La Sécurité à l'heure d'internet

OCTOBRE 2000

LE CIGREF

Le Cigref, Club informatique des grandes entreprises françaises, existe depuis 1970. Sa finalité est la promotion de l'usage des systèmes d'information comme facteur de création de valeurs pour l'entreprise. Il constitue un lieu privilégié de rencontre et d'échange d'informations entre les responsables des grandes entreprises françaises ou européennes utilisatrices d'importants systèmes d'information. Ce partage d'expériences vise à faire émerger les meilleures pratiques. Chaque année, le Cigref réalise des études sur des sujets d'intérêt commun.

Rapports publiés par le Cigref en 2000 :

Gérer les connaissances
Défis, enjeux et conduite de projet

Impacts et usages de la messagerie électronique

Java, langage et architecture
Fiche technologique

Le phénomène Linux en entreprise (à paraître)
Fiche technologique

Mobilité et GSM (à paraître)
Fiche technologique

Nomenclature 2000 (édition de septembre 2000)
Les emplois-métiers du système d'information

Observatoire 2000 des Télécoms

XML, vers un format universel ?
Fiche technologique

Ces rapports peuvent être obtenus en se connectant sur le site web du Cigref : www.cigref.fr

PARTICIPANTS

Ce rapport est issu des réflexions et des contributions des participants aux réunions du groupe de travail sécurité, dont l'activité a été coordonnée par Philippe Verdier, directeur des systèmes d'information de La Poste.

Gilles Afchain	Cogema
Eric Allouard	Danone
Michel Amoury	CCF
Antoine Arrivet	Danone
Michel Barry	L'Oréal
Pierre Bartaire	AP-HP
Philippe Biscondi	Caisse des Dépôts et Consignations
Eric Blanc	AP-HP
Pascal Boisgibault	RATP
Alain Bouillé	La Poste
André Bour	MFP
Monique Bureau	Maaf
Daniel Caron	CNCA
Jean-Louis Carton	MGEN
Francis Cauvé	Banque de France
Bernard Charpentier	Retraites Unies
Jean-Paul Charron	SNCF
Jean-Claude Chausset	Cogema
Richard Chenuc	Informatique CDC
Thibault Chevillotte	Axa
Annie Coussinet	BDPME
Alain Cudel	Amadeus
Jean-Pierre David	Dassault Aviation
Eric Dupriez	AP-HP
Jacky Dutilh	Hennessy (groupe LVMH)
Brice Favreau	Macif
Jean-Louis Fleisch	MMA
Gérard Forestier	Informatique CDC
Jean-Pierre Girault	Renault SA
Jean-François Gornet	EDF/Gaz de France
Alain Gourmelen	Maaf
Philippe Guerin	Grepac
Dominique Guillaume	Framatome
Nicolas Helle	Cegetel
Michel Houssay	Crédit foncier de France
Silvio Inebria	ANPE
Michel Janin	Cnav-TS
Pierre Jorelle	L'Oréal
Jean-Pierre Jousselin	CCF
Patrick Lautier	Générale des Eaux
Christian Lauwick	France Telecom
Georges Le Du	Crica
Alexandre Le kim	Cogema
Sylvère Léger	AGF
Ly Kim Lény	Technip
Marie-Christine Lopez	Mairie de Paris
Jean-Luc Mancip	SNCF
Eric Matoussowsky	La Française des Jeux
patrick Mery	Cnav-TS
Romain Miller	Framatome
Ho Danh Nguyen	Hennessy (groupe LVMH)
Danh Nguyen-Ngoc	Technip
Eric Pichon	Cogema
Jean-Louis Piquepé	France Télécom
Olivier Porte	CNRS
François Pourbaix	EDF/Gaz de France
Philippe Pujalte	Cogema
Jean-Claude Puyfages	L'Oréal
Didier Quincerot	SMABTP
Jean Raguin	Framatome
Pierre-Luc Refalo	Cegetel
Pierre-Pascal Regnault	TotalFina Elf
Serge Saghroune	Accor
Arnaud Sarrazin	RATP
Jean Sulpice	Informatique CDC
Jean-Louis Szuba	EADS
Janick Taillandier	RATP
Pierre Tarif	Lyonnaise des Eaux
Maurice Thaï	Air Liquide
Jean-Pierre Tingaud	Framatome
Didier Tirard	Manpower
Olivier Tresor	Manpower
Rémi Trousset	Cegetel
Philippe Verdier	La Poste
Alain Vielpeau	Crédit Lyonnais
François Villette	Axa
Jacqueline Vinck	ANPE
Philippe Zanini	Mairie de Paris

Nous remercions tout particulièrement Éric Blanc, Alain Bouillé, Francis Cauvé, Thibault Chevillotte, Alain Cudel, Éric Matoussowsky, Pierre-Luc Refalo et Serge Saghroune pour leur contribution au groupe de travail ainsi que Monique Bureau, Jean-Louis Fleish et Pascal Boisgibault pour leur relecture du rapport.

L'étude a été rédigée par Stéphane Rouhier (Cigref).

SOMMAIRE

TABLE DES ILLUSTRATIONS

1. INTRODUCTION

La sécurité informatique est un concept très large qui englobe à la fois la sécurité applicative (contrôle applicatif), la sécurité système (sécurité des systèmes d'exploitation), la sécurité de l'exploitation (plan de continuité et de sauvegarde), la sécurité logique (gestion des accès au système d'information) la sécurité physique (protection des sites) et la sécurité des télécommunications.

Une autre classification possible revient à définir la sécurité par ses objectifs, à savoir la confidentialité (accès physique, accès logique, gestion et protection des documents), la disponibilité (sauvegarde, maintenance, secours, archivage) et l'intégrité (antivirus...).

Dans le cadre de ce groupe de travail, seuls les thèmes de la sécurité logique, de la sécurité applicative et de la sécurité des télécommunications ont été abordés. Volontairement, le thème plus général du « *Risk Management* » n'a pas été traité. Le groupe sécurité a mis l'accent cette année plus particulièrement sur la sécurité internet et la sécurité des messageries. Certains thèmes comme l'administration, les tableaux de bord et les métiers de la sécurité ont seulement été abordés et seront approfondis l'an prochain.

L'objectif de la politique de sécurité est de garantir un niveau de risque acceptable pour l'entreprise en mettant en œuvre une architecture de sécurité prenant en compte l'environnement technique, humain, organisationnel et réglementaire de l'entreprise.

1.1 Une prise de conscience accrue des vulnérabilités du système d'information

On assiste depuis un an environ à la « découverte » des risques liés à l'usage d'internet et à l'interconnexion des réseaux. À l'exception des PME, cette prise de conscience est quasi générale. Elle émane à la fois des fournisseurs, des utilisateurs, des médias (cf. I Love You) et des pouvoirs publics (cf. le discours de Lionel Jospin à Hourtin, la création de la DCSSI et du Cert Administration, le programme d'action de l'Union européenne, le sommet du G8...).

En revanche, la prise de conscience des grandes entreprises des enjeux de la sécurité ne date pas d'hier mais elle a pris une nouvelle envergure. En effet, le passage de l'entreprise étendue à l'entreprise virtuelle a renforcé les besoins des directions des systèmes d'information (DSI) en matière de sécurité.

Les principaux facteurs de développement du marché de la sécurité sont :

- l'ouverture du système d'information de l'entreprise aux clients, partenaires, fournisseurs voire aux concurrents ;
- l'explosion des attaques virales, intrusions, dénis de service et usurpations d'adresses ;
- la multiplication des projets de *B-to-C* et *B-to-B* (places de marché...) ;
- l'essor de la mobilité intra et interentreprises ;
- la mise en place d'architecture multitiers ;
- le développement des accès distants ;
- le développement de la télémaintenance applicative.

1.2 Les risques externes l'emportent sur les risques internes

Sur la base d'une enquête réalisée par le Cigref auprès de ses membres, on constate que les principales attaques proviennent de facteurs extérieurs tels que les virus, les attaques par dénis de service, etc.

On assiste donc à une inversion des tendances puisque historiquement les grandes entreprises estimaient que les risques internes étaient plus élevés. Or, ce sont les risques externes qui sont les moins prévisibles, donc les moins maîtrisables et les plus insupportables pour les entreprises. La sécurité a donc encore de beaux jours devant elle.

1.3 La recrudescence des attaques virales : l'exemple de I love you

Comme toutes les entreprises, les membres du Cigref ont été confrontés à ce virus. Une enquête réalisée en interne nous a permis de dresser le bilan suivant :

- I Love You a connu au moins 30 mutations ;
- les dégâts ont dans l'ensemble été relativement limités ;
- les dommages ont été moins importants qu'avec le virus Melissa ;
- les dommages ont été variables selon le type de messagerie utilisée (importants avec Outlook, nuls avec les autres messageries) ;
- les éditeurs d'antivirus et les fournisseurs d'accès internet ont été réactifs même si le support n'a pas toujours suivi ;

- les administrateurs de messagerie ont bien joué leur rôle (information des utilisateurs, désactivation des fonctions de *scripting*, cloisonnement des messageries) ;
- les attaques virales ne remettent pas en cause le choix du type de messagerie ni l'utilisation de la messagerie ;
- la vitesse de propagation des virus tend à augmenter ;
- nous n'en sommes qu'au tout début des attaques virales.

1.4 Des handicaps à surmonter

Les entreprises françaises ont encore quelques handicaps à surmonter :

- leur budget sécurité reste inférieur à celui des entreprises américaines ;
- les directions générales ne sont pas encore toutes sensibilisées à la nécessité d'une politique de sécurité ;
- toutes les entreprises ne sont pas dotées d'une organisation ni d'un responsable sécurité ;
- l'approche technique ne suffit pas. Il faut avoir une approche globale et tenir compte des aspects humains, organisationnels et réglementaires ;
- les entreprises françaises manquent d'outils pour mesurer et comparer l'efficacité de leur politique de sécurité ;
- les entreprises françaises ne sont pas assez réactives face aux attaques virales et aux tentatives d'intrusion (exploitation des journaux...).

Côté fournisseurs, on peut regretter parfois :

- un discours trop « alarmiste » ;
- une certaine uniformité de l'offre ;
- un manque de « support » lors des attaques virales.

Les sources d'information fiables, gratuites et indépendantes restent encore rares. Parmi les sources d'information payante on peut citer les sites web des éditeurs d'antivirus, les lettres d'information de société de conseil (Lexsi...) et les trois Cert nationaux (*Computer Emergency Response Team*) existants[1].

[1] Les Cert sont des organismes offrant des prestations payantes de veille, de support sur incidents, de formation et d'études dans le domaine de la sécurité et d'Internet. Il existe trois Cert en France : le Cert Renater, le Cert IST et le Cert Administration.

1.5 Quels enjeux pour l'entreprise ?

La problématique pour l'entreprise est simple :

- Comment concilier l'ouverture de l'entreprise avec la sécurité du système d'information ?
- Comment trouver un compromis entre le coût et la performance du système d'information ?

Les mesures de sécurité étant souvent coûteuses et contraignantes, leur mise en œuvre doit être adaptée aux réels enjeux. La difficulté vient aussi du fait que l'entreprise évolue dans un environnement économique et humain dynamique (fusion, acquisition, changement de partenaires et de fournisseurs, changement dans les alliances, départ et arrivée de collaborateurs...). La politique de sécurité doit donc s'adapter à ce changement de décor permanent.

Or, la politique de sécurité souffre encore d'un problème de légitimité dans l'entreprise. Trop souvent elle est vue comme un poste de coût par la direction générale alors que les risques en termes d'image (détournement de nom de domaine, *hoaxes*) de coûts et d'immobilisation (attaques virales, dénis de service...) peuvent être très élevés.

De plus le responsable sécurité a parfois un problème de « positionnement » dans l'entreprise et l'impression de servir d'alibi plutôt que d'être clairement impliqué dans la stratégie informatique de l'entreprise et en particulier pour internet.

Le manque de légitimité du responsable sécurité, souvent associé à un manque de moyens, constitue à nos yeux l'un des principaux freins au développement de la politique de sécurité dans l'entreprise.

1.6 Vers une politique de sécurité globale ?

Pourquoi est-il devenu indispensable de mettre en place une politique de sécurité aujourd'hui ? La politique de sécurité s'avère incontournable car elle permet de garantir :

- l'image de l'entreprise ;
- la disponibilité du système d'information ;
- l'intégrité et la confidentialité des informations ;
- l'authentification des personnes et le contrôle des accès aux sources d'information de l'entreprise ;
- la sécurité des transactions électroniques (*B-to-C* et *B-to-B*) ;

- la non-révocation des paiements ;
- le respect des obligations juridiques ;
- la protection du patrimoine de l'entreprise.

En revanche, de l'avis des participants, la politique de sécurité n'a pas vocation à régler tous les dysfonctionnements de l'entreprise.

De même, il est impossible aujourd'hui de garantir un niveau de sécurité à 100 % mais seulement un niveau de risque acceptable. Les risques peuvent également être partiellement couverts par des polices d'assurance.

Il faut bien voir de toute façon que la politique de sécurité n'est pas un projet mais un processus permanent qui intègre l'ensemble des évolutions affectant la sécurité de l'entreprise. La sécurité du SI doit s'intégrer dans la vie des projets et des services.

La définition, la mise en œuvre de la politique de sécurité restent complexes car elles supposent à la fois une méthode, une organisation, des outils, des procédures, des règles et des hommes.

Enfin, les responsables sécurité sont unanimes sur le fait que la sécurité est l'affaire de tous et ne peut fonctionner que si la direction générale est impliquée et que les salariés sont responsabilisés. Elle repose notamment sur une bonne définition préalable du domaine d'application et des objectifs, une bonne organisation, une bonne coordination des différentes directions de l'entreprise et sur un audit régulier.

Les directions métiers sont d'ores et déjà impliquées à la fois dans la définition des informations sensibles et dans l'application de la politique de sécurité du groupe.

De même, la DRH est associée, notamment en ce qui concerne la gestion des droits d'accès (début et fin de contrat) et le suivi du personnel au sens large (salariés, stagiaires, prestataires extérieurs, fournisseurs et partenaires).

C'est en misant sur un investissement matériel (infrastructures, personnel...) et immatériel (formation, audit...) régulier que l'entreprise pourra garantir la pérennité et l'efficacité de sa politique de sécurité.

2. COMMENT BÂTIR UNE POLITIQUE DE SÉCURITÉ ?

2.1 La mise en place de la politique de sécurité

Le *Security Handbook*, dans sa RFC 2196, définit la politique de sécurité comme « une formalisation des règles auxquelles doivent se conformer les gens qui ont accès aux technologies et à l'information d'une organisation ».

On peut définir la politique de sécurité comme :

- une doctrine ;
- une architecture ;
- une organisation ;
- un processus de contrôle ;
- un programme de sensibilisation.

La mise en place de la politique de sécurité suppose au préalable une définition du domaine d'application et de ses objectifs.

2.1.1 Définir ses objectifs

Les participants au groupe de travail considèrent que la politique de sécurité doit répondre à l'ensemble des objectifs suivants :

- authentification ;
- contrôle d'accès ;
- intégrité ;
- imputabilité ;
- confidentialité ;
- non-répudiation ;
- disponibilité ;
- audit ;
- assurance.

Il s'agit avant tout de protéger l'intégrité, la confidentialité et la disponibilité des informations. L'authentification permet de vérifier l'identité de l'utilisateur et d'acquérir la preuve que l'utilisateur est bien ce qu'il prétend être. L'intégrité permet de se protéger contre toute modification non autorisée d'information. L'imputabilité est la possibilité d'attribuer une action à son auteur. La confidentialité permet d'empêcher toute divulgation non autorisée d'informations sensibles. La non-répudiation permet de s'assurer qu'une transaction a effectivement eu lieu. La disponibilité vise à garantir le fonctionnement des informations de

l'entreprise. L'audit permet l'enregistrement, le contrôle et l'évaluation de la sécurité. Enfin, l'assurance passe par des contrats d'assurances adaptés aux principaux risques.

La sécurité doit être basée sur des critères d'efficacité et d'économie.

2.2 Cartographier les risques

2.2.1 Évaluer les risques

Le responsable sécurité doit, avant de mettre en place sa politique de sécurité, avoir une vision globale du patrimoine à protéger. il doit aussi répertorier et évaluer les risques de l'entreprise en termes de divulgation, altération ou destruction. Ces risques sont multiformes. Ce sont à la fois :

- des risques internes et externes ;
- des risques métier et des risques informatiques ;
- des risques liées à la personne, des risques liés aux procédures et des risques liés aux protocoles et aux matériels ;
- des risques connus et des risques inconnus ;
- des risques supportables ou non ;
- des risques prévisibles et imprévisibles ;
- des risques maîtrisables ou non.

À chaque risque, il faut affecter un degré de probabilité et de faisabilité (cf. figure 1). Le responsable sécurité doit, en liaison avec les directions métiers, qualifier et quantifier les risques internes et externes. Le RSSI (responsable de la sécurité des systèmes d'information) doit ensuite estimer quels sont les risques maîtrisables par des mesures procédurales, physiques, préventives (« antirelayage » de trames, fermeture de ports, de passerelles...) ou correctives (*patches*, plan de secours...).

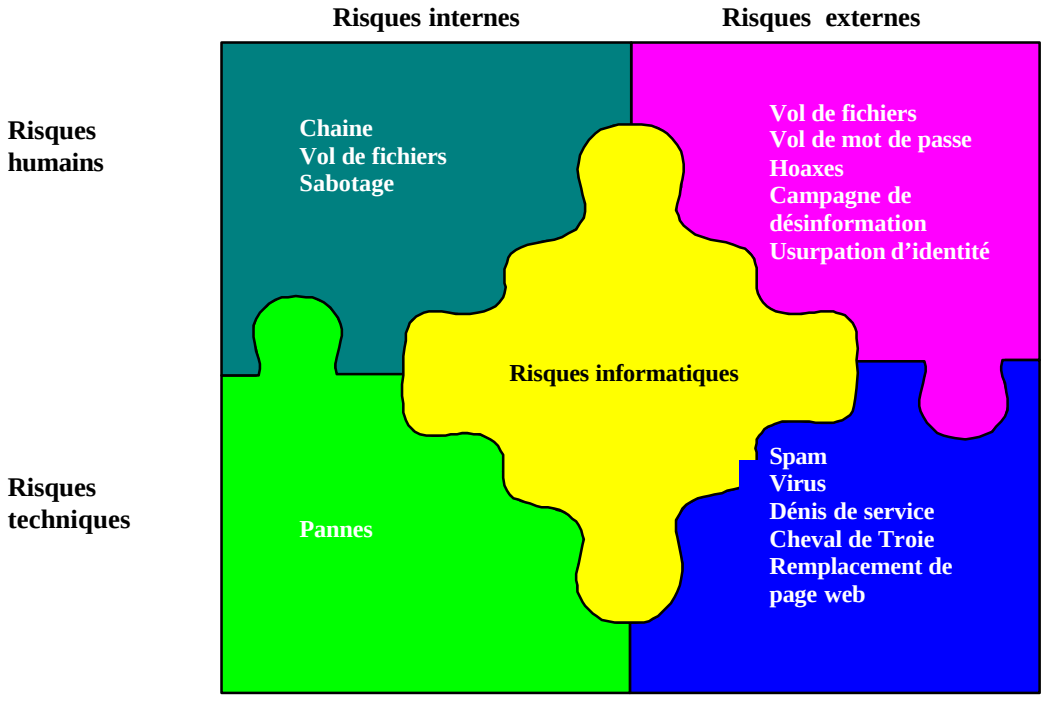
Tous les risques ne sont pas forcément prévisibles ni maîtrisables. Ainsi, les attaques par déni de service distribué (DDOS) sont par nature de grande envergure et imprévisibles. Une des parades consiste généralement à fermer son site ou à chercher à identifier l'origine de l'attaque, ce qui est difficile car le ou les attaquants utilisent généralement des sites relais pour faire rebondir leur attaques.

Il ressort des travaux du groupe que la sécurité informatique n'a pas vocation à couvrir tous les risques de l'entreprise. Un certain nombre de risques, notamment les risques métiers, peuvent être couverts par d'autres moyens tels que les polices d'assurances.

	Faisabilité	Probabilité	Gravité
1	La menace est réalisable par tout public	La menace est certaine	Les conséquences sont très limitées
2	La menace est réalisable avec des connaissances de base et des moyens standards	La menace est probable	Gêne limitée à un service une commande, quelques dizaines de kF
3	La menace nécessite un bon niveau d'expertise et du matériel spécifique	La menace est peu probable	Conséquences importantes pour le service, perte entre 500 kF et 1 MF
4	La menace nécessite des moyens exceptionnels ou une association d'experts particulièrement compétents	La menace est très improbable	Pertes très importantes pouvant mettre en péril les activités de l'entreprise

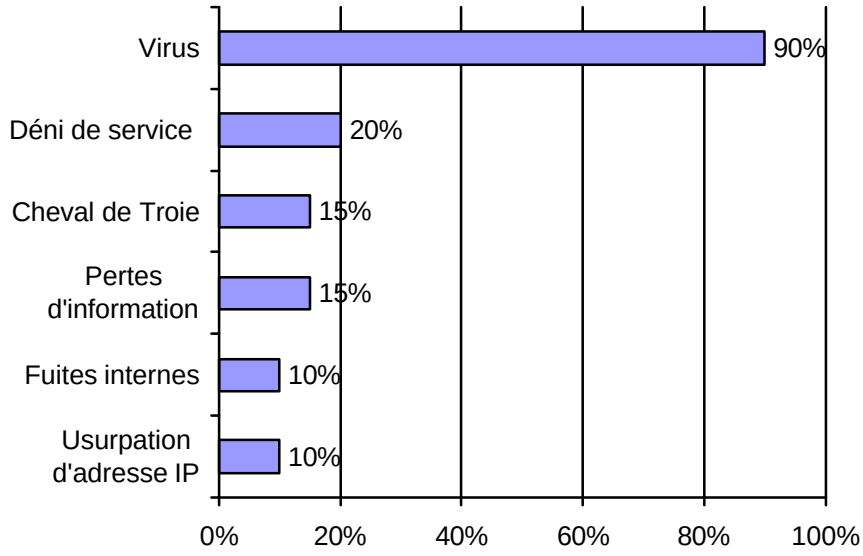
Source : Maaf

Figure 1 : Échelle de probabilité, de faisabilité et de gravité des risques informatiques.



Source : Cigref

Figure 2 : Cartographie des risques informatiques.



Source : Cigref

Figure 3 : Bilan des principales attaques subies par les grandes entreprises en 1999.

2.2.2 Les risques externes l'emportent sur les risques internes

Sur la base d'un questionnaire envoyé fin 1999 aux membres de Cigref, on constate que les principales attaques proviennent de facteurs extérieurs : virus, attaques par dénis de service...

Historiquement, les entreprises estimaient que les risques internes étaient plus élevés, mais l'on assiste depuis peu à une inversion des tendances : les risques externes l'emportent maintenant sur les risques internes. Or, ce sont ceux qui sont les moins prévisibles, donc les moins maîtrisables et les plus insupportables pour les entreprises. Parmi eux, ont peut citer les dénis de service (DOS), les remplacements de page web, les usurpations de noms de domaines, les vols de numéros de cartes bleues et les vols de fichiers.

2.2.3 Évaluer les risques humains

Le facteur humain est l'une des composantes clés de la sécurité.

C'est un élément incontournable de la politique de sécurité mais c'est aussi un maillon faible. Un élément fort, car si le salarié se sent concerné, la politique de sécurité sera un succès. Un maillon faible aussi, car si le salarié se sent lésé, il cherchera à se venger par tous les moyens (virus...). L'actualité montre malgré tout que

ce risque existe davantage chez les informaticiens que chez les autres salariés de l'entreprise.

Les risques humains concernent plusieurs catégories de population dans l'entreprise : le personnel informatique, les stagiaires, les intérimaires, les consultants, les SSII en délégation et, de manière générale, les prestataires extérieurs. Ce sont donc soit des personnes disposant de droits d'accès privilégiés, soit des personnes mobiles et pas toujours clairement identifiées.

Par ailleurs, il faut bien voir que la sécurité est ambivalente. D'un côté elle permet de garantir au salarié un environnement de travail sûr, mais d'un autre côté, elle peut devenir un instrument de contrôle et de surveillance du salarié.

Les risques en matière de sécurité ne sont pas seulement humains et organisationnels, il y a aussi des risques techniques liés à la fragilité du système d'information.

2.2.4 Évaluer la fragilité de son SI

Les responsables sécurité considèrent que les points de fragilité existent à plusieurs niveaux : messagerie, accès distant, accès internet. Ces points de fragilité peuvent être résorbés si les systèmes d'exploitation sont suffisamment sécurisés. Même si d'autres points de fragilité existent, nous nous attarderons sur ces trois-là.

