La sécurité des réseaux informatiques

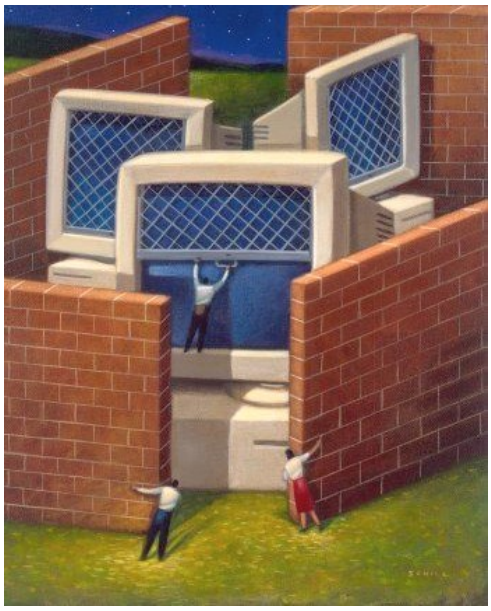
I. Communication en réseau : pourquoi protéger ses données ?

1. La menace grandit !
2. Un chef d'entreprise responsable de son système d'information
3. Le respect de la vie privée des salariés contre la sécurité des réseaux
4. La protection des données à caractère personnel, une obligation légale
5. Des impacts fonctionnels, financiers et structurels lourds de conséquences
6. Le respect des contrats et des partenaires commerciaux
7. L'intelligence économique : un trésor de guerre à protéger
8. La motivation des salariés en jeu
9. Un cadre juridique national peu convaincant pour les entreprises

II. Communication en réseau : comment protéger ses données ?

1. Avoir une connaissance précise des valeurs à protéger
2. Effectuer une veille informatique efficace
3. Connaître et gérer son matériel
4. Surveiller !
5. Changer les comportements humains
6. Mettre en place un système de protection complet et évolutif
7. Quelques solutions pour protéger son réseau « efficacement »
8. L'intervention de l'Etat par une politique nationale de sécurité

Lexique - Sites Internet - Bibliographie



La sécurité des réseaux informatiques

Ces dernières années, la mondialisation, notamment sous ses aspects économiques et financiers, a engendré des projets informatiques de dimension mondiale. On notera en particulier le passage informatique à l'an 2000 (Y2K), qui a nécessité la vérification et la conversion de 300 à 600 milliards de lignes de programmes potentiellement affectées dans le monde. En Europe, le chantier du passage à l'euro a représenté un coût sensiblement identique à celui du passage à l'an 2000 sur le périmètre européen. Or, si ces modifications ont eu au premier plan pour but de maintenir le fonctionnement des logiciels ou des systèmes d'exploitation, on ne peut écarter de ces objectifs le premier, celui de la protection des données.
Dans le cadre d'une concurrence exacerbée, l'intelligence économique est devenue une arme redoutable avec pour support tout désigné l'informatique.
Comment protéger efficacement ces données volatiles qui sont devenues si précieuses ?
La réponse paraît simple au regard des nombreuses solutions de protection proposées aux entreprises. Toutefois, l'inépuisable inventivité des hackers (pirates informatiques), la protection des libertés individuelles ou encore l'évolution fulgurante des technologies sont autant de murs qui se dressent face aux chefs d'entreprise.

I. Communication en réseau : pourquoi protéger ses données ?

Parler de « protection informatique » à un dirigeant, c'est tout de suite évoquer chez lui la notion de coût. Parler de « protection informatique » aux salariés et c'est le terme de « méfiance » voire de « défiance » qui est brandi tel un étendard.
Alors pourquoi protéger si cela est aussi pesant ? Tout simplement parce que les intérêts protégés (les données informatiques) ont une plus grande valeur.

La menace est-elle réelle ? La réponse est incontestablement positive !
Plus de la moitié des 3600 vulnérabilités affectant des logiciels découvertes en 2007 n'ont pas encore été corrigées en 2008 ! C'est l'une des conclusions du rapport annuel X-Force, publié par la branche Internet Security Systems d'IBM.
Ce qui est inquiétant c'est que ce constat peut être renouvelé chaque année !

1. La menace grandit !

Plus de 155 vulnérabilités sont déclarées par semaine. Le temps moyen entre la publication de la vulnérabilité et de son exploitation est de 5,6 jours. Le délai de survie d'un ordinateur sans correctif de sécurité et sans protection vis-à-vis d'Internet est en moyenne de 10 minutes !

Des chiffres qui font peur mais que l'on peut relativiser en constatant les efforts réalisés par les entreprises européennes pour se protéger. Vélizy-Villacoublay, le 30 janvier 2008 - Gunnebo, l'un des leaders mondiaux de systèmes et de services de sécurité intégrés, a sponsorisé le premier baromètre européen de la sécurité électronique réalisé par le Cabinet Concomitance. Selon ces résultats, on peut noter un fort taux d'équipement des entreprises européennes en matériels et logiciels de protection. Ainsi, plus de 90% des entreprises sondées ont installé des systèmes de détection d'intrusion ; plus de 80% ont également mis en place des solutions de contrôle d'accès dans leurs locaux. Les budgets consacrés à la sécurité électronique sont en augmentation sur 2007 et 2008. 44% des entreprises européennes sondées ont déclaré que leur budget en sécurité électronique était en augmentation sur 2007 et 2008, alors que 38% ont indiqué qu'il restera stable et seulement 8% d'entre elles ont annoncé le diminuer.

Alors quel est le véritable problème de cette menace ? C'est qu'elle a toujours un temps d'avance sur ceux qui la combattent !
La menace développe en permanence de nouveaux outils de guerre. Partant d'une étude sur les émanations acoustiques de nos claviers d'ordinateurs, trois chercheurs de l'université de Berkeley ont perfectionné la technique d'écoute pour déterminer nos mots de passe à partir du son émis par chaque touche. Grâce à cette méthode de piratage, 80% des mots de passe peuvent être trouvés ! Quelle parade ? Aucune pour le moment !

2. Un chef d'entreprise responsable de son système d'information

Dans la plupart des entreprises, le système d'information est placé sous la direction du chef d'entreprise. Il en est de même pour la sécurité des données. Mais qu'en est-il de sa responsabilité au niveau juridique et pénal ?

Le chef d'entreprise est responsable de la sécurité du système d'information. La Loi et la jurisprudence ont de plus en plus tendance à le confirmer. Nous sommes dans un système où, tout étonnant que cela puisse paraître, le chef d'entreprise peut être à la fois victime d'une attaque et responsable juridiquement. C'est probablement l'une des conséquences que l'on n'avait peut-être pas mesurée suite à l'avènement d'Internet dans notre société moderne.

Qu'est-ce qu'Internet si ce n'est l'interopérabilité des réseaux et des systèmes… Nous devenons tous responsables les uns des autres car nous sommes tous connectés les uns aux autres. A partir du moment où la sécurité du système d'information est défaillante, il est inutile de rechercher la responsabilité chez les autres.

