TD 2 / Sécuriser un smartphone dans le cadre d'une entreprise

SÉCURISER UN SMARTPHONE PROFESSIONNEL

Aujourd'hui, on peut tout faire avec son téléphone et les salariés peuvent utiliser un smartphone professionnel pour travailler à distance. Que ce soit à usage professionnel ou à usage personnel, sécuriser son smartphone est essentiel.
D'après une étude de CheckPoint Software, 97 % des entreprises dans le monde ont déjà subi une cyberattaque sur leurs smartphones professionnels.

On va d'abord voir les principales menaces pour un smartphone, ensuite les différentes techniques des cybercriminels et enfin comment sécuriser un smartphone professionnel avec des bonnes pratiques et une solution logicielle.

I) Les menaces et techniques

- **Les principales menaces pour un smartphone**

La menace la plus évidente est le vol du smartphone, pour la valeur de l'objet en question.
Ensuite, il y a la perte ou le vol des données. Les applications mobiles corrompues peuvent demander des droits comme la géolocalisation, l'accès à la messagerie ou l'activation du microphone qui peuvent être exploitées par les cybercriminels.
Les hackeurs profitent des problèmes de sécurité des réseaux Wi-Fi publics et peuvent accéder librement au smartphone.

- **Les différentes techniques des cybercriminels**

Le phishing ou hameçonnage consiste à tromper la cible avec un email dont l'objectif est de l'amener à transmettre des informations confidentielles comme des codes d'accès et des mots de passe.

Le malware est un programme informatique qui permet de s'emparer des données contenues dans le smartphone, et d'accéder au réseau de la société.

Le logiciel malveillant ransomware qui crypte le contenu du smartphone et qui interdit l'accès à celui-ci. Le cybercriminel demande le paiement d'une rançon pour décrypter les données et déverrouiller le portable.

L'attaque man in the middle (ou l'homme du milieu) qui intercepte des communications entre deux parties par un élément extérieur.

II) Comment sécuriser un smartphone professionnel

- **Les bonnes pratiques de sécurité**

D'abord, il faut sensibiliser les collaborateurs à la sécurité.

Pour corriger les failles de sécurité, il faut faire les mises à jour du système d'exploitation et des applications.

Installer des applications téléchargées à partir des boutiques officielles d'applications.

Faire attention aux applications et aux données à laquelle elles ont accès, par exemple, que l'application n'ait que l'accès aux données de localisation le temps d'utilisation et pas en dehors.

Gérer les identités numériques avec un contrôle de l'accès à certaines applications si tous les services n'ont pas besoin d'un accès à tout.

Installer une application de sécurité mobile incluant un anti-virus (Avast Mobile, Norton, McAfee)

Installer un VPN qui permet de chiffrer et d'anonymiser vos données.

Pour que les données de la mémoire interne ne soient pas accessibles aux hackers, on peut activer la double authentification et chiffrer son smartphone via les paramètres de l'appareil.

On peut chiffrer les données en mettant un mot de passe pour accéder aux fichiers sensibles.

On peut activer l'effacement à distance si le téléphone est perdu ou volé ou si quelqu'un a pu avoir accès aux données sensibles.

Ne jamais se connecter à des réseaux Wi-Fi publics. Les pirates peuvent facilement attaquer ces réseaux vulnérables et endommager les appareils qui y sont connectés.

Concernant les mots de passe, il faut en employer des complexes et différents pour tous les comptes et penser à les modifier régulièrement.

Utiliser plusieurs boîtes mails dont une privée et une publique

- **Une application MDM (Mobile Device Management)**

C'est une application permettant la gestion de flotte d'appareils mobiles (tablettes, smartphones, ordinateurs portables) effectuée au niveau du service informatique de l'organisation. Grâce aux outils MDM, les entreprises peuvent suivre, surveiller, dépanner et effacer les données de l'appareil en cas de vol, de perte ou d'intrusion détectée.

Les outils MDM ont plusieurs fonctionnalités :

- **Gestion des appareils**
    - Configuration, restriction et maintenance des appareils à distance
    - Double espace de travail personnel et professionnel

- **Gestion des applications**
    - Bloquer ou supprimer des applications et logiciels potentiellement dangereux et malveillants
    - Mettre à jour des applications à distance pour éviter les failles
- **Sécurité des données**
    - Chiffrer les informations confidentielles de l'entreprise
    - Utilisation de mots de passe forts
    - Effacer et contrôler les données à distance
- **Économie de temps et d'argent**
    - Automatisation d'un grand nombre de processus de surveillance

Pour finir, une vidéo explicative de ce que peux faire une solution de Mobile Device Management.
https://www.youtube.com/watch?v=mOB4WV1X16U

III) Conclusion

Pour conclure, sécuriser un smartphone professionnel est impératif dans un environnement où les cybermenaces sont omniprésentes. En suivant les bonnes pratiques de sécurité et en utilisant des solutions de gestion de flotte d'appareils mobiles MDM, les entreprises peuvent protéger efficacement leurs données et assurent un environnement de travail à distance sécurisé pour leurs employés.

SOURCES :

Comment sécuriser son smartphone professionnel - francenum.gouv.fr

Comment sécuriser vos téléphones mobiles professionnels ? (orange.fr)

Les bonnes pratiques pour sécuriser son téléphone mobile professionnel | Prixtel

La sécurité des téléphones portables pour l'entreprise | Everphone

RGPD et smartphones professionnels : quelle sécurité ? (dpo-agency-rgpd.fr)

Smartphones professionnels : comment et pourquoi sécuriser les smartphones de vos collaborateurs ? – Blog (certideal.com)

Sécurité mobile : avez-vous les bons réflexes ? – La Poste Mobile
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/appareils-mobiles

https://fr.wikipedia.org/wiki/Mobile_device_management

https://www.lemagit.fr/definition/Mobile-Device-Management-MDM

https://www.ibm.com/fr-fr/topics/mobile-device-management

https://www.goto.com/fr/resources/what-is-mdm-mobile-device-management-guide

https://www.ipsys.be/news/Les-avantages-du-Mobile-Device-Management#:~:text=La%20MDM%20permet%20aux%20départements,nombre%20de%20processus%20de%20surveillance.

https://www.youtube.com/watch?v=mOB4WV1X16U