Communiqués de presse

Selon une étude sponsorisée par IBM, les développeurs d'applications mobiles n'investissent pas dans la sécurité

La nouvelle technologie IBM Mobile Threat Management permet de lutter contre les logiciels malveillants sur les mobiles

Paris - 20 mars 2015: IBM et l'Institut Ponemon dévoilent ce jour une étude révélant l'état alarmant de l'insécurité dans le domaine de la mobilité. Les résultats montrent que près de 40% des grandes entreprises, dont beaucoup font partie du classement Fortune 500, ne prennent pas les précautions nécessaires pour sécuriser les applications mobiles qu'elles conçoivent pour les clients. L'étude révèle également que les entreprises protègent mal leurs périphériques mobiles BYOD (Bring Your Own Device) des cyber-attaques – permettant ainsi aux pirates d'accéder facilement aux données des utilisateurs, de l'entreprise et des clients.

Le nombre de cyber-attaques mobiles continue à croître. À tout moment, un code malveillant peut infecter plus de 11,6 millions d'appareils mobiles1. L'étude de l'Institut Ponemon et d'IBM, qui a étudié les pratiques de sécurité de plus de 400 grandes entreprises, a constaté qu'une société type teste moins de la moitié des applications mobiles qu'elle conçoit. En outre, 33% des entreprises ne testent jamais leurs applications – créant ainsi pléthore de points d'entrée pour puiser dans les données de la société par le biais d'appareils non sécurisés. Bien que ces chiffres puissent paraître choquants, ils ne sont pas surprenants étant donné que 50% de ces entreprises ne consacrent aucun budget à la sécurité mobile.

« Construire la sécurité des applications mobiles n'est pas une priorité pour les entreprises, ce qui donne aux pirates l'occasion de décortiquer la façon dont les applications sont développées, de débloquer les appareils mobiles et de puiser dans les données confidentielles », déclare Caleb Barlow, Vice President of Mobile Management and Security chez IBM. « Les entreprises ont besoin de penser à la sécurité de la même façon que les cyber-criminels très efficaces qui travaillent de manière collaborative conçoivent des attaques. Pour aider les entreprises à adopter des stratégies mobiles intelligentes, nous nous sommes appuyés sur la solide expertise en sécurité d'IBM Security Trusteer, en apportant ce que nous avons appris de la protection des données les plus sensibles dans les entreprises complexes - comme par exemple les principales banques mondiales - et en l'appliquant au domaine du mobile ».

Les pirates profitent désormais des applications mobiles non sécurisées les plus connues, des réseaux WiFi publics et autres pour s'emparer des données cruciales souvent hébergées sur les appareils mobiles BYOD ou ceux de l'entreprise. De plus, ils utilisent également les appareils mobiles comme une porte d'entrée vers l'entreprise et son réseau interne hautement confidentiel.

L’Institut Ponemon dévoile l’état alarmant de l'insécurité mobile

La nouvelle étude, menée par l'Institut Ponemon avec IBM, a trouvé d’importantes failles de sécurité dans la façon dont la plupart des entreprises construisent et déploient des applications mobiles pour leurs clients. Les entreprises étudiées, dont 40% font partie du classement Fortune 500, opèrent dans des secteurs qui travaillent sur des données hautement sensibles, parmi lesquels les services financiers, la santé et l’industrie pharmaceutique, le secteur public, le divertissement et la distribution.

Parmi ces entreprises, chacune consacre une moyenne de 34 millions de dollars par an au développement d'applications mobiles. Sur ce budget énorme, cependant, seul 5,5% est actuellement alloué à faire en sorte que les applications mobiles soient sécurisées contre les cyber-attaques avant qu'elles ne soient mises à la disposition des utilisateurs. 50% de ces entreprises ne consacrent aucun budget à la sécurité.

Tendant à prioriser la vitesse de mise sur le marché et l'expérience utilisateur, l'étude révèle que beaucoup de ces entreprises vérifient rarement les failles de sécurité de leurs applications mobiles - voire jamais – et souvent trop tard – offrant ainsi des points d'entrée que les pirates exploitent de plus en plus. Ces failles permettent aux cyber-voleurs d'accéder à des données personnelles et de l’entreprise qui sont confidentielles via les appareils mobiles de l’entreprise ou le BYOD. Selon le rapport IBM X-Force, sur la seule année 2014, plus d’1 milliard de données personnelles identifiables (PII) ont été compromises à la suite de cyber-attaques2.