Il y a quelques années, une affaire célèbre a opposé le site "kitetoi" et son journaliste et la société TATI. Il a été reproché au journaliste d'avoir frauduleusement accédé au système

d'information du grand magasin, ce qui est un délit classique du code pénal (art 323-1). La Cour d'appel de Paris a cependant relaxé le journaliste sur le motif que "le système d'information du grand magasin portait des déficiences sur le plan technique".

Qu'encourt un chef d'entreprise qui reconnaît que son système d'information a été "piraté" parce qu'il n'a rien fait en termes de protection ?
La responsabilité civile du dirigeant peut être engagée sur le fondement de l'article 1383 du Code civil : L'article 1383 du Code civil permet en effet d'engager la responsabilité civile d'un dirigeant pour des dommages causés à la société ou aux tiers du fait de sa négligence, voire de son imprudence, dès lors qu'il n'a pas mis en œuvre des mesures de sécurité raisonnables pour protéger le réseau contre des atteintes extérieures ou intérieures. Ainsi le chef d'entreprise pourrait voir sa responsabilité civile engagée si du fait de sa négligence, l'entreprise subissait une perte de données qui lui serait très dommageable (par exemple perte d'une donnée particulièrement stratégique ou diffusion d'une information confidentielle dont la diffusion prématurée peut désorganiser l'entreprise…).
Cependant, pour que sa responsabilité soit engagée sur ce fondement, le dirigeant doit tout de même faire preuve d'une incapacité avérée et répétée à prendre la moindre mesure de protection du système d'information de l'entreprise".

Quid de la responsabilité pénale ? C'est dans le cadre du respect de la vie privée des salariés étudié ci-dessous que cette responsabilité peut être par exemple engagée.

3. Le respect de la vie privée des salariés contre la sécurité des réseaux

De nombreuses affaires récentes ont mis en avant le problème du respect de la vie privée sur le lieu de travail au travers de l'utilisation parfois abusive de l'informatique et des réseaux.
En octobre 2001, la Cour de cassation avait estimé qu'un salarié français avait droit, même lors de son temps de travail et sur le lieu professionnel, au respect de sa vie privée, et que celui-là impliquait en particulier le secret des correspondances par e-mail. Six ans plus tard, une décision de la Cour de cassation vient de nouveau confirmer ce premier arrêt fondateur dit « arrêt Nikon ».

Dans une affaire opposant la société The Phone House à un ancien salarié, Christopher B., licencié pour faute grave en novembre 2002, la chambre sociale de la Cour de cassation a rappelé en 2007 *« qu'il n'appartient pas à l'employeur de prendre connaissance des messages personnels émis ou reçus grâce à l'outil informatique mis à la disposition du salarié pour son travail »*.

En accordant ce droit aux salariés, la jurisprudence sait-elle qu'elle ouvre ainsi une brèche importante dans la sécurité des réseaux informatiques ? En effet, si un dossier personnel peut contenir des correspondances personnelles sans danger, il peut également renfermer des logiciels malveillants téléchargés par le salarié. Lorsque l'on sait qu'une simple image peut inclure un virus incorporé de manière invisible... !
Ce dossier « personnel » devient ainsi pour le responsable informatique et le chef d'entreprise un véritable nid à problèmes.

4. La protection des données à caractère personnel, une obligation légale

A l'origine, internet servait principalement à relier des chercheurs en informatique. La circulation des documents ne posait donc aucun problème de confidentialité et les données étaient acheminées « en clair » sur le réseau. Mais, l'ouverture d'internet à un usage commercial a modifié les comportements. Des informations confidentielles circulant sur les liaisons, la sécurité des communications est devenue une préoccupation importante.

La facilité des intrusions ou divulgations de données à caractère personnel est apparue comme une menace pour la vie privée, les libertés individuelles et publiques. La question est aujourd'hui particulièrement préoccupante du fait du développement du commerce électronique qui se fonde notamment sur un "marché" des données personnelles : celles-ci sont en effet des outils de marketing permettant au commerçant de fidéliser son client en lui proposant un service sur mesure déduit de l'analyse de son comportement sur le réseau. Ainsi, les annonceurs publicitaires ont recours à des logiciels espions, installés sur l'ordinateur à l'insu de l'utilisateur, qui collectent des informations sur l'internaute ou ses habitudes de connexion.

Un autre phénomène mettant en danger la protection des données personnelles des internautes se développe actuellement : le phishing ou hameçonnage. Il s'agit d'un courrier électronique qui persuade l'utilisateur de révéler des données personnelles sensibles par usurpation d'identité en imitant un site internet censé représenter une véritable société. Le courrier électronique non sollicité a donc cessé d'être une simple nuisance et devient peu à peu une activité de nature frauduleuse. En effet, les "polluposteurs" louent ou vendent désormais à des sociétés, aux fins de prospection, les listes d'adresses électroniques qu'ils ont récoltées.

Du point de vue législatif, la lutte contre la collecte et le traitement déloyaux de données à caractère personnel débute avec l'adoption par la France, de la "loi relative à l'informatique, aux fichiers et aux libertés" du 6 janvier 1978, qui institue la Commission nationale de l'informatique et des libertés **(**CNIL**),** autorité chargée de veiller à la protection des données personnelles et de la vie privée.

En 1981, le Conseil de l'Europe a élaboré la "*Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*" qui reste à ce jour, dans ce domaine, le seul instrument juridique contraignant sur le plan international, à vocation universelle, ouverte donc à l'adhésion de tout pays y compris non membre du Conseil de l'Europe. Cette Convention définit un certain nombre de principes pour que les données soient collectées et utilisées de façon loyale et licite. Ainsi, elles ne peuvent être collectées que dans un but précis et ne peuvent être utilisées de manière incompatible avec ce but ; elles doivent être exactes, proportionnées à cet objectif et conservées uniquement pendant le délai nécessaire à sa réalisation. Le texte établit, en outre, le droit d'accès et de rectification de la personne concernée et exige une protection spéciale pour les données sensibles (l'appartenance religieuse, les opinions politiques,les données génétiques ou médicales…).

Dans le droit fil de cette Convention du Conseil de l'Europe, l'Union européenne a adopté en octobre 1995 la directive 95/46/CE qui constitue le texte de référence, au niveau européen, en matière de protection des données à caractère personnel. Celle-ci met en place un cadre réglementaire visant à établir un équilibre entre un niveau élevé de protection de la vie privée des personnes et la libre circulation des données à caractère personnel au sein de l'Union européenne.

5. Des impacts fonctionnels, financiers et structurels lourds de conséquences

Au niveau fonctionnel, l'entreprise peut subir une perte de crédibilité, d'exploitation (indisponibilité des outils), de compétitivité (vol d'informations), de savoir faire (destruction de données).
Par exemple, une société de sondage pour la télévision a subi le vol d'un fichier contenant le profil psychologique des sondés. Elle a du verser 3 millions d'euros de dommages et intérêts et, quelques temps plus tard, on a assisté à sa fermeture.

