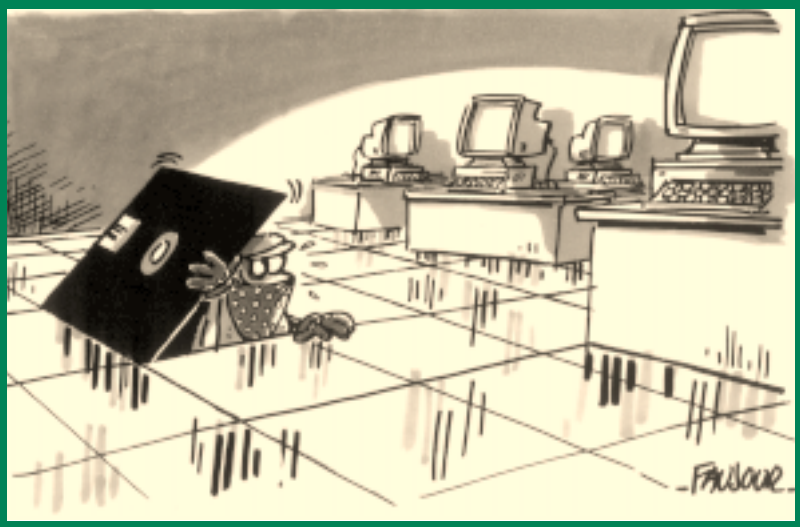
Guide de la sécurité
des systèmes d'information



à l'usage
des directeurs

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Guide de la sécurité
des systèmes d'information
à l'usage des directeurs

Cet ouvrage a été conçu et rédigé par

Robert Longeon
Chargé de mission à la sécurité
des systèmes d'information du CNRS

Jean-Luc Archimbaud
Chargé de mission à la sécurité
des réseaux du CNRS

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Avant-propos

Pourquoi protéger les produits de la recherche scientifique

La mission principale du CNRS est de faire effectuer toutes recherches présentant un intérêt pour l'avancement de la science ainsi que pour le progrès économique, social et culturel du pays. Il a aussi pour vocation de contribuer à l'application et à la valorisation des résultats de la recherche (Décret n°82-993 – *JO* du 25 novembre 1982).

Qu'ils soient ou non susceptibles de conduire à des applications industrielles ou commerciales, les résultats de la recherche constituent un bien commun, un patrimoine de la communauté nationale qui, à juste titre, peut prétendre à être la première à en tirer profit. Ce patrimoine scientifique, confié de plus en plus à des circuits électroniques chargés de le traiter, transformer, présenter, transmettre et conserver, chacun se doit de veiller à son intégrité face aux menaces, accidentelles ou malveillantes, qui pourraient l'altérer.

L'accès, par Internet notamment, à une masse en forte croissance d'informations scientifiques actualisées en temps réel ainsi que la possibilité de la traiter automatiquement, permet à nombre d'organisations, officielles ou privées, de disposer d'indicateurs sur l'émergence de l'innovation et ainsi de mieux orienter leurs recherches. L'innovation scientifique et technologique est donc devenue l'enjeu d'un marché stratégique de la connaissance où il n'y a plus guère d'amis ni d'alliés.

Il est donc indispensable d'assurer la protection physique de l'information scientifique élaborée par les laboratoires qui, lorsqu'elle est stockée sans précautions sur le disque dur d'un ordinateur relié à l'Internet, peut être lue, copiée, modifiée ou détruite à partir d'un poste de travail situé aux antipodes sans que, trop souvent hélas, le propriétaire s'en aperçoive.

Comment les protéger

Pour se prémunir contre une utilisation des réseaux qui viserait à s'approprier indûment des informations, il est nécessaire d'appliquer strictement les recommandations de ce guide. Il n'est pas inutile d'en rappeler quelques-unes :

- Adopter une architecture du réseau apte à interdire, ou tout au moins compliquer, toute tentative frauduleuse de pénétration.
- Assurer une surveillance permanente des connexions extérieures afin de détecter au plus tôt tout accès anormal.
- Gérer rigoureusement les logins et les mots de passe en veillant plus particulièrement à n'accorder aux chercheurs non permanents que les facilités strictement indispensables à leurs travaux et à les leur retirer dès la fin de leur séjour.
- Imposer des précautions supplémentaires aux chercheurs souhaitant se connecter de l'extérieur – et *a fortiori* lors d'un séjour à l'étranger –, par exemple l'emploi de mots de passe à usage unique.
- Utiliser, en cas de nécessité, les nouveaux procédés de chiffrement pour assurer la discrétion des échanges de messagerie et de données.
- N'effectuer les travaux les plus sensibles et ne stocker les fichiers confidentiels que sur des machines physiquement déconnectées du réseau.

