KASPERSKY lab

GUIDE DES BONNES PRATIQUES

Sécurité des appareils mobiles

www.kaspersky.fr

VOTRE GUIDE DES BONNES PRATIQUES EN MATIÈRE DE SÉCURITÉ DES APPAREILS MOBILES.

Les menaces à la sécurité des appareils mobiles augmentent de façon exponentielle.

Sur **12** mois, les produits de sécurité Kaspersky Lab ont signalé **3,5** millions de détections de programmes malveillants sur les appareils mobiles de plus d'**un** million d'utilisateurs[1].

Les appareils mobiles sont indispensables à la vie professionnelle. Mais à mesure que leurs capacités augmentent, les risques associés en matière de sécurité des données croissent eux aussi. Vous savez combien il est difficile de sécuriser une force de travail de plus en plus mobile et dispersée géographiquement, avide de médias sociaux et de technologies dans le cloud. Il est pourtant possible de dire « oui » aux technologies mobiles, BYOD compris, essentielles à l'amélioration de la productivité, sans toutefois ouvrir de nouvelles brèches.

Les fonctionnalités des appareils nomades les plus prisées par les employés attirent tout autant les pirates informatiques, les usurpateurs de données, les auteurs de programmes malveillants et autres cyber-criminels. Sans oublier la facilité avec laquelle ces appareils sont volés ou oubliés dans les taxis et bacs de sécurité des aéroports.

Les recherches menées par Kaspersky Lab ont permis d'établir qu'en moyenne 23 % des organisations ont subi des vols d'appareils mobiles ; 19 % ont perdu des données suite à un vol, 14 % d'entre elles faisant état de divulgations ou partages accidentels de données par le biais d'appareils mobiles[2].

Le coût moyen d'une atteinte à la sécurité s'élevant actuellement à 50 000 $ pour une PME[3], personne ne s'étonnera que 38 % des professionnels de la sécurité informatique considèrent la protection des données confidentielles contre les fuites comme une priorité absolue[4].

Utilisation des appareils personnels au bureau (BYOD)

Le problème ne se limite pas aux programmes malveillants ou aux vols ; la tendance qui consiste à utiliser des appareils personnels au bureau contribue à une prolifération de plus en plus complexe des smartphones et autres appareils dans les entreprises de toutes tailles. Tandis que la frontière entre usage professionnel et usage personnel s'estompe, la gestion et le contrôle informatiques deviennent un problème épineux. La mobilité est une épée à double tranchant pour les personnes dont le travail consiste à préserver la productivité du personnel tout comme la sécurité des données. De ce fait, 69 % des professionnels de la sécurité informatique considèrent les appareils mobiles comme le plus grand risque porté aux données sensibles et réglementées[5]. Et plus de la moitié des employés âgés de 21 à 31 ans se disent disposés à contourner les politiques de l'entreprise interdisant l'utilisation des appareils personnels[6].

1 Securelist, http://securelist.com/analysis/publications/66978/mobile-cyber-threats-a-joint-study-by-kaspersky-lab-and-interpol/ Octobre 2014.
2 Kaspersky Lab, Rapport sur les risques mondiaux liés à la sécurité informatique 2014.
3 Kaspersky Lab, Sécurité informatique : Combattre la menace silencieuse, 2013.
4 Kaspersky Lab, Rapport sur les risques liés à la sécurité informatique, 2014.
5 Ponemon Institute, Risk of Regulated Data on Mobile Devices and in the Cloud, 2013.
6 Forbes, http://fortune.com/2013/10/21/employees-really-want-to-use-their-personal-devices-at-work/

Comment assurez-vous la prise en charge des appareils personnels sans que cela ne devienne un véritable casse-tête ? Comment contrôlez-vous les activités de l'utilisateur final lorsqu'il télécharge des applications dans une chambre d'hôtel dans un fuseau horaire différent ? Que se passe-t-il s'il oublie son smartphone à l'arrière d'un taxi ? Êtes-vous en mesure de gérer facilement ces possibilités depuis un point central ?

La gestion des appareils mobiles (MDM) et la gestion des applications mobiles (MAM) apportent une réponse à la plupart de ces questions...