Au niveau financier, l'entreprise peut endurer des pertes de valorisation boursière, des pertes d'exploitation, des pertes de compétitivité ou enfin des extorsions ou détournements de fonds.

Ainsi, par exemple, une banque américaine a du verser une rançon de 10 millions de dollars lors d'un chantage à la destruction de données sensibles obtenues frauduleusement par un pirate informatique.

Autre exemple, le vol d'un cœur de métier a causé un manque à gagner majeur pour un éditeur de logiciels suite à la mise en circulation de versions pirates.

Enfin, dernier exemple au niveau financier, le vol d'argent auprès de banques en ligne a été plusieurs fois mentionné à la Une des journaux. Ainsi, en 2006, le Guardian rapporte que les banques françaises ont été victimes de multiples vols. Des pirates russes auraient pillé plus d'un million d'euros sur des comptes français, en piégeant la victime par un mail vérolé. Selon un expert en sécurité, ces vols auraient pu être évités par l'utilisation d'un antivirus mis à jour !

Au niveau structurel, l'entreprise peut subir une perte de confiance interne et externe dans l'entreprise.
Ainsi, selon un article de Christophe GUILLEMIN publié le 28 janvier 2008 sur le site zdnet.fr (Source : http://www.zdnet.fr/actualites/informatique/0,39040745,39377868,00.htm), « *Jérôme Kerviel aurait profité des défaillances de la politique de sécurité informatique. Le trader à l'origine de la fraude record de 5 milliards d'euros aurait simplement exploité les lacunes de la politique de sécurité de la Société générale. Des identifiants et mots de passe permettant l'accès à des applications sensibles n'étaient pas changés régulièrement !* »
Comment confier son argent à une banque qui ne possède pas un système de protection informatique performant ? Sans vouloir fustiger la Société Générale, c'est sans nul doute la question que se pose aujourd'hui le client lambda avant d'ouvrir un compte auprès de cette société. Suite à cette affaire, la troisième banque française dévoile une perte record de 7 milliards d'euros, dont 5 milliards attribués aux agissements frauduleux du trader.

6. Le respect des contrats et des partenaires commerciaux

Si je suis sous traitant que se passe-t-il s'il y a une perte d'informations sur les processus industriels ?
Dans le cadre des franchises, le savoir-faire implique une habileté manuelle et/ou intellectuelle acquise par le franchisé. Pour pouvoir être protégé, il doit être identifiable, avoir une valeur marchande mais surtout il lui faut rester secret !

Sans aller jusqu'à parler des cas où le secret défense est en cause, on perçoit aisément les situations dans lesquelles certaines entreprises se voient contraintes à un secret et donc à une protection renforcée des données.

Dans un contrat, le « secret commercial », correspond à des éléments que l'entreprise considère comme confidentiels. En français le mot « secret », traduisant que la chose est cachée et que son détenteur ne doit pas divulguer, le mot « commercial » traduisant son caractère économique.

Le « know-how » ou « savoir-faire » correspond à des procédés ou tours de main mis au point par un fabricant et ignorés des autres, conservés secrets et produisant des effets économiques. L'étendue de cette obligation de confidentialité est généralement la plus large possible mais elle peut faire l'objet de précisions. Dans un « accord de collaboration », la stipulation explicite d'une « clause confidentialité » est toujours très générale et il est parfois spécifié dans les contrats internationaux l'emploi du terme « informations du propriétaire», souvent couplé avec « confidentielles». Dans d'autres contrats internationaux cette « clause confidentialité » est parfois rédigée sous la forme de « clause d'exclusivité », « clause d'informations exclusives » ou « informations privatives ou protégeables ».

Dans un règlement de 1996, la Commission européenne a créé les « accords de licence sur l'information technique non protégée par des brevets (par exemple, descriptifs de procédés de fabrication, recettes, formules, modèles ou dessins), appelés communément "savoir–faire" » - Il est donc souhaitable de prévoir des clauses de protection, en limitant l'accès à l'information entreposée dans un endroit sûr.

Des sanctions existent (*pour divulgation de secret de fabrique - Code pénal, art.418*) et font peser sur les chefs d'entreprise une lourde responsabilité sur un domaine qu'ils ne maîtrisent pas toujours et qu'ils se contentent de sous-traiter auprès de sociétés spécialisées dans la sécurité informatique.

7. L'intelligence économique : un trésor de guerre à protéger

Voir l'article d'Anne-Gaëlle SAIAH sur « l'intelligence économique » publié sur le site du CREG : http://www.creg.ac-versailles.fr/article.php3?id_article=205

L'information est devenue une ressource stratégique pour les acteurs publics et privés. La difficulté n'est plus de l'obtenir mais de la gérer et de la protéger car ce sont ces deux dimensions qui en font un avantage compétitif et qui font de l'intelligence économique un outil stratégique indispensable.

Ces remarques évoquent aussitôt l'affaire de la jeune stagiaire poursuivie par l'équipementier français Valeo pour s'être emparée de fichiers informatiques confidentiels entre février et avril 2005. Cette dernière a été finalement condamnée par le tribunal correctionnel de Versailles à un an de prison dont deux mois fermes.

Mais ces vols de données sont-ils toujours établis ou peuvent-ils passer inaperçus ?

8. La motivation des salariés en jeu

Un salarié travaille d'autant plus sereinement s'il sait que son travail (donc tous ses efforts) ne risque pas d'être anéanti (ou volé) en quelques secondes par une faille du système de protection du réseau.

A l'inverse, il faut faire attention à ce que la lourdeur de certaines manipulations engagées par un processus de protection mal pensé n'occasionne pas l'effet inverse. Ainsi, des mots de passe trop souvent demandés, des gestes répétitifs de contrôle exigés… sont autant de pertes de temps et de concentration qui peuvent devenir exaspérants. Le regard trop souvent désabusé porté par les salariés sur ces systèmes de protection résulte souvent d'un manque d'implication réelle et de compréhension.

9. Un cadre juridique national peu convaincant pour les entreprises

Tout d'abord, les malfaiteurs sont difficilement identifiables car ils agissent à distance, à travers des relais. Si les attaques sont souvent transfrontalières, les lois ne le sont pas.
Ensuite, la lenteur de la coopération judiciaire inter Etats s'ajoute aux différences de législations nationales.
Ainsi, l'impunité reste très souvent de fait.
Enfin, il est difficile de prouver l'effraction réelle. Seule la mise en place d'une sécurité forte peut conduire à prouver le vol et les pertes engendrées.
Toutefois, on ne peut remettre en doute la volonté du pouvoir politique de mettre en place des systèmes globaux de communication et d'information, d'alerte et de recommandations (pour preuve, l'ouverture du site gouvernemental pour favoriser la sécurité des systèmes d'information : http://www.ssi.gouv.fr/fr/index.html - ou encore, le portail gouvernemental de la sécurité informatique : http://www.securite-informatique.gouv.fr/)
Enfin, la loi Godfrain du 5 janvier 1988 se présente comme la pierre angulaire d'une législation très répressive contre la fraude informatique.

