Lookout®

KEVIN MAHAFFEY ET MIKE MURRAY

Le spectre des risques mobiles :

Comprendre l'étendue des risques de la mobilité pour les données d'entreprise

Le spectre des risques mobiles :

Comprendre l'étendue des risques de la mobilité pour les données d'entreprise

Il est temps que les entreprises gèrent les risques différemment. Si les appareils mobiles occupent désormais une place centrale dans notre vie personnelle et professionnelle, la plupart des entreprises restent focalisées sur le point de terminaison traditionnel : l'ordinateur.

Malgré les nombreuses similitudes que présentent les ordinateurs et les points de terminaison mobiles en matière de risques, il ne suffit pas d'étendre les mesures de sécurité actuelles de vos ordinateurs à l'ensemble de vos appareils mobiles. Il est nécessaire de repenser la gestion des risques de l'entreprise pour faire face aux risques mobiles à l'aide de solutions spécifiques conçues par des experts en sécurité.

C'est pour accompagner cette évolution que Lookout a créé la Matrice des risques mobiles. L'objectif est d'aider les organismes de sécurité à comprendre l'étendue des risques liés aux appareils mobiles et de leur présenter des données attestant la prévalence du risque mobile.

LA MATRICE DES RISQUES MOBILES

Vecteurs

Composantes du risque

Composantes du risque	APPLICATIONS	APPAREILS	RÉSEAU	WEB ET CONTENU
MENACES	Menaces applicatives Les applications malveillantes peuvent dérober des informations, endommager les appareils et accorder des accès à distance non autorisés.	Menaces pesant sur l'appareil Les menaces pesant sur l'appareil peuvent entraîner des pertes de données majeures à cause des autorisations accrues dont bénéficient les hackers.	Menaces pesant sur le réseau Les données sont menacées via les connexions au Wi-Fi ou au réseau cellulaire.	Menaces Web et de contenu Ces menaces incluent les URL malveillantes ouvertes à partir d'e-mails ou de messages SMS de phishing.
VULNÉRABILITÉS LOGICIELLES	Vulnérabilités applicatives Même les éditeurs de logiciels connus développent des applications potentiellement vulnérables.	Vulnérabilité de l'appareil La fenêtre de vulnérabilité désigne le délai entre le lancement d'un nouveau correctif et son installation.	Vulnérabilité du réseau Les appareils mobiles se retrouvent connectés à des réseaux plus hostiles que les ordinateurs portables et sont moins protégés.	Vulnérabilités du Web et du contenu Les formats de contenu incorrects, tels que les vidéos et les photos, peuvent permettre l'accès non autorisé aux appareils.
COMPORTEMENT ET CONFIGURATIONS	Comportements et configurations de l'application Les applications mobiles peuvent faire fuiter des données, telles que des contacts.	Comportements et configurations de l'appareil Débogage USB pour Android ou installation d'applications depuis d'autres sites que les app stores officiels.	Comportements et configurations du réseau Routeurs mal configurés, portails captifs inconnus ou filtrage du contenu.	Comportements et configurations du Web et du contenu Sites Web qui ne chiffrent pas les données de connexion ou laissent fuiter des données.

Téléchargez ici une version imprimable de la Matrice des risques mobiles.

Pour créer cette matrice, Lookout a étudié son immense ensemble de données issues de code mobile et d'attaques applicatives, Web et réseau, recueillies auprès d'entreprises et d'utilisateurs standard, et s'est appuyé sur dix années de recherche sur les menaces et les vulnérabilités mobiles.

Les entreprises devront évidemment appréhender chaque élément de la Matrice des risques mobiles en fonction des activités qu'elles exercent. Par exemple, une société développant des secrets industriels cruciaux pourrait juger que ses dirigeants sont des cibles à haut risque dont les appareils mobiles doivent être soumis à un niveau de protection plus élevé, même si la prévalence globale des logiciels espions visant iOS est faible.

