PERFORMANCE NUMÉRIQUE
Votre rendez-vous mensuel

Comment sécuriser vos terminaux mobiles ?

Les tablettes et smartphones ont permis aux entreprises de gagner en productivité. Mais l'usage de terminaux mobiles n'est pas sans risque. Selon une étude parue en 2014, 82% des responsables informatiques et des professionnels de la sécurité estiment que le coût induit par les incidents de sécurité mobile est en augmentation[1].

Plusieurs facteurs expliquent ce phénomène. D'abord les terminaux mobiles sont moins bien protégés que les ordinateurs. Les solutions de sécurité qui leur sont destinées restent moins nombreuses et l'installation de pare-feu et d'anti-virus est encore loin d'être systématique. Les utilisateurs sont également moins prudents : vols ou pertes d'appareils restent fréquents. Enfin, la tentation est grande pour les salariés de faire un usage personnel de leur terminal professionnel. Or, la navigation sur des sites infectés, le téléchargement d'applications corrompues ou le branchement d'un appareil mobile sur l'ordinateur familial pour recharger la batterie peuvent mettre en danger la sécurité du système d'information de l'entreprise.

Cette notice explique l'importance de sécuriser un appareil mobile et propose quelques mesures à mettre en place pour y parvenir.

Quels sont les risques ?

Les menaces pèsent à la fois sur les appareils, leurs fonctions et les données qu'ils contiennent.

Elles peuvent avoir des conséquences directes en rendant le terminal hors d'usage (impossibilité de passer des appels, d'envoyer/recevoir des emails…) et indirectes dans le cas d'un usage frauduleux de l'appareil (usurpation des droits sur les fonctions utilisation, du carnet d'adresse…).

> Sur les terminaux mobiles

En premier lieu, un smartphone ou une tablette peuvent être volés. Leur petit format et leur valeur économique en font des cibles de choix pour les pickpockets.

L'utilisateur peut également être une menace pour son propre terminal mobile. La perte ou la casse sont des causes fréquentes de remplacement d'appareils mobiles.

Enfin, il arrive que des dysfonctionnements (de la batterie par exemple) soient à l'origine d'une panne du terminal.

> Sur les fonctions et applications

Les logiciels malveillants ou malwares représentent une des principales menaces pour les fonctions d'un terminal mobile (appel, internet, GPS…) et ses applications.

Introduit via la pièce jointe d'un email ou d'un MMS, une connexion USB à un ordinateur infecté, ou encore le téléchargement d'une application malicieuse, ils peuvent altérer voire supprimer le fonctionnement de l'appareil (impossibilité de passer des appels, applications inutilisables, luminosité défaillante…). De manière plus pernicieuse, un malware peut également être utilisé pour usurper les droits de l'utilisateur (sans qu'il s'en aperçoive immédiatement) : achats en son nom, accès aux applications…

[1] « The impact ok Mobile Devices on Information Security » (Conséquences de l'utilisation des terminaux mobiles sur la sécurité des informations) – Check Point Software technologies, 2014 http://bit.ly/1dMQhs7.

Par ailleurs, en cas de vol du terminal, si l'accès aux applications est libre (mot de passe absent ou mémorisé), tous les services de l'entreprise pourront potentiellement être utilisés (messagerie, extranet, Facebook…).

Une erreur de manipulation ou une panne peuvent également être à l'origine d'une altération ou d'une perte des fonctions ou applications d'un terminal mobile.

> Sur les données

Suite à l'introduction d'un malware dans le smartphone ou la tablette, les données peuvent à la fois être altérées et volées. L'utilisateur ne s'en rend pas aussitôt compte mais son carnet d'adresse, son agenda, les données de l'entreprise (fichiers), ses mots de passe, les messages entrants et sortants et leurs pièces jointes, ou encore ses données personnelles (photos) peuvent être récupérés.

Il est possible que les données soient également supprimées ou endommagées de manière fortuite par l'utilisateur ou à cause d'un dysfonctionnement de l'appareil ou d'un service.