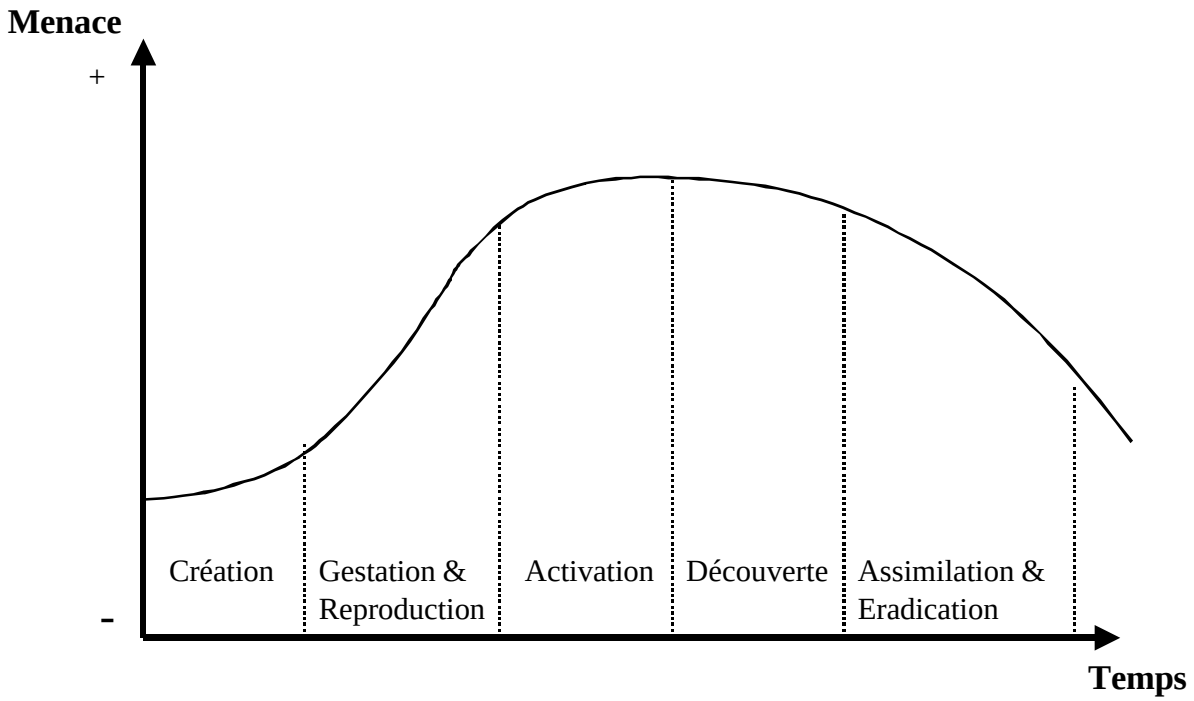
Les menaces sont connues et répertoriées. On peut les classer en trois grandes catégories.

- les risques liées à la messagerie : les virus, le *spam* ou UCE (*Unsolicited Commercial E-mail*).
- les risques liés à l'accès distant : le vol de mot de passe (*packet sniffing*), le vol de données (*data theft*), l'altération de données (*data alteration*), l'usurpation d'identité (*identity spoofing*).
- les risques liés à internet : les virus, les dénis de service distribués (*Distributed Denial Of Service*), les chevaux de Troie (*Trojan Horse*), les remplacements de page web, les usurpations de noms de domaines.

L'entreprise n'est heureusement pas totalement démunie face à ces risques.

Pour les risques liés à la messagerie, l'entreprise doit pouvoir être en mesure de garantir l'authentification de l'émetteur et du récepteur, l'intégrité du message, la confidentialité des informations. La parade contre le *spam* par exemple consiste à filtrer les domaines « spammeurs » par le serveur de courrier ou par le routeur. On peut aussi procéder à un filtrage sémantique. Il

est conseillé également d'interdire le « relayage ». Pour lutter efficacement contre les virus, il est conseillé de surveiller le trafic de courrier internet au niveau de la passerelle, d'analyser sur le serveur de messagerie les messages entrants et sortants, de choisir deux éditeurs d'antivirus différents, l'un pour le poste client, l'autre pour le serveur et d'avoir les dernières mises à jour des logiciels antivirus. Il faut bien voir que le risque lié aux virus par exemple n'est pas constant dans le temps (cf. figure).



Source : Cigref

Figure 4 : Le cycle de vie d'un virus.

- Pour les risques liés à l'accès distant, la solution consiste à chiffrer l'infrastructure de transport (RPV) et les communications (SSL...) et à faire de l'authentification plus ou moins forte par un mot de passe, un jeton, ou une PKI avec ou sans carte à puce (cf. *infra*).
- Enfin, pour les risques liés à internet, il n'y a pas de solution miracle. Pour les attaques par déni de service distribué, Cisco par exemple propose pour ses équipements les mesures préventives suivantes : 1/ utiliser la commande Unicast RPF pour vérifier l'origine de l'adresse IP, 2/ filtrer toutes les espaces d'adresse RFC1918 utilisant des listes de contrôle d'accès, 3/ appliquer des filtres *ingress* et *egress* utilisant ACL, 4/ utiliser CAR pour limiter le débit maximal des paquets ICMP

et 5/ configurer le débit maximal pour les paquets SYN. Pour les remplacements de pages web, il est recommandé de vérifier les interfaces CGI utilisés (cf. *infra*).

Mais il ne suffit pas de sécuriser son système, il faut aussi être conscient des failles de ses prestataires et de ses partenaires, faute de quoi une attaque par rebond est toujours possible.

2.2.5 Connaître les faiblesses de ses partenaires et de ses prestataires

Les entreprises sont de plus en plus amenées dans le cadre de leur métier à ouvrir leur système d'information à leurs partenaires et fournisseurs *via* des extranets. Cette remarque est particulièrement vraie pour le secteur industriel (automobile, aéronautique...) où les acteurs en amont et en aval sont fortement intégrés dans la chaîne de production.

La mise en place d'un extranet suppose la sécurisation des accès, l'identification et l'authentification des utilisateurs externes et le compartimentage de l'intranet, du progiciel de gestion intégré et des bases de données.

Les entreprises utilisent également des prestataires extérieurs (FAI, SSII, éditeurs...) pour accéder à internet, héberger leur site web ou leur site de commerce électronique, mettre en place un portail avec des abonnements à des canaux d'information, faire de la télémaintenance ou de la téléadministration à distance. Toutes ces opérations impliquent également que le niveau de sécurité de ces partenaires soit testé, que ce niveau de sécurité soit le même que celui de l'entreprise contractante pour éviter toute attaque par rebond.

Mais il ne suffit pas de protéger son système et celui de ses partenaires, encore faut-il connaître les bogues de certains protocoles et outils. Ces erreurs de conception sont en effet largement connues et exploitées par les *hackers*.

2.2.6 Gérer les failles de certains produits et protocoles

On peut citer les travaux du Cert CC et du SANS Institute (juin 2000) qui recensent les 10 failles les plus critiques sur internet, à savoir :

1. les faiblesses de Bind (*Berkeley Internet Name Domain*), nxt, qinv, in.named.

2. les vulnérabilités dans les programmes CGI (*Common Gateway Interface*) et les extensions d'application (ex. : Cold Fusion) installés sur les serveurs web ;

3. les faiblesses dans les procédures d'appel à distance (RPC) (ToolTalk, Calendar Manager) ;

4. les failles de sécurité dans les RDS (*Remote Data Services*) du serveur web de Microsoft Internet Information Server (IIS) ;

5. les faiblesses de Sendmail (*buffer overflow*), les attaques *pipe* et Mimebo, qui permettent de compromettre immédiatement le *root* ;

6. les faiblesses de Sadmind et Mounted ;

7. le partage global de fichiers et le partage inapproprié d'information via Netbios et certains ports sous Windows NT, Unix ou MacIntosh ;

8. les mots de passe utilisateur, en particulier le mot de passe *root*, administrateur sans mot de passe ou avec un mot de passe faible.

9. les vulnérabilités de type débordement de *buffer* (*buffer overflow*) ou les configurations incorrectes sur les protocoles de messagerie Imap et Pop.

10. Le choix d'un « *community string* » SNMP par défaut et public.

Ces vulnérabilité sont décrites en détail en annexe, ainsi que les conseils pour y remédier. Des attaques récentes (I Love You) ont également montré comment les macro et les *scripts codes* pouvaient se diffuser facilement *via* les pièces jointes dans Internet Explorer et Office 2000. En plus, certains de ces virus et des codes malicieux peuvent même se diffuser sans qu'il y ait besoin d'ouvrir de pièces jointes (exécution de *script code* et d'active X).

2.2.7 Le phénomène des hackers

Les pirates sont des individus dont l'objectif est :

- de s'introduire dans le réseau de l'entreprise par défi ;
- de voler ou de détruire des données informatiques.

Le mouvement *hacker* remonte au début des années 1970. C'est un mouvement contestataire « *underground* » qui revendique le droit à la transparence et à la liberté d'accès à l'information. Le monde des pirates n'est pas un monde homogène. On peut en effet distinguer plusieurs catégories de pirates :

- les « *hackers* » : les pirates informatiques qui s'introduisent dans des sites privés « pour le plaisir » de briser les défenses et sans but destructif ;

- les « *crackers* » : les pirates informatiques qui s'introduisent dans les sites privés pour nuire, pour détruire ou voler des données ;
- les « *phreakers* » : les pirates informatiques qui trouvent des moyens pour exploiter les liaisons téléphoniques ;
- les « *carders* » : les pirates informatiques qui travaillent sur le piratage des moyens de paiement électronique.

Le monde des *hackers* est en perpétuelle évolution, ce qui rend difficile toute tentative de classification. Le mode de fonctionnement des pirates est de type communautaire et libre : les outils de piratage sont mis à la disposition de tout le monde.

Outils	Fonctions
Virus	Paralyse le SI
Cheval de Troie	Prend le contrôle à distance de la machine après dépôt d'un fichier
Sniffers	Intercepte les transmissions de données
Crackers	Déchiffre les mots de passe
Keystrokers	Enregistre les frappes du clavier
Scanners	Identifie les failles de sécurité du réseau
War Dialer	Automatise les connexions téléphoniques

Source : Technologies Internationales

Figure 5 : Principaux outils utilisés par les pirates.

On assiste de plus en plus à une « professionnalisation » des pirates. Les pirates agissent de moins en moins à titre individuel et travaillent de plus en plus en équipes ou, dans le cas d'attaque par DOS, en s'appuyant sur les serveurs web d'entreprises « neutres » pour faire rebondir leurs attaques.

2.3 Définir une architecture de sécurité

2.3.1 Choisir une architecture de sécurité

Il n'existe pas un modèle d'architecture unique en matière de sécurité aujourd'hui. Néanmoins il y a un certain nombre de « fondamentaux » à respecter. Des composants de l'architecture technique fournissent déjà des services de sécurité : MVS (RACF), Unix, Sybase, mais ces services restent spécifiques et limités à l'équipement.

Une architecture de sécurité typique dans un environnement de type internet ou intranet se compose des « briques » suivantes :

- le *firewall* ou pare-feu ;
- les outils de détection d'intrusion (IDS) ;
- les antivirus ;
- le contrôle d'accès (mot de passe, jeton, SSO, cartes à puce ou PKI) ;
- une zone démilitarisée (DMZ) ;
- le serveur web ;
- le serveur d'authentification (Radius, Tacacs+) ;
- le serveur d'accès distant ;
- le chiffrement des messages ;
- le réseau privé virtuel (RPV) ;
- l'annuaire LDAP ;
- l'administration et la surveillance de réseau.

Une fois ces « briques » de base réunies, il faut organiser l'architecture de sécurité dans son ensemble (« le ciment »), puis définir les procédures, les règles d'organisation, les règles d'accès, les règles d'administration et les plans de secours.

Cette architecture peut être relativement complexe à mettre en œuvre car les grandes entreprises présentent un certain nombre de spécificités :

- héritage du système d'information existant (*mainframe*) ;
- environnement hétérogène, multi-systèmes d'exploitation et multisystèmes ;
- environnement multisites ;
- environnement international ;
- problématique de la mobilité et de l'accès distant ;
- gestion de plusieurs dizaines de partenaires et de fournisseurs.

Les règles de base sont les suivantes :

- cloisonner les différentes parties du réseau et poser à chaque intersection un ou plusieurs pare-feu ;
- ne pas utiliser le pare-feu comme un serveur web en même temps ;

- ne pas surestimer les performances d'un pare-feu (*buffer overflow*, mauvaise configuration du pare-feu...)[2] ;
- configurer éventuellement les pare-feu pour interdire le routage automatique ;
- allouer éventuellement des adresses IP spécifiques pour le réseau interne (RFC 1918) ;
- si les données de l'intranet sont vraiment sensibles, prévoir un accès internet sur des postes isolés ;

Les architectures de sécurité seront étudiées plus en détail l'an prochain par le groupe de travail.

2.4 L'organisation de la politique de sécurité

2.4.1 Quels sont les acteurs concernés ?

La politique de sécurité doit associer à la fois des responsables fonctionnels et des responsables opérationnels. De la même façon, elle doit faire intervenir des directions verticales (métiers) et des directions horizontales (DG, DSI, DRH) de l'entreprise. Enfin elle doit englober le siège, les filiales et le réseau de partenaires et de fournisseurs de l'entreprise.

2.4.2 Exemple de l'organisation de la politique de sécurité à La Poste

La Poste possède près de 17 000 implantations sur le territoire national, emploie 300 000 employés et utilise 100 000 postes de travail.

La Poste est organisée autour de trois métiers :

- services financiers ;
- courrier ;
- colis et Logistique.

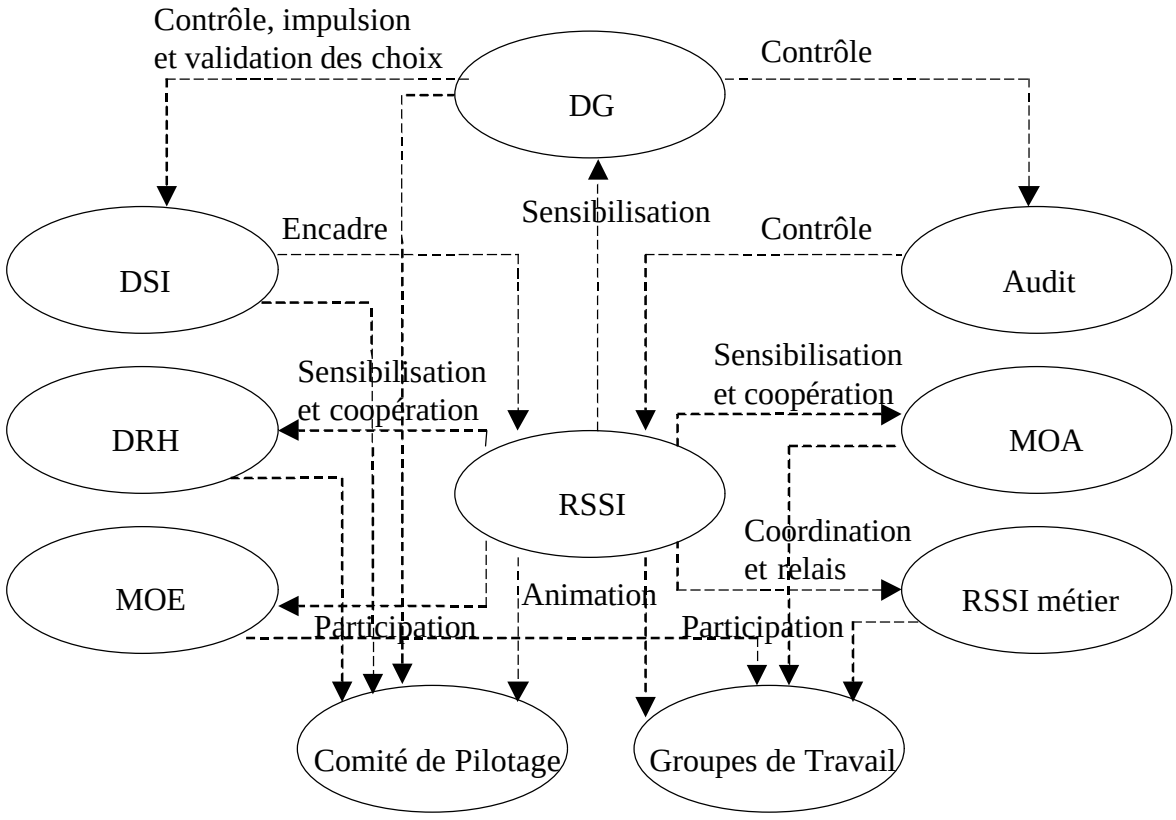
Les principaux acteurs impliqués dans la définition, la mise en œuvre et le contrôle de la politique de sécurité à La Poste sont:

- la direction générale ;
- la direction des systèmes d'information ;
- le Responsable de la sécurité des systèmes d'information (RSSI) ;
- le RSSI métier ou correspondant sécurité ;
- la maîtrise d'ouvrage (MOA) ;

[2] Un pare-feu ne protège pas contre des utilisateurs internes malveillants, ni contre des connexions qui ne passent pas par le pare-feu, contre des menaces complètement nouvelles ou contre les virus.

- l'architecte ;
- la maîtrise d'œuvre (MOE) ;
- les administrateurs ;
- le contrôleur de la sécurité ;
- l'auditeur interne ;
- l'utilisateur final.

Le schéma ci-dessous résume un exemple parmi d'autres d'organisation de la politique de sécurité en entreprise.



Source : Cigref, d'après La Poste

Figure 6 : Schéma d'organisation générale de la politique de sécurité.

La direction générale valide les principaux objectifs de la politique de sécurité et est informée de l'évolution et des menaces qui pèsent sur le SI.

La direction des systèmes d'information est garante de la sécurité des systèmes d'information.

Le responsable de la sécurité des systèmes d'information (RSSI) est rattaché à la DSI et dépend d'elle pour son budget. Le RSSI est la personne qui, au niveau de l'entreprise, formalise la politique de sécurité (objectifs, procédures, instruments).

Le RSSI métier ou opérationnel est le correspondant sécurité du RSSI au sein des branches métiers de l'entreprise.

L'architecte est la personne qui met en place l'architecture de sécurité.

La maîtrise d'œuvre regroupe les concepteurs et les développeurs chargés des développements applicatifs.

Le contrôleur de la sécurité est chargé de la détection des vulnérabilités et l'auditeur de la vérification de l'ensemble du processus.

La Poste a mis en place des structures complémentaires de pilotage et de coordination :

- un comité de pilotage, chargé de définir et piloter le programme de sécurité de l'entreprise, de présenter éventuellement le budget sécurité au conseil d'administration ;
- des groupes de travail, chargés d'élaborer et de mettre en place les standards de sécurité, par exemple pour la sécurité des réseaux, la sécurité des systèmes et la sécurité des applications.

La Poste a mis également en place un programme de surveillance pour s'assurer du respect des règles, ce qui comprend notamment :

- la mise en place d'outils de détection d'exceptions sur les environnements techniques de production ;
- l'audit des incidents de sécurité pour les systèmes sensibles et les connexions réseaux sensibles (internet) ;
- la mise en place de cellules de surveillance (réseau, systèmes d'exploitation) ;
- la mise en place de procédures de gestion d'exceptions.

Enfin l'administration de la sécurité et la gestion des droits d'accès (qui a accès à quoi ?) est considérée comme un point clé de la politique de sécurité.

2.4.3 Remarques complémentaires sur l'organisation de la politique de sécurité

Les membres du Cigref n'ont pas tous la même conception de l'organisation de la politique de sécurité. Le mode de fonctionnement de la politique de sécurité variera selon :

- la taille et la structure de l'entreprise ;
- le degré d'internationalisation de l'entreprise ;
- le degré d'exposition aux risques de l'entreprise (défense, aéronautique, nucléaire...) ;
- le degré d'ouverture de l'entreprise vers ses partenaires ;
- le mode de management de l'entreprise (centralisé, décentralisé).

Les structures ne sont pas identiques d'un membre à l'autre. Certains membres, par exemple, se sont dotés d'une cellule de crise, présidée par le directeur du SI ou par un de ses représentants et qui se réunit chaque fois que des accidents liés au SI apparaissent.

Concernant l'organisation, il faut répartir les tâches entre la direction générale, la DSI, l'audit et les directions métiers.

Les membres du groupe de travail sont tous unanimes sur le fait que l'organisation doit être est basée sur le principe de la « séparation des pouvoirs ». Il faut distinguer notamment la personne qui :

- définit et fait évoluer les règles de sécurité ;
- met en œuvre et respecte les règles de sécurité ;
- contrôle l'application des règles de sécurité.

Généralement, c'est la direction générale qui fixe les grandes orientations, le RSSI qui définit les règles de sécurité, la DSI et les directions métiers qui les mettent en œuvre et l'audit qui en contrôle l'application.

Il est certes possible de confier la définition et la mise en œuvre des règles à la même personne, ce qui permet de gagner en réactivité mais ce qui peut aussi poser des problèmes d'efficacité (goulot d'étranglement, responsabilité...).

Inversement, si trop d'acteurs sont impliqués dans la politique de sécurité, cela risque d'être contre-productif, de diluer les responsabilités et de ralentir le processus de décision.

L'efficacité de la politique de sécurité dépendra *in fine* de la bonne coopération entre ces différentes entités et de l'existence

de procédures écrites, validées, accessibles et appliquées par tous.

2.5 La sensibilisation de l'entreprise à la problématique de la sécurité

Si toutes les directions, branches métiers et filiales de l'entreprise doivent être sensibilisées à l'importance de la sécurité, cette sensibilisation ne revêt pas nécessairement les mêmes formes ni les mêmes modalités.

Cette sensibilisation peut être stratégique, technique, juridique. Elle concerne à la fois les acteurs de la politique de sécurité et les utilisateurs finaux. Dans certains cas, il ne s'agira que d'une sensibilisation légère, dans d'autres cas d'une formation intensive.

Les actions de sensibilisation seront généralement menées en interne, tandis que les actions de formation seront menées en externe par le biais d'organismes de formation généralistes ou spécialisés (Apogée, Bull Formation, Cap gemini Institut, CF6, CS Institut, IBM, Learning International, Orsys, Sun Microsystems...).

Parfois, le succès de la politique de sécurité implique une coopération renforcée avec certaines directions clés (cas de la DRH et de la DSI notamment). Dans ce cas, la formalisation et la modélisation des procédures se feront en interne.

2.5.1 La sensibilisation de la direction générale

Le RSSI se trouve vis-à-vis de la direction générale dans une situation ambivalente. Il doit en effet à la fois « faire peur » pour obtenir des moyens et en même temps « rassurer » pour justifier son budget. Il ne faut pas que la sécurité apparaisse comme un frein systématique aux projets de commerce électronique de l'entreprise. Tout est affaire de « dosage », sachant de toute façon que la direction générale est par ailleurs largement sensibilisée par la presse et par les cabinets de conseil.

La sensibilisation de la direction générale passe par une communication sur les risques informatiques mais aussi par la remontée d'indicateurs pertinents permettant aux cadres dirigeants d'évaluer le degré d'exposition de l'entreprise aux risques informatiques.

La direction générale doit également être impliquée dans la démarche de sécurité de l'entreprise. Elle doit valider la politique de sécurité, en particulier les objectifs, les exigences de sécurité ainsi que l'organisation. C'est elle qui doit valider les principales orientations de sécurité.

2.5.2 La formation et la sensibilisation des utilisateurs

La formation des utilisateurs comprend plusieurs niveaux de formation et peut revêtir plusieurs modalités.

Il faut effectivement distinguer :

- la formation des formateurs ;
- la formation des correspondants sécurité métier ;
- la formation des propriétaires de l'information ;
- la sensibilisation des utilisateurs finaux de l'information ;
- la formation des techniciens.

Les besoins seront plus ou moins sophistiqués selon les populations concernées. La formation peut se faire soit en interne, soit en externe, soit de manière mixte. La formation des formateurs peut se faire par exemple à l'extérieur et la formation des utilisateurs finaux en interne. L'entreprise peut aussi vouloir développer sa propre méthode de formation. La sensibilisation peut se faire au moyen de supports variés (guide, livret, affichage, écran de mise en garde, tapis de souris…).

2.5.3 L'implication de la DRH, de la DSI et des correspondants sécurité

Le RSSI seul ne peut réussir à mettre en place et maintenir une politique de sécurité pour l'ensemble du groupe. Pour cela, il doit disposer de « relais » opérationnels dans chaque branche métier et dans chaque filiale.

Le bon fonctionnement au quotidien implique également une bonne coopération avec la direction des ressources humaines pour ce qui concerne l'authentification et la gestion des droits d'accès et une bonne collaboration avec la direction des systèmes d'information pour tout ce qui a trait à l'intégrité, la confidentialité et la disponibilité du SI.

2.6 L'administration de la sécurité

L'administration de la sécurité est une tâche complexe, car le responsable sécurité doit appréhender de manière globale et centralisée des risques localisés, enfouis ou diffus (intrusions, virus…).

L'administration implique à la fois des tâches opérationnelles et des tâches de management. L'administrateur doit chercher à automatiser au maximum les tâches opérationnelles pour pouvoir se consacrer davantage à ses fonctions de management, de contrôle et de supervision.

