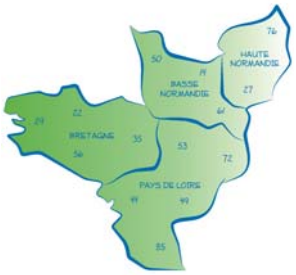


Mercredi 16 novembre 2011

Coopération concours Grand Ouest
Centre organisateur : Service Interrégional des Concours
adossé au CDG 35

Sujet national pour l'ensemble des Centres de Gestion organisateurs du concours

CONCOURS EXTERNE D'ATTACHE TERRITORIAL

- SESSION 2011 -

Spécialité Analyste

RÉDACTION D'UNE NOTE AYANT POUR OBJET DE VÉRIFIER L'APTITUDE À L'ANALYSE D'UN DOSSIER PORTANT SUR LA CONCEPTION ET LA MISE EN PLACE D'UNE APPLICATION AUTOMATISÉE DANS UNE COLLECTIVITÉ TERRITORIALE

Durée : 4 h 00
Coefficient : 4

Ce document comprend un sujet de 2 pages et un dossier de 35 pages.
S'il est incomplet, en avertir un surveillant.

RAPPEL
⇨ **Vous ne devez faire apparaître aucun signe distinctif dans votre copie,** ni votre nom ou un nom fictif, ni signature ou paraphe.
⇨ Aucune référence (nom de collectivité, nom de personne, …) autre que celle figurant le cas échéant sur le sujet ou dans le dossier ne doit apparaître dans votre copie.
⇨ Seul l'usage d'un stylo soit noir, soit bleu, est autorisé (bille, plume ou feutre). L'utilisation d'une autre couleur, pour écrire ou souligner, sera considérée comme un signe distinctif, de même que l'utilisation d'un surligneur.
Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
Les feuilles de brouillon ne seront en aucun cas prises en compte.

<u>Sujet</u> :

Le 8 novembre dernier, une attaque virale a menacé le système informatique de la commune de X. Le virus, nommé Conficker, s'est introduit sur le réseau à la suite d'un manque de vigilance d'un agent, contaminant 4 serveurs sur 10 et une trentaine de postes de travail sur 150. Cette intrusion a engendré une interruption de services de 2 jours, le temps d'effectuer la maintenance corrective nécessaire sur l'ensemble du parc.

Vous êtes attaché territorial analyste au service informatique de la ville de X. sur le poste de responsable sécurité et systèmes.

Le Directeur général des services de la collectivité vous sollicite sur la problématique de la sécurité des données et des accès au système d'information de la collectivité.

Dans ce cadre, vous rédigerez une note à son attention à l'aide des seuls éléments du dossier.

SOMMAIRE DU DOSSIER

Dossier de 35 pages

Certains documents peuvent comporter des renvois à des notes ou à des documents volontairement non fournis car non indispensables à la compréhension du sujet.

DOCUMENT 1

CNIL, "10 conseils pour la sécurité de votre système d'information" – octobre 2009

La loi "informatique et libertés" impose que les organismes mettant en œuvre des fichiers garantissent la sécurité des données qui y sont traitées. Cette exigence se traduit par un ensemble de mesures que les détenteurs de fichiers doivent mettre en œuvre, essentiellement par l'intermédiaire de leur direction des systèmes d'information (DSI) ou de leur responsable informatique.

1. Adopter une politique de mot de passe rigoureuse

L'accès à un poste de travail informatique ou à un fichier par identifiant et mot de passe est la première des protections. Le mot de passe doit être individuel, difficile à deviner et rester secret. Il ne doit donc être écrit sur aucun support. La DSI ou le responsable informatique devra mettre en place une politique de gestion des mots de passe rigoureuse : un mot de passe doit comporter au minimum 8 caractères incluant chiffres, lettres et caractères spéciaux et doit être renouvelé fréquemment (par exemple tous les 3 mois). Le système doit contraindre l'utilisateur à choisir un mot de passe différent des trois qu'il a utilisés précédemment. Généralement attribué par l'administrateur du système, le mot de passe doit être modifié obligatoirement par l'utilisateur dès la première connexion. Enfin, les administrateurs des systèmes et du réseau doivent veiller à modifier les mots de passe qu'ils utilisent eux-mêmes.

2. Concevoir une procédure de création et de suppression des comptes utilisateurs

L'accès aux postes de travail et aux applications doit s'effectuer à l'aide de comptes utilisateurs nominatifs, et non « génériques » (compta1, compta2…), afin de pouvoir éventuellement être capables de tracer les actions faites sur un fichier et, ainsi, de responsabiliser l'ensemble des intervenants. En effet, les comptes « génériques » ne permettent pas d'identifier précisément une personne. Cette règle doit également s'appliquer aux comptes des administrateurs systèmes et réseaux et des autres agents chargés de l'exploitation du système d'information.

3. Sécuriser les postes de travail

Les postes des agents doivent être paramétrés afin qu'ils se verrouillent automatiquement au-delà d'une période d'inactivité (10 minutes maximum) ; les utilisateurs doivent également être incités à verrouiller systématiquement leur poste dès qu'ils s'absentent de leur bureau. Ces dispositions sont de nature à restreindre les risques d'une utilisation frauduleuse d'une application en cas d'absence momentanée de l'agent du poste concerné. Par ailleurs, le contrôle de l'usage des ports USB sur les postes « sensibles », interdisant par exemple la copie de l'ensemble des données contenues dans un fichier, est fortement recommandé.

4. Identifier précisément qui peut avoir accès aux fichiers

L'accès aux données personnelles traitées dans un fichier doit être limité aux seules personnes qui peuvent légitimement y avoir accès pour l'exécution des missions qui leur sont confiées. De cette analyse, dépend « le profil d'habilitation » de l'agent ou du salarié concerné. Pour chaque mouvement ou nouvelle affectation d'un salarié à un poste, le supérieur hiérarchique concerné doit identifier le ou les fichiers auxquels celui-ci a besoin d'accéder et faire procéder à la mise à jour de ses droits d'accès. Une vérification périodique des profils des applications et des droits d'accès aux répertoires sur les serveurs est donc nécessaire afin de s'assurer de l'adéquation des droits offerts et de la réalité des fonctions occupées par chacun.

5. Veiller à la confidentialité des données vis-à-vis des prestataires

Les interventions des divers sous-traitants du système d'information d'un responsable de traitement doivent présenter les garanties suffisantes en terme de sécurité et de confidentialité à l'égard des données auxquels ceux-ci peuvent, le cas échéant, avoir accès. La loi impose ainsi qu'une clause de confidentialité soit prévue dans les contrats de sous-traitance. Les éventuelles interventions d'un prestataire sur des bases de données doivent se dérouler en présence d'un salarié du service informatique et être consignées dans un registre. Les données qui peuvent être

considérées « sensibles » au regard de la loi, par exemple des données de santé ou des données relatives à des moyens de paiement, doivent au surplus faire l'objet d'un chiffrement.

« A noter » : l'administrateur systèmes et réseau n'est pas forcément habilité à accéder à l'ensemble des données de l'organisme. Pourtant, il a besoin d'accéder aux plates-formes ou aux bases de données pour les administrer et les maintenir. En chiffrant les données avec une clé dont il n'a pas connaissance, et qui est détenue par une personne qui n'a pas accès à ces données (le responsable de la sécurité par exemple), l'administrateur peut mener à bien ses missions et la confidentialité est respectée.

6. Sécuriser le réseau local

Un système d'information doit être sécurisé vis-à-vis des attaques extérieures.

Un premier niveau de protection doit être assuré par des dispositifs de sécurité logique spécifiques tels que des routeurs filtrants (ACL), pare-feu, sonde anti intrusions, etc. Une protection fiable contre les virus et logiciels espions suppose une veille constante pour mettre à jour ces outils, tant sur le serveur que sur les postes des agents. La messagerie électronique doit évidemment faire l'objet d'une vigilance particulière. Les connexions entre les sites parfois distants d'une entreprise ou d'une collectivité locale doivent s'effectuer de manière sécurisée, par l'intermédiaire des liaisons privées ou des canaux sécurisés par technique de « tunneling » ou VPN (réseau privé virtuel). Il est également indispensable de sécuriser les réseaux sans fil compte tenu de la possibilité d'intercepter à distance les informations qui y circulent : utilisation de clés de chiffrement, contrôle des adresses physiques des postes clients autorisés, etc. Enfin, les accès distants au système d'information par les postes nomades doivent faire préalablement l'objet d'une authentification de l'utilisateur et du poste. Les accès par internet aux outils d'administration électronique nécessitent également des mesures de sécurité fortes, notamment par l'utilisation de protocoles IPsec, SSL/TLS ou encore HTTPS.

« A noter » : Un référentiel général de sécurité, relatif aux échanges électroniques entre les usagers et les autorités administratives (ordonnance 2005-1516), doit voir le jour prochainement (voir projet sur le site www.ssi.gouv.fr). Il imposera à chacun des acteurs des mesures de sécurité spécifiques.

7. Sécuriser l'accès physique aux locaux

L'accès aux locaux sensibles, tels que les salles hébergeant les serveurs informatiques et les éléments du réseau, doit être limité aux personnels habilités. Ces locaux doivent faire l'objet d'une sécurisation particulière : vérification des habilitations, gardiennage, portes fermées à clé, digicode, contrôle d'accès par badge nominatifs, etc. La DSI ou le responsable informatique doit veiller à ce que les documentations techniques, plans d'adressages réseau, contrats, etc. soient eux aussi protégés.

8. Anticiper le risque de perte ou de divulgation des données

La perte ou la divulgation de données peut avoir plusieurs origines : erreur ou malveillance d'un salarié ou d'un agent, vol d'un ordinateur portable, panne matérielle, ou encore conséquence d'un dégât des eaux ou d'un incendie. Il faut veiller à stocker les données sur des espaces serveurs prévus à cet effet et faisant l'objet de sauvegardes régulières. Les supports de sauvegarde doivent être stockés dans un local distinct de celui qui héberge les serveurs, idéalement dans un coffre ignifugé. Les serveurs hébergeant des données sensibles ou capitales pour l'activité l'organisme concerné doivent être sauvegardés et pourront être dotés d'un dispositif de tolérance de panne. Il est recommandé d'écrire une procédure « urgence – secours » qui décrira comment remonter rapidement ces serveurs en cas de panne ou de sinistre majeur. Les supports nomades (ordinateurs portables, clé USB, assistants personnels etc.) doivent faire l'objet d'une sécurisation particulière, par chiffrement, au regard de la sensibilité des dossiers ou documents qu'ils peuvent stocker. Les matériels informatiques en fin de vie, tels que les ordinateurs ou les copieurs, doivent être physiquement détruits avant d'être jetés, ou expurgés de leurs disques durs avant d'être donnés à des associations. Les disques durs et les périphériques de stockage amovibles en réparation, réaffectés ou recyclés, doivent faire l'objet au préalable d'un formatage de bas niveau destiné à effacer les données qui peuvent y être stockées.

9. Anticiper et formaliser une politique de sécurité du système d'information

L'ensemble des règles relatives à la sécurité informatique doit être formalisé dans un document accessible à l'ensemble des agents ou des salariés. Sa rédaction requiert l'inventaire préalable des éventuelles menaces et vulnérabilités qui pèsent sur un système d'information. Il convient de faire évoluer régulièrement ce document, au regard des modifications des systèmes et outils informatiques utilisés par l'organisme concerné. Enfin, le paramètre « sécurité » doit être pris en compte en amont de tout projet lié au système d'information.

10. Sensibiliser les utilisateurs aux « risques informatiques » et à la loi "informatique et libertés"

Le principal risque en matière de sécurité informatique est l'erreur humaine. Les utilisateurs du système d'information doivent donc être particulièrement sensibilisés aux risques informatiques liés à l'utilisation de bases de données. Cette sensibilisation peut prendre la forme de formations, de diffusion de notes de service, ou de l'envoi périodique de fiches pratiques. Elle sera également formalisée dans un document, de type « charte informatique », qui pourra préciser les règles à respecter en matière de sécurité informatique, mais aussi celles relatives au bon usage de la téléphonie, de la messagerie électronique ou encore d'internet. Ce document devrait également rappeler les conditions dans lesquelles un salarié ou un agent peut créer un fichier contenant des données personnelles, par exemple après avoir obtenu l'accord de son responsable, du service juridique ou du CIL de l'entreprise ou de l'organisme dans lequel il travaille.

Ce document doit s'accompagner d'un engagement de responsabilité à signer par chaque utilisateur.

A noter : veiller à ce que les utilisateurs nettoient régulièrement leurs vieux documents et messages électroniques sur leurs postes. De même, nettoyer régulièrement le répertoire d'échange partagé entre les différents services afin qu'il ne se transforme pas en espace « fourre-tout » (fichiers personnels des agents mélangés avec des dossiers sensibles)

EBIOS : un outil simple et puissant

La gestion des risques est largement décrite et préconisée dans la presse, les normes, la réglementation… EBIOS® (Expression des Besoins et Identification des Objectifs de Sécurité) est la méthode de gestion des risques de l'ANSSI. Opérationnelle, modulaire et alignée avec les normes, c'est la boîte à outils indispensable pour toute réflexion de sécurité des systèmes d'information (SSI). Voici comment EBIOS peut vous être utile.

