Kingston TECHNOLOGY

Stockage USB : le chiffrement matériel permet-il de prévenir les risques ?

#KingstonIsWithYou

Stockage USB : le chiffrement matériel permet-il de prévenir les risques ?

Avant-propos et contenu

La cybersécurité est plus que jamais une préoccupation pour les entreprises, mais un trop grand nombre d'entre elles sont mal informées et mal préparées face aux menaces de cybersécurité. Aux États-Unis, seules 50 % des entreprises ont mis en place un plan de cybersécurité. Parmi elles, 32 % n'ont pas mis à jour leur plan de cybersécurité depuis le début de la pandémie de COVID-19. Or, selon UpCity, de nombreuses entreprises sont passées à des modèles de travail à distance ou hybrides au cours de cette période. Et la fréquence des cyberattaques ne fait qu'augmenter. Au niveau mondial, le nombre d'entreprises victimes d'attaques de ransomware est passé de 37 % en 2020, à 66 % en 2021[1].

Une cybersécurité compromise peut avoir des effets dévastateurs sur une entreprise. Outre le coût monétaire des cyberattaques, la perte de données, de sécurité et de réputation peut avoir des conséquences négatives à bien des égards, à court et à long terme.

Les clés USB sont un vecteur courant des menaces de cybersécurité. En raison de leur simplicité d'utilisation (il suffit de les brancher sur une machine pour qu'elles soient prêtes à être utilisées) elles sont devenues omniprésentes dans de nombreuses entreprises. Cependant, c'est justement cette simplicité qui rend les clés USB si vulnérables aux attaques : il suffit d'une clé égarée ou volée pour qu'une personne malveillante accède à des données potentiellement sensibles. C'est là que le chiffrement peut jouer un rôle important pour sécuriser l'utilisation des clés USB et atténuer les risques associés aussi bien pour l'individu que pour l'entreprise. Dans cet eBook, nous proposons des réponses aux questions clés suivantes :

- Pourquoi les clés USB chiffrées sont-elles si importantes pour se protéger contre les cyberattaques ?
- Comment les entreprises se rendent-elles vulnérables ?
- Que peuvent-elles faire pour se protéger ?

Table des matières	Pages
Contributeurs	3
Différence entre les clés USB basiques et les clés USB chiffrées	4
Pourquoi utiliser des clés USB chiffrées ?	5
Qui coure un risque ?	6-7
Comment les entreprises peuvent-elles réduire le risque de cyberattaques ?	8
Résumé et informations sur Kingston	9

Stockage USB : le chiffrement matériel permet-il de prévenir les risques ?

Contributeurs

Cet eBook a été créé par les principales figures du secteur de l'informatique et des technologies émergentes, en collaboration avec notre propre expert technique.

David Clarke

Thompson Reuter a inscrit David parmi les 10 personnes les plus influentes du « Top 30 des leaders d'opinion et penseurs les plus influents sur les médias sociaux, la gestion des risques, la conformité et le reg-tech au Royaume-Uni ». Il figure dans la liste des 50 meilleurs experts mondiaux de Kingston Technology reg-tech : technologie au service de la réglementation en banque.

Pasi Siukonen

Pasi dirige une équipe d'experts chargés de soutenir les départements de Kingston, tels que les relations publiques, le marketing, les ventes, le support technique et le service clientèle des produits Kingston. Il focalise ses efforts sur les gammes Flash et SSD.

Différence entre les clés USB basiques et les clés USB chiffrées

Alors qu'il est extrêmement simple d'accéder aux clés USB basiques (non chiffrées) et de les utiliser, le chiffrement matériel ajoute plusieurs couches de sécurité – à la fois physiques et numériques – qui rendent le stockage USB beaucoup plus sûr. La facilité d'accès, le faible coût et la portabilité des clés USB non chiffrées les rendent très pratiques pour l'utilisateur. Mais aussi pour les personnes malveillantes qui cherchent à voler des données sensibles, à introduire des logiciels malveillants ou des ransomwares dans un réseau d'entreprise, etc. Les clés USB étant largement utilisées, les possibilités de cyberattaques sont nombreuses. Il existe deux risques principaux associés aux clés basiques :

- **Attaques de ransomware (ou « rançongiciels ») :** ces attaques visant les clés USB consistent à introduire des logiciels malveillants dans les réseaux d'une entreprise pour chiffrer ses informations et/ou ses systèmes, et ensuite demander une rançon pour les restituer. Elles sont souvent causées par des BadUSB et sont devenues le type de logiciel malveillant le plus répandu.
- **Vol de données :** il suffit d'une clé perdue, volée ou laissée sans surveillance sans les mesures de sécurité appropriées pour qu'une personne malveillante puisse facilement accéder aux données qui y sont stockées. Il peut s'agir d'informations sur les clients, de code source ou de données financières et de performance sensibles.