1. ADOPTER LA GESTION DE FLOTTE MOBILE

La gestion de flotte mobile (MDM) offre aux professionnels de l'informatique la possibilité d'étendre leur stratégie et leurs politiques de sécurité traditionnelles à tous les appareils, quel que soit le lieu où ils se trouvent. À l'aide d'un logiciel MDM, vous pouvez automatiser plus efficacement et de façon économique les tâches de gestion et de contrôle vitales (configuration des appareils, mises à jour logicielles et sauvegarde/restauration). Tout en préservant la sécurité des informations d'entreprise sensibles en cas de vol, de perte ou de pratiques abusives de la part de l'utilisateur final.

Que rechercher dans une solution MDM ?

- Prise en charge de plusieurs plateformes

  Sécuriser et gérer plusieurs types d'appareils et plateformes est un véritable défi. Une solution MDM qui prend en charge plusieurs plateformes avec une interface unifiée et des politiques intégrées n'est pas seulement économique, elle évite aussi d'avoir à gérer plusieurs systèmes tout en permettant une flexibilité sur les appareils actuels et futurs.

- Possibilité d'élaborer des politiques solides

  Pour mettre en œuvre les meilleures pratiques en matière de gestion des appareils mobiles, vous devrez créer des politiques se rapportant exclusivement aux appareils mobiles et qui définissent clairement les éléments suivants, notamment :

  - Comment les appareils seront-ils déployés ?
  - Quelles sont les applications autorisées à s'exécuter ?
  - Qui peut faire quoi sur les réseaux de l'entreprise ?
  - Quelles seront les procédures mises en œuvre en cas de perte ou de vol ?

  Les définitions de vos politiques doivent offrir un certain niveau de granularité et de flexibilité ; vous devez pouvoir, par exemple, appliquer des politiques différentes à différents utilisateurs et groupes en fonction de leurs besoins. Étendez cette granularité à l'appareil lui-même (par exemple, en empêchant les appareils débloqués ou compromis d'accéder aux données de l'entreprise, ou en les verrouillant à distance) et vous disposez d'une couche de sécurité supplémentaire.

2. METTRE PLEINEMENT À PROFIT LA GESTION DES APPLICATIONS MOBILES

La gestion des applications mobiles (MAM) porte sur la livraison, l'administration et le contrôle des applications sur les smartphones et tablettes des utilisateurs finaux. Idéalement, toute solution EMM (Enterprise Mobility Management) devrait englober la gestion des applications et des données d'application, ainsi que des paramètres de configuration et des micrologiciels des appareils. On peut donc considérer que MAM est complémentaire à MDM et en constitue même un sous-ensemble.

Alors que la perte ou le vol d'appareil est clairement un problème beaucoup plus important pour les smartphones et les tablettes que pour les stations de travail fixes, les applications demeurent un chemin d'accès royal pour les programmes malveillants sur tous les terminaux. En outre, le déploiement d'applications est devenu central dans l'utilisation des appareils mobiles, alors même que la qualité et le volume des applications de loisir et de divertissement téléchargées sur les appareils mobiles appartenant aux employés est hors de votre contrôle professionnel.

Une solution MAM doit séparer les données personnelles des données d'entreprise pour vous permettre d'appliquer des politiques de sécurité supplémentaires aux applications d'entreprise sur l'appareil. Cette séparation est réalisée par la mise en conteneur.

Mise en conteneur

Même les utilisateurs les plus rigoureux peuvent, par inadvertance, exposer les systèmes et les contenus de l'entreprise à des risques en téléchargeant des applications personnelles ou en accédant à du contenu personnel depuis leur appareil. C'est là que la mise en conteneur entre en jeu. Cette solution simple sépare les contenus personnels des contenus professionnels sur l'appareil, ce qui vous donne un contrôle complet sur les données d'entreprise et vous permet de protéger ces données contre les risques liés à l'utilisation d'appareils personnels.