Mais les systèmes informatiques ne sont pas vulnérables qu'aux attaques extérieures. L'incendie, l'explosion ou le dégât des eaux, l'insouciance, la maladresse ou la malveillance d'un collègue, peuvent perturber gravement le fonctionnement de cet incomparable outil de travail et de communication. Il faut donc, outre les mesures détaillées plus haut, sauvegarder en un lieu sûr et distant les informations et les données que l'unité ne peut se permettre de perdre.

Il vous appartient en tant que directeur de définir et mettre en œuvre la politique de sécurité de votre laboratoire, d'inciter chacun de vos collaborateurs à en prendre conscience et à s'y impliquer. Ce guide est le fruit de l'expérience de toute la communauté scientifique et nous comptons sur vous pour l'enrichir des cas concrets auxquels vous pourriez être confrontés.

Philippe Schreiber
Fonctionnaire de Défense du CNRS

Sommaire

Introduction

La qualité de nos recherches dépend étroitement des échanges et des débats que nous pouvons mener au sein de notre communauté scientifique. Cette dépendance est telle, qu'on considère de plus en plus la capacité de communiquer comme un indicateur significatif « de dynamisme ». Le réseau Renater et l'Internet ont constitué une évolution majeure. Ils sont maintenant si naturels, qu'on croirait qu'ils ont toujours existé. Les facilités offertes pour les transferts de fichiers, le courrier électronique, les listes de diffusion, les webs, les forums – entre autres – ont permis un développement spectaculaire et fructueux des échanges scientifiques. Mais, parallèlement à la mutation extraordinaire de nos méthodes de travail qu'a induit cette évolution, nous assistons à des phénomènes parasitaires inquiétants – notamment depuis l'ouverture d'Internet à des activités privées ou commerciales – qui confirment la nécessité, pour les organismes qui veulent pouvoir librement communiquer, stocker et traiter les données, de protéger leurs systèmes d'information.

De nouvelles formes de malveillance ont récemment fait leur apparition ; elles risquent de perturber gravement le fonctionnement des laboratoires. Certaines de ces malveillances constituent des crimes ou des délits et peuvent entraîner des poursuites judiciaires ; d'autres provoquent une entrave à la communication scientifique. Plus inquiétante encore est l'apparition d'une délinquance organisée qui cherche à pénétrer les systèmes pour s'approprier de l'information et la monnayer aux plus offrants. L'information, même d'apparence anodine, constitue après compilation, recoupements et traitements, une valeur marchande pour des groupes de mieux en mieux structurés. De ce point de vue, nous avons dépassé l'époque du vulgaire bricoleur solitaire qui, par jeu ou par défi, cherche à pénétrer les systèmes les mieux protégés. Les pirates d'aujourd'hui opèrent en bande, plus ou moins infiltrée par les mafias ; ils utilisent des recettes toutes prêtes qu'ils récupèrent sur des sites spécialisés et, contrairement à la légende, ne sont guidés par aucune éthique. Pour ces prédateurs d'un nouveau type, les laboratoires universitaires et les différents instituts de recherche constituent des cibles privilégiées. Nos principaux partenaires dans les collaborations internationales, qu'ils soient américains,

européens ou japonais, prennent très au sérieux ces menaces ; il arrive même qu'ils nous montrent du doigt pour ce qu'ils considèrent comme du laxisme de notre part. À l'évidence, notre organisme ne peut rester plus longtemps à l'écart de cette mobilisation et ignorer ces dangers, sans courir les risques graves de voir nos systèmes d'information se dégrader progressivement, notre patrimoine scientifique se faire piller et nos partenaires internationaux se détourner de nous, de crainte de compromettre leur propre sécurité.

