RSSI & MOBILITÉ

La checklist pour lancer la sécurisation de votre flotte !

www.samsung.com

POURQUOI UN EBOOK SUR LA SÉCURITÉ MOBILE ?

Virus, vers, chevaux de Troie, sites malveillants, applications néfastes, *phishing, spywares, malwares*, pertes, vols ou endommagements d'appareils mobiles... La liste des menaces potentielles pesant sur les smartphones et les tablettes est longue et les risques économiques sont bien réels. 68 % des entreprises présentent une faille de sécurité et 58 % d'entre elles ne pensent pas pouvoir se remettre d'une cyberattaque[1].

Pourtant, la plupart des mobinautes ne mesurent pas les dangers qu'ils font courir au SI et aux données de l'entreprise. Avec l'adoption grandissante des terminaux mobiles dans l'environnement professionnel, leur sécurisation s'impose comme cruciale et pressante. Le sujet est vaste, complexe et parfois sensible.

Voilà pourquoi nous vous proposons un guide 100 % pratique. De la mobilité de vos collaborateurs jusqu'au cadre légal entourant la sécurité des données professionnelles, en passant par les fonctions clés des solutions de gestion d'une flotte mobile... Tout est passé au crible.

Cet ebook complet permet aux responsables de la sécurité de comprendre de bout en bout les enjeux de la gestion de la flotte mobile, afin de lancer sereinement le déploiement d'un projet de sécurisation. Bien sûr, nos équipes d'experts seront heureuses de vous apporter des réponses complémentaires, adaptées à votre entreprise, vos métiers et vos problématiques.

[1] Présentation Samsung Atelier Assises 2016

Bonne lecture !

Vous vous lancez dans un projet ?

CONTACTEZ NOS EXPERTS ›

SOMMAIRE

1

PROTÉGER SA FLOTTE MOBILE : OUI, MAIS POURQUOI ?

En quelques années, les usages mobiles se sont généralisés dans l'environnement professionnel : 80 %[2] des employés réalisent aujourd'hui une partie de leur travail en dehors du bureau. Même si l'utilisation des smartphones et tablettes améliore la productivité et constitue un facteur de satisfaction pour les collaborateurs, des failles de sécurité majeures menacent les entreprises. La sécurisation des appareils est donc une question hautement sensible et stratégique pour toute organisation. Il revient à chaque RSSI d'en connaître les tenants et les aboutissants.

[2] http://ideas.microsoft.fr/mobilite-france-chiffres-teletravail-byod-applications-metiers/#LYOvfZx2iyMhY1M9.97

PROTÉGER SA FLOTTE MOBILE : OUI, MAIS POURQUOI ?

POUR ÉVITER LES FUITES OU PERTES DE DONNÉES

Sans mesures de protection adaptées, les risques de pertes de données sont élevés. Des informations vitales pour l'entreprise (commandes, factures, renseignements sensibles sur les clients et les collaborateurs, etc.) sont menacées. La prise de conscience de cet enjeu est plus que jamais indispensable quand on sait qu' **en 2014, 74 %[3] des entreprises françaises déclaraient ne pas avoir fait installer d'antivirus sur les appareils mobiles de leurs salariés.**

POUR SE PRÉMUNIR DES *MALWARES*

Les actes de malveillance, cyberattaques, erreurs humaines, pertes, vols, et autres dégradations. sont des sources potentielles d'incidents. Les appareils mobiles sont également exposés aux *malwares* transmis via Bluetooth ou lors de connexions à des réseaux WiFi publics non protégés. Le téléchargement d'applications est aussi à sécuriser : au cours des 6 derniers mois de l'année 2015, près de **37 millions de *malwares* mobiles ont ainsi été identifiés sur les *app stores* de Google Play et d'Apple4.**

POUR MINIMISER LES RISQUES DE BAISSE DE PRODUCTIVITÉ

Le fait d'investir dans la sécurité mobile permet de prévenir des dommages économiques notables, liés à la fois à la perte de données essentielles d'un point de vue commercial, à l'interruption des systèmes d'information et de communication ou encore à la contamination des applications métier, **entraînant une baisse de performance voire l'impossibilité pour les collaborateurs de travailler.** Certaines solutions de gestion de la sécurité mobile vous permettent par ailleurs de pousser les mises à jour – de sécurité ou liées à des applications métier – de manière rapide sur l'ensemble des mobiles de vos collaborateurs : plus de perte de temps !

POUR RÉPONDRE AUX EXIGENCES LÉGALES

La sécurisation des données sensibles est un impératif légal. Avec **l'article 34 de la Loi informatique et libertés,** la CNIL (Commission nationale de l'informatique et des libertés) impose aux entreprises françaises de se donner les moyens de les protéger. Elle peut d'ailleurs sanctionner les entreprises qui ne prennent pas les mesures nécessaires (en 2015, elle a effectué 510 contrôles, 93 mises en demeure et prononcé 10 sanctions[5]).

[3] https://clusif.fr/publications/menaces-informatiques-et-pratiques-de-securite-en-france-edition-2016-support-de-conference/

[4] http://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf

[5] https://www.cnil.fr/sites/default/files/atoms/files/cnil-36e_rapport_annuel_2015_0.pdf

SÉCURITÉ MOBILE :
5 conseils pour une veille efficace

1. **Se poser les bonnes questions pour commencer sa veille**
(objectifs, moyens, etc.)