Cette administration se fait souvent par le biais de solutions d'administration système (Bullsoft, CA, Tivoli et HP) ou réseau (Checkpoint, Nortel) du marché intégrant des modules de gestion de la sécurité. Ces solutions fournissent à l'administrateur des remontées d'alerte qui lui permettent d'établir des tableaux de bord.

L'administration de la sécurité se compose de plusieurs éléments :

- la gestion des droits d'accès, l'identification et l'authentification des utilisateurs sur les différentes plates-formes ;
- la configuration et l'administration des équipements réseaux et système ;
- la supervision du réseau (surveillance du réseau, surveillance des anomalies et intrusions, mise en place du plan de secours) ;
- dans un souci de séparation des tâches doivent être effectués par des personnes différentes.

Les principales difficultés auxquelles se heurte l'administrateur sont les suivantes :

- les offres ne prévoient pas toujours la gestion unifiée des droits d'accès ;
- les offres ne prennent pas systématiquement en compte les utilisateurs distants ;
- les offres ne prennent pas systématiquement en compte le format X509 ;
- les outils d'administration génèrent parfois la remontée de fausses alertes ;
- les outils d'administration génèrent parfois des alarmes difficiles à interpréter ;
- l'administrateur manque souvent de temps pour analyser les *logs* fournis ;
- l'administrateur manque aussi d'un référentiel interentreprises pour comparer les données recueillies dans un même secteur d'activité.

2.6.1 Retour d'expérience de La Poste sur la gestion des droits d'accès

L'expérience montre que la gestion des droits d'accès (qui a accès à quoi dans l'entreprise ?) n'est pas optimale. En effet, un certain nombre de carences existent :

- l'accès est souvent attribué sans véritable processus d'approbation ;

- les niveaux d'accès sont souvent plus élevés que nécessaire ;
- l'accès n'est pas systématiquement révisé en cas de mutation ;
- l'accès n'est pas systématiquement supprimé en cas de départ.

Par ailleurs, les propriétaires de données ne jouent pas toujours un rôle actif dans le processus de contrôle et ne font pas de *reporting* régulier.

Côté utilisateurs, les procédures d'administration des accès ne sont pas toujours connues et les délais d'obtention des mots de passe sont parfois élevés. Enfin, les procédures peuvent être manuelles et varier d'un métier à un autre ou d'un site à un autre.

La gestion des droits d'accès suppose au préalable une classification de l'information selon son degré de sensibilité (normale, confidentielle...). Ce contrôle est du ressort des directions métiers. Le niveau de contrôle sur l'information se fait à deux niveaux : d'une part un contrôle de base, d'autre part un contrôle « renforcé » pour les informations sensibles. Enfin, il faut prévoir un mécanisme de dérogation au contrôle, mais celui-ci doit être le plus limité possible.

La gestion des droits d'accès suppose également une étroite collaboration entre la DSI et la DRH pour gérer les droits d'accès du salarié le plus finement possible (arrivée, mouvement, départ).

Il faut bien voir que la gestion des droits d'accès peut aussi se faire avec un outil séparé de la solution d'administration.

Les attentes des administrateurs en matière d'outil de gestion d'accès sont les suivants :

- automatisation du processus de demande d'accès ;
- automatisation du processus d'approbation des demandes ;
- authentification des approbateurs ;
- suivi en ligne des demandes en cours ;
- utilisation de profils pour accélérer le processus de demande d'accès ;
- base de données indiquant qui a accès à quoi ;
- lien avec les bases RH.

Mais le choix d'un outil ne dispense pas de mettre en place des procédures et un partage des tâches entre l'administrateur, les métiers et les ressources humaines.

2.6.2 L'authentification

L'accès à l'information suppose au préalable l'authentification de la personne. Celle-ci permet de filtrer l'accès à la ressource. Généralement, l'authentification se fait soit par le biais :

- d'une combinaison chiffrée (mot de passe, PIN) ;
- d'un objet (carte à puce, jeton, certificat) ;
- des caractéristiques physiques de la personne (empreinte vocale, digitale, rétinienne).

Les différents systèmes d'authentification existants sont le mot de passe, le mot de passe à usage unique (*One Time Password*), l'authentifiant unique (*Single Sign On*), le certificat (PKI), la biométrie.

Les certificats peuvent être basés sur des cartes à puce. Les mots de passe numériques sont souvent calculés sur une calculette appelée jeton ou *token*.

Le système d'authentification le plus utilisé reste le mot de passe. En moyenne, chaque salarié possède entre 3 et 5 mots de passe. Viennent ensuite l'authentifiant unique, puis la carte à puce et le jeton. Plus récemment, les certificats à clé publique ont fait leur entrée dans le monde de l'entreprise, mais leur usage reste encore relativement confidentiel et les projets restent pour l'instant des projets pilotes, à petite échelle. Mais là aussi des changements sont susceptibles d'intervenir dans les prochains mois en raison des projets d'approvisionnement en ligne et de places de marché qui se développent chez les grands comptes. En revanche, la biométrie n'est quasiment pas utilisée aujourd'hui en entreprise.

Les principaux risques liés à l'authentification sont :

- l'usurpation d'identité ;
- l'absence de répudiation ;
- le craquage des mots de passe ;
- le vol ou la perte de l'authentifiant (mot de passe, carte à puce, jeton ou certificat).

L'authentification doit répondre à trois exigences contradictoires :

- l'administration doit être le plus simple possible pour l'administrateur (demande, gestion, distribution, révocation) ;
- l'utilisation doit être le plus simple possible pour l'utilisateur (mot de passe mémorisable, stockage...) ;
- la sécurité doit malgré tout être garantie pour éviter tout risque de vol ou de craquage de la part d'un *hacker* (structure, longueur du mot de passe, périodicité, stockage des clés...).

		Avantages	Inconvénients
Ce que je connais	Mot de passe	- peu coûteux	- vol, perte et oubli, *post-it* - souvent craquable - partageable
	Single Sign On	- accès unifié et facilité à mémoriser - administration simplifiée	- coût - vol, perte - pas d'accès « universel » - durée de mise en place du projet - formation des administrateurs
Ce que je possède	Carte à puce	- réflexe « carte bleue » - support pour les PKI	- faible taux d'équipement PC en lecteur carte à puce - vol, perte, oubli du code
	Jeton (*token*)	- mot de passe aléatoire - *one time password*	- coût - pérennité ? - vol, perte
	Certificat (PKI)	- multi-usages - multi-supports	- pas encore de gestion des habilitations applicatives - administration et stockage des clés
Ce que je suis	Biométrie	- identifie la personne - non falsifiable - fiabilité élevée	- saisie lente et contraignante - faible taux d'équipement - coûteux

Source : Cigref

Figure 7 : Avantages et inconvénients des différentes solutions d'authentification.

2.6.3 L'accès distant

On peut définir l'accès distant comme un accès depuis l'extérieur aux ressources internes du réseau d'entreprise. L'accès se fait *via* une connexion non permanente, établie physiquement ou logiquement en début de session. Les informations transitent partiellement ou totalement *via* le réseau public (RTC, RNIS, GSM, Internet).

Les principaux enjeux en matière d'accès distant sont :

- la maîtrise de la qualité de service : le nombre et les exigences des utilisateurs distants augmentent alors que les débits offerts restent faibles (56,6 kb/s en RTC dans le meilleur des cas) ;
- la maîtrise des coûts : elle passe notamment par un meilleur contrôle des communications téléphoniques ;
- la maîtrise de la sécurité : elle passe par l'authentification et le contrôle d'accès, la confidentialité, l'intégrité des informations échangées et la traçabilité des accès.

L'accès distant permet de répondre à un certain nombre de besoins tels que :

- le nomadisme : utilisateurs, administrateurs ;
- le télétravail à domicile ;
- le raccordement de « petits » sites ;
- l'accès de tierces personnes : fournisseurs, partenaires, clients.

Les ressources demandées par les utilisateurs distants sont généralement bien identifiées :

- l'accès à la messagerie d'entreprise ;
- l'accès à l'intranet / internet ;
- l'accès au SI de gestion et de pilotage.

Les risques liés à l'accès distant sont le vol de mot de passe (*packet sniffing*), le vol de données (*data theft*), l'altération de données (*data alteration*), l'usurpation d'identité (*identity spoofing*).

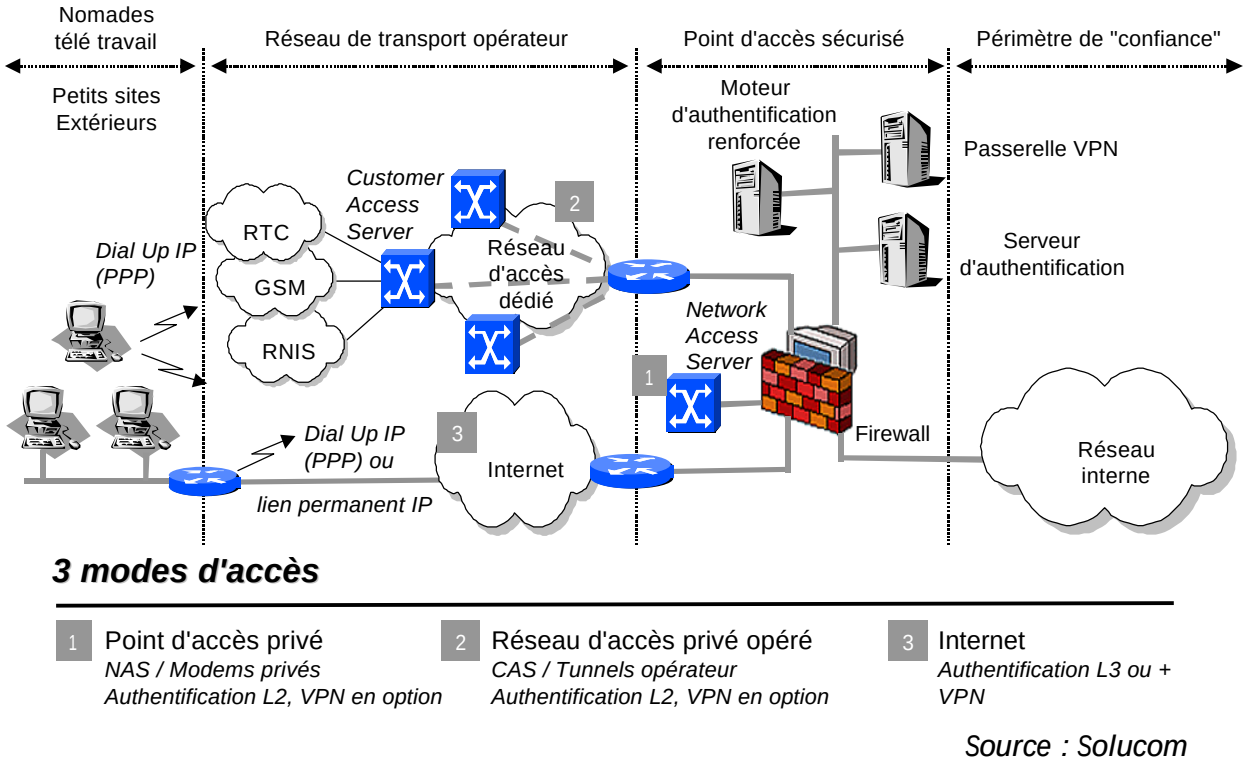


Figure 8 : Quels modes d'accès distants au système d'information de l'entreprise ?

La sécurité est assurée par plusieurs « barrières » :

- la connexion n'est que temporaire ;
- l'accès est limité à certaines ressources ;
- l'authentification se fait *via* un mot de passe statique ou dynamique, un jeton ou une carte à puce ;
- une base d'authentification ou un serveur d'authentification renforcé (Radius, Tacacs+) permet de vérifier l'identité de la personne connectée ;
- un réseau privé virtuel d'opérateur assure le chiffrement de la liaison point à point.

L'accès au SI de l'entreprise peut se faire de trois manières :

- *via* un point d'accès privé ;
- *via* un réseau d'accès privé opéré (RPV) ;
- *via* internet.

Les réseaux privés virtuels d'opérateurs permettent l'accès distant sécurisé aux informations de l'entreprise par le biais d'une infrastructure partagée ou publique. Le RPV constitue en quelque sorte une « privatisation» partielle du réseau public. Un RPV est

construit soit directement sur internet, soit sur l'infrastructure d'un opérateur (IP, ATM, *Frame Relay*).

Le RPV peut être réalisé sous deux formes :

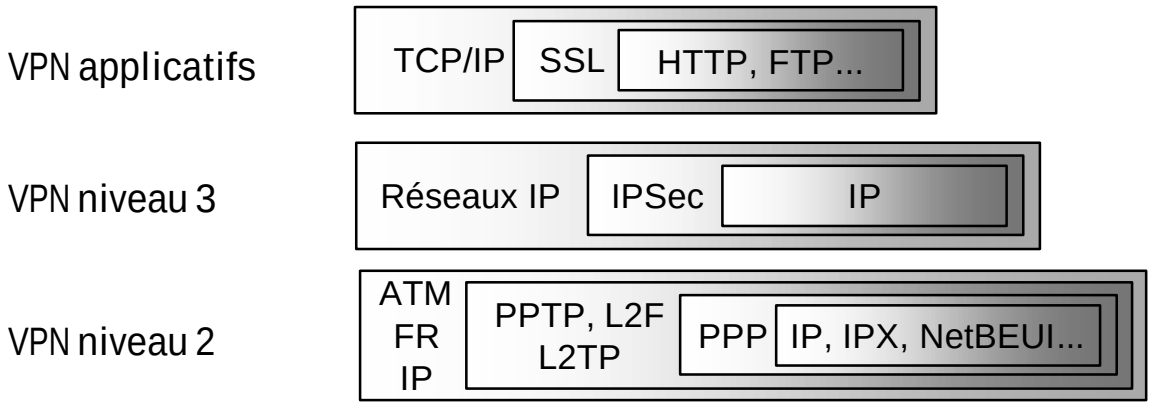
- le mode transport : pas de modification de l'entête de la trame du paquet ;
- le mode tunnel : encapsulation selon un protocole de *tunneling*.

On peut classer les RPV selon leurs usages :

- les RPV d'accès ;
- les RPV Intranet ;
- les RPV Extranet ;
- les RPV Voix ;
- les RPV Voix / Données / Multimédia.

On peut aussi dresser une typologie des RPV selon leur niveau Iso. On trouve alors :

- les RPV de niveau 2 ;
- les RPV de niveau 3 ;
- les RPV applicatifs.



Source : Solucom

Figure 9 : Typologie des réseaux privés virtuels.

Les RPV de niveau 2 reposent soit sur le protocole PPTP soit sur le protocole L2TP. (le protocole L2TF a été abandonné). PPTP (*Point To Point Tunneling Protocol*) est un protocole qui a été développé par Microsoft, 3Com, Ascend et a été normalisé par l'IETF (RFC 2637). Ce protocole est largement répandu, du fait de

la large présence de Microsoft en entrepirse. L2TP (*Layer 2 Tunneling Protocol*) a été normalisé par l'IETF (RFC 2661). Il permet l'établissement de tunnels de bout en bout, à travers le réseau de l'opérateur. Il est recommandé d'utiliser IPSec en complément pour protéger le tunnel.

Les RPV de niveau 3 reposent sur le protocole IPSec. IPSec est une norme de l'IETF, dont la première version date de 1995. Une version améliorée est sortie fin 1998 (gestion dynamique des clés). IPSec existe en mode tunnel (RFC 2401) et en mode transport (RFC 2402, 2406). L'authentification se fait *via* MD5 ou SHA, le chiffrement avec du DES ou du 3-DES. La gestion des clés se fait via IKE (*Internet Key Exchange*, RFC 2407).

Les RPV de niveau applicatif reposent sur SSL. Le RPV applicatif repose sur un serveur mandataire (*proxy*) au niveau du point d'accès. SSL (*Secure Socket Layer*) est un protocole développé à l'origine par Netscape pour sécuriser toutes les communications sur internet. SSL s'interpose entre le protocole TCP/IP et les protocoles applicatifs (HTTP, FTP, Telnet...) qu'il sécurise ainsi. SSL a été normalisé par l'IETF sous la dénomination TLS (*Transport layer Protocol*), RFC 2246. Il utilise les algorithmes RSA et MD5. En matière de chiffrement, il utilise RC2, RC4, DES ou 3DES. SSL supporte les certificats X509. SSL est utilisé dans le cadre de HTTP-S.

Les offres d'opérateurs de RPV sont nombreuses. On peut citer notamment celles de Cegetel (Service PC Itinérant), Equant (PPP Dial Access), Siris (Nomadia), Transpac (Global Intranet Accès Commutés), Global One, Worldcom, ISDNet, Infonet, BT, Cable & Wireless...

2.6.4 Retour d'expérience de la Française des Jeux sur l'accès distant

La Française des Jeux regroupe 700 personnes réparties sur 3 sites. Le nombre d'utilisateurs distants est resté jusqu'à présent relativement faible (30 personnes) mais risque d'augmenter du fait du passage au 35 heures. Ces nomades sont soit des informaticiens d'astreinte, soit des responsables régionaux.

L'architecture initiale se composait d'un accès distant *via* RTC au travers de trois serveurs d'accès distant qui géraient localement les accès et les mots de passe. Un système de *call back* (rétro-appel) permet d'identifier l'utilisateur. Cette solution présentait un certain nombre d'inconvénients : le système du *call back* limitant la mobilité du nomade et l'obligeant à se connecter toujours à partir d'un même lieu. La gestion des utilisateurs ne se faisait que de manière locale et la traçabilité restait faible.

La Française des Jeux a choisi de faire évoluer cette architecture en rajoutant des serveurs d'authentification ACE (Security Dynamics) et ACS (Cisco), d'équiper les utilisateurs distants de cartes *token* (Secur ID) et de permettre l'accès *via* des numéros verts et de supprimer le mécanisme de *call back*. Security Dynamics a été choisi car il couvrait l'ensemble des plates-formes de la Française des Jeux.

La Française des Jeux envisage d'étendre cette solution d'authentification renforcée à l'ensemble des accès et des utilisateurs. Par ailleurs, l'entreprise pense faire évoluer les jetons vers des solutions de type cartes à puce mais juge que la technologie n'est pas encore suffisamment mûre.

2.7 Quelques conseils pour conclure

En résumé, il est souhaitable de respecter quelques recommandations simples en matière de politique de sécurité.

- Répertorier, classifier et protéger les sources d'information critiques de l'entreprise.
- Veiller à la confidentialité des informations sensibles à tous moments, y compris durant leur transport.
- Veiller à l'intégrité des informations critiques et de l'environnement informatique (sauvegarde, *back-up*, plan de secours).
- Séparer les tâches et les compétences pour les opérations sensibles.
- Identifier chaque utilisateur de manière unique et vérifiable.
- Choisir un mode de contrôle d'accès en fonction des besoins et de la criticité de l'information (mots de passe, SSO, jeton, carte à puce, PKI...).
- Auditer les évènements clés liés à la sécurité.
- Faire régulièrement des audits de réseau et des tests d'intrusion.
- S'abonner à une ou plusieurs lettres d'information et suivre régulièrement les forums de discussion sur les failles en matière de sécurité.
- Sensibiliser régulièrement le personnel.

En ce qui concerne plus particulièrement les risques liés à internet et à la messagerie, nous recommandons les mesures suivantes :

- Procéder à un inventaire des machines connectées directement sur le web.

- Mettre en place une zone démilitarisée (DMZ) entre internet et le réseau local.
- Prévoir deux antivirus d'éditeurs différents sur le poste client et sur le serveur.
- Mettre à jour régulièrement les versions de logiciels, de systèmes d'exploitation et les *patches*.
- Éviter autant que possible le recours à la télémaintenance.
- Changer régulièrement les mots de passe des utilisateurs.
- Ne pas installer d'exécutable sur les stations de travail.
- Chiffrer les mots de passe administrateur ou système.
- Chiffrer les sessions, les fichiers et les communications entre sites, voire de poste à poste.
- Fermer tous les ports internet non utilisés ou à risque (vidéo...).
- Utiliser un scanner interne de détection des ports.
- Conserver les journaux et faire régulièrement des analyses de *log*.
- Développer, si nécessaire, des outils pour surveiller et analyser les fichiers de *logs* ou les fichiers sensibles.

3. COMMENT SUIVRE ET ÉVALUER UNE POLITIQUE DE SÉCURITÉ ?

3.1 Le suivi de la politique de sécurité

Pour assurer le suivi, le responsable sécurité doit s'assurer :

- d'une part que l'analyse des informations de type *logs* est bien effectuée ;
- d'autre part élaborer des indicateurs et des ratios lui permettant de se constituer une grille d'analyse et un instrument de pilotage efficace du SI de l'entreprise.

3.1.1 *L'analyse des* logs

L'analyse et la conservation des *logs* est impérative pour le responsable sécurité, à deux titres :

- d'une part, elle lui permet de connaître l'origine, la date et la nature de l'attaque subie ;
- d'autre part, elle peut constituer un début de preuve juridique en cas de contentieux ou de procès.

Mais très souvent, faute de ressources, le responsable sécurité n'a pas les moyens en temps d'analyser les remontées de *logs*.

3.1.2 *La mise en place de tableaux de bord*

La mise en place d'un tableau de bord est nécessaire pour plusieurs raisons. Il permet en effet de :

- disposer d'un outil de pilotage ;
- avoir une vision comparative dans le temps et dans l'espace ;
- justifier les plans d'actions et le budget.

Le tableau de bord peut avoir soit un but opérationnel, soit un but stratégique. La vocation d'un tableau de bord opérationnel est de fournir des indicateurs qualitatifs ou quantitatifs immédiatement utilisables par le responsable sécurité, le correspondant sécurité ou la DSI. Au contraire, la vocation d'un tableau de bord stratégique est de fournir des indicateurs permettant d'évaluer le risque informatique par rapport aux autres risques de l'entreprise (pour le *risk manager*), d'évaluer les écarts entre les objectifs et les résultats (pour l'audit) ou de dresser un bilan coûts/avantages de la politique de sécurité (pour la direction générale).

La méthode à suivre est la suivante :

- validation des indicateurs proposés par le pôle sécurité ;
- mise en œuvre ;
- exploitation des résultats.

Il ne suffit pas de créer une fois un tableau de bord, encore faut-il l'alimenter et le publier régulièrement. La périodicité pour un tableau de bord opérationnel peut être mensuelle. Un tableau de bord stratégique peut en revanche avoir une périodicité moins élevée et être publié sur une base trimestrielle, semestrielle ou annuelle.

Les indicateurs utilisés peuvent être :

- quantitatifs ou qualitatifs ;
- quantifiables ou non ;
- financiers, RH, qualité, projet ;
- etc.

Les responsables sécurité peuvent s'appuyer sur des méthodes telles que BS7799, CSI Ipak ou Cobit en matière de management de la sécurité ou sur les méthodes Méhari ou Mélissa développées par le Clusif en matière de risques et de vulnérabilités.

Pour le tableau de bord opérationnel, on peut mettre en place des indicateurs par domaine :

1. disponibilité ;
2. intégrité ;
3. continuité ;
4. confidentialité ;
5. cloisonnement ;
6. « auditabilité ».

Remarque : Le thème des tableaux de bord a été rapidement abordé par le groupe de travail cette année. Nous traiterons ce sujet plus en détail l'an prochain.

	Quantifiable	Non quantifiable
Auditabilité	- Journaux (*logs*) - Tests de vulnérabilité	
Cloisonnement	- Licences (tests d'intrusion, gestion du filtrage/routage)	- Comportements individuels (modems pirates)
Continuité	- Contrat de *back-up* - Stockage des bandes - Assurance	- Charges & procédures de sauvegarde
Intégrité	- Licences (antivirus, gestion des accès et authentification)	- Gestion des mots de passe - Comportements individuels
Disponibilité	- Plan de secours - Sauvegardes - % information sauvegardée	- Erreur humaine
Confidentialité	- Sensibilisation - Contrôle d'accès physique et logique - Chiffrement - Ratio du nombre d'utilisateurs sécurisés par carte à puce - Ratio du nombre d'utilisateurs ayant une messagerie sécurisée - Ratio du nombre d'utilisateurs certifiés	- Comportements individuels

Sources : AP-HP et Cegetel

Figure 10 : Exemples d'indicateurs pour un tableau de bord.

3.2 L'évaluation de la politique de sécurité

L'efficacité d'une politique de sécurité repose sur son évaluation. L'évaluation peut être réalisée par des organismes de contrôle interne (audit) ou par des organismes de contrôle externes (cabinets de conseil, SSII). Cette évaluation doit de toute façon se faire à intervalle régulier, L'évaluation interne se fait par le biais d'une procédure d'audit classique (questionnaire...) tandis que l'évaluation externe se fera par le biais de tests d'intrusion.

3.2.1 L'évaluation interne : l'audit

Il existe deux types d'audits : l'audit technique et l'audit de gestion. Il ne sera ici question que de l'audit de gestion.

L'audit de gestion est un système d'évaluation *a posteriori* qui permet de mesurer l'écart entre le référentiel et la réalité, autrement dit, entre les objectifs fixés et les objectifs atteints en matière de sécurité.

