CHIFFREMENT LOGICIEL ET CONFORMITÉ RÉGLEMENTAIRE : UNE SOLUTION MOINS COÛTEUSE MAIS AVEC DES RISQUES DE SÉCURITÉ MAJEURS

EXIGENCES RÉGLEMENTAIRES ET DE CONFORMITÉ

La sécurité des données était autrefois reléguée aux seuls départements informatiques. Mais en raison des violations continues des données des consommateurs, les gouvernements du monde entier ont imposé aux entreprises de plus en plus d'exigences en matière de chiffrement et de protection de toutes les données permettant d'identifier les personnes.

De l'HIPAA dans le secteur des soins de santé, au RGPD dans la zone EMEA et le CCPA en Californie, le chiffrement des catégories de données protégées est désormais obligatoire en vertu des réglementations. Depuis plus de trois ans, les réglementations, les amendes et les risques juridiques associés sont montés en flèche. Aussi, les organisations chargées de la conformité se sont multipliées de manière exponentielle.

Avec ces changements, les départements informatiques ont eu du mal à suivre le rythme de la sécurité et faire face à l'augmentation des coûts. Tout au long de la pandémie de COVID, les budgets ont été consacrés à des investissements supplémentaires en matériel et en pare-feu, au détriment du chiffrement des données.

On a pu observer une hausse du chiffrement logiciel à l'aide de Microsoft BitLocker® ou de logiciels de gestion unifiée des terminaux de sociétés comme Symantec ou McAfee, entre autres. Certaines entreprises et certains consommateurs utilisent également des clés USB standard avec des logiciels de type « coffre-fort » proposés par certains fournisseurs.

CHIFFREMENT ET DONNÉES EN TRANSIT

Les employés et les consommateurs ont besoin d'emporter leurs données avec eux. Ils disposent de plusieurs options :

1. Les services cloud : Ils sont formidables, car ils sont accessibles depuis n'importe quel appareil pouvant se connecter à Internet. Cependant, la flexibilité a un prix. Le stockage des données dans le cloud prive l'utilisateur ou l'entreprise du contrôle sur leurs données. Qui plus est, il présente un risque potentiel car nous avons déjà observé des serveurs cloud laissés sans verrouillage ou accessibles.
2. Clés USB standard : Bien que le transport d'une clé USB semble plus sûr, le risque d'exposition des données en cas de perte de la clé peut être important. On a ainsi entendu parler de nombreux cas de personnes ayant trouvé des clés USB perdues contenant des informations secrètes. Sans citer les blanchisseries dont les tiroirs regorgent de clés USB perdues par leurs clients.
3. Clés USB à chiffrement matériel : Ces clés USB présentent des architectures personnalisées qui intègrent un contrôleur de chiffrement et un contrôle d'accès intégrés. Les données sont chiffrées à l'aide du chiffrement AES-256 bits le plus puissant en mode XTS en général. Il existe également d'autres mesures de protection disponibles pour atténuer les attaques physiques et celles visant le firmware. Ces clés sont fabriquées par des sociétés spécialisées dans les dispositifs de sécurité et, bien que plus chères que les clés USB standard, elles offrent une meilleure sécurité des données. Les clés FIPS 197 ou FIPS 140-2 niveau 3 peuvent ajouter des niveaux de protection plus élevés, pour une plus grande tranquillité d'esprit.
4. Clés USB standard avec chiffrement logiciel : Par souci de sécurité, comme l'exigent les réglementations, il est possible d'utiliser le chiffrement logiciel avec BitLocker ou d'autres outils. Ce sont des options décentes car elles sont relativement peu coûteuses et offrent le même chiffrement AES-256 XTS .

Il n'est pas surprenant de constater que, dans la plupart des cas, les entreprises et les industries ont tendance à opter pour l'option 4, à savoir l'utilisation de clés USB standard avec chiffrement logiciel. Et ce, parce que le chiffrement logiciel via BitLocker ou d'autres utilitaires de stockage sécurisé des données sont « gratuits ».

LE CHIFFREMENT LOGICIEL N'EST PAS CONFORME À LA RÉGLEMENTATION

Dans l'esprit de nombreux professionnels de la sécurité d'entreprise, le chiffrement logiciel offre exactement les mêmes capacités de chiffrement que les clés USB à chiffrement matériel, mais à moindre coût. Mais est-ce la voie à suivre ? Les budgets étant serrés, les entreprises se tournent vers le chiffrement logiciel pour assurer leur conformité, sans en connaître réellement les inconvénients.

