere

-**Installez des logiciels ant-spyware pour détecter et supprimer les logiciels malveillants**

Exemple Spybot Search & Destroy, As-Aware

-**Appliquez des mesures de sécurité similaires à vos smartphones et tablettes, y compris le chiffrement et les mises à jours régulières**

-**Formez-vous sur les meilleures pratiques en matière de sécurité informatique et restez informé des dernières menaces**

Voici donc les outils nécessaires et les méthodes a suivre lorsque vous faites du télétravail mais a l'inverse voici une liste des outils et des logiciels qui ne peuvent être présents sur les postes informatiques de votre entreprise

Voici la liste :

-**Les jeux-vidéos**

-**Les logiciels de partage de fichiers peer-to-peer** (P2P), tels que **BitTorrent**, peuvent être utilisés pour le partage de fichier illégal de fichers et peuvent présenter des risques de sécurité

-Les applications de streaming video, comme etflic ou Hulu, peuvent être distrayantes et gourmandes de bande passante

-**Les logiciels de messagerie instantanée personnelle**, qui ne sont pas liés au travail, peuvent poser des risques de sécurité et de confidentialité

-**Les applications de médias sociaux personnelles** peuvent être distrayantes et ne sont pas appropriées pour une utilisation pendant les heurs du travail

-**Limitez l'utilisation de navigateur Web** autres que ceux autorisés par l'entreprise, car ils peuvent poser des risques de sécurité et de conformité

-**Les outils de modifications du système d'exploitation ou du registre tels que les « optimiseurs de système »**, peuvent endommager le système ou causer des problèmes de comptabilités

-**L'utilisation de mineurs de cryptomonnaie ou de portefeuilles de cryptomonnaie non autorisées** peut consommer des ressources informatiques et poser des risques de sécurité

-Tout le logiciel ou outil conçu pour contourner les systèmes de sécurité , y compris les logiciels de pirtage , ne doit jamais être présent sur un poste informatique professionnel

-Les employés doivent s'abstenir d'installer tout logiciel ou application non autorisé par le service de l'entreprise

-Les logiciels qui ne sont plus pris en charge ou qui ne reçoivent plus de mise à jour de sécurité ne devraient pas être utilisées, car ils peuvent présenter des vulnérabilités

-Limitez l'installation d'extensions de navigateurs non essentielles car certaines peuvent poser des risques de sécurité ou de confidentialités.

Durant le télétravail vous allez donc devoir communiquer entre votre poste a domicile et l'entreprise ou bien alors avec d'autres personnes.

Ils existent donc différents logiciel de messagerie et de communication plus sécurisez que les autres.

Voici la liste :

Microsoft Teams (L'une des plus connus et utilisés) est une plateforme de collaboration et de communication intégrée à Microsoft 365. Elle offre des fonctionnalités de messagerie instantanée, d'appels vidéo, de partage de fichiers et de collaboration en temps réel

Sécurité : Microsoft Teams prend en charge le chiffrement de données en transit et au repos, l'authentification à deux facteurs (2FA) et la gestion des droits d'accès aux documents partagés.

slack

Slack est une plateforme de messagerie instantanée et de collaboration d'équipe très populaire. Il permet de créer des canaux de discussion, de partager des fichiers et de se connecter à d'autres outils

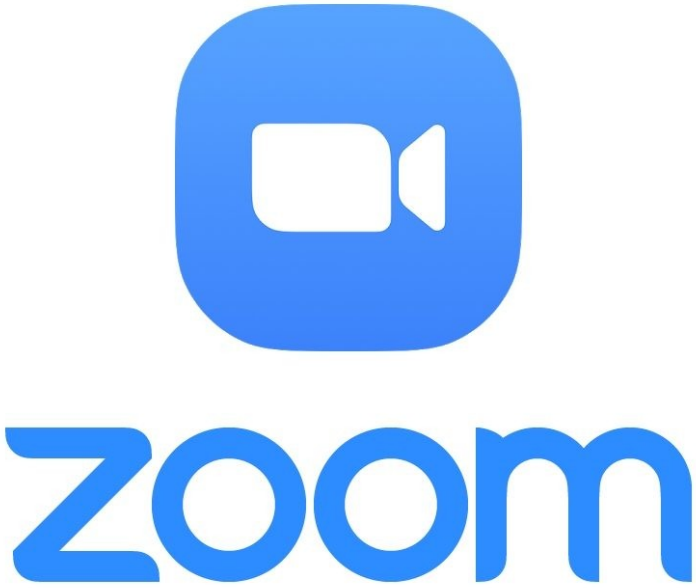
S**écurité : Slack** propose des fonctionnalités de sécurité avancées, notamment la possibilité d'activer la vérification en deux étapes (2FA), de gérer les autorisations d'accès et de chiffrer les données en transit et au repos

Signal est une application de messagerie instantanée open source qui met l'accent sur la sécurité et la confidentialité. Elle offre le chiffrement de bout en bout pour toutes les communications.