L'audit a pour objectif de : vérifier la fiabilité de l'information fournie par les différents services, s'assurer de l'efficacité de la réalisation des tâches informatiques, contrôler le respect des politiques énoncées par la direction générale, consigner dans un rapport les remarques et les observations formulées.

L'audit s'inscrit souvent dans une démarche qualité (normes Iso 9000...).

L'audit peut porter sur plusieurs thèmes : l'organisation de la fonction informatique, l'architecture du SI, la bureautique, les télécommunications, la gestion du SI, la politique de sécurité...

L'audit se déroule généralement en trois phases : un examen préliminaire (prise de connaissance générale, recueil d'information, analyse préliminaire), une analyse approfondie (analyse et évaluation du contrôle, évaluation de l'efficacité...) et le rapport d'audit final (projet, commentaires, rédaction finale). L'audit se fait généralement sur la base d'un questionnaire et d'entretiens en face-à-face.

Cet audit de gestion peut s'accompagner d'un audit plus technique, combinant systèmes de détection d'intrusion, tests d'intrusion et scanners de vulnérabilité.

3.2.2 L'évaluation interne : les systèmes de détection d'intrusion

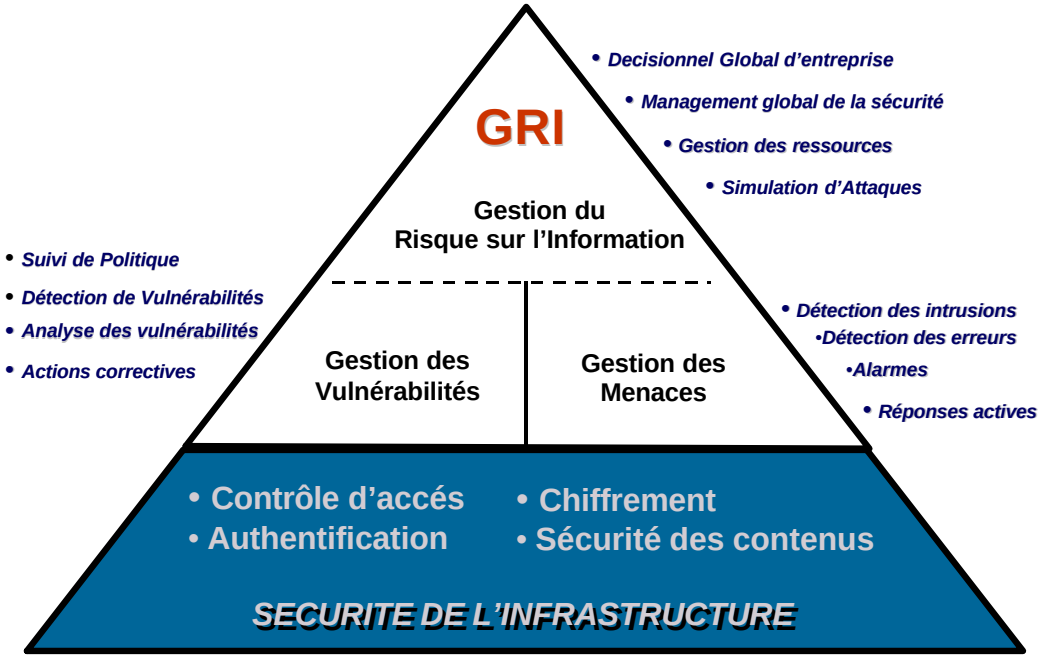
Les systèmes de détection d'intrusion (*Intrusion Detection System* ou IDS) sont des équipements analysant l'activité du réseau sur lequel ils sont connectés ou l'activité de la machine sur laquelle ils sont installés, afin de déceler :

- des signes d'intrusion (*intrusion detection*) : attaques provenant de l'extérieur ou de l'intérieur du réseau de l'entreprise ;
- des signes de violation (*misuse detection*) : attaques provenant d'utilisateurs outrepassant leurs droits.

Les risques liés à l'intrusion sont des risques de perte d'information, de pénétration et d'immobilisation du système d'information.

Quelle est la différence entre un IDS et un scanner de vulnérabilité ? Les scanners sont « proactifs » : ils aident à l'identification de vulnérabilités sur les systèmes et les réseaux. Les IDS sont réactifs : ils permettent d'enregistrer l'activité du

réseau ou d'une machine et d'identifier une attaque ou une tentative d'attaque afin de pouvoir réagir.



Source : ISS

Figure 11 : La gestion du risque sur l'information.

On distingue 4 grands types de systèmes de détection d'intrusion :

1. les *Network Based IDS* (basés sur le réseau) ;
2. les *Host Based IDS* (basés sur un serveur) ;
3. les *Application Based IDS* (basés sur une application) ;
4. les *Target Based IDS* (basés sur une cible).

Les Network Based IDS sont conçus pour s'interfacer et fonctionner avec la plupart des pare-feu (ISS par exemple s'interface avec Checkpoint).

Pour le choix, il est conseillé d'adopter des IDS « mixtes ». Mais aujourd'hui ces solutions sont rares. Actuellement seuls ISS,

Cybersafe et Axent proposent des offres mixtes de type « *network-based* » et « *host-based* ».

	Avantages	Inconvénients
Network Based IDS	- Facilité de déploiement dans un réseau - Complémentaires d'outils tels que les pare-feu, - Facilitent le suivi de la sécurité, - Vision générale du trafic réseau	- Limitation avec les débits des réseaux, - Détection uniquement des attaques connues, - Pas de prise en compte du comportement de la machine, vers laquelle sont destinés les paquets, - Inefficaces face à de bons "hackers" utilisant la technique de la fragmentation de paquets.
Host Based IDS	- Analyse précise du trafic arrivant sur la machine, - Analyse fine des données internes de la machine	- Pas de consolidation des informations entre IDS, - Portabilité - Surcharge du CPU.
Application Based IDS	- Analyse les données des fichiers d'une application précise	- Pas d'IDS Application-based disponible d'aujourd'hui
Target Based IDS	- Identification d'un Cheval de Troie, - Signature des fichiers et contrôle d'intégrité	- Peu voire pas d'IDS Target-based disponible d'aujourd'hui

Source : Ernst & Young

Figure 12 : Comparaison des différents systèmes de détection d'intrusion.

Un IDS se compose de 4 modules :

- un module d'analyse des données (*event analyser*) ;
- un module de sauvegarde des données (*event database*) ;
- un module de capture des données (*event generator*) ;
- un module de réponse (*response unit*).

Un IDS fonctionne soit sur une approche comportementale, soit sur une approche de type « scénario ».

- L'approche comportementale est basée sur la construction de profils d'utilisateur, puis sur comparaison entre l'activité réelle et le profil. Tout comportement déviant est considéré comme suspect. Les méthodes utilisées sont des méthodes statistiques, des méthodes à base de systèmes experts ou à base de réseaux de neurones...

- L'approche par scénarios repose sur la construction de scénarios d'attaques et la comparaison entre le scénario et l'audit. Les méthodes utilisées sont celles des systèmes experts, des algorithmes génétiques et du *pattern matching*.

	Avantages	**Inconvénients**
Approche comportementale	- Détection d'intrusion inconnue possible	- Définition d'un profil "moyen" difficile - Un utilisateur peut avoir un comportement "bizarre" en permanence - L'environnement peut se modifier brutalement - Un utilisateur peut changer de comportement
Approche par scénarios	- Prise en compte des comportements exacts des attaquants	- Mise à jour des scénarios - Base de règles délicate à construire - Seules les attaques scénarisées sont détectées

Source : Protection des Systèmes d'Information

Figure 13 : Avantages et inconvénients des méthodes de fonctionnement d'un système de détection d'intrusion.

Le traitement des données peut se faire soit en temps réel (*network based IDS*), soit en différé (*host-based*, *application-based* et *target-based IDS*).

Les IDS permettent de fournir :

- une analyse des signatures des attaques ;
- une analyse statistique ;
- une analyse d'intégrité.

Les IDS peuvent ensuite prendre des contre-mesures, par exemple modifier l'environnement utilisé lors de l'attaque, valider l'intégrité de l'IDS, générer une alarme en temps réel.

Où faut-il placer un IDS ? Les outils de détection d'intrusion peuvent être placés à différents endroits sur le réseau :

- devant ou derrière un pare-feu ;
- sur un routeur ;
- sur un *switch* ;
- sur un serveur ;
- sur une station.

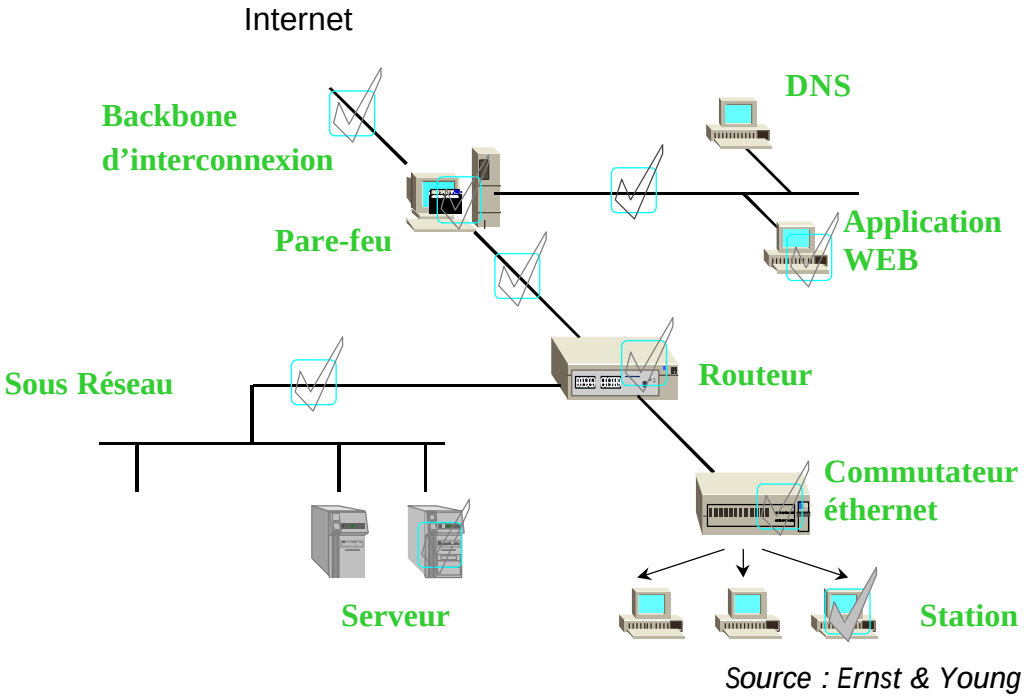


Figure 14 : Emplacements d'un système de détection d'intrusion sur le réseau.

Les critères à prendre en compte dans le choix d'un IDS sont :

1. une base de connaissance des attaques la plus complète possible et mise à jour fréquemment ;
2. une capture exhaustive du trafic réseau lorsque le débit augmente (plus de 100 Mb/s) ;
3. une configuration rapide ;
4. une administration facile ;
5. une bonne ergonomie ;
6. la possibilité d'exécuter une contre-mesure ;

7. la possibilité de générer des rapports simples ou exhaustifs, sous divers formats ;

8. un flux d'information chiffré et authentifié, entre la console et les agents ;

9. la stratégie à long terme du constructeur ;

10. le prix du produit.

Éditeurs	Produits
Axent	Omniguard Intruder Alert et NetProwler
Cisco	NetRanger Cisco Secure Intrusion Detection System
CyberSafe Corp	Centrax
Infostream	Watchdog
Internet Tools	ID Track
ISS	RealSecure
Network Associates Inc.	CyberCop Monitor
Network ICE Corp	BlackICE Defender et Entreprise Icepac
Network Security Wizards	Dragon
NFR Intrusion Detection Appliance	Network Flight Recorder

Source : Cigref

Figure 15 : Principaux outils de détection d'intrusion du marché.

Mais les outils de détection d'intrusion ne sont pas non plus des produits miracles. Ils présentent en effet un certain nombre de lacunes :

- les outils restent propriétaires (absence d'interopérabilité entre outils, comparaison des performances difficiles) ;
- les attaques sont parfois indétectables (envois de paquets altérés) ;
- les outils sont attaquables (module d'analyse, module d'archivage, module de contre-mesures) ;

- la preuve est difficile à établir devant un tribunal (recevabilité de la preuve, datation de l'événement).

Quelles sont les perspectives d'évolution des IDS ?

Les prochaines générations d'IDS vont intégrer des fonctions de CVE (*Common Vulnerability and Exposure*), d'analyse du trafic chiffré, de détection à haut débit (1Gb/s), de leurres et d'hameçons, de contre-mesures intelligentes vers la machine attaquante.

Les outils de détection d'intrusion devraient intégrer aussi des certificats X509 et un langage qui permette de développer ses propres signatures d'attaques.

Enfin l'interopérabilité entre les constructeurs devrait être améliorée (standards CIDF, OPSEC/CCI ou ANSA) et les rapports entre constructeurs consolidés ainsi que la possibilité de faire du traitement temps réel et temps différé.

3.2.3 Retour d'expérience d'axa sur les tests d'intrusion

Les tests d'intrusion ou tests de pénétration sont des actions d'évaluation visant à tester les vulnérabilités du SI sur un périmètre et sur une période donnée.

3.2.3.1 Quels sont les objectifs ?

Les objectifs d'un test de pénétration peuvent être de démontrer la vulnérabilité d'un système (approche de type « audit ») ou développer l'assurance dans la sécurité (approche de type « conseil »).

Il s'agit de tester l'étanchéité du dispositif en décelant les failles du système en vue de garantir la confidentialité, l'intégrité et la disponibilité des services.

La démarche de type « audit » n'implique pas la collaboration du personnel interne et suppose qu'aucune information sur le système à tester ne soit divulguée.

La démarche de type « conseil » implique la collaboration du personnel interne et la fourniture de renseignements concernant l'architecture du SI.

Mettre en place une procédure de tests d'intrusion oblige à se poser les questions suivantes :

- Quels sont les objectifs ?
- Qui sont les commanditaires (direction générale, audit ou DSI) ?

- Qui réalise les tests (tests en interne ou tests en externe) ?
- Quelle société choisir (entreprises avec label...) ?
- Quel type de test (test global, ciblé, informatique, télécoms...) ?
- Quelle méthode (à l'insu de l'équipe informatique ou de manière officielle) ?
- Quelle périodicité (tests épisodiques ou tests réguliers) ?
- Quelle garantie d'efficacité ?
- Quelle garantie de confidentialité (garantie contractuelle, charte, certification) ?
- Quel coût et quelle répartition des coûts ?

3.2.3.2 Quels sont les critères de choix ?

Les principaux critères à retenir dans le choix d'un prestataire sont les suivants :

- maîtrise des outils de test du marché ;
- existence d'un service de veille sur les vulnérabilités ;
- existence de moyens de tests et d'essais suffisants ;
- références clients ;
- certification (Iso 9000, BSI 7799, Cisa, fédération des professionnels de l'intrusion...) ;
- pas de réalisation de tests en avant-vente ;
- respect de règles déontologiques de base (non-destruction d'informations stockées, non-perturbation du service opérationnel, non-divulgation d'informations sensibles, « ménage » après les tests...) ;
- approche structurée et transparente des tests (lotissement) ;
- journalisation de l'ensemble des actions effectuées ;
- proposition de parades aux failles détectées ;
- engagement sur la composition de l'équipe intervenant (stabilité dans la composition, CDI, pas de sous-traitance non déclarée) ;
- accord de confidentialité consistant (divulgation limitée des informations relatives à la prestation).

3.2.4 L'auto-évaluation au quotidien : les scanners de vulnérabilité

Les scanners de vulnérabilité sont un bon complément aux IDS et aux tests d'intrusion. Ils permettent de surveiller les vulnérabilités en temps réel du réseau, du système, des applicatifs et des bases de données.

À la différence des systèmes de détection d'intrusion, les scanners de vulnérabilité sont actifs : ils aident à l'identification de vulnérabilités en temps réel sur les systèmes et les réseaux.

4. L'ÉVOLUTION DU CADRE TECHNOLOGIQUE EN MATIÈRE D'AUTHENTIFICATION

4.1 Les Public Key Infrastructures ou infrastructures de gestion de clé

L'infrastructure à clé publique IGC ou PKI en anglais) repose sur la cryptologie asymétrique. La cryptologie asymétrique fait appel à quatre éléments :

- une entité appelée « porteur de certificat » ;
- une clé publique ;
- une clé privée ;
- un certificat numérique.

Le certificat permet d'associer une clé publique à un « sujet », ce qui permet l'authentification de la personne.

Le certificat contient à la fois des informations sur le certificat, sur le porteur et sur l'autorité de certification. Le certificat repose actuellement sur la norme X509 v3.

Le stockage de la clé privée et du certificat se fait soit sur le serveur ou sur le PC, soit sur une carte à puce.

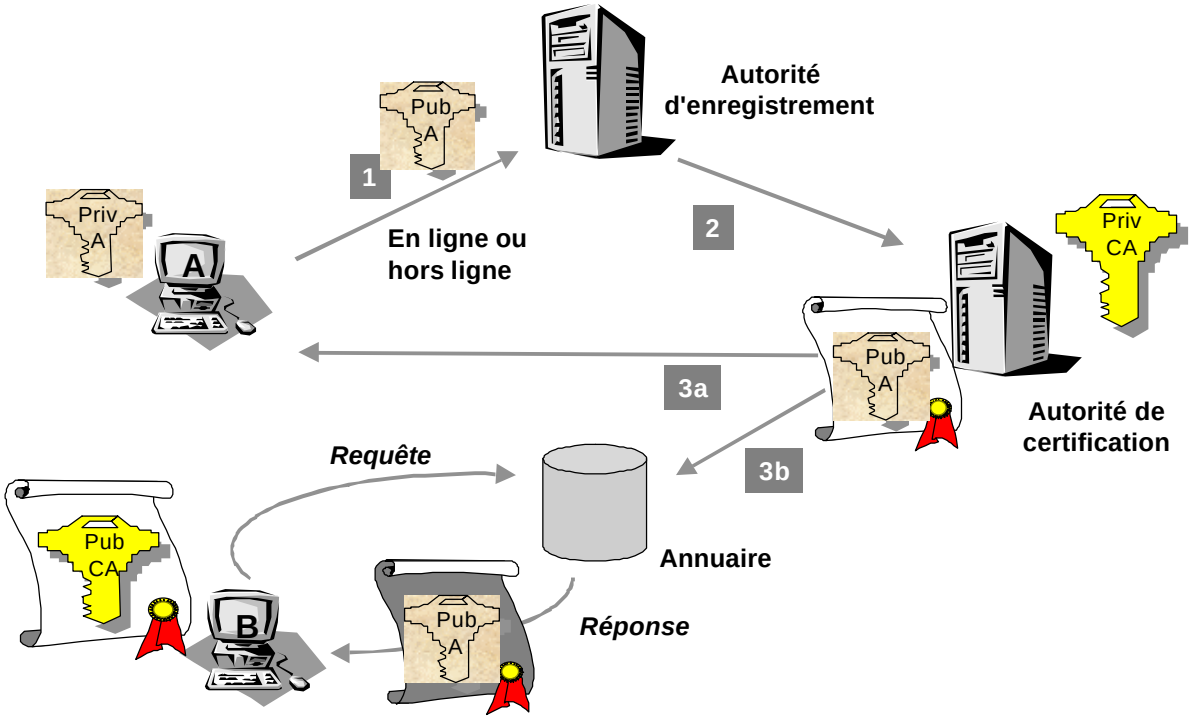
La PKI peut être gérée soit intégralement à l'intérieur de l'entreprise, soit partiellement externalisée auprès d'un opérateur de certification.

En mode externe, le processus de certification fait intervenir trois acteurs :

- l'autorité de certification (AC) – interne – ou *Certification Authority* (CA) qui fixe les règles et définit les critères requis pour obtenir un certificat ;
- l'autorité d'enregistrement (AE) – interne – ou *Registration Authority* (RA) qui vérifie et contrôle l'identité de l'individu et donne la clé publique et l'identité de l'individu à l'opérateur de certification ;
- l'opérateur de certification (externe) qui génère le certificat sous le contrôle de l'autorité de certification (AC).

En mode interne, le processus de certification ne requiert que deux acteurs :

- l'autorité d'enregistrement (AE) ou *Registration Authority* (RA) qui fixe les règles et définit les critères requis pour obtenir un certificat, collecte les informations nécessaires (identité du demandeur, clé publique...) et approuve les demandes, e) et les listes de révocation (*Certification Revocation List* ou CRL).
- l'opérateur de certification (interne) qui génère le certificat sous le contrôle de l'autorité de certification (AC).



Source : Solucom

Figure 16 : Mode de fonctionnement d'une PKI en interne.

L'infrastructure à clé publique (PKI) permet de garantir :

- l'authentification ;
- la confidentialité ;
- l'intégrité ;
- la non-répudiation.

La PKI peut être utilisée soit à l'intérieur de l'entreprise, soit entre l'entreprise et ses clients, ses partenaires et ses fournisseurs. Les usages (théoriques) de la PKI en environnement entreprise sont donc extrêmement variés :

- communications entre serveurs web et navigateurs ;
- messagerie (S/Mime) ;
- paiement sécurisé (SET, SSL) ;
- *B-to-B* ;
- *B-to-C* ;
- internet mobile (certificats sur téléphone mobile ou sur assistant numérique) ;
- internet et *Corporate Banking* ;
- Gestion de la chaîne logistique ;
- RPV et accès distant (IPSec / IKE).

PKI	Éditeurs
PKI interne	- Baltimore (Unicert) - Entrust (Entrust/PKI) - Lotus (Domino R5) - Microsoft (Windows 2000 PKI) - RSA Security (RSA Keon) - Sun / Netscape (Certificate Server) - Sagem
PKI externe	- GTE Cybertrust (racheté par Baltimore) - Certplus (Gemplus, FT, EADS, Verisign, CIBP) - Certinomis (La Poste, Sagem) - VeriSign (possède 15 % de Certplus) - Thawte (racheté par Verisign)

Source : Cigref

Figure 17 : Principaux acteurs dans le domaine de la PKI.

4.2 Retour d'expérience d'Amadeus sur les PKI

Amadeus a été créé en 1987 par quatre compagnies aériennes (Air France, Lufthansa, Iberia et SAS) et introduit en bourse en 1999.

La vocation d'Amadeus est de distribuer l'offre de fournisseurs du monde du voyage (compagnies aériennes, chaînes de location de voitures ou hôtelières principalement) aux agents de voyages ou aux agents de compagnies aériennes et plus récemment aux entreprises et aux voyageurs eux-mêmes.

Ses principaux concurrents sont les autres GDS (*Global Distribution System*) tels que Galileo ou l'américain Sabre.

Le système central d'information d'Amadeus situé dans la banlieue de Munich est un complexe constitué de plusieurs

dizaines d'unités centrales auxquelles sont raccordés plus de 250 000 terminaux *via* un réseau international privé constitué de multiples liens à haute vitesse.

Amadeus et ses quelques 70 filiales emploient environ 5 000 personnes, opérant dans 136 pays.

Fondamentalement, les PKI permettent de pourvoir à des besoins d'identification et d'authentification ainsi que de garantir la confidentialité et l'intégrité des donnés.

Elle peut également pourvoir à la non-répudiation (signature et accusé de réception) ainsi qu'à l'horodatage (moyennant le recours à un tiers de confiance).

Par contre, la PKI n'a pas vocation à répondre aux besoins d'autorisation (contrôle d'accès) même si au travers de ses services d'authentification elle constitue une base précieuse pour bâtir cette dernière. Enfin, elle ne protège pas des attaques de déni de service.

Amadeus s'est intéressé aux PKI il y a maintenant près de deux ans et a été amené a en mettre en place quatre différentes à ce jour :

- Lotus Notes et sa PKI propriétaire intégrée ;
- Secude (seule PKI initialement homologuée SAP) ;
- PKI basée sur MS - CS (Microsoft Certificate Server) ;
- PKI Domino 5 et sa PKI intégrée.

Les deux dernières ont fait l'objet de développement en interne. Ces PKI ont été utilisées en environnement *B-to-C* ou *B-to-E (Business-to-Employee)*. Ceux sont des PKI privées et non hiérarchisées.

Amadeus a tiré les leçons suivantes de son expérience en matière de PKI :

- grâce aux plates-formes disponibles sur le marché, la génération de certificats est facile. C'est la construction de la PKI qui est difficile...
- la technologie ne représente que 20 % du travail, le reste concerne l'organisation, les procédures, la définition de rôles ;
- c'est un projet structurant : il faut définir précisément l'organisation, qui fait quoi, qui a accès à quoi ;
- la tenue à jour du répertoire de tous les utilisateurs n'est pas le moindre des problèmes.

Mais les problèmes non encore abordés restent encore nombreux :

- échanges inter PKI ;
- accès au répertoires mutuels ;
- compatibilité des PSC ;
- PKI hiérarchisée ;
- chaînage des certificats ;
- utilisation pour le courrier électronique ;
- gestion des clés de signature (aspect juridiques) ;
- gestion du cycle de vie complet des certificats (renouvellement, recouvrement...) ;
- l'intégration dans de multipleS applications et clients ;
- la gestion de grandes quantités de certificats.