II. Communication en réseau : comment protéger ses données ?

Le premier « document » chiffré connu remonte à l'Antiquité. Il s'agit d'une tablette d'argile, retrouvée en Irak, et datant du XVI^{e} siècle av. J.-C. Un potier y avait gravé sa recette secrète en supprimant des consonnes et en modifiant l'orthographe des mots. Ainsi, depuis toujours, l'Homme a cherché à protéger ses données…
Aujourd'hui, les exigences de sécurité des systèmes d'information sont analysées avec l'échelle « *Evaluation Assurance Level* ». Pour les applications civiles, les exigences de sécurité ne dépassent en général pas le niveau EAL 4+. Pour les applications militaires, les exigences de sécurité vont des EAL 5 à 7.
Quelles sont les valeurs à protéger ? Quels moyens techniques encouragent cette protection ? Enfin, sont-ils correctement utilisés ? Ce sont les questions auxquelles nous allons répondre maintenant.

1. Avoir une connaissance précise des valeurs à protéger

Pour sécuriser les données sensibles, il faut tout d'abord avoir conscience des actifs de l'entreprise à protéger, et de leur valeur.

Différentes classifications des actifs existent, sans qu'il y ait de normalisation de tous les types d'actifs.
Une liste est proposée par la norme ISO 13335-1 (concepts et modèles de sécurité informatique) : personnes, capacité à fournir un produit, un service, actifs physiques, informations / données (structurées ou non), actifs intangibles.

Le modèle d'intelligence économique considère que l'enrichissement et la protection du patrimoine informationnel regroupent les points clés suivants :

- L'éthique (la protection de la vie privée et des données individuelles, l'application d'une déontologie dans le recueil d'informations et les pratiques d'influence, l'application d'une rigueur d'ontologique dans la sous-traitance d'information et de l'influence)

- Les connaissances et les compétences (l'identification et l'évaluation des connaissances et des compétences, la protection (droit, propriété intellectuelle…), la maîtrise des TIC)

- La création de valeur, avec plusieurs types de valeurs : (actionnaire, client, personnel, collectivité, partenaires).

- L'image (perception, évaluation, promotion)

Chaque entreprise cherchera donc à lister ces éléments correspondant à une richesse (un avantage stratégique) plus ou moins importante et, en fonction de ce niveau de richesse, installera un système de protection adapté.

2. Effectuer une veille informatique efficace

La veille informatique est un concept qui consiste à se tenir au courant des avancées technologiques dans le domaine de l'informatique afin d'anticiper les futurs besoins.

Le problème rencontré par cette veille est la complexité de sa gestion du fait des nombreux éléments qui la composent.

Tout d'abord, au niveau de l'évolution technologique. L'entreprise doit se tenir au courant des nouvelles composantes physiques et logicielles du réseau informatique (systèmes d'exploitation, serveurs, firewalls, routeurs, applications, clients, bureautique, bases de données ... plus de 20 000 produits édités par 7 000 constructeurs sont à surveiller !)
D'autre part, et nous l'avons vu dans la partie précédente (*I. 1. La menace grandit !*), la veille doit également porter sur les risques informatiques (nouveaux virus et autres programmes malveillants).

La plupart du temps les entreprises sous-traitent ces tâches fastidieuses. Mais peut se poser alors le problème de l'indépendance et de la fiabilité de ces sociétés de veille. Ne seraient-elles pas tentées d'exagérer les problèmes afin de gonfler leurs activités ?

Il n'en demeure pas moins que cette veille est indispensable surtout dans un contexte d'économie fortement concurrentielle où chaque problème peut être vécu comme une menace importante.

3. Connaître et gérer son matériel

Sécuriser son réseau informatique signifie également connaître son matériel et se préoccuper de sa gestion (achat, entretien, renouvellement).

Connaître son matériel…

Tout d'abord, connaître son matériel signifie au moment de l'achat d'avoir à l'esprit les éléments attendus tant au niveau des capacités que du suivi (SAV performant : garantie avec intervention sur site, remplacement dans les 24 h du PC défectueux,…)
Ensuite, il s'agit de rentabiliser ce travail effectué au niveau de l'achat en proposant aux salariés une formation afin de présenter les capacités de ce nouveau matériel et la procédure à suivre en cas de problème.

Gérer son matériel…

Sur le plan de la gestion, cette phase est également primordiale si l'on souhaite un système pérenne. On parle alors ici des mises à jour régulières à effectuer sur le système d'exploitation ou les logiciels tels que l'antivirus, les « nettoyages » de disques durs, les défragmentations…

Cette gestion est également à réaliser au niveau du recensement des unités. En effet, on ne peut tolérer le vol ou la perte d'ordinateurs qui contiennent des informations importantes. Ce

problème est d'ailleurs rendu complexe pour deux raisons : premièrement, la gestion des ordinateurs portables ou PDA qui sont souvent « prêtés » aux salariés et rapportés à leur domicile.
Selon une enquête menée en 2007 auprès de 2 000 chauffeurs de taxis à travers onze grandes villes, des milliers de téléphones portables, assistants personnels, ordinateurs portables et clés USB sont oubliés dans les taxis chaque jour.
Par exemple, sur les six derniers mois seulement, les Londoniens ont oublié 54 874 téléphones portables (soit plus de 2 par taxis), 4 718 assistants personnels ou Pocket PC, 3 179 ordinateurs portables et 923 clés USB à l'arrière des taxis... et ces chiffres ne concernent que les terminaux ayant fait l'objet d'une déclaration de perte !
Londres n'est pas un cas isolé en matière de voyageurs « distraits ». Il semblerait que les terminaux mobiles connaissent le même destin affligeant à Sydney, Bombay, Stockholm, San Francisco, Washington, Helsinki, Francfort, Berlin, Munich et Oslo.

Deuxièmement, afin de réduire la fracture numérique, la loi de finance 2008 inclue un amendement proposé par le Sénat sur le don d'ordinateurs amortis aux salariés. On imagine le travail complémentaire mais surtout les risques supplémentaires que cela implique !

Renouveler son matériel…

Les cycles de renouvellement des ordinateurs étant de plus en plus courts, ceux-ci se trouvent régulièrement recyclés mais sans que les données, souvent confidentielles, qui y sont stockées soient réellement effacées. Lors du renouvellement des parcs informatiques, il est primordial de placer la sécurité en tête des priorités. Une étude réalisée par le leader de la récupération de données démontre que seulement 18% des professionnels informatiques utilisent des outils dédiés à la suppression de données. Or, les entreprises risquent de subir des coûts préjudiciables si elles ne mettent pas en place des procédures d'effacement de données avant de céder leur ancien matériel informatique. En effet, le risque majeur est de livrer des informations confidentielles lors du recyclage ou lors de dons de leurs équipements informatiques. Les RSSI doivent s'assurer que les données sont réellement supprimées en utilisant un produit dédié. Il incombe également aux DSI et aux RSSI de sensibiliser les différentes entités de l'entreprise sur l'importance de la sécurité des données et sur les bonnes pratiques à suivre pour supprimer des fichiers. C'est uniquement quand l'ensemble du personnel sera familiarisé avec ces procédures que les données critiques de l'entreprise seront en sécurité.