2. **Choisir des outils efficaces pour collecter l'info :**
réseaux sociaux, forums et agrégateurs de flux

3. **Consulter les sites de références**
(CNIL, ANSSI, CLUSIF, etc.)

4. **Participer aux évènements spécialisés**
pour suivre les évolutions technologiques

5. **Remonter systématiquement jusqu'aux informations**
données par les constructeurs.

Vous voulez en savoir plus ?

Lisez notre article complet sur les bonnes pratiques de veille !

LIRE L'ARTICLE ›

2

BIEN PRÉPARER LE DÉPLOIEMENT DE SON PROJET DE SÉCURISATION

Avant de se lancer dans le déploiement de la sécurité mobile, un état des lieux général s'impose. Il s'agit de faire le point sur la stratégie actuelle de l'entreprise en matière de protection et d'identifier les menaces potentielles, à court et à long terme. Quelle que soit la taille de l'organisation (PME ou grandes entreprises), la préparation du projet de sécurisation ne s'improvise pas. Voici quelques éléments clés à retenir.

BIEN PRÉPARER LE DÉPLOIEMENT DE SON PROJET DE SÉCURISATION

◯ DÉFINIR LES CONTOURS DU PROJET

Comme dans tout projet, il s'agit d'analyser les besoins réels. L'élaboration d'un cahier des charges est ici incontournable. Celui-ci définit le périmètre du projet : gestion basique de la flotte ou sécurisation avancée. **Pour une grande entreprise déclarée OIV (Opérateur d'importance vitale), les besoins sont poussés,** le cadre juridique est contraignant et le projet de déploiement peut s'étaler sur plusieurs mois. **Pour une PME, il s'agit d'abord de s'équiper d'une solution permettant de gérer efficacement la flotte** puis de mettre en place les mesures de sécurité liées aux enjeux spécifiques de l'entreprise.

◯ CARTOGRAPHIER PRÉCISÉMENT LA FLOTTE MOBILE

Ce travail consiste à répertorier tous les appareils utilisés dans l'entreprise (nombre, type de matériel et d'OS) et savoir qui a accès à quoi (données, outils, connexions). Il permet aussi d'évaluer l'hétérogénéité du parc mobile et sa facilité d'intégration dans le SI.

◯ IDENTIFIER LES DIFFÉRENTS PROFILS D'UTILISATEURS

C'est-à-dire faire le point sur les différentes situations d'utilisation des appareils mobiles. Vos collaborateurs sont-ils sédentaires, mobiles, en télétravail ? Ces éléments auront un impact sur la solution de gestion à déployer et la politique à appliquer.

◯ L'APPROCHE MOBILE : BYOD, CYOD OU COPE ?

Les systèmes en place dans les organisations varient. On trouve le **BYOD** (*Bring Your Own Device* pour « prenez vos appareils personnels »), le **CYOD** (*Choose Your Own Device*, quand le collaborateur peut utiliser son appareil personnel dans un cadre professionnel à condition qu'il ait été choisi parmi une présélection approuvée par l'entreprise), ou encore le **COPE** (*Corporate Owned, Personally Enabled,* lorsque le mobile appartient à l'entreprise mais peut être utilisé pour des usages personnels).

3 SCÉNARIOS QUI DOIVENT VOUS ALERTER

Imaginez le pire est le meilleur moyen d'éviter de probables déconvenues en matière de protection des données.

Cas n° 1

Un collaborateur perd son téléphone lors d'un salon professionnel qui rassemble plusieurs concurrents de votre entreprise. L'appareil n'était pas protégé par un mot de passe et contenait votre proposition de réponse à un appel d'offre que vous étiez sur le point de gagner contre un de ces concurrents.

Cas n° 2

Un collaborateur reçoit une facture par mail et l'ouvre. Il s'agit en réalité d'un *malware* qui s'installe sur le *device*. Un concurrent étranger peu scrupuleux a maintenant accès à tout votre réseau et donc vos documents d'entreprise (factures, plans de comptes, réponses à appels d'offres, présentations PowerPoint de la stratégie de l'année prochaine et du focus commercial...).

Cas n° 3

En voyage d'affaires, un collaborateur se connecte au réseau WiFi non sécurisé d'un hôtel et accède à son VPN. Entre temps un *malware* a déjà été placé sur son smartphone et son mot de passe et ses identifiants sont sur une plateforme de revente de données sur internet, en libre accès pour vos concurrents ou détracteurs.

Pour évaluer les risques encourus,
lisez l'article « Sécurité des mobiles :
comment éviter le scénario catastrophe ? »

LIRE L'ARTICLE ›

3

SÉCURITÉ DES DONNÉES : QUE DIT LA LOI ?

L'aspect légal est à prendre compte dans un projet de sécurisation. Même si elle ne remplace pas l'expertise d'un service juridique (à solliciter systématiquement sur ces questions !), la connaissance de ces quelques règles peut aider à baliser le projet. Tour d'horizon rapide des aspects réglementaires.

Que disent le Code Civil et le Code du Travail ?