4.3 La problématique de l'externalisation

La question de l'externalisation de la PKI auprès d'un opérateur de certification peut se poser. En effet, l'entreprise peut décider soit de gérer intégralement en interne les certificats et d'être sa propre autorité de certification, soit de confier la production de certificats ou la fourniture de services de certification à des prestataires externes.

Cette décision dépendra de la taille de l'entreprise, de la taille du projet, du calendrier, du montant du budget, du savoir-faire développé par l'entreprise, de sa culture d'entreprise et du degré de confiance accordé à l'autorité de certification (pérennité de l'entreprise, coût des solutions, moyens de sécurité mis en œuvre...).

En résumé, les usages de la PKI sont pour l'instant essentiellement internes et pour des projets de petite envergure. Le déploiement d'une PKI à grande échelle en entreprise s'avère un projet réellement structurant, qui implique une réflexion organisationnelle relativement poussée. Pourtant, les projets sont surtout réalisés à l'étranger, même si des projets nationaux de plus grande envergure commencent à apparaître dans les administrations (ministère des finances, ministère de l'éducation nationale) et dans les grandes entreprises.

Banque et Assurance	ABN Amro, Bank of England, Bank of Ireland, NatWest, BBS, APCA, The Chase Manhattan Bank, New York Life, Mackenzie Financial, Bank of Bermuda, Scotiabank, Axa (projet), CDC (projet), MMA (projet)
Gouvernement	UK Ministry of Defence, Australian Tax Office, Australian Payments Clearing Association (APCA), NI NHS, MIPEX, European Commission, Dept of Foreign Affairs, Quebec Ministry of Justice, ministère de l'éducation nationale, ministère des finances (projet), Cnav (projet)
Industrie	**Aerospatiale Matra** (projet), **France Télécom** (projet en interne)
Poste	Royal Mail, Universal Postal Union, Uruguay Post, PTT Post – KeyMail, La Poste (projet)
Réseaux de commerce électronique	GEIS, TradeLink (Hong Kong), TradeVan (Taiwan), EDI (Malaysia), NETS (Singapore), IBM
Santé	Liberalis (Réseau Santé FT)
SSII	Perot Systems
Tiers de confiance	PTT Post, Belgacom, Telenor, Alphatrust, KMD, ID.Safe,
Transports et tourisme	Amadeus

Source : Cigref et éditeurs

Figure 18 : Principaux retours d'expérience et projets connus en matière de PKI.

5. L'ÉVOLUTION DU CADRE JURIDIQUE DE LA SÉCURITÉ

Les principales obligations légales et réglementaires en matière de SI concernent la protection des informations nominatives, la protection de la propriété intellectuelle, la fraude informatique, la cryptologie, le secret des communications, l'archivage des documents magnétiques. Les obligations contractuelles des entreprises portent sur les contrats de travail et les contrats de service (clauses de confidentialité).

Les membres du groupe ont surtout travaillé sur la réglementation en matière de chiffrement, de signature électronique et de protection des données personnelles.

Le droit national et communautaire en matière de sécurité informatique et de commerce électronique est un droit en pleine mutation qui a connu de nombreux changements au cours de ces deux dernières années. Ainsi, la France a connu une double réforme avec :

- le décret du 17 mars 1999 sur la réforme du régime juridique des moyens de cryptographie ;
- la loi du 13 mars 2000 sur la signature électronique et les documents électroniques.

La question du respect de la vie privée et de l'exploitation des données personnelles est aussi un thème qui a des incidences en matière de sécurité.

5.1 L'évolution de la réglementation sur la signature électronique

La signature électronique s'inscrit dans la même problématique que les PKI, car elle repose sur la notion de certificats.

5.1.1 Le cadre juridique communautaire

Une position commune a été arrêtée par le Conseil le 28 juin 1999 et la directive a été adopté par le Parlement européen le 13 décembre 1999.

D'après cette directive, la signature électronique a la même valeur juridique que la signature manuscrite et on ne peut pas invoquer la non-validité de la signature électronique pour refuser la transaction. Les annexes 2 et 3 présentent les systèmes de signature avancée (l'annexe 2 parle de la certification et l'annexe 3 des conditions sur la signature).

5.1.2 La situation dans les autres pays communautaires

La plupart des pays membres de l'Union européenne ont élaboré une loi sur la signature électronique, soit antérieurement, soit postérieurement à la directive communautaire de 1998.

La circulaire du 9 décembre 1999 prévoit une procédure de notification de la Commission par les états membres pour tout projet de textes relatifs aux services de la société de l'information.

En juin 2000, les pays ayant notifié leurs projets relatifs à la signature électronique étaient selon le ministère de la justice : l'Allemagne, l'Autriche, la Belgique, l'Espagne, la Grèce, l'Irlande, l'Italie et le Luxembourg.

Selon le ministère, l'Allemagne, l'Italie, la France et l'Autriche sont les seuls pays qui définissent dans leur loi nationale le régime juridique de la signature électronique. Les projets espagnols, luxembourgeois et belge visent toutes les formes de signature électronique mais ils ne leur reconnaissent pas à toutes la même valeur juridique.

1. L'Autriche a un projet de loi fédérale sur les signatures électroniques et un projet de règlement. L'objet du projet de loi est de définir un cadre légal pour la création et l'emploi de signature électronique. La loi fédérale serait applicable à des systèmes fermés et dans les échanges électroniques ouverts avec les tribunaux et les administrations, sauf dispositions contraires. Les effets juridiques dépendent du niveau de sécurité et des classes de certificat employées (certificat qualifié ou non). Il n'y a pas de régime d'autorisation préalable mais un régime de déclaration auprès de la commission Telekom Control, organisme de contrôle chargé de la mise à jour de la liste des certificats valides et révoqués. Le Telekom Kontrol assiste l'organisme de contrôle pour le contrôle des prestataires de services de certification (PSC) et des produits. Il enregistre les PSC dès leur déclaration d'activité, tient les listes de certificats pour les PSC et assure un service de révocation dans le cas de l'arrêt ou de l'interdiction d'activité d'un PSC.

2. L'Allemagne a édicté une loi antérieure à la directive européenne sur la signature électronique. L'Allemagne a donc cherché à actualiser ses textes nationaux au regard de la directive européenne, notamment sur les critères communs de contrôle et d'évaluation de la sécurité des techniques de l'information. La reconnaissance et l'application de ces critères communs constituent le préalable à une utilisation élargie des signatures électroniques au niveau international.

3. La Belgique a notifié à la commission le 10 février 2000 un projet de loi relatif à l'activité des PSC. Le projet de loi pose le principe de la neutralité technologique, de l'accréditation volontaire et définit l'effet juridique de la signature électronique. Le PSC est libre de demander ou non l'accréditation. Les personnes physiques et morales sont libres d'utiliser une signature électronique ou manuscrite et de recourir à un PSC accrédité ou non. Le projet de loi introduit la reconnaissance juridique des signatures électroniques avancées et organise le régime juridique des PSC, leur contrôle et le mode de sanction.

4. L'Espagne a elle aussi un projet de loi et un projet de règlement relatif à la signature électronique. Le projet de loi prévoit un régime de libre concurrence, l'emploi de la signature électronique dans les administrations publiques et un système d'accréditation volontaire. Un registre public des PSC sera crée au ministère de la justice. L'inspection et le contrôle de l'activité des PSC seront effectués par le ministère des travaux publics. Le projet de loi énonce aussi les infractions et les sanctions. Le projet de décret précise que l'organisme compétent en matière d'accréditation et de certification est le ministère des travaux publics. L'évaluation des PSC et des produits se fera par le biais d'organismes publics ou privés accrédités, indépendants des PSC.

5. L'Irlande a publié dès juin 1998 un livre blanc sur les signatures électroniques et la cryptologie. Ce livre blanc énonçait des principes généraux tels que la liberté de production, d'importation et d'utilisation de la cryptologie pour assurer l'intégrité et la confidentialité des échanges et proposait que les signatures, contrats et documents électroniques aient pleine valeur juridique. Le *Electronic Commerce Act* de 1999 préfigure les dispositions de la directive sur la signature électronique. Cette loi reconnaît la validité juridique des signatures électroniques, des signatures électroniques avancées et des documents électroniques à l'exception des testaments, actes de propriété et actes judiciaires. La loi ne prévoit pas d'autorisation préalable des PSC. Elle prévoit par contre la reconnaissance mutuelle et définit la responsabilité des PSC.

6. En Italie la loi du 15 mars 1997 et le décret du 10 novembre 1997 prévoient le dispositif de la signature numérique et lui accorde la même valeur qu'à la signature manuelle. Elle peut être authentifiée par un officier ministériel. Le décret du 8 février 1999 énonce les modalités techniques et définit les conditions d'agrément des PSC. Les PSC sont des sociétés par action dont le capital social est au moins égal à celui exigé

pour les établissements financiers. L'organisme de contrôle, créé en 1993, vérifie que les PSC remplissent les conditions requises. Le délai de conservation des clés publiques par les PSC est d'au moins 10 ans.

7. Le Luxembourg a un projet de loi sur le commerce électronique. Ce projet aura des répercussions sur le code civil, le nouveau code de procédure civile, le code pénal et le code de commerce. Le projet de loi traite des services internet, des services financiers, des communications commerciales, des contrats électroniques, des paiements électroniques et des signatures électroniques. Le titre II de la loi aborde le régime de la preuve et de la signature. L'accréditation, l'octroi, le retrait des licences et la surveillance relèvent de la compétence du ministère de l'économie. L'accréditation est facultative. Les PSC sont tenus au respect du secret professionnel et à la protection des données à caractère personnel. Les PSC émettant des certificats qualifiés sont tenus à des obligations de vérification des informations et à la reconnaissance des certificats émis par les pays tiers.

5.1.3 Le cadre juridique national

D'après la loi française du 13 mars 2000, la signature électronique a la même valeur juridique que la signature manuscrite. Les articles 1316 et 1317 du code civil ont été modifiés en conséquence. Les décrets d'application ne sont toujours pas sortis en France. Le gouvernement a lancé un appel à commentaire sur le projet de décret jusqu'au 15 septembre 2000. Le décret devrait sortir d'ici la fin de l'année.

Quels sont les usages possibles de la signature électronique ? La signature électronique peut être utilisée en interne ou en externe, pour la signature de courrier électronique ou de contrat, dans des relations de type *B-to-C* ou *B-to-B*.

Quels sont les risques liés à la signature électronique ? Les risques sont que la signature électronique soit fausse, principalement au niveau de l'association « entité-clé publique ». D'où l'intérêt d'avoir un bon certificat. Mais le risque de fausse signature existe aussi dans le hors ligne. La signature manuscrite est même presque plus facile à falsifier que la signature électronique ! Il ne faudrait pas donc que l'on demande aujourd'hui davantage de garanties sur internet que dans la vie des affaires hors ligne.

5.2 Vie privée et protection des données personnelles

Deux textes concernent la protection de la vie privée face à la collecte de données personnelles :

- la loi informatique et libertés du 6 janvier 1978 ;
- la directive communautaire du 24 octobre 1995.

La directive communautaire de 1995 oblige la société qui détient les informations sur une personne à l'informer lorsqu'elle revend ce fichier à une autre entreprise. Aujourd'hui, le droit de collecte et de traitement des données personnelles est libre, à condition que le fichier soit déclaré à la Cnil[3] (la ou les finalités du fichier doivent être précisées dans la déclaration).

On distingue deux catégories de personnes : les clients et les prospects.

Pour les clients, la collecte de certaines données est interdite (celles concernant les origines ethniques, les pratiques religieuses, les pratiques sexuelles, les convictions politiques et philosophiques). Les autres données peuvent être collectées mais ne peuvent pas être recoupées avec des données permettant l'identification ou exportées vers des pays où le niveau de protection du consommateur est moindre (principe du « *Safe Harbour* »).

Pour le prospect, la directive de 1995 impose le respect des conditions suivantes : principe de finalité (art.6 de la directive), consentement indubitable (art. 7f de la directive), information préalable (art. 10 et 11 de la directive), droit d'opposition (article 11).

Les intéressés doivent être informés de l'existence de ce fichier (depuis la directive) et ont un droit de rectification des données, mais uniquement si les données sont erronées ou fausses.

Le droit français ne prévoyait pas (avant la directive) de droit d'opposition absolu de la part de la personne « fichée » en cas de revente du fichier. En revanche, la directive communautaire prévoit ce droit d'opposition absolue en matière de prospection commerciale. La directive n'a pas encore été transcrite mais elle est invocable en droit interne.

Le champ d'application de la loi française est le suivant : toutes les données collectées en France, même si elles sont traitées ensuite à l'étranger, sont soumises à la législation française.

[3] Les intranets d'entreprise doivent aussi être déclarés à la Cnil.

Dans le cadre de transfert de données hors de la Communauté européenne, la directive autorise le transfert du fichier vers un pays tiers si les personnes concernées sont préalablement informées et si le pays tiers présente un niveau équivalent de protection.

Dans la pratique, la Cnil n'a pas toujours les moyens de sa mission. Une solution qui tend à se développer est l'élaboration de codes de conduite de la part des entreprises étrangères basées en France (IBM par exemple).

Les questions qui restent en suspens aujourd'hui sont :

- l'application concrète du principe de *Safe Harbour* entre les États-Unis et l'Europe ;
- la collecte dans les annuaires ;
- les frontières de l'information du consommateur.

6. QUEL RÔLE ET QUEL POSITIONNEMENT POUR LE RESPONSABLE SÉCURITÉ ?

Si les grandes entreprises françaises ont toutes un responsable sécurité groupe, toutes les entreprises n'ont pas à ce jour de RSSI, notamment les PME et les TPE.

De plus, par comparaison avec les pays étrangers, les budgets de sécurité restent encore faibles et ne sont pas toujours clairement identifiés ni séparés du reste du budget informatique, ce qui n'est pas forcément un handicap si le RSSI intervient en tant que conseiller.

Par ailleurs, il n'y a pas un mais plusieurs métiers autour de la sécurité.

L'appellation varie d'une entreprise à l'autre :

- responsable de la sécurité du système d'information (RSSI) ;
- administrateur sécurité ;
- expert sécurité ;
- etc.

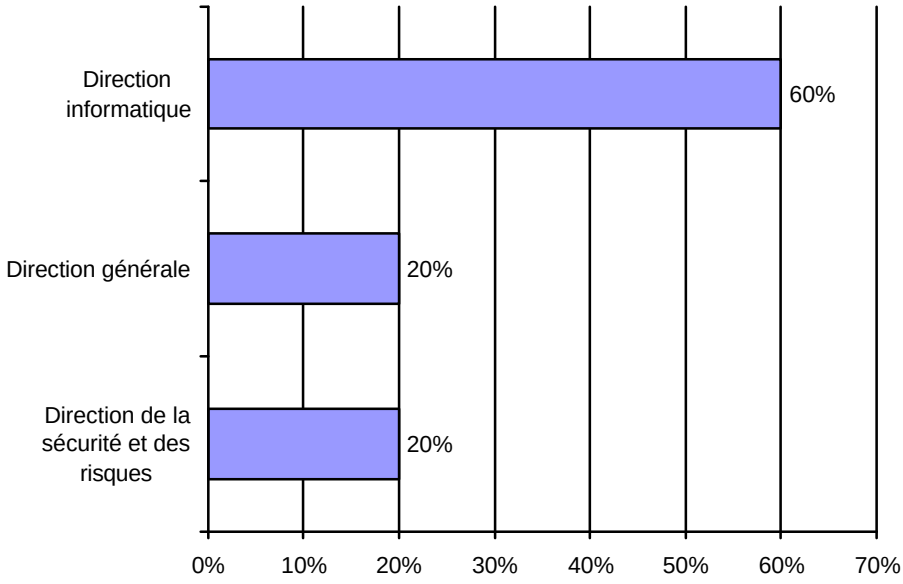
L'appellation traditionnelle est celle de RSSI. Le RSSI est rattaché à la direction informatique ou à la direction générale.

Le RSSI peut être soit un responsable fonctionnel, soit un responsable opérationnel, soit remplir des tâches mixtes. Il assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte. Il peut intervenir directement sur tout ou partie des systèmes informatiques et télécoms de son entité.

Il effectue un travail de veille technologique et réglementaire sur son domaine et propose des évolutions qu'il juge nécessaires pour garantir la sécurité logique et physique du système d'information dans son ensemble. Il est l'interface reconnue des exploitants et des chefs de projets mais aussi des experts et des intervenants extérieurs pour les problématiques de sécurité de tout ou partie du SI.

Les fonctions du RSSI sont les suivantes :

- architecte ;
- administrateur[4] ;
- superviseur, animateur et coordinateur ;
- auditeur, contrôleur et testeur ;
- éducateur ;
- veilleur.



Source : Cigref

Figure 19 : Qui définit la politique de sécurité dans votre entreprise ?

En résumé, on peut regrouper les activités du RSSI en cinq grandes catégories :

1. Définition de la politique de sécurité (analyse des risques, étude des moyens et préconisations, définition des mécanismes et processus de sécurité...).

2. Suivi et *reporting* du niveau général de sécurité de l'entreprise.

3. Veille technologique, prospective et apport d'expertise en matière de sécurité.

[4] La fonction d'administration est généralement confiée au RSSI métier ou opérationnel.

4. Sensibilisation et formation aux enjeux de la sécurité.

5. Audit et contrôle.

La définition de la politique de sécurité passe par :

- la définition du domaine d'application et des objectifs de sécurité ;
- la définition et la mise en place des procédures ;
- la définition de l'organisation et de la politique de sécurité.

L'analyse des risques implique :

- l'analyse des risques et évaluation des conséquences ;
- la remontée de l'ensemble des éléments qui permettent de prendre les décisions ;
- l'étude des moyens d'assurer la sécurité et le respect de leur application ;
- l'établissement d'un plan de secours et de sauvegarde.

L'étude des moyens et des préconisations a pour but :

- la validation technique des outils de sécurité ;
- la définition des normes et des standards de sécurité ;
- la participation à l'élaboration des règles de sécurité au niveau global de l'entreprise ou du groupe.

La définition des mécanismes et processus de sécurité doit prévoir :

- l'élaboration d'un volet sécurité pour tous les projets informatiques majeurs ;
- la spécification des contrôles devant être réalisés par les entités opérationnelles ;
- les propositions d'amendement et de mise à jour de la stratégie, de la politique et des procédures de sécurité de l'entreprise ;
- la formalisation avec le service juridique des clauses contractuelles de sécurité pour les contrats avec les fournisseurs, sous-traitants et prestataires extérieurs.

Le suivi et le *reporting* du niveau général de sécurité de l'entreprise comprennent :

- le suivi général du plan d'action de sécurité et la mise à jour annuelle de ce plan ;
- la définition et la mise en place de tableau de bord ;

- l'élaboration d'un rapport annuel de synthèse pour le DSI ;
- la proposition de nouveaux domaines d'investigation.

La veille technologique et la prospective assurent :

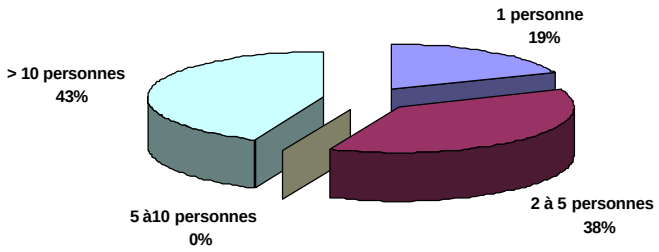
- le suivi des évolutions réglementaires et techniques de son domaine ;
- la veille et la mise en place des évolutions nécessaires pour garantir la sécurité logique et physique du SI dans son ensemble ;
- la veille des outils d'attaques ;
- l'apport à la demande de la DSI ou d'un utilisateur d'une expertise sécurité sur les systèmes en place ou les projets en cours.

La sensibilisation et la formation aux enjeux de la sécurité supposent :

- la sensibilisation de la direction générale ;
- la formation des directions opérationnelles et métiers ;
- la participation à la réalisation de la charte de sécurité ;
- la réalisation de supports de sensibilisation, l'animation des réunions de sensibilisation à la sécurité ;
- le conseil et assistance auprès des équipes.

L'audit et le contrôle permettent de garantir que :

- les plans de sécurité ont été faits suivant les plans préétablis ;
- les équipes ont pris toutes les mesures permettant de gérer la sécurité.



Source : Cigref

Figure 20 : Taille de l'équipe sécurité.

Les qualités requises du RSSI sont :

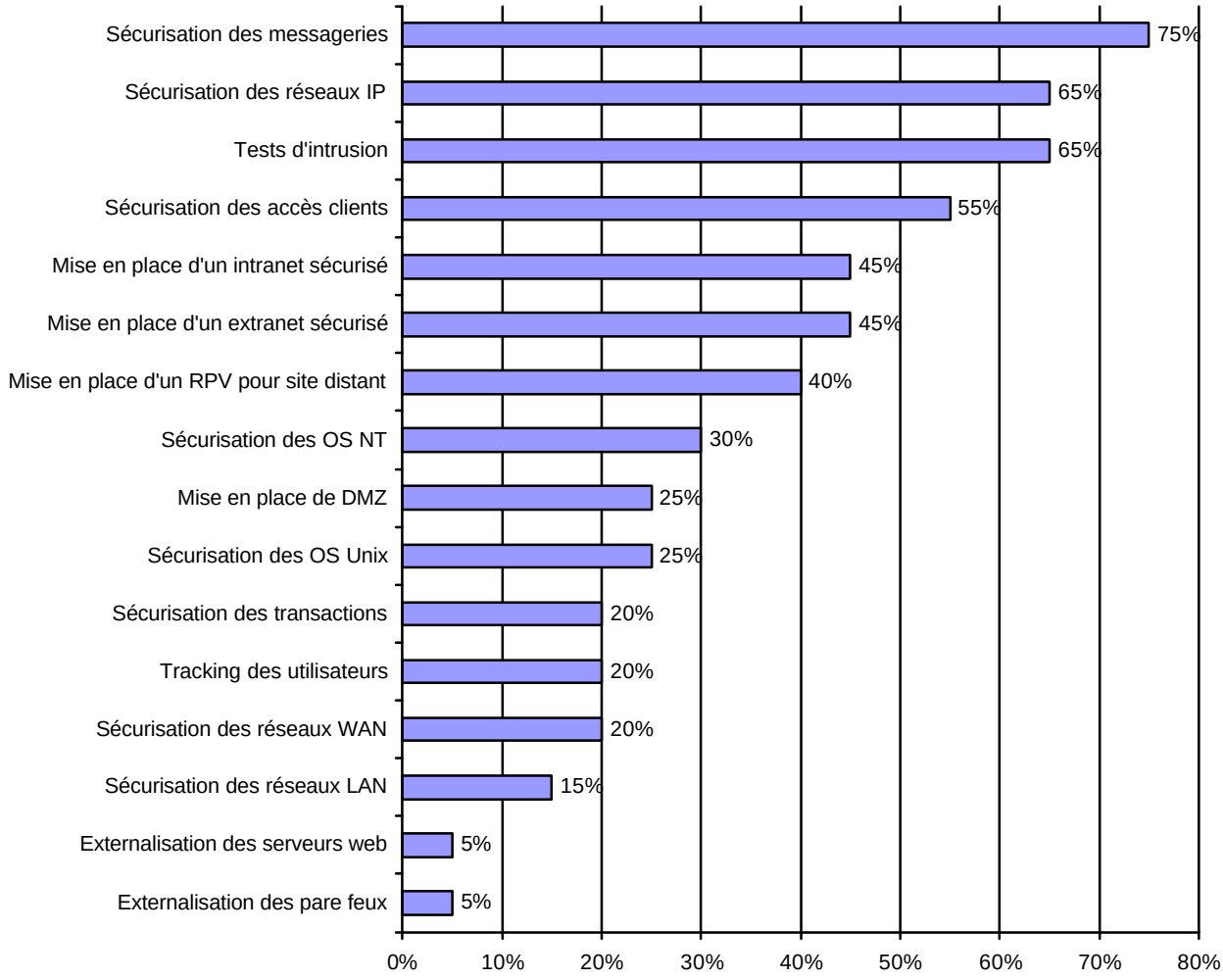
- le savoir-faire technologique : connaissance des normes et procédures de sécurité I&T, des protocoles réseaux et internet, connaissance du marché de la sécurité, évaluation et maîtrise des risques I&T ;
- le savoir-faire général : législation sur la sécurité (chiffrement…), connaissance de l'entreprise (environnement, organes, fonctionnement), méthode d'analyse de risques, capacité à mener des projets avec des acteurs multiples, pratique de l'anglais courant ;
- l'attitude comportementale : forte personnalité et sens du relationnel, rigueur, sens de la méthode et probité intellectuelle, capacité de conviction, d'analyse et de synthèse, ouverture d'esprit et pragmatisme, facilité et rapidité d'adaptation, capacité de négociation, de communication et de rédaction.

Le métier de RSSI va évoluer dans les prochaines années, notamment sous l'impact du *e-business* (projets *B-to-B* et *B-to-C*), de l'ouverture des réseaux vers l'internet et de l'évolution rapide des technologies et des standards. Une certaine pénurie de spécialistes commence déjà à se faire sentir. Le thème du RSSI sera abordé plus en détail l'an prochain.