Dans ce domaine, il subsiste un certain nombre d'idées reçues, à la fois de la part des utilisateurs, ce qui peut se comprendre, mais aussi de la part des professionnels de la sécurité, ce qui est moins compréhensible. Ainsi, l'effacement banal des fichiers n'est pas suffisant. Le bouton « Supprimer » ne fait que mettre à jour une table qui indique au système d'exploitation que le fichier a été effacé. Bien que l'utilisateur ne puisse pas accéder au fichier, le contenu entier du fichier est toujours présent, cela signifie que n'importe qui disposant de connaissances techniques pourrait les rechercher si l'ordinateur échouait entre de mauvaises mains.
De même, beaucoup d'utilisateurs croient que le reformatage de leur disque suffit à effacer les anciennes données, ce n'est pas le cas. Tout comme pour l'effacement, le formatage met à jour des tables indiquant que tous les fichiers et catalogues ont été supprimés, mais il n'efface pas physiquement les données sur le support de stockage !

4. Surveiller !

La surveillance est la réaction naturelle impliquée par la peur de la cybercriminalité. Les méthodes sont nombreuses et les entreprises qui proposent ces services rivalisent d'ingéniosité pour étoffer leurs offres.

La traçabilité des documents dématérialisés est l'une de ces méthodes. Elle permet très simplement de savoir à tout moment où se trouve un document, d'où il vient et quels sont les acteurs qui ont pu le lire, le modifier, l'imprimer… Cette procédure de surveillance peut se révéler intéressante dans le cadre d'une malveillance en apportant la preuve de la responsabilité de chacun dans le processus d'acheminement de l'information qui peut parfois être long et complexe.

Les enregistreur de frappes qui ont été à l'origine conçu par des « pirates informatiques » pour soutirer des informations sont désormais des outils de surveillance de plus en plus convoités par les chefs d'entreprise désireux de tout savoir sur l'activité de leur salarié.

La vidéosurveillance a pris une ampleur incroyable dans le prolongement des politiques sécuritaires pour voir aujourd'hui fleurir plus de 20.000 caméras dans les rues. Pourquoi ce qui fonctionne dans la rue ne fonctionnerait-il pas dans les entreprises ? Encadré par le droit (*code du travail - article L 432-2-1 : le comité d'entreprise doit être informé et consulté préalablement à la décision de mise en œuvre des caméras dans la mesure où elles permettent un contrôle de l'activité des salariés. - article L 121-8 : l'employeur ne peut mettre en œuvre un tel système de contrôle du salarié sans l'en informer préalablement*), ces systèmes permettent une sécurisation accrue et sont donc de plus en plus utilisés par les chefs d'entreprise.

Le badgeage et la biométrie existent depuis longtemps mais la baisse du prix de ces technologies, leur facilité de fonctionnement et la sécurité qu'elles peuvent apporter séduisent de plus en plus de chefs d'entreprise. Ces deux technologies permettent de surveiller les entrées et sorties de la société avec des informations précises sur les lieux d'entrée et de sortie et sur les horaires.

La géolocalisation des salariés est enfin le système le plus récemment mis en place par les entreprises pour surveiller leurs salariés et donc la possibilité de fuite d'informations. La CNIL s'est prononcée positivement sur ce sujet en posant bien évidemment un cadre à cette utilisation : http://www.cnil.fr/fileadmin/documents/approfondir/dossier/geolocalisation/Guide-geolocalisation.pdf
Au départ, cette surveillance ne concernait que les GPS des véhicules de sociétés lors des déplacements professionnels. Mais, jusqu'où cette « traque » peut-elle aller ? La société Autodesk propose déjà depuis 2004 un logiciel de suivi des salariés en temps réel grâce une localisation de leur téléphone portable : http://usa.autodesk.com/adsk/servlet/item?siteID=123112&id=6128682

5. Changer les comportements humains

La plupart des problèmes de sécurité observés dans les entreprises révèlent une responsabilité importante des utilisateurs (les salariés). La menace provient donc souvent de l'intérieur ! Afin de limiter les effets négatifs de ces comportements, les entreprises doivent mettre en place des observations (enquêtes) et réagir suite aux résultats obtenus par des formations.

1er exemple : l'utilisation des mots de passe

Le spécialiste de la sécurité des données Safenet vient de publier une étude sur l'utilisation des mots de passe au sein des entreprises. Elle est le résultat d'enquêtes menées en France, en Allemagne, au Royaume-Uni et aux Etats-Unis auprès de 67 000 personnes.
Selon cette étude, les entreprises prennent peu à peu conscience de l'importance de renforcer la qualité des mots de passe. Pourtant, l'augmentation de la longueur et la complexification des mots de passe ne sont pas toujours positives. Selon l'étude de SafeNet, 47 % des personnes interrogées ont de cinq à dix mots de passe différents pour accéder aux applications de leur entreprise. Avec des mots de passe de plus en plus longs, compliqués et renouvelés plus souvent, les risques en termes d'utilisation sont accrus : les utilisateurs sont en effet souvent amenés à les noter sur un papier ou les oublient tout simplement.
En France, SafeNet a constaté une augmentation des utilisateurs qui notent leurs mots de passe. Ainsi, dans une entreprise de 1000 personnes, 500 écrivent les mots de passe et 350 le communiquent à autrui **!**
Comme nous venons de le voir, un mot de passe long peut être difficile à retenir, et sera souvent inscrit sur un bout de papier à côté du poste, ce qui pourrait compromettre la sécurité de celui-ci dans un environnement partagé. Il faut donc trouver des moyens mnémotechniques pour fabriquer et retenir facilement de tels mots de passe :

- Phonétique : "J'ai acheté 3 CD pour cent euros cet après-midi" : ght3CD%E7am ;
- Méthode des premières lettres : "Un tiens vaut mieux que deux tu l'auras" : 1tvmQ2tl'A.

Quelques recommandations :

- Avoir des mots de passe de 10 caractères minimum.
- Utiliser des caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux).
- Ne pas utiliser de mot de passe ayant un lien avec soi (noms, dates de naissance…).
- Le même mot de passe ne doit pas être utilisé pour des accès différents.
- Changer de mot de passe régulièrement.
- En règle générale, ne pas configurer les logiciels pour qu'ils retiennent les mots de passe.
- Éviter de stocker ses mots de passe dans un fichier ou lieu proche de l'ordinateur si celui-ci est accessible par d'autres personnes.
- Si possible, limiter le nombre de tentatives d'accès.

2ème exemple : une charte informatique souvent transgressée

Une enquête menée auprès des salariés américains par l'organisation indépendante ISACA, révèle que plus d'un tiers (35%) des employés ont déjà transgressé les politiques informatiques de leur entreprise au moins une fois, et que près d'un sixième (15%) ont déjà utilisé le partage de fichiers P2P (peer-to-peer) au moins une fois sur leur lieu de travail, ouvrant ainsi la porte à de graves failles de sécurité et exposant aux risques des informations personnelles et professionnelles sensibles. La plupart des employés pensent à tort que ces comportements n'apportent que peu, voire pas de risque du tout, à leur entreprise.