Le risque SSI dans EBIOS : un exemple éclairant

Définition du risque : c'est un scénario qui combine un événement redouté (sources de menaces, bien essentiel, critère de sécurité, besoin de sécurité, impacts) et un ou plusieurs scénarios de menaces (sources de menaces, bien support, critère de sécurité, menaces, vulnérabilités).

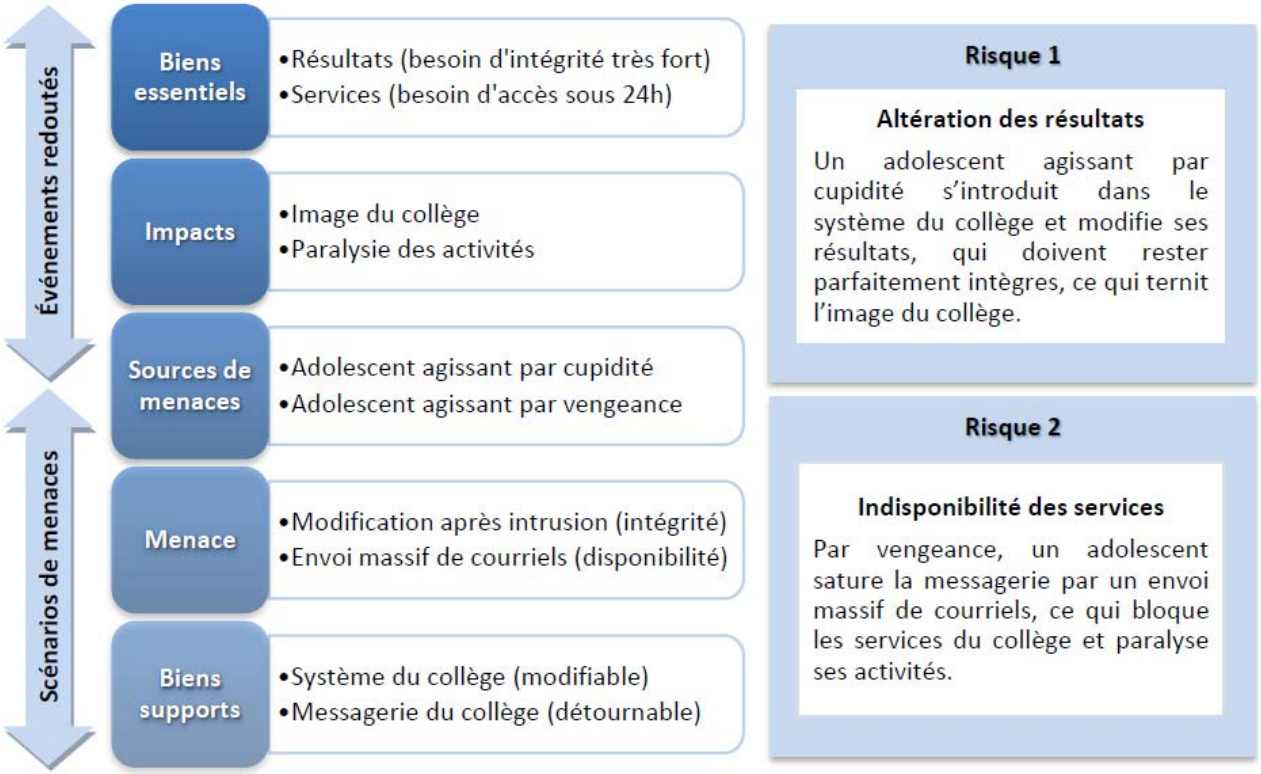
On estime son niveau par sa gravité (hauteur des impacts) et sa vraisemblance (possibilité qu'il se réalise).

Un adolescent de 15 ans « pirate » le système informatique de son collège pour améliorer ses notes.

Un adolescent de quinze ans a en effet été interpellé pour s'être introduit dans le système informatique de son collège dans le but de modifier ses résultats scolaires. Dépité de n'avoir pu atteindre ce but, le collégien a saturé le système informatique en expédiant plus de 40 000 courriels, manœuvre qui a provoqué une indisponibilité pendant quatre jours.

[Sources Internet : Le Point.fr et ZDNet]

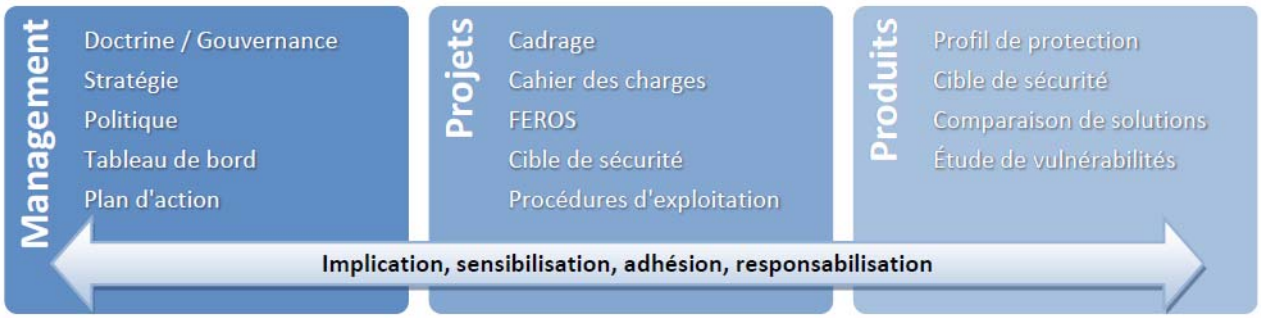
À partir de ce fait divers et de la définition du risque d'EBIOS, nous pouvons mettre deux risques en évidence.



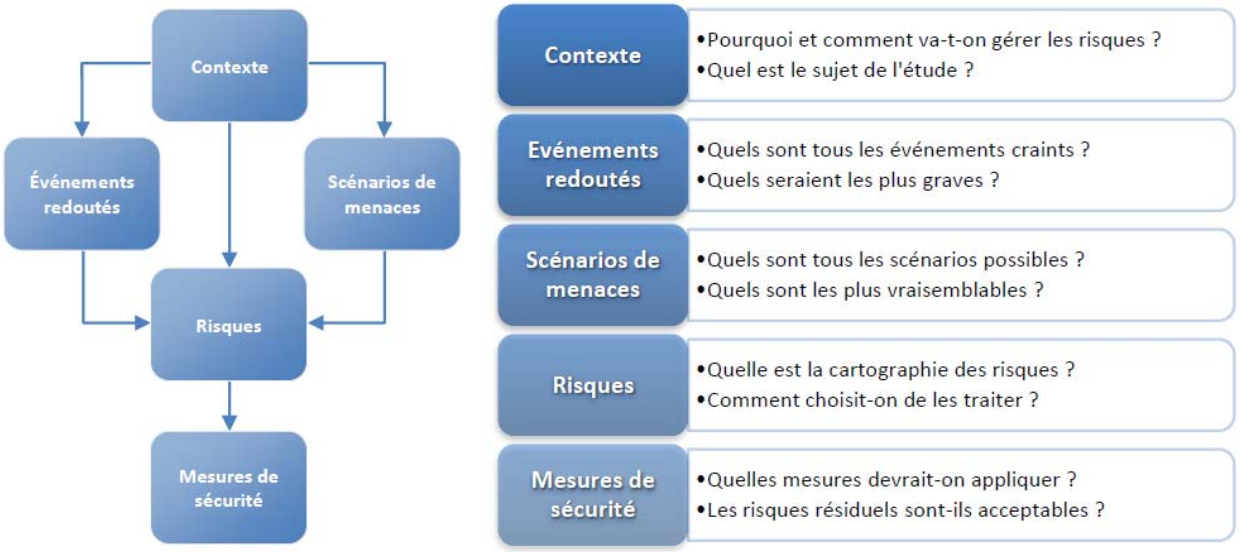
Une étude EBIOS appliquée au système du collège aurait permis, simplement et rapidement :

- d’identifier ces deux risques, ainsi que tous les autres qui pèsent sur le système d’information du collège ;
- d'estimer leur niveau (gravité, vraisemblance), les cartographier et prendre des décisions en conséquence ;
- de choisir les mesures nécessaires et suffisantes en termes de prévention, de protection et de récupération.

EBIOS est le "tout terrain" pour gérer les risques



Les 10 questions essentielles pour gérer les risques



Grands principes à appliquer

Pour réussir une étude et son application, il convient de respecter 4 grands principes de mise en œuvre :

- employer EBIOS comme une boîte à outils pour une efficacité maximale ;
- utiliser la méthode avec souplesse pour adhérer au langage et aux pratiques de l’organisme ;
- améliorer progressivement l’étude, en temps réel, pour rester cohérent avec la réalité ;
- rechercher une adhésion des acteurs du système d’information pour élaborer des solutions de protection.

Une mise en œuvre facilitée

La méthode dispose de bases de connaissances riches et enrichissables, d'un logiciel libre et gratuit, de formations et d'une documentation variée. La communauté des experts et utilisateurs de gestion des risques (industriels, administrations, prestataires, universitaires…) se réunit régulièrement au Club EBIOS pour échanger des expériences et enrichir le référentiel. EBIOS ne vous protège pas des risques, elle vous permet d’en faire prendre conscience aux décideurs.

Exit les mots de passe statiques, place aux jetons, certificats et autres moyens biométriques. Questions-clés, définitions, liens utiles et citations : l'essentiel de ce qu'il faut savoir en un coup d'œil.

On appelle authentification forte tout système permettant un accès informatique après une double vérification. L'objectif est de pallier les faiblesses de l'authentification unique par mot de passe. En effet, les mots de passe peuvent être volés, forcés et posent un problème de mémorisation à l'utilisateur et de renouvellement à l'entreprise. S'ils restent en usage dans les environnements où l'impératif de sécurité est faible, grâce à leur rapport qualité / prix imbattable, ils montrent certaines limites dans des contextes à sécurité élevée.

L'authentification forte consiste donc à mixer différentes stratégies d'authentification : une carte magnétique et une identification par l'iris par exemple, ou un certificat électronique et un code alphanumérique affiché à l'écran sur des sites bancaires. Ces informations sont ensuite mises en relation avec une solution de gestion des identités et des accès, elle-même en relation avec un annuaire ou un méta-annuaire de l'entreprise qui référence tous les utilisateurs du parc informatique ainsi que leurs droits.

En raison du coût de l'authentification forte, son usage reste aujourd'hui réservé aux grands comptes ou, plus généralement, aux secteurs critiques de l'industrie et des services (banque, énergie, défense, aéronautique, automobile, recherche scientifique). Elle se retrouve toutefois de plus en plus fréquemment utilisée par des entreprises de taille modeste qui souhaitent ouvrir leur système d'information à l'extérieur par des accès mobiles aux réseaux privés virtuels (VPN) de l'entreprise.

Le principe du jeton

L'authentification forte s'appuie sur d'autres concepts que celui des mots de passe. Le premier d'entre eux étant celui du jeton unique. Le principe est simple : il s'agit d'un algorithme de génération de mots de passe unique, à durée de vie courte, qui se synchronise avec une application cliente installée sur le poste de travail. Cet algorithme peut être installé sur une calculette se contentant alors d'afficher le code généré, sur une clé USB, qu'il faudra brancher à l'appareil, ou sur une carte à puces qui transmet le code par contact avec un appareil de lecture. Le mot de passe ainsi généré n'est valable que pour une période de temps de 1 à 2 minutes.

Cette technique minimise l'impact du vol de mots de passe mais ne fait que reporter le problème. En effet, s'il permet de lutter efficacement contre l'intrusion à distance, l'authentification repose désormais sur un élément physique qui risque d'être dérobé. De plus, le jeton ne corrige pas le problème de la mémorisation des mots de passe par l'utilisateur car un salarié qui perd ou oublie son système de jeton ne peut pas non plus accéder à son poste ou à ses applications.

Il existe également des cartes reposant sur le principe du jeton unique mais sans code à saisir pour l'utilisateur. La transmission de ce code s'effectue alors par ondes sonores, mais nécessite la mise en place d'un récepteur. Enfin, le principe du jeton est aussi appliqué sur des cartes plastiques imprimés. Sur ces cartes figurent une série de numéro et l'utilisateur découvre leur ordre d'entrée et la composition du code unique lors de la phase d'authentification. Le logiciel client se charge de lui indiquer la ligne et la colonne du chiffre à saisir pour s'authentifier.