Le salarié a le droit d'utiliser son téléphone professionnel à des fins personnelles, à condition qu'il le fasse de façon modérée. L'employeur peut quant à lui interdire l'accès à certains sites Internet (forums, réseaux sociaux, sites de téléchargements, *app stores*, etc.) sur les appareils professionnels. **L'article 9 du Code Civil garantit à chacun le droit au respect de sa vie privée** : les emails et documents stockés sur la messagerie ou les mobiles professionnels sont, à partir du moment où ils sont identifiés comme personnels, considérés comme relevant de la correspondance privée et l'employeur n'a pas le droit de les consulter. D'où l'intérêt de distinguer les usages par la conteneurisation qui garantit le respect de la vie privée des collaborateurs tout en sécurisant les données professionnelles !

Que dit la CNIL ?

La Commission nationale de l'informatique et des libertés impose la sécurisation des données sensibles avec **l'article 34 bis de la Loi Informatique et libertés** : « Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ». Les entreprises françaises doivent donc se donner les moyens de protéger leurs données, selon leur nature, sans quoi elles pourraient être tenues responsables en cas de fuites.

Quelles obligations pour les OIV ?

Conscient des enjeux de cybersécurité, l'État français a fait voter fin 2013 la loi de programmation militaire. **Une liste de plus de 200 entreprises, protégée par le secret de la Défense Nationale et dont la mise en danger pourrait être extrêmement dommageable pour le fonctionnement de l'ensemble du pays, ont alors été classées OIV** (Opérateurs d'importance vitale). Ces entreprises appartiennent notamment au secteur du transport, de la santé, de la finance, de l'énergie, de l'industrie, ou encore des télécoms. Les OIV sont tenues par l'ANSSI (Agence nationale pour la sécurité des systèmes d'information) de respecter une réglementation renforcée, passant par :

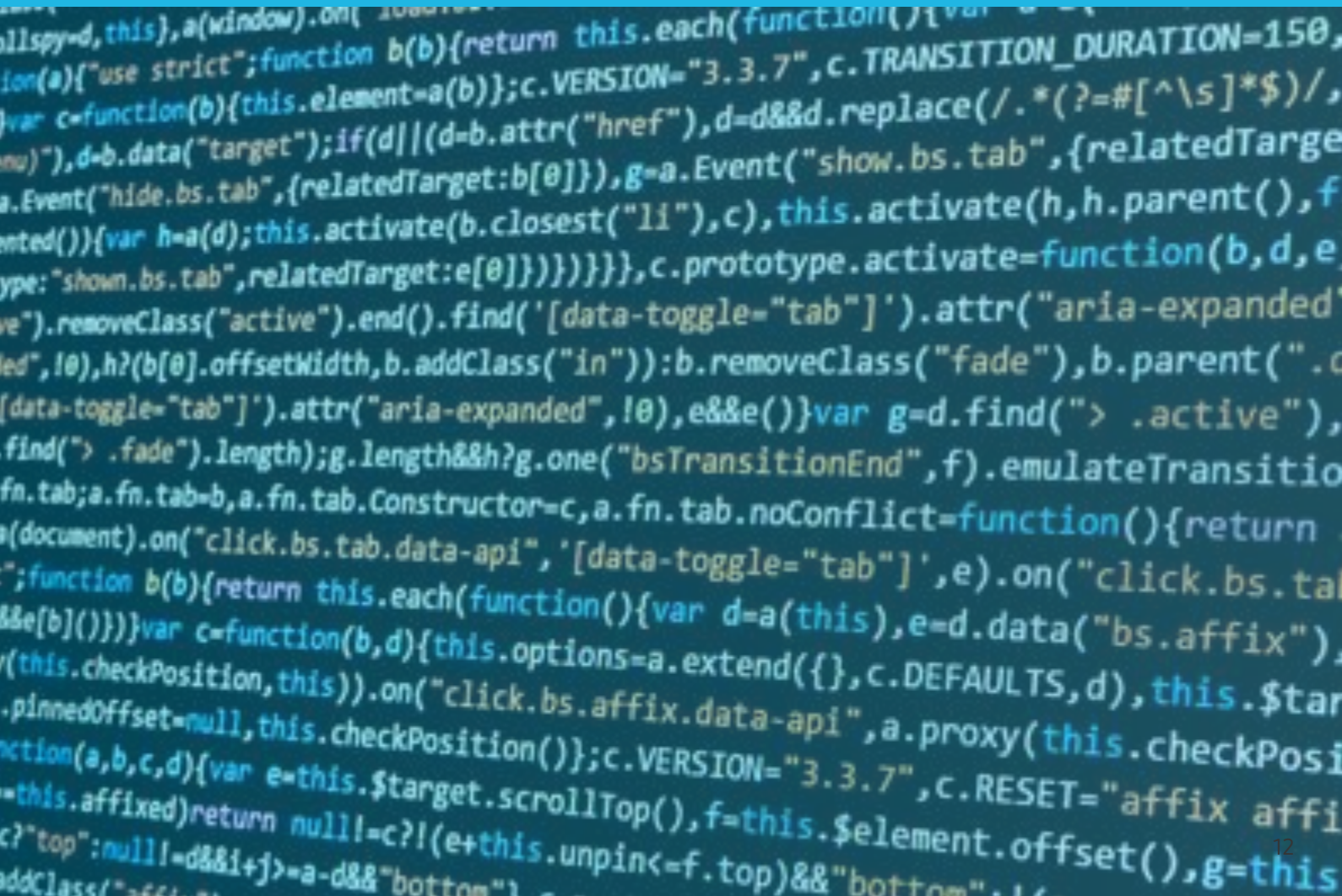
- l'instauration de systèmes de détection d'événements affectant la sécurité des SI ;
- la déclaration des incidents, notamment ceux touchant leur flotte mobile ;
- la mise en place d'une série de contrôles et de réponses à apporter en cas de crise majeure.

