CHIFFREMENT DES DONNÉES, LE GUIDE DES BONNES PRATIQUES

SOMMAIRE

LE CHIFFREMENT EN TOUTE SIMPLICITÉ. LES DONNÉES AVANT TOUT.

La protection proactive des données est un impératif général. Les principaux marchés dans le monde obligent les entreprises de toutes tailles à mettre en œuvre des mesures de sécurité et de confidentialité des données. Qu'il s'agisse des directives PCI DSS, HIPAA, SOX, DPP au niveau de l'UE, PIPA au Japon ou de la loi britannique relative à la protection des données (Data Protection Act), les autorités tendent à exiger des entreprises qu'elles prennent des mesures visant à protéger les données sensibles. Au Royaume-Uni, par exemple, l'ICO (Information Commissioner Office), la commission relative aux informations, a indiqué que les pertes de données « non protégées par chiffrement » risquent d'entraîner l'adoption de nouvelles mesures réglementaires.

1. INTRODUCTION

Dans une étude récemment menée par Kaspersky Lab, 29 % des entreprises ont affirmé avoir subi une perte ou un vol d'appareil mobile. Selon Kensington, un ordinateur portable est volé toutes les 53 secondes.[1&2]

Au vu de ces statistiques vous êtes peut-être déjà en train d'estimer les coûts de remplacement du matériel, mais le principal problème n'est pas là. Ces coûts ne sont certainement pas les bienvenus pour votre entreprise mais, en cas de perte des données, il y a fort à parier qu'ils soient le cadet de vos soucis. Lorsqu'un ordinateur portable ou un appareil est volé ou perdu, la réparation des dégâts occasionnés par la fuite des données représente plus de 80 % des coûts associés[3] à cet incident et ce, quelle que soit la taille de l'entreprise.

Si l'on tient compte du nombre croissant d'amendes infligées par les autorités pour violation des données, des préjudices causés à la réputation d'une société et de l'impact sur la fidélisation des clients, il n'est donc guère surprenant que les coûts liés à la violation des données aillent bien au-delà du simple remplacement des équipements. 85% des clients dans le monde se disent prêts à s'adresser à la concurrence si leurs informations personnelles étaient perdues ou piratées et 47 % seraient favorables à une action en justice.[4]

Sans compter que la perte des données sensibles n'est pas obligatoirement liée à la perte physique d'un périphérique. Les données sensibles de l'entreprise, la propriété intellectuelle et les secrets commerciaux sont devenus la cible des attaques de programmes malveillants.

