

LES CINQ MEILLEURES PRATIQUES DE LA PROTECTION DE DONNÉES DE SAUVEGARDE

Le cryptage des sauvegardes devrait faire partie des nombreuses activités composant une stratégie de sécurité complète. Dans de nombreux domaines, le stockage s'est effectué pendant un certain temps hors du champ d'intervention des responsables de la sécurité, car leur principale préoccupation portait sur des points précis tels que la sécurité réseau, la détection/prévention des intrusions et la protection des systèmes hôtes. L'infrastructure de stockage - stockage primaire et plus précisément les copies du stockage primaire - risque par conséquent de devenir le talon d'Achille des stratégies de sécurité. Les politiques en matière de sécurité des données sont du ressort de la société et devraient être un élément fondamental de la stratégie de sécurité d'une entreprise. Elles peuvent alors donner lieu à des politiques stratégiques et opérationnelles grâce aux efforts combinés des organisations de sécurité et de stockage. À cette fin, le stockage doit faire partie intégrante de la stratégie de sécurité de la société.

Pour atteindre ces objectifs, une entreprise doit mettre en place une pratique organisée autour de cinq axes principaux :

- 01** L'affectation des responsabilités, des devoirs et des autorisations
- 02** L'évaluation des risques
- 03** Le développement d'une procédure de protection des données
- 04** La communication de la procédure
- 05** L'exécution et l'évaluation de la procédure

01 AFFECTATION DES RESPONSABILITÉS, DES DEVOIRS ET DES AUTORISATIONS

Faites de la sécurité du stockage un élément essentiel de vos politiques et de votre structure de sécurité de l'information. Même si les sociétés décident que les responsabilités en matière de sécurité de stockage ou des sauvegardes doivent reposer sur l'équipe de stockage, elles doivent néanmoins harmoniser ces mesures de sécurité avec celles assurant la sécurité du reste de l'infrastructure. L'harmonisation des mesures de stockage et de sauvegarde contribuera à la consolidation de la protection du système dans son ensemble.

Répartissez les tâches lorsque les données sont très sensibles. Il est plus prudent de s'assurer que la personne qui autorise les accès n'est pas celle chargée de l'exécution.

90 %
des entreprises qui subissent des pertes de données significatives mettent la clé sous la porte dans les deux ans qui suivent.

Source : CHAMBRE DE COMMERCE DE LONDRES

02 ÉVALUATION DES RISQUES LIÉS AU STOCKAGE PAR RAPPORT À LA SÉCURITÉ DE L'INFORMATION

ANALYSEZ LES RISQUES DE TOUTE LA PROCÉDURE DE SAUVEGARDE.

Les responsables doivent examiner chaque étape de leur procédure de sauvegarde afin de déceler les éventuelles failles de sécurité. Un administrateur de bandes pourrait-il créer secrètement des copies des bandes de sauvegarde ? Les conteneurs sont-ils soigneusement rangés ? Existe-t-il une chaîne de traçabilité stricte qui permet le suivi de vos bandes de sauvegarde du début à la fin ? Si les données sont sauvegardées et transférées sans cryptage, des failles de ce type pourraient faire de ces données sensibles une cible facile.

ANALYSEZ LES COÛTS/AVANTAGES DU CRYPTAGE DES DONNÉES DE SAUVEGARDE.

Si l'analyse des risques révèle de nombreuses failles, l'organisation doit se demander si le cryptage n'est pas justifié. Cette étude ne doit pas se limiter aux seules licences d'utilisation des logiciels ou au coût des périphériques et doit également inclure les coûts des opérations liées au cryptage dans les processus de sauvegarde et de récupération après sinistre, ainsi que l'impact du cryptage sur le temps de récupération. Afin de déterminer s'il est économiquement viable ou non de mettre en œuvre le cryptage de manière généralisée ou partielle, le coût total du cryptage doit être comparé aux risques potentiels et à la probabilité d'une atteinte à la sécurité. Étant donné les récentes séries d'événements, le cryptage sur bande des données sensibles s'avère un investissement très utile.