4

CONNAÎTRE LES FAILLES : 3 POINTS À SURVEILLER DE PRÈS

La sécurisation des terminaux mobiles ne doit pas être faite à la légère. Il faut savoir identifier les failles potentielles, qui peuvent intervenir à plusieurs niveaux, pour mieux se prémunir des menaces et incidents. L'intérêt des pirates pour les failles de sécurité aura basculé des postes de travail aux smartphones et tablettes d'ici 2017[6]. Ne pas laisser de « portes ouvertes » est un premier pas important vers la sécurisation des appareils et du SI dans son ensemble. Les outils, prestataires ou partenaires choisis pour accompagner le projet de sécurisation jouent des rôles clés.

[6] http://www.bitdefender.fr/blog-enterprise/Securite-des-applications-mobile-le-prochain-vecteur-dattaque-des-pirates-1634.html



LA FIABILITÉ DU *HARDWARE*

Dans un environnement mobile, la sécurisation du *hardware* est fondamentale. Au niveau matériel, un terminal doit être muni d'éléments uniques et facilement identifiables. Les composants doivent être tracés grâce à **une clé unique, propre au constructeur et à l'appareil**, et seuls les modules du système d'exploitation bénéficiant d'une permission spéciale doivent pouvoir y accéder. Le processus de démarrage est aussi une phase critique à surveiller et à protéger. Beaucoup de *malwares* se servent de la procédure de démarrage séquentielle et ajoutent dans la chaîne un *bootloader* malveillant pour compromettre tout l'appareil dès l'allumage. S'assurer qu'un appareil ne court aucun risque à son démarrage est donc crucial.

L'INTÉGRITÉ DE L'OS

Des failles existent dans tous les systèmes d'exploitation (OS). Protéger l'appareil mobile passe donc par la sécurisation de l'OS lui-même. Les constructeurs ont développé des **systèmes de contrôle d'accès obligatoire** qui préservent les données contre toute tentative d'accès non autorisée. Ils ont également mis en place des systèmes globaux de validation des politiques informatiques afin de détecter des actions interdites. Le **noyau**, élément central de l'OS de toute plateforme, est aussi à surveiller. Son analyse périodique doit garantir que son code n'a pas été modifié par un *malware*.

LA SÉCURISATION DE LA COUCHE APPLICATIVE

Quand l'appareil mobile n'est pas exclusivement réservé à l'activité professionnelle, il est primordial de sécuriser la couche applicative. Plusieurs moyens existent :

- **La conteneurisation** (ou *dual persona*) consiste à séparer les environnements professionnel et personnel en les faisant coexister de façon étanche sur un même mobile ;
- **Le VPN** (*Virtual Private Network* ou « réseau privé virtuel ») permet de relier de façon sécurisée les terminaux des collaborateurs dans un réseau commun privé en changeant l'adresse IP source des connexions et en chiffrant la transmission et les données échangées ;
- **Les *SmartCards* ou CAC** (Cartes d'accès commun) sont des cartes à puce permettant de numériquement signer, chiffrer et déchiffrer des documents sensibles et d'établir des connexions réseau sécurisées. Elles offrent un niveau de protection avancé ;
- **Avec les systèmes de SSO** (authentification unique), les utilisateurs n'ont besoin de s'identifier qu'une seule fois pour accéder aux différentes applications professionnelles et aux systèmes logiciels. En plus de simplifier la vie des collaborateurs, cette stratégie permet de réduire le nombre d'appels au RSSI relatifs à des problèmes d'identification.

D'OÙ PROVIENNENT LES FAILLES DE SÉCURITÉ SUR UN TERMINAL MOBILE ?

- **De l'humain :**
  les collaborateurs constituent la source principale des failles de sécurité, qui peuvent être involontaires (étourderie, manque de protection, pratiques à risque) ou volontaires (transmission de données confidentielles) ;

- **Des applications :**
  certaines publicités intégrées aux applications peuvent rediriger l'utilisateur vers des sites malveillants ;

- **Du système d'exploitation :**
  des virus du type chevaux de Troie ou des *malwares* du type *Ghost push* viennent paralyser l'OS, ;

- **Du *hardware* :**
  des composants matériels sont mal protégés.

D'où proviennent les failles de sécurité mobile ?

La réponse en image.

VOIR L'INFOGRAPHIE ›

5

MAM, MDM, MCM : QUELLES SOLUTIONS POUR QUELLES UTILISATIONS ?

