Votre meilleure protection contre la perte de données

Ne démarrez pas votre journée sur un temps d'arrêt.

CARBONITE® an opentext™ company | WEBROOT® an opentext™ company

Réduction de risque

En 2017, un article paru dans The Economist déclarait que les données étaient désormais la ressource la plus précieuse au monde, supplantant le pétrole.[1] « Les smartphones et Internet ont rendu les données abondantes, omniprésentes et bien plus précieuses », indique l'article. L'article citait comme facteur principal à cela une augmentation du volume de données générées et la capacité de l'intelligence artificielle et des algorithmes à en extraire de la valeur. Bien que tout cela soit toujours vrai aujourd'hui, cette image ne dresse pas un tableau complet de la véritable valeur des données.

Les données personnelles, telles qu'un nom, un numéro de sécurité sociale, une date de naissance et des numéros de compte, valent environ 56 EUR sur le dark web.[2] Mais il s'agit là seulement du montant que les cybercriminels paieront pour utiliser les données d'un individu à des fins malveillantes. Il faut également prendre en compte les coûts que cela implique pour les personnes dont les données tombent entre de mauvaises mains. La perte moyenne pour les titulaires de carte bancaire dont les données ont été exposées se situe entre 1 015 et 1 920 EUR.[3] En outre, il convient d'ajouter le coût de la restauration du crédit compromis, qui se situe entre 15 et 124 EUR par mois.[4] L'ensemble de ces facteurs donne une image plus complète de la valeur réelle des données et de la nécessité de les protéger.

ANALYSE DES ACTIVITÉS

Il s'agit du même calcul que celui que les entreprises doivent effectuer pour déterminer la valeur des actifs informatiques, le coût et les conséquences de la perte de données et la nécessité de systèmes conçus pour la prévention des sinistres découlant d'une perte de données. Étant donné que les données commerciales sont beaucoup plus précieuses que les données personnelles, l'ampleur du problème est d'autant plus important.

Le coût d'une perte de données d'entreprise est d'environ 117 EUR par enregistrement de données.[5] Mais, tout comme pour les données personnelles, d'autres facteurs sont à prendre en compte. Il convient de prendre en considération le coût de la perte d'accès aux données et à l'infrastructure informatique critique. Pour les petites et moyennes entreprises (PME), le coût moyen de chaque heure d'arrêt non planifié se situe entre 9 036 et 21 236 EUR.[6] Et comme pour les données personnelles, il ne s'agit pas seulement du coût de la perte de données mais aussi du coût de la réparation des dommages. Selon les professionnels de l'informatique, les pertes de données consomment 81 % des ressources informatiques.[7] Ajoutez à cela les dommages en termes de réputation, la perte d'opportunités commerciales, la perte de confiance et les pénalités légales et de conformité qui peuvent résulter d'un seul événement de perte ou de violation de données. Si ces facteurs de coût sont plus difficiles à quantifier, ils sont sans aucun doute bien réels et substantiels.

PRÉVENTION DE LA PERTE DE DONNÉES

En ce qui concerne la perte de données, la question n'est pas de savoir « si » elle va se produire mais « quand ». Plus de 60 % des entreprises ont déclaré avoir perdu des données au cours d'une année.[8] Pour imaginer le nombre de façons différentes dont les entreprises peuvent perdre des données, pensez aux différents appareils, systèmes et plates-formes qui composent les environnements informatiques complexes d'aujourd'hui. Auparavant, les dispositifs physiques et l'infrastructure étaient au centre des préoccupations. Aujourd'hui, avec la prédominance des plateformes et des services cloud, les responsables informatiques doivent également prendre en compte la disponibilité des services cloud et la récupérabilité des données cloud. La seule façon de protéger les appareils, applications et données qui y sont hébergés est d'anticiper tous les scénarios de perte de données possibles. Les diverses situations à envisager incluent, mais sans s'y limiter :

PANNE MATÉRIELLE

SURTENSION

PANNE DE DISQUE

ERREUR HUMAINE

CORRUPTION DE FICHIER

SUPPRESSION OU REMPLACEMENT ACCIDENTELS

INFECTION PAR VIRUS

VOL D'APPAREILS

EXFILTRATION DE DONNÉES

PANNE DU SERVICE CLOUD

MAUVAISE CONFIGURATION DES AUTORISATIONS

PERTE DE MATÉRIEL (INONDATIONS, INCENDIES, FOUDRE, PANNE DE COURANT)