7. QUELLES ÉVOLUTIONS ?

7.1 Les priorités des grandes entreprises : la sécurisation de la messagerie et du réseau IP

Interrogées sur leurs priorités dans les six prochains mois, les grandes entreprises membres du Cigref jugent prioritaires la sécurisation de leur messagerie et du réseau IP. Viennent ensuite la mise en place de tests d'intrusion, la sécurisation des accès distants et la sécurisation des intranets et extranets.

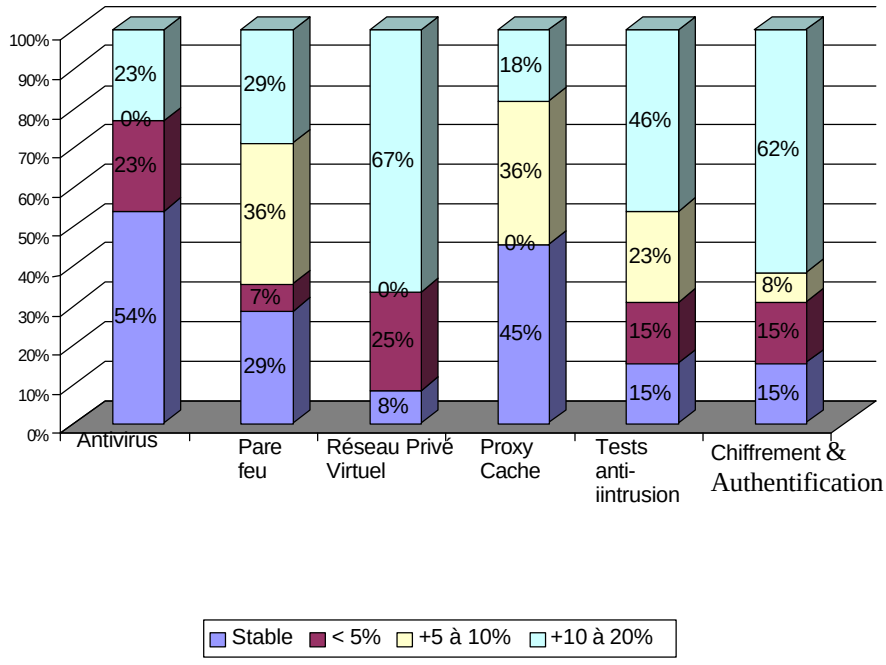


Source : Cigref

Figure 21 : Priorités des grandes entreprises en l'an 2000.

Les responsables sécurité estiment que leur budget sécurité va continuer à enregistrer une forte croissance l'an prochain. Pour rappel, entre 1999 et 2000, les dépenses concernant les antivirus, les pare-feu et les serveurs *proxy cache* étaient restées relativement stables. Les principales hausses avaient eu lieu sur les postes suivants :

- réseau privé virtuel (RPV IP) ;
- solutions d'authentification (PKI) ;
- solutions de chiffrement renforcées ;
- outils de détection d'intrusion ;
- scanners de vulnérabilité ;
- services de conseil et d'intégration.



Source : Cigref

Figure 22 : Évolution des principaux postes de dépense entre 1999 et 2000.

7.2 Les axes de développement pour l'année 2000–2001

Les grands axes de travail retenus pour l'an prochain concerneront principalement l'élaboration et la mise en place des tableaux de bord, la définition des architectures de sécurité, la gestion des annuaires, la gestion de la sécurité et de la mobilité ainsi qu'une mise à jour des thèmes étudiés cette année.

ANNEXE 1 : Évolution de la réglementation sur le chiffrement

Le chiffrement permet d'assurer l'authentification, la confidentialité et l'intégrité des messages. Mais le chiffrement est surtout la base de *l'e-commerce* et de *l'e-business*. Pour des raisons de défense nationale et d'ordre public, les réglementations en matière de chiffrement sont presque exclusivement des réglementations nationales.

Le cadre juridique communautaire

Il n'existe pas à l'heure actuelle de règlement ou de directive communautaire en matière de chiffrement, sauf l'exportation de moyens de cryptologie à double usage qui est régie par l'accord de Wassenaar et le réglement communautaire du 19 décembre 1994.

L'exportation des moyens et prestations de cryptologie est régie soit par l'accord de Wassenaar, soit pour les pays non signataires en application des législations nationales spécifiques.

L'accord de Wassenaar du 11 juillet 1996, qui s'applique uniquement entre les pays signataires (33 pays dont la France) et le règlement communautaire du 19 décembre 1994, qui s'applique pour les états membres de l'Union européenne, ont instauré un contrôle à l'exportation pour les biens à double usage (usage civil et militaire).

L'accord de Wassenaar a pour objectif la mise en œuvre d'une politique commune d'exportation. Mais cet accord n'est pas directement applicable et doit être transposé au préalable en droit interne.

Le règlement et la décision du Conseil du 19 décembre 1994 instituent une politique commune au niveau européen en matière de biens à double usage. Elle repose sur les principes communautaires suivants : principe de libre circulation, principe de reconnaissance mutuelle des licences d'exportation. Le règlement est actuellement en cours de révision.

La situation dans les autres pays industrialisés

Si l'on compare la régime français avec celui des pays étrangers, on constatera qu'il n'y a quasiment pas de réglementation limitant l'utilisation dans les autres pays.

Les États-Unis par exemple n'imposent que des restrictions à l'exportation (la situation est en train de changer). Les seuls pays à avoir mis en place des restrictions à l'utilisation sont des pays comme la Chine, la Russie, Singapour, Taiwan.

De plus, si la réglementation est trop stricte, elle risque d'être inapplicable et d'entraîner des effets de contournement.

Le cadre juridique national

Le paysage législatif français a fortement évolué depuis le décret de 1939 qui considérait le chiffrement comme une arme de guerre. La loi du 29 décembre 1990 sur les télécommunications marque les débuts d'une réglementation civile. La loi du 26 juillet 1996 sur les télécommunications tente de prendre en considération les aspects économiques et commerciaux. Enfin les décrets de mars 1999 marquent la libéralisation jusqu'à 128 bits pour la cryptologie symétrique.

L'organe administratif chargé du contrôle des activités de cryptologie en France s'appelle le SCSSI (Service central de la sécurité des systèmes d'information. C'est un département du Secrétariat général pour la défense nationale (SGDN), placé sous l'autorité du Premier ministre. Le SCSSI contrôle les activités de cryptologie. Il est l'organe chargé des procédures de déclaration et d'autorisation de mise sur le marché.

Récemment, le SCSSI s'est transformé en DCSSI (Direction centrale de la sécurité des systèmes d'information). Il ne s'agit pas que d'un changement d'appellation mais aussi d'un changement de dimension :

- il s'agit d'une direction et non plus d'un service ;
- la direction n'est plus dirigée par un militaire mais par un civil (Henri Serres) ;
- près de 60 personnes vont être recrutées.

On distingue deux types de moyens et prestations de cryptologie :

- moyens et prestations permettant d'assurer des fonctions de confidentialité ;
- les autres moyens et prestations (essentiellement authentification et intégrité) ne permettant pas d'assurer des fonctions de confidentialité.

Il y a 4 types de procédures concernant la fourniture et l'utilisation des moyens et prestations de cryptologie :

- Exemption de toutes formalités : cette procédure dispense de toute déclaration. L'utilisation et la fourniture sont libres.
- Déclaration simplifiée : cette procédure est applicable aux moyens et services n'assurant pas de fonctions de confidentialité.

- Déclaration standard : en plus de la partie administrative la déclaration comprend une partie technique. Si au bout d'un mois, le DCSSI n'a pas formulé de demande d'information complémentaire, le fournisseur peut commercialiser sa solution sur le marché français.
- Autorisation préalable : le dossier comporte une partie administrative et une partie technique. Si au bout de quatre mois après l'avis de réception, la demande n'est pas rejetée, elle est réputée accordée.

Seuls les produits sont soumis à déclaration. Les composants, algorithmes et protocoles n'ont pas à être déclarés.

La loi de 1996 libéralise partiellement la cryptologie en identifiant les usages de la cryptographie :

- utilisation libre si le produit ne peut pas assurer des fonctions de confidentialité ;
- utilisation soumise à autorisation si le produit permet d'assurer des fonctions de confidentialité et si la longueur de la clé est supérieure à une certaine taille.

Le décret d'application de cette loi fixe cette limite à 40 bits. Au-delà de 40 bits, les clés doivent être déposées chez des tiers de séquestre agréés par le ministère de la défense.

Dans la pratique, le système de tiers de séquestre n'a jamais fonctionné car il s'est avéré beaucoup trop lourd à mettre en place et à gérer (Seul Thomson avait été agréé et n'a jamais été utilisé).

Le décret du 17 mars 1999 introduit un changement : la fixation de la taille limite à 128 bits.

Le tableau ci-dessous résume le nouveau cadre juridique depuis 1999.

En échange de cette libéralisation de l'utilisation et de l'allègement des procédures de commercialisation, le législateur a cherché à :

- renforcer les obligations de déchiffrement qui pèsent sur les utilisateurs (livraison des clés à la demande du juge par exemple) ;
- renforcer les moyens de déchiffrement mis à la disposition de l'administration.

	Moyens assurant la confidentialité	Moyens assurant l'authentification l'intégrité
< 40 bits	- Utilisation : exemption de formalité - Fourniture : déclaration standard - Importation : exemption de formalité - Exportation : autorisation préalable	- Utilisation : libre - Fourniture : déclaration simplifiée
de 40 à 128 bits	- Utilisation : libre si utilisation privée ; déclaration standard si utilisation professionnelle si le produit n'est pas déclaré en France - Fourniture : déclaration - Importation : déclaration	- Utilisation : libre - Fourniture : déclaration simplifiée
> 128 bits	- Utilisation, importation, exportation et fourniture : soumis à autorisation	- Utilisation : libre - Fourniture : déclaration simplifiée

Figure 23 : Législation française en matière d'utilisation, fourniture, importation et exportation de produits de cryptologie.

Le décret applicatif de la déclaration sur la libéralisation de l'usage de la cryptographie en France

4050 JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE 19 mars 1999

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

PREMIER MINISTRE

Décret n° 99-199 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation

NOR : *PRMX9903476D*

Le Premier ministre,

Vu le règlement (CE) n° 3381/94 du Conseil en date du 19 décembre 1994 modifié instituant un régime communautaire de contrôle des exportations de biens à double usage, notamment son article 2 ;

Vu la directive 98/34/CE du Parlement européen et du Conseil en date du 22 juin 1998, modifiée par la directive 98/48/CE du Parlement européen et du Conseil en date du 20 juillet 1998, prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information ;

Vu la loi n° 90-1170 du 29 décembre 1990 modifiée sur la réglementation des télécommunications, notamment son article 28 ;

Vu le décret n° 98-101 du 24 février 1998 définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie, notamment son article 4,

Décrète :

Art. 1er. – Pour chacune des catégories de moyens et de prestations de cryptologie figurant dans la première colonne du tableau annexé au présent décret, les opérations pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation sont indiquées dans la deuxième colonne du même tableau.

Art. 2. – Le décret n° 98-207 du 23 mars 1998 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation est abrogé.

Art. 3. – Le présent décret sera publié au *Journal officiel* de la République française.

Fait à Paris, le 17 mars 1999.

LIONEL JOSPIN

ANNEXE

MOYENS OU PRESTATIONS	OPÉRATIONS (*) pour lesquelles la déclaration se substitue à l'autorisation
1. Matériels ou logiciels offrant un service de confidentialité mis en œuvre par un algorithme dont la clef est d'une longueur inférieure ou égale à 40 bits.	F
2. Matériels ou logiciels offrant un service de confidentialité mis en œuvre par un algorithme dont la clef est d'une longueur supérieure à 40 bits et inférieure ou égale à 128 bits.	F, U, I (1)
3. Equipements conçus ou modifiés pour utiliser la cryptologie faisant appel à des techniques analogiques tels que : *a)* Equipements utilisant des techniques de mélange de bandes « fixes » ne dépassant pas 8 bandes et où les changements de transposition ne s'effectuent pas plus d'une fois toutes les secondes ; *b)* Equipements utilisant des techniques de mélange de bandes « fixes » dépassant 8 bandes et où les changements de transposition ne s'effectuent pas plus d'une fois toutes les dix secondes ; *c)* Equipements utilisant l'inversion à fréquence « fixe » et où les changements de transposition ne s'effectuent pas plus d'une fois toutes les secondes ; *d)* Equipements de fac-similé ; *e)* Equipements de radiodiffusion pour audience restreinte ; *f)* Equipements de télévision civile.	F

(1) L'utilisation et l'importation ne sont soumises à déclaration que si elles concernent un matériel ou un logiciel qui n'a pas fait l'objet préalablement d'une déclaration par leur producteur, un fournisseur ou un importateur, et si ledit matériel ou ledit logiciel n'est pas exclusivement destiné à l'usage privé d'une personne physique.

(*) F : fourniture ; U : utilisation ; E : exportation ; I : importation.

Figure 24 : décret n° 99-199 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation.

Décret n° 99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable

NOR : *PRMX9903477D*

Le Premier ministre,

Vu le règlement (CE) n° 3381/94 du Conseil en date du 19 décembre 1994 modifié instituant un régime communautaire de contrôle des exportations de biens à double usage, notamment son article 2 ;

Vu la directive 98/34/CE du Parlement européen et du Conseil en date du 22 juin 1998, modifiée par la directive 98/48/CE du Parlement européen et du Conseil en date du 20 juillet 1998, prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information ;

Vu la loi n° 90-1170 du 29 décembre 1990 modifiée sur la réglementation des télécommunications, notamment son article 28 ;

Vu le décret n° 98-101 du 24 février 1998 définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie, notamment son article 2,

Décrète :

Art. 1er. – Pour chacune des catégories de moyens et de prestations de cryptologie figurant dans la première colonne du tableau annexé au présent décret, les opérations dispensées de toute formalité préalable sont indiquées dans la deuxième colonne du même tableau.

Art. 2. – Le décret n° 98-206 du 23 mars 1998 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable est abrogé.

Art. 3. – Le présent décret sera publié au *Journal officiel* de la République française.

Fait à Paris, le 17 mars 1999.

LIONEL JOSPIN

ANNEXE

MOYENS OU PRESTATIONS	OPÉRATIONS (*) dispensées de toutes formalités préalables
1. Matériels ou logiciels offrant un service de confidentialité mis en œuvre par un algorithme dont la clef est d'une longueur inférieure ou égale à 40 bits.	U, I
2. Matériels ou logiciels offrant un service de confidentialité mis en œuvre par un algorithme dont la clef est d'une longueur supérieure à 40 bits et inférieure ou égale à 128 bits, à condition, soit que lesdits matériels ou logiciels aient préalablement fait l'objet d'une déclaration par leur producteur, un fournisseur ou un importateur, soit que lesdits matériels ou logiciels soient exclusivement destinés à l'usage privé d'une personne physique.	U, I
3. Equipements conçus ou modifiés pour utiliser la cryptologie faisant appel à des techniques analogiques tels que : *a)* Equipements utilisant des techniques de mélange de bandes « fixes » ne dépassant pas 8 bandes et où les changements de transposition ne s'effectuent pas plus d'une fois toutes les secondes ; *b)* Equipements utilisant des techniques de mélange de bandes « fixes » dépassant 8 bandes et où les changements de transposition ne s'effectuent pas plus d'une fois toutes les dix secondes ; *c)* Equipements utilisant l'inversion à fréquence « fixe » et où les changements de transposition ne s'effectuent pas plus d'une fois toutes les secondes ; *d)* Equipements de fac-similé ; *e)* Equipements de radiodiffusion pour audience restreinte ; *f)* Equipements de télévision civile.	U, E, I
4. Cartes à microprocesseur personnalisées ou leurs composants spécialement conçus, incapables de chiffrer le trafic de messages ou les données fournies par l'utilisateur ou leur prestation de gestion de clef associée.	F, U, E, I
5. Equipements de réception de télévision de type grand public, sans capacité de chiffrement numérique et où le déchiffrement numérique est limité aux fonctions vidéo, audio ou de gestion.	F, U, E, I
6. Radiotéléphones portatifs ou mobiles destinés à l'usage civil qui ne sont pas en mesure de procéder au chiffrement de bout en bout.	F, U, E, I
7. Equipements autonomes de lecture de disques vidéo numériques, de type grand public, sans capacité de chiffrement, où le déchiffrement est limité aux informations vidéo, audio, informatiques et de gestion.	F, U, E, I
8. Moyens matériels ou logiciels spécialement conçus pour assurer la protection des logiciels contre la copie ou l'utilisation illicite, dont les fonctions de déchiffrement ne sont pas accessibles à l'utilisateur.	F, U, E, I
9. Equipements de contrôle d'accès, tels que machines automatiques de distribution de billets, imprimantes libre-service de relevés de compte ou terminaux de points de vente, protégeant les mots de passe, numéros d'identification personnels ou autres données similaires empêchant l'accès non autorisé à des installations, mais ne permettant pas le chiffrement des fichiers ou des textes, sauf lorsqu'il est directement lié à la protection des mots de passe ou des numéros d'identification personnels.	F, U, E, I
10. Moyens ou prestations conçus pour protéger des mots de passe, des codes d'identification personnels ou des données d'authentification similaires, utilisés pour contrôler l'accès à des données, à des ressources, à des services ou à des locaux, sous réserve qu'ils ne permettent de chiffrer que les fichiers de mots de passe ou de codes d'identification et les informations nécessaires au contrôle d'accès.	U, E, I
11. Moyens ou prestations conçus pour élaborer ou protéger une procédure de signature, une valeur de contrôle cryptographique, un code d'authentification de message ou une information similaire, pour vérifier la source des données, prouver la remise des données au destinataire, ou bien détecter les altérations ou modifications subreptices portant atteinte à l'intégrité des données, sous réserve qu'ils ne permettent de chiffrer que les informations nécessaires à l'authentification ou au contrôle d'intégrité des données concernées.	U, E, I
12. Systèmes de gestion de facturation inclus dans les dispositifs de relevés de compteurs dont les fonctions de chiffrement sont directement liées au comptage.	F, U, E, I
13. Equipements dotés de moyens de cryptologie lorsqu'ils accompagnent les personnalités étrangères sur invitation officielle de l'Etat.	U, E, I
14. Stations de base de radiocommunications cellulaires commerciales civiles présentant toutes les caractéristiques suivantes : *a)* Limitées au raccordement de radiotéléphones qui ne permettent pas d'appliquer des techniques cryptographiques au trafic de messages entre terminaux mobiles, sauf sur les liens directs entre radiotéléphones et stations de bases (connues sous le nom d'interface radio) ; *b)* Et ne permettant pas d'appliquer des techniques cryptographiques au trafic de messages sauf sur l'interface radio.	F, U, I

(*) F : fourniture ; U : utilisation ; E : exportation ; I : importation.

Figure 25 : décret n° 99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable.

ANNEXE 2 : Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique

J.O. Numéro 62 du 14 Mars 2000 page 3968

Lois

LOI no 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (1)

NOR : JUSX9900020L

L'Assemblée nationale et le Sénat ont adopté,
Le Président de la République promulgue la loi dont la teneur suit :

Article 1er
I. - L'article 1316 du code civil devient l'article 1315-1.
II. - Les paragraphes 1er, 2, 3, 4 et 5 de la section 1 du chapitre VI du titre III du livre III du code civil deviennent respectivement les paragraphes 2, 3, 4, 5 et 6.
III. - Il est inséré, avant le paragraphe 2 de la section 1 du chapitre VI du titre III du livre III du code civil, un paragraphe 1er intitulé : « Dispositions générales «, comprenant les articles 1316 à 1316-2 ainsi rédigés :
« Art. 1316. - La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission.
« Art. 1316-1. - L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.
« Art. 1316-2. - Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support. «

Article 2
L'article 1317 du code civil est complété par un alinéa ainsi rédigé :
« Il peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par décret en Conseil d'État. «

Article 3
Après l'article 1316-2 du code civil, il est inséré un article 1316-3 ainsi rédigé :
« Art. 1316-3. - L'écrit sur support électronique a la même force probante que l'écrit sur support papier. «

Article 4
Après l'article 1316-3 du code civil, il est inséré un article 1316-4 ainsi rédigé :
« Art. 1316-4. - La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.
« Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État. «

Article 5
A l'article 1326 du code civil, les mots : « de sa main « sont remplacés par les mots : « par lui-même «.

Article 6
La présente loi est applicable en Nouvelle-Calédonie, en Polynésie française, à Wallis-et-Futuna et dans la collectivité territoriale de Mayotte.
La présente loi sera exécutée comme loi de l'État.
Fait à Paris, le 13 mars 2000.

Jacques Chirac

Par le Président de la République :

Le Premier ministre,
Lionel Jospin

Le garde des sceaux, ministre de la justice,
Elisabeth Guigou

Le ministre de l'intérieur,
Jean-Pierre Chevènement

Le ministre de l'économie,
des finances et de l'industrie,
Christian Sautter

Le secrétaire d'État à l'outre-mer,
Jean-Jack Queyranne

Le secrétaire d'État à l'industrie,
Christian Pierret

(1) Loi no 2000-230.
- Directive communautaire :

Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.
- Travaux préparatoires :
Sénat :
Projet de loi no 488 (1998-1999) ;
Rapport de M. Charles Jolibois, au nom de la commission des lois, no 203 (1999-2000) ;
Discussion et adoption le 8 février 2000.
Assemblée nationale :
Projet de loi, adopté par le Sénat, no 2158 ;
Rapport de M. Christian Paul, au nom de la commission des lois, no 2197 ;
Discussion et adoption le 29 février 2000.

ANNEXE 3 : Les différents modes de chiffrement

Le chiffrement permet d'assurer l'authentification, la confidentialité et l'intégrité des messages et des transactions au sein de l'entreprise ou vers l'extérieur.

Les principaux facteurs de développement du chiffrement en entreprise sont :

- la croissance de l'usage de la messagerie ;
- le développement de l'accès distant ;
- l'essor du commerce électronique ;
- l'internationalisation des groupes ;
- les besoins de sécurisation du SI ;
- l'intelligence économique.

Le chiffrement peut être utilisé pour plusieurs usages :

- des besoins internes : messagerie électronique, accès distant, signature électronique et certificats, transactions en ligne (*B-to-B*) ;
- des besoins externes : signature électronique et certificats, transactions en ligne (*B-to-C*).

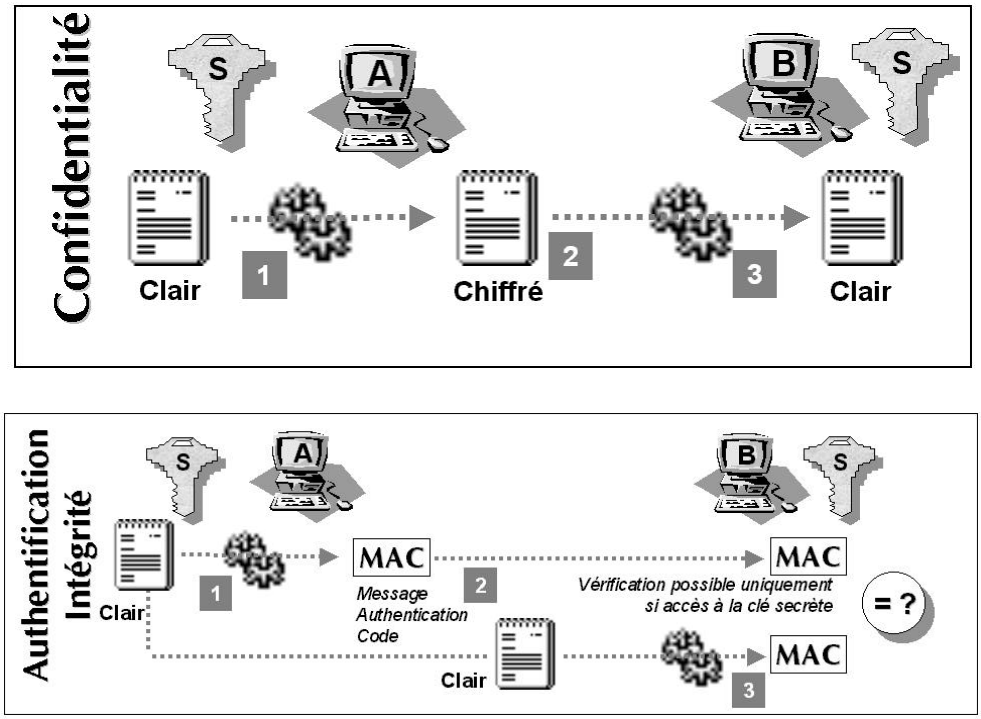
On distingue traditionnellement deux types de chiffrement : le chiffrement symétrique (ou chiffrement à clé secrète) et le chiffrement asymétrique (ou chiffrement à clé publique).

Historiquement, les premiers systèmes de chiffrement utilisaient le chiffrement symétrique. La tendance actuelle étant plutôt de d'utiliser le chiffrement asymétrique ou de mélanger les deux types de chiffrement.