Selon la taille de l'entreprise, les besoins et le niveau de sécurisation attendu, plusieurs offres logicielles existent. MAM, MDM, MCM… les solutions d'EMM (*Enterprise Mobility Management* ou « gestion de la mobilité d'entreprise ») disponibles sur le marché se multiplient, de la plus complète à la plus ciblée. Elles proposent des outils pour gérer et sécuriser la flotte mobile, les applications ou la gestion de contenus. Pour y voir plus clair, voici un aperçu des alternatives existantes et des fonctions clés de chacune d'entre elles.

Le *Mobile Device Management* (MDM)

Cette solution, la plus complète, prend la forme d'une console d'administration centralisée. Ce système permet de **prendre la main, à distance, sur tous les équipements mobiles** d'une entreprise. L'offre fonctionnelle est très étendue : mises à jour, verrouillage ou suppression des données en cas de perte ou de vol du terminal, segmentation des environnements personnels et professionnels ou encore contrôle de l'accès aux applications. La solution est idéale si les contraintes de sécurité sont très fortes.

Le *Mobile Application Management* (MAM)

Contrairement au MDM, qui se focalise sur la gestion du terminal, ce système se concentre sur **le déploiement et l'administration des applications utilisées dans l'entreprise** sur les appareils mobiles des collaborateurs. Il permet principalement de créer des listes noires et blanches d'applications, de mettre en place un *store* d'entreprise regroupant des applications certifiées par la DSI et de distribuer à tous les utilisateurs les applications dont ils ont besoin. Il est efficace pour contrôler les téléchargements d'applications et sécuriser certains contenus.

Le *Mobile Content Management* (MCM)

Axé essentiellement sur l'administration des contenus, il permet d'établir des **règles d'accès et de modification des informations internes** (documents PDF, PowerPoint, Excel, Word, etc.) depuis les différents terminaux de la flotte mobile. Son intérêt est d'offrir un contrôle accru aux données potentiellement sensibles de l'entreprise.

MDM, MAM, MCM : quelle solution pour gérer sa flotte mobile ?

Consultez notre article complet.

LIRE L'ARTICLE ›

LES 3 FONCTIONS CLÉS DU MDM

1 Gestion simplifiée

- Désactivation du mode multi-utilisateurs ;
- Blocage des mises à jour *Over The Air* incompatibles avec les applications professionnelles ;
- Prise de main à distance d'un smartphone ou d'une tablette pour le réparer.

2 Sécurisation accrue des données

- Utilisation imposée de mots de passe hautement sécurisés ;
- Chiffrage automatique des données ;
- Détection du débridage (*root*) d'un appareil ;
- Blocage de toute modification du *firmware* ;
- Verrouillage à distance de l'accès au smartphone ou à la tablette et effacement de son contenu.

3 Création d'un conteneur professionnel (séparation des environnements pro et perso)

- Mise en place d'un VPN pour sécuriser la transmission des données depuis le conteneur professionnel ;
- Création de listes blanches et noires d'applications dans le conteneur professionnel ;
- Blocage de l'accès à certains sites ;
- Duplication de certaines applications pour autoriser un accès depuis deux comptes différents (pro et perso).

Gestion, sécurisation, conteneurisation : les clés du MDM

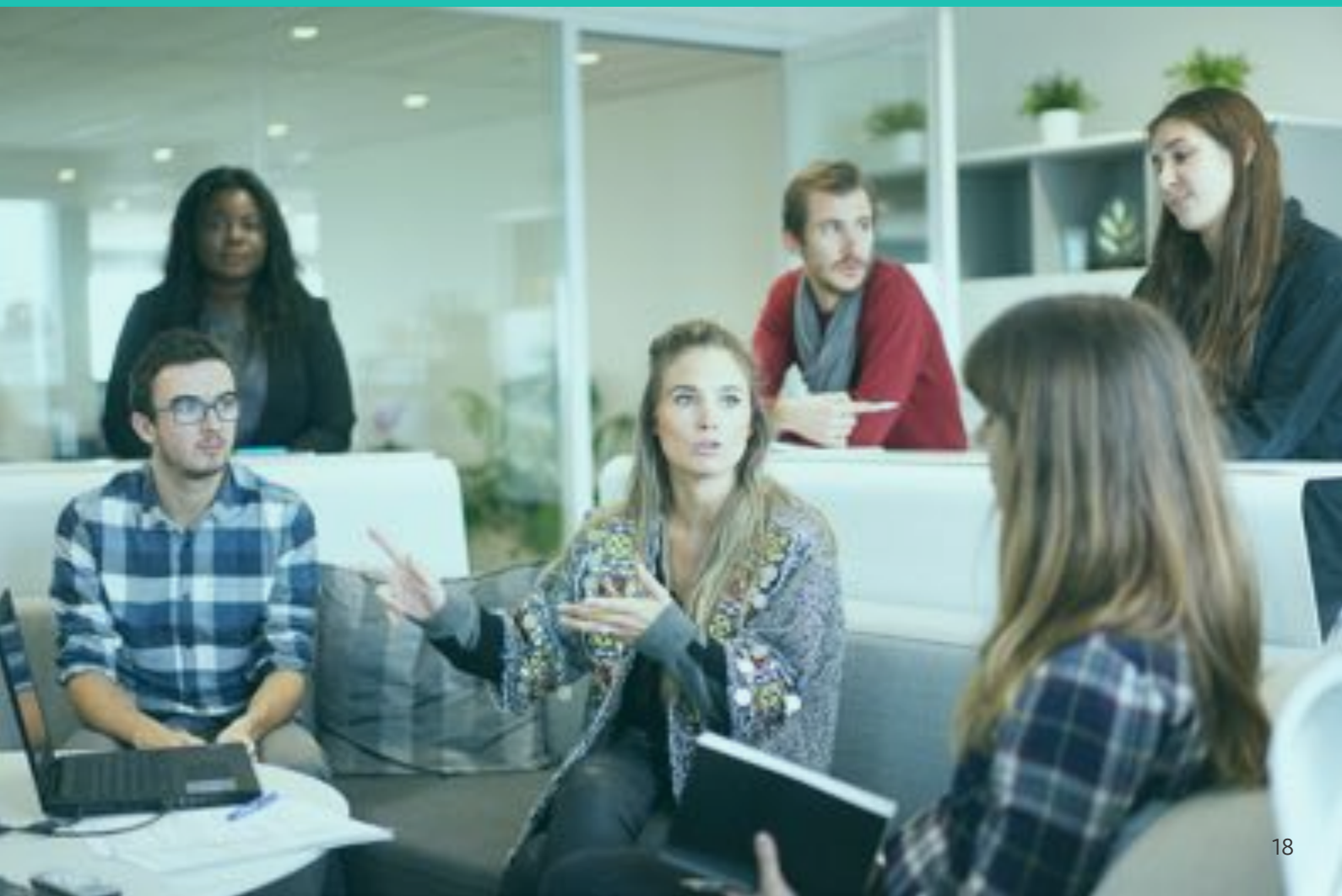
Toutes les fonctionnalités du MDM.