Lors de la création d'applications mobiles, l’expérience de l'utilisateur final est plus importante que sa sécurité et sa vie privée. Selon l'étude, 65% des entreprises établissent que la demande des clients ou leur besoin met souvent en danger la sécurité de leurs applications, et 77% citent l’urgence de livrer l’application comme la raison principale pour laquelle les applications mobiles contiennent un code vulnérable.

Parmi les entreprises qui analysent leurs vulnérabilités avant de déployer des applications sur le marché, seulement 15% d'entre elles testent leurs applications aussi souvent que nécessaire pour être efficace.

Comme le BYOD ne cesse de croître, les risques liés aux appareils mobiles augmentent

Le BYOD (Bring Your Own Device) est de plus en plus répandu, et devient même une nécessité pour les entreprises. Le défi se pose lorsque les employés se connectent à des réseaux non sécurisés ou téléchargent des applications non sécurisées à partir de sources non fiables, ce qui rend le smartphone vulnérable aux logiciels malveillants. Comme dévoilés dans les conclusions de l'Institut Ponemon, même les applications issues d'entreprises fiables, disponibles dans les app stores traditionnels peuvent comporter des risques énormes.

Selon l'étude Ponemon, si la plupart des employés sont de «grands utilisateurs d'applications », plus de la moitié (55%) d'entre eux indiquent que leur entreprise n'a pas de politique qui définit l'utilisation acceptable des applications mobiles dans le cadre professionnel, et une grande majorité des entreprises – 67% - permettent aux employés de télécharger des applications non vérifiées sur leurs appareils de travail. En outre, 55% des entreprises indiquent que les employés sont autorisés à utiliser et télécharger des applications business sur leurs appareils personnels (BYOD).

IBM MobileFirst Protect s'associe à Mobile Threat Management

Pour se défendre contre les cyber-criminels qui profitent de cette immense opportunité, IBM a lancé une nouvelle technologie de gestion des menaces mobiles (MTM) via son offre IBM MobileFirst Protect (anciennement MaaS360). En utilisant une technologie qui exploite l'intelligence autour des menaces avancées, IBM MobileFirst Protect Threat Management détecte automatiquement les activités suspectes sur les appareils mobiles et stoppe les logiciels malveillants au moment où l'appareil est piraté. Proposé à travers le Cloud et mise à jour au fil de l'eau, cette technologie aide les entreprises à être en permanence bien armées contre l'évolution rapide des attaques et des menaces sophistiquées.

IBM MobileFirst Protect Threat Management offre désormais une protection automatique et très intuitive contre les pirates en puissance, qui ciblent de plus en plus les appareils mobiles d'entreprise ou personnels utilisés dans le cadre du travail (BYOD). Construit par IBM Security, cette nouvelle technologie de gestion des menaces intègre la puissance flexible du Cloud, le contrôle global de la gestion de la mobilité d'entreprise, et les outils de défense les plus sophistiqués créés contre les logiciels malveillants et la fraude mobile.

Pour essayer gratuitement IBM MobileFirst Protect Threat Management, cliquez sur : http://bit.ly/1DG5AtF.

Pour télécharger le rapport de l'Institut Ponemon, "The State of Mobile Application Insecurity" aller sur : http://ibm.co/1F595xW.

Pour plus d'informations : http://www.ibm.com/security.

A propos d'IBM Security

La plateforme de sécurité IBM apporte la sécurité intelligente pour aider les organisations à protéger les personnes, les données, les applications et les infrastructures. Les solutions IBM couvrent la gestion des identités et des accès, le SIEM (Security Information and Event Management), la sécurité des données, la sécurité des applications, la gestion du risque, la gestion des terminaux, la nouvelle génération de protection contre les intrusions et d'autres sujets. IBM dispose d'une des plus importantes organisations au monde de recherche et développement et de services dans le domaine de la sécurité.

Pour plus d'informations : http://ibm.com/security.

Suivez notre actualité sur Twitter @IBMSecurityFR

1 Arxan Technologies,

https://www.arxan.com/assets/1/7/Arxan_Application_Protection_with_IBM_Trusteer_-_Solution_Brief.pdf

2 Rapport IBM X-Force Threat Intelligence, 1er trimestre 2015

http://ibm.co/1wEMKV3