Les certificats électroniques

Deuxième solution d'authentification forte mise en place, cette fois-ci pour sécuriser les accès aux services Internet : les certificats électroniques, qui appliquent en partie le principe du jeton sur le Web. Les certificats électroniques sont des fichiers attestant de l'identité de l'auteur en liant par exemple son mot de passe à des renseignements personnels (date de naissance, numéro de sécurité sociale…). Le certificat électronique envoie ensuite ces informations à un serveur central

qui vérifie que ce fichier est bien représenté dans sa base de données avant de lui autoriser l'accès aux services Web.

Contrairement au principe du jeton, les certificats électroniques disposent d'une durée de vie plus longue, en moyenne de quelques semaines mais qui peut s'étaler sur plusieurs années. Autre différence, le jeton n'est pas émis par une carte que possède l'utilisateur mais par le serveur, après saisie des données personnelles de l'utilisateur. Aussi, si l'utilisateur perd son certificat électronique, il peut en redemander un autre et s'authentifier rapidement.

Il existe toutefois deux limites aux certificats électroniques. D'abord, cela implique un cadre juridique strict de gestion des identifiants utilisateurs et il paraît délicat d'imposer à l'utilisateur une base de données centrale où repose l'ensemble de ses certificats traçant ses connexions. D'autre part, le certificat électronique peut être intercepté, volé, répliqué et utilisé en accédant au poste de l'internaute, ce qui ne garantit donc pas que le porteur du certificat soit bien son créateur.

La biométrie

Sans doute la méthode la plus prometteuse, mais aussi la plus délicate à mettre en œuvre, la biométrie appartient à la catégorie des technologies d'authentification forte. Elle repose sur des systèmes de capture d'images couplés à une base de données centrale stockant les informations personnelles. On distingue 4 catégories d'applications à la biométrie : la reconnaissance digitale, la reconnaissance d'iris, la reconnaissance faciale et la reconnaissance vocale. L'avantage de ces méthodes est clair : l'utilisateur a toujours sur lui ses "codes d'authentification" et ne peut les perdre ou les oublier...

Il existe toutefois - outre son coût - plusieurs limites à la biométrie. Tout d'abord l'aspect juridique, les droits des personnes étant fichés, leurs caractéristiques morphologiques aussi. Ces bases de données sont à rapprocher de celles utilisées par la police et donc soumises à des lois très strictes. D'autre part, les données peuvent être falsifiées dans le cas de la reconnaissance digitale ou de la reconnaissance vocale.

Enfin, la biométrie pose le problème de la qualité de l'authentification. Ces méthodes ne sont en effet pas toujours fiables à 100%, ce qui empêche des utilisateurs de bonne foi d'accéder à leur système. L'un des axes de recherche de la biométrie porte donc sur la multimodalité, c'est-à-dire la combinaison de plusieurs méthodes d'identification par voie biométrique.

Algorythmes et protocoles

Les solutions d'authentification forte s'appuient sur de nombreux protocoles de sécurité, de manière à acheminer l'information personnelle de l'utilisateur de la manière la plus sure jusqu'au serveur d'authentification. Sur le Web, le protocole HTTPS se base sur le procédé de cryptographie SSL (Secure Sockets Layers) qui s'assure que les paquets échangés entre le serveur et le client ne sont pas lisibles de l'extérieur. Dans les réseaux étendus d'entreprise, cette fonction est assumée par le protocole IPSec, géré par la majorité des réseaux privés virtuels (VPN).

Dans les réseaux internes, il existe différentes couches de sécurité. Sur les réseaux mobiles, le protocole 802.11i remplit ce rôle de cryptage tandis que les réseaux fixes utilisent depuis longtemps le 802.10. Mais derrière l'ensemble de ces protocoles se trouve l'algorithme de cryptage AES (Advanced Encryption Standard), créé en 1998 et capable de générer des clés uniques de 128 à 256 bits. Ce système offre des milliards de possibilités de code, ce qui le rend presque insensible à des techniques de déchiffrage par la force (en essayant de multiples combinaisons).

Parallèlement à AES, il existe le protocole de cryptage PGP, fréquemment utilisé pour chiffrer le contenu des e-mails envoyés sur Internet. Cet algorithme est mis à disposition de tous en libre accès depuis 1991 et a donné lieu à de nombreuses implémentations depuis.

LIVRE III : Des crimes et délits contre les biens.
TITRE II : Des autres atteintes aux biens.

CHAPITRE III : Des atteintes aux systèmes de traitement automatisé de données.

Modifié par Loi n°2004-575 du 21 juin 2004 - art. 45 JORF 22 juin 2004

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Article 323-3

Modifié par Loi n°2004-575 du 21 juin 2004 - art. 45 JORF 22 juin 2004

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Article 323-3-1

Créé par Loi n°2004-575 du 21 juin 2004 - art. 46 JORF 22 juin 2004

Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-4

Modifié par Loi n°2004-575 du 21 juin 2004 - art. 46 JORF 22 juin 2004

La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-5

Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;

2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;

3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;

4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;

6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;

7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35.

Article 323-6

Modifié par LOI n°2009-526 du 12 mai 2009 - art. 124

Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

Article 323-7

Modifié par Loi n°2004-575 du 21 juin 2004 - art. 46 JORF 22 juin 2004

La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.

DOCUMENT 5

Stéphane Bellec et Christophe Elise, site internet 01 Informatique,

"Priorité au poste de travail" , 27 août 2008

Sujet considéré comme banal, parent pauvre des projets de sécurité, la protection des postes de travail n'a pourtant jamais été plus d'actualité. Fuite des données confidentielles, pertes et vols d'ordinateurs portables ont rappelé que l'architecture réseau seule ne suffit pas à sécuriser les postes.

Doit-on encore et toujours sécuriser le poste de travail en entreprise ? Si la question peut surprendre, elle est loin d'être une simple provocation. Il n'est pas absurde de penser que, par défaut, si le système d'information est sécurisé, les postes de travail le seront. Et s'il est un concept qui a prédominé à ce sujet ces dix dernières années, c'est bien celui de la sécurité périmétrique.

Dès lors, pourquoi se soucier de la protection de postes de travail retranchés au sein de la forteresse créée par toute entreprise et sécurisés par une infrastructure réseau moderne ? Passerelles antivirus, pare-feu, boîtiers UTM (Unified Threat Management, ou gestion unifiée des menaces), systèmes de prévention d'intrusion (IPS pour Intrusion Prevention System) aux débits surboostés, appliances de filtrage de contenu… devraient être bien suffisants. Hélas, cette façon de raisonner n'est pas réaliste. Le poste de travail, aux mains d'un utilisateur lambda, reste un point majeur de vulnérabilité des systèmes d'information. Son pouvoir d'attraction pour de multiples nuisances n'a cessé de croître : virus, vers, spywares, malwares, phishing, chevaux de Troie… Mal contrôlé, il peut finir sa vie comme minable “ zombie ” d'un botnet.

La tentation du poste client léger ou virtualisé

Cette dernière tendance souligne – contrairement au postulat suggéré par la question d'introduction – l'importance de sécuriser avec soin ses postes de travail. Et la croissance des ordinateurs mobiles au sein des parcs d'entreprises a renforcé cette prise de conscience. Fort heureusement, le marché a su s'adapter à l'évolution des menaces et proposer des parades. Reste aux sociétés à considérer le chantier de la sécurisation des postes de travail avec autant de sérieux que d'autres projets d'infrastructures. “ On a longtemps pensé se débarrasser de la problématique en combinant antivirus et protection périmétrique. Le poste de travail n'était pas une priorité, il le redevient ”, constate Etienne Busnel, directeur de l'entité sécurité chez Euriware.

Face au problème, certaines entreprises choisissent d'autres voies, celles de la simplification du poste de travail avec le recours aux clients légers ou à la virtualisation. Une approche teintée de nostalgie selon Thierry Ramard, PDG d'Ageris Group : “ On rebanalise ainsi le poste de travail en revenant à la période où l'architecture qui dominait était celle d'un terminal peu intelligent, doté de peu de puissance et de capacité, dans un monde où l'informatique était centralisée. ”

Faut-il un chiffrement des portables ?

La sécurisation de ces postes n'implique pas forcément un parcours semé d'embûches. Pour cerner le problème, trois points fondamentaux sont à envisager : qui accède aux postes de travail ? Quelle est la cible de sécurité et comment y répondre ? Comment s'assurer du suivi et de la cohérence de l'ensemble ? C'est en fonction des réponses à ces questions que se fera le choix entre les solutions du marché. Avec une règle à respecter : évaluer les briques technologiques seulement selon les risques et les objectifs fixés par l'entreprise. Ainsi, prendre conscience de la pertinence du chiffrement n'a d'intérêt que si l'on réalise que celui-ci ne s'adresse pas exclusivement aux ordinateurs portables. D'ailleurs, ces derniers n'ont pas nécessairement tous besoin de cette technologie.

De même, si SSO (Single Sign-On, ou authentification unifiée) séduit les utilisateurs, il est parfois délicat à mettre en œuvre, et ne peut être considéré comme le sésame miraculeux du contrôle d'accès. L'authentification forte s'impose, mais que préférer, token ou carte à puce ? Les suites intégrées combinent des fonctionnalités à utiliser à la demande, mais le client unique reste le seul garant des performances et d'une intégration digne de ce nom. En outre, toutes les fonctions de

sécurité ne sont pas nécessairement à déployer au niveau du poste de travail. Indirectement, ce dernier est aussi protégé par des choix faits en amont au niveau du réseau.

L'authentification forte présente sur tous les postes de travail

L'entreprise qui tient à assurer la sécurité de son parc et au-delà, celle de son système d'information, doit pouvoir authentifier les utilisateurs de ses machines. Le seul couple identifiant-mot de passe est dépassé. Place aux tokens et cartes à puce.

Le Single Sign-On (SSO, ou authentification unifiée) est un des rares dispositifs avec lequel on augmente à la fois le niveau de sécurité et le confort d'utilisation de la machine. Ainsi, un responsable de la sécurité des systèmes d'information (RSSI) peut obtenir les moyens de mettre en œuvre un projet de contrôle d'accès aux postes de travail, une étape indispensable à toute politique de sécurité. Le Single Sign-On n'est pas la seule solution, mais de nombreuses entreprises gagneraient à renforcer ou repenser leur stratégie de contrôle. Une réalité qui mérite d'être rappelée, d'après Etienne Busnel, directeur du département sécurité chez Euriware : “ La tendance a longtemps été de se reposer sur le contrôle d'accès physique aux locaux. On faisait simplement confiance aux utilisateurs puisqu'ils étaient entrés légitimement dans les bâtiments. ”

Une reconnaissance simple avec des jetons

La progression de la mobilité et l'usage des machines portables ont fait prendre conscience de l'imprudence de cette approche. Et à travers elle, de celle du seul recours au couple identifiant-mot de passe comme moyen de sécurisation. Le marché le clame depuis trois ans : à bas le mot de passe unique ! Une rengaine pertinente, même si elle est surtout reprise par les acteurs de l'authentification forte. L'utilisation pour cette dernière de jetons (token), simples d'utilisation, s'est d'ailleurs démocratisée dans les entreprises. Même si d'aucuns tempèrent le recours à ce type de mécanismes. “ Mieux vaut un bon mot de passe qu'un mauvais certificat logiciel ”, prévient Gérôme Billois, manager chez Solucom Sécurité. Des processus déficients de gestion, de délivrance ou de renouvellement du certificat peuvent conduire à un échec. Ce qui serait dommage, tant les usages de cette authentification forte dépassent le seul cadre du poste de travail.

Une identification visuelle avec la carte à puce

Le badge unique apparaît comme une solution de transition souple pour les sociétés en retard sur cette question du contrôle d'accès. La carte à puce, invention bien française, a alors un sérieux avantage sur les jetons : elle peut aussi accueillir une photo en surface. A travers les informations contenues dans la puce, la carte ouvre alors des perspectives d'authentification à trois facteurs : ce que son titulaire sait, avec le code PIN, ce qu'il possède, via la carte et une identification visuelle, et qui il est, à travers un lecteur biométrique.

Ce qui était encore qu'un scénario hypothétique en 2005 est donc devenu une réalité. “ Le badge unique permet de rentrer dans les locaux, la bande magnétique vous permet de déjeuner à la cantine, la carte à puce d'accéder à votre poste ”, explique Edouard Jeanson, expert sécurité chez Sogeti. On notera que, dans cet exemple, la biométrie est passée à la trappe. L'intégration de plus en plus courante de cette technique dans les postes mobiles pourrait toutefois changer la donne.

Une sécurisation pas assez personnalisée

Le poste de travail, qu'il soit fixe ou mobile, a beau être retranché au sein de réseau, il doit être équipé d'une protection solide. Adaptés à la cible, ces outils de sécurisation font trop souvent la part belle aux suites intégrées et à leurs nombreuses fonctions.