3ème exemple : Quand l'entreprise s'expose elle-même au risque

Malgré des contrôles accrus et des risques légaux ainsi que techniques toujours plus élevés pour les responsables, le piratage de logiciels est aussi développé dans les entreprises que chez les particuliers.
Le bilan des contrôles réalisés en 2005 par la Business Software Alliance (BSA), l'association de lutte contre le piratage logiciel, révèle que la France, sans accéder aux sommets atteints par la Chine, se situe dans le peloton de tête des pays où le piratage est le plus développé : **71,1 %**

des logiciels utilisés dans les entreprises françaises contrôlées sont des copies illégales, pour une estimation de 47 % en moyenne. Si le manque à gagner pour l'économie du logiciel (3,19 milliards de dollars uniquement en France) ne semble pas un argument capable de convaincre les chefs d'entreprise de rentrer dans la légalité, les risques juridiques et techniques encourus devraient les inciter à obtenir les précieuses licences. Les sociétés prises en flagrant délit de piratage ont ainsi dû payer en 2005 une amende de moyenne 45 000 euros, amende qui peut atteindre 1,5 million d'euros dans les cas les plus graves, assortis d'une peine de trois ans de prison.

6. Mettre en place un système de protection complet et évolutif

Un système complet…

La première raison qui explique une intrusion dans un système informatique est la présence d'une petite faille. Une entreprise qui se contente de mettre en place un système de sécurité reposant sur une seule technologie ou un seul logiciel ne serait pas assez prévoyante.

En effet, les « pirates informatiques » redoutent une chose par-dessus tout, c'est le temps ! Chaque seconde qui passe est une seconde au cours de laquelle ils peuvent être attrapés ! Plus le système sera complexe, plus le temps passé à vouloir le pénétrer sera long.

Contourner le système de badgeage à l'entrée puis trouver un mot de passe efficacement créé tout en évitant les caméras de surveillance relève alors du parcours du combattant.

Un système évolutif…

Si le temps est l'ennemi des « pirates informatiques », l'évolution technologique est la faiblesse des entreprises.

Un système obsolète révèle rapidement ses déficiences par l'absence de suivi dans les mises à jour logiciels ou dans le défaut de maintenance régulière du matériel. Les cybercriminels le savent bien et préfèrent s'attaquer à un système dépassé plutôt qu'à un nouveau système même si parfois le défi peut les inciter à le faire.

7. Quelques solutions pour protéger son réseau « efficacement »

La protection des entrées et sorties du réseau (pare-feu, compte réseau…)

La mise en place d'un pare-feu…

Un pare-feu (appelé aussi *coupe-feu*, *garde-barrière* ou firewall en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet).

Un système pare-feu n'offre cependant pas une protection totale. Les firewalls ne protègent que dans la mesure où l'ensemble des communications vers l'extérieur passe systématiquement par leur intermédiaire et qu'ils sont correctement configurés. Ainsi, les accès au réseau extérieur par contournement du firewall sont autant de failles de sécurité.

C'est notamment le cas des connexions effectuées à partir du réseau interne à l'aide d'un modem ou de tout moyen de connexion échappant au contrôle du pare-feu.
De la même manière, l'introduction de supports de stockage provenant de l'extérieur sur des machines internes au réseau ou bien d'ordinateurs portables peut porter fortement préjudice à la politique de sécurité globale.
Enfin, afin de garantir un niveau de protection maximal, il est nécessaire d'administrer le pare-feu et notamment de surveiller son journal d'activité afin d'être en mesure de détecter les tentatives d'intrusion et les anomalies.
La mise en place d'un firewall doit donc se faire en accord avec une véritable politique de sécurité.

La création de comptes réseau…

L'accès aux données sur un poste fixe se fait par accès à un compte d'utilisateur. Ce compte va permettre de filtrer les entrées par un identifiant et un mot de passe mais il permet également de donner des droits et des interdictions sur certaines fonctionnalités en fonction du public visé.

La protection contre les virus, les espions, les spams et le phishing

Les antivirus…

Avec l'arrivée de Microsoft sur le marché de la sécurité, on s'attendait à voir disparaître quelques acteurs. Pour le moment, c'est au phénomène inverse que l'on assiste. De nouveaux éditeurs débarquent et l'offre est plus que jamais pléthorique. Il devient d'autant plus difficile pour les entreprises de choisir que tous ces antivirus arborent désormais les logos de laboratoires autonomes d'évaluation des performances comme VB100 ou ICSA.
Toutefois, certains logiciels passent à côté de certains « malwares ». Certains éditeurs mettent parfois plus de vingt-quatre heures pour générer une protection contre une nouvelle menace à même de se répandre en quelques minutes à travers les e-mails. De même, les défenses proactives qui protègent le système en temps réel contre les menaces les plus perfides du Net affichent des performances très variables. Enfin, les tarifs pratiqués ne reflètent pas toujours les performances attendues.

Les « anti-espions »…

Ce type de protection se révèle être primordial pour une entreprise. L'espionnage industriel n'est pas une illusion !
Il faut donc choisir un logiciel disposant d'un bouclier « temps réel » qui agit sur les espions au moment même où ceux-ci tentent de s'installer : ici, la prévention est souvent plus efficace que l'éradication à posteriori.
De nombreux logiciels de défense sont proposés (Ad-aware, Spybot,…) mais, il peut être utile de vérifier soit même le fonctionnement de ses machines. Le responsable informatique pourra par exemple examiner de temps en temps l'activité anormal de certains programmes dans le gestionnaire de tâches…

Les « anti-spams »…

Menace moins grande, le pollupostage n'en demeure pas moins une gêne pour le bon fonctionnement de l'entreprise et la sécurité des données. Une information de qualité doit être claire, disponible et accessible. Le pollupostage rend la recherche de cette qualité plus

difficile à obtenir. Face à une multitude d'informations comment ne pas se tromper en effaçant l'information utile ?
Sur ce point, une véritable formation des salariés sur la gestion des courriels est de mise : savoir repérer un spam d'une véritable information, savoir rédiger un courriel afin d'assurer une « authenticité » vis-à-vis du destinataire…

Les filtres anti hameçonnage…

Parmi des dernières malveillances observées, l'hameçonnage utilise des courriels dans lesquels l'expéditeur se fait passer pour un établissement financier. Lorsque que l'internaute clique sur le lien contenu dans le courriel, il se retrouve sur un faux site, imitant celui de sa banque, qui récupère ses données personnelles (mot de passe, numéro de compte…).
Les sites bancaires sont évidemment les premiers visés mais on imagine aisément une utilisation de cette technique sur d'autres types de sites.
Sur ce point, des outils de protection sont développés (*Microsoft fournit ce type d'outil sur son navigateur*) mais il faut, encore une fois, préciser que l'attention des utilisateurs reste importante. Ainsi, avant de saisir des informations sensibles sur un site, on peut tout simplement vérifier l'adresse inscrite sur le navigateur et reconnaître une adresse fiable du type : « www.société.com » à l'inverse d'une adresse peu fiable du type : « www.perso.free.fr/mapage/accueil.html »

Protéger et limiter les connexions sans fil (wifi, bluetooth…)

Le problème qui se pose ici pour les entreprises est celui du vol d'informations mais aussi la possibilité de ralentir les connexions internet ou d'être tenu pour responsable si la personne qui pirate votre ligne télécharge des fichiers illégaux.