Quel est le problème des clés USB à chiffrement logiciel ? Les données au repos et en transit ne sont-elles pas chiffrées par AES-256 XTS? En général, elles le sont. Le problème est le suivant : Le chiffrement logiciel est considéré comme un « chiffrement amovible ».

Attendez ... amovible ? Cela signifie-t-il qu'une clé USB chiffrée par logiciel peut voir son chiffrement désactivé par un utilisateur ?

La réponse est : oui. Les utilisateurs peuvent supprimer la fonction de chiffrement logiciel de leurs clés USB. Pourquoi le feraient-ils, me demanderez-vous ? Parce qu'ils le peuvent. Et parce qu'ils veulent simplement accéder aux fichiers sans devoir utiliser de mot de passe, ou parce qu'ils ont oublié le mot de passe et doivent utiliser leur clé USB.

COMMENT SUPPRIMER LE CHIFFREMENT LOGICIEL D'UNE CLÉ USB CHIFFRÉE ?

Pour un utilisateur qui souhaite éviter de devoir saisir des mots de passe complexes pour accéder à ses données, le processus est simple :

1. Insérer la clé chiffrée par logiciel dans un ordinateur
2. Formater la clé
3. Une fois la clé formatée, tout le chiffrement est supprimé
4. Copier les fichiers contenant des informations secrètes ou confidentielles sur la clé pour pouvoir y accéder facilement

Cette opération est facile à réaliser par les utilisateurs : il suffit d'utiliser un ordinateur dont l'accès n'est pas restreint. Même si les services informatiques ont restreint l'utilisation des commandes de formatage sur les ordinateurs de l'entreprise, cette opération peut être réalisée sur tout autre ordinateur n'appartenant pas à l'entreprise.

Vient la question de la conformité. Si le chiffrement des données est supprimé (ce qui est simple), la clé fournie par l'entreprise est désormais non chiffrée. Et les données qui étaient chiffrées sur le disque sont considérées comme perdues à jamais une fois le chiffrement supprimé via la méthode ci-dessus (les clés de chiffrement sont liées aux données). Toute donnée copiée sur le périphérique une fois le chiffrement supprimé est considérée comme non sécurisée et potentiellement non conforme, ce qui peut entraîner une violation des réglementations HIPAA, GDPR, CCPA, et bien d'autres.

LES CONSÉQUENCES DES PERTES DE CLÉS NON CHIFFRÉES

Si une clé USB désignée par l'entreprise est perdue et retrouvée (même si l'entreprise ne le sait pas au départ mais l'apprend plus tard par les réseaux sociaux), elle s'expose à des exigences de conformité particulières, ce qui peut la contraindre à :

1. mener une enquête approfondie pour identifier les données perdues ;
2. déterminer si une violation légale a eu lieu, en consultation avec le service juridique ;
3. déterminer si les clients doivent être informés.

Et c'est là qu'une simple perte de clé USB peut s'avérer être très coûteuse. Les honoraires d'avocat dépassant plusieurs centaines de dollars de l'heure, ce processus de conformité peut entraîner des milliers de dollars de dépenses, en plus des amendes potentielles, des poursuites judiciaires des clients et autres, et de l'embarras causé par l'exposition des données.

Lorsque l'on évalue le chiffrement logiciel pour sa mise en œuvre peu coûteuse, on ne tient pas compte de ces risques et leurs énormes conséquences financières.

L'utilisation de clés USB non chiffrées sur un réseau d'entreprise présente un autre risque. C'est ce qu'on appelle communément le « BadUSB ». Le BadUSB est une classe de logiciels malveillants qui a été utilisée par des acteurs mal intentionnés pour franchir le pare-feu des entreprises et introduire des logiciels malveillants dans leurs cyberdéfenses via des périphériques de stockage USB.

BadUSB

Lorsqu'une clé USB est insérée dans un ordinateur, le contrôleur du chipset de l'ordinateur s'associe au contrôleur de la clé USB via un firmware. Cet échange a lieu avant même que le système d'exploitation, tel que Microsoft/macOS/Linux, ne détecte qu'une clé USB a été connectée. Chaque clé USB possède un firmware qui s'exécute lorsqu'elle est connectée à un port USB.