“ La sécurisation du poste de travail, qui est une problématique d'infrastructure, n'a nécessairement pas le même enjeu que la sécurisation d'un processus ” témoigne Gérôme Billois, manager chez Solucom Sécurité. Cependant cette tâche, qui n'est pas à négliger, n'a rien d'ingrat. Ne serait-ce que parce que le poste de travail est le lieu naturel pour incarner la politique de sécurité de l'entreprise. Ainsi la protection du réseau ne saurait se concevoir sans considérer d'abord celle de ces postes. Laquelle débute par leur contrôle d'accès.

Définir la problématique n'est pas difficile. “ Quelle est la cible de sécurité de mon poste de travail et comment vais-je y répondre au mieux ? ” Tel est, selon Gérôme Billois, le début de la réflexion. Bien que la réponse dépende des besoins de l'entreprise, on distingue souvent quatre cibles aux quelles il faudra adapter un degré de sécurisation : le poste bureautique traditionnel, le poste nomade, le poste à sécurité renforcée, et le poste dit métier (points de vente, terminaux industriels, etc.).

On le voit bien, c'est l'usage qui est fait du poste de travail qui conditionne son niveau de sécurité. “ L'utilisateur peut avoir à traiter des données plus ou moins sensibles. Le socle minimal de sécurisation commun à l'ensemble des postes est, par exemple, l'antivirus ”, développe Thierry Ramard, PDG d'Ageris Group, société spécialisée en management de la sécurité de l'information. C'est autour de cette brique logicielle que s'est construite ces dix dernières années la sécurisation des postes d'utilisateur. Au fur et à mesure que les menaces se sont diversifiées, il est devenu nécessaire d'adopter une sécurité multicouche. A l'antivirus s'est ajouté l'antispam, l'antispyware, le pare-feu personnel, le réseau privé virtuel, le Host IPS (pour Intrusion Prevention System). Et d'un logiciel unique, administrable à distance sur l'ensemble des postes du parc via une seule console, on est passé à l'ère de la suite intégrée, multifonctionnelle. Une suite que l'on peut comparer à un couteau suisse de la sécurité. Mais dont la performance est rarement au rendez-vous.

Des suites devenues des “ usines à gaz ”

“ Ces suites sont gourmandes en ressources, et le poste, se retrouvant surchargé par ces fonctions au détriment des autres processus, finit par ne faire que de la sécurité ! ” relève Gérôme Billois. Elles ne sont donc que très rarement utilisées à 100 % de leurs capacités. D'autant qu'un poste trop verrouillé peut contraindre son utilisation. Ce que confirme Etienne Busnel, directeur du département sécurité chez Euriware : “ On finit souvent par désactiver le pare-feu pour arriver à faire fonctionner correctement les applications. ” Yvan Lhotellier, directeur technique chez Integralis, renchérit : “ Beaucoup d'entreprises ne veulent que l'antivirus et le pare-feu. Ajoutez un HIPS et cela vous génère des logs gigantesques inexploitables ”.

De la suite intégrée devenue une“ usine à gaz ”, on évolue donc peu à peu vers le logiciel client unique. Ce dernier a la particularité de proposer un ensemble de fonctions partageant un seul noyau. D'où une meilleure intégration des fonctions entre elles, mais aussi du client dans le poste de travail. Néanmoins, peu d'éditeurs maîtrisent encore l'art subtil du client unique, une technologie encore jeune. “ Symantec propose la meilleure intégration du marché autour d'un noyau unique. De leur côté, McAfee et, plus surprenant, Checkpoint, lequel n'est pourtant pas un spécialiste du poste de travail, ne sont pas très loin du leader ”, estime Gérôme Billois.

Un socle de sécurité minimum

Suite intégrée ou client unique, on en revient toujours à un socle minimum à mettre en œuvre, qui passe en premier lieu par un durcissement de la sécurité affectée au poste. Ce qui implique une limitation des droits des utilisateurs, un renforcement des autorisations d'accès aux répertoires, l'arrêt des processus et services inutiles, voire le blocage des périphériques externes (disque dur, clé USB, iPod). L'antivirus accompagne cette démarche avec une logique qui ne doit surtout pas être ni binaire, ni isolé. Son usage doit être considéré non seulement en rapport avec les autres technologies de filtrage, pare-feu et HIPS, mais avec le reste des outils de sécurité présents dans le système d'information.

Face à l'infiltration d'un programme malveillant (ou cheval de Troie), ce sont encore la cible de sécurité et l'adéquation à la politique de sécurité globale de l'entreprise qui priment. “ Un cheval de Troie sur une machine n'est pas nécessairement grave s'il n'a pas d'impact sur le métier, sur la productivité ”, affirme – à raison – Frédéric Guy, business development manager Europe du Sud chez Trend Micro. Le danger d'un tel programme est surtout son utilisation par un botmaster pour prendre le contrôle de la machine. Afin de se prémunir contre ces dangers, les éditeurs d'antivirus travaillent sur des systèmes de réputation de sites et de serveurs, qui veillent à ce qu'aucun cheval de Troie ne puisse être téléchargé, et empêchent toute communication entre la machine infectée et le pirate. Etienne Busnel rappelle que “ selon ce qui a été installé sur la passerelle, la protection au niveau du poste de travail peut être plus légère ”. Une logique valide pour le parc statique. Par exemple, celui-ci, grâce aux boîtiers multifonctions UTM installés au

niveau du réseau, verra la charge qu'il subit en termes de filtrage allégée. “ Soyez pertinents, ayez un environnement homogène ” conseille Frédéric Guy.

Mieux protéger les postes nomades

Si l'important sujet de la sécurisation du poste de travail demande une réelle attention, il n'est pas indépendant de la politique de sécurité établie au niveau du réseau de l'entreprise. Combiner antivirus, pare-feu et HIPS sur un poste fixe n'a pas grand sens lorsque ces produits agissent déjà par ailleurs dans le réseau. D'autant plus que“ sur un parc de milliers de machines, vous en aurez toujours certaines infectées, insiste Gérôme Billois. Donc il faut maîtriser la propagation, savoir gérer la crise afin de la contenir et pouvoir reprendre le poste ”. Qui dit reprise du poste dit sauvegarde et synchronisation des données. Un domaine connexe de la sécurisation qui ne doit être oublié.

Au chapitre des briques à évaluer en fonction de la cible de sécurité, le chiffrement a force de loi dès lors qu'on évoque les postes nomades. “ Les risques d'être volés ou perdus sont plus élevés ”, note Etienne Busnel. Ceux-ci bénéficient souvent d'un contrôle de conformité supplémentaire afin de s'assurer que les outils mis en place et la politique de sécurité définie sont toujours d'actualité. “ Il s'agit d'une problématique de protection du patrimoine informationnelle de l'entreprise ”, souligne Edouard Jeanson, expert sécurité chez Sogeti. “ Je chiffre mes données pour une population sensible. ” Le chiffrement – de dossiers, de fichiers – va de pair avec le verrouillage des périphériques externes. Les données ne doivent pas être accessibles en cas de vol, ni échapper à la vigilance de l'entreprise par le biais d'un simple transfert sur une clé USB. Yvan Lhotellier, directeur technique chez Integralis, précise que les entreprises focalisent leurs investissements sur les ordinateurs portables : “ Des solutions unifiées, faciles à administrer, transparentes pour l'utilisateur, existent sur le marché. ” Ainsi, le choix d'un outil et son déploiement chez un grand compte s'effectuent souvent dans un délai de six mois maximum.

Les entreprises commencent à réaliser l'importance de leur information, et de sa préservation, en acceptant d'y consacrer les moyens nécessaires. Une bonne opportunité pour les RSSI de mettre à jour le niveau de sécurisation global de leur parc de postes de travail.

La gestion automatisée de parc, vecteur de protection

Les tâches dédiées à la sécurité du poste de travail ont besoin d'être centralisées et automatisées avec les outils ad hoc de gestion de parc. La tentation du poste client léger ou du PC virtualisé existe aussi pour réduire les risques sécuritaires.

“ Un poste de travail bien sécurisé doit avant tout être bien administré. ” Tels furent les propos de John Thompson, directeur d'Altiris, au moment du rachat de son entreprise par Symantec l'an dernier. Il est vrai que si le poste de travail doit être équipé des accessoires nécessaires à sa protection (antivirus, antispam, pare-feu, etc.), ces outils seront inutiles si l'administration ne suit pas. Qu'entend-on par administrer la sécurité ?

Les éditeurs Symantec-Altiris, McAfee, Criston, Landesk et Microsoft sont les principaux acteurs de ce marché. Ils ont tous pour objectif d'effectuer toutes les actions de sécurité du poste de travail. Mais pas seulement. Selon Philippe Charpentier, de Symantec-Altiris, il existe trois principes clés : automatiser, standardiser et maintenir à jour. L'automatisation a pour but de réduire les risques et les erreurs liés au facteur humain. Ces dernières sont souvent dues à la complexité de certaines procédures. Automatiser a également comme avantage de réduire les coûts. La standardisation, qu'elle soit appliquée au niveau serveur ou poste de travail, lutte contre l'hétérogénéité d'un parc. En effet, plus il y a de systèmes d'exploitation différents, plus le risque existe que le nombre de failles de sécurité soit important. “ Enfin, termine Philippe Charpentier, si on pense très souvent à prendre en compte les mises à jour des outils de sécurité, il ne faut pas négliger pour autant celles du système d'exploitation lui-même. ”

Travailler davantage les opérations de restauration

Cinq grandes catégories d'outils viennent constituer un socle commun contribuant à l'administration de la sécurité du PC. D'abord, ceux concernant la gestion d'inventaire. A priori, on pourrait se demander quel est le rôle de cet élément de base de la gestion d'un parc de machines en termes de sécurité. Pourtant, son rôle consistant à faire un état de ce qui est présent sur une

machine, cette fonction aide l'administrateur à mesurer la déviance du poste inventorié par rapport à l'état de départ. Plus les écarts seront grands, plus l'homogénéité du parc est menacée. Ensuite viennent les correctifs logiciels et automatiques liés aux outils de sécurité et du système. La distribution manuelle des mises à jour est la troisième brique. Elle consiste à effectuer la maintenance des applicatifs métier développés pour ou par l'entreprise. Autre outil, celui assurant le suivi des déploiements système et applicatif. Comme l'assure Raphaël Chauvel, directeur technique chez Criston : “ Quand une attaque est passée, il faut savoir limiter les dégâts. ” Un administrateur doit donc être capable de réagir vite et de restaurer une application ou un système complet. Ce qui implique une gestion des images de toutes ces ressources. McAfee travaille d'ailleurs sur une prochaine version de Virusscan, qui pourra mettre à jour les images pour une restauration sécurisée.

Une console pour superviser en temps réel

Cinquième et dernier élément, mais pas le moindre : la console d'administration de la sécurité. Véritable tableau de bord, elle est là pour fournir l'outil de supervision en temps réel à l'administrateur. Elle a pour mission de centraliser les informations et les événements relatifs à la sécurité. Les consoles les plus évoluées, les Siem (Security Information and Event Management), intègrent aussi la production de rapport et de tableaux de bord à des fins d'analyse.

Au-delà du choix de ces outils, on peut s'interroger sur le débat entre client léger ou client virtualisé et sur leur efficacité respective en ce qui concerne la sécurité du poste client. L'avantage du client léger est qu'il repose sur l'accès à des applications lourdes fonctionnant sur le serveur distant. Le poste de travail virtualisé sera plus autonome en terme de connexions une fois les programmes chargés. Une variante existe dans la virtualisation applicative. Des produits comme Software Virtualisation Solution (SVS) d'Altiris, Thinstall ou encore Softricity de Microsoft proposent ce genre de solution. Thinstall propose, par exemple, d'isoler complètement une application Windows en l'enfermant dans une capsule autonome qui pourra fonctionner sur n'importe quelle plate-forme Windows sans jamais dialoguer ni toucher au système…

La sécurité des postes de travail passe par une mise en œuvre de mesures pour prévenir
- les tentatives d'accès frauduleux ;
- l'exécution de virus ;
- la prise de contrôle à distance, notamment via internet.

Les risques d'intrusion dans les systèmes informatiques sont importants et peuvent conduire à l'implantation de virus ou de programmes «espions».

Les précautions élémentaires

- Limiter le nombre de tentatives d'accès à un compte. En fonction du contexte, ce nombre peut varier entre trois et dix. Lorsque la limite est atteinte, il est préférable de bloquer la possibilité d'authentification à ce compte temporairement ou jusqu'à l'intervention d'un administrateur du système ;
- installer un «pare-feu» (firewall) logiciel, et limiter les ports de communication strictement nécessaires au bon fonctionnement des applications installées sur le poste de travail ;
- utiliser des antivirus régulièrement mis à jour ;
- prévoir une procédure de verrouillage automatique de session en cas de non-utilisation du poste pendant un temps donné. Pour les opérations de maintenance, il convient de mettre fin à une session après une à cinq minutes d'inactivité. Pour d'autres opérations moins critiques (accès à une application métier par exemple), un délai de quinze minutes doit permettre de garantir la sécurité sans compromettre l'ergonomie d'utilisation ;
- prévoir d'afficher, lors de la connexion à un compte, les dates et heures de la dernière connexion.