Pour remédier aux problèmes de confidentialité des échanges sur les réseaux sans fils, le standard 802.11 intègre un mécanisme simple de chiffrement des données, il s'agit du WEP, *Wired equivalent privacy*.
La clé de session partagée par toutes les stations est statique, c'est-à-dire que pour déployer un grand nombre de stations WiFi il est nécessaire de les configurer en utilisant la même clé de session. Ainsi la connaissance de la clé est suffisante pour déchiffrer les communications.
Dans le cas de la clé de 40 bits, une attaque par force brute (c'est-à-dire en essayant toutes les possibilités de clés) peut très vite amener le pirate à trouver la clé de session. De plus une faille décelée par Fluhrer, Mantin et Shamir concernant la génération de la chaîne pseudo-aléatoire rend possible la découverte de la clé de session en stockant 100 Mo à 1 Go de traffic créés intentionnellement.

Le WEP n'est donc pas suffisant pour garantir une réelle confidentialité des données même si la protection s'avère suffisante pour se protéger des petites tentatives d'intrusion.

Aujourd'hui, de nouvelles formules de cryptage ont été développées et se présentent comme plus sécurisées. Il s'agit du WPA et du WPA2 couplé au TKIP. Ces protections bien configurées interdisent toute intrusion dans le système Wifi de l'entreprise.
Mais faut-il encore les mettre en place et ne pas subir les attaques des war-driver ! Une pratique venue tout droit des Etats-Unis consiste à circuler dans la ville avec un ordinateur portable (voire un assistant personnel) équipé d'une carte réseau sans fil à la recherche de réseaux ouverts. Il s'agit du war driving. Des logiciels spécialisés dans ce type d'activité permettent même d'établir une cartographie très précise en exploitant un matériel de

géolocalisation (*GPS*, *Global Positionning System*). Les cartes établies permettent ainsi de mettre en évidence les réseaux sans fil déployés non sécurisés. De nombreux sites capitalisant ces informations ont vu le jour sur internet, si bien que des étudiants londoniens ont eu l'idée d'inventer un "langage des signes" dont le but est de rendre visible les réseaux sans fils en dessinant à même le trottoir des symboles à la craie indiquant la présence d'un réseau wireless, il s'agit du « war-chalking » (francisé en *craieFiti* ou *craie-fiti*). Deux demi-cercles opposés désignent ainsi un réseau ouvert offrant un accès à Internet, un rond signale la présence d'un réseau sans fil ouvert sans accès à un réseau filaire et enfin un W encerclé met en évidence la présence d'un réseau sans fil correctement sécurisé.
Un risque supplémentaire à prendre en compte très sérieusement par les entreprises !

Mettre en place un système de sauvegarde automatisée

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 "PRA" (plan de reprise d'activité) ou le "PS" (plan de secours).
En terme de support, les serveurs ont depuis toujours requis des supports à grande capacité de stockage. La bande magnétique a longtemps été le principal vecteur ; puis sont venus les cartouches numériques, les CD-R et DVD-R (dont la durée de vie vient d'être remise en cause par une étude) et enfin aujourd'hui les disques durs à grands formats (téraoctets).

Aujourd'hui, les copies de sûreté dites "en ligne" deviennent populaires et, 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. 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.

La signature électronique ou l'authentification des données

Pour rappel, depuis mars 2000, la signature numérique d'un document a en France la même valeur légale qu'une signature sur papier, conformément à la loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information.
La signature numérique est un mécanisme permettant d'authentifier l'auteur d'un document électronique et de garantir son intégrité, par analogie avec la signature manuscrite d'un document papier. Un mécanisme de signature numérique doit présenter les propriétés suivantes :
- Une signature authentique : L'identité du signataire doit pouvoir être retrouvée de manière certaine ;
- Une signature infalsifiable : La signature ne peut pas être falsifiée. Quelqu'un d'autre ne peut se faire passer pour un autre ;

- Une signature non réutilisable: La signature n'est pas réutilisable. Elle fait partie du document signé et ne peut être déplacée sur un autre document ;
- Une signature inaltérable : Un document signé est inaltérable. Une fois qu'il est signé, on ne peut plus le modifier
- Une signature irrévocable : La personne qui a signé ne peut le nier (c'est la non répudiation).

8. L'intervention de l'Etat par une politique nationale de sécurité

Vous constatez une intrusion ou une tentative d'intrusion dans votre système d'information ? Des données ont été modifiées, introduites ou supprimées ?

Il existe des services spécialisés mis en place par l'Etat pour déposer plainte directement :

- L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) qui dépend de la Direction centrale de la Police judiciaire.

- La Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI) qui dépend de la Direction régionale de la Police judiciaire de la Préfecture de Police de Paris

- La Direction de la surveillance du territoire (DST)

Au-delà de ces différentes ramifications créées au niveau du ministère de l'intérieur, le pouvoir politique a également institué des sites internet d'informations et de recommandations :

Le site mis en place par le Gouvernement pour favoriser la sécurité des systèmes d'information : http://www.ssi.gouv.fr/fr/index.html

Le portail gouvernemental de la sécurité informatique :
http://www.securite-informatique.gouv.fr/

Ce qui pouvait être jugé parfois comme peu important et devant relever de la gestion des entreprises elles-mêmes est aujourd'hui une priorité nationale imposant une intervention conséquente de l'Etat.
Le pouvoir politique montre sa volonté de mettre en place une action globale à la hauteur de la menace existante. Ce n'est pas seulement l'entreprise X qui est menacée par la cybercriminalité mais l'ensemble de l'économie du pays !

▲ ▲ ▲

La protection des réseaux informatiques s'impose donc comme une réalité et une obligation pour les entreprises françaises qui évoluent dans le cadre de la mondialisation des échanges avec une économie fortement concurrentielle.
Le knowledge management devient un véritable « trésor de guerre » qu'il faut protéger à tout prix des voisins et de leurs convoitises.
L'évolution permanente des technologies oblige à une réaction régulière et maîtrisée car cela a tout de même un coût et contraint très souvent les salariés à des efforts d'adaptation.

Gardons tout de même à l'esprit que l'homme demeure au centre de la veille et qu'il doit par lui-même participer activement à cette sécurité des données. Et cela, il le fera s'il ne se trouve pas défié par ces outils de protection (cyber surveillance).