Les politiques de sécurité et de protection des données peuvent être appliquées aux applications sécurisées dans le « conteneur » professionnel d'un appareil personnel ou d'entreprise, ce qui est particulièrement utile pour le BYOD. Avec la fonction de suppression sélective de Kaspersky Lab, lorsqu'un employé quitte l'entreprise en emportant son appareil, il est possible d'effacer du téléphone le contenu du ou des conteneurs concernés, y compris toutes les données sensibles ou liées à l'activité professionnelle, sans affecter les données personnelles.

La fonction de chiffrement du conteneur ajoute une couche de protection supplémentaire à votre stratégie de sécurité mobile. Conformément aux bonnes pratiques pour la protection contre le vol des appareils mobiles, le chiffrement imposé des données réduit l'impact des retards de suppression sur un appareil perdu ou volé.

En veillant à ce que seules les données chiffrées puissent quitter le conteneur d'un appareil, vous vous protégez contre les violations de données et remplissez les exigences de conformité en matière de protection des données. La technologie de chiffrement des appareils mobiles de Kaspersky Lab peut être automatisée ; la transparence pour l'utilisateur assure la conformité avec les politiques de sécurité. Il est également possible de chiffrer intégralement l'appareil mobile grâce aux fonctions MDM de Kaspersky Lab.

3. ACTIVER LA PROTECTION CONTRE LE VOL ET LA SÉCURITÉ DES CONTENUS

Verrouiller physiquement les petits appareils ultramobiles est presque impossible, mais vous pouvez verrouiller les données qu'ils contiennent et contrôler ce qui se passe en cas de perte.

La solution EMM de Kaspersky Lab intègre des fonctionnalités antivol et de protection des contenus qui peuvent être activées à distance afin d'empêcher tout accès non autorisé aux données confidentielles, notamment :

- **Verrouillage à distance** : empêche l'accès non autorisé à un appareil sans avoir à supprimer les données.
- **Géolocalisation** : utilise les coordonnées GPS pour situer l'emplacement de l'appareil sur une carte. Ces informations peuvent être envoyées au propriétaire de l'appareil.
- **Contrôle SIM** : verrouille un téléphone à distance en cas de perte ou de vol, même lorsque sa carte SIM est remplacée, et envoie le nouveau numéro au propriétaire légitime.
- **Suppression sélective/à distance** : efface l'intégralité des données enregistrées sur l'appareil ou uniquement les informations sensibles de l'entreprise.
- **Alarme et mugshot** : informe les voleurs que vous êtes au courant du vol. Vous pouvez même demander à votre téléphone de les photographier à des fins d'identification.

4. ... ET RESPONSABILISER VOS UTILISATEURS

L'une des façons de réduire les retards de mise en œuvre des mesures de sécurité antivol ci-dessus est de donner plus de moyens aux utilisateurs. Avec un portail en libre-service, l'employé peut réagir immédiatement à la perte d'un appareil, où qu'il se trouve. Tout d'abord, il peut tenter de retrouver l'appareil en le localisant sur la carte, en faisant une capture d'écran ou en lui envoyant un signal d'alarme. Si cela ne suffit pas, l'utilisateur peut le bloquer, effacer le profil entreprise ou supprimer entièrement toutes les données contenues sur la tablette ou le smartphone perdu.

En encourageant les employés à activer eux-mêmes les contrôles antivol, vous combattez leur tendance naturelle à attendre dans l'espoir de retrouver l'appareil plutôt que de signaler immédiatement l'incident. Cette approche réduit les délais d'activation et améliore la sécurité, tout en vous facilitant la tâche.

Autre avantage, le portail libre-service de Kaspersky Lab permet également aux utilisateurs d'enregistrer leurs appareils sur le réseau d'entreprise, ce qui vous libère d'une autre tâche administrative.

5. LUTTER CONTRE LES PROGRAMMES MALVEILLANTS POUR MOBILES

Les appareils sont exposés à des risques d'attaque même lorsqu'ils ne sont pas perdus ou volés. Il est surprenant de constater combien les entreprises insistent pour disposer de logiciels de lutte contre les programmes malveillants et de protections antispam sur leurs réseaux fixes, alors qu'elles montrent moins d'entrain à appliquer la même stratégie à leurs appareils mobiles.

