KASPERSKY lab

GUIDE DES BONNES PRATIQUES

Chiffrement

www.kaspersky.fr

VOTRE GUIDE DES BONNES PRATIQUES CONCERNANT LE CHIFFREMENT.

Agir pour la protection des données.

La protection proactive des données est un impératif mondial pour les entreprises. Kaspersky Lab peut vous aider à mettre en œuvre la plupart des meilleures pratiques en matière de protection et de chiffrement des données.

L'importance du chiffrement

Plus de **816** millions de données ont été compromises depuis 2005[1]. Rien qu'au cours des quatre premiers mois de 2015, plus de **101** millions de données ont été exposées[2].

Il se passe rarement une semaine sans qu'un piratage de données de grande ampleur ne fasse la une de l'actualité. Le Identity Theft Resource Center a proclamé 2014 « Année du piratage de données », citant les données stockées sur les appareils mobiles ou amovibles et les violations d'accès internes par des employés non autorisés à accéder à des données sensibles parmi les principales causes de fuite ou de perte de données[3]. Près d'une entreprise sur cinq interrogée par Kaspersky Lab a subi des pertes de données des suites directes de vols d'appareils[4].

Les recherches de Kaspersky Lab ont révélé que le coût moyen d'une perte de données en 2014 s'élevait à **636 000 $** pour une grande entreprise et à **33 000 $** pour une PME[4]. Sans compter que la perte des données sensibles n'est pas obligatoirement liée à la perte physique d'un appareil. Les données sensibles de l'entreprise, la propriété intellectuelle et les secrets commerciaux sont devenus la cible des attaques de programmes malveillants.

Les conséquences ne se limitent pas au coût direct d'une violation, à la perte de clients fidèles ou aux atteintes à l'image de l'entreprise (72 % des entreprises ont dû reconnaître publiquement un incident[4]). Sur la plupart des grands marchés, la sécurité et la confidentialité des données sont désormais une obligation légale et certains pays contraignent les organisations à chiffrer les données sensibles.

Qu'il s'agisse des directives PCI DSS, HIPAA, SOX, DPP en ce qui concerne l'Union européenne, la loi PIPA au Japon ou le Data Protection Act au Royaume-Uni, 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 des mesures réglementaires.

Que vous vous trouviez confronté au vol d'un ordinateur portable, à la perte d'un appareil 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 Privacy Rights Clearing House : http://www.privacyrights.org/data-breach
2 Identity Theft Resource Center 2015 : http://www.idtheftcenter.org/images/breach/ITRCBreachStatsReport2015.pdf
3 Identity Theft Resource Center 2015 : http://www.idtheftcenter.org/Press-Releases/2014breachstatistics.ht
4 Kaspersky Lab : Rapport sur les risques liés à la sécurité informatique 2014

Les meilleures pratiques en matière de chiffrement

La technologie de chiffrement de Kaspersky Lab protège les données importantes en cas de perte ou de vol d'un appareil ou d'attaques malveillantes ciblées.

1. METTEZ EN PLACE DES POLITIQUES QUE VOUS CONSOLIDEREZ PAR LA SUITE PAR DES TECHNOLOGIES

Comme pour la plupart des stratégies en matière de sécurité, les meilleures pratiques de chiffrement commencent par l'établissement de politiques solides. Allez-vous chiffrer les disques intégralement ? Les appareils 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 des 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 :

- **Impliquer toutes les parties prenantes concernées** : gestion informatique, opérations, finances, RH, etc. Ces acteurs vous aideront à déterminer le type d'informations nécessitant une protection supplémentaire.
- **Contrôler les accès** : inutile de sécuriser quoi que ce soit si tout le monde y a accès. Collaborer 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, par précaution supplémentaire, à un audit des contrôles d'accès afin d'en garantir la pertinence.
- **Identifier vos besoins en matière de conformité** : PCI DSS, HIPAA, SOX, DPP au niveau de l'Union européenne, PIPA au Japon ou Data Protection Act au Royaume-Uni. 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 de carte 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.
- **Effectuer 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 d'exécuter votre programme de chiffrement.
- **Privilégier la simplicité** : minimisez la tâche de l'utilisateur final et le risque d'intrusion par la mise en œuvre de technologies prenant en charge l'authentification unique.

2. CHIFFREMENT INTÉGRAL DU DISQUE OU CHIFFREMENT DES FICHIERS ?

La réponse est simple : 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.