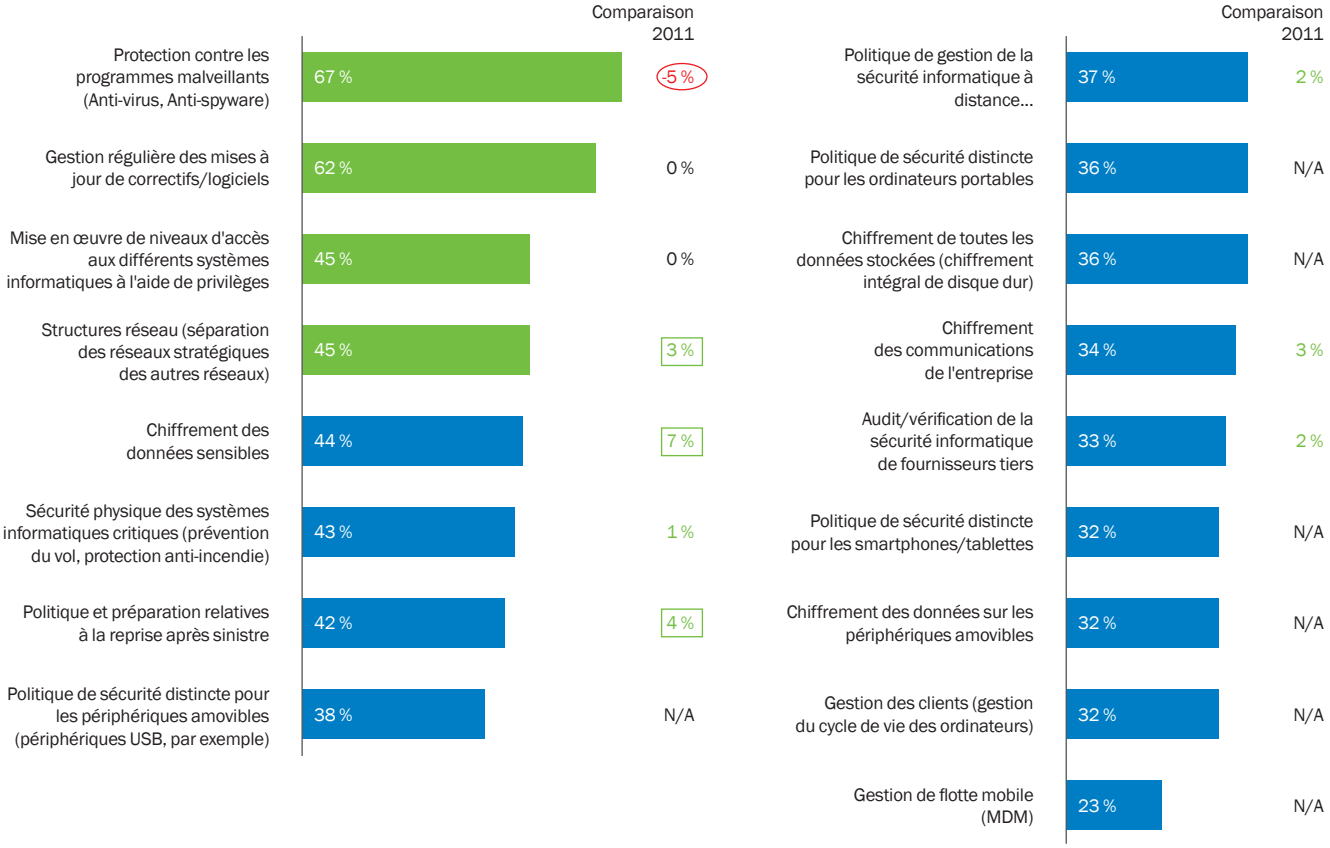
Le Ponemon Institute révèle que la valeur moyenne d'un ordinateur portable perdu s'élève à 49 246 $, 2 % seulement étant imputables aux coûts de remplacement matériel. Le chiffrement peut, en moyenne, réduire de plus de 20 000 $ le coût d'un ordinateur portable.[5] Que vous vous trouviez confronté au vol d'un ordinateur portable, à la perte d'un périphérique de stockage ou au vol de données par des programmes malveillants, le chiffrement offre une garantie dans la mesure où les criminels ou individus non autorisés ne pourront pas exploiter les données sensibles.

Quelle est donc la meilleure approche à adopter ?

1 Source : rapport 2012 de Kaspersky sur les risques informatiques mondiaux
2 Source : Kensington : The Cost of Stolen or Lost Laptops, Tablets and Phones (Le coût des vols ou pertes d'ordinateurs portables, tablettes et téléphones), 2012
3 Source : Ponemon : The Billion Dollar Lost Laptop Problem (2012)
4 Source : Unisys Security IndexTM : RÉSUMÉ MONDIAL 18 october 2011 (Wave 2H'11)
5 Source : Ponemon : The Cost of a Lost Laptop (2009)

2. APPROCHES RECOMMANDÉES

Il n'y a pas si longtemps, le chiffrement était considéré comme l'apanage du secteur public ou des grandes entreprises disposant de budgets importants. La technologie a bien évolué depuis lors. À l'heure actuelle, les entreprises de toutes tailles peuvent se permettre de mettre en œuvre des solutions de chiffrement efficaces et simples à gérer.



L'utilisation du chiffrement est de plus en plus répandue pour lutter contre la perte de données.[6]

Les pages suivantes présentent quelques recommandations permettant de garantir l'adoption d'une stratégie de chiffrement performante au sein de votre entreprise.