Comprendre les menaces mobiles

Il est de plus en plus fréquent d'entendre parler de menaces mobiles dans les journaux télévisés, sur Internet ou dans la presse. Comme on a pu le constater avec Pegasus, un logiciel espion commercial très évolué qui a attaqué des appareils iOS et Android, les menaces mobiles ne cessent de gagner en sophistication. Dans la Matrice des risques mobiles, Pegasus est classé comme une menace au niveau des appareils. Cependant, ce logiciel espion prévoyait le phishing de la cible, devenant ainsi une menace au niveau du Web et du contenu, et exploitait les vulnérabilités logicielles. Les attaques malveillantes utilisent plusieurs vecteurs pour accéder aux données : c'est un élément dont il faut avoir conscience si l'on veut bien comprendre les menaces mobiles.

Qu'est-ce qu'une menace applicative ?

Les applications mobiles malveillantes peuvent causer de nombreux préjudices et notamment voler des informations, occasionner des dommages physiques aux appareils et surveiller les activités d'un utilisateur ou d'une entreprise.

Il s'agit souvent d'applications mobiles légitimes contenant du code malveillant, de logiciels malveillants qui s'infiltrent sur un appareil par le biais d'un exploit ou parce que l'utilisateur n'a pas fait attention aux autorisations qu'il accordait ou d'applications dangereuses dont les intentions sont masquées, comme une application lampe torche récupérant toutes les données personnelles à des fins commerciales non autorisées ou malfaisantes.

De nombreuses entreprises pensent que leur solution de gestion des appareils mobiles (MDM pour Mobile Device Management) suffit à les protéger des applications malveillantes. Cependant, comme les utilisateurs peuvent « sideloader » des applications sur leur téléphone, Lookout constate que les appareils d'entreprise de ses clients continuent d'être exposés à des applications malveillantes.

Quelle est la prévalence des menaces applicatives ?

Au cours du 4e trimestre 2016 et du 1er trimestre 2017, 47 appareils d'entreprise Android sur 1 000 protégés par Lookout et seulement 1 appareil iOS sur 1 000 ont été confrontés à des menaces applicatives.[1]

Comment se protéger des menaces applicatives ?

Pour être exhaustive, une stratégie de protection contre les menaces applicatives doit prévoir, en plus d'une solution de Mobile Threat Defense :

- Une solution MDM et de gestion des applications mobiles (MAM pour Mobile Application Management) pour les appareils d'entreprise
- Des systèmes de détection d'intrusion (IDS pour Intrusion Detection System) et de prévention d'intrusion (IPS pour Intrusion Prevention System)
- L'inclusion des informations propres aux appareils mobiles dans les flux de Threat Intelligence et le contrôle réseau (mise sur liste noire des serveurs de commande et contrôle dans les pare-feu par exemple)
- La détection et l'analyse des téléchargements d'applications mobiles grâce au filtrage URL et aux contrôles de sécurité Web

[1]Les données analysées sont issues d'un vaste sous-ensemble mondial de capteurs Lookout personnels ou d'entreprise. Elles ont été recueillies entre le 15 avril 2016 et le 16 avril 2017. Les données d'entreprise proviennent d'appareils Android et iOS d'institutions financières, de prestataires de soins de santé, d'organismes gouvernementaux et d'entreprises d'autres secteurs majeurs. Les données personnelles proviennent de plus de 100 millions d'appareils Android et iOS d'utilisateurs du monde entier.

Quelles sont les menaces inhérentes aux appareils ?

Les menaces de sécurité qui touchent les systèmes d'exploitation et les firmwares des appareils mobiles peuvent entraîner des pertes de données majeures et permettre la surveillance car elles donnent aux attaquants des niveaux d'autorisation plus élevés que ceux habituellement accordés aux applications.

Le logiciel espion Pegasus est un exemple frappant de menace ciblée, à faible prévalence et ayant une forte incidence sur les appareils iOS et Android. Il suffit d'un simple clic sur un SMS de phishing exploitant l'ingénierie sociale pour que Pegasus puisse surveiller les conversations qui se déroulent à proximité de l'appareil en utilisant les appareils photos et le micro du téléphone, suivre les déplacements des victimes et voler les messages de clients chat chiffrés de bout en bout.

