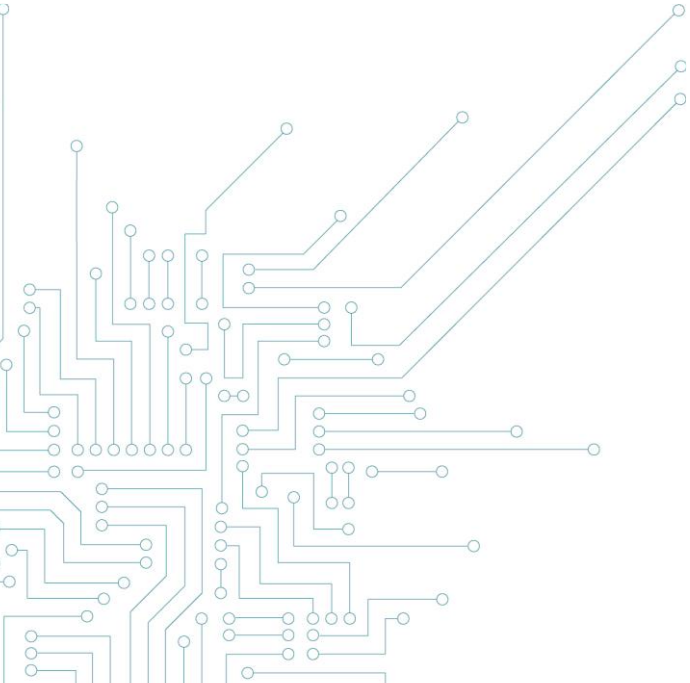
CENTRE FOR CYBER SECURITY BELGIUM

UNDER THE AUTHORITY OF THE PRIME MINISTER

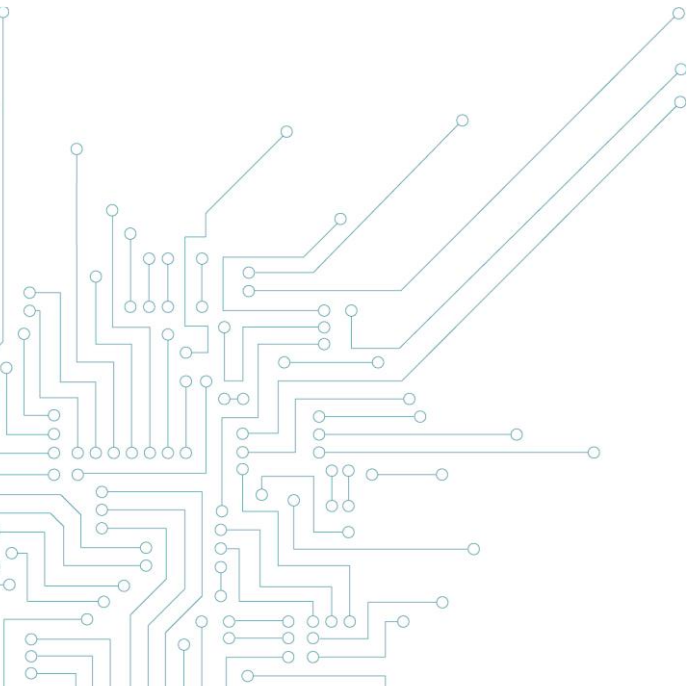
.be

Comment garder le contrôle de vos appareils mobiles ?



Avril 2023

Table des matières



1 Introduction

Il est plus facile de garantir la protection de l'environnement et des données d'une entreprise sur place, mais les utilisateurs finaux peuvent également accéder aux données sur leurs appareils mobiles et parfois personnels, et éventuellement en conserver des copies.

Par « appareil mobile », l'on entend tout actif autorisé à accéder au réseau et aux ressources de l'organisation depuis l'extérieur, et donc à la fois les ordinateurs portables et les smartphones. Les ordinateurs portables sont toutefois généralement fournis par l'entreprise et sont donc inclus dans la stratégie de sécurité, configurés et renforcés par le service IT avant d'être remis au travailleur.

Cet article se concentrera donc principalement sur les smartphones, professionnels ou personnels, utilisés par les employés. Ces appareils et leurs dispositifs connectés (montres, etc.) sont une porte ouverte sur le monde entier, notamment via les réseaux sociaux. Ils hébergent des données personnelles, professionnelles ou confidentielles importantes.

Que vous soyez un simple citoyen, employé dans un secteur critique, ministre, militaire, etc., les données collectées doivent être soigneusement protégées. Il s'agit notamment de votre localisation, de vos données biométriques et de vos habitudes. Ces informations sont précieuses et risquent de faire l'objet de fuites involontaires ou d'espionnage, que ce soit de la part d'entreprises privées, de concurrents, de pays étrangers ou de criminels.