Ce qu'il ne faut pas faire

- Utiliser des systèmes d'exploitation obsolètes (une liste mise à jour régulièrement est disponible à l'adresse internet : http://www.certa.ssi.gouv.fr/

Pour aller plus loin

- Limiter les applications nécessitant des droits de niveau administrateur pour leur exécution ;
- limiter les services du système d'exploitation s'exécutant sur le poste de travail à ceux qui sont strictement nécessaires ;
- installer les mises à jour critiques des systèmes d'exploitation sans délai en programmant une vérification automatique périodique hebdomadaire ;
- mettre à jour les applications lorsque des failles critiques ont été identifiées et corrigées ;
- concernant les virus, se référer au document du CERTA disponible à l'adresse internet http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-007/ pour des recommandations plus complètes.

LIVRE II : Des crimes et délits contre les personnes.
TITRE II : Des atteintes à la personne humaine.
CHAPITRE VI : Des atteintes à la personnalité.

Section 5 : Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques.

Article 226-16

Modifié par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004

Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2° du I de l'article 45 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Article 226-16-1-A

Créé par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004

Lorsqu'il a été procédé ou fait procéder à un traitement de données à caractère personnel dans les conditions prévues par le I ou le II de l'article 24 de la loi n° 78-17 du 6 janvier 1978 précitée, le fait de ne pas respecter, y compris par négligence, les normes simplifiées ou d'exonération établies à cet effet par la Commission nationale de l'informatique et des libertés est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

Article 226-16-1

Créé par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004

Le fait, hors les cas où le traitement a été autorisé dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 précitée, de procéder ou faire procéder à un traitement de données à caractère personnel incluant parmi les données sur lesquelles il porte le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

Article 226-17

Modifié par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004

Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites* à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

Article 226-18

Modifié par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004

Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

Article 226-18-1

Créé par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004

Le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

Article 226-19

Modifié par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004

Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou

indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

Est puni des mêmes peines le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté.

Article 226-19-1
Créé par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004

En cas de traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende le fait de procéder à un traitement :

1° Sans avoir préalablement informé individuellement les personnes sur le compte desquelles des données à caractère personnel sont recueillies ou transmises de leur droit d'accès, de rectification et d'opposition, de la nature des données transmises et des destinataires de celles-ci ;

2° Malgré l'opposition de la personne concernée ou, lorsqu'il est prévu par la loi, en l'absence du consentement éclairé et exprès de la personne, ou s'il s'agit d'une personne décédée, malgré le refus exprimé par celle-ci de son vivant.

Article 226-20
Modifié par Loi n°2000-321 du 12 avril 2000 - art. 6
Modifié par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004

Le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi.

Est puni des mêmes peines le fait, hors les cas prévus par la loi, de traiter à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa.

Article 226-21
Modifié par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004

Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

Article 226-22
Modifié par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004

Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 Euros d'amende lorsqu'elle a été commise par imprudence ou négligence.

Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit.

Article 226-22-1
Créé par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004

Le fait, hors les cas prévus par la loi, de procéder ou de faire procéder à un transfert de données à caractère personnel faisant l'objet ou destinées à faire l'objet d'un traitement vers un État n'appartenant pas à la Communauté européenne en violation des mesures prises par la Commission des Communautés européennes ou par la Commission nationale de l'informatique et des libertés mentionnées à l'article 70 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

Article 226-22-2
Créé par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004

Dans les cas prévus aux articles 226-16 à 226-22-1, l'effacement de tout ou partie des données à caractère personnel faisant l'objet du traitement ayant donné lieu à l'infraction peut être ordonné. Les membres et les agents de la Commission nationale de l'informatique et des libertés sont habilités à constater l'effacement de ces données.

Article 226-23
Modifié par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004

Les dispositions de l'article 226-19 sont applicables aux traitements non automatisés de données à caractère personnel dont la mise en œuvre ne se limite pas à l'exercice d'activités exclusivement personnelles.

Article 226-24
Modifié par LOI n°2009-526 du 12 mai 2009 - art. 124

Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies à la présente section encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par les 2° à 5° et 7° à 9° de l'article 131-39.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

---

* **Article 34 de la loi n° 78-17 du 6 janvier 1978**
Modifié par la loi n°2004-801 du 6 août 2004 - art. 5 JORF 7 août 2004

Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Des décrets, pris après avis de la Commission nationale de l'informatique et des libertés, peuvent fixer les prescriptions techniques auxquelles doivent se conformer les traitements mentionnés au 2° et au 6° du II de l'article 8.

Finalité

Les copies de sûreté sont utiles principalement à deux choses :

- La première et la plus évidente est de permettre de restaurer un système informatique dans un état de fonctionnement suite à un incident (perte d'un support de stockage tel que disque dur, bande magnétique, etc., ou de tout ou partie des données qu'il contient).
- La seconde, incluse dans la première mais certainement la plus courante, est de faciliter la restauration d'une partie d'un système informatique (un fichier, un groupe de fichiers, un système d'exploitation, une donnée dans un fichier, etc.) suite à une suppression accidentelle ou à une modification non désirée.

La technique la plus fréquente est la recopie des données sur un support indépendant du système initial (ordinateur local, serveur, etc.).

L'opération inverse qui consiste à réutiliser des données sauvegardées s'appelle une restauration. On parle de « stockage » pour les données sauvegardées en attente d'une éventuelle restauration.

Critères de choix

Le choix d'une technique de sauvegarde se fera en prenant en compte :

- la capacité de stockage du support (le volume d'information)
- la vitesse de sauvegarde,
- la fiabilité du support (notamment après une longue période de stockage),
- la simplicité de classement,
- la facilité à restaurer les données,
- et bien sûr le coût de l'ensemble.

Intervient également la possibilité de sélectionner les données à sauvegarder. Enfin pour les grands systèmes de sauvegarde, il faut tenir compte de critères physiques : volume physique des supports de stockage, poids, sensibilité à la température, à l'humidité, à la poussière, à la lumière.

Stratégies de sauvegarde

On distingue la sauvegarde d'un poste individuel et la sauvegarde sur serveur. L'une et l'autre s'adressent à la même nature d'information (la donnée informatique) et ont le même objectif (protéger l'information et permettre de la retrouver si elle était perdue), mais les méthodes de sauvegarde sont différentes pour plusieurs raisons :

- les données sur poste client sont réputées moins importantes que les données gérées sur des systèmes centraux ;
- les utilisateurs sont moins sensibilisés au risque de perte de données que les professionnels de l'informatique ;
- ils ont également moins de formation sur les techniques de sauvegarde ;
- les moyens techniques sont moins développés sur poste individuel que sur serveur, même si des progrès importants ont été réalisés ces dernières années (chute du rapport coût/volume des supports de sauvegarde, simplification des interfaces de sauvegarde, sauvegarde sans intervention de l'utilisateur, etc.)

De fait la sauvegarde des données des postes individuels reste marginale dans la stratégie d'utilisation des ordinateurs. Cependant les entreprises, en généralisant l'usage des micro-ordinateurs et du partage des ressources en réseau, ont ressenti un besoin de sécurité qui a favorisé le développement d'outils de sauvegarde sur micro-ordinateurs, lesquels gagnent petit à petit le monde de la micro-informatique personnelle.

Sauvegarde sur serveur

La sauvegarde s'inscrit dans une démarche plus globale qui consiste à assurer la continuité d'activité d'un système informatique ou, en cas de défaillance, son redémarrage le plus vite possible. Cette démarche est souvent formalisée dans un document qui peut porter des noms divers, par exemple le Plan de reprise d'activité (PRA) ou le plan de secours, et qui fait appel soit à des automatismes (ex. donner l'alerte en cas de coupure de courant ou de perte d'accès à une unité de stockage) soit à des gestes manuels (ex. remplacer des bandes magnétiques défectueuses). La tendance est à l'automatisation, réputée plus sûre dans les situations d'urgence que les opérations manuelles.

En termes de support, les serveurs ont depuis toujours requis des supports à grande capacité de stockage. La bande magnétique a longtemps été le principal vecteur, du fait de sa grande capacité, de son coût faible (par rapport aux autres supports), de sa capacité de réutilisation et de sa relative stabilité au temps et à l'usure. Puis sont venus les cartouches numériques (bandes magnétiques intégrées dans un boîtier plastique type DAT, DLT, SDLT, LTO), les disques durs et plus récemment les médias optiques, ré inscriptibles ou non, tels que les CD-R, DVD-R ou formats similaires.

Sauvegarde sur système client

Au cours des années 1975–95, la plupart des utilisateurs d'ordinateurs personnels (PC) associaient principalement le terme "backup" au fait de faire des copies sur disquettes. Avec le développement de micro-ordinateurs mieux équipés, les utilisateurs personnels ont adopté des supports plus performants : disques optiques (CD-ROM ou DVD), clés USB. De même, les ordinateurs intègrent des fonctions de sauvegarde de plus en plus évoluées, par exemple :

- des outils intégrés au système d'exploitation tels que les "points de restauration" que l'on peut exécuter avant d'installer un nouveau logiciel et qui remettront le système en l'état d'avant l'installation si l'utilisateur le demande ;
- des logiciels capables de faire une image parfaite du système à un moment donné (image appelée un "ghost", en référence au logiciel du même nom, mot qui signifie "fantôme" en anglais) ; cette image sera stockée sur l'ordinateur lui-même ou sur un support externe.

Sauvegarde sur Internet

Avec la banalisation des connexions Internet à large bande et à haut débit, de plus en plus d'utilisateurs recourent à ce type de service de sauvegarde.
On peut différencier deux méthodes:

Sauvegarde en ligne

Aujourd'hui, les copies de sûreté dites « en ligne »1 deviennent populaires Elles consistent à se connecter à un site Internet, appelé « hébergeur », et à y transférer ses données. Les avantages sont multiples :

- minimiser le risque de perte puisque le site est géré par un professionnel qui fait lui-même des sauvegardes ;
- accéder à ses données à partir de n'importe quel ordinateur connecté à Internet ;
- souvent le coût de cette prestation est modique, parfois même gratuit pour les petites sauvegardes.

L'inconvénient majeur est de laisser ses données à disposition d'un tiers qui peut à loisir les consulter, les modifier, les dupliquer, les publier ou en faire commerce ; et même les rendre indisponibles (cas des faillites, rachats de sites par des concurrents, ou différend commercial avec l'hébergeur). Évidemment, des dispositions contractuelles viennent réguler ces risques mais elles ne peuvent empêcher l'hébergeur d'agir techniquement de façon malveillante. Une des parades à la consultation abusive consiste à chiffrer / crypter les données.

Un autre inconvénient vient des limites imposées sur le stockage ou la récupération des données : pour maîtriser l'usage de ses disques et de sa bande passante, un hébergeur peut limiter contractuellement son client à un volume de stockage ou de données consultées au-delà duquel il bloque l'accès aux données.

Ce qu'il faut retenir d'important dans l'utilisation de ce processus de sauvegarde en ligne sont les critères suivants :

1. Les données doivent êtres cryptées/chiffrées avant de remonter via Internet chez l'hébergeur. Ce qui induit que le prestataire ne peut pas exploiter les données du client par définition.
2. L'hébergeur se doit d'avoir deux copies de vos données, pour se prémunir aussi d'une panne de son côté. (Si possible sur des réseaux différents, des réseaux électriques différents, voir une infrastructure géographique différente). Ne pas oublier que si le client à une panne en même temps que le prestataire, la solution est caduque pour le client dans ce cas de figure.
3. L'hébergeur doit avoir vis à vis des professionnels une assurance "Responsabilité d'Exploitation" adéquate avec le service proposé, afin que le client dans un cas ultime "puisse être couvert."
4. Le tarif des solutions n'est pas le plus important, le plus important sont la mise à disposition des données, et la couverture du prestataire.

Sauvegarde en Pair à pair (P2P)

L'évolution des méthodes d'échange de fichier rendent depuis un certain temps possible la sauvegarde en mode "Pair à Pair". Cette technique s'appuie sur un service collaboratif ou chacun protège ses données sur les espaces de stockage des autres.

Les avantages sont multiples :

- minimiser le risque de perte et disposer d'une protection à distance répondant aux problèmes de vol, incendie, inondation;
- les espaces de stockage ne sont pas limités en taille;
- entièrement gratuit;
- une sauvegarde entièrement automatisée et périodique;
- L'inconvénient majeur de cette technique est qu'elle s'adresse uniquement aux particuliers mais ne répond pas aux besoins des entreprises; il faut veiller à ce que les données soient entièrement encryptées afin de les rendre illisibles sur les espaces de stockage des autres. Cette technique doit s'inscrire au sein de groupe de confiance.

Méthodes (Types) de sauvegarde les plus courantes

La méthode la plus simple est la sauvegarde complète ou totale (appelée aussi "full backup") ; elle consiste à copier toutes les données à sauvegarder que celles-ci soient récentes, anciennes, modifiées ou non.