La sécurité des systèmes d'information (SSI) au CNRS s'est toujours présentée dans un contexte spécifique difficile. Naguère encore, les mots mêmes de « sécurité » ou de « protection du patrimoine scientifique » étaient tabous. Le rôle du « Fonctionnaire de Défense » restait très obscur et pour certains inquiétant. Les correspondants sécurité étaient jugés comme accessoires, souvent inutiles. Les mises en garde sur les risques des réseaux ouverts ne suscitaient trop souvent qu'indifférence. La règle était « la science exclusivement ». Aujourd'hui, ce seuil est pour l'essentiel dépassé ; la grande majorité des personnels, dans la plupart des laboratoires, est prête à s'impliquer activement dans la mise en œuvre d'une véritable politique de sécurité pourvu qu'il trouve auprès de leur Direction un soutien et des orientations. Ce guide est fait pour aider les directeurs dans ce rôle.

1
Les menaces de l'Internet

En quoi l'interconnexion des réseaux – le réseau mondial – modifie-t-elle les exigences de sécurité ? Quelles sont les nouvelles menaces qui guettent nos systèmes d'information depuis l'ouverture des services d'Internet au «grand public» ? Ce sont des questions qu'aujourd'hui personne, surtout pas un responsable, ne peut ignorer.

1.1 La sécurité des systèmes d'information

Tout d'abord, qu'entendons-nous par « sécurité des systèmes d'information » ?

Systèmes d'information

L'information se présente sous trois formes : les données, les connaissances et les messages. On a l'habitude de désigner par « système d'information » l'ensemble des moyens techniques et humains qui permet de stocker, de traiter ou de transmettre l'information. De fait, on confond souvent, même si ce n'est pas très exact, la notion de « systèmes et réseaux informatiques » et celle de « systèmes d'information (SI) ». On dira donc qu'un système d'information est *« tout moyen dont le fonctionnement fait appel d'une façon ou d'une autre à l'électricité et qui est destiné à élaborer, traiter, stocker, acheminer, présenter ou détruire l'information »* (AGI n°900/SGDN).

Sécurité

Le concept de sécurité des systèmes d'information recouvre un ensemble de méthodes, techniques et outils chargés de protéger les ressources d'un système d'information afin d'assurer :

- la disponibilité des services : les services (ordinateurs, réseaux, périphériques, applications…) et les informations (données, fichiers…) doivent être accessibles aux personnes autorisées quand elles en ont besoin ;
- la confidentialité des informations : les informations n'appartiennent pas à tout le monde ; seuls peuvent y accéder ceux qui en ont le droit ;
- l'intégrité des systèmes : les services et les informations (fichiers, messages…) ne peuvent être modifiés que par les personnes autorisées (administrateurs, propriétaires…).

La « politique de sécurité » du laboratoire est l'expression de ces objectifs. Elle indique l'ensemble des mesures à prendre, des structures à définir et l'organisation à mettre en place afin :

- d'empêcher (ou tout au moins freiner) la détérioration, l'utilisation anormale ou la pénétration des systèmes et réseaux ;
- de détecter toute atteinte, malveillante ou non, à l'intégrité, la disponibilité et la confidentialité des informations ;
- d'intervenir afin d'en limiter les conséquences et, le cas échéant, poursuivre l'auteur du délit.

Valeur et propriétés d'une information

On ne protège bien que ce à quoi on tient, c'est-à-dire ce à quoi on associe « une valeur ». La trilogie confidentialité, intégrité, disponibilité, détermine la valeur d'une information. La sécurité des systèmes d'information (SSI) a pour but de garantir la valeur des informations qu'on utilise. Si cette garantie n'est plus assurée, on dira que le système d'information a été altéré (*corrupted*). Une altération

n'est pas uniquement le fait de malveillances. Il est plus souvent encore, la conséquence de pannes, de maladresses, d'accidents ou d'erreurs humaines dont les plus fréquentes sont les erreurs de conception. Ces phénomènes relèvent de la « sûreté de fonctionnement » qui est une autre manière d'appréhender la sécurité globale. Les sauvegardes, le fonctionnement en mode de repli, la redondance, etc. font aussi partie de la trousse à outils traditionnelle de la sécurité prise dans son sens général.

Avec le développement de l'informatisation des échanges (courriers officiels, transactions financières, commerciales…), la simple affirmation de la valeur de l'information n'est plus suffisante. Il est nécessaire d'y adjoindre des propriétés nouvelles comme l'authentification (garantie de l'origine d'un message, de l'auteur d'un document), la paternité (l'information ne peut pas être répudiée par son auteur), la traçabilité (on connaît le circuit qu'a suivi une information), etc. La préservation et la garantie de ces propriétés ressortent encore de la fonction « sécurité ».