6 Source : rapport 2012 de Kaspersky sur les risques informatiques mondiaux

3. DÉFINISSEZ DES POLITIQUES, RENFORCEZ LES AVEC DES OUTILS

En termes de chiffrement, comme dans de nombreuses stratégies de sécurité, il est recommandé de commencer par mettre en place de solides politiques : qu'est-ce que vous allez chiffrer ? L'intégralité des disques? Les périphériques de stockage amovibles ? Certains types de données, de fichiers ou de dossiers ? Vous souhaitez peut-être que certains documents ne soient pas lisibles par certains utilisateurs mais accessibles à d'autres ? Pourquoi ne pas bénéficier d'une solution alliant un peu des deux ?

Pour la plupart des entreprises, la priorité consiste à mettre à disposition les informations destinées aux personnes concernées, au moment opportun. En associant des politiques efficaces à des technologies adaptées, vous y parviendrez sans compromettre la sécurité.

Commencez, avant tout, par :

- **Inclure toutes les parties prenantes**, à savoir la direction informatique, les services administratifs et financiers. Ils vous aideront à déterminer les types d'informations nécessitant une protection supplémentaire.
- **Contrôler les accès** : inutile de sécuriser quoi que ce soit si tout le monde y a accès. Collaborez avec les parties prenantes pour identifier les utilisateurs ayant besoin d'un accès, les types d'informations auxquels ils doivent pouvoir accéder, ainsi que le moment où ils doivent pouvoir y accéder. Procédez régulièrement, à titre préventif, à un audit des contrôles d'accès afin d'en garantir la pertinence.
- **Identifiez vos besoins en matière de conformité** aux normes PCI DSS, HIPAA, SOX, DPP au niveau de l'UE, PIPA au Japon ou à la loi britannique relative à la protection des données (Data Protection Act). Vous n'êtes peut-être pas au fait du nombre croissant de réglementations entrant en vigueur en matière de protection des données, mais bon nombre de vos collaborateurs le sont. Identifiez les réglementations, législations, directives et autres facteurs externes qui régissent la manière dont les données sont sécurisées ou échangées au sein de l'entreprise. Définissez des politiques qui prennent en compte ces nouvelles normes. Vous pouvez, par exemple, effectuer un chiffrement automatique des données concernant les cartes de crédit des clients ou des numéros de sécurité sociale des employés.
- **En résumé**, rédigez votre politique par écrit, demandez à la direction de l'avaliser et informez-en vos utilisateurs finaux, sans oublier les tiers qui gèrent vos données sensibles. Qu'ils n'apprécient pas une telle démarche n'est pas un problème, l'essentiel est qu'ils ne puissent pas accéder à vos données.
- **Effectuez une sauvegarde**. Il est toujours recommandé de sauvegarder vos données avant d'installer un nouveau logiciel, quel qu'il soit. Il en va de même pour le chiffrement. Assurez-vous de sauvegarder toutes les données de vos utilisateurs finaux avant de lancer votre programme de chiffrement.

4. CHIFFREMENT INTÉGRAL DU DISQUE OU CHIFFREMENT DES FICHIERS ?

Une seule réponse : les deux. Les solutions de chiffrement offrent généralement deux options : chiffrement intégral du disque et chiffrement au niveau des fichiers, chacune présentant ses propres avantages :

4.1 Avantages du chiffrement intégral du disque :

- Cette option protège les « données statiques » résidant au plus proche du disque dur (chaque secteur du disque est chiffré). Autrement dit, l'intégralité des données de votre disque dur sont chiffrées, y compris le contenu des fichiers, les métadonnées, les informations des systèmes de fichiers ainsi que l'arborescence des répertoires. Seuls les utilisateurs authentifiés peuvent accéder au disque chiffré. Outre les disques durs, la technologie de chiffrement intégral du disque peut être appliquée aux supports amovibles tels que des lecteurs USB ou des disques durs externes.
- Adoptez un processus d'authentification avant le démarrage qui obligera les utilisateurs à suivre ce processus pour accéder aux données avant même le lancement du système d'exploitation. Vous renforcez ainsi la sécurité en cas de perte ou de vol de l'ordinateur portable puisqu'aucune donnée ne pourra être lue directement à partir de la surface du disque et que le système d'exploitation ne pourra pas être démarré.
- Le chiffrement du disque complet comprend également une politique de « réglage permanent » qui élimine de l'équation tout choix émanant de l'utilisateur ; proposez un accès via un processus d'authentification unique, vos utilisateurs ne s'apercevront de rien.
- Le principal atout de cette solution est d'éliminer les risques d'erreurs commises par les utilisateurs puisque tout est chiffré. En revanche, elle ne peut pas protéger les données en transit, notamment les informations partagées entre les périphériques. Si vous suivez ces recommandations et avez opté pour une solution qui permet également le chiffrement au niveau des fichiers, cela ne vous posera pas de problème.