Les avis d'experts divergent à propos de la vulnérabilité des différents systèmes d'exploitation mobiles. Apple et Windows contrôlent d'avantage les applications installées. Android est plus ouvert et donc potentiellement plus vulnérable. Sa domination du marché en fait une cible de choix pour les hackers.

Sécuriser son système d'information

Avant d'assurer la sécurité des terminaux mobiles, il est essentiel de garantir celle du système d'information de l'entreprise.

> Protéger les informations stratégiques

Les informations stratégiques ne doivent pas sortir de l'entreprise : **pas d'envoi par email ou d'enregistrement sur un appareil mobile.** Cette mesure de protection tient avant tout au comportement responsable des utilisateurs. Il est important de faire des rappels réguliers sur les risques potentiels et les bonnes pratiques.

Il est possible de restreindre les droits des utilisateurs sur certaines données mais attention à ne pas entraver leur travail.

> Sécuriser les accès distants

Les serveurs FTP[2] et les services de partage de fichiers sur Internet doivent être utilisés avec prudence car ils peuvent comporter des failles de sécurité.

Le serveur FTP est un espace créé sur le serveur de l'entreprise et accessible par Internet via un identifiant et un mot de passe. C'est une solution de partage de fichiers intéressante mais pas assez étanche pour héberger des données sensibles. Mal configuré, il peut même ouvrir une brèche dans le système d'information de l'entreprise.

Les services de partage de fichiers et les espaces de stockage de données mis à disposition par l'éditeur du système d'exploitation de l'appareil ne sont pas non plus infaillibles. En cas de vol de l'appareil mobile, le compte de l'utilisateur peut être usurpé. La plateforme peut également présenter des failles de sécurité. Enfin, les fichiers peuvent être hébergés ou transiter par un pays où les règles sur la confidentialité des données sont moins élaborées (pays blacklistés par la CNIL) ou qui autorisent les autorités locales à un droit de regard.

Les données accessibles à distance ne doivent pas présenter un caractère stratégique pour l'entreprise comme un fichier clients, des données comptables, des plans…

Sécuriser les terminaux

> Authentification

L'appareil, les applications liées à l'entreprise et les données doivent être protégés par un système d'authentification.

L'accès à l'appareil

Il ne s'agit pas nécessairement de faire d'un terminal mobile un coffre-fort. Des règles simples peuvent simplement être observées : mise en place d'un code PIN (autres que 0000 ou 1234) ou changer celui par défaut, mise en veille automatique au bout de 5 minutes, tentatives de déverrouillage limitées…

Si l'appareil est perdu et retrouvé par un individu lambda, une simple protection le découragera de passer des appels ou d'utiliser les applications.

L'accès aux fonctions

Un système d'authentification est également fortement recommandé dans le cas où le terminal dispose d'applications métiers ou permettant d'accéder à des informations de l'entreprise (solutions de partage de fichiers).

Les mots de passe trop évidents devront évidemment être évités. Privilégier au moins 8 caractères mélangeant majuscules, minuscules et chiffres.

L'accès aux données

Encore une fois, il est fortement déconseillé de stocker des informations stratégiques sur un terminal mobile.

[2] FTP : L'espace créé sur le serveur est communément appelé « serveur FTP » car il utilise un protocole nommé FTP pour File Transfer Protocol (protocole de transfert de fichiers).

Si cela s'avère impératif, les données doivent absolument être chiffrées grâce aux fonctionnalités de chiffrement proposées par le terminal ou via une application téléchargée.

Il est préférable que la flotte d'appareils mobiles de l'entreprise soit homogène afin de faciliter leur sécurisation (même version d'antivirus, même processus de sauvegarde...).

> Blocage et effacement à distance

En cas de vol ou de perte d'une tablette ou d'un smartphone, il est préférable de verrouiller son accès afin d'éviter une utilisation frauduleuse. Les données peuvent également être supprimées à distance (le terminal est remis à zéro, comme s'il sortait de l'usine) si l'appareil contient toujours la carte SIM (souvent retirée rapidement par les voleurs). En outre, même s'il s'agit d'un équipement professionnel, il convient également de s'assurer du consentement de l'utilisateur avant de procéder à un effacement à distance.

Selon les modèles, il convient au préalable de télécharger une application spéciale ou de paramétrer les options de l'appareil.