DÉCOUVRIR L'ARTICLE ›

6

SÉCURITÉ MOBILE : 5 ARGUMENTS POUR CONVAINCRE VOTRE DIRECTION

Les RSSI connaissent déjà l'intérêt du recours à des solutions de sécurité des mobiles. Mais qu'en est-il des décideurs ? Comprennent-ils précisément les enjeux ? Disposent-ils de tous les éléments pour valider un projet ? Les projets de sécurisation mobile peuvent faire face aux délais, blocages et incompréhensions entre les différents niveaux d'une entreprise : DSI, direction générale, filiales ou équipes distantes... Convaincre les dirigeants devient alors un vrai challenge. Voici 5 bonnes raisons d'investir dans le déploiement d'outils de protection de votre flotte d'appareils.



SÉCURITÉ MOBILE :
5 ARGUMENTS POUR CONVAINCRE VOTRE DIRECTION

LE COÛT ÉLEVÉ DU RISQUE

Une cyberattaque coûte en moyenne **773 000 €**[7] à une entreprise en 2016. Et c'est sans compter les effets néfastes sur la réputation et l'image de marque ! Se remettre d'une telle attaque prend en moyenne **9 semaines**[8]. Le risque d'une attaque d'envergure sans protection efficace met l'entreprise en péril d'un point de vue financier. Le facteur coût est donc à prendre en compte !

LE TEMPS GAGNÉ PAR LA DSI

Une stratégie globale de sécurisation simplifie considérablement le travail du RSSI et de son équipe. Avec une véritable **politique d'anticipation des risques et d'harmonisation des procédures de sécurité**, le service informatique passe moins de temps à réparer les systèmes endommagés et à répondre aux appels des collaborateurs en difficulté.

L'EFFICACITÉ LOGISTIQUE

Se doter d'un outil de gestion des dispositifs mobiles permet d'avoir une meilleure visibilité de la flotte. Depuis une console d'administration centralisée de type MDM, le RSSI gère les appareils, les applications et les données mobiles. **Chaque appareil est enregistré, associé à un utilisateur et tracé**. Toutes les informations sont centralisées, ce qui permet de réagir rapidement en cas de perte ou de vol. Ce mode de gestion renforce par ailleurs le sentiment d'appartenance des collaborateurs à l'entreprise : l'utilisation d'un badge d'accès directement intégré au mobile, par exemple, contribue à doter l'entreprise d'une image moderne et dynamique. Et ce type d'outils a de quoi attirer et retenir les nouveaux talents !

[7-8] http://www.nttcomsecurity.com/fr/uploads/documentdatabase/FR_Report_Risk_Value_Public_Approved_v2.pdf

SÉCURITÉ MOBILE :
5 ARGUMENTS POUR CONVAINCRE VOTRE DIRECTION

LA VALORISATION DE LA RSE

Les approches tolérantes des doubles utilisations (personnelle et professionnelle) des appareils mobiles contribuent au bien-être en entreprise de tous les collaborateurs. Amener son mobile personnel au travail ou utiliser son appareil professionnel pour un usage privé sont des pratiques rendues possibles par les fonctionnalités de sécurité des outils de gestion mobile. **Grâce au principe de conteneurisation**, l'entreprise protège de façon optimale les données et applications professionnelles tout en rassurant les collaborateurs, dont les données personnelles sont stockées dans un conteneur distinct, inaccessibles à l'employeur – le respect de la vie privée et le droit à la déconnexion des collaborateurs, tels que définis par la loi, en sont d'autant plus facilités.