IDENTIFIEZ LES DONNÉES SENSIBLES.

Identifiez les fichiers, bases de données et rubriques considérés comme étant suffisamment sensibles par les différentes unités professionnelles pour justifier un coût de protection supplémentaire. Sachez en outre où vos données sont sauvegardées. Il arrive souvent que les données soient dupliquées dans l'environnement. Il est important de disposer de politiques et procédures permettant de bien savoir, à tout moment, où les données sont conservées. Par exemple, les sociétés ont des informations dans des ordinateurs portables qui sont susceptibles d'exister également sur le réseau ou dans une base de sauvegarde utilisée sur le PC.

03 DÉVELOPPEMENT D'UN PROGRAMME DE PROTECTION DE L'INFORMATION

ADOPTER UNE APPROCHE MULTICOUCHE DE LA SÉCURITÉ.

Adoptez une approche multicouche pour la protection des données en appliquant les pratiques les plus adaptées du réseau de données au réseau de stockage, tout en ajoutant des techniques spécifiques aux caractéristiques des données non utilisées. Ces pratiques incluent les aspects suivants :

- **AUTHENTIFICATION** Appliquez des techniques multi-niveaux d'authentification et d'anti-usurpation.
- **AUTORISATION** Accordez des privilèges basés sur des rôles et des responsabilités plutôt qu'un accès administratif intégral. Lorsque cela est possible, augmentez les responsabilités en fonction des rôles de chacun pour la gestion administrative des applications de stockage - en particulier les sauvegardes.
- **CRYPTAGE** Toutes les données sensibles stockées ou copiées doivent être cryptées. Il en va de même pour toutes les données d'interface de gestion transmises sur un réseau public. Les données sensibles sont généralement définies comme contenant des informations personnelles ou bien des secrets de fabrication.
- **CONTRÔLE** Des registres d'exploitation administrative doivent être conservés par chaque utilisateur afin d'assurer traçabilité et responsabilité.

FAITES UNE COPIE DE VOS BANDES DE SAUVEGARDE.

Disposer d'une seule et unique copie de ses données n'est jamais une bonne idée. Même si la durée de vie des supports sur bande est parfois longue, des dommages physiques et environnementaux sont néanmoins possibles. La meilleure solution est de copier les bandes de sauvegarde et de conserver ses copies sur un site distant. La méthode de copie conseillée consiste à reproduire une nouvelle bande avec les données de la bande originale. Cette méthode présente le double avantage de vérifier que les données de sauvegarde sont lisibles et d'éliminer la moindre erreur sur la bande.

La raison la plus souvent invoquée pour ne pas avoir de politique de duplication de bande est le manque de temps. D'un point de vue pratique, les sauvegardes prennent trop de temps, rendant difficile la duplication des données en temps utile. Il existe plusieurs méthodes permettant de résoudre ce problème. La première commence par l'optimisation du système de sauvegarde afin de réduire le temps requis pour exécuter la sauvegarde originale. Ensuite, plusieurs lecteurs de bandes à grande vitesse peuvent être utilisés pour créer la seconde copie qui sera stockée sur un autre site. Certains paquets de logiciels de sauvegarde permettent de créer une copie lors de la création de l'original.



Bien que cette méthode ne présente pas l'avantage de la vérification mentionné dans le paragraphe précédent, elle permet néanmoins de faire l'économie du temps de reproduction - une copie quelconque est toujours mieux que pas de copie du tout. Quelle que soit la taille de votre société, une combinaison de lecteurs de bandes à grande vitesse, de bandothèques virtuelles et de services professionnels contribue à satisfaire à cette exigence importante.

METTEZ EN PLACE UNE CHAÎNE DE TRAÇABILITÉ STRICTE ASSURANT UN SUIVI COMPLET DE LA GESTION DES SUPPORTS.

