# Les salariés doivent aussi prendre conscience des conséquences des failles de sécurité | Le Net Expert Informatique

## Les salariés doivent aussi prendre conscience des conséquences des failles de sécurité

**Lors des Assises de la Sécurité MobileIron présentera sa plateforme conçue pour sécuriser et gérer les systèmes d'exploitation tout en préservant la confidentialité des données personnelles. Pour Sid-Ahmed Lazizi, Directeur Général France, MobileIron Il est essentiel de faire prendre conscience aux salariés des conséquences potentielles des failles de sécurité, tout comme définir le type de données auquel on peut ou ne peut pas accéder depuis un appareil portable.**

Global Security Mag : Qu'allez-vous présenter à l'occasion des Assises de la Sécurité ?
Sid-Ahmed Lazizi : Lors des Assises de la Sécurité, MobileIron présentera sa plateforme conçue pour sécuriser et gérer les systèmes d'exploitation modernes dans le cadre d'une utilisation de terminaux divers et variés. Elle prend en compte l'identité, le contexte et les règles de confidentialité établies pour définir le niveau approprié d'accès aux données et services des entreprises. MobileIron sécurise les données statiques sur les terminaux, dans les applications et dans le cloud. Son action de sécurisation porte également sur les data-in-motion (données dynamiques) lorsqu'elles circulent entre le réseau d'une entreprise, les terminaux et les référentiels de stockage. Grâce à MobileIron, les services informatiques peuvent assurer la sécurité des données des entreprises où qu'elles soient, tout en préservant la confidentialité des données personnelles des employés. Cette plateforme se compose de trois produits :
MobileIron Core : serveur qui permet aux services informatiques de définir des règles de sécurité et de gestion sur les systèmes d'exploitation mobiles les plus répandus
MobileIron Client : logiciel qui réside sur les appareils afin d'y appliquer les règles définies par le service informatique
MobileIron Sentry : passerelle intelligente qui sécurise le trafic des données entre les appareils mobiles et les systèmes back-end de l'entreprise

**GS Mag : Quelle va être le thème de votre conférence cette année ?**
Sid-Ahmed Lazizi : Le thème de notre conférence qui aura lieu le 2 octobre à 11h est « Le nouveau modèle de sécurité en entreprise ». Les employés choisissent de plus en plus de travailler sur des terminaux mobiles dotés de systèmes d'exploitation modernes tels que Android, iOS ou Windows 10, et ce en lieu et place des ordinateurs de bureau traditionnels et des outils conçus pour Windows. Le défi engendré en termes de sécurité par ces nouveaux systèmes d'exploitation est bien différent de ceux de l'ancienne ère du PC, ce qui nécessite d'aborder la situation sous un autre angle et d'utiliser une technologie nouvelle.

**GS Mag : Quel est votre message aux RSSI ?**
Sid-Ahmed Lazizi : À mesure que les terminaux mobiles et objets connectés se multiplient, s'adaptent et intègrent le monde de l'entreprise, les services informatiques découvrent de nouvelles menaces qui pèsent sur les données et doivent relever de nouveaux défis pour les protéger. Ils doivent repenser leurs stratégies et infrastructures informatiques pour permettre une utilisation sûre et efficace de ces terminaux et objets, qui représentent une véritable opportunité d'augmenter la productivité des collaborateurs de l'entreprise.
Les technologies portables étant relativement récentes, elles se développent et s'améliorent constamment. Elles présentent le même défi que celui des smartphones quand ces derniers sont apparus. En effet, lorsque les technologies mobiles ont commencé à s'imposer, la réponse initiale des directions informatiques fut de réguler ou restreindre les accès mobiles. Cette approche s'est révélée majoritairement inefficace, les employés trouvant de plus en plus de solutions pour contourner les recommandations de leur département IT.
Liés aux smartphones, les technologies portables vont très rapidement débarquer en entreprise Etant donné que la restriction n'est pas toujours une option viable, reste le problème de la sécurité des données. Pour commencer, les départements informatiques devraient se concentrer sur les plateformes qui permettent de gérer et de sécuriser au niveau fichier, ce que certaines sociétés avancées font déjà sur mobile. Ces types de services garantissent la protection des données de l'entreprise même si le dépôt central de stockage des données est corrompu.
Les départements informatiques devront également travailler main dans la main avec les équipes RH et juridique pour définir un cadre d'utilisation clair de ces appareils mobiles au sein de l'entreprise, tout comme rappeler les risques de sécurité induits par l'accès aux données de l'entreprise sur des appareils portables ou similaires. Idéalement, ces règlements devraient être communiqués aux employés de façon positive pour valider le potentiel d'exploitation des appareils mobiles à la fois sur le plan professionnel et personnel.

Il est essentiel de faire prendre conscience aux salariés des conséquences potentielles des failles de sécurité, tout comme définir le type de données auquel on peut ou ne peut pas accéder depuis un appareil portable. Cela permettra de favoriser la relation de confiance entre les directions informatiques et les employés.

---

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

---

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : https://www.globalsecuritymag.fr/Sid-Ahmed-Lazizi-MobileIron-Les,20150716,54434.html