4.2 Avantages du chiffrement au niveau des fichiers :

Grâce à ce processus, les « données statiques » ainsi que les « données en circulation » sont protégées. Vous pouvez également chiffrer des fichiers et des dossiers spécifiques, quel que soit le périphérique utilisé. Des solutions haut de gamme permettent aux fichiers chiffrés de conserver leur chiffrement, même lorsqu'ils sont copiés via le réseau, les rendant ainsi non lisibles par des individus non autorisés, quel que soit l'emplacement où ces fichiers sont stockés ou copiés. Cette technologie offre aux administrateurs la possibilité de chiffrer automatiquement des fichiers en fonction d'attributs tels que l'emplacement (par exemple, tous les fichiers résidant dans le dossier Mes Documents), le type de fichier (par exemple, tous les fichiers texte, feuilles de calcul Excel etc.) ou le nom de l'application procédant à l'écriture du fichier. Une solution performante supportera, par exemple, le chiffrement des données écrites par Microsoft Word, indépendamment du dossier ou du disque.

- Le chiffrement au niveau des fichiers offre plus de souplesse aux entreprises qui cherchent à appliquer des politiques d'accès aux informations à un niveau granulaire. Seules les données à caractère sensible sont chiffrées (conformément aux politiques définies par l'administrateur), permettant ainsi le support des cas de figure utilisant des données mixtes.
- Il facilite également la maintenance des systèmes de manière simple et sécurisée. Les fichiers de données peuvent, de ce fait, rester sécurisés et les fichiers logiciels ou système sont accessibles, facilitant les mises à jour ou d'autres opérations de maintenance. Les directeurs financiers peuvent, par exemple, s'appuyer sur ce type de chiffrement s'ils souhaitent ne pas divulguer des informations internes à l'entreprise aux administrateurs système.
- En outre, cette technologie permet de contrôler efficacement les privilèges, offrant ainsi aux administrateurs la possibilité de définir des règles de chiffrement précises destinées à des applications et à des scénarios d'utilisation spécifiques. Grâce à ce contrôle, ils décident du moment où ils souhaitent mettre à disposition des données chiffrées, voire même bloquer complètement l'accès à ces données pour des applications précises, par exemple :
  - simplifier les sauvegardes sécurisées en s'assurant que les données restent chiffrées pendant leur transfert, leur stockage et leur restauration, quels que soient les paramètres des politiques en vigueur au niveau du terminal sur lequel les données sont restaurées ;
  - empêcher l'échange de fichiers chiffrés par messagerie instantanée ou sur Skype, sans toutefois restreindre les échanges de messages légitimes.

En adoptant une approche combinée de chiffrement de disque et de fichiers, les entreprises peuvent bénéficier des avantages des deux méthodes, par exemple choisir le chiffrement des fichiers uniquement pour les ordinateurs de bureau, tout en appliquant un chiffrement intégral des disques sur tous les ordinateurs portables.

5. PENSEZ À CHIFFRER LES SUPPORTS AMOVIBLES

Certaines clés USB sont aujourd'hui capables de stocker jusqu'à plus de 100 Go, et des disques durs portables tenant dans le creux de la main ont des capacités de stockage de données de l'ordre de plusieurs téraoctets. Soit un volume considérable d'informations potentiellement stratégiques pouvant traîner dans la poche d'une veste partie au pressing, être oubliées au contrôle de sécurité d'un aéroport ou tout simplement tomber par terre sans qu'on s'en aperçoive.

