La situation de la sécurité des clés USB en France

Synthèse

Sponsorisé par Kingston Technology

Préparé indépendamment par Ponemon Institute LLC

Date de publication : novembre 2011

La situation de la sécurité des clés USB en France

Ponemon Institute, novembre 2011

Introduction

Sponsorisé par Kingston Technology, Ponemon Institute est heureux de présenter les résultats de sa recherche sur la situation de la sécurité des clés USB en France. Le but de cette recherche est de mieux comprendre comment les entreprises et organisations publiques complexes gèrent les exigences de sécurité et de confidentialité des données collectées et stockées sur des clés USB.

Nous sommes convaincus que la leçon à tirer de cette recherche est que les organisations comprennent qu'elles courent des risques à cause de la négligence des employés mais que trop souvent elles ne prennent pas les mesures nécessaires pour sécuriser les clés USB. Notre étude révèle aussi que, malgré la petite taille de ces dispositifs, les violations de données personnelles pouvant découler de clés USB perdues ou volées peuvent être énormes. Plus de 75 % des participants affirment qu'une violation de données personnelles a été causée par le fait que des informations sensibles ou confidentielles étaient stockées sur une clé USB perdue ou volée.

Voici 10 habitudes de sécurité liées aux clés USB que de nombreuses organisations ayant participé à l'étude ne pratiquent pas :

1. Fournir aux employés des clés USB agréées et de qualité, à vocation professionnelle.
2. Créer des politiques et programmes de formation définissant les utilisations acceptables et inacceptables des clés USB.
3. S'assurer que les employés qui ont accès à des données sensibles et confidentielles utilisent uniquement des clés USB sécurisées.
4. Déterminer la fiabilité et l'intégrité des clés USB avant l'achat, en vérifiant leur conformité aux principales normes de sécurité, et s'assurer que ces outils ne contiennent pas de codes malveillants.
5. Déployer le cryptage des données stockées sur la clé USB.
6. Surveiller et suivre les clés USB dans le cadre de procédures de gestion des actifs.
7. Analyser les périphériques pour détecter les virus ou infections par des logiciels malveillants.
8. Utiliser des mots de passe ou verrous.
9. Crypter les données sensibles sur les clés USB.
10. Déployer des procédures pour récupérer les clés USB perdues.

Nous avons interrogé 444 spécialistes de l'informatique en France, possédant en moyenne 10 ans d'expérience de l'informatique ou de la sécurité informatique. La plupart des participants (62 %) étaient sous la responsabilité hiérarchique du directeur informatique alors que 59 % avaient un statut de superviseur ou supérieur dans leurs organisations. 60 % de ces participants reconnaissent qu'il est très important ou important que les clés USB respectent des normes strictes en matière de sécurité des données.

La section suivante présente les principales conclusions de notre enquête indépendante. Globalement, nos résultats montrent clairement que les organisations ne traitent pas les risques potentiels au niveau de la protection et de la sécurité des données découlant de la myriade de clés USB dangereuses utilisées dans de nombreuses organisations. Il faut savoir que dans de nombreuses questions de l'enquête, plusieurs réponses étaient autorisées. Les fréquences de réponses indiquées dans les principales conclusions peuvent donc dépasser 100 %.

Conclusions clés

Les risques représentés par les clés USB non cryptées sont ignorés. Les participants semblent généralement être pessimistes quant aux mesures prises par leurs organisations pour protéger les informations sensibles et confidentielles sur les clés USB. Bien que 60 % des spécialistes de l'informatique ayant participé à cette étude comprennent l'importance de normes de sécurité très strictes pour les données des clés USB, moins d'un tiers (30 %) affirment que leur organisation considère que la protection des informations confidentielles et sensibles collectées et temporairement stockées sur ces périphériques est une priorité élevée.

Renforçant cette absence de priorité accordée à la sécurité des clés USB, seuls 22 % des participants affirment que leur organisation a mis en place des procédures, contrôles et politiques de gestion pour mettre fin à, ou limiter, le mauvaise usage des clés USB par les employés dans leur travail. Il est encore plus grave de constater que seulement 19 % affirment posséder les technologies appropriées pour empêcher ou détecter les infections par des logiciels malveillants pouvant résider sur les clés USB avant leur utilisation par les employés au travail. 15 % affirment que leur organisation possède des technologies appropriées pour empêcher ou détecter rapidement le téléchargement de données confidentielles sur les clés USB par des parties non autorisées.

Les employés sont négligents quand ils utilisent des clés USB, ce qui fait courir des risques aux données sensibles des organisations. Les employés font les choses suivantes en permanence ou très souvent : utilisation de clés USB sans obtenir l'autorisation préalable de le faire (85 %) ou perte de clés USB sans informer les autorités appropriées de ces incidents (86 %). Cependant, moins de la moitié (40 %) des personnes interrogées affirment que leur organisation fournit aux employés des clés USB agréées pour un usage professionnel. Bien au contraire, 70 % affirment que les employés utilisent habituellement ou très souvent les clés USB génériques distribuées 'gratuitement' lors des conférences, salons et autres événements.

Les organisations devraient être plus nombreuses à posséder des règlements applicables définissant l'utilisation acceptable des clés USB, et appliquer ces règlements. 46 % des participants affirment que leur organisation a un règlement de sécurité relatif aux clés USB. Parmi les organisations qui ont un règlement, 40 % affirment exiger que leurs employés ayant accès aux données sensibles et confidentielles utilisent exclusivement des clés USB sécurisées. Mais plus de la moitié (53 %) des participants déclarent que leur organisation n'insiste pas sur le respect du règlement, principalement parce qu'elle fait confiance à l'intégrité des employés et ne possède pas les outils ou ressources nécessaires.