La cryptographie à clé secrète (chiffrement symétrique)

Les algorithmes à clés secrètes ou symétriques permettent le chiffrement et déchiffrement d'un message à l'aide d'une même clé connue des deux interlocuteurs et échangée au préalable.

Les principaux algorithmes à clés secrètes sont DES (40 ou 56 bits), 3DES (112 à 168 bits), RC2, RC4, RC5, IDEA (128 bits), Blowfish (128 bits), Skipjack...



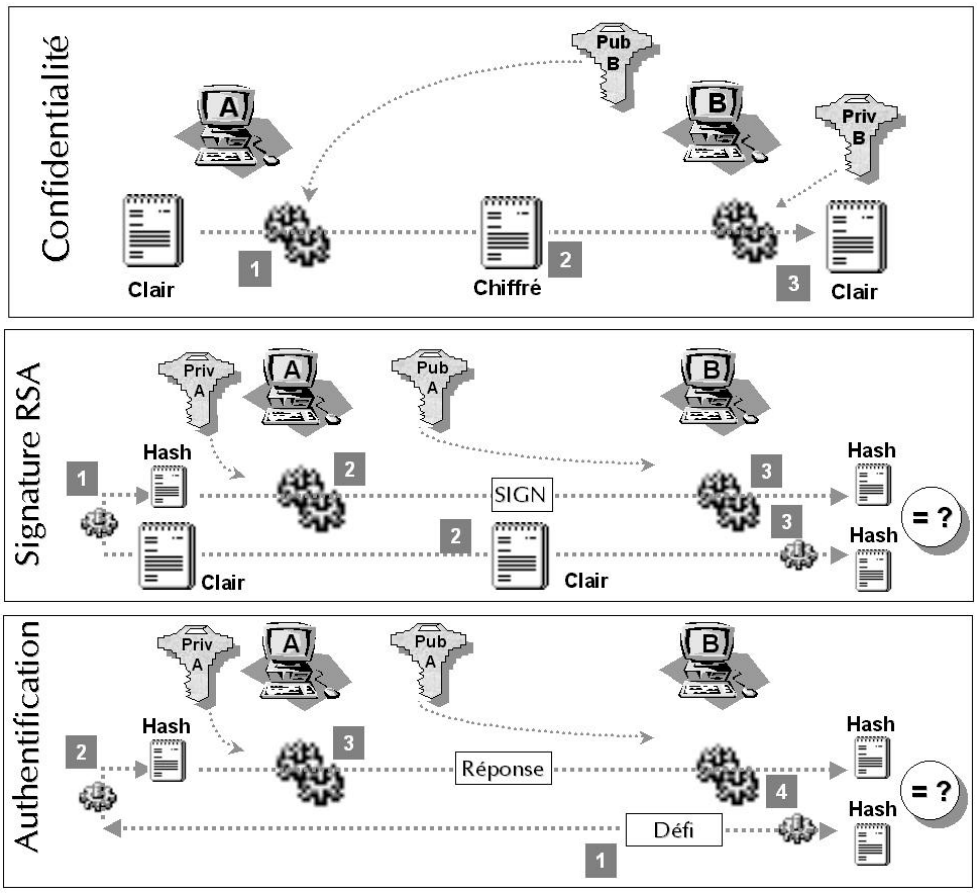
Source : Solucom

Figure 26 : Schéma de fonctionnement de la cryptographie à clé secrète.

La cryptographie à clé publique (chiffrement asymétrique)

Les algorithmes à clés publiques ou asymétriques sont basés sur un couple de clés (une clé publique et une clé privée), une clé servant à chiffrer, l'autre à déchiffrer. Chacune des clés peut servir à chiffrer ou à déchiffrer. La clé publique est connue de tous, tandis que la clé privée doit rester confidentielle. Les principaux algorithmes à clés publiques sont RSA, El Gamal et DH.

La solidité des mécanismes de cryptographie asymétrique est directement fonction de l'association entité–clé publique. Cette association est réalisée de manière sûre principalement par une infrastructure de gestion de clé publique (IGC en français ou PKI en anglais).



Source : Solucom

Figure 27 : Schéma de fonctionnement de la cryptographie à clé publique.

	Avantages	Inconvénients
Cryptographie à clé secrète / symétrique	- rapidité de traitement de l'information	- protection / stockage de la clé privée - pas de répudiation de l'émetteur - pas de preuve vis-à-vis des tiers - pas de gestion de l'authentification (certificat) - adapté pour une petite communauté d'utilisateurs
Cryptographie à clé publique / asymétrique	- permet la signature - preuve vis-à-vis des tiers - permet l'authentification - permet la transmission d'élément secret entre deux personnes sans accord préalable	- protection / stockage de la clé privée - procédé moins rapide que le chiffrement symétrique

Source : Cigref

Figure 28 : Avantages et inconvénients de la cryptographie symétrique et asymétrique.

ANNEXE 4 : Les failles de quelques produits et protocoles

Les faiblesses de Bind (Berkeley Internet Name Domain), nxt, qinv, in.named

Bind est un logiciel utilisé par les serveurs DNS qui permet d'identifier les machines connectées sur internet sans connaître leur adresse IP. Selon une enquête réalisée à la mi-1999, la moitié des serveurs DNS connectés à internet tournaient sous des versions vulnérables de Bind. Cette vulnérabilité permet de réaliser une attaque *via* Bind. L'attaquant efface les *logs* systèmes et installe des outils qui lui permettent de prendre la main et d'avoir les droits d'administrateur. À partir de là, il peut lancer des attaques sur des systèmes distants extérieurs. Cette vulnérabilité affecte les systèmes Unix et Linux. Toutes les versions antérieures à Bind v.8.2.2 sont vulnérables.

Les conseils pour corriger ce défaut sont de désactiver la fonction Bind Name Daemon sur tous les systèmes qui ne sont pas autorisés à être serveurs DNS. Certains experts recommandent même carrément de retirer le logiciel.

Sur les machines qui sont des serveurs DNS autorisés, il faut prendre la dernière version de Bind (la v.8.2.2 avec le patch level5).

Il faut utiliser Bind en tant qu'utilisateur non privilégié.

Il faut utiliser Bind dans une structure d'annuaire sécurisée.

Les vulnérabilités dans les programmes CGI (*Common Gateway Interface*) et les extensions d'application (ex : Cold Fusion) installés sur les serveurs web.

La plupart des serveurs web utilisent des programme CGI (*Common Gateway Interface*) pour fournir de l'interactivité dans les pages web. Une grande partie des serveurs web utilisent des programmes CGI de démonstration installés par défaut. Or ces CGI comprennent un certain nombre de failles. Ces failles sont relativement faciles à découvrir et peuvent être utilisées par les intrus pour vandaliser les pages web (insertion d'images, substitution de pages), pour voler des informations sur les cartes de crédits ou pour installer des *back doors* pour rendre possible des intrusions ultérieures. Un exemple connu de faille CGI est la substitution de la photo de Janet Reno par celle d'Adolf Hitler sur le site web du département américain de la justice. Le serveur web Allaire de Cold Fusion par exemple contient des programmes échantillons qui sont vulnérables. Tous les serveurs web sont susceptibles d'être affectés.

La parade consiste en règle générale à retirer les programmes de démonstration peu sûrs des systèmes de production, à écrire des programmes CGI sûrs, à ne pas faire tourner les serveurs web en *root*.

Il faut aussi penser à se débarrasser des interpréteurs de script CGI dans les annuaires *bin* et à ne pas activer des CGI sur des serveurs web qui n'en ont pas besoin.

Les faiblesses dans les procédures d'appel à distance (RPC) (ToolTalk, Calendar Manager).

La procédure d'appel à distance (*Remote Procedure Call*) permet à un ordinateur d'exécuter un programme sur un autre ordinateur. Cette procédure est généralement utilisée pour accéder à des services réseaux tels que les fichiers partagés dans NFS. Les vulnérabilités causées par les défauts de RPC sont activement exploitées. La majorité des attaques par déni de services distribués lancées pendant l'année 1999 et 2000 sont dues aux vulnérabilités de RPC. Le département de la défense américain a été victime d'une attaque exploitant les défauts de RPC. Cette vulnérabilité affecte les systèmes Unix et Linux.

Dans la mesure du possible, il faut retirer ces fonctions des serveurs qui sont directement accessibles d'internet.

Quand il faut les mettre en place, il faut veiller à installer les derniers *patches* disponibles.

Les failles de sécurité dans les RDS (*Remote Data Services*) du serveur web de Microsoft Internet Information Server (IIS).

Cette vulnérabilité affecte les systèmes sous Windows NT et Windows 2000 utilisant internet Information Server. Les défauts dans RDS sont exploités par les attaquants pour utiliser les commandes à distance avec des privilèges d'administrateur. Il semblerait qu'il existe d'autres failles telles que les fichiers « .htr ».

La prudence veut que les entreprises qui utilisent IIS installent les derniers *patches* et mises à jour pour corriger toutes les failles connues de IIS.

Les faiblesses de Sendmail (*buffer overflow*), les attaques pipe et Mimebo, qui permettent de compromettre immédiatement le *root*.

Sendmail est le programme qui envoie, reçoit et fait suivre les courriers électroniques sur les systèmes d'exploitation Unix et Linux. La large diffusion de Sendmail sur internet en fait une cible privilégiée pour les attaquants. Plusieurs failles ont été

découvertes dans Sendmail au cours de ces dernières années. La première a été découverte par le Cert CC en 1988. L'attaque la plus classique consiste à envoyer un message manuel à la machine utilisant Sendmail qui l'interprète comme une instruction lui demandant d'envoyer son fichier de mots de passe à la machine de l'attaquant. Cette vulnérabilité affecte les systèmes Unix et Linux.

La solution consiste à télécharger la dernière version de Sendmail.

Et ne pas faire tourner Sendmail en mode démon sur les machines qui ne sont ni des serveurs de messagerie ni des relais de messagerie.

Les faiblesses de Sadmind et Mounted.

Sadmind est un outil d'administration à distance pour les systèmes Solaris. Mounted contrôle les accès aux partitions NFS montées sur des Unix. Sadmind et Mounted peuvent être affectés par des débordements de *buffer (buffer overflow*), ce qui permet aux attaquants de prendre le contrôle avec un accès maître. Mounted affecte les systèmes Unix et Linux, tandis que Sadmind affecte uniquement le système d'exploitation Solaris de Sun.

Il est recommandé de désactiver ces fonctions sur les serveurs qui sont directement accessibles depuis internet.

Il est recommandé d'installer les derniers *patches* disponibles.

Le partage global de fichiers et le partage inapproprié d'information via Netbios et les ports 135 à 139 de Windows NT (445 dans Windows 2000), ou sur Unix les exports NFS sur le port 2049, ou sur Macintosh web Sharing ou sur AppleShare/IP sur le port 80, 427 et 548.

Ces services permettent le partage de fichier sur le réseau. Quand ils sont mal configurés, ils peuvent exposer des fichiers systèmes critiques ou donner aux intrus accès à l'ensemble du fichier système. Beaucoup d'administrateurs utilisent ces services pour rendre leurs fichiers systèmes lisibles afin d'améliorer la convivialité de l'accès aux données. Quand le partage de fichiers est permis sur les machines Windows, celles-ci deviennent vulnérables au vol d'informations et à des virus (exemple : le vers 911 récemment sur Windows 95 et 98 qui connectait le modem sur le n°911). Netbios peut aussi être utilisé pour obtenir des informations systèmes sensibles sur des systèmes Windows NT. Les informations utilisateurs et groupes, les informations systèmes et certains clés d'immatriculation peuvent être obtenues par une connexion « *null session* » au service de session Netbios. Cette information est utilisée typiquement pour deviner un mot de

passe ou pour monter une attaque contre une cible NT. Cette vulnérabilité affecte les systèmes Unix, NT et Macintosh. Les remèdes sont les suivants :

- s'assurer que seuls les annuaires requis sont partagés sur les disques ;
- ne permettre le partage que sur certaines adresses IP spécifiques, car les noms de DNS peuvent être usurpés (*spoofing*) ;
- pour les systèmes NT, s'assurer que tous les partages sont protégés avec des mots de passe solides.

Pour les systèmes NT, empêcher les énumérations d'utilisateurs, groupe, système et clés d'immatriculation *via* des connections de type « *null session* ». Bloquer les connections entrantes au service de session Netbios au niveau du routeur ou de l'hôte NT.

Les mots de passe utilisateur, en particulier le compte *root*/administrateur sans mot de passe ou avec un mot de passe faible.

Certains systèmes ont des comptes « démo » ou « invité » sans mot de passe ou avec des mots de passe par défaut connus de tous. Certains systèmes d'administration de base de données installent les comptes d'administration avec un mot de passe par défaut. Enfin, certains administrateurs débordés choisissent souvent des mots de passe système par défaut qui sont aisément devinables voire même des blancs. Tout cela facilite la tâche des attaquants. Les intrusions se font généralement par bonds successifs.

Il est recommandé d'avoir une politique de gestion des mots de passe (changement et vérification fréquente).

Il faut s'assurer que les cadres dirigeants possèdent également un mot de passe.

Il est conseillé de supprimer systématiquement les mots de passe par défaut sur les machines ayant un accès internet.

Il faut obtenir une autorisation écrite pour tester les mots de passe et il faut tester les mots de passe avec des programmes de *cracking*.

Il est préférable de créer des mots de passe à durée de vie limitée et de garder un historique des précédents mots de passe pour éviter de les réutiliser.

Les vulnérabilités de type débordement de *buffer (buffer overflow)* ou les configurations incorrectes sur les protocoles de messagerie Imap et Pop.

Imap et Pop sont les deux protocoles d'accès distant à la messagerie permettant à l'utilisateur d'accéder à sa messagerie soit à partir du réseau interne, soit *via* un accès distant. Le caractère ouvert de ces protocoles les rend particulièrement sensibles aux attaques. En effet, il y a souvent un ou plusieurs ports ouverts sur le pare-feu pour permettre aux nomades de consulter leur messagerie à distance. Cette vulnérabilité affecte les systèmes Unix et Linux.

Il est recommandé de désactiver ces fonctions sur les machines qui ne sont pas des serveurs de messagerie.

Il est conseillé d'utiliser les derniers *patches* et les dernières versions disponibles.

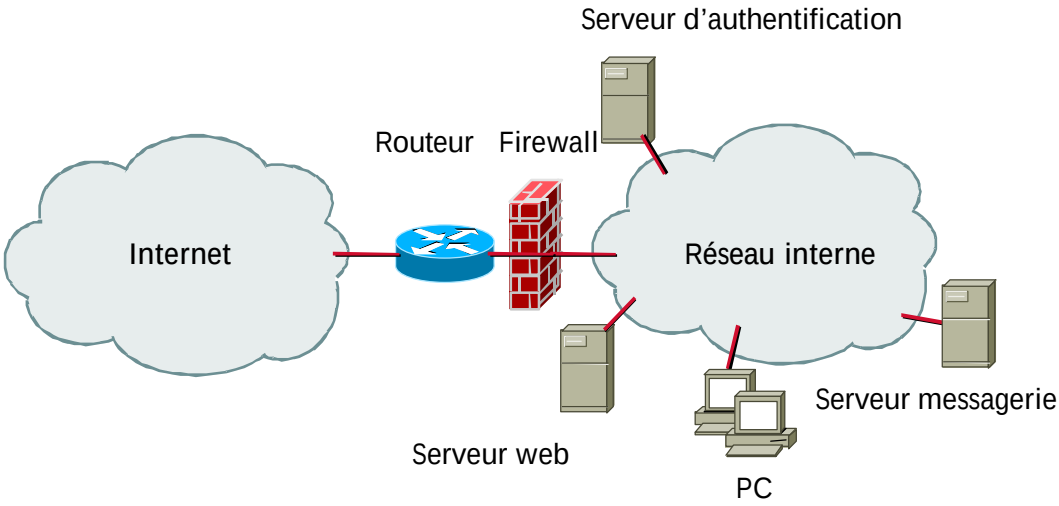
Il est conseillé également d'utiliser SSH et SSL pour chiffrer les mots de passe et ne pas les faire circuler en clair sur internet.

Le choix d'un « *community string* » SNMP par défaut et public.

SNMP (*Simple Network Management Protocol*) est utilisé par les administrateurs réseaux pour surveiller et administrer tous les équipements connectés au réseau (du routeur à l'imprimante en passant par le PC). SNMP utilise un « *community string* » non crypté comme seul mécanisme d'authentification. L'absence de chiffrement pose un problème mais, en plus, la plupart des équipements utilisent un *community string* par défaut et, qui plus est, public. Les attaquants peuvent utiliser cette faille dans SNMP pour reconfigurer ou fermer un équipement à distance.

ANNEXE 5 : Exemples d'architectures de sécurité

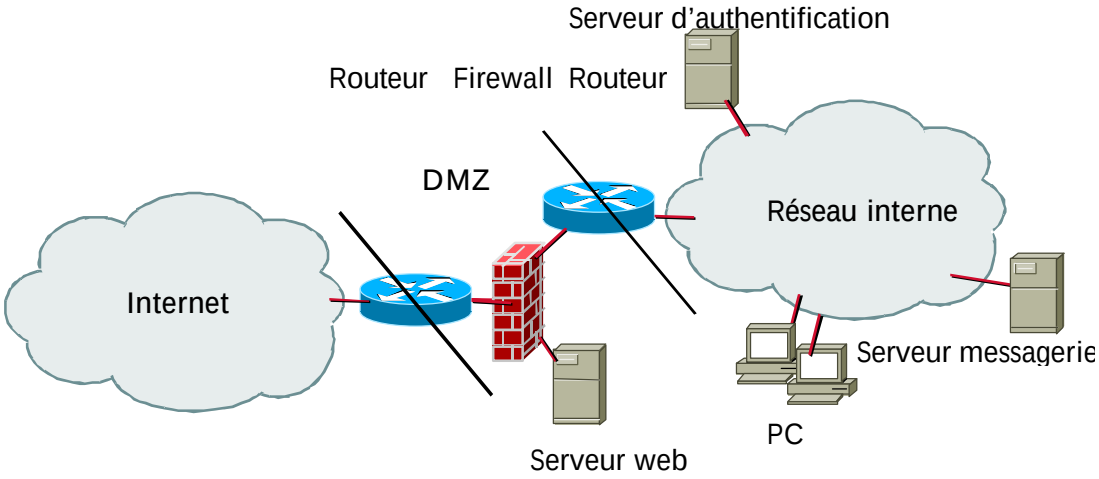
Dans le premier schéma, le pare-feu est placé en bastion, devant le serveur web, mais derrière le routeur pour filtrer les paquets entrants. Le serveur d'authentification, quant à lui, est placé en retrait avec le serveur de messagerie. Le pare-feu est composé de deux cartes, l'une pour le réseau local, l'autre pour le réseau internet.



Source : Cigref

Figure 29 : Architecture de sécurité avec pare-feu en bastion.

Dans le deuxième schéma, une zone démilitarisée (DMZ) sépare strictement le réseau interne et le réseau externe (internet). Le routeur externe donne accès à ce périmètre de sécurité dans lequel sont logés les serveurs publics de l'entreprise. Toutes les machines internes, y compris le pare-feu ne sont pas visibles de l'extérieur. Il faut dans ce cas définir une politique d'usage des modems dans l'entreprise et interdire toutes les connexions pirates à internet pour éviter tout risque de contournement du périmètre de sécurité. Cette architecture est l'architecture la plus souvent mise en place dans les entreprises. Il est possible de raffiner la solution en séparant la DMZ en deux zones : une DMZ publique, où sont logés les serveurs web publics, les serveurs radius et les serveurs d'accès distant et une DMZ privée où sont placés les serveurs de messagerie et les serveurs intranet.

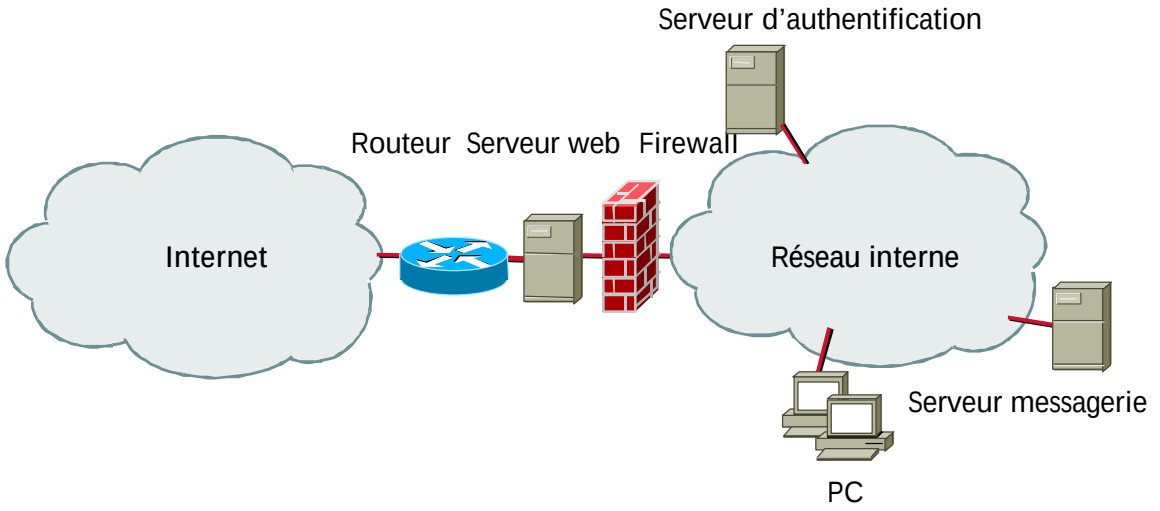


Source : Cigref

Figure 30 : Architecture de sécurité avec pare-feu en zone démilitarisée (DMZ).

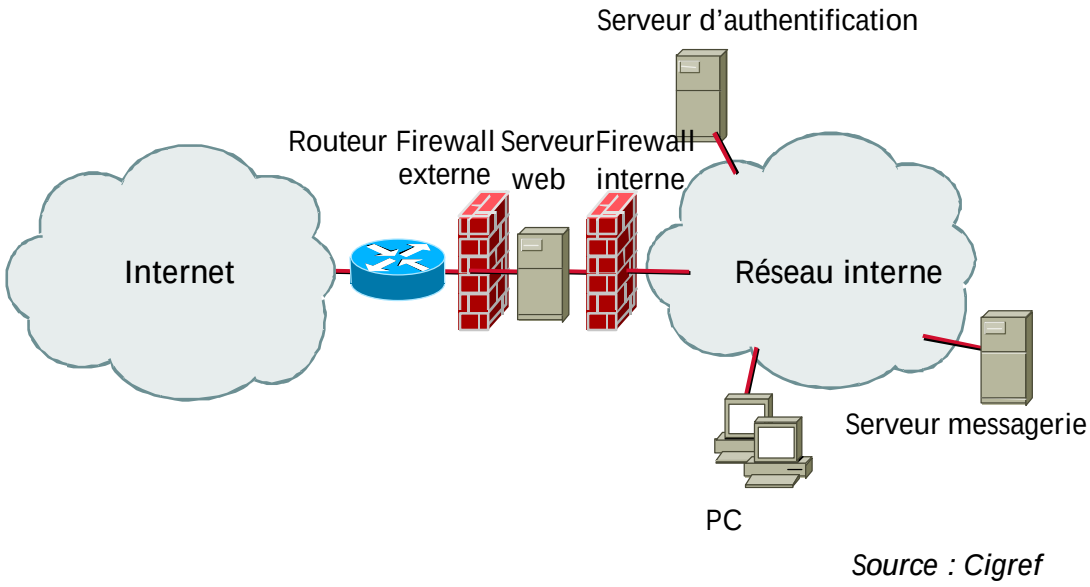
Dans le troisième schéma, le serveur web est placé devant le pare-feu, donc exposé aux attaques extérieures. L'avantage est qu'il offre un bon cloisonnement des systèmes. L'inconvénient est que cela pose des problèmes de mise à jour du serveur et des problèmes de partage de fichiers.

Enfin, dans le dernier schéma, le serveur web est encadré par deux pare-feu qui le protègent à la fois des attaques externes et internes. La position du serveur web facilite également l'exploitation, le suivi et les mises à jour.



Source : Cigref

Figure 31 : Architecture de sécurité avec serveur web « sacrifié ».



Source : Cigref

Figure 32 : Architecture de sécurité avec double fortification pour serveur web.