Les problèmes de sécurité des données ne sont pas seulement techniques et ne dépendent pas toujours directement de l'utilisateur. Ils peuvent également découler de la législation du pays où les données sont hébergées. En effet, la législation de certains pays autorise le gouvernement à consulter les données échangées et stockées pour les comptes d'utilisateurs. Il pourrait aussi bien s'agir d'une solution cloud qui synchronise automatiquement les données que des publications des utilisateurs sur les réseaux sociaux.

Si vous êtes une autorité publique ou si vous pouvez personnellement représenter un risque en raison de votre position ou de vos connaissances, il convient de miser sur votre protection même dans un contexte privé et, au moins, de séparer complètement votre vie numérique personnelle et professionnelle. De plus, il serait intéressant de limiter de manière générale les données personnelles que vous partagez sur les réseaux sociaux. Elles pourraient être utilisées contre vous ou contre votre entourage pour vous atteindre.

Dans cet article, nous aborderons les meilleures pratiques et les technologies impliquées dans les technologies de Mobile Device Management (MDM) sur les appareils mobiles. Celles-ci visent à protéger les données qui compromettent la sécurité du réseau de l'entreprise ainsi que les données personnelles.
Aujourd'hui, la plupart des solutions MDM incluent la DLP. Nous évoquerons donc l'intégration des appareils mobiles avec des solutions MDM.

2 Politique de gestion des appareils

La première étape consistera pour l'organisation à définir quels sont les risques. Comme indiqué dans l'introduction, la situation variera en fonction de vous-même, de la taille de l'entreprise, de la criticité du secteur, des capacités des concurrents, bref : de votre valeur et de la valeur des données que vous protégez.

Dans la plupart des cas, la politique de l'organisation en matière de device provisioning sera l'une des suivantes:

- Corporate-owned device : l'appareil est acheté et configuré par l'organisation.

- Bring Your Own Device (BYOD) : les outils et accès de l'organisation sont configurés sur l'appareil de l'employé.

La meilleure approche consistera en un équilibre entre la sécurité et le confort de travail des employés. Restreindre les accès au maximum est une solution plus sûre, mais elle compliquera la vie des employés et sera peut-être contre-productive.
Si les employés sont autorisés à utiliser leurs appareils personnels (peut-être pour des raisons financières pour l'organisation), il est normal qu'ils restent propriétaires de leur matériel et qu'ils conservent des autorisations suffisantes.

Dans une situation BYOD, l'appareil reste la propriété de l'utilisateur, et non de l'organisation. Cela complique quelque peu la tâche du service IT en matière de sécurité.

Les situations Corporate owned sont plus claires. Le service IT peut mettre en place toutes les restrictions qu'il souhaite, par exemple supprimer l'accès administratif à l'appareil, choisir les applications installées, restreindre l'accès aux ressources en fonction de l'emplacement, bloquer les synchronisations avec des fournisseurs externes, ainsi que toutes les politiques nécessaires pour empêcher les actions non désirées.
Mais est-il possible d'instaurer de telles mesures sur des appareils personnels ? Nous tenterons de répondre à cette question dans la suite de cet article.

3 Configuration de sécurité minimale

Lorsque vous traitez des données, vous devez toujours vous assurer que la personne qui y accède est identifiée et qu'elle dispose de privilèges suffisants. Il convient également de garantir que le canal par lequel les données transitent ne peut pas être lu par quelqu'un d'autre, et que les données ne seront pas lues par un tiers durant leur stockage. Ces trois principes garantissent l'intégrité, la confidentialité et l'authenticité.

Suivant ceux-ci, tout appareil mobile qui accède à des informations professionnelles ou les stocke doit au moins :

- être configuré pour l'identification des utilisateurs et l'authentification forte (mot de passe fort, MFA),
- être crypté,
- être équipé d'un logiciel anti-malware à jour (voire d'un EDR qui détectera également les comportements anormaux plutôt que seulement les signatures connues),
- et utiliser un virtual private networking (VPN) pour accéder au réseau de l'entreprise.

Intune offre déjà de nombreuses possibilités pour un environnement d'entreprise Microsoft, le cas le plus fréquent. La solution peut également gérer des appareils IOS si les employés possèdent à la fois des appareils Android et IOS.

4 Renforcement des appareils mobiles

Les mesures suivantes doivent être prises pour améliorer la sécurité des appareils et des données :

- L'appareil est enregistré via une solution MDM,
- Des sauvegardes sont effectuées régulièrement,
- Formation des utilisateurs à la Data Loss Prevention et aux meilleures pratiques en la matière,
- Une classification des données est organisée (le labelling et la classification sont deux concepts différents),
- Les politiques relatives à la gestion, à la classification et à l'utilisation des données sont élaborées et expliquées au niveau de l'organisation (la norme de classification des données doit être incorporée dans la politique de sécurité globale de votre organisation),
- Un logiciel DLP mobile surveille les utilisateurs mobiles, même si ce type de logiciel est désormais souvent inclus dans les solutions MDM.