Le GPS peut aussi être utilisé pour localiser le terminal.

> Sauvegardes

Les données d'un terminal mobile sont le plus souvent sauvegardées sur un ordinateur ou un espace virtuel mis à disposition par l'éditeur du système d'exploitation. Il s'agit en fait d'une copie des données mise à jour à une fréquence variable. Cette actualisation des informations copiées du terminal vers le deuxième support s'appelle la « synchronisation ».

L'opération inverse est réalisée lorsque l'utilisateur souhaite importer ses données sur un nouvel appareil (synchronisation du deuxième support vers le terminal).

Les entreprises disposant d'un parc de terminaux mobiles important et homogène peuvent avoir recours à des solutions de gestion dédiées appelées MDM (Mobile Device Management). Ces logiciels permettent de gérer le code d'accès sur le terminal, de bloquer son utilisation et d'effacer les données à distance, ou encore de sécuriser la navigation web et l'accès aux données de l'entreprise.
Des solutions destinées aux PME commencent à voir le jour. Avec le rachat par Google d'une start-up spécialisée dans la sécurité des terminaux mobiles en 2014, le MDM pourrait s'ouvrir un peu plus aux petites structures.

> Connexions automatiques aux réseaux

Il est préférable de désactiver la connexion automatique aux wifis publics afin que les terminaux ne se connectent pas à n'importe quel réseau. De même, il est conseillé de ne pas activer le bluetooth pour éviter toute connexion avec un appareil mobile inconnu.

> Mise à jour de l'os et des applications

Le système d'exploitation du terminal mobile et les applications doivent être mis à jour. Les actualisations permettent d'améliorer les fonctions mais aussi de corriger les failles de sécurité.

> Autorisation d'accès aux applications

Il convient de rester vigilant lors de l'installation d'une application. Certaines réclament un accès très large aux données du terminal : carnet d'adresse, géolocalisation…

Ces données sont en général utilisées à des fins publicitaires.

> Firewall et anti-virus

Les appareils mobiles doivent être protégés de la même manière qu'un ordinateur avec, a minima, un pare-feu (firewall) qui contrôle les entrées et sorties des données, et un antivirus qui bloque les logiciels malveillants.

Ces outils sont disponibles sur les plateformes de téléchargement d'applications. Les solutions payantes offrent parfois plus de fonctionnalités que celles qui sont gratuites. L'écart de prix se justifie parfois par la notoriété de l'éditeur dans le domaine de la sécurité (sur ordinateur principalement).

Certaines de ces applications proposent une fonction de contrôle des applications avant leur installation sur le terminal.

Sensibiliser les utilisateurs

Dernier volet de la sécurisation des terminaux mobiles, la maîtrise du facteur humain.

L'utilisateur est à la fois une menace (il peut être à l'origine de pannes ou d'erreurs) et une vulnérabilité (inattention exploitée par un voleur, crédulité utilisée par un malware).

Notes, affichage, rappels réguliers, charte informatique, guide de bonnes pratiques dédié au nomadisme… Les actions de sensibilisation doivent être constantes pour être intégrées par les utilisateurs.

Une liste de bonnes pratiques peut ainsi être communiquée régulièrement :

- Eviter d'utiliser des réseaux sans fil publics notamment dans les lieux très fréquentés (donner la possibilité aux salariés de se connecter en 3G si Internet leur est indispensable pour travailler)
- Ne pas stocker de données sensibles sur le terminal (téléchargement de documents, emails importants…)
- Télécharger des applications uniquement sur des plateformes officielles
- Télécharger des applications reconnues et mises à jour
- Utiliser des mots de passe longs incluant chiffres, lettres, majuscules, minuscules et caractères spéciaux
- Ne pas laisser le terminal dans les mains de ses proches
- Rester vigilant lors de déplacements professionnels
- …

Votre prochain rdv numérique :
« Améliorer l'ergonomie mobile de son site grâce au responsive design »

VOTRE CONTACT

Samuel COSTE

05 53 35 80 31 - 06 20 42 97 58
s.coste@dordogne.cci.fr
www.dordogne.cci.fr

CCI DORDOGNE