La chaîne de traçabilité fait référence à l'acte, à la manière, au traitement, à la supervision et/ou au contrôle des supports ou des informations (généralement, mais pas toujours, sur bande). L'objectif ultime d'une chaîne de traçabilité réussie est la préservation de l'intégrité des ressources. Les aspects suivants sont à prendre en compte.

Les supports amovibles doivent faire l'objet d'un suivi à l'aide de code-barres et des rapports détaillant l'emplacement actuel des supports doivent être générés. Une bonne pratique consiste à établir un rapport quotidien des bandes à envoyer vers un site de stockage distant et de celles qui sont arrivées à expiration et qui doivent être récupérées afin d'être recyclées ou détruites. Des procédures d'exploitation standard certifiées doivent être en place pour s'assurer que ces mesures sont bien appliquées.

L'emplacement du site de conservation et les procédures d'accès au stockage sur le site distant doivent être analysés par rapport aux mesures de sécurité. Les supports doivent être placés dans des conteneurs verrouillés avant de quitter le centre de données et le suivi qui s'ensuit doit être effectué au niveau du conteneur. Ce suivi doit être effectué par numérisation de code-barres chaque fois qu'un conteneur est déplacé, de même dans les centres de données et sur les sites de conservation. Il ne doit être possible d'accéder aux conteneurs que contre signature et ils doivent toujours être rangés pour éviter d'être exposés au vol.

Comparez régulièrement l'inventaire des supports stockés sur le site distant (une fois par mois au moins) avec les bandes conservées en interne.

Il s'agira de comparer la lecture physique des bandes stockées sur le site distant à la sauvegarde informatique afin de détecter d'éventuelles incohérences. S'il manque des supports, des mesures adéquates doivent être prises.

Une fois le support devenu obsolète ou si son intégrité est insuffisante, il doit être correctement détruit. La destruction se fait généralement par la destruction de la cartouche, en brouillant les données qu'elle contient ou en la détruisant purement et simplement pour la rendre inutilisable. La destruction des données peut être effectuée sur site à l'aide d'un équipement de dégaussage approprié, ou via un service tiers. (Si vous effectuez la destruction de données sur site, assurez-vous que l'équipement de dégaussage est adapté au support). La destruction de données doit idéalement être effectuée par une entreprise délivrant un certificat de destruction.

COMPRENEZ LE PROCESSUS DE LA CHAÎNE DE TRAÇABILITÉ DE VOS DONNÉES.

Autre élément essentiel dans le traitement des supports sécurisés : s'assurer que les entreprises extérieures spécialisées dans le stockage de documents sur site distant respectent les meilleures pratiques. Voici quelques aspects de base à prendre en considération :

- VULNÉRABILITÉ SUR SITE

Ne déposez pas de bandes dans un conteneur non verrouillé comme une boîte ouverte devant être ramassée à la réception, par exemple. La collecte doit respecter une procédure opérationnelle standard suivant laquelle un responsable du service informatique remet le colis contre signature à un représentant du fournisseur dûment habilité.

- VÉRIFICATIONS DES ANTÉCÉDENTS JUDICIAIRES

Lorsqu'une société stocke vos données sensibles, vous devez vous assurer qu'elle effectue des vérifications des antécédents judiciaires de chacun de ses employés.

- LA SOCIÉTÉ DOIT DISPOSER D'UNE PROCÉDURE COMPLÈTE DE TRAÇABILITÉ

Consultez l'entreprise de stockage sur site distant pour connaître la procédure complète de prise en charge du support. Vérifiez que l'accent est mis sur la sécurité physique, ainsi que sur les

mécanismes d'audit et de contrôle garantissant le respect de la procédure. Il est déconseillé de faire acheminer des données sensibles dans un véhicule portant en grandes lettres le nom du fournisseur, car cela permet de savoir qu'il transporte des données sensibles.

- **SAUVEGARDE SÉCURISÉE DES CONTENEURS**

La sauvegarde sécurisée des conteneurs concerne le suivi des bacs et des conteneurs, mais pas de leur contenu. La plupart des entreprises de stockage sur site distant prennent en charge ce type de sauvegarde.