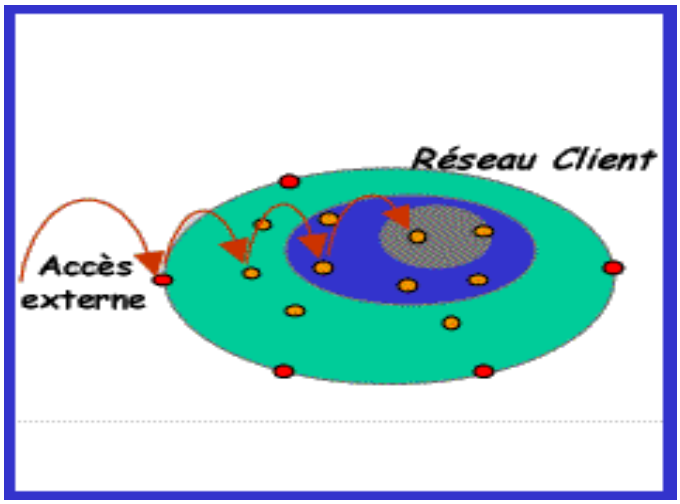
ANNEXE 6 : Schéma de fonctionnement d'une attaque par intrusion

La méthode suivie par les cabinets est calquée sur les pratiques des *hackers*. De manière générale une opération d'intrusion s'apparente à une succession de « bonds » de la périphérie du SI aux équipements centraux.

- bond 0 : accès à des équipements techniques périphériques (pare-feu, serveurs applicatifs, autocommutateurs…) ;
- bond 1 : contrôle des serveurs généraux et des passerelles d'accès aux centraux ;
- bond 2 : accès aux centraux.

Chaque bond se décompose lui même en 3 phases : une phase d'approche, une phase de contact et une phase d'attaque.

- une phase d'approche : permettant d'identifier la nature des points d'accès possibles ;
- une phase de contact : permettant de qualifier l'accès et d'entrer en contact avec celui-ci pour tester sa réactivité (analyseurs de ports, les scanners téléphoniques, les testeurs X25…) ;
- une phase d'attaque : permettant ou non la prise de contrôle.



Source : CF6 / Telindus

Figure 33 : Schéma de fonctionnement d'une attaque par intrusion.

ANNEXE 7 : Liste des principaux acteurs par marché

Liste des principaux acteurs du marché

Segments de marché	Principaux acteurs
Administration	BMC Software, Bull, Cisco, Computer Associates, Content Technologies, HP, IBM / Tivoli, Matranet, Nortel Networks, Rainbow Technologies,
Antivirus	Computer Associates, Command Software, Content Technologies, eSafe Technologies, F-Secure, Memco (Platinum), Network Associates, Panda Software, Sophos, Symantec, Trend Micro,
Authentification	ActivCard, Axent, Bull, Cisco, Computer Associates, Dassault, Funk Software, Gemplus, Matranet, Network Associates, Racal, RSA, SafeData, Sagem, Sclumberger, Sun Microsystem, Thawte, WatchGuard Technologies
Biométrie	- Reconnaissance faciale : Identification Technologies, Keyware Technologies, Miros, Viisage, Visionics - Reconnaissance digitale : American Biometric Corp., Biometric Access Corp., Digital Persona, Indentix, National Registry, Sony, WhoVision - Reconnaissance rétinienne : EyeDentify, IriScan - Reconnaissance vocale : Intelitrak, Keyware Technologies, Veritel
Chiffrement	Baltimore, CS SI, F-Secure, Matranet, MSI, Network Associates, Racal, Rainbow Technologies, Thomson CSF, Sagem, Symantec,
Détection d'intrusion (IDS)	Axent, BindView, Cisco, Computer Associates, ISS, Network Associates, NFR
Formation	Apogée, Bull Formation, Cap gemini Institut, CF6, CS Institut, IBM, Learning International, Orsys, Sun Microsystems...
Test de surveillance	Axent, Cisco, HP, ISS, Memco (Platinum), Network Associates, web Trend Corporation
Pare-feu	3Com, Axent, BorderWare Technologies, Bull, Check Point, Cisco, Computer Associates, F-Secure, Lucent, HP, IBM, Matranet, Network Associates, Sun Microsystem, WatchGuard Technologies
PKI	- Interne : Baltimore, Entrust, Lotus, Microsoft, RSA, Sun / Netscape, - Externe : Baltimore, Certplus, Certinomis, VeriSign, Thawte,
Porte Monnaie Electronique (PME)	Moneo, Modeus, Mondex, ...
Smart Card	Bull, Gemplus, Schlumberger,
Solution de paiement sécurisé	Cybercomm,
SSII	Apogée / Compaq, Arthur Andersen, Arès, Bull, Cap Gemini, CF6 / Telindus, CS SI, CSC Peat Marwick, Deloitte Touche & Tohmatsu, Ernst & Young, Euriware, Expertel Consulting, Hervé Schauer Consultants, IBM Global Services, MSI, Steria, Sysicom / USweb CKS, Ubizen, XP Conseil Lefebvre Consultants,
SSO	Axent, Bull, BMC Software, Computer Associates, IBM / Tivoli, Microsoft, Novell, Unisys
RPV	- Constructeurs : 3Com, Axent, Bull, BorderWare Technologies, Check Point, Cisco, Computer Associates, Dassault, Entrust, F-Secure, Intel, IBM, Lucent, Microsoft, MSI, Nortel, Redcreek, Sun Microsystem, Thomson, WatchGuard Technologies - Opérateurs : FT, Cegetel, Siris, Equant, Global One, Worldcom, ISDNet, Infonet, BT, Cable & Wireless...

Source : Cigref

ANNEXE 8 : Sites internet de référence

Index des sites internet utilisés

Avert (*Antivirus Emergency Response Team*)

www.avert-labs.com

Axent Technologies (racheté par Symantec)

www.axent.com

Baltimore

www.baltimore.com

Bull

www.bull.fr

Cert

www.cert.org

Certinomis

www.certinomis.com

Certplus

www.certplus.com

Checkpoint Software

www.rsasecurity.com

Cisco

www.cisco.com

Clusif

www.clusif.asso.fr

Cnil

www.cnil.fr

Computer Associates

www.ca.com

Entrust

www.entrust.com

First (*Forum of Incident & Response Security Team*)

www.first.org

F-Secure

www.f-secure.com

Gemplus

www.gemplus.com

HP

www.hp.com

Internet Security System

www.iss.net

Matranet

www.matranet.com

Microsoft

www.microsoft.com

Network Associates

www.nai.com

Novell

www.novell.com

RSA Security

www.rsasecurity.com

Sagem

www.sagem.com

SANS Institute

www.sans.org

Schlumberger

www.schlumberger.com

Sun Microsystems

www.sun.com

Symantec

www.symantec.com

Trend Micro

www.antivirus.com

Verisign

www.verisign.com

ANNEXE 9 : Lexique

Active X : technologie développée par Microsoft pour apporter de l'animation et de l'interactivité dans les pages HTML statiques que l'on trouve sur le web. Cette technologie englobe des documents ActiveX, des contrôles ActiveX et des scripts.

Applet Java : les *applets* sont des petits programmes exécutables qui sont stockés sur le serveur et qui sont rapatriés sur le poste client (en même temps que le document HTML associé) puis exécutés sur celui-ci.

Audit : l'audit permet de vérifier de manière régulière et aléatoire l'efficacité des contrôles de la bonne application des règles et de la bonne utilisation des outils. Contrairement aux tests d'intrusion, qui permettent de tester les vulnérabilités externes, l'audit permet de diagnostiquer les dysfonctionnements internes.

Authentification : l'authentification est l'action qui permet de s'assurer de l'identité de quelqu'un par différents moyens (mot de passe, mot de passe unique, carte à puce, jeton, certificat, biométrie). L'authentification est le terme dérivé de l'anglais pour désigner l'identification.

Autorité de certification (AC) : organisme chargé de définir les critères, les modalités d'attribution et d'émission de certificats.

Autorité d'enregistrement (AE) : organisme chargé de recueillir les demandes de certificats et de contrôler l'identité et le rôle du demandeur.

Back door : porte dérobée sur un logiciel créé, soit par l'éditeur au moment de la conception du logiciel, soit par un intrus avec un utilitaire et qui permet de récupérer des informations à l'insu de la société utilisatrice du logiciel.

Bombe logique : programme malveillant dont le déclenchement s'effectue à une date prédéterminée, en exploitant la date du système ou le lancement d'une commande.

Certification Authority (CA) : voir Autorité de certification.

Cert : *Computer Energency Response Team.* Organisme offrant des prestations payantes de veille, de support sur incidents, de formation et d'étude dans le domaine de la sécurité et d'internet. Il existe trois Cert en France : le Cert Renater, le plus ancien, le Cert IST et le Cert Administration, le plus récent. Le Cert Renater concerne les instituts de recherche (CNRS...), le Cert IST (Industrie, Services et Tertiaires) vise les grandes entreprises du secteur privé tandis que le Cert Administration s'adresse aux entreprises publiques et à leurs organismes de tutelle. Les trois

Cert nationaux collaborent. Au niveau mondial, l'organisation est pyramidale : tout les Cert nationaux sont reliés entre eux et sont fédérés par le FIRST (Forum of Incident and Response Security Team) et le Cert CC (Coordination Center) .

Cert IST : Cert Industrie Services et Tertiaires. Ce Cert a été crée par quatre partenaires : Alcatel, le Cnes, Elf Aquitaine et France Télécom. Il propose des prestations payantes de veille, de support sur incidents, de formation et d'étude dans le domaine de la sécurité et d'internet.

Certificat : un certificat est délivré par l'Autorité de certification et permet de garantir l'identité d'un intervenant dans une communication *via* internet.

CGI : *Common Gateway Interface*. Standard permettant d'interfacer une application externe avec un serveur d'informations de type web. On va par exemple utiliser un programme CGI si l'on veut mettre à jour une base de données à partir d'informations qui ont été saisies dans un formulaire HTML.

CRL : *Certificate Revocation List*. Liste de révocation des certificats.

Chiffrement : le chiffrement permet d'assurer l'authentification, la confidentialité et l'intégrité des messages. On distingue deux types de chiffrement :

- les *algorithmes à clés secrètes ou symétriques* qui permettent le chiffrement et déchiffrement d'un message à l'aide d'une même clé connue des deux interlocuteurs et échangée au préalable. Les principaux algorithmes à clés secrètes sont DES, 3DES, RC2, RC4 / RC5, IDEA, Skipjack...
- les *algorithmes à clés publiques ou asymétriques* qui sont basés sur un couple de clés (une clé publique et une clé privée), une clé servant à chiffrer, l'autre à déchiffrer. Les principaux algorithmes à clés publiques sont RSA et DH.

Cheval de Troie : fonction placée dans un programme en apparence inoffensif, destinée à voler des données ou des mots de passe. Backorifice est un exemple de cheval de troie existant sur les version Windows 95, 98 et NT.

Confidentialité : la confidentialité permet de s'assurer qu'un message privé ne peut pas être lu par d'autres personnes que le destinataire. La confidentialité peut être réalisée par le chiffrement ou par la gestion des droits d'accès.

Cookies : fichier inscrit sur le disque dur de l'internaute lors de sa visite d'un site web permettant de garder ses coordonnées et son comportement d'une session à l'autre.

Cryptologie : ensemble des techniques (principes, méthodes, moyens) de transformation de l'information en vue de préserver sa confidentialité et son intégrité.

Déni de service : attaque très connue sur l'internet et très dure à contrer. Cette attaque consiste à mettre hors service une machine donnée en la sollicitant plus qu'elle ne peut le supporter (*buffer overflow* par exemple). Les serveurs de messagerie, par exemple, peuvent faire l'objet d'attaques par refus de service.

DDOS : *Distributed Denial of Service*. Déni de service distribué.

DES : *Data Encryption Standard*. Mécanisme de chiffrement symétrique des données utilisant la même clé pour le chiffrement et le déchiffrement.

Disponibilité : la disponibilité vise à garantir l'accès aux informations critiques de l'entreprise.

DMZ : *Demilitarized Zone*. Zone démilitarisée, située entre le réseau interne de l'entreprise et internet. Un réseau DMZ est un réseau isolé du réseau de l'entreprise mais protégé par le pare-feu où des règles de filtrage différentes seront appliquées en fonction de la destination du paquet de données : vers le réseau interne ou vers la zone démilitarisée. Les pare-feu qui permettent cette configuration comportent au minimum trois cartes réseau.

DNS : *Domain Name Server*. Serveur permettant d'établir la correspondance entre un nom de domaine et une adresse IP.

Firewall : pare-feu. Un pare-feu est un système ou un ensemble de systèmes qui permettent d'établir une politique de contrôle d'accès entre deux réseaux. L'objectif d'un pare-feu est d'éviter l'intrusion de pirates dans le réseau de l'entreprise et de permettre et contrôler l'accès des employés aux services de l'internet. Le pare-feu est un équipement logiciel ou matériel permettant de filtrer, de relayer, de masquer des paquets IP ainsi que la translation d'adresse IP. Le pare-feu peut être installé soit sur un routeur, soit en équipement *stand alone.* Le pare-feu peut intégrer des mécanismes d'identification, d'authentification et de chiffrement. Le pare-feu peut également intégrer des fonctions de gestion, de surveillance, d'audit et de statistiques. Les pare-feu doivent protéger le réseau interne mais également se protéger eux-mêmes. Ils doivent proposer des mécanismes performants pour authentifier les utilisateurs. Ils doivent posséder des mécanismes d'alerte, d'audit et de journalisation. Les pare-feu

doivent enfin posséder une interface graphique ergonomique, permettre la traduction d'adresses IP, le support de réseaux privés virtuels, le support multi-plates-formes.

First : *Forum of Incident & Response Security Team*. Organisme fédérant au niveau mondial les différents Cert.

Hoaxes : messages électroniques colportant des rumeurs ou des fausses informations (ex : les fausses alertes virales, la diffusion gratuite des terminaux Wap d'Ericsson...).

IDS : *Intrusion Detection System*. Voir système de détection d'intrusion.

IGC : infrastructure de gestion de clés. L'infrastructure de gestion de clés est une architecture de sécurité visant à garantir l'authentification, la non-répudiation, la confidentialité et l'intégrité des messages ou des transactions, à l'intérieur de l'entreprise ou lors d'échanges avec l'extérieur. L'infrastructure de gestion de clés repose sur la notion de chiffrement asymétrique qui lui-même est basé sur quatre éléments : une entité appelée « porteur de certificat », une clé publique, une clé privée et un certificat numérique.

Informations nominatives : au sens de la loi du 6 janvier 1978, sont nominatives les informations qui « permettent sous quelque forme que ce soit, directement ou non, l'identification de personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou morale ».

Intégrité : l'intégrité permet de s'assurer qu'un message n'a pas été modifié entre sa création par l'émetteur et sa lecture par le récepteur. Elle est assurée par des techniques de signature électronique (« *Digital Signature* »).

IP : *Internet Protocol*. Protocole de niveau 3 (réseau) utilisé pour transmettre des paquets de données (datagrammes) entre deux sous-réseaux différents. L'IETF *(Internet Engineering Task Force)* est chargée de faire évoluer les protocoles d'interconnexion de réseaux dans le cadre de TCP-IP.

IPSec : *Internet Protocol Security*. Protocole permettant la construction de tunnel virtuel sur IP chiffré de bout en bout.

Kerberos : système d'authentification réseau utilisé sur des réseaux non sécurisés et basé sur un modèle de distribution de tickets / jetons.

Lan : *Local Area Network.* Réseau local ou réseau local

d'entreprise, par opposition au Wan.

LDAP : *Lightweight Directory Access Protocol*. Protocole d'accès au service d'annuaire fonctionnant au dessus de TCP/IP. Il offre un standard d'accès conforme à la norme d'annuaire X500 pour les postes clients, les applications et les serveurs web à travers l'internet et l'intranet.

Malveillance : Intention de nuire. Les actes de vandalisme, de sabotage, de fraude, de détournement et d'altération volontaire sont des actes de vandalisme.

MAN : *Metropolitan Area Network.* Réseau Métropolitain. Réseau intermédiaire entre le réseau local et le réseau étendu.

Mot de passe dynamique : mot de passe non réutilisable, modifié à chaque connexion de l'utilisateur.

Mot de passe statique : mot de passe réutilisable à chaque connexion de l'utilisateur.

NCSA : *National Computer Security Association*. Organisme américain reconnu dans le domaine de la sécurité sur l'internet. Le NCSA délivre des certificats attestant qu'un produit de sécurité répond à certains critères qu'il a déterminés.

Non-répudiation : la non-répudiation permet de s'assurer qu'une transaction a effectivement eu lieu. La non-répudiation est essentielle dans les transactions bancaires sur l'internet.

PGP : *Pretty Good Privacy*. Technique de chiffrement de données (et notamment de messages électroniques) associant deux types de chiffrement : un chiffrement symétrique et un chiffrement asymétrique. PGP a été développé par Philip Zimmermann.

PIN : *Personal Identification Number*. Numéro d'identification personnel. Système d'authentification par mot de passe utilisé sur les terminaux GSM, les cartes bleues et les postes nomades.

PKI : *Public Key Infrastructure*. infrastructure de gestion de clés.

Plan de continuité : ensemble de procédures et de moyens permettant de poursuivre l'exploitation avec une interruption minimale en cas d'indisponibilité majeure (incendie, destruction...) d'un système d'information.

Plan de reprise : ensemble de procédures et de moyens à mettre en œuvre lors d'un sinistre permettant de retrouver un niveau de service normal. Le plan de continuité est d'un des volets du plan de reprise.

Plan de sauvegarde : ensemble de procédures et de moyens permettant de disposer de copies de sauvegarde, fichiers, et procédures suffisamment à jour et en état pour redémarrer l'exploitation après incident.

PSC : prestataires de services de certification.

Registration Authority : voir Autorité d'enregistrement.

RPV : les réseaux privés virtuels (*Virtual Private Network*) permettent d'utiliser le réseau public, en toute sécurité, comme support de communication entre différents sites de l'entreprise. Les réseaux privés virtuels sont réalisés par le mise en place de tunnels de communication privés (technique de tunneling).

RSA : *Rivest Shamir Adelman.* Algorithme de chiffrement à clé publique.

RSSI : Responsable de la sécurité des systèmes d'information.

Scanner de vulnérabilité : les scanners de vulnérabilités scrutent un système, un réseau afin d'identifier des vulnérabilités pouvant être exploitées lors d'une attaque. Il existe deux catégories de scanner :

- les actifs : les scanners *network-based* exécutent des scripts d'attaques *via* le réseau et enregistrent la réponse du système ;
- les passifs : les scanners *host-based* scrutent les configurations d'une machine, les mots de passe faibles par exemple.

La différence entre un scanner de vulnérabilité et un IDS est la suivante :

- les scanners sont « proactifs » : ils aident à l'identification de vulnérabilités sur les systèmes et les réseaux ;
- les IDS sont réactifs : ils permettent d'enregistrer l'activité du réseau ou d'une machine et d'identifier une attaque ou une tentative d'attaque afin de pouvoir réagir.

Sécurité applicative : la sécurité applicative vise à contrôler en amont la robustesse et la solidité des applications (connaissance des failles, de la méthodologie de développement, audit et contrôle des programmes, définition des contrats et des clauses de responsabilité...).

Sécurité de l'exploitation : la sécurité de l'exploitation vise à garantir le bon fonctionnement et la continuité du système d'information par la gestion des configurations et des mises à jour, le suivi et résolution des incidents, la mise en place de plan de secours, de sauvegarde et de continuité.

Sécurité logique : la sécurité logique traite de la gestion de l'accès à l'information. Elle repose sur trois actions : l'identification, l'authentification et l'autorisation. La sécurité logique comprend également la prévention des infections virales, la sauvegarde des données. La gestion des droits d'accès suppose au préalable une classification de l'information selon son degré de sensibilité (normale, confidentielle...).

Sécurité physique : la sécurité physique traite des aspects liés à la sécurité des systèmes (matériel, câble...) et de leur environnement (accès aux locaux, alimentation, climatisation, etc.). Elle comprend notamment la gestion des normes de sécurité, la protection des sources énergétiques, le contrôle des accès aux bâtiments, le contrôle et le marquage des matériels, le plan de maintenance.

Sécurité des télécommunications : la sécurité des télécommunications concerne à la fois la sécurité des infrastructures (les couches basses du réseau - niveaux 1 à 3 Iso) et la sécurité applicative (les couches hautes du réseau). L'objectif est de garantir à l'utilisateur une connexion de bout en bout fiable et sécurisée grâce à des protocoles sécurisées, des logiciels de chiffrement et des technologies de type *tunneling* et réseau privé virtuel. La sécurité des télécommunications doit se concevoir en synergie avec les autres volets de la sécurité (applicative, logique, physique...).

Serveur web : processus qui tourne en tâche de fond sur un ordinateur connecté au réseau, dans le but de rester à l'écoute de demandes de documents effectuées à l'aide d'un logiciel client web (*browser* ou navigateur) et de les servir. Par extension, on appelle serveur web la machine sur laquelle tourne le processus web (ou démon httpd).

SET : *Secure Electronic Transaction.* Protocole proposé par Visa et Mastercard pour sécuriser les transactions commerciales sur internet.

Signature électronique : procédé permettant d'identifier une personne ou un document *via* un certificat.

SIM : *Subscriber Identification Module*. Carte à microprocesseur située à l'intérieur des téléphones portables gérant les informations relatives à l'abonné.

Smart Card : carte à puce contenant un microcontrôleur, de la mémoire vive, de la mémoire morte et une interface de communication avec l'extérieur (boîtier ou liaison radio).

Spaming ou UCE (*Unsolicited Commercial E-mail*) : envoi d'un message non sollicité (souvent d'origine publicitaire) à un grand nombre de personnes *via* leur messagerie électronique. La parade consiste à filtrer les domaines « spammeurs » par le serveur de courrier ou par le routeur en bloquant toutes les adresses des « spammeurs ». On peut aussi procéder à un filtrage sémantique. Il est conseillé également d'interdire le « relayage ».

SSL : *Secure Socket Layer*. Protocole développé par Netscape pour sécuriser toutes les communications sur l'internet. SSL s'interpose entre le protocole TCP/IP et les protocoles applicatifs (HTTP, FTP, Telnet,...) qu'il sécurise ainsi.

SSO : *Single Sign On.* Mot de passe unique permettant à l'utilisateur d'être reconnu sur de nombreux systèmes hétérogènes *(Mainframe*, Base de données, Unix...) en ne s'authentifiant qu'une seule fois.

Système de détection d'intrusion : équipements analysant l'activité du réseau sur lequel ils sont connectés ou l'activité de la machine sur laquelle ils sont installés, afin de déceler :

- des signes d'intrusion (*intrusion detection*) : attaques provenant de l'extérieur ou de l'intérieur du réseau de l'entreprise ;
- des signes de violation (*misuse detection*) : attaques provenant d'utilisateurs outrepassant leurs droits.

Pour la différence entre un IDS et un scanner de vulnérabilité, voir la définition de « Scanner de vulnérabilité ».

Tunneling : mécanisme de chiffrement et d'encapsulation d'une trame de données (IP ou autre) dans une seconde trame (IP) lui servant de véhicule pour traverser l'internet. Ce mécanisme créé ainsi des tunnels de communication sécurisés.

Trojan Horse : voir Cheval de Troie.

Vers : programmes conçus pour se déplacer et se reproduire à travers les réseaux informatiques, en vue de déclencher des actions malveillantes. Ils sont généralement composés de plusieurs segments dispersés à travers le réseau. On peut citer comme exemple le vers I-Worm.ExploreZip ou le vers PrettyPark.Worm. Les vers commencent aussi à apparaître sur les terminaux mobiles wap avec une diffusion *via* le carnet d'adresses.

Virus : programme conçu pour perturber le fonctionnement d'un ordinateur. Les virus sont capables de se reproduire et de se répandre dans le système d'information. On dénombre plus de 30 000 virus dans le monde aujourd'hui. Le virus est une

infection informatique (comme la bombe logique ou le cheval de Troie ou le vers). Le virus diffère de la bombe logique, car la bombe logique vise une cible unique et n'est pas auto-propageable. Le virus diffère aussi du cheval de Troie, car le cheval de Troie ne vise pas à détruire ou à paralyser mais seulement à pénétrer par effraction sur un ordinateur et à voler des données ou des mots de passe. Le virus est un code parasite auto-propageable (comme le vers). Les principaux vecteurs de transmission des virus sont : le téléchargement de fichiers sur internet, la messagerie électronique, les disquettes, l'annuaire du salarié ou de l'entreprise. On distingue plusieurs types de virus : les virus systèmes, les virus applicatifs, les virus multi-modes et les virus macros. Les virus systèmes (Tchernobyl, Emperor..) se diffusent par le secteur de partition du disque dur ou le secteur de démarrage de l'unité logique amorçable. Les virus applicatifs se diffusent par les programmes exécutables (.com, .exe, .sys, .drv, .bin, .ovl, .ovy). les virus macros (Melissa, CS.Gala...) se diffusent par l'intermédiaire de fichier utilisant un macrolangage et non plus par des programmes exécutables. La prochaine cible pour les « éditeurs » de virus devrait être les *applets* Java et les composants active X.

VPN : *Virtual Private Network*. Voir Réseau privé virtuel

Wan : *Wide Area Network.* Réseau étendu. Par opposition au Lan, désigne tout réseau qui dépasse l'étendue d'un seul site et qui permet l'interconnexion de plusieurs sites distants.

Wap : *Wireless Application Protocol*. Protocole qui optimise l'accès à internet pour les terminaux mobiles. Les pages web sont simplifiées mais leur transmission se fait à faible débit (9,6 kb/s).