1.2 L'agression par l'Internet

Les sources de dysfonctionnement des systèmes d'information sont diverses et variées. Elles ont le plus souvent des causes d'origine « humaines » :

- les sauvegardes sont mal faites ou mal gérées et rendent le système sensible aux pannes, aux maladresses et aux sinistres ;
- l'absence d'une vision globale de la sécurité, traitée par petits morceaux, au cas par cas débouche immanquablement sur un manque d'organisation (qui fait quoi dans quelle structure ?) et plus spécialement sur de mauvaises architectures réseaux ;
- le manque de consignes claires qui permettraient à chacun de savoir ce qu'il a à faire, ce qu'il peut faire et ce qu'il n'a pas le droit de faire.

Mais le nouvel environnement créé par l'Internet agit également sur la sécurité. Les réseaux mettent en relation entre eux des millions d'individus aux motivations très différentes. Il convient d'en connaître les dangers pour se protéger.

Les laboratoires sont raccordés à l'Internet par le réseau Renater, lui-même fédération de réseaux régionaux gérée dans la forme juridique d'un GIP. Internet est le réseau des réseaux. Il est mondial et ouvert. Il est bâti sur un protocole de communication normalisé (TCP/IP) et offre un ensemble de services distribués, dont les plus connus sont WWW alias HTTP pour la consultation des serveurs web, SMTP pour la messagerie, FTP pour le transfert de fichiers, TELNET pour l'accès interactif. Il en existe encore de nombreux autres, plusieurs dizaines… Les agressions par le réseau utilisent la plupart du temps une faille de sécurité dans l'un de ces services.

L'agression peut être « opportuniste ». L'agresseur a repéré (par un programme de balayage d'Internet) une possibilité de rentrer dans votre système, il en profite. Dans ce cas, c'est l'occasion qui fait le larron. C'est ce profil d'agression que nous débusquons le plus fréquemment dans nos systèmes, œuvre souvent de néophytes.

Une autre forme d'agression est l'agression ciblée, elle est l'œuvre de professionnels. Un professionnel du piratage est guidé par son avidité (intellectuelle, politique, religieuse, financière…). Son souci, c'est la discrétion, la rapidité et l'efficacité. Il a l'avantage de l'initiative : il sait quand, où et comment porter son attaque. Il dispose souvent d'information sous forme électronique (données). Il ne connaît pas les frontières (sauf pour s'installer sous la protection d'une législation laxiste). Il sait ne pas laisser de traces ou les effacer. Cette forme d'agression suit des principes précis :

- L'agresseur vous connaît ou commencera par effectuer une recherche de renseignements (caractéristiques de votre système d'information, équipements informatiques, centres de compétence, horaire de travail, effectifs…).
- Il a ses propres procédures et n'utilise pas forcément l'une des nombreuses méthodes d'attaque qui sont disponibles sur Internet.
- L'attaque porte surtout sur les maillons les plus faibles de la chaîne de traitement de l'information (personnel, télétraitement, maintenance…).

Contre ces attaques, l'ingénieur système est dans la situation d'un gardien de but à qui on aurait bandé les yeux. Exception faite de quelques virtuoses (il y en a dans nos laboratoires !) qui ont affiché de « belles prises » à leur tableau de chasse, ce type d'agression reste la plupart du temps indétectée.

1.3 Comment se manifeste une agression

Du temps où l'informatique était centralisée, les menaces « physiques » (pénétration dans des locaux informatiques sans autorisation, vol, vandalisme…) représentaient les menaces majeures. En ces temps bénis, la protection pouvait se résumer en quelques mesures de contrôle d'accès : grosses serrures, sas et gardiens étaient la panoplie usuelle. La situation est aujourd'hui bien différente. Certes, il y a toujours les vols de matériel, l'utilisation de la console maîtresse pour pénétrer un système ou le piégeage d'un réseau Ethernet ou public pour le mettre sur écoute ; mais globalement, la dangerosité de ce type de menaces, dont les remèdes sont connus et éprouvés, est sans commune mesure avec les agressions menées par le réseau, qui se réalisent sans la présence physique de l'agresseur. Ces agressions par le réseau ont maintenant très largement atteint un seuil critique et ont ne sait pas toujours quelle parade leur opposer. Dans le palmarès de cette nouvelle délinquance, on retrouve pêle-mêle :

Tout ce qui porte atteinte à l'intégrité du système

– Le piégeage de systèmes (bombes logiques, cheval de Troie, sniffeurs…) afin de nuire au laboratoire ou de se donner les moyens de revenir plus tard.
– La modification des informations afin de porter atteinte à l'image du laboratoire (exemple : modification des pages web du laboratoire).
– L'utilisation des ressources du site visé.
– Une intrusion en vue « d'attaques par rebond », c'est-à-dire qu'une autre cible est visée, votre système servant seulement de « point de passage ». Le laboratoire est alors complice involontaire du piratage.