Avantages du chiffrement intégral du disque :

La technologie de chiffrement intégral du disque (FDE) est l'une des méthodes les plus efficaces que puisse adopter une entreprise pour se protéger du vol ou de la perte de données. Quoi qu'il arrive à l'appareil, le FDE permet aux entreprises de s'assurer que toutes les données sensibles sont totalement illisibles et inexploitables pour les criminels ou les indiscrets.

- Cette option protège les « données statiques » 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 dans un boîtier USB.

- Recherchez l'authentification avant démarrage (PBA). Les utilisateurs sont invités à présenter et à authentifier leurs données d'identification avant le démarrage du système d'exploitation, ce qui apporte une couche de sécurité supplémentaire. Rien ne peut être lu directement à partir de la surface du disque dur par les voleurs, et le système d'exploitation ne peut pas non plus être démarré.

  La technologie de chiffrement de Kaspersky Lab fournit l'authentification PBA avec en option l'authentification unique, et elle fonctionne par ailleurs avec les claviers non-QWERTY pour une meilleure expérience utilisateur. Les solutions de chiffrement qui prennent en charge l'authentification par carte à puce et jeton à l'aide d'une authentification à double facteur éliminent le besoin de mots de passe supplémentaires, ce qui améliore l'expérience utilisateur.

- Recherchez une solution de chiffrement qui procède à des vérifications de compatibilité avec tout le matériel réseau **avant** la mise en œuvre, pour vous éviter des soucis ultérieurs. Les solutions qui prennent en charge les plateformes UEFI, y compris les tout derniers ordinateurs portables et stations de travail Windows 8 et ultérieurs, vous assureront d'être prêt pour le futur.

  De même, la prise en charge de la technologie Intel AES-NI – dernière amélioration de l'algorithme AES (Advanced Encryption Standard) qui accélère le chiffrement pour les familles de processeurs Intel Xeon et Core (ainsi que certains processeurs AMD) – et des dernières normes de disque GPT contribue à une stratégie de chiffrement complète.

- Activez le partage sécurisé des données au sein de l'entreprise en utilisant le chiffrement FDE sur les lecteurs amovibles.

- 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. L'authentification à double facteur apporte une couche de protection supplémentaire et élimine la nécessité de noms d'utilisateur et de mots de passe supplémentaires, pour simplifier davantage l'utilisation. Les solutions de chiffrement qui prennent en charge le contrôle des accès basé sur les rôles (RBAC) permettent de déléguer la gestion du chiffrement en fonction des rôles/fonctions pour plus de facilité.

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 appareils. 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.

Avantages du chiffrement au niveau des fichiers (FLE) :

Fonctionnant au niveau du système de fichiers, le FLE permet non seulement la protection des « données statiques » mais sécurise également les « données en cours d'utilisation ». Avec le FLE, des fichiers et dossiers spécifiques d'un appareil donné peuvent être chiffrés. Des solutions haut de gamme permettent aux fichiers chiffrés de conserver leur chiffrement, même lorsqu'ils sont copiés via le réseau, les rendant ainsi illisibles à des individus non autorisés, indépendamment de l'emplacement où ils sont stockés ou copiés. Cette technologie offre aux administrateurs la possibilité de chiffrer automatiquement des fichiers en fonction d'attributs tels que l'emplacement (p. ex., tous les fichiers résidant dans le dossier Mes Documents), le type de fichier (p. ex., tous les fichiers texte, feuilles de calcul Excel etc.) ou le nom de l'application procédant à l'écriture du fichier. Une solution performante prendra, par exemple, en charge le chiffrement des données écrites par Microsoft Word, indépendamment du dossier ou du disque.

- Le FLE 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 la prise en charge 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 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 FDE/FLE du chiffrement, les entreprises peuvent bénéficier des avantages des 2 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.

3. METTEZ EN ŒUVRE UN CHIFFREMENT DES SUPPORTS AMOVIBLES

À l'heure actuelle, certaines clés USB sont 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 appareils. Grâce à celui-ci, les données transférées d'un terminal vers un appareil amovible sont systématiquement chiffrées. Pour ce faire, vous pouvez appliquer des politiques de FDE ou de FLE à l'ensemble des appareils et garantir ainsi la protection des données sensibles en cas de perte ou de vol.

