

Comment bien protéger



ACCESS

vos données ?

Par **Marjorie Dos Santos** Photos DR

LES DONNÉES SONT VITALES POUR L'ENTREPRISE. POUR LES PROTÉGER CONTRE TOUTES LES MENACES EXTERNES ET INTERNES, IL EXISTE DES SOLUTIONS SIMPLES ET EFFICACES. AFIN D'ÉVITER LEUR PERTE OU LEUR DIVULGATION, DE NOMBREUX ÉDITEURS PROPOSENT DES SOLUTIONS INTÉGRANT LES TROIS CRITÈRES DE SÉCURITÉ : LA DISPONIBILITÉ (PAR LA SAUVEGARDE), L'INTÉGRITÉ (PAR LE CHIFFREMENT) ET LA CONFIDENTIALITÉ VIA LES CONTRÔLES D'ACCÈS.

SAUVEGARDER

La sauvegarde, ou le backup en anglais, est une opération qui consiste à dupliquer et sécuriser les données contenues dans le système d'information. Autrement dit, faire une copie de sécurité permet de se prémunir contre la destruction du centre de stockage, les malveillances, les erreurs de manipulation, les défaillances physiques, les conflits logiciels, les attaques virales, etc. Différentielle ou incrémentielle (voir encadré), elle correspond à la première strate de sécurité : la disponibilité des données. En effet, à n'importe quel moment,

vous devez être en mesure de récupérer les données sauvegardées pour pouvoir les restaurer. « Il faut garder en tête que la sauvegarde est un moyen, la restauration est LA finalité », insiste Cyril Voisin, chef de programme sécurité chez Microsoft. Toutefois, une sauvegarde mal faite (par exemple, en écrasant les restaurations précédentes) ne permet pas une restauration efficace et complète.

SAUVEGARDE LOCALE OU EXTERNALISÉE ?

Les deux ! Jadis, les sauvegardes se faisaient sur bande, sur disquette ou sur cartouche. Aujourd'hui, une PME peut sauvegarder ses informations sur CD, sur disque dur externe ou encore sur clé USB. Néanmoins un problème subsiste. Tout comme les anciennes méthodes, ces nouveaux supports ont des failles : certes, ils sont moins coûteux mais ils peuvent être altérés lors de déplacements ou, pis encore, brûlés lors d'un incendie. « Une bonne sauvegarde, c'est une sauvegarde faite tous les mois sur un mois, tous les jours sur une semaine, etc. Et surtout, la bonne stratégie est de faire une sauvegarde locale et une sauvegarde externalisée », explique Cyril Voisin. Le principe est simple : les données sont transférées via Internet vers des serveurs extérieurs à la société pour une sécurité maximale. >

SAUVEGARDE INCRÉMENTIELLE ET DIFFÉRENTIELLE

Outre la sauvegarde totale (full backup) qui réalise une copie conforme de toutes les données, il existe deux types de sauvegardes. La première, appelée incrémentielle, permet de copier tous les éléments modifiés depuis la sauvegarde précédente, offrant ainsi la possibilité de se concentrer uniquement sur les fichiers modifiés et réduisant le volume de stockage. Toutefois, la sauvegarde incrémentielle implique de posséder toutes les sauvegardes précédentes pour un backup complet. Par exemple : vous réalisez une sauvegarde complète le lundi. La sauvegarde incrémentielle faite le mardi sera réalisée par rapport au lundi, le mercredi par rapport au mardi, etc. La sauvegarde différentielle, quant à elle, effectue une copie de fichiers créés ou modifiés depuis la dernière sauvegarde complète, quelles que soient les sauvegardes intermédiaires : si vous effectuez une sauvegarde complète le lundi et que vous faites une sauvegarde différentielle le samedi, la référence sera la sauvegarde du lundi, autrement dit le backup se fera du lundi au samedi.