Il faut noter que de nombreuses solutions MDM proposent essentiellement une protection réactive via la mise en conteneur. Les technologies de sécurité mobile de Kaspersky Lab, quant à elles, comprennent un moteur puissant de lutte contre les programmes malveillants, le spam et le phishing assisté par des technologies reposant sur le cloud, afin de détecter et de bloquer les attaques en temps réel avant qu'elles n'atteignent l'appareil, plutôt que de compter entièrement sur la mise en conteneur pour former une barrière protectrice.

Les analyses programmées et à la demande contribuent également à assurer une protection maximale ; les analyses et mises à jour automatiques « over-the-air » sont des éléments essentiels de toute stratégie MDM efficace.

6. OPTER POUR UNE GESTION CENTRALISÉE

34% des PME ont intégré des appareils mobiles dans leurs systèmes informatiques au cours de l'année passée, un taux presque identique à celui des grandes entreprises[7]. Les technologies de Kaspersky Lab vous permettent de gérer la sécurité des appareils mobiles à partir de la même console que celle que vous utilisez déjà pour la sécurité du réseau et des terminaux. Vous évitez ainsi le travail supplémentaire et les frustrations associés à plusieurs solutions distinctes et aux consoles de commande souvent incompatibles qui les accompagnent.

Les grandes organisations avec des services informatiques très structurés doivent aussi s'assurer que tout centre de contrôle prend en charge le contrôle des accès basé sur les rôles (RBAC), de façon à pouvoir assigner, par exemple, la responsabilité administrative du contrôle des appareils mobiles ou des applications à une personne en particulier au sein de l'équipe.

7. GAGNER EN EFFICACITÉ GRÂCE À L'AUTOMATISATION

En simplifiant et en automatisant la configuration sécurisée de nombreux appareils, vous réduisez non seulement le fardeau du service informatique, mais vous favorisez également l'adoption des bonnes pratiques en matière de sécurité mobile. De nombreuses tâches qui incombent à l'administrateur en charge de la sécurité mobile, par exemple la certification Windows ou PKI, peuvent être automatisées de manière sûre et efficace. Les grandes entreprises peuvent opter pour encore plus de simplification grâce à certaines technologies de type Kerberos Key Distribution Center.

La gestion à l'aide d'un portail Web présente de nombreux avantages en cas de déplacements, tandis qu'un portail utilisateur en libre-service, comme nous l'avons vu, permet de responsabiliser l'utilisateur.

Après avoir mis en place vos politiques et règles de base, le déploiement centralisé peut être réalisé en un simple clic, que vous gériez 10 ou 1 000 appareils.

---

7 Kaspersky Lab, Rapport sur les risques liés à la sécurité informatique 2014.

POUR FINIR...

Le déploiement, la gestion et la sécurisation de votre environnement informatique mobile ne doivent pas nécessairement rimer avec coût élevé et complexité. La solution EMM de Kaspersky Lab vous permet de configurer sans effort la sécurité des appareils mobiles ; un agent mobile installé sur les appareils fournira toute la protection dont vous avez besoin contre les menaces actuelles. Tous les appareils mobiles sont configurés avec des paramètres approuvés, ce qui permet de les sécuriser en cas de perte, de vol ou de pratiques abusives de l'utilisateur.

En matière de sécurité des appareils mobiles et de protection contre la violation des données, la taille n'a pas d'importance : quel que soit le nombre d'utilisateurs et d'appareils que vous gérez, si vous ne les contrôlez pas correctement, ils épuiseront vos ressources, sans mentionner les risques d'atteinte à la sécurité.

Imaginez pouvoir allier sécurité et protection contre la violation des données, mais aussi mobilité, productivité optimale et simplicité. Les technologies de gestion des appareils mobiles et de sécurité renforcée des appareils mobiles de Kaspersky Lab vous permettent de le faire.


Twitter.com/
KasperskyFrance


Facebook.com/
KasperskyLabFrance


Youtube.com/
KasperskyFrance

Kaspersky Lab
www.kaspersky.fr

Tout savoir sur la sécurité
sur Internet :
www.securelist.com
http://www.viruslist.com/fr/

Rechercher un partenaire près de chez vous :
http://www.kaspersky.fr/partners/buyoffline/liste-des-partenaires

KASPERSKY lab