BadUSB : attaque qui permet d'exploiter la vulnérabilité des clés USB dotées d'un firmware non protégé. Ces clés peuvent alors être programmées pour diffuser des logiciels malveillants. Ces outils malveillants sont incroyablement courants et facilement disponibles pour les cybercriminels. Or, les utilisateurs y sont trop peu sensibilisés, ce qui rend ces attaques trop faciles à réaliser. Il suffit de remplacer le firmware d'une clé basique par un firmware piraté où la clé USB peut se faire passer pour un clavier et exécuter des scripts pour attaquer le firewall. Étant donné que les cyberattaques sont souvent menées via des personnes en interne peu méfiantes, avec ou sans intention malveillante, il est extrêmement important que les entreprises utilisent des clés chiffrées qui utilisent un firmware protégé et signé numériquement pour les prévenir, afin de réduire les chances de réussite des cybercriminels.

> **Le coût de la reconstruction de l'infrastructure, voire du paiement de la rançon et d'autres extorsions, est énorme comparé aux coûts des clés USB gérées.**
> **- David Clarke**

Pourquoi utiliser des clés USB chiffrées ?

Les clés chiffrées sont spécifiquement conçues pour protéger les données qu'elles contiennent, ainsi que tous les appareils auxquels elles peuvent être connectées, ce qui en fait des outils précieux dans l'arsenal informatique de toute entreprise. Les menaces de cybersécurité étant devenues de plus en plus sophistiquées, les fonctionnalités des clés USB chiffrées le sont aussi, ce qui leur permet de garder une longueur d'avance sur les cybercriminels qui cherchent à exploiter ces appareils. Comme on peut le constater avec la gamme de produits à chiffrement matériel Kingston IronKey™, des fonctionnalités telles que le chiffrement AES 256 bits en mode XTS (le plus puissant), un boîtier robuste et inviolable, un firmware à signature numérique, des claviers virtuels, des modes Complexe ou Phrase de passe, entre autres, ont été développées et ajoutées au fil des ans pour garantir que les utilisateurs sont bel et bien protégés contre les attaques de toutes sortes.

Les risques de cybersécurité sont si souvent mal compris que de nombreuses entreprises choisissent d'utiliser des clés basiques, malgré les diverses vulnérabilités qu'elles comportent. Leur facilité d'accès, leur faible coût et l'utilisation du chiffrement logiciel jouent un rôle à cet égard, tout comme l'absence de processus d'approbation des clés USB par l'entreprise. Trop souvent, il n'existe pas de politiques ou de processus de 'meilleures pratiques' organisationnelles pour se conformer aux diverses normes informatiques et de cybersécurité, telles que les meilleures pratiques gouvernementales ISO27001, GDPR, SOC2 et WISP. Cela signifie que les risques sont souvent évalués sur la base d'opinions plutôt que de preuves, laissant ainsi de nombreuses entreprises vulnérables aux attaques.

Certains pensent se protéger en ajoutant un chiffrement logiciel à leurs clés basiques. Mais c'est une fausse économie, car il existe sur Internet de nombreux outils gratuits ou payants permettant de pirater les clés chiffrées par logiciel. Par ailleurs, les utilisateurs peuvent supprimer le chiffrement logiciel par un simple reformatage de la clé. Que ce soit pour des raisons de commodité ou pour utiliser les clés sur des systèmes d'exploitation non pris en charge. À l'inverse, le chiffrement matériel est permanent, il ne peut pas être désactivé. Les clés à chiffrement matériel sont conçues pour être inviolables et pour détecter les tentatives de violation. Et elles utilisent un firmware signé numériquement pour garantir l'authenticité et l'intégrité de la clé. Les clés chiffrées telles que l'IronKey VP50 présentent également deux autres fonctionnalités : la limitation des tentatives de saisie mot de passe (protection contre les attaques par force brute) et un clavier virtuel (protection contre l'enregistrement du clavier et de l'écran). Elles sont donc conforme aux meilleures pratiques du secteur contre les acteurs malveillants qui visent à obtenir les mots de passe des utilisateurs peu méfiants.

> Si la clé Ironkey détecte que le firmware a été altéré, elle se bloque et ne démarre pas, ce qui renforce la cybersécurité. - Pasi Siukonen

Qui coure un risque ?