➤ DES SOLUTIONS EXISTENT

Faire ou faire faire, telle est la question. Souvent, une PME n'a ni le temps ni les moyens de s'occuper de sa restauration. Il existe alors de nombreuses solutions et de multiples prestataires qui vous aident dans cette opération. « *Outre la régularité, une bonne sauvegarde sait se faire oublier, tout en cryptant vos données* », souligne Olivier Mauras, fondateur de Beemo Technologie. À vous alors de choisir les solutions qui correspondent le plus à vos besoins : la plus simple d'utilisation, la plus économique, etc. Parmi elles, on retrouve l'outil Carbonite accessible pour 49 euros par poste et par an avec un stockage illimité et un service client (voir encadré fonctionnement). Mais également les produits Neobe Backup (pour 25 euros HT par mois pour 8 Go) ou NetApp. Symantec, quant à lui, propose deux outils : Backup Exec et Backup Exec System Recovery qui aident la PME à redevenir opérationnelle après un crash, et ce, afin de maintenir la continuité des activités et de réduire l'impact des interruptions non planifiées. Autre prestataire : Athena Global Services qui a développé ShadowProtect (décliné en trois offres : Desktop Edition, Server ou IT), une solution de sauvegarde qui crée des

copies exactes des systèmes, des applications installées, des fichiers et des paramètres utilisateurs. Ces images peuvent par la suite être restaurées depuis n'importe quel ordinateur. Enfin, F-Secure a lancé un service de backup en ligne qui met à disposition des utilisateurs l'automatisation de la sauvegarde et une capacité d'archivage illimitée. Le fonctionnement de ces solutions est généralement le même, à savoir, l'installation d'un logiciel ou d'une application sur votre ordinateur. L'outil scanne automatiquement les fichiers pour que ceux-ci soient sauvegardés. Parallèlement à cette opération, les données sont cryptées puis envoyées via Internet sur des serveurs externes, pouvant être récupérées en cas de restauration.

BEEMO TECHNOLOGIE

Fondée en 2002 par deux experts en sécurisation, Oliver Mauras et Gabriel Biberian, Beemo Technologie est une société spécialisée dans la sauvegarde des données sécurisées. S'adressant à ses débuts aux TPE/PME, Beemo Technologie a développé sa solution de sauvegarde Data Safe Restore. Il s'agit d'une offre cumulant une BeeBox (serveur local) et des serveurs externalisés. Installée chez le client, la BeeBox reçoit l'ensemble des données de l'entreprise. Ces dernières sont passées à l'antivirus (en partenariat avec Sophos) avant d'être cryptées, compressées et stockées non seulement sur la BeeBox, pour un redémarrage immédiat de l'activité, mais également, via Internet, sur deux serveurs (l'un à Lyon, l'autre à Marseille). Cette double protection écarte ainsi tous risques de pertes définitives des données en cas d'incendie ou de crash des serveurs de Beemo Technologie. Et tout cela automatiquement, sans aucune intervention humaine. La sauvegarde, faite sur disque pour des raisons de pérennité, peut être planifiée selon votre volonté et vos besoins. En termes de coût, le premier forfait démarre à 59 euros HT par mois pour 5 Go compressées, puis 119 euros HT par mois pour 20 Go compressés et 239 euros HT par mois au-delà.

CARBONITE : COMMENT ÇA FONCTIONNE ?

- ◆ **Première étape** : l'installation d'un programme sur votre PC qui recherche en permanence en arrière plan les fichiers à sauvegarder (nouveaux ou modifiés).
- ◆ **Deuxième étape** : la sauvegarde des documents se fait uniquement lorsque votre ordinateur est inutilisé. À l'inverse, lorsque vous travaillez, Carbonite se met en sommeil, évitant ainsi tout ralentissement.
- ◆ **Troisième étape** : quels fichiers ont été sauvegardés ? La présence de point sur vos fichiers indique ce qui a été ou non sauvegardé. Ainsi, l'absence de point signifie que le fichier n'a pas été sauvegardé ; le point jaune/orange indique qu'il est en attente alors que le point vert précise que la sauvegarde a été faite. Un point en « anneau vert » (un point vert percé d'un trou en son milieu) signifie que le dossier est sauvegardé, mais que certains de ses fichiers ou sous-dossiers ne sont pas sélectionnés pour la sauvegarde. Toutefois, tous les autres fichiers du dossier sont sauvegardés.
- ◆ **Quatrième étape** : la récupération des données, quant à elle, se fait en un simple clic et vous permet de restaurer l'ensemble des données perdues rapidement.
- ◆ **Cinquième étape** : en termes de confidentialité, chaque donnée est chiffrée deux fois avant de quitter le PC. Ces informations restent cryptées sur les serveurs sécurisés de Carbonite.