De nombreuses entreprises ne sont pas préparées à la perte de données : 39 % des entreprises ne disposent pas de plan de réponse aux incidents ni de stratégie de prévention des pertes de données.[8] Ce sont ces entreprises qui appellent les spécialistes de la reprise après sinistre dans l'espoir de récupérer leurs données perdues ou corrompues d'un coup de baguette magique. Si elles ont de la chance, elles peuvent récupérer les fichiers supprimés dans la corbeille. Dans de nombreux cas, la perte de données n'est découverte qu'après l'expiration de la période de conservation dans la corbeille. Dans d'autres cas, par exemple en cas de rançongiciels ou d'actes d'initiés malveillants, les auteurs infectent ou vident la corbeille pour compliquer la tâche.

Lorsque l'on considère le coût et les conséquences de la perte de données, et en tenant compte du risque que certains dégâts puissent être irréparables, il est évident qu'il est impératif de mettre en œuvre un plan de reprise après sinistre avant que ne survienne tout incident de perte de données.

UN PLAN DE RÉCUPÉRATION DE DONNÉES

Lorsqu'une entreprises subit une perte de données, une récupération réussie dépendra des éléments suivants :

- Combien de temps faut-il pour récupérer les données ?
- Combien de temps les utilisateurs doivent-ils attendre avant de pouvoir y accéder à nouveau ?
- Quelle quantité de données est récupérable ?
- Quelle est l'efficacité du processus ?

Les professionnels de l'informatique désignent souvent les objectifs de récupération par les termes RTO (objectif de temps de récupération) et RPO (objectif de point de récupération). L'établissement de RTO et RPO permet d'assurer l'alignement entre le plan de sauvegarde et les objectifs de récupération. Selon une enquête, 61 % des PME souhaitent une reprise complète des applications critiques en quatre heures ou moins.[9] Dans une autre enquête, seulement 24 % des professionnels de l'informatique ont déclaré qu'ils pouvaient assurer une reprise en moins de quatre heures.[7] Ainsi, soit les objectifs de reprise des PME sont irréalistes, soit la plupart des professionnels de l'informatique ne peuvent pas répondre aux exigences strictes des organisations qu'ils servent.

CONSEILS DE PRO

Des temps d'arrêt excessifs sur les systèmes critiques peuvent se révéler catastrophiques pour les entreprises, en particulier pour les petites et moyennes entreprises qui tolèrent moins les perturbations et les pertes de revenus. Une récupération de données réussie peut être essentielle à la survie de l'entreprise et implique de disposer des bons outils. Il existe des outils conçus pour une récupération à petite échelle, tout comme il existe des outils conçus pour une récupération à grande échelle. L'atteinte des objectifs de reprise après sinistre est rarement due à la chance. Quatre facteurs clés détermineront votre capacité à mettre en œuvre une stratégie réussie :

1. Identifiez les données, applications et systèmes critiques pour l'entreprise et hiérarchisez-les en fonction de leur caractère essentiel pour cette dernière.
2. Explorez les options technologiques dont les capacités correspondent aux exigences de l'entreprise.
3. Configurez les cibles et les emplacements de sauvegarde pour vous adapter à une gamme complète de scénarios de sinistre.
4. Développez les compétences et le savoir-faire pour mener à bien la récupération après sinistre.

Hiérarchisation des données

Les différents types de données, d'applications et de systèmes ont des objectifs de récupération différents. Plus les données sont essentielles, plus la récupération est critique pour que l'entreprise continue de fonctionner sans interruption. Connaître l'impact des temps d'arrêt pour des données, des applications et des systèmes spécifiques vous aide à déployer la bonne solution de récupération en fonction de l'importance de ces données et systèmes pour l'entreprise.

Configurations de sauvegarde et de restauration

Il peut être plus rapide de récupérer des données à partir d'une source locale que d'une source distante. Mais en cas de panne locale, une sauvegarde hors site peut sauver la mise. Le déploiement idéal comprend des sauvegardes redondantes, où les copies sont stockées à la fois sur site et hors site, comme dans le cloud, pour garantir qu'un point de récupération est disponible pour tout scénario de sinistre.