En fait, toutes les entreprises qui ne sont pas en mesure de contrôler l'accès à leurs clés USB courent un risque. Et bien souvent, elles ne sont pas conscientes de la nature exacte de ce risque. Cependant, certaines entreprises, de par leurs caractérstiques, peuvent être des cibles plus attrayantes, et plus vulnérables, pour les cybercriminels.

Les données des entreprises des secteurs de la santé et de la finance sont non seulement beaucoup plus attrayantes pour les cybercriminels, mais elles ont également un impact plus grave aussi bien pour l'entreprise que pour ses clients. En 2017, au Royaume-Uni, une cyberattaque visant le NHS a provoqué l'annulation de plus de 19 000 rendez-vous, et lui a coûté 92 millions de livres sterling en perte de production et pour la restauration des données et des systèmes. Non seulement cela a empêché les patients concernés de recevoir des soins de santé, mais le NHS a été fortement critiqué pour ne pas avoir réagi de manière suffisamment rapide ou substantielle aux alertes de cybermenaces précédentes. Toutes les entreprises doivent être à jour et bien informées en matière de cybersécurité. Mais celles qui traitent des informations sensibles, notamment des données de catégorie spéciale, doivent redoubler de vigilance à l'égard des risques de cybersécurité.

Plus la valeur de l'entreprise, mesurée par le chiffre d'affaires, est élevée, plus la récompense est grande pour les acteurs malveillants. Et donc, plus le risque de cybermenaces est grand. Toutefois, cela ne signifie pas que les petites entreprises ne doivent pas se préoccuper de la cybersécurité. Si les grandes entreprises peuvent être des cibles plus attrayantes pour les cyberattaques, elles disposent souvent aussi des ressources et du personnel dédié pour y faire face. D'autre part, de nombreuses PME ne disposent pas d'équipes dédiées à la cybersécurité et n'appliquent pas les règles de gestion des clés USB aux cadres supérieurs, ce qui les rend particulièrement vulnérables et peut avoir des conséquences dévastatrices. Certaines études montrent que les petites et moyennes entreprises sont en fait davantage ciblées par les cyberattaques.

Le risque est encore plus grand pour les employés occupant des postes de cadres supérieurs. En effet, ces personnes sont facilement repérables et disposent souvent de privilèges exécutifs dans leur entreprise, ce qui signifie que les cybercontrôles (tels que les procédures de gestion des clés USB) ne leur sont pas appliqués, ce qui en fait des cibles lucratives pour les cybercriminels. C'est là que les clés avec un chiffrement matériel toujours actif (tout comme le fait de se maintenir informé sur la cybersécurité et de suivre les meilleures pratiques et processus) peuvent largement contribuer à réduire les risques et à se protéger contre les attaques.

> La plupart des violations les plus récentes ont été commises par des acteurs malveillants qui se sont spécialisés pour tirer profit des personnes en internes, que ces dernières le fassent de façon volontaire ou non. - David Clarke

Qui coure un risque ?

> Les entreprises ne font pas assez pour contrer les menaces de cybersécurité. - David Clarke

La chaîne d'approvisionnement est un autre point de vulnérabilité potentiel pour les entreprises. Les attaques par ce vecteur ne sont que trop fréquentes. En 2013, le détaillant américain Target a été victime de l'une des plus grandes violations de données de l'histoire du commerce de détail, exposant les informations de cartes de débit et de crédit de plus de 40 millions de clients. Bien que Target lui-même prenait la cybersécurité très au sérieux, puisqu'il venait d'installer un vaste système de cybersécurité 6 mois avant l'attaque, les attaquants avaient infiltré l'un des fournisseurs tiers de Target, et ont eu accès à son principal réseau de données par leur intermédiaire. Au total, 90 procès ont été intentés contre Target, et l'entreprise a perdu 61 millions de dollars en raison de cette violation. Bien qu'elle n'ait pas été directement responsable de l'attaque, cette faiblesse dans la cybersécurité de sa chaîne d'approvisionnement a suffi à causer de gros dommages, tant financiers que pour sa réputation.

Les solutions de contournement des employés peuvent également être une source de vulnérabilité. Si ces solutions de contournement peuvent permettre aux employés d'être plus efficaces dans leur travail quotidien, les processus de sécurité de base et les meilleures pratiques sont bien trop souvent négligés, comme la gestion des mots de passe. Bien que les conseils du NCSC et du CISA soient assez simples, ils sont souvent plus difficiles à mettre en pratique, surtout par les employés qui ne sont pas familiers avec l'informatique et la cybersécurité. Si le fait de disposer d'une équipe dédiée à la cybersécurité peut certainement aider, le fait de donner aux employés les bons outils (tels que des clés à chiffrement matériel) peut largement contribuer à atténuer les risques liés aux solutions de contournement des employés.