CRYPTER POUR MIEUX SE PROTÉGER

Qu'il s'agisse de Beemo Technologie, Athena Global Services, SkyRecon ou encore Symantec, tous proposent le chiffrement des données. En effet, vous devez assurer à vos partenaires

➤ l'intégrité des données : elles ne doivent en aucun cas, lors de leur sauvegarde, de leur traitement, de leur transmission ou leur stockage, être altérées ou détruites volontairement ou accidentellement. L'implémentation d'un logiciel de chiffrement prend alors toute sa dimension : empêcher la lecture et l'utilisation des informations sensibles par une personne non autorisée. « *S'il y a cryptage des données sensibles, il y a moins de risque de piratage* », confie Thierry Cosavella, directeur d'Athena Global Services. « *Il est fortement conseillé de chiffrer les données sensibles car celles-ci ne peuvent être lues qu'avec la bonne clef. Résultat, même en cas de vol ou de perte, les informations sont préservées* », ajoute Fernando Rynne, directeur général Encryption Group chez Trend Micro. Le principe du cryptage repose essentiellement sur des clés de chiffrement. Ces dernières pouvant être symétriques (la même clé sert à chiffrer et à déchiffrer) ou asymétriques (deux clés, l'une pour chiffrer, l'autre gardée secrète pour le déchiffrement).

Présentées sous plusieurs formes (mots ou phrases, chiffres, code binaire), il est préconisé d'utiliser des clés de 128 ou 256 bits. Plus elles sont longues, plus il sera difficile de les « cracker ».

USAGE EXTERNE

Dans un monde où la mobilité n'a de cesse de se développer, où les commerciaux doivent pouvoir communiquer avec leur société, Internet et la connexion à distance sont devenus des outils incontournables pour une PME soucieuse de prospérer. Le risque de divulgation ou d'altération dû à la perte ou au vol d'un ordinateur, d'une clé USB, d'une malveillance ou encore d'un espionnage industriel s'amplifie également. Pour preuve, selon une étude IDC portant sur le vol d'ordinateurs portables, une entreprise se fait voler en moyenne quatre ordinateurs par an. Il faut donc protéger les ordinateurs portables et les données qui y sont intégrées. Pour cela, il existe une multitude de solutions : TrueCrypt, un logiciel de chiffrement libre d'accès et gratuit pour les PME ayant peu de moyens, BitLocker de Microsoft (Windows Vista) et StormShield de SkyRecon. Cette solution offre deux niveaux

de sécurisation des données. Le premier, dit global, réalise le chiffrement du disque avec authentification. Les utilisateurs doivent obligatoirement entrer un mot de passe avant chaque chiffrement. Les fichiers, quant à eux, sont cryptés à la volée, permettant ainsi de différencier chacun d'entre eux (voir paragraphe « contrôle d'accès » ci-dessous).

USAGE INTERNE

Nécessaire pour toute opération externe, le chiffrement peut également l'être au sein de votre société. Fuite de données, divulgation d'informations confidentielles, espionnage industriel, les risques sont nombreux. Notamment pour la messagerie électronique qui est le premier média utilisé par les entreprises pour communiquer. En effet, selon des sources Trend Micro « *près de 80 % de la propriété intellectuelle des entreprises sont contenus dans leur messagerie* ». Et là est le problème, les mails envoyés sont transmis via Inter-

net, ces derniers pouvant être facilement interceptés et lus par des pirates peu scrupuleux et intéressés par leur contenu. Pour cela, Trend Micro a développé Email Encryption, une solution de chiffrement automatique pour la messagerie et les données sensibles. Cette offre qui inclut l'enscription et la gestion des clés par Trend Micro coûte 45 €. Athena Global Services propose également un outil qui chiffre les communications par email : CenturionMail 3.0. Utiliser une solution de chiffrement vous permet non seulement de transmettre vos informations sensibles en toute sécurité et de les rendre parfaitement intègres aux yeux de la loi et de vos partenaires. Toutefois, si les menaces externes sont bien présentes, ne négligez pas les menaces internes : la malveillance, la fuite de données accidentelle, etc.