Cette méthode est aussi la plus fiable mais elle est longue et très coûteuse en termes d'espace disque, ce qui empêche de l'utiliser en pratique pour toutes les sauvegardes à effectuer. Afin de gagner en rapidité et en temps de sauvegarde, il existe des méthodes qui procèdent à la sauvegarde des seules données modifiées et/ou ajoutées entre deux sauvegardes totales. On en recense deux :

- La sauvegarde différentielle
- La sauvegarde incrémentielle

La restauration d'un disque avec l'une de ces méthodes s'avère plus longue et plus fastidieuse puisqu'en plus de la restauration de la sauvegarde différentielle ou des sauvegardes incrémentielles, on doit également restaurer la dernière sauvegarde complète. Les fichiers supprimés entre-temps seront restaurés ou non (en fonction des fonctionnalités du logiciel de sauvegarde utilisé).

Afin de comprendre la différence entre les deux méthodes, nous prendrons l'exemple d'un plan de sauvegarde selon le cycle suivant :

- Une sauvegarde complète au jour J (dimanche soir par exemple)
- Une sauvegarde des fichiers modifiés ou nouveaux du jour J+1 au jour J+6 (du lundi soir au samedi soir inclus)
- Une sauvegarde complète au jour J+7 (dimanche soir suivant)

Mécanisme

Pour pouvoir différencier ces différentes méthodes de sauvegarde/archivage (complète, incrémentielle, différentielle), le mécanisme mis en place est l'utilisation d'un marqueur

d'archivage. Chaque fichier possède ce marqueur d'archivage, qui est positionné à "vrai" lorsque l'on crée ou modifie un fichier. On peut comprendre cette position comme "Je viens d'être modifié ou créé : je suis prêt à être archivé donc je positionne mon marqueur à vrai". Ce marqueur est appelé aussi attribut d'archivage (ou bit d'archivage). Sous Windows, cet attribut est modifiable et peut être visualisé par la commande ATTRIB (attribut A pour archive). Le système de sauvegarde peut aussi constituer une base de données contenant les définitions des fichiers et utiliser un marquage interne.

Sauvegarde complète

Lors d'une sauvegarde complète, on va remettre à "0" l'attribut du fichier pour mémoriser le fait que le fichier a été enregistré. Lorsque l'on travaille avec la date, on mémorise la date de la dernière sauvegarde de façon à pouvoir différencier les fichiers qui ont été sauvegardés des autres (date de dernière modification).

- Détail technique : lors d'une sauvegarde complète, tous les fichiers sont sauvegardés, indépendamment de la position du marqueur (vrai ou faux). Une fois le fichier archivé, celui-ci se voit attribuer la position de son marqueur (ou son bit) à "faux" (ou à "0").

Sauvegarde différentielle

La sauvegarde différentielle effectue une copie des fichiers créés ou modifiés depuis la dernière sauvegarde complète, quelles que soient les sauvegardes intermédiaires. En d'autres termes, la sauvegarde complète du jour J sert de référence pour identifier les fichiers créés, modifiés ou ajoutés et ainsi ne sauvegarder que ces derniers du jour J+1 au jour J+6.

La restauration faite à partir de ce type de sauvegarde nécessite la recopie sur disque de la dernière sauvegarde complète et de la sauvegarde différentielle la plus récente.

Avec notre exemple, si la restauration se porte sur un disque complet qui a été sauvegardé le jour J+2, on doit alors recopier sur disque la sauvegarde complète du jour J et la sauvegarde différentielle du jour J+2 afin d'avoir la dernière version des données.

Cependant lorsqu'il s'agit de la restauration d'un fichier ou d'un répertoire qui a été sauvegardé le jour J+2 seule la dernière sauvegarde, ici la différentielle, est utile.

- Détail technique : lors d'une sauvegarde différentielle, tous les fichiers dont le marqueur est à "vrai" sont sauvegardés. Une fois le fichier archivé, celui-ci garde la position de son marqueur tel qu'il l'avait avant la sauvegarde.

Sauvegarde incrémentale ou incrémentielle

Cette méthode consiste à sauvegarder les fichiers créés ou modifiés depuis la dernière sauvegarde quel que soit son type (complète, différentielle ou incrémentielle).

Exemple : une sauvegarde complète est réalisée le jour J. Le jour J+1, la sauvegarde incrémentielle est réalisée par référence au jour J. Le jour J+2, la sauvegarde incrémentielle est réalisée par référence au jour J+1. Et ainsi de suite.

Si la restauration se porte sur un disque complet qui a été sauvegardé le jour J+4, on doit alors recopier sur disque la sauvegarde du jour J et les sauvegardes incrémentielles des jours J+1, J+2, J+3 et J+4 afin d'obtenir la dernière version de la totalité des données.

Cependant lorsqu'il s'agit de la restauration d'un fichier ou d'un répertoire qui a été sauvegardé le jour J+3, seule la dernière sauvegarde, ici l'incrémentielle, est utile.

La sauvegarde incrémentale peut également porter sur les seuls octets modifiés des fichiers à sauvegarder. On parle alors de sauvegarde incrémentale octet. Cette méthode est celle qui permet d'optimiser le plus l'utilisation de la bande passante. Elle rend possible la sauvegarde de fichiers de plusieurs Gigaoctets, puisque seul un pourcentage minime du volume est transféré à chaque fois sur la plateforme de sauvegarde.

- Détail technique : lors d'une sauvegarde incrémentielle, tous les fichiers dont le marqueur est à "vrai" sont sauvegardés. Une fois le fichier archivé, celui-ci se voit attribué la position de son marqueur à "faux".

Sauvegarde, archivage et rétention

La rétention permet de faire la différence entre sauvegarde et archivage : la rétention est le temps pendant lequel la donnée sauvegardée est conservée intacte. Un travail de rétention courte est assimilé à un travail de sauvegarde classique : la donnée est protégée contre sa disparition/son altération. Un travail de rétention longue (une ou plusieurs années) est assimilé à un travail d'archivage et aura pour but de retrouver la donnée à une date précise, sur demande express.

Par exemple, une rétention de 4 semaines implique que l'instance des données sauvegardées à une date précise seront toujours disponibles jusqu'à 28 jours après leur sauvegarde. Après ces 28 jours, d'un point de vue logique, les données n'existent plus dans le système de sauvegarde et sont considérées comme introuvables. Physiquement, les pistes utilisées pour enregistrer cette sauvegarde peuvent être effacées.

Plus la rétention est longue et plus le nombre d'instance sauvegardé pour un même objet fichier ou dossier est important. Plus la rétention est longue et plus la sauvegarde tend vers un mécanisme d'archivage qui nécessitera un système de recherche et d'indexation approprié. Plus la rétention est longue et plus l'espace nécessaire pour stocker les travaux de sauvegarde sera important.

Formule de calcul de l'espace de sauvegarde nécessaire

Cette formule permet de dimensionner une librairie de sauvegarde (bande ou disque VTL).

Dans le cas d'une sauvegarde classique, c'est-à-dire sauvegarde totale le week-end (vendredi soir) et sauvegardes incrémentielles les autres jours ouvrés de la semaine, du lundi au jeudi (pas le vendredi) soit quatre jours :

- soit D l'espace de donnée utile à sauvegarder,
- soit R la rétention des travaux souhaité, exprimé en semaine,
- soit T le taux de modification par jour des fichiers de l'espace à sauvegarder,
- la formule suivante est obtenue : D x R + (D x T%) x 4 = capacité de sauvegarde.

Exemple : 100 Go au total à sauvegarder avec une rétention de 3 semaines et un taux de modification de 20% par jour donne 100 x 3 + (100 x 20%) x 4 = 380 Go. 380 Go seront nécessaires pour sauvegarder nos 100 Go de données avec une rétention de 3 semaines et une modification de 20% par jour.

Des innovations technologiques telles que les snapshots ou la déduplication permettent de réduire cette valeur d'une façon très intéressante.

Techniques complémentaires

La sauvegarde de données peut être réalisée en utilisant des techniques plus ou moins sophistiquées. La méthode la plus simple est de parcourir les répertoires et les fichiers d'un poste de travail ou d'un serveur, mais on se trouve vite limité par le nombre de fichiers et par le volume de données, qui ont un impact direct sur le temps de sauvegarde. Pour contourner ces limitations, plusieurs approches sont envisageables :

- compression des données sauvegardées, utilisé par la majorité des solutions de sauvegarde
- technique de snapshot: prise d'image instantanée d'un disque, en particulier dans un SAN (voir Gestion par volumes logiques)
- sauvegarde en mode bloc (protocole NDMP en particulier pour les NAS)
- technique de déduplication pour limiter le volume des sauvegardes en éliminant les doublons
- technique de déduplication à la source permettant de ne stocker qu'une seule fois un fichier, même si celui-ci a été dupliqué et renommé sur les postes sauvegardés, les doublons n'étant présents que dans les index
- une combinaison de ces différentes techniques

Notes
1. ↑ Traduction littérale du terme anglo-saxon on line qui signifie « connecté »

DOCUMENT 9

Alain Bastide, site interne Indexel.net,

"Six questions à se poser pour sécuriser ses données", 13 avril 2011

Les données informatiques sont indispensables au bon fonctionnement de votre entreprise. Etes-vous certain de les sauvegarder correctement et de leur appliquer une politique de sécurité adaptée ?

Le système d'information est vital pour le bon fonctionnement de l'entreprise. Pourtant, une société sur quatre ne protège pas correctement ses données (notre article : Perte de données, une entreprise sur quatre n'est pas protégée). Une récente étude réalisée par Iron Mountain auprès de 900 décideurs informatiques européens confirme cette situation. Elle révèle que seulement 30 % des PME conservent leurs bandes de sauvegarde sur un site distant. Comment s'assurer que vos données sont correctement sécurisées ? Voici six questions qui vous permettront de réaliser un audit et d'identifier les mesures correctives à mettre en œuvre.

1. Mes informations physiques et mes données sont-elles archivées en toute sécurité ?

Les informations doivent être stockées sur un autre site, à l'abri des fuites accidentelles et des sinistres (incendie, dégât des eaux, cambriolage). Si l'entreprise préfère les conserver sur son site, elle doit passer régulièrement en revue son dispositif de sécurité physique, ce qui peut poser des problèmes particuliers aux PME. Pour nombre d'entre elles, mieux vaut sans doute s'adresser à un tiers de confiance pour le stockage, la gestion et la destruction des données en conformité avec une législation de plus en plus complexe et stricte.

2. Quelle est la durée de conservation légale de mes données ?

En perpétuelle évolution, le cadre réglementaire international, européen et français impose des durées de conservation variables selon la nature des données. Déterminer quels documents doivent être conservés et pour combien de temps élimine le risque de les détruire trop tôt, par simple ignorance de la réglementation. Cette démarche permet également de réduire les coûts de stockage en ne conservant que les données essentielles.

3. Mon entreprise est-elle capable de récupérer rapidement ses données après un sinistre ?

En d'autres termes, quel est mon plan de reprise d'activité (PRA) après un sinistre informatique ? Quelles sont les procédures ? Ont-elles été testées ? Sont-elles fiables ? La sauvegarde n'est pas suffisante. Il faut s'assurer que les données sauvegardées pourront être réutilisées rapidement pour ne pas bloquer le bon fonctionnement de l'entreprise.

4. Mon entreprise dispose-t-elle d'une politique de sécurité ?

L'accès aux informations sensibles doit être minutieusement réglé et nécessite donc une politique particulière qui couvre tous les aspects, par exemple la sécurité dans les échanges de dossiers avec un prestataire de services externe, la sauvegarde et le chiffrement des informations ou encore l'authentification des salariés. Cela vaut également pour les informations sorties du site, par exemple par des collaborateurs travaillant à domicile. Le stockage, l'archivage, la gestion et la restauration des informations doivent être sécurisées. La méthode consistant à empiler des cartons dans des armoires ou sous des escaliers ne satisfait pas à ces critères.

5. Les utilisateurs sont-ils sensibilisés ?

Dans de nombreux cas, les pertes de données sont liées à une erreur humaine : absence de sauvegarde régulière, suppression d'un fichier qui n'a jamais été sauvegardé, perte d'une clé USB, etc. Les collaborateurs de l'entreprise doivent être conscients de la responsabilité qui leur incombe en matière de gestion des données sensibles. Il est par exemple important de bien dissocier les données confidentielles et les données publiques. Et la DSI doit leur fournir une procédure claire pour le stockage et la sauvegarde de leurs données.

6. Comment les périphériques mobiles sont-ils pris en compte ?

Entre les clés USB, les smartphones, ordinateurs portables et autres tablettes numériques, de nombreuses données sensibles de l'entreprise se promènent un peu partout dans le monde. La DSI doit donc évaluer les risques liés à ces équipements, tant en termes de perte ou de vol que de sauvegarde.