> Les clés USB à chiffrement matériel sont aujourd'hui faciles à adopter et à intégrer dans les politiques de cybersécurité existantes : elles proposent toute une série d'interfaces (graphique, clavier, écran tactile), prennent en charge de nombreux systèmes d'exploitation, et possèdent des capacités qui répondent aux besoins de chaque entreprise. - Pasi Siukonen

Comment les entreprises peuvent-elles réduire le risque de cyberattaques ?

Du point de vue de l'entreprise, il y a un certain nombre de mesures qui peuvent être prises pour sécuriser les terminaux et protéger les données. Sans GRC (Gouvernance, Risque, Conformité), la cybersécurité est vouée à l'échec. Il est donc extrêmement important que les entreprises connaissent et suivent les processus pour se protéger. La mise en place d'un solide logiciel de sécurité des terminaux peut également neutraliser un certain nombre de cybermenaces, tout en étant aussi réactif que possible lorsqu'il s'agit de corriger les failles de sécurité.

> **En termes de gestion des risques, l'adoption ou non de politiques de chiffrement est une question aussi importante, voire plus importante, que la sauvegarde de vos données. - Pasi Siukonen**

Au niveau individuel cependant, le chiffrement matériel peut réduire considérablement les vulnérabilités face aux menaces de cybersécurité. Le travail à distance et le travail hybride ont connu une forte croissance, et cette tendance va persister. Si on ajoute à cela l'augmentation des cyberattaques l'année dernière, il est plus important que jamais de s'assurer que les employés à tous les niveaux de l'entreprise manipulent, transfèrent et lisent les données de l'entreprise en toute sécurité. Les clés USB à chiffrement matériel permettent aux utilisateurs de continuer à bénéficier de la portabilité et de la simplicité des clés USB, tout en réduisant considérablement les risques qui y sont associés. Alors qu'une clé USB basique égarée ou volée peut entraîner une perte de données, d'argent, de réputation et plus encore, les clés USB à chiffrement matériel sont conçues pour protéger les données sensibles contre un large éventail d'attaques. Et comme les cybercriminels développent en permanence de nouvelles techniques d'attaque, les clés chiffrées continuent d'évoluer pour relever ces nouveaux défis.

Au final, le coût de la gestion d'une cyberattaque peut être énorme. Certes, l'adoption et l'utilisation de clés chiffrées dans l'ensemble de l'entreprise peuvent nécessiter une approbation et une mise en place plus complexes. Mais sur le long terme, elles peuvent permettre à l'entreprise d'économiser énormément d'argent, à la fois en termes de coûts d'extorsion et de perte de revenus due à une réputation entachée. Rien que les frais juridiques d'une violation peuvent facilement compenser le coût supplémentaire des clés USB à chiffrement matériel.

> **Grâce à son engagement à long terme à fournir d'excellentes solutions USB chiffrées, la gamme Kingston permet à toute entreprise de répondre à ses besoins en matière de cybersécurité : chiffrement matériel conforme aux normes industrielles, conception conforme à la politique de gestion des terminaux, capacités de gestion des appareils. - Pasi Siukonen**

Synthèse

Chez Kingston, nous sommes toujours à l'affût des développements dans le domaine de la cybersécurité. Nous veillons à ce que nos clés chiffrées IronKey soient conformes aux dernières exigences et répondent aux besoins de cybersécurité des entreprises, petites et grandes. Comme la cybersécurité continue d'être une préoccupation croissante au niveau mondial, nous sommes convaincus qu'avec les bons outils et les bonnes connaissances à leur disposition, les entreprises peuvent relever ces défis de front, tout en se protégeant elles-mêmes, leurs employés et leurs clients.

À propos de Kingston

Fort de plus de 35 ans d'expérience, Kingston dispose des connaissances nécessaires pour identifier et résoudre vos problèmes de données mobiles - afin de permettre à votre personnel de travailler en toute sécurité sans compromettre votre organisation.

#KingstonIsWithYou

1. https://www.techtarget.com/searchsecurity/news/252516423/Sophos-66-of-organizations-hit-by-ransomware-in-2021

©2022 Kingston Technology Europe Co LLP et Kingston Digital Europe Co LLP, Kingston Court, Brooklands Close, Sunbury-on-Thames, Middlesex, TW16 7EP, Angleterre. Tél: +44 (0) 1932 738888 Fax: +44 (0) 1932 785469. Tous droits réservés.
Toutes les marques commerciales et les marques déposées sont la propriété de leurs détenteurs respectifs