Ce qui pose véritablement problème avec les menaces inhérentes aux appareils, c'est que l'ensemble de la sécurité et de la gestion de l'appareil repose sur l'hypothèse que l'appareil lui-même n'a pas été compromis. Or, il est certain que si un appareil mobile a été compromis, le conteneur qui héberge les données d'entreprise, ainsi que les solutions MDM et MAM, peuvent l'être également.

La situation est encore plus grave pour les entreprises qui se servent des appareils mobiles dans le cadre d'une solution d'authentification multifacteur car ce système place une trop grande confiance dans le « jeton logiciel » stocké sur l'appareil et utilisé comme deuxième facteur par défaut.

Les chercheurs de l'équipe de renseignement de sécurité de Lookout ont constaté que de nombreux chevaux de Troie bancaires exploitaient cette stratégie pour compromettre l'appareil, voler le mot de passe lors de sa saisie ainsi que le code du second facteur, puis se connecter à la banque à l'aide du jeton envoyé par SMS.

Avant d'instaurer des contrôles de sécurité sur un téléphone, que ce soit pour protéger les données d'entreprise ou pour y placer un jeton permettant d'accéder à d'autres ressources, il faut donc impérativement sécuriser l'appareil.

Quelles sont les menaces pesant sur le réseau ?

Les menaces réseau exploitent certaines faiblesses dans la façon dont les applications et sites Web établissent des sessions SSL/TLS sur les réseaux Wi-Fi, mobiles et autres. Ces attaques peuvent être exécutées directement par des attaquants ou par des logiciels malveillants utilisant des méthodes automatisées. Parmi ces incidents figurent par exemple les attaques de type man-in-the-middle, l'usurpation de certificat, le stripping des protocoles SSL/TLS et les régressions de version de suite cryptographique SSL/TLS.

Avant, les attaques réseau existaient déjà mais elles restaient rares. De plus, ce qui se trouvait à l'intérieur du pare-feu était généralement considéré en sécurité. Cependant, depuis quelques années, la mobilité fait que les appareils rencontrent de plus en plus de réseaux. Chaque jour, les appareils de votre parc mobile passent ainsi plus de temps sur des réseaux externes que sur des réseaux contrôlés par l'entreprise. Ces attaques réseau étaient peu répandues lorsque tous les appareils restaient la plupart du temps dans l'entreprise, mais il s'agit désormais d'un véritable problème.

Quelle est la prévalence des menaces pesant sur le réseau ?

L'an dernier, moins de 10 appareils d'entreprise sur 1 000 (0,8 %) ont été confrontés à une attaque de type man-in-the-middle.

Ces chiffres peuvent inclure des interceptions de données d'entreprise non intentionnelles, dues par exemple au filtrage du contenu opéré dans les écoles. Mais même si ces interceptions ont lieu sans intention de nuire, elles constituent néanmoins une « attaque » contre les mesures de protection qui visent à empêcher la consultation des données en transit.

Qu'est-ce qu'une menace Web et de contenu ?

La plupart du temps, le contenu malveillant est transmis par le biais d'e-mails ou de SMS de phishing comportant des liens qui redirigent les utilisateurs vers des sites Web ressemblant à des pages de connexion officielles. Dans le cas de Pegasus, un SMS de phishing envoie vers un site Web qui tire profit d'une vulnérabilité du navigateur puis d'une vulnérabilité du noyau de l'appareil.

La probabilité de saisir ses informations de connexion sur une page de phishing est trois fois plus élevée pour un utilisateur mobile que pour un utilisateur d'ordinateur, selon une étude réalisée en 2011 par IBM. Les messages de phishing contiennent habituellement des liens qui mènent à des sites Web malveillants entraînant des drive-by downloads ou l'injection de code malveillant sur l'appareil.

Comment se protéger des menaces Web et de contenu ?

Il est absolument essentiel de lutter contre les menaces de contenu car c'est généralement par ce biais que les attaquants accèdent aux données d'entreprise. Pour bloquer une menace de contenu, il est souvent nécessaire de bloquer l'intégralité de la kill-chain très tôt, par exemple le SMS qui entraîne le déploiement de Pegasus ou le drive-by download qui installe un cheval de Troie sur l'appareil de l'utilisateur.