5 Solutions anti-malware

Aujourd'hui, le principal système d'exploitation mobile, Android, propose un système de sandboxing pour les applications. Cela signifie que, par défaut, les applications ne peuvent pas interagir entre elles et ont un accès limité au système d'exploitation.
Les applications d'entreprise peuvent ainsi cohabiter avec les applications personnelles tout en garantissant une séparation stricte. Vous pouvez par exemple télécharger deux versions de votre application de messagerie préférée, l'une professionnelle et l'autre personnelle, avec des listes de contacts et un historique distincts.

Les systèmes IOS garantissent une séparation encore plus marquée et limitent considérablement les interactions entre les applications sans le consentement de l'utilisateur. Les logiciels antivirus fonctionnent donc difficilement dans des environnements IOS, car ils ne peuvent pas analyser les actions des autres applications.

En outre, de nombreuses menaces nécessitant auparavant l'utilisation de logiciels malveillants tiers sont aujourd'hui prises en charge par défaut lorsque le système d'exploitation est configuré correctement. Cela concerne aussi bien les smartphones que les ordinateurs portables. Mais même si la sécurité anti-malware intégrée est performante, n'oubliez pas qu'elle doit être mise à jour à tout moment. Les mises à jour des applications et du système d'exploitation peuvent être automatiques, mais celles envoyées par les fabricants peuvent nécessiter une intervention manuelle.

6 Mobile Device Management

Adopter une politique de gestion des appareils appropriée et claire est le premier pas vers la réussite.
Des outils vous aideront ensuite à atteindre vos objectifs et à garder le contrôle de vos appareils mobiles.
Attention, ajouter une couche de protection supplémentaire nécessitera du temps et du personnel pour la gérer (application des correctifs de sécurité, des mises à jour, test de nouvelles marques, etc.).

De nombreux fournisseurs mettent sur le marché différentes solutions Mobile Device Management (MDM).
Chaque actif est enregistré dans le dispositif MDM avant d'être remis à l'employé.
L'appareil est alors gérable à distance par le service IT, ce qui améliore considérablement le processus d'intégration et le temps de maintenance.

Ces solutions permettent de disposer d'un inventaire actualisé de vos actifs, de gérer les applications qu'ils contiennent, de les surveiller, de les effacer, de les localiser et d'appliquer des politiques comme la MFA, le cryptage, l'obligation de se connecter à l'environnement de l'entreprise via un VPN et d'opter pour un mot de passe fort, la détection de l'exfiltration des données, etc. Voici les principales caractéristiques d'une bonne gestion d'une flotte d'appareils mobiles.

Il existe deux grandes façons de gérer les appareils mobiles à l'aide d'une solution MDM. La première est d'isoler complètement l'appareil. La seconde consiste à créer deux environnements distincts et isolés sur le même appareil. Cette dernière solution est la plus difficile à mettre en œuvre et peut parfois se révéler lourde pour le matériel.

Les failles de sécurité proviendront principalement de l'installation d'applications malveillantes auxquelles l'utilisateur donnera des droits d'accès au stockage, ou d'applications légitimes dont la gestion des données en arrière-plan n'est pas contrôlée.
Dans les deux cas, la solution MDM donnera au département IT le droit de sélectionner efficacement les applications approuvées en matière de sécurité des appareils et de gestion des données. Les critères de sélection reposeront à la fois sur les besoins de l'entreprise et sur des tests de sécurité de l'application.

Voici quelques-unes des solutions MDM les plus courantes :

- Ivanti MobileIron
- VMWare Workspace ONE
- BlackBerry Unified Endpoint Management
- Microsoft Intune
- Citrix Endpoint Management
- IBM MaaS360
- Cisco Meraki
- Kandji (pour IOS)
- etc.