LA REDÉFINITION DE LA DSI

La réponse aux enjeux de sécurité mobile contribue plus largement à un retour de la DSI, longtemps reléguée à un rôle de prestataire interne, parmi les directions stratégiques de l'entreprise. La mise en place d'une politique de sécurisation mobile de l'entreprise fait ainsi de la DSI un véritable partenaire et la rapproche notamment des métiers et de leurs besoins spécifiques. Au-delà du seul sujet de la sécurité, **la DSI se positionne comme un élément actif de la vie de l'entreprise**, contribuant à la transformation des systèmes et mettant les outils informatiques au service d'une vision globale.

7

LES ÉTAPES INCONTOURNABLES DU PROJET « SÉCURITÉ MOBILE »

La transition vers une flotte mobile 100 % sécurisée est plus ou moins rapide selon les besoins : simple gestion d'applications ? Ou déploiement de grande ampleur avec fonctionnalités de sécurisation avancées ? Dans tous les cas, elle se prépare méthodiquement. Que l'on parte de zéro ou pas, mener un projet de sécurisation d'une flotte d'appareils mobiles se fait progressivement. Étape par étape, voici le processus idéal.

LES ÉTAPES INCONTOURNABLES DU PROJET « SÉCURITÉ MOBILE »DE SÉCURISATION

DÉFINIR UNE POLITIQUE RÉALISTE

Définissez clairement les besoins de votre entreprise en matière de sécurité mobile, à court et à moyen terme. Si une politique de sécurité générale est déjà en place, il s'agit d'y intégrer harmonieusement des exigences en matière de mobilité. Cette mise à plat de la situation passe par le ***mapping*** **de votre environnement mobile actuel**. Il s'agit d'inventorier la flotte d'appareils pour évaluer son hétérogénéité et sa capacité d'intégration dans le SI. Reste ensuite à définir la politique la plus appropriée : responsabilités autour de la protection des données, usages mobiles autorisés, cas spécifiques, etc.

S'APPUYER SUR DES PARTENAIRES « EXPERTS »

Le rôle des partenaires (ou prestataires) est d'accompagner le client au fil de **toutes les étapes du projet** : identification des besoins, proposition de solutions techniques, évaluation de la situation, tests, mise en production, gestion du maintien en condition opérationnelle. Se tourner vers les équipes d'accompagnement des constructeurs, comme l'équipe Samsung, est une option fiable pour plusieurs raisons : l'expertise est naturellement beaucoup plus avancée qu'en interne et **les délais sont souvent plus courts**, car les besoins sont cernés rapidement et avec précision.

CHOISIR LES TERMINAUX

Au-delà de la sécurisation de votre flotte actuelle, de nouveaux appareils mobiles devront probablement être intégrés pour répondre à des besoins métier spécifiques. Si le choix de ces terminaux vous revient, il vous faudra trouver, en fonction du budget alloué, **le plus haut niveau de sécurité matériel possible** (*hardware*, OS et applications), afin de sélectionner des appareils au meilleur rapport qualité/prix disponibles sur le marché. La facilité d'approvisionnement est également à prendre en compte. Le MCO (maintien en condition opérationnelle) du matériel est enfin à évaluer pour anticiper les coûts d'entretien et les possibilités de mises à jour.

LES ÉTAPES INCONTOURNABLES DU PROJET « SÉCURITÉ MOBILE »DE SÉCURISATION

SÉLECTIONNER UNE SOLUTION

L'arbitrage sur le choix de la solution prend en compte à la fois les **besoins *corporate*** de l'entreprise (modalités de sécurisation et gestion des données) et les **besoins spécifiquement liés aux métiers**, nécessitant parfois le déploiement d'une ou plusieurs applications dédiées. MDM, MAM, MCM... Complètes ou ciblées, les solutions sont multiples et sont à adapter aux spécificités de l'organisation.

TESTER LA FAISABILITÉ

L'étape du POC (*Proof of Concept*) est déterminante. Il s'agit de déterminer la faisabilité de l'intégration de la solution de gestion au sein de votre SI. C'est l'occasion de **tester à plusieurs niveaux les fonctionnalités de la solution choisie**, de prévenir en temps et en heure toute faille de sécurité potentielle, voire de compléter votre liste de prérequis. À l'occasion du premier test en conditions réelles, il faut procéder au couplage du matériel à la solution logicielle envisagée (MDM, MAM, MCM). Il met en évidence certaines problématiques, notamment d'incompatibilité, qui étaient jusqu'alors imprévisibles.

LANCER LE DÉPLOIEMENT

Une fois l'intégration pilote effectuée, vient le temps du déploiement à proprement parler de la solution. Après des **correctifs** inévitables dans ce genre de projet, tout l'enjeu est de conserver votre flotte mobile en état de marche optimal. Une veille attentive et régulière permet de rester au courant des mises à jour, des patchs disponibles et des nouveaux risques à anticiper. Elle sera également utile pour **actualiser la sécurisation et assurer le MCO** de l'ensemble des appareils mobiles de l'entreprise.