En plus d'une solution de Mobile Threat Defense, la lutte contre les menaces Web et de contenu nécessite que le filtrage des e-mails et l'antispam intègrent des protections contre le phishing spécifiques et que le contenu Web soit protégé contre le filtrage de manière tout à fait adaptée aux mobiles. Il faut également prévoir des outils de sécurité pour les réseaux sociaux afin de mettre les utilisateurs à l'abri d'éventuelles tentatives de phishing, sachant que ces attaques ciblent souvent les appareils mobiles, comme c'était le cas du cheval de Troie ViperRAT qui a infecté l'Armée de défense d'Israël en 2016.

Comprendre les vulnérabilités logicielles mobiles

Ces nombreuses menaces qui visent la technologie mobile ne sont pas les seuls obstacles à la sécurisation de l'environnement mobile. Les applications et les appareils eux-mêmes présentent des vulnérabilités susceptibles d'entraîner un incident de sécurité.

Qu'est-ce qu'une vulnérabilité applicative ?

Comme les logiciels PC, les applications mobiles comportent des vulnérabilités. Le problème est pourtant beaucoup plus grave dans le cas des applications mobiles car elles sont souvent conçues par de petites équipes de développeurs et ce sont les utilisateurs finaux qui les choisissent la plupart du temps. À l'inverse, les applications PC sont généralement vérifiées par le service informatique et développées par de grands éditeurs de logiciels.

Quelle est la prévalence des vulnérabilités applicatives ?

Les chercheurs de l'équipe de renseignement de sécurité de Lookout ont procédé à une analyse approfondie de nombreuses applications de travail et de productivité populaires disponibles sur Android et iOS. Ces contrôles ont révélé des vulnérabilités très variées, à la fois en termes de niveau de sophistication requis de la part de l'attaquant et d'impact pour l'utilisateur final. Du côté des vulnérabilités à haut risque et très sophistiquées, Lookout a découvert des failles qui permettraient aux attaquants d'accéder aux informations affichées par l'utilisateur dans une application mais aussi au compte de service cloud de la victime et à toutes les données liées à ce compte.

L'utilisation dangereuse d'addJavascriptInterface par Android est un exemple de vulnérabilité applicative à forte prévalence qui était susceptible de toucher plus de 90 000 applications d'après Lookout. Il s'agit d'un problème logistique de correctif insoluble.

Comment se protéger des vulnérabilités applicatives ?

Bien que les contrôles de sécurité des données transférées par les applications mobiles se soient améliorés ces dernières années, il arrive que des éditeurs de logiciels, même connus, développent des applications comportant des failles de sécurité qui mettent en danger les données des utilisateurs et des entreprises.

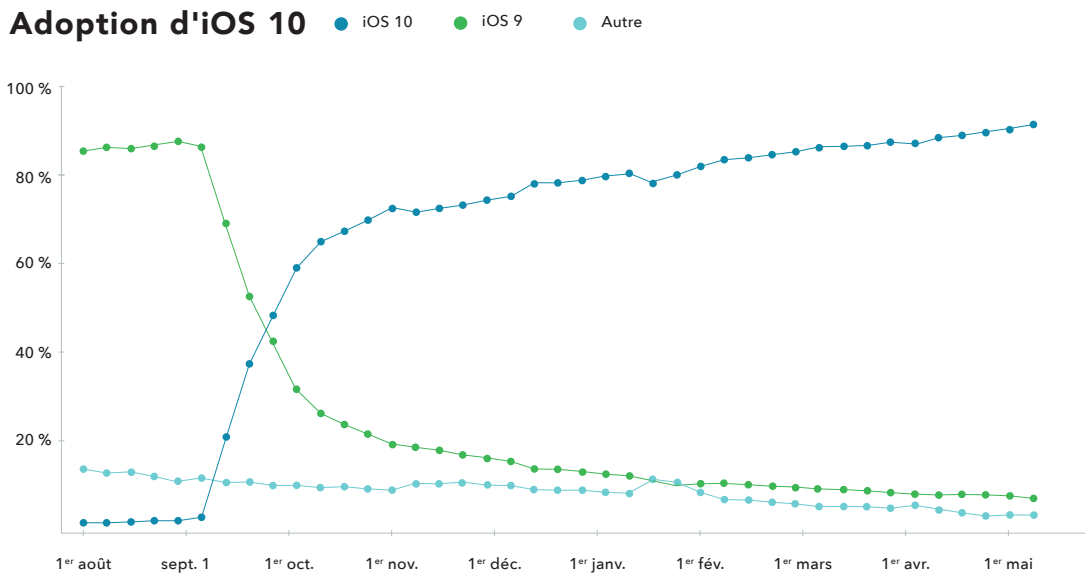
Les évaluations App Security détectent régulièrement des contrôles de sécurité insuffisants concernant les données en transit. Ces lacunes peuvent entraîner des conséquences importantes, telles que la fuite accidentelle d'informations sensibles ou la possibilité pour les acteurs malveillants d'attaquer directement l'appareil d'une victime. La gravité de ces risques dépend du niveau de sophistication et de l'imagination de l'adversaire.