Formation : Sensibilisation Utilisateurs

Considérer l'utilisateur comme l'un des maillons faible de la chaine de Sécurité des SI peut paraître indélicat, et pourtant, les « erreurs humaines » par négligence ou par manque d'information représentent les menaces les plus courantes pesant sur les Systèmes d'Information.
Sensibiliser l'ensemble du personnel aux bonnes pratiques en matière de Sécurité est l'un des moyens les plus efficaces de diminuer les risques de compromission de votre Système d'Information.
A l'issue de cette formation, les utilisateurs seront responsabilisés et impliqués dans le respect de votre charte informatique.

Objectifs

Pour la Direction SI :

- Diminuer les risques liés à la sécurité en interne = renforcer sa sécurité globale
- Diminuer les risques d'intrusion, de vols ou pertes de données, de ruptures de service
- Former ses utilisateurs à la charte mise en place dans sa société

Pour le formé :

- Augmenter ses compétences en matière de sécurité : (re) connaître les menaces existantes,
- savoir réagir face à une attaque, changer son comportement
- Prendre conscience de son rôle dans la chaine de sécurité du SI
- Appréhender les bonnes pratiques et les règles de sécurité de base

Durée

Cette formation se déroule sur 1/2 journée ou 1 jour.
La présente formation aura lieu dans les locaux d'Openshere (Sainte-Marie) ou dans vos propres locaux.

Pré Requis

Aucun Pré-Requis

Public Visé

Ce cours s'adresse aux :

- Utilisateurs du SI
- Utilisateurs à « risques » : les nomades commerciaux, les V.I.P.
- Les décideurs dans les PME
- Les correspondants informatiques des PME

Contenu de la formation

Cette formation peut être adaptée en fonction de vos objectifs, de vos contraintes et de vos enjeux interne.

INTRODUCTION A LA SECURITE INFORMATIQUE

- Définition : qu'est-ce que la sécurité informatique ?
- Les chiffres

DEFINITION DU SYSTEME D'INFORMATION

- Architecture des ordinateurs
- Architecture des réseaux et Internet

- La notion de patrimoine informationnel

LES FONDAMENTAUX DE LA SECURITE INFORMATIQUE

- Les critères DICP, l'authentification
- Quelques définitions : menaces, vulnérabilités, risques,
- Principales Méthodologies de gestion de la sécurité

LES MENACES ET LES PROTECTIONS ACTUELLES

- Les applications à risque
- Les menaces en détail
- Les techniques de protection, leurs limites

LES MOTS DE PASSE

- Les attaques sur les mots de passe
- Créer un bon mot de passe

L'UTILISATEUR : UN DES MAILLONS DE LA CHAINE DE SECURITE DES SI

- Le social engineering ou l'art de la manipulation
- Les comportements à risque
- Les bons réflexes au quotidien
- Réagir face à un évènement
- Le cas des nomades

UNE UTILISATION ETHIQUE ET JURIDIQUEMENT CONFORME

- La charte d'entreprise et les responsabilités de chacun
- Vie privée, vie professionnelle
- L'usage raisonnable des biens de l'entreprise
- La CNIL

Ce texte est avant tout un code de bonne conduite. Il a pour objet de préciser la responsabilité des utilisateurs en accord avec la législation afin d'instaurer un usage correct des ressources informatiques et des services Internet, avec des règles minimales de courtoisie et de respect d'autrui.
Pour tout renseignement complémentaire, vous pouvez vous adresser au Directeur des Systèmes d'information

1. Définitions

On désignera de façon générale sous le terme " ressources informatiques ", les moyens informatiques ainsi que ceux auxquels il est possible d'accéder à distance, à partir du réseau administré par la Ville.

On désignera par " services Internet ", la mise à disposition par des serveurs locaux ou distants de moyens d'échanges et d'informations diverses : Web, messagerie, forum…

On désignera sous le terme " utilisateur ", les personnes ayant accès ou utilisant les ressources informatiques et services Internet.

On désignera sous le terme " Ville " les entités administratives de la Ville de D..

2. Accès aux ressources informatiques et services Internet

L'utilisation des ressources informatiques et l'usage des services Internet ainsi que du réseau pour y accéder ne sont autorisés que dans le cadre exclusif de l'activité professionnelle des utilisateurs conformément à la législation en vigueur.

Il faut noter que la capacité d'accéder à une information n'implique pas que l'accès soit effectivement autorisé.

L'utilisation des ressources informatiques partagées de la Ville et la connexion d'un équipement sur le réseau sont en outre soumises à autorisation. Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Ces autorisations peuvent être retirées à tout moment. Toute autorisation prend fin lors de la cessation même provisoire de l'activité professionnelle qui l'a justifiée.

La Ville pourra en outre prévoir des restrictions d'accès spécifiques à son organisation : filtrage d'accès sécurisé et filtrage des courriels.

3. Règles d'utilisation, de sécurité et de bon usage

Tout utilisateur est responsable de l'usage des ressources informatiques et du réseau auxquels il a accès. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale.

L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation ou leur détournement à des fins personnelles.

En particulier :

- il doit appliquer les recommandations de sécurité,
- il doit assurer la protection de ses informations et il est responsable des droits qu'il donne aux autres utilisateurs, il lui appartient de protéger ses données en utilisant les différents moyens de sauvegarde individuels ou mis à sa disposition,
- il doit signaler toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater,
- il doit suivre les règles en vigueur au sein de la Ville pour toute installation de logiciel,
- il choisit des mots de passe sûrs, gardés secrets et en aucun cas ne doit les communiquer à des tiers,

- il s'engage à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux, à travers des matériels dont il a l'usage,
- il ne doit pas utiliser ou essayer d'utiliser des comptes autres que le sien ou de masquer sa véritable identité,
- il ne doit pas tenter de lire, modifier, copier ou détruire des données autres que celles qui lui appartiennent en propre, directement ou indirectement. En particulier, il ne doit pas modifier le ou les fichiers contenant des informations comptables ou d'identification,
- il ne doit pas quitter son poste de travail ni ceux en libre-service sans se déconnecter en laissant des ressources ou services accessibles lors d'absence prolongée (rendez-vous extérieur, pause déjeuner…).

4. Conditions de confidentialité

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, et ceux qui sont publics ou partagés. En particulier, il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs et qui ne sont pas explicitement libres d'accès . (quand bien même ceux-ci ne les auraient pas explicitement protégées). Cette règle s'applique également aux conversations privées de type courrier électronique dont l'utilisateur n'est destinataire ni directement, ni en copie. Si, dans l'accomplissement de son travail, l'utilisateur est amené à constituer des fichiers tombant sous le coup de la loi Informatique et Libertés, il devra auparavant solliciter le Directeur Général des Services et le Directeur des systèmes d'informations, pour une demande à la CNIL (voir 9. Rappel des principales lois françaises) et en avoir reçu l'autorisation. Il est rappelé que cette autorisation n'est valable que pour le *traitement* défini dans la demande et pas pour le *fichier* lui-même.

5. Respect de la législation concernant les logiciels

Il est strictement interdit d'effectuer des copies de logiciels commerciaux pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle. Ces dernières ne peuvent être effectuées que par la Direction Informatique.

Par ailleurs l'utilisateur ne doit pas installer de logiciels à caractère ludique, ni contourner les restrictions d'utilisation d'un logiciel.

6. Préservation de l'intégrité des systèmes informatiques

L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes informatiques et des réseaux que ce soit par des manipulations anormales du matériel, ou par l'introduction de logiciels parasites connus sous le nom générique de virus.

7. Usage des services Internet (Web, messagerie, forum…)

L'utilisateur doit faire usage des services Internet dans le cadre exclusif de ses activités professionnelles et dans le respect de principes généraux et des règles propres aux divers sites qui les proposent ainsi que dans le respect de la législation en vigueur.

En particulier :

- il ne doit pas se connecter ou essayer de se connecter sur un serveur autrement que par les dispositions prévues par ce serveur ou sans y être autorisé par les responsables habilités,
- il ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède,
- il ne doit pas usurper l'identité d'une autre personne et il ne doit pas intercepter de communications entre tiers,
- il ne doit pas utiliser ces services pour proposer ou rendre accessible aux tiers des données et informations confidentielles ou contraires à la législation en vigueur,
- il doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques par courrier, forums de discussions…
- il n'émettra pas d'opinions personnelles étrangères à son activité professionnelle susceptibles de porter préjudice à la Ville,

- il doit s'imposer le respect des lois et notamment celles relatives aux publications à caractère injurieux, raciste, pornographique, diffamatoire.

Utilisation de la messagerie externe :

Une adresse internet du type xxxxx@ville-D.fr permet à certains services d'échanger des courriers électroniques. Cette adresse n'est utilisable que dans un cadre professionnel et l'utilisateur est prévenu qu'une copie de tout mail reçu est conservée automatiquement et devient consultable par l'autorité territoriale, représentée par le maire ou le directeur général des services. Par conséquent les courriers reçus par ce biais ne bénéficient pas de la protection de la correspondance privée.

La messagerie ne se substitue pas au courrier papier, notamment quand le contenu du message doit comporter le visa de l'autorité territoriale. Dans ce cas précisez à l'émetteur par messagerie qu'une réponse écrite lui sera envoyée, respectant le circuit de validation de la ville.

La messagerie est un outil de communication au même titre que le téléphone ou le courrier papier.

Chaque utilisateur doit veiller à prendre connaissance régulièrement du contenu de sa messagerie.

8. Analyse et contrôle de l'utilisation des ressources

Pour des nécessités de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable et notamment de la loi sur l'informatique et les libertés.

9. Rappel des principales lois françaises :

Il est rappelé que toute personne sur le sol français doit respecter la législation française en particulier dans le domaine de la sécurité informatique :

- la loi du 6/1/78 dite "informatique et liberté",(cf. http://www.cnil.fr/)
- la législation relative à la fraude informatique, (article 323-1 à 323-7 du Code pénal),(cf. http://www.legifrance.gouv.fr/citoyen/code.cgi)
- la législation relative à la propriété intellectuelle(cf. http://www.legifrance.gouv.fr/citoyen/code.cgi)
- la loi du 04/08/1994 relative à l'emploi de la langue française,(cf. http://www.culture.fr/culture/dglf/)
- la législation applicable en matière de cryptologie. (cf. http://www.telecom.gouv.fr/francais/activ/techno/crypto0698_1.htm)

10. Application

La présente charte s'applique à l'ensemble des agents de la ville, tous statuts confondus, et plus généralement à l'ensemble des personnes, permanentes ou temporaires, utilisant les moyens informatiques de la Ville ainsi que ceux auxquels il est possible d'accéder à distance directement ou en cascade à partir du réseau administré par la Ville.

Le Maire

Une prise en compte balbutiante des incidents de sécurité

Les collectivités ont encore, à l'instar des entreprises, une gestion peu organisée des incidents avec dans un peu plus d'un quart de celles interrogées une cellule dédiée (6 %) ou participant (20 %) à la gestion de ces incidents. Cela conduit 5 % des collectivités seulement à déposer plainte pour des incidents de sécurité alors que, par exemple, 38 % d'entre elles déclarent avoir subi des vols ou disparitions de matériels informatiques. Autre conséquence plus inquiétante encore : seules 7 % des collectivités déclarent effectuer une évaluation financière des incidents qu'elles subissent. On note sur ces points une forte disparité en fonction du type de collectivités. Ainsi régions et départements déclarent à 19 % avoir porté plainte pour des incidents de sécurité au cours de l'année.