Sécurité Signal est largement reconnu pour son niveau élevé de sécurité, et il est recommandé pour les communications confidentielles.

Wire est une plateforme de messagerie sécurisée qui prend en charge les appels vocaux et vidéos cryptés, ainsi que le partage de fichier sécurisé

Sécurité Wire utilise le chiffrement de pour toutes les communications et offre des fonctionnalités de contrôle d'accès aux messages.



Proton Mail est un service de messagerie électronique sécurisé qui propose le chiffrement de bout en bout pour les courriels.

Sécurité ProtonMail protège la confidentialité des courriels et offre des fonctionnalités avancées de sécurité des e-mails, telles que la vérification en deux étapes

Zoom for Business es tune version professionnelle de Zoom, une plateforme de vidéoconférence très utilisée. Elle prend en charge les réunions vidéo sécurisées et les webinaires

Sécurité Zoom propose des fonctionnalités de sécurité, notamment la protection par mot de passe, les salles d'attente virtuelles et le chiffrement de bout en bout pour les appels.

Jitsi Meet est une solution de visioconférence open-source qui permet des appels vidéo sécurisés avec le chiffrement de bout en bout

Sécurité Jitsi Meet est réputé pur son respect de la confidentialité de la sécurité des utilisateurs

Vous vous doutez aussi qu'il existe donc une politique de sécurité des mots de passe sur les postes en informatiques et la voici

-**Les mots de passe doivent contenir au moins huit caractères** et ils doivent inclure une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux(@, !,#$,etc…)

-**Les utilisateurs doivent changer leur mot de passe au moins tous les trois mois** et donc les nouveaux mots de passe ne peuvent pas être identiques aux anciens et les derniers mots de passe ne doivent pas être réutilisé

-**Le verrouillage de compte après un certains nombre spécifiques tentatives de connexion infructueuses**(par exemple, 5 tentatives)

-**L'authentification a deux facteurs est obligatoire**

-**Les mots de passe ne doivent pas être stockés en texte clair**

-**Les utilisateurs doivent être informés des meilleures pratiques en matière de sécurité des mots de passe et de l'importance de ne pas les divulguer**

-**Évites de partagés les comptes**, si c'est nécessaire ils doivent être régulièrement par la direction

-**Les activités liées aux mots de passe**, telles que les modifications et les réinitialisation, doivent être surveillées et auditées régulièrement

-**Une procédure de réponse aux incidents en cas de compromission de mot de passe doit être mis en place**

-**L'accès aux systèmes et aux données doit être immédiatement révoqué lorsque l'employé quitte l'entreprise ou change de rôle**

-**Les utilisateurs sont tenus de garder leurs mot de passe confidentiels et de ne pas les partager avec d'autres personnes**

-**Les données de mots de passe stockées doivent être cryptées** pour éviter toute compromission en cas de violation de sécurité

Donc suite à ces différents outils et la politique des mots de passe vous vous demandez sûrement pourquoi on met en place une politique de BYOD

Tout d'abord **l'avantage** du BYOD c'est aussi la **productivités des employés grâce à la familiarité de vos propres appareils**, cela nous réduits des coûts d'achats et de maintenance des équipement pour l'entreprise, mais aussi il y a donc la flexibilité pour vous les employés de **travailler n'importe ou avec leurs appareils préférés** mais cela engendre aussi des **risques comme la fuite de données sensibles si les appareils personnels ne sont correctement sécurisés** et cela peut mettre en danger vous et la société.

Comme par exemple la sociéte **Target** Corporation en 2013 qui a été victime d'une importante violation de données qui a compromis les informations de millions de cette attaque a été attribuée en partie à un accès non autorisé à travers le réseau de la société via les systèmes de point de vente, qui étaient connectés à des appareils BYOD. Les pirates ont réussi à exploiter des vulnérabilités de sécurité dans ces systèmes pour accéder aux données sensibles des clients. Cette affaire a mis en lumière l'importance de la sécurité dans les environnements BYOD et a incité de nombreuses entreprises à renforcer leurs pratiques de sécurité et de gestion des dispositifs BYOD.

La mise en place et **l'intervention de professionnel en cybersécurité vendra une fois par mois pour vous former sur comment protéger vous et vos appareils quand vous faites du télétravail, des quizz et des questionnaires seront donc imposé aussi par la suite de ces réunions, si vos résultats sont correctes un système de récompense à été mis en place plus vous aurez des résultats bon plus vous monterez en grade. Jusqu'à arrivé au grade Sécurité ou vous pourrez donc aider, et formés les futurs employés de notre entreprise sur le BYOD.**

Des vidéos seront installées dans l'entreprise et diffuseront des rappels, des risques ou des cas d'attaques d'informatiques pour continuer et vous rappeler les dangers du numérique.

On met aussi actuellement en place un système d'équipe technique pour que vous ayez de l'aide dés que vous aurez un souci technique.

LE RÈGLEMENT DU BYOD SERA MIS A JOUR SI BESOIN

Synthèse du BYOD :