Les solutions de chiffrement les plus efficaces s'intègrent à des capacités de contrôle étendu des appareils, afin de prendre en charge l'application granulaire des politiques jusqu'aux numéros de série d'appareils précis.

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.

Optez pour une technologie de cryptographie 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. Choisissez une solution de chiffrement qui utilise la norme Advanced Encryption Standard (AES) avec une longueur de clé de 256 bits, une gestion des clés et un stockage en dépôt simplifiés. La prise en charge de la technologie Intel® AES-NI ainsi que des plateformes UEFI et GPT aidera votre stratégie à résister à l'épreuve du temps.

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.

Optez pour une sécurité multiniveaux

Les utilisateurs finaux et les appareils perdus ne sont pas les seules causes de perte de données. Les voleurs de données développent des programmes malveillants de plus en plus sophistiqués capables d'accéder aux systèmes et de voler les données sans faire de bruit, voire d'agir plusieurs années sans être détectés. Même si le chiffrement rend les données volées inexploitables, il est beaucoup plus efficace lorsqu'il constitue une couche complémentaire dans le cadre d'une stratégie plus vaste de sécurité intégrée, comprenant des contrôles de haute qualité des programmes malveillants, des appareils et des applications réduisant ensemble le risque que des criminels n'accèdent aux systèmes et ne volent des données sensibles.

Aucune stratégie de chiffrement conforme aux bonnes pratiques ne saurait être complète sans couches intégrées de protection contre les programmes malveillants et de contrôles, pour détecter et atténuer les effets des codes malveillants, tout en analysant, détectant et gérant par ailleurs les vulnérabilités qui exposent les organisations à la perte de données. Tout cela sans désagrément pour l'utilisateur, voire sans qu'il n'en soit même conscient.

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 de 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.

Administrer de manière centralisée

Le chiffrement a acquis la réputation d'être trop complexe à implémenter et à gérer. Cette situation est due en grande partie au fait que des solutions anciennes plus traditionnelles sont proposées séparément des protections contre les programmes malveillants et autres technologies de sécurité informatique, engendrant ainsi une complexité inutile. 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 de mise en œuvre : 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 multiniveaux totalement intégrée permet non seulement de gagner du temps et de l'argent mais simplifie aussi considérablement le processus d'adoption du logiciel.

Les solutions faciles à gérer sont les plus efficaces. Choisissez-en une permettant d'effectuer les tâches d'administration via une seule console, selon une seule politique. Vous réduirez ainsi votre investissement et supprimerez les problèmes de compatibilité entre divers composants devant être gérés séparément.

Une bonne pratique consiste à appliquer des paramètres de chiffrement des terminaux dans le cadre de la même politique que celle appliquée aux paramètres de protection contre les programmes malveillants, de contrôle des appareils et 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 à l'appareil. Une plateforme technologique étroitement intégrée présente en outre l'avantage d'améliorer l'ensemble des performances des systèmes.

POUR FINIR...

Kaspersky Endpoint Security for Business peut contribuer à faire des bonnes pratiques de chiffrement une réalité pour les entreprises de toutes tailles.

Une intégration totale des technologies inégalées de Kaspersky Lab pour la protection contre les programmes malveillants et le contrôle et la gestion des terminaux assure une véritable sécurité multiniveaux sur la base d'un code commun. Les paramètres de chiffrement peuvent s'appliquer sous la même politique que la protection contre les programmes malveillants, le contrôle des appareils et d'autres éléments de sécurité des terminaux. Il n'est pas nécessaire de déployer et d'administrer plusieurs solutions distinctes. La compatibilité du matériel réseau est automatiquement vérifiée avant l'application du chiffrement ; les plateformes UEFI et GPT bénéficient d'une prise en charge standard.

Cette approche intégrale est rendue possible par le code unifié de Kaspersky Lab : nos développeurs créent des logiciels et technologies interagissant de façon transparente, fournissant ainsi aux utilisateurs une plateforme de sécurité intégrée au lieu d'une série de produits hétéroclites.

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


Twitter.com/
KasperskyFrance


Facebook.com/
KasperskyLabFrance


Youtube.com/
KasperskyFrance

Kaspersky Lab
www.kaspersky.fr

Tout savoir sur la sécurité
sur Internet :
www.securelist.com
http://www.viruslist.com/fr/

Rechercher un partenaire près de chez vous :
http://www.kaspersky.fr/partners/buyoffline/liste-des-partenaires

KASPERSKY lab