Une vision contrastée des incidents

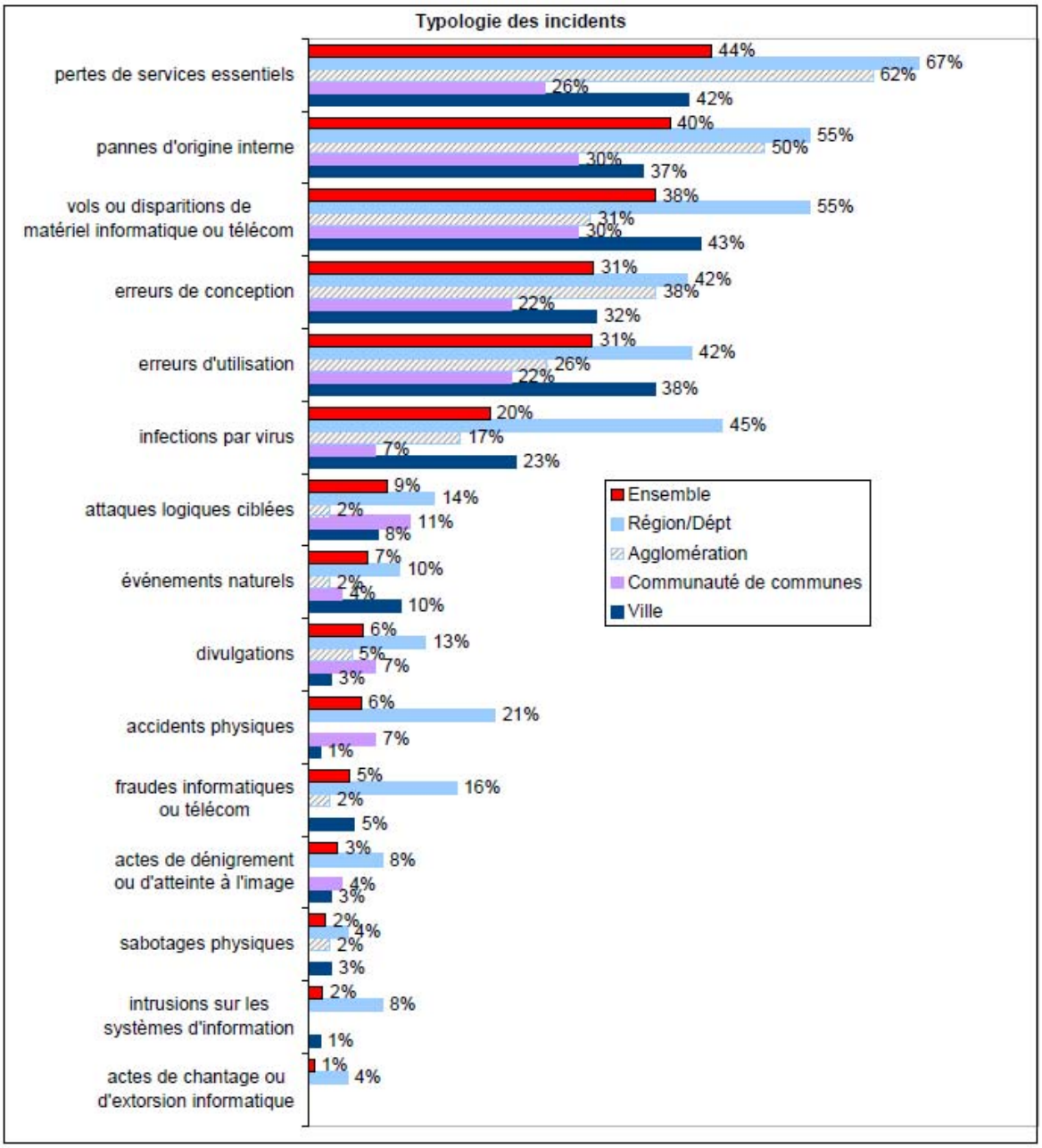


Figure 55 : typologie des incidents pour les collectivités

Les vols ou disparitions de matériels informatiques sont toujours une cause importante de sinistralité. Et les intrusions sur les systèmes d'information (1 à 8 %) et autres fraudes (2 à 16 %) atteignent des niveaux non négligeables.

Une collectivité sur 5 touchée par les virus

Parmi les 20 % ayant subi une infection virale, 13 % ont une origine interne et 24 % ont une origine indéterminée. De l'aveu même des RSSI, l'impact de ces infections n'est pas négligeable une fois sur cinq environ. Lorsque les collectivités sont victimes d'infections virales, elles le sont en moyenne 11 fois, certaines l'ayant été plus de 100 fois…

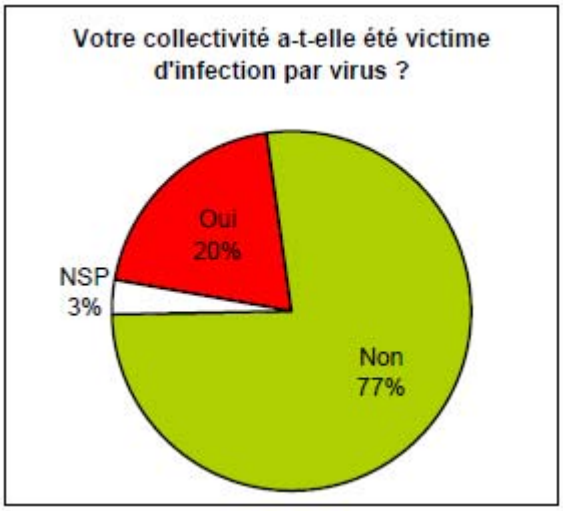


Figure 56 : taux d'infection par virus dans les collectivités

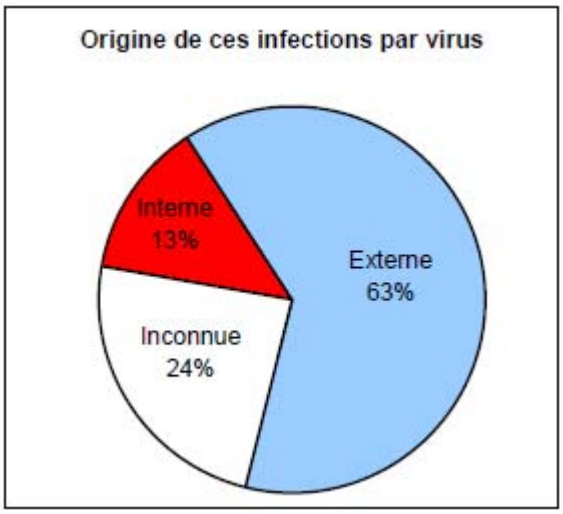


Figure 57 : origine des infections virales pour les collectivités

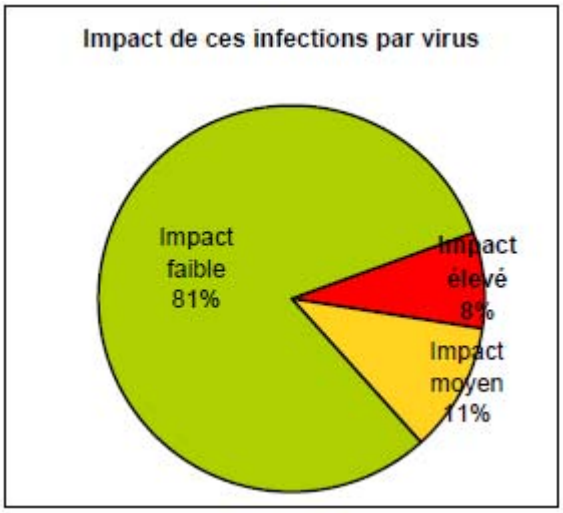


Figure 58 : impact des infections virales pour les collectivités

60 % des collectivités touchées …

Bien qu'il n'y ait pas de cellule de collecte et de traitement des incidents au sein des collectivités, plus d'un RSSI sur deux estime avoir subi des sinistres l'année passée. 7 % d'entre eux en recensent même plus de 50 et certains plus de… 400 !

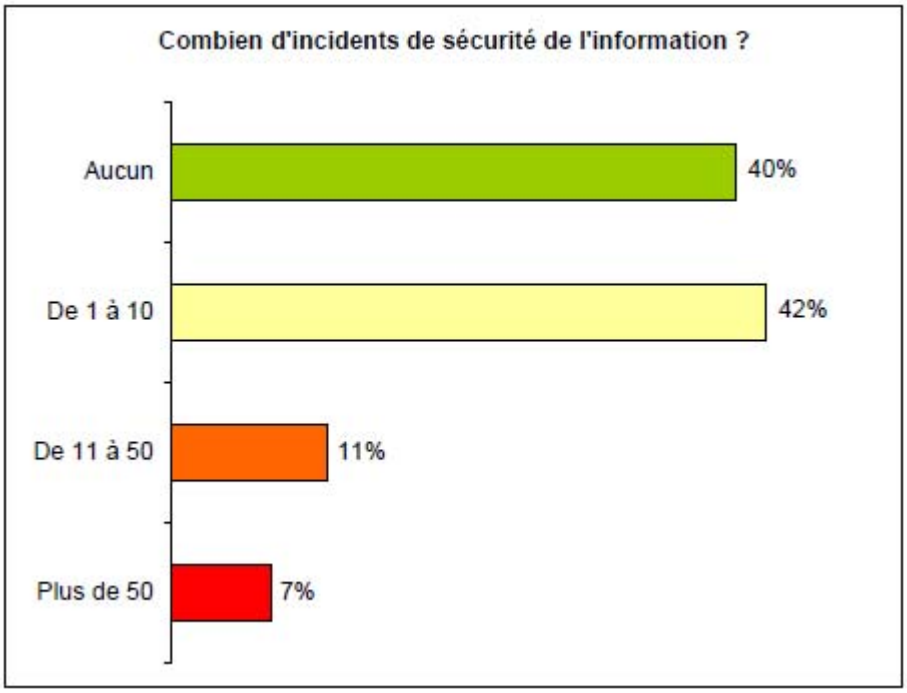


Figure 59 : nombre d'incidents de sécurité recensés l'an dernier par les collectivités

… pour un bilan peu flatteur

La conclusion est que si 60 % des collectivités confessent des incidents, 74 % ne sont pas organisées pour collecter et traiter ces événements, 95 % ne déposent jamais de plainte et 93 % n'évaluent même pas l'impact financier de ces incidents.

Les botnets

- *Un courriel contenant une pièce jointe est envoyé à l'ensemble des salariés d'une entreprise. Dans le lot, au moins l'un d'eux exécute la pièce jointe. Dés lors une connexion sortante est créée qui permet alors au pirate de disposer d'un accès à l'intérieur de l'entreprise pour y dérober des données sensibles.*

- *Une banque étrangère est attaquée. Plusieurs millions d'euros sont détournés. Les policiers identifient une adresse IP d'un artisan français. Une perquisition est effectuée, le titulaire de la ligne internet est placé en garde à vue. L'analyse informatique établira que la machine de l'intéressé est compromise et a servi de rebond pour réaliser l'attaque.*

Impacts judiciaires

Lorsque le maître du botnet passe à l'attaque, il se cache derrière les machines compromises. Ainsi seules les adresses IP des connexions en rapport avec celles-ci apparaissent au niveau du serveur cible. C'est donc les propriétaires d'ordinateurs « zombies » qui sont les premiers inquiétés (perquisition, garde à vue, etc …) et qui devront prouver leur innocence.

Glossaire :

Attaque par déni de service (denial of service attack) : attaque ayant pour but de rendre indisponibles un service ou l'accès à un service. (réseaux, sites internet, etc...)

Pare-feu (firewall) : logiciel ou matériel dont la fonction est de mettre en oeuvre la politique de sécurité du réseau d'une entreprise et des informations qui y transitent en cloisonnant notamment le réseau local et le réseau internet.

Définition :

Abréviation de roBOTs en réseaux (NET) . Réseaux d'ordinateurs détournés à l'insu de leurs propriétaires.
Les Botnets peuvent servir à paralyser un serveur, à diffuser du spam mais également à commettre des délis comme le vol de coordonnées bancaires et identitaires à grande échelle.

Impacts financiers

Paralyser un serveur d'entreprise par une attaque de type «déni de service» peut engendrer de grosses pertes financières. Ceci peut par exemple mettre hors service une interface de vente en ligne et ainsi, priver l'entreprise de nombreuses transactions financières, ou encore rendre inutilisable une boîte aux lettres et empêcher ainsi la société d'accéder à des informations importantes pour son fonctionnement.

Impacts sur l'image

Rendre le système d'information inutilisable ou faire l'objet d'une enquête judiciaire ternit inévitablement l'image de l'entreprise auprès des clients, fournisseurs, partenaires, opinions publiques … Il en découle bien souvent des rumeurs plus ou moins fondées qui au final font les affaires de la concurrence.

AVIS D'EXPERT :

Les botnets sont de plus en plus puissants et sont désormais l'œuvre des groupes mafieux qui cherchent sans cesse à accroître la puissance de frappe en contaminant un nombre toujours croissant de machines afin d'augmenter la capacité de leur réseau.

Préconisations

Il est nécessaire de sécuriser intelligemment l'entreprise. Pour cela il faut bien évidemment veiller à la mise à jour des différents logiciels afin de limiter les failles mais aussi se poser les bonnes questions pour mettre en place une politique de sécurité adaptée : Qu'avons-nous sécurisé? Par rapport à qui? Contre quoi? Pour combien de temps? Jusqu'à quel niveau d'attaque? La sécurité informatique ne peut se faire dans la généralité. Elle doit être adaptée au contexte.

LES POINTS CLES A RETENIR

Il est impératif d'activer la mise à jour automatique et de veiller à ce qu'elle soit appliquée à l'ensemble du parc informatique dans les délais les plus brefs.
Il est aussi nécessaire de définir les logiciels utiles et nécessaires en y mettant obligatoirement un anti virus et un firewall.
Le maillon faible reste les employés. Il faut les sensibiliser aux risques, à la richesse de l'information et au social engineering.

Les attaques touchent fréquemment les établissements financiers et les sites disposant d'une grosse activité sur le web (adossée à un fichier client souvent important).
La finalité des pirates est d'obtenir une rançon en échange du retour à la normal dans le trafic de la société visée.

DOCUMENT 14

Schéma : comment fonctionne le ver Conficker ?Microsoft sécurité, mise à jour 2010