Sachant qu'un nombre croissant d'entreprises encouragent l'utilisation d'applications mobiles gérant des données sensibles sur les utilisateurs et les entreprises, il faut s'attendre à ce que les adversaires accentuent leurs efforts pour exploiter les faiblesses des applications et accéder à ces informations.

Qu'est-ce qu'une vulnérabilité de l'appareil ?

Les appareils mobiles comportent eux aussi de nombreuses vulnérabilités connues. Google et Apple publient régulièrement des bulletins de sécurité présentant une liste de plus en plus longue de correctifs destinés à éliminer les vulnérabilités des appareils fraîchement découvertes.

Les entreprises peuvent évaluer leur exposition aux vulnérabilités des appareils en suivant la « demi-vie de vulnérabilité », c'est-à-dire la durée entre le lancement d'un nouveau correctif et son installation par la moitié du parc mobile. En général, les programmes de mobilité de type BYOD ont une demi-vie de vulnérabilité plus longue que les programmes utilisant des appareils appartenant à l'entreprise et la fenêtre est plus étendue pour les parcs Android que pour les parcs iOS. La fenêtre de vulnérabilité pour ces deux plates-formes mobiles reste dans tous les cas nettement plus longue que la demi-vie de vulnérabilité moyenne d'un appareil d'entreprise, estimée à 30 jours selon le fournisseur de gestion des vulnérabilités Qualys.



Les données fournies par Mixpanel indiquent qu'iOS a atteint plus de 90 % d'adoption d'iOS 10 en huit mois.

Quelle est la prévalence des vulnérabilités de l'appareil ?

Si l'on considère les appareils personnels protégés par Lookout en avril 2017, seuls 43 % des utilisateurs avaient mis à jour leur système d'exploitation iOS vers la version 10.3 ou ultérieure, 42 % avaient la version 10.2 et 6 % la version 9.3.5.

Cela signifie qu'un grand nombre d'utilisateurs utilisent des appareils ne disposant pas des dernières mises à jour de sécurité. Environ 15 % des utilisateurs iOS sont exposés aux vulnérabilités d'iOS liées à WebKit, le moteur de rendu utilisé par Safari, l'App Store et de nombreuses applications iOS.

En ce qui concerne le Samsung Galaxy S6, 92 % des utilisateurs n'ont pas mis à jour leur système d'exploitation vers la dernière version, 7.0 Nougat.

Qu'est-ce qu'une vulnérabilité du réseau ?

Une vulnérabilité du réseau permet d'attaquer un appareil via le réseau ou d'en intercepter les données, en tirant parti d'une vulnérabilité du système d'exploitation.

Lors d'une conférence à Black Hat Asia en mars 2017, des chercheurs ont montré comment exploiter un appareil iOS à distance via Wi-Fi sans aucune intervention de l'utilisateur en contournant totalement la sandbox iOS. Plus récemment encore, un article de SC Magazine a révélé qu'Apple avait publié la version iOS 10.3.1 pour corriger une faille qu'un attaquant à proximité d'un appareil vulnérable pouvait exploiter via le Wi-Fi.