7 Quelles mesures pour une gestion efficace des appareils mobiles (Checklist) ?

7.1 Les ingrédients d'un bon contrôle des appareils mobiles...

- Définir une liste acceptable d'appareils et de plateformes mobiles autorisés à se connecter au(x) réseau(x) de l'entreprise.
- Adopter une norme de sécurité mobile qui définit les exigences et les bases de configuration pour les appareils et les plateformes mobiles.
- Signaler, suivre et gérer les pertes ou les vols d'appareils au moyen d'un processus standard et d'une solution MDM.
- Déployer une plateforme centralisée de gestion des appareils mobiles et l'utiliser pour contrôler et suivre l'utilisation des appareils, les configurations, etc. et effectuer des contrôles d'intégrité (jail break detection, etc.) avant d'autoriser l'accès aux ressources internes.
- Définir un ensemble de permissions d'accès et de méthodes de configuration pour les appareils BYOD et les intégrer à la solution MDM.
- Ne donner l'accès aux données et applications confidentielles sur les appareils mobiles que via un sandbox sécurisé et isolé ou un container sécurisé.
- S'assurer que les appareils mobiles mettent en œuvre des cas d'utilisation DLP (data loss prevention) de base, tels que la surveillance et l'alerte, et sont intégrés à l'infrastructure SIEM de l'entreprise à des fins de surveillance.
- S'assurer que les appareils BYOD mettent en œuvre des niveaux de restriction et de contrôle de sécurité identiques ou supérieurs à ceux des appareils mobiles appartenant à l'entreprise.

7.2 Les appareils doivent être cryptés

- Tous les appareils présentent des capacités de cryptage fortes lors du stockage et de la transmission.
- Des technologies de chiffrement intégral des disques sont mises en œuvre (BitLocker dans Windows, Filevault dans MacOS, par ex.) avec une authentification pre-boot.
- Des algorithmes approuvés par les FIPS (U.S. Federal Information Processing Standards), tels que l'AES, ou des normes industrielles équivalentes, sont mis en œuvre.
- Les normes de cryptage sont personnalisées et ajustées en fonction de la criticité de l'appareil et des données qui y sont stockées.

7.3 Les appareils mobiles doivent être configurés et renforcés correctement

- Des contrôles doivent être mis en œuvre pour empêcher toute modification non autorisée des configurations et des bases de référence.
- Il convient également d'établir et de publier des normes de configuration sécurisée ou de renforcement pour toutes les plateformes technologiques, y compris les plateformes mobiles telles que iOS, Android, etc.
- Les utilisateurs finaux n'ont pas de privilèges d'administrateur sur leur terminal.

- Des correctifs sont régulièrement apportés aux systèmes d'exploitation ou aux applications des appareils.
- Les appareils ne disposant pas des derniers correctifs de sécurité doivent être mis en quarantaine et corrigés avant d'être connectés au réseau.
- Les images et les normes de référence/de construction sont examinées et mises à jour périodiquement.
- Des outils automatisés sont utilisés pour détecter les écarts par rapport aux normes de configuration de la sécurité, et des mesures correctives sont prises en temps utile pour combler ces écarts.

7.4 Vous devez installer une détection host-based, comme un logiciel anti-malware

Vous trouverez des informations utiles et complètes dans notre article sur le sujet : https://cert.be/en/paper/recommendations-anti-virus-edr-and-xdr-security-solutions

7.5 Vous devez assurer le suivi des appareils mobiles et des logiciels

- Il existe un inventaire centralisé de tous les logiciels et appareils autorisés et non autorisés, qui contient des informations appropriées sur les actifs (propriétaire, criticité, etc.).
- Il convient de revoir et de corriger l'inventaire des actifs au moins une fois par an.

7.6 Vous devez mettre en place un suivi de la propriété et du cycle de vie des appareils mobiles

- Les appareils critiques doivent être surveillés dans l'ensemble de l'organisation et ont un propriétaire défini.
- Les appareils, y compris le matériel et les logiciels, sont surveillés tout au long de leur cycle de vie, de l'acquisition à la mise au rebut, et tous les changements de propriétaire sont signalés.
- Un processus de gestion des changements est élaboré afin d'assurer les demandes et acceptations de modifications relatives aux appareils tout au long de leur cycle de vie.
- Suivi automatisé des actifs grâce à l'inventaire des actifs.

7.7 Vous devez étiqueter et examiner vos appareils mobiles

- Les appareils sont étiquetés avec la classification de sécurité appropriée.
- Les appareils sont réexaminés périodiquement et réétiquetés lors des changements d'actifs.

Sources :

- Lindros, E. T. K. (2023, 4 février). *5 Ways to Prevent Data Loss in Mobile Environments*. CIO. https://www.cio.com/article/288235/mobile-security-5-ways-to-prevent-data-loss-in-mobile-environments.html
- Geekflare. (2021, 25 septembre). *8 meilleures solutions de prévention des pertes de données qui pourraient vous faire économiser des millions*. https://geekflare.com/fr/data-loss-prevention-solutions/
- Desai, P. (2023, 7 mars). *Step-by-Step New Windows Autopilot Setup Guide [2023]*. Prajwal Desai. https://www.prajwaldesai.com/new-windows-autopilot-setup-guide/
- *Antivirus and other security software. (n.d.).* https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/antivirus-and-other-security-software