Tout ce qui porte atteinte à la confidentialité des informations

– La récupération d'informations sensibles (mot de passe, articles avant publications, données personnelles, etc.).
– La fouille des messages, des données, des répertoires, des ressources réseaux…
– L'usurpation d'identité.

Tout ce qui porte atteinte à la disponibilité des services

– La paralysie du système (considéré ensuite comme un exploit par les pirates qui l'ont réalisée).
– La saturation d'une ressource (serveur, imprimante…).
– Les virus et vers informatiques.

1.4 Les techniques d'agression utilisées

Quelques exemples des techniques d'agressions par Internet, parmi les plus courantes, utilisées contre nos laboratoires, illustreront mieux notre propos. Les pirates commencent la plupart du temps par une recherche systématique des sites mal administrés.

La recherche de trous de sécurité sur les serveurs

Tout logiciel comporte des bogues dont certains sont des trous de sécurité, des anomalies qui permettent de violer le système sur lequel tourne le programme. Si c'est un programme d'application réseau, ces trous peuvent être exploités à distance *via* Internet. Les pirates recherchent systématiquement les sites mal administrés en procédant à un balayage de l'Internet avec des programmes appelés « *scan* ». Ces programmes découvrent à distance toutes les stations du réseau local et testent la présence de « vieilles versions » des logiciels réseau sur ces stations avec des trous de sécurité connus. Les vieilles versions de « *sendmail* », le serveur de courriers électroniques, sont les plus testées. C'est pourquoi, veillez bien à avoir toujours la dernière version d'un logiciel (surtout pour le *sendmail*) et filtrez les applications sur le routeur d'entrée et sur les serveurs (*cf.* chapitre 4.5).

Une fois le site mal administré repéré, l'exploitation des vulnérabilités est à la portée de n'importe quel malfrat : on trouve sur Internet des sites proposant des programmes tout prêts accompagnés de toutes les explications détaillées pour pénétrer les systèmes en utilisant les trous de sécurité connus.

Blocage des systèmes ou de la liaison d'entrée

Des méthodes (concrètement des programmes) sont très connues pour perturber fortement les systèmes et les réseaux et ont été très souvent utilisées ces derniers mois pour :

- Bloquer un système (par exemple en ouvrant à distance un grand nombre de connexions ou en émettant certains messages, « *pings longs* »). Les constructeurs ont corrigé ces erreurs dans les nouvelles versions de leurs systèmes. Une version récente installée sur chaque système constitue le remède.
- Surcharger la liaison d'accès à l'Internet d'un site (jusqu'à la bloquer) en envoyant des messages (*echo broadcast*) auxquels toutes les stations locales répondent engendrant ainsi un surcroît très volumineux de trafic. Un filtre adapté sur le routeur d'entrée est une bonne solution.

SPAM – Relais de messagerie

Un autre type de délit consiste à utiliser le serveur de messagerie d'un site pour envoyer des messages souvent publicitaires à un grand nombre de destinataires, en cachant son identité. Ce site sert alors de « relais » sans avoir donné son accord et son nom apparaît dans l'origine des messages. Cette attaque bloque la messagerie du site utilisé à son insu (surcharge des files d'attente dans le serveur), nuit à l'image du laboratoire (cela engendre des centaines de messages de protestation des victimes de ces publicités) et peut engager la responsabilité du laboratoire. Cette utilisation détournée est en très forte hausse ces derniers temps. Peut-être ce succès est-il dû à sa facilité de mise en œuvre et à l'anonymat qu'elle assure (*cf.* http://www.isoc.asso.fr/AUTRANS98/at-abus.htm).

Pour se protéger contre ce type de malveillance, il faut avoir un seul serveur de messagerie par laboratoire, bien administré, avec une version du logiciel serveur (*sendmail*) récente où la fonction « relay » est invalidée.