Quelle est la prévalence des vulnérabilités du réseau ?

Alors que la quasi-totalité des suites de sécurité des points de terminaison depuis Windows XP inclut un pare-feu et une solution de détection/prévention d'intrusion de l'hôte (HIDS /HIPS), les appareils mobiles bénéficient d'une protection moindre et sont plus souvent confrontés à des réseaux plus hostiles que la plupart des ordinateurs portables.

Qu'est-ce qu'une vulnérabilité du Web et du contenu ?

Les formats de contenu incorrects, dans les pages Web, les vidéos et les photos notamment, peuvent créer des vulnérabilités spécifiques servant à exploiter une application ou des composants du système d'exploitation précis pour obtenir un accès non autorisé à l'appareil.

L'exemple le plus connu est Stagefright, une vulnérabilité d'appareil exploitée par un fichier vidéo pour accéder aux bibliothèques multimédias d'Android, et ainsi aboutir à l'exploitation de l'appareil via de nombreux vecteurs. Parmi ces vecteurs figurent les MMS, ainsi que des canaux arbitraires tels que le téléchargement de fichiers sur Internet, où les fichiers média sont lus.

Comment se protéger des vulnérabilités du Web et du contenu ?

Même si la grande majorité des vulnérabilités Web et de contenu sont liées à une vulnérabilité applicative ou de l'appareil, les entreprises doivent bien faire la distinction afin de réaliser des contrôles complémentaires empêchant leur exploitation. Les vulnérabilités de contenu transmises via le Web peuvent être éliminées grâce au pare-feu du contenu Web existant, au moins au sein de l'entreprise ou sur le VPN. Par ailleurs, la mise en place d'une meilleure protection du contenu des e-mails et de solutions de sécurité pour les réseaux sociaux contribue à prévenir le phishing mobile et donc à bloquer le contenu qui tente d'exploiter une vulnérabilité avant même qu'il n'atteigne l'appareil mobile.

Comprendre les comportements et les configurations

Dans la plupart des cas, les employés constituent un facteur de risque particulièrement important. Ils ont tendance à utiliser leurs appareils mobiles personnels pour le travail alors que la configuration de ces appareils respecte rarement la politique de sécurité de l'entreprise. Nombre de RSSI mettraient en place une politique BYOD s'ils étaient en mesure d'en assurer la sécurité. Pour offrir une mobilité sécurisée, il faut d'abord avoir une visibilité totale sur les comportements et les configurations.

Que sont les risques liés aux comportements et configurations de l'application ?

Des comportements d'application risqués peuvent entraîner la fuite de données d'entreprise accessibles à certaines applications.

Il s'agit par exemple :

- d'applications qui accèdent à des données d'entreprise sensibles et à des services de stockage sur un cloud public qui ne sont pas contrôlés par l'entreprise
- d'applications qui accèdent à des données soumises à des exigences de conformité, telles que les informations de carte bancaire ou des données à caractère personnel, mais qui ne protègent pas suffisamment l'utilisation, la transmission et le stockage de ces données

Quelle est la prévalence des risques liés aux comportements et configurations de l'application ?

Entre le 4e trimestre 2016 et le 1er trimestre 2017, parmi les appareils d'entreprise protégés par Lookout, 11 % des appareils iOS ont été confrontés au sideloading et 30 % des applications avaient accès aux contacts, 30 % au GPS, 31 % au calendrier, 39 % au micro et 75 % à l'appareil photo.

De plus, 43 % des appareils d'entreprise iOS étaient connectés à Facebook et 14 % à Twitter.

Quels sont les risques liés aux comportements et configurations de l'appareil ?

Les risques liés aux comportements et configurations des appareils sont largement dus aux employés qui pratiquent le jailbreak ou le root mais également à ceux qui ne configurent tout simplement aucun mot de passe sur leur appareil. Les comportements et configurations de l'appareil incluent le débogage USB pour Android, l'installation d'applications depuis des boutiques d'applications non officielles et certains profils de configuration d'entreprise sur iOS. Le recours à une solution de gestion des appareils mobiles permet de résoudre la plupart de ces problèmes.