Les acteurs mal intentionnés ont appris qu'ils pouvaient introduire des logiciels malveillants par le biais de ce mécanisme d'association en remplaçant le firmware qui s'exécute sur la clé USB par un autre firmware (malveillant) qui injecte des logiciels malveillants dans le système informatique cible dès lors qu'il communique avec la clé USB. Une clé USB standard ne dispose d'aucune sécurité sur son firmware interne, lequel est exécuté par son contrôleur. C'est ainsi que BadUSB est né, les bonnes clés USB étant utilisées comme armes pour pénétrer les pare-feu et les cyberdéfenses.

De nombreuses entreprises tentent d'interdire l'utilisation de clés USB sur leurs systèmes, et vont même jusqu'à remplir les ports USB d'époxy. Cependant, certains de leurs employés ont besoin de transporter des données avec eux sur des clés USB. Par exemple, les cadres qui doivent emporter des données pour travailler ou les fournir à des conseillers juridiques ou financiers externes qui ne sont pas sur le cloud de l'entreprise ; les sous-traitants qui ont besoin de données pour travailler mais ont un accès limité aux bases de données de l'entreprise ; les analystes financiers qui sont pressés de boucler les rapports mensuels et doivent travailler à domicile.

Comme le montre l'analyse précédente, il existe un risque important à utiliser cette solution standard de clé USB + chiffrement logiciel. À première vue, ce qui semblait moins cher s'avère être potentiellement très nuisible et beaucoup plus coûteux. Il suffit de 2 à 3 heures de consultation d'un avocat au sujet d'une violation potentielle des données pour perdre toutes les économies réalisées en optant pour la solution la moins chère.

LES CLÉS USB À CHIFFREMENT MATÉRIEL SONT LA MEILLEURE OPTION POUR LA CONFORMITÉ RÉGLEMENTAIRE

Voici pourquoi les clés USB avec chiffrement matériel sont le meilleur choix pour ces applications réglementaires :

1. Le chiffrement des clés USB chiffrées au niveau du matériel est toujours activé : Il n'y a aucun moyen pour les utilisateurs de désactiver le chiffrement, de réinitialiser les règles de mot de passe (longueur minimale, complexité) ou de désactiver les tentatives automatiques de saisie du mot de passe. Contrairement au chiffrement logiciel qui n'empêche pas les tentatives répétées de saisie de mot de passe par le biais d'attaques logicielles par dictionnaire, les versions matérielles limitent les tentatives de saisie du mot de passe. Et elles verrouillent les données après 10 saisies (voire moins) d'un mot de passe erroné. C'est très sécurisant à l'ère des super ordinateurs.
2. Les clés à chiffrement matériel utilisent des contrôleurs de chiffrement de première qualité et intègrent de nombreuses fonctions de sécurité : Bien que nous ne divulguions pas toujours toutes les contre-mesures de sécurité, il en existe une pour se protéger du BadUSB. À l'usine, avant de charger le firmware sur les clés à chiffrement matériel, il est signé numériquement. Cela signifie que, lorsque ces clés USB chiffrées sont insérées, le contrôleur de chiffrement vérifie d'abord l'intégrité du firmware par le biais de la signature numérique, et ne le charge que s'il passe la vérification. Toute tentative de remplacement du firmware bloquera la clé, laquelle deviendra non fonctionnelle, et donc inoffensive.
3. Les clés USB à chiffrement matériel peuvent avoir des identifiants de produit (PID) personnalisés, configurés pour une entreprise spécifique : Un identifiant numérique peut être programmé sur ces clés haut de gamme de sorte que, si elles sont connectées au pare-feu interne ou externe de l'entreprise, elles peuvent être identifiées en tant que clés fournies par l'entreprise. Par exemple, si un employé perd la clé de l'entreprise et achète le même modèle au détail, cette nouvelle clé ne sera pas validée sur le réseau de l'entreprise. Cette personnalisation ajoute une autre couche de sécurité à l'utilisation des clés USB.
4. Les clés à chiffrement matériel permettent de réaliser des économies très rapidement : Le simple fait de réduire et d'éliminer les risques rend leur cycle d'amortissement très court.

Kingston est le plus grand fabricant mondial de clés USB chiffrées, proposées dans diverses gammes et fourchettes de prix. Contactez directement Kingston pour savoir comment nous pouvons assurer votre conformité grâce à nos solutions USB chiffrées pour les cadres, les employés, les sous-traitants, etc.