Les organisations utilisent des critères similaires pour choisir les clés USB que pour d'autres technologies de mémoire ou de stockage. Les trois principaux critères dans l'achat des clés USB sont : le prix, la certification et les tests de sécurité, et la possibilité d'empêcher des attaques par des logiciels malveillants, botnets et virus. En ce qui concerne les autres périphériques de stockage de données, les organisations tiennent compte du prix, de la certification et des tests de qualité puis de la compatibilité avec les normes de cryptage de haut niveau.

58 % des organisations ne testent pas la fiabilité et l'intégrité des clés USB. 42 % affirment acheter leurs clés USB uniquement auprès de fournisseurs de confiance. Environ la moitié (49 %) ne font rien pour empêcher leurs employés d'utiliser des clés USB de mauvaise qualité.

Les clés USB sont omniprésentes dans une organisation, et la plupart ne sont pas sécurisées. Sur la base de notre enquête, il y aurait en moyenne plus de 50 130 clés USB utilisées par les employés des organisations représentées dans cette étude. En moyenne, les participants estiment que moins de la moitié (43 %) de ces dispositifs sont sécurisés. Les types d'informations sensibles ou confidentielles les plus souvent mises sur une clé USB sont : les

documents confidentiels non financiers, les données des clients et les données des consommateurs.

Même si ces dispositifs sont de petite taille, les violations de données personnelles découlant de la perte de clés USB peuvent être dévastatrices. La vaste majorité des participants (75 %) affirment être absolument certains (34 %) ou être convaincus qu'il était très probable (41 %) qu'une violation de données personnelles avait été causée par la présence d'informations sensibles ou confidentielles stockées sur une clé USB perdue ou volée. Au cours des 24 derniers mois, en moyenne, 4,6 incidents séparés mettant en jeu la perte d'informations sensibles ou confidentielles se trouvant sur une clé USB perdue ou volée se sont produits dans les organisations ayant participé à cette étude. 46 % des participants sont absolument certains ou pensent que ces clés contenaient des données relatives aux clients, aux consommateurs ou aux employés.

C'est souvent la négligence des utilisateurs plutôt que leur malveillance qui est à l'origine de la perte de clés USB. En moyenne, 66 % de toutes les clés USB manquantes sont le résultat d'une négligence plutôt que d'une fraude, d'un vol ou d'autres actes malveillants. Ces résultats montrent que des programmes et politiques de formation et de sensibilisation devraient être les premières mesures prises par les organisations pour améliorer la situation de la sécurité des clés USB.

Conclusion

Les clés USB sont devenues une technologie indispensable pour les employés dans toutes les organisations.Mais comme le montre cette étude, les clés USB perdues ou volées représentent de grands risques pour les informations les plus sensibles et confidentielles d'une organisation. Même si les organisations semblent comprendre qu'elles doivent devenir plus proactives pour éviter la négligence des employés, les pratiques de sécurité des clés USB ne semblent pas faire partie de leur stratégie globale de protection des données.

Dans notre introduction à ce rapport, nous mentionnons 10 habitudes de sécurité relatives aux clés USB que les organisations devraient mettre en pratique sans le faire. Malheureusement, notre étude montre que cela peut représenter un défi pour les spécialistes de l'informatique et de la sécurité informatique car seulement 30 % déclarent que leur organisation considère la protection des données confidentielles et sensibles collectées et temporairement stockées sur des lecteurs USB comme une priorité élevée.

En présentant les résultats de cette étude, nous souhaitons montrer que, même si les clés USB peuvent avoir l'air inoffensives, les conséquences d'une violation de données provenant d'une clé USB perdue ou volée peuvent être énormes. 75 % des participants à cette étude affirment être absolument certains ou convaincus qu'il était très probable qu'une violation de données personnelles dans leur organisation était due à des informations sensibles ou confidentielles stockées sur une clé USB perdue ou volée.

En moyenne, au cours des 24 derniers mois, les organisations ayant participé à cette enquête ont perdu 10 691 enregistrements relatifs aux clients, consommateurs et employés stockés sur des clés USB. D'après l'étude 2010 du Ponemon Institute intitulée « Coût annuel d'une violation de données personnelles », les conséquences financières d'une violation de données confidentielles suite à la perte ou au vol d'enregistrements peuvent être significatives. Selon notre recherche, le coût moyen par enregistrement perdu ou volé en France est de 138 €. Nous estimons que cette somme énorme est suffisante pour convaincre les entreprises de la nécessité d'introduire des politiques, des procédures et des programmes de formation pour atténuer les risques d'une violation de données confidentielles se trouvant sur une clé USB.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute se consacre à la recherche indépendante et à l'éducation faisant progresser les pratiques responsables de gestion des informations et de la vie privée dans le secteur privé et public. Notre mission est d'organiser des études empiriques de haute qualité sur des questions critiques touchant à la gestion et la sécurité des informations sensibles relatives aux personnes et organisations.

En tant que membre du **Council of American Survey Research Organizations (CASRO)**, nous respectons des normes strictes en matière de confidentialité des données, respect de la vie privée et normes éthiques de recherche. Nous ne recueillons pas d'informations permettant d'identifier les personnes physiques (ou d'informations permettant d'identifier les personnes morales dans nos études auprès des entreprises). Nous appliquons aussi des normes de qualité strictes pour faire en sorte que les participants ne se voient pas poser de questions superflues, non pertinentes ou déplacées.