S'il est impossible d'agir sur le manque d'attention des utilisateurs, les conséquences de ce genre d'incidents peuvent toutefois être contrôlées. Toute stratégie de chiffrement efficace repose notamment sur le chiffrement des périphériques. Grâce à celui-ci, les données transférées d'un terminal vers un périphérique amovible sont systématiquement chiffrées. Pour ce faire, vous pouvez appliquer des politiques de chiffrement de disque ou de fichiers à l'ensemble des périphériques et garantir ainsi la protection des données sensibles en cas de perte ou de vol.

Si vous utilisez des informations sensibles hors de votre périmètre de sécurité, vous devez adopter le « mode portable ». Supposons que vous effectuez une présentation lors d'une conférence. Vous devez utiliser une clé USB pour transférer vos données sur un ordinateur public sur lequel aucun logiciel de chiffrement n'est installé. Vous devez faire en sorte que vos données restent protégées, même lors de leur transfert de votre ordinateur portable vers le système de présentation. Pour ce faire, les meilleures solutions intègrent un mode portable. Celui-ci permet d'utiliser et de transférer en toute simplicité des données sur un support amovible chiffré, même sur les ordinateurs sans logiciel de chiffrement.

6. CHOISISSEZ UNE TECHNOLOGIE DE CHIFFREMENT ÉPROUVÉE

L'efficacité d'une stratégie de chiffrement dépend directement de la qualité des technologies sur lesquelles elle s'appuie. Les algorithmes de chiffrement pouvant être facilement piratés ne servent absolument à rien. Le chiffrement AES (Advanced Encryption Standard) à clés de 256 bits est considéré comme la référence en matière de techniques de chiffrement. Cette méthode utilisée par l'administration américaine constitue la norme professionnelle la plus répandue au monde. Ne sous-estimez pas l'importance des clés : votre algorithme de chiffrement n'aura aucune efficacité si la clé correspondante n'est pas suffisamment sûre. Des clés facilement piratables rendent un programme de chiffrement totalement inutile. De la même façon, une gestion intelligente des clés est essentielle à l'efficacité d'un système de chiffrement : avoir une porte blindée ne sert pas à grand-chose si on laisse la clé sous le paillasson.

7. N'OUBLIEZ PAS LA PROTECTION CONTRE LES PROGRAMMES MALVEILLANTS

Les données stockées sur un ordinateur portable courent un risque de perte, même sans vol ou perte du support. De plus en plus, les cybercriminels ciblent les informations sensibles stockées sur les appareils professionnels portables ; ils écrivent du code malveillant permettant de les dérober à l'insu de leur utilisateur.

Aucune stratégie de chiffrement ne peut être considérée comme complète si elle n'intègre pas une protection contre les programmes malveillants capable de détecter les codes conçus pour dérober les informations sensibles stockées sur un ordinateur portable. Les meilleures pratiques préconisent l'automatisation des mises à jour et analyses des outils de protection contre les programmes malveillants, sans intervention de la part de l'utilisateur.

8. QUE FAIRE EN CAS DE MOT DE PASSE OUBLIÉ?

On oublie ses mots de passe presque aussi souvent qu'on perd une clé USB ou un smartphone. Parfois, même le meilleur matériel ou système d'exploitation subit des pannes, empêchant ainsi d'accéder à des informations essentielles. Conservez vos clés de chiffrement à un emplacement de stockage centralisé. Cela facilitera considérablement le déchiffrement des données en cas d'urgence.

Une solution de chiffrement de qualité doit fournir aux administrateurs des outils simples de restauration des données dans les cas suivants :

- Lorsque l'utilisateur final en a besoin (en cas de mot de passe oublié, par exemple)
- Lorsque l'administrateur en a besoin pour la maintenance ou en cas de problème technique, par exemple lorsqu'un système d'exploitation ne démarre plus ou qu'un disque dur est endommagé et doit être réparé.