Correspondance technologique

Une fois le caractère critique des données identifié, la protection appropriée peut être déployée. Différentes technologies peuvent vous aider à atteindre différents objectifs. Les instantanés permettent une récupération à partir d'un moment donné, tandis que la réplication en temps réel crée un système secondaire qui peut prendre le relais à tout moment. En fonction des besoins, il est possible d'aligner le niveau de données avec la technologie appropriée.

Compétences et savoir-faire

Investir dans la reprise après sinistre en tant que compétence peut sembler exagéré. Mais en cas de catastrophe, les entreprises doivent être prêtes à mettre en œuvre un plan de reprise après sinistre. Il est essentiel pour les PME d'accéder à des outils via des tableaux de bord faciles à utiliser et une gestion centralisée. Les entreprises peuvent également sous-traiter leur plan de reprise après sinistre à un fournisseur de services.

OUTILS SPÉCIALISÉS

Personne ne sait quand une perte de données se produira ni comment, mais il y a toujours un risque et personne n'a envie d'être confronté à une telle situation. Compte tenu du fait qu'il n'y a aucun moyen de savoir quelle forme prendra la perte de données, il est nécessaire de disposer d'un outil pour quasiment chaque éventualité. Voici un exemple de cas d'utilisation de reprise après sinistre et les solutions technologiques qui y répondent.

Cas d'utilisation	Solution technologique
Perte simple de fichiers et de dossiers	Récupération granulaire
Panne de courant imprévue	Sauvegarde cohérente en cas de panne Sauvegarde cohérente avec les applications
Panne matérielle catastrophique	Restauration sans système d'exploitation
Panne du système de niveau 1	Basculement local instantané
Restauration de machine virtuelle	Restauration rapide de machine virtuelle (MV)
Restauration de la version précédente d'une base de données	Récupération à un point dans le temps
Données des bureaux distants/succursales	Topologie satellite/coffre-fort central
Suppression/remplacement accidentels	Récupération de fichiers/dossiers locaux
Panne du site local	Dispositif de récupération virtuelle Récupération hors site/cloud
Windows Server corrompu	Restauration de l'état du système

AU-DELÀ DES MEILLEURES PRATIQUES

Lorsque les meilleures pratiques sont continuellement validées dans le monde réel, elles deviennent des pratiques fondées sur des preuves, connues pour fournir des résultats optimaux lorsqu'elles sont appliquées de manière cohérente. Les pratiques de reprise après sinistre ont été suffisamment testées dans le monde réel pour que l'on connaisse avec certitude les pratiques et procédures les plus fiables pour atteindre les résultats souhaités. Les pratiques fondées sur des données probantes pour atteindre les objectifs de rétablissement prédéterminés comprennent :

Déploiement flexible – Toutes les données et tous les systèmes n'ont pas besoin du même niveau de protection. Les données critiques (niveau 1) nécessitent des niveaux de service plus stricts que les données historiques ou d'archives. Différents serveurs et applications peuvent nécessiter différents types de sauvegarde. Certaines applications peuvent nécessiter une sauvegarde sans système d'exploitation tandis que d'autres ne nécessitent qu'une sauvegarde de fichiers et de dossiers. La forme de sauvegarde déterminera la méthode utilisée pour récupérer les données, la rapidité avec laquelle les données peuvent être récupérées, le potentiel de perte de données et l'intensité de l'effort de récupération.

Options de configuration – Différents types de données sont également sauvegardés sur différentes cibles. Pour une récupération rapide des données critiques, la sauvegarde sur une cible locale permet de garantir le temps de récupération le plus rapide possible. Pour les organisations possédant plusieurs succursales, chaque emplacement peut nécessiter un environnement de sauvegarde local. Chacun de ces emplacements peut ensuite être répliqué dans un référentiel central. La sauvegarde virtuelle et la sauvegarde cloud sont également nécessaires pour protéger les serveurs dans leurs environnements natifs. Physique vers virtuel, virtuel vers physique et cloud vers cloud sont toutes des topologies également réalisables. Il est essentiel de disposer de différentes options de configuration pour protéger les données en fonction des objectifs de restauration de chacun de ces systèmes.