LEXIQUE

Cheval de troie :
Initialement un cheval de Troie désignait un logiciel se présentant comme un programme normal destiné à remplir une tâche donnée, voire ayant parfois un nom connu (en quelque sorte "déguisé" sous une fausse apparence), mais qui, une fois installé exerçait une action nocive totalement différente de sa fonction "officielle".
Actuellement le terme désigne à peu près tout programme qui s'installe de façon frauduleuse (souvent par le biais d'un mail ou d'une page web piégés) pour remplir une tâche hostile à l'insu de l'utilisateur. Les fonctions nocives peuvent être l'espionnage de l'ordinateur, l'envoi massif de spams, l'ouverture d'un accès pour un pirate...

Déni de service :
C'est une attaque très évoluée visant à rendre indisponible une machine en la submergeant de trafic inutile.

Enregistreur de frappe (Keylogger) :
C'est un logiciel espion qui a la particularité d'enregistrer les touches frappées sur le clavier sous certaines conditions et de les transmettre via les réseaux. Par exemple, certains enregistreurs de frappe analysent les sites visités et enregistrent les codes secrets et mots de passe lors de la saisie. Certains keyloggers sont capables d'enregistrer les URL visitées, les courriers électroniques consultés ou envoyés, les fichiers ouverts, voire de créer une vidéo retraçant toute l'activité de l'ordinateur !

Hacker (pirate informatique) :
Pirate ou expert en informatique, au choix. Spécialiste du forçage des systèmes de sécurité et de l'intrusion dans les sites protégés. Parfois malveillant ou malhonnête, souvent simple farceur. Un hacker inspiré a par exemple remplacé la page d'accueil de la CIA pendant quelques heures par une page de sa fabrication intitulée Central Stupidity Agency.

Hameçonnage (Phishing) :
Pratique illicite d'obtention d'informations personnelles, qui est l'évolution la plus récente du spam. Elle consiste à envoyer à des destinataires des messages apparemment licites provenant d'une institution reconnue, telle une banque. Ces messages contiennent souvent des liens vers de faux sites web qui sont utilisés pour collecter des informations confidentielles concernant des utilisateurs.

Logiciel espion (Spyware) :
Egalement appelé espiogiciel, qui infecte un ordinateur à l'insu de l'utilisateur dans le but de collecter et de transmettre à des tiers, des informations sur ses habitudes de navigation, voire de consommation.

Pare feu (firewall) :
C'est un élément du réseau informatique, logiciel et/ou matériel, qui a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant les types de communication autorisés ou interdits.

Pharming :
Cette méthode consiste à rediriger automatiquement l'internaute vers un faux site (imitant celui de sa banque), lorsqu'il souhaite aller sur le vrai site, mais sans qu'il n'ait besoin de cliquer sur un lien quelconque car le détournement de l'adresse se fait au niveau d'Internet.

Pollupostage (Spam ou spamming) :
Technique de prospection de masse visant à adresser, grâce à un robot de gestion d'adresses électroniques, un même message à une liste de diffusion sans accord préalable des membres de celle-ci. Cette technique est utilisée notamment pour l'envoi de messages publicitaires.

Portes dérobées (backdoors) :
Point d'accès confidentiel à un système d'exploitation, à un programme ou à un service en ligne. Ces passages secrets sont ménagés par les concepteurs des logiciels pour fournir des accès privilégiés pour les tests ou la maintenance. Mais les pirates qui les découvrent peuvent déjouer tous les mécanismes de sécurité et rentrer dans le système.

Virus informatique :
Programme informatique écrit dans le but de se propager à d'autres ordinateurs en s'insérant dans des programmes légitimes appelés "hôtes". Il peut aussi avoir comme effet, recherché ou non, de nuire en perturbant plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre à travers tout moyen d'échange de données numériques comme internet, mais aussi les disquettes, les cédéroms, les clefs USB, etc.

Sites Internet :

■ Le site mis en place par le Gouvernement pour favoriser la sécurité des systèmes d'information : http://www.ssi.gouv.fr/fr/index.html

■ Portail gouvernemental de la sécurité informatique : http://www.securite-informatique.gouv.fr/

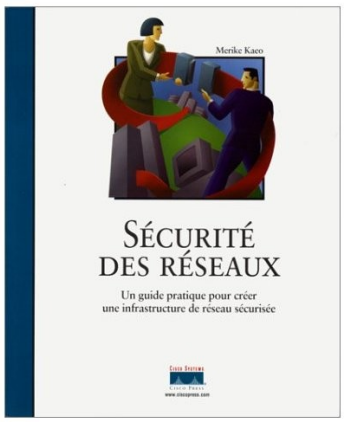
■ Le magasine européen de la sécurité : http://www.mag-securs.com/

■ Le livre blanc sur la sécurité informatique à destination des PME : http://www.checkpoint-mkg.com/newsletter04/wp-pme.pdf

Bibliographie :

La sécurité des réseaux de Tom Thomas

Initiez-vous à la sécurité des réseaux ! - Découvrez l'ennemi (le pirate) et les techniques qu'il emploie - Familiarisez-vous avec les outils et les technologies de sécurité - Protégez votre réseau à l'aide d'un pare-feu, d'un routeur et d'autres équipements dédiés - Découvrez la sécurité des réseaux sans fil - Préparez-vous aux incidents de sécurité. Bienvenue dans le monde des réseaux. Les réseaux informatiques sont aujourd'hui omniprésents et indispensables, mais leur sécurité est souvent insuffisante. Avec la prolifération des virus, des vers ou autres menaces en provenance d'Internet, les entreprises prennent conscience de la nécessité d'augmenter la sécurité de leurs réseaux. Pour pouvoir implémenter des mesures de protection efficaces, il convient de comprendre la logique d'attaque des pirate et les moyens dont ils disposent. Aucune expérience préalable requise. Cet ouvrage explique les principes de la sécurité des réseaux dans un style clair et simple, accessible à tous. Il passe en revue les principales technologies permettant de mettre en œuvre et de contrôler cette sécurité. Que vous débutiez une carrière dans ce domaine ou souhaitiez acquérir une compréhension globale du sujet, ce livre est pour vous.



La sécurité des réseaux de Kaeo et Merike

Peut-il y avoir réseau sans souci de sécurité ? Non, car sous-estimer les enjeux sécuritaires d'une installation informatique connectée à l'extérieur peut faire peser des risques sérieux sur la stratégie même de l'entreprise. Merike Kaeo nous offre un ouvrage qui repositionne la sécurité à son véritable rang. Le livre a pour objectif de couvrir l'ensemble de la problématique liée à la sécurité des réseaux. Et cet objectif est atteint.

Abordant en premier le thème de la cryptographie qui s'avère à la base de tout, l'auteur traite par la suite l'ensemble des éléments permettant la mise en oeuvre d'une vraie politique sécuritaire en entreprise. Les mesures sécuritaires développées en interne comme en externe, la gestion d'incidents ainsi que les protections élaborées dans le cadre de l'accès distant sont autant de sujets qui font l'objet d'un développement de qualité.