Lorsqu'un utilisateur oublie son mot de passe, une méthode d'authentification alternative consiste à lui demander de répondre correctement à une série de questions.

9. CENTRALISEZ POUR SIMPLIFIER

L'une des critiques les plus fréquemment exprimées par les entreprises souhaitant déployer un système de chiffrement est que ceux-ci se révèlent trop compliqués à mettre en œuvre et à gérer. Nombre de solutions de l'ancienne génération n'intègrent pas en effet directement la protection contre les programmes malveillants, complexifiant ainsi davantage la situation. La gestion de plusieurs solutions (protection contre les programmes malveillants, contrôle des terminaux, chiffrement, etc.), même lorsqu'elles proviennent du même fournisseur, est à la fois coûteuse et chronophage à toutes les étapes du cycle d'adoption : achat, formation, provisionnement, gestion des politiques, maintenance et mise à niveau doivent tous être traités de manière distincte pour chaque composant. C'est pourquoi une approche intégrée permet non seulement de gagner du temps et de l'argent, mais simplifie en outre considérablement le processus d'adoption du logiciel.

Les solutions faciles à gérer sont les plus efficaces. Choisissez-en une permettant dès le départ d'effectuer les tâches d'administration via une seule console, en vertu d'une seule et même politique. Vous réduirez ainsi le montant de votre investissement et supprimerez les problèmes de compatibilité entre divers composants devant être gérés séparément. Une bonne pratique consiste à appliquer les paramètres de chiffrement des terminaux à la même politique que celle utilisée pour les paramètres de protection contre les programmes malveillants, paramètres de contrôle des périphériques et paramètres de protection des terminaux. La meilleure pratique, consistant à mettre en œuvre des politiques intégrées et cohérentes, devient ainsi applicable. Les services informatiques peuvent, par exemple, d'une part, autoriser la connexion d'un support amovible autorisé à un ordinateur portable et d'autre part, appliquer des politiques de chiffrement au périphérique. Une plate-forme technologique étroitement intégrée présente en outre l'avantage d'améliorer l'ensemble des performances des systèmes.

10. CONCLUSION

Kaspersky Endpoint Security for Business peut contribuer à faire des meilleures pratiques de chiffrement une réalité pour les entreprises de toutes tailles. En associant les systèmes de chiffrement les plus solides à nos propres technologies de protection contre les programmes malveillants et de contrôle des terminaux, notre plate-forme intégrée contribue à protéger les données sensibles contre les risques liés à la perte ou au vol de périphériques, tout en isolant les informations des programmes malveillants utilisés pour dérober des données.

Des contrôles précis et de nombreuses fonctionnalités peuvent facilement être déployés depuis une seule console de gestion, offrant ainsi aux administrateurs une vue réellement centralisée de leur environnement de sécurité, qu'il s'agisse de machines virtuelles ou physiques ou de périphériques mobiles et amovibles.

Contrairement à de nombreuses approches classiques de la protection des données, Kaspersky Endpoint Security for Business propose une approche intégrale de la gestion centralisée des politiques : les politiques de chiffrement sont définies au sein des mêmes politiques générales de protection contre les programmes malveillants, de contrôle des périphériques, de contrôle des applications et de protection des terminaux. Cette approche intégrale est rendue possible par le code unifié de Kaspersky : nos développeurs créent des logiciels et technologies interagissant de façon transparente, fournissant ainsi aux utilisateurs une plate-forme de sécurité au lieu d'une suite de produits hétéroclites.

L'intégration étroite des composants de sécurité essentiels tels que la protection contre les programmes malveillants, le chiffrement, le contrôle des applications et celui des périphériques simplifie la gestion et la surveillance, tout en apportant de la stabilité, des politiques intégrées, des fonctions de compilation des rapports et des outils intuitifs.

Un seul fournisseur, un seul coût, une seule installation, soit la garantie d'une sécurité totale.

IDENTIFIER.
CONTRÔLER. PROTÉGER.

Avec Kaspersky, maintenant, c'est possible !
kaspersky.fr/business-security

Be Ready for What's Next

Kaspersky Lab France
www.kaspersky.fr