Intrusion dans un système

Pour prendre le contrôle d'un système, les agresseurs doivent commencer par s'y introduire. Il faut donc que quelqu'un (ou « quelque chose») leur ouvre une porte :

- un identificateur (login/passwd) a été « prêté » ou « récupéré » (vol de mot de passe) ;
- un compte a été laissé à l'abandon (sans mot de passe par exemple) ;
- une application réseaux installée a été mal maîtrisée (configuration mauvaise ou trop ouverte) ;
- une ancienne version d'un logiciel dont les failles de sécurité ont été publiées est encore en service sur une machine ;

– un logiciel installé « en mode *debug* », dont on oublie trop qu'il ouvre béant un trou de sécurité ;
– un utilisateur interne a aidé volontairement l'agresseur.

Un système qui a été pénétré – on dira que le système est « compromis » ou « violé » – n'est plus fiable : il faut le réinstaller ainsi que tous les systèmes du même partitionnement réseau. L'intrusion dans un sous-réseau complet ou dans un système, est « mère de toutes les malveillances ». Elle constitue la menace principale. Le milieu de la recherche y est extrêmement vulnérable.

Il n'est pas question, dans le cadre de ce guide, de rentrer dans les détails des diverses techniques d'intrusion, mais penchons-nous quelques instants sur celle qui reste, dans le palmarès des diverses techniques établi par Renater, l'incident le plus recensé : le vol de mot de passe.

La plupart des pirates informatiques sont loin d'être les « petits génies » décrits par une littérature complaisante. Leurs méthodes sont classiques. La plus utilisée commence par la récupération d'un couple « *login-password* » leur permettant de se connecter au système comme simple utilisateur. Ce premier pas franchi, le reste n'est souvent plus que jeu d'enfant ! Il y a sur l'Internet tout ce qu'il faut, programmes, modes d'emploi détaillés, description des méthodes, etc., pour lui permettre, une fois un compte utilisateur volé, d'acquérir les droits de l'administrateur (*root*, super utilisateur) en quelques minutes !

Quelles sont les méthodes utilisées pour découvrir un couple « nom – mot de passe » ?

- La première et la plus banale est la recherche des comptes sans mots de passe (guests, visitors…) qui sont installés par défaut sur certaines machines. Des programmes de balayage automatique de sites (les scans) permettent de trouver ces comptes.

- Des méthodes opportunistes dans lesquelles l'agresseur cherche à tirer profit d'une circonstance favorable :
  – Le mot de passe a été prêté.
  – Le mot de passe a été trouvé (par hasard ou non) sur un autocollant sous le clavier, dans le tiroir d'un bureau, dans un agenda, ou bien repéré à la dérobée au moment de la frappe.
  – Le mot de passe a pu être deviné grâce aux informations recueillies sur un utilisateur.

- Des méthodes systématiques dans lesquelles l'agresseur commence par la récupération du fichier des mots de passe chiffrés qui par défaut est accessible à tous sur les machines Unix. Une fois ce vol accompli, le pirate a tout son temps pour rechercher sur son PC, tranquillement chez lui, les mots de passe faibles du fichier. Avec CRACK, le programme bien

connu des initiés, un mot de passe tiré d'un dictionnaire (il y en a de toutes sortes qu'on peut télécharger à partir de l'Internet en différentes langues et sur différents thèmes), ou d'une composition proche d'un mot du dictionnaire, ne résiste pas très longtemps.

La sécurité commence donc par des mesures de précautions élémentaires pour limiter toute usurpation d'identité d'un utilisateur connu du système :

- Il faut avoir une procédure de réception des machines qui inclut la suppression des comptes sans mot de passe.
- Il faut sensibiliser les utilisateurs pour qu'ils adoptent des bons mots de passe et qu'ils les gardent secrets (*cf.* http://www.urec.cnrs.fr/securite/docs/92.07.mot.de.passe.txt).
- L'administrateur doit mettre en œuvre des fonctionnalités du système : pour cacher le fichier des mots de passe chiffrés (*shadow password*) et pour limiter la validité d'un mot de passe. Il doit tester la robustesse des mots de passe avec le logiciel CRACK (celui-là même qu'utilisent les pirates).

Écoute du réseau Ethernet

Un réseau Ethernet est fondamentalement un réseau « à diffusion » ; toute information qui circule sur ce réseau peut être captée par toutes les stations du réseau (même celles qui ne sont pas destinataires des messages). On peut donc espionner un réseau Ethernet. Un sniffeur est un programme installé sur une machine pour « écouter le réseau » et collecter tous les couples « *login/password* » qui transitent en clair sur l'Ethernet local. Ce programme peut être installé à distance, et on le retrouve dans presque tous les cas d'intrusion.

Quelques recommandations pour limiter ce problème d'écoute :

- Quand vous êtes « en déplacement », vous ne pouvez jamais être sûr qu'un sniffeur n'est pas installé sur le réseau sur lequel vous travaillez. C'est pourquoi, si vous devez vous connecter à votre laboratoire lors d'une invitation à l'étranger, utilisez plutôt un mot de passe provisoire ou un compte particulier.
- Quand vous êtes prévenu d'une intrusion, demandez que soit vérifié rapidement si un sniffeur n'a pas été installé. Si c'est le cas, il est indispensable de changer tous les mots de passe, sur toutes les stations. Sans cette précaution, vous pouvez être certain que l'« alien » y est toujours, et qu'après s'être fait oublier pendant quelques semaines, il réapparaîtra ! Le directeur doit intervenir pour faire comprendre à chacun cette mesure.
- On peut limiter la diffusion d'un réseau Ethernet (et ainsi réduire l'écoute possible) en utilisant des commutateurs, des routeurs, des concentrateurs (*hubs*) sécurisés. Cela fait partie d'une bonne architecture de réseau.

– La charte utilisateur est l'occasion de sensibiliser les personnels du laboratoire sur le caractère délictueux de ce comportement et de diminuer ainsi la « menace interne ».

Attaques des services réseau

Les serveurs web ou FTP anonyme ou de messagerie peuvent être facilement attaqués s'ils sont mal configurés ou mal administrés. Cette vulnérabilité, mais aussi la nécessité de contrôler la diffusion d'informations faite par le laboratoire, rendent impérative la maîtrise de tous les serveurs réseau. Il ne faut pas tolérer que des utilisateurs aux velléités individualistes installent des serveurs « sauvages ». Ils sont toujours mal administrés, donc vulnérables et mettent la sécurité de l'ensemble du réseau en péril. La charte et un réseau structuré sont les bons moyens d'arriver à faire comprendre et appliquer cette règle.

Comportements délictueux de certains utilisateurs de nos laboratoires

Certains utilisateurs ont des comportements inadmissibles qui doivent être corrigés ou sanctionnés :

– Échanges de mots de passe (fichiers de mots de passe) ou d'informations sur les failles éventuelles d'un site (entre étudiants de différents établissements).
– Envoi de message à caractère injurieux, raciste, pédophile, etc. ou mise à disposition (par des liens vers des URL indésirables) de ceux-ci sur des serveurs ftp ou web du laboratoire.
– Récupération (stockage et [re]diffusion) de logiciels connus pour être piratés (sur sites warez*), de contenus protégés par un droit d'auteur et dupliqués, ou de tous autres contenus répréhensibles au vu de la loi.

Ces comportements délictueux doivent être sanctionnés avec la plus grande détermination.

* Un site warez est généralement un FTP-anonyme, ouvert en écriture, «squatté» par des pirates qui y ont créé une arborescence cachée pour y déposer des binaires illicites (textes, photos, programmes piratés,…), afin de pouvoir les échanger anonymement dans des forums de discussions. Le laboratoire est ainsi compromis dans des trafics qui sont parfois extrêmement graves !

2
Le rôle du management dans la sécurité

La détermination et la supervision de la politique de sécurité sont des fonctions de direction. Rien de valable ne peut se faire sans le directeur : encore faut-il qu'il en connaisse tous les enjeux. L'argument « la sécurité, c'est le problème d'un administrateur système » n'est-il pas une forme de démission ? N'est-ce pas avouer qu'on cherche des solutions techniques à des problèmes qui sont d'abord organisationnels ? Certes, avec davantage de moyens, nous ferions plus et mieux. Certains laboratoires en savent quelque chose ! Cependant, à un moment ou à un autre, il faut bien faire avec ce qu'on a... le mieux possible. Cet autre argument, « la sécurité, ça coûte trop cher », n'est-il pas l'excuse facile au laxisme ?

2.1 À quoi sert la sécurité ?

Nous avons mentionné au début du chapitre précédent