Quelle est la prévalence des risques liés aux comportements et configurations de l'appareil ?

Parmi les appareils mobiles d'entreprise protégés par Lookout, 1 appareil iOS sur 1 000 a été jailbreaké et 5 appareils Android sur 1 000 ont été rootés.

Quels sont les risques liés aux comportements et configurations du réseau ?

Les risques liés aux comportements et configurations du réseau résultent de l'utilisation de réseaux Wi-Fi publics par les employés. Plus les utilisateurs finaux sont imprudents lorsqu'ils se connectent au Wi-Fi public, plus les données d'entreprise sont menacées.

Lorsqu'ils sont en déplacement, les employés peuvent utiliser le Wi-Fi dans les aéroports, les hôtels, les cafés ou d'autres lieux publics sans savoir s'ils se connectent à un routeur mal configuré, à un portail captif inconnu ou à un réseau qui déchiffre le trafic pour filtrer le contenu.

Quelle est la prévalence des risques liés aux comportements et configurations du réseau ?

Pour saisir l'ampleur de ce problème, il faut prendre le nombre d'appareils utilisés par les employés d'une entreprise, sachant que certains en possèdent plusieurs, et le multiplier par le nombre de réseaux auxquels ces appareils se connecteront. Dans le cas d'une multinationale, les données sont donc exposées à un nouveau risque de fuite sur mobile très élevé.

Quels sont les risques liés aux comportements et configurations du Web et du contenu ?

Dans une entreprise, les employés ouvrent régulièrement des pièces jointes provenant de personnes inconnues et cliquent sur des liens reçus par SMS ou sur d'autres applications de messagerie. Les pièces jointes peuvent contenir n'importe quel type de contenu mais sont souvent des fichiers multimédias. Lorsqu'ils accèdent à ces fichiers, les employés s'exposent à un risque d'exploitation et de phishing par un contenu ou une page Web malveillants.

Protéger votre entreprise face au spectre des risques mobiles

Pour étendre votre programme de sécurité à la technologie mobile, vous devrez tout d'abord examiner chaque élément de la Matrice des risques mobiles puis élaborer une stratégie adaptée à votre environnement de sécurité pour gérer ces risques.

En matière d'appareils mobiles, chaque entreprise a ses propres habitudes et ses besoins varient en fonction des activités qu'elle exerce. Après avoir évalué la probabilité et l'impact de ces risques, les entreprises seront en mesure de mettre sur pied une stratégie de sécurité sur mesure, préférable à une approche standardisée.

Commencez par vous interroger sur deux points clés de votre système de sécurité :

1. Comment évaluez-vous le risque de chaque élément de la matrice dans votre environnement actuel ?
2. Ensuite, quelles mesures avez-vous prises pour contrôler ces éléments ?

En général, les services de sécurité s'aperçoivent qu'ils disposent d'une visibilité très limitée sur la plupart des risques mobiles et que les systèmes en place ne leur permettent pas de les contrôler correctement.

« Les responsables de la sécurité et des risques chargés d'assurer la sécurité des points de terminaison et des mobiles doivent s'intéresser rapidement aux différents outils de MTD puis les implémenter progressivement en plus de leur solution EMM ».

Prévisions 2017 du Gartner : Sécurité des points de terminaison et des mobiles, nov. 2016

Le mieux est alors de suivre la recommandation de Gartner qui suggère que : « les responsables de la sécurité et des risques chargés d'assurer la sécurité des points de terminaison et des mobiles s'intéressent rapidement aux différents outils de MTD (Mobile Threat Defense) puis les implémentent progressivement en plus de leur solution EMM ».

Les services de sécurité qui acquièrent une visibilité totale sur le spectre des risques, préviennent efficacement les menaces mobiles, garantissent la réputation des applications mobiles et gèrent les vulnérabilités mobiles permettront à leurs employés de profiter pleinement de la technologie mobile, en toute sécurité.

À propos des auteurs

Kevin Mahaffey

CTO et cofondateur de Lookout

Lire d'autres publications de Kevin

Mike Murray

Vice Président du département Security Intelligence

Lire d'autres publications de Mike