- **CONTRÔLES DE SÉCURITÉ PHYSIQUE**

Les installations doivent être correctement sécurisées. Aucune personne non autorisée ne doit pouvoir accéder aux salles des coffres.

- **CONTRÔLE DE L'ENVIRONNEMENT**

Les bandes et autres supports ne doivent jamais être stockés dans le coffre d'un véhicule, ni à aucun autre emplacement non contrôlé sur le plan environnemental. Pour le stockage des bandes, l'environnement doit être strictement contrôlé, et notamment la température, l'humidité et l'électricité statique. La poussière est l'ennemi de la plupart des supports et périphériques d'enregistrement. L'environnement de sauvegarde et d'archivage doit toujours rester propre et sans poussière. Il est conseillé d'utiliser un chiffon doux antistatique pour nettoyer l'extérieur des cartouches et la poussière doit être éliminée des fentes ou des racks de stockage à l'aide d'une bombe d'air comprimé. Les bandes doivent être expédiées dans un support électrostatique plutôt qu'empilées dans un bac ou une boîte en carton. Bien que d'apparence robuste, les bandes peuvent être aisément endommagées si elles ne sont pas manipulées correctement.

ENVISAGEZ L'ELECTRONIC VAULTING

Il faut savoir que la sauvegarde électronique des données à distance permet d'éviter le transport d'informations sur des supports physiques dans un véhicule. Il existe actuellement plusieurs sociétés qui offrent aux professionnels de l'informatique la possibilité de sauvegarder les données via Internet. Les données peuvent être cryptées et déplacées via Internet vers une infrastructure de sauvegarde sécurisée.

L'Electronic Vaulting n'est pas forcément une solution pour toutes les données d'une société, mais peut s'avérer pratique pour des données réparties sur des serveurs de fichiers ou des ordinateurs personnels. Ces données peuvent représenter 60 % des informations d'une entreprise et il est difficile pour le service informatique de les contrôler.

Assurez-vous que le fournisseur offrant ces services crypte les données pendant leur transfert et pendant leur conservation. En outre, demandez au fournisseur comment la disponibilité des informations est assurée. Sont-elles sauvegardées sur bande ? Sont-elles répliquées sur un autre site ? Assurez-vous que les pratiques de récupération après sinistre du fournisseur relèvent d'une norme exceptionnelle. Déterminez avec lui la manière dont la disponibilité des informations est assurée en cas de récupération ou de contentieux.

Lorsqu'une société stocke vos données sensibles, vous devez vous assurer qu'elle effectue des vérifications des antécédents judiciaires de chacun de ses employés.

04 COMMUNICATION DES PROCÉDURES DE PROTECTION ET DE SÉCURITÉ DE L'INFORMATION

Après la mise en place complète des procédures de protection et de traitement des données sensibles, il est important de s'assurer que les personnes responsables de leur sécurité sont formées et informées. Les politiques de sécurité constituent l'aspect le plus important de l'affectation des responsabilités et autorisations.

TENEZ INFORMÉS LES DIRECTEURS COMMERCIAUX DES RISQUES, DES CONTRE-MESURES ET DES COÛTS.

Les pertes de données et les atteintes à la propriété intellectuelle constituent un problème de nature commerciale, et non informatique. C'est pourquoi le responsable de la sécurité informatique (CISO) doit commencer par informer les cadres commerciaux des risques, menaces et pertes potentielles en cas d'atteinte à la sécurité des données, ainsi que du coût des diverses contre-mesures de sécurité. Ainsi, les décideurs auront un avis éclairé sur le rapport coût/avantage des investissements liés à la sécurité des données.

ÉVALUEZ LES RISQUES ET FORMEZ LE PERSONNEL.