LE CONTRÔLE D'ACCÈS

Dernier critère de sécurité en matière de protection des données, le contrôle d'accès aux ressources physiques (bâtiment, local à serveurs, etc.) et logiques (ordinateur, système d'exploitation, etc.) protège les informations de toute

“S'il y a cryptage des données sensibles, il y a moins de risque de piratage”

➤ maladresse ou indiscretion, assurant la confidentialité. Le principe est simple : le contrôle d'accès consiste à vérifier si une personne (employé, prestataire externe, etc.) est habilitée à accéder à certaines informations de la société. Chaque utilisateur doit disposer d'un droit et d'un niveau d'accès unique à son environnement de travail, lequel comprend les logiciels de données, les outils de communication (messagerie, etc.). La plupart du temps, ce contrôle peut être réalisé à l'aide d'une authentification forte, prenant la forme soit d'un mot de passe et d'un login, soit d'une clé, d'une carte à puce ou encore de la biométrie (voir encadré Easydentic).

DES NIVEAUX D'ACCÈS

Selon les documents proposés par le Clusif (www.clusif.asso.fr), il existe trois niveaux pour la gestion des identités et des accès : le DAC (Discretionary Access Control) qui se traduit par « rien n'est autorisé sauf ce qui est permis par le propriétaire », le MAC (Mandatory Access Control) qui autorise l'accès à une ressource s'il y a un niveau d'habilitation, et enfin le RBAC (Role Based Access Control) pour lequel chaque décision d'accès est basée sur le rôle auquel l'utilisateur est attaché. Mais pour Luc Tentillier, directeur associé de Kernel Networks, « un bon contrôle d'accès ne doit pas uniquement se limiter à la gestion des accès mais doit prendre en compte également la gestion des identités ». Cette dernière, sans tomber dans l'extrême surveillance, permet de

tracer chaque utilisateur, chaque fichier entrant ou sortant. Pour répondre aux enjeux de la sécurité informatique, Kernel Networks développe et intègre au sein des PME et grands comptes des

solutions de gestion d'identités grâce à l'utilisation d'une carte à puce pouvant être bloquée en cas d'intrusion suspecte. De son côté, Athena Global Services propose Savemova, une gamme complète d'authentification forte composée de quatre éléments : Savernova PWcard (une carte à

puce gérant et sécurisant les mots de passe), Savernova internet ID pour la sécurisation des connexions externes à votre réseau d'entreprise ou de votre eBusiness, Savemova network ID pour l'administration de mots de passe sûrs dans votre réseau, sans changement d'infrastructure et, enfin, Savernova SSO pour l'accès rapide à toutes vos pages web protégées en oubliant login et mot de passe. Toutefois, sachez que si vous êtes une PME avec peu de moyens, sécuriser ses postes avec un mot de passe et un login constitue une première protection de vos données.

N'HÉSITEZ PLUS

La plupart des PME ont pris conscience de l'importance de la sécurité informatique et ont installé un antivirus, un firewall, un antispam, etc. Mais cela ne suffit pas. Une entreprise sur deux fait faillite suite à un crash dans lequel elle a perdu l'ensemble de ses données. Les protéger devient inévitable. Alors, n'hésitez plus, sécurisez vos données ! ■

“Près de 80 % de la propriété intellectuelle des entreprises sont contenus dans leur messagerie”

EASYDENTIC, SPÉCIALISTE DE LA BIOMÉTRIE

Créée en 2004, Easydentic s'adresse aux TPE/PME et leur propose des solutions biométriques pour la sécurisation des accès et des locaux, à travers sa filiale Eden. Ainsi, en collaboration avec Hitachi, la société a développé un nouveau lecteur biométrique appelé « Biovein ». Ce dernier, basé sur le système d'identification du réseau veineux, n'est autre qu'un capteur optique qui « photographie » les veines des doigts. Il suffit juste pour l'utilisateur de placer son doigt dans l'emplacement prévu à cet effet et de laisser l'analyse se faire pour accorder ou non le droit d'accès à l'entreprise. L'avantage ? Situé sous la peau, le « réseau veineux » ne laisse aucune trace, contrairement à l'empreinte digitale. L'abonnement associé au package revient à 150 euros par accès et par mois et intègre les serveurs, les logiciels, le lecteur et la maintenance. La biométrie peut donc être une alternative aux badges d'accès ou une complémentarité. À vous de faire votre choix !