CAS D'USAGE « PME »

Contexte

- PME ayant des besoins simples de gestion de flotte (service de messagerie) ;
- Ne disposant pas de DSI.

Solution

- Aide au déploiement avec un prestataire : identification des besoins, choix des terminaux, digitalisation de la politique de partage des données ;
- Implémentation d'un service de messagerie sans compétences techniques requises.

Résultat

- Prise en main rapide et intuitive ;
- Grande valeur ajoutée perçue en interne.

CAS D'USAGE « GRANDE ENTREPRISE »

Contexte

- Groupe industriel, plus de 10 000 utilisateurs, seulement 2 personnes à la DSI ;
- Forts enjeux de conduite du changement et de définition des besoins.

Solution

- Long travail d'identification et de sélection des produits intégrables dans l'environnement SI et dans celui de l'entreprise ;
- Prise en compte des besoins segmentée service par service ;
- Intégration progressive des produits jusqu'à la généralisation à toute l'organisation.

Résultat

- Temps d'implémentation divisé par 3 ;
- Satisfaction utilisateur.

8

QUELQUES BONNES PRATIQUES POUR LIMITER LES DÉFAILLANCES

Aucune entreprise n'est à l'abri d'une défaillance ou d'une erreur humaine. L'utilisateur est à l'origine de la plupart des failles de sécurité. Les fuites de données confidentielles, actes de malveillance ou cyberattaques peuvent avoir des conséquences économiques désastreuses pour l'entreprise. Ces incidents sont pourtant évitables. Le RSSI a la responsabilité de communiquer ces quelques règles et d'expliquer à chaque collaborateur comment et pourquoi les respecter.

QUELQUES BONNES PRATIQUES POUR LIMITER LES DÉFAILLANCES

SENSIBILISER AUX BONNES PRATIQUES

Elles relèvent souvent du bon sens, mais doivent être comprises et appliquées par tous. La préparation de supports de communication explicites permet de mieux faire passer ces messages.

- Exiger la création d'un **mot de passe sécurisé**, suffisamment complexe et à usage unique ;
- Demander systématiquement de vérifier la **source des connexions** (réseaux WiFi ouverts) et des téléchargements (pièces jointes et liens douteux) ;
- Ne télécharger des applications que dans les ***stores* officiels** ; Insister sur les dangers du **partage de données** entre environnements mobiles personnels et professionnels ;
- Mettre en garde les utilisateurs sur les risques du recours aux **modes *root* et *jailbreak*** de leur appareil.

FORMER LES COLLABORATEURS

L'idéal est d'organiser des formations, individuelles ou en petits groupes, en répétant les sessions à différentes reprises. Le fait d'accompagner les collaborateurs avec pédagogie les sensibilise plus efficacement aux problématiques de la sécurité mobile. C'est le meilleur moyen de protéger l'organisation contre des attaques.

COUVRIR SES ARRIÈRES

Un dernier bon réflexe est de partir du principe que vos collaborateurs ne respecteront pas forcément toutes les règles à la lettre... C'est là que l'utilisation d'une bonne solution de gestion et de protection de votre flotte mobile prend tout son sens !

Mobilité : 5 réflexes de sécurité à acquérir

Pour en savoir plus :

LIRE L'ARTICLE COMPLET ›

EN BREF

ASSURER LA RÉUSSITE DU DÉPLOIEMENT DE VOTRE SOLUTION DE GESTION DE LA SÉCURITÉ MOBILE

En résumé, la réussite du déploiement d'un projet de sécurisation mobile repose sur différents éléments clés :

- **La connaissance des enjeux de sécurité et du cadre légal en place ;**
- **Une préparation efficace du projet, reposant sur une analyse approfondie des besoins ;**
- **La compréhension des dispositifs de sécurité (*hardware* et couche applicative) d'un terminal et des fonctions clés offertes par les outils de gestion de la flotte mobile ;**
- **La bonne maîtrise d'un argumentaire destiné à convaincre les décideurs de l'entreprise ;**
- **Une méthodologie de déploiement minutieuse, étape par étape ;**
- **La formation des collaborateurs de l'entreprise à l'utilisation sécuritaire de leurs appareils mobiles.**

Les différentes étapes nécessaires à la transition vers un environnement mobile sécurisé peuvent donner le vertige : demandez conseil auprès des constructeurs ! Ils sauront vous guider dans votre démarche en vous proposant des solutions personnalisées ou prédéfinies.

Les équipes Samsung seront heureuses de vous aider à avancer dans les prochaines étapes de votre projet. N'hésitez pas à nous contacter **!**

À PROPOS DE SAMSUNG DIVISION ENTREPRISES

Partenaire technologique privilégié des entreprises et des administrations, Samsung Electronics Co., Ltd, conçoit et développe un écosystème innovant de solutions pour répondre aux enjeux de la transformation digitale (smartphones, tablettes, affichage, impression, climatisation, dispositifs médicaux, solutions logicielles). Porté par une vision de la technologie au service de l'usage, Samsung accompagne les entreprises pour optimiser leur productivité, renforcer leur relations clients et valoriser leur organisation.

Pour en savoir plus :
www.samsung.com/fr/business

CONTACTER