Les données du groupe ESG montrent clairement qu'« une mesure de prévention vaut dix mesures de correction ». Les entreprises qui évaluent les risques et forment leur personnel sont plus à même de mettre en œuvre des politiques, des procédures et des technologies de sécurité qui protègent les données importantes. Par ailleurs, une infrastructure vulnérable et un personnel inexpérimenté constituent une véritable bombe à retardement - ce qui justifie tout l'effort à consacrer à la sécurité.

05 EXÉCUTION ET ÉVALUATION DU PLAN DE SÉCURITÉ DE PROTECTION DE L'INFORMATION

La protection des données n'est pas une question de technologie, mais une affaire de procédures. C'est pourquoi il est important de tester les procédures. Au fur et à mesure que la taille d'une société augmente, les besoins en matière de protection des données et des informations évoluent, de sorte que les pratiques de sécurité doivent également changer. Une fois le plan développé, défini et communiqué aux personnes concernées, il faut alors l'exécuter. Assurez-vous que les outils, les technologies et les méthodologies requis sont en place pour servir à la classification des informations.

Testez la procédure une fois qu'elle est en place. N'oubliez pas que le test doit inclure la sauvegarde et la récupération. Tentez d'injecter toute menace possible dans le système, y compris la perte de serveur et de bande, les problèmes de réseau, de périphériques, de classification des données et tout autre scénario susceptible d'affecter l'activité de l'entreprise. Effectuez le test avec du personnel peut-être moins familiarisé avec le système. Ce test permettra de voir si la procédure est facile à suivre et si elle peut être exécutée par un remplaçant au cas où la personne habituellement en charge de cette tâche ne serait pas disponible, pour cause de maladie, de congé ou de licenciement.

Il faut **19 jours**
pour re-saisir 20 Mo
de données perdues.

SOURCE : REALTY TIMES

Toutes les **15 secondes,**
un disque dur tombe
en panne.

SOURCE : HARRIS INTERACTIVE

2 000 ordinateurs
portables sont volés
ou perdus chaque jour.

SOURCE : HARRIS INTERACTIVE

VOS INFORMATIONS MÈNENT LEUR PROPRE VIE, NOUS SOMMES LÀ POUR VOUS AIDER À CHAQUE ÉTAPE

Nous sommes en mesure de vous aider à gérer l'information à toutes les étapes de son cycle de vie, à réduire les coûts et à gagner en efficacité.



**ANALYSE
ET CONSEIL**



**STOCKAGE
ET PROTECTION**



**NUMÉRISATION
ET INDEXATION**



**ACCÈS,
CONSULTATION
ET RÉCUPÉRATION**



**DESTRUCTION
SÉCURISÉE**

UN PARTENAIRE DE CONFIANCE

Quelle que soit la taille ou l'activité de votre entreprise, nous vous proposons des services spécialisés élaborés dans le respect des principes clés suivants :

CONFIANCE

Depuis près de 60 ans, la confiance est au cœur de notre partenariat avec les entreprises, petites ou grandes. Nous sommes implantés dans plus de 1 000 sites à travers le monde.

SÉCURITÉ

Grâce à nos installations sécurisées, nos équipes expérimentées et nos processus optimisés, vos informations sont toujours en sécurité.

EXPERTISE

Nos collaborateurs, nos procédures et nos technologies témoignent de notre solidité et de l'étendue de nos compétences. La compréhension des défis à relever en matière de conformité nous permet de vous aider à exploiter au mieux vos informations tout en réduisant les coûts.

ZOOM CLIENT

Notre engagement à offrir des services d'excellence vous garantit une assistance 24/7.

DÉVELOPPEMENT DURABLE

En vous aidant à réduire le volume d'informations à conserver et à recycler les documents qu'il n'est pas nécessaire de garder, nous vous permettons d'atteindre vos propres objectifs en termes de développement durable.

CONTACTEZ-NOUS AUJOURD'HUI

Pour plus d'informations et de conseils sur ce qu'Iron Mountain peut vous offrir en matière de gestion de l'information, rendez-vous sur le site www.ironmountain.fr ou appelez-nous au 0800 215 218.