Gestion centrale – Les talents de reprise après sinistre représentent une ressource limitée. Peu d'entreprises peuvent consacrer un rôle à la protection des systèmes et à la limitation des sinistres. Le plus souvent, c'est au personnel informatique (qui gère souvent différentes tâches) qu'il incombe d'assurer la résilience des systèmes. La capacité de gérer les sauvegardes et d'effectuer la restauration à partir d'une console centrale simplifie les pratiques et les procédures de protection des données. Cela permet de garantir que les ressources informatiques critiques peuvent se concentrer sur d'autres priorités stratégiques.

PLATEFORME DE PROTECTION DES DONNÉES CARBONITE

Carbonite est l'un des principaux fournisseurs de protection complète des données pour les différents types de données et de systèmes dans les environnements informatiques actuels. La plateforme complète de protection des données de Carbonite comprend des solutions avancées pour assurer l'intégrité, la survie et l'accessibilité des données pour toutes les entreprises, quels que soient leur taille ou leur secteur.

Avec une pile complète de solutions de Carbonite, les entreprises peuvent mettre en œuvre une approche de protection des données axée sur la récupération en premier lieu, en déterminant d'abord l'urgence des données ou du système, puis en déployant la forme de protection qui fournira les objectifs de récupération pour ce système.

Carbonite contribue à garantir des niveaux de disponibilité plus élevés en protégeant les données des entreprises contre des événements indésirables, tels que les ransomwares, la perte de données et les pannes majeures. Carbonite soutient également la conformité pour les entreprises des industries réglementées.

CYBER- RÉSILIENCE

La cyber-résilience signifie pouvoir rester opérationnel, même face aux cyberattaques et à la perte de données. C'est pourquoi Carbonite et Webroot ont uni leurs forces pour fournir des solutions de protection des postes et des réseaux, de sensibilisation à la sécurité et de sauvegarde des données et de reprise après sinistre, ainsi que des services de renseignement sur les menaces utilisés par les principaux fournisseurs de technologies du marché dans le monde entier. Webroot et Carbonite exploitent la puissance de l'apprentissage automatique pour protéger des millions d'entreprises et de particuliers, et sécuriser le monde connecté. Les sociétés Carbonite, Webroot et OpenText exploitent le Cloud et l'intelligence artificielle pour fournir des solutions complètes de cyber-résilience aux entreprises, aux particuliers et aux fournisseurs de services gérés.

[1] The Economist, The world's most valuable resource is no longer oil, but data
[2] Bleepingcomputer, What Your Personal Information is Worth to Cybercriminals
[3] Wikipedia, Identity theft in the United States
[4] Investopedia, How Much Does It Cost to Repair My Credit?
[5] Ponemon Institute, 2018 Cost of a Data Breach Study
[6] IDC, The Growth Opportunity for SMB Cloud and Hybrid Business Continuity
[7] Spiceworks: Carbonite Backup & Disaster Recovery Survey
[8] Ponemon Institute, 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses
[9] Price Waterhouse Coopers: The Global State of Information Security Survey

CARBONITE® an opentext™ company | WEBROOT® an opentext™ company

Contactez-nous pour en savoir plus
Téléphone : +33 (0)1 47 96 55 41
E-mail : France-smbc@opentext.com

À propos de Webroot et de Carbonite

Les sociétés Carbonite, Webroot et OpenText exploitent le Cloud et l'intelligence artificielle pour fournir des solutions complètes de cyber-résilience aux entreprises, aux particuliers et aux fournisseurs de services gérés. La cyber-résilience signifie pouvoir rester opérationnel, même face aux cyberattaques et à la perte de données. C'est pourquoi nous avons uni nos forces pour fournir des solutions de protection des postes et des réseaux, de sensibilisation à la sécurité et de sauvegarde des données et de reprise après sinistre, ainsi que des services de renseignement sur les menaces utilisés par les principaux fournisseurs de technologies du marché dans le monde entier. Nous exploitons la puissance de l'apprentissage automatique pour protéger des millions d'entreprises et de particuliers, et sécuriser le monde connecté. Webroot et Carbonite sont implantés en Amérique du Nord, en Europe, en Australie et en Asie. Découvrez la cyber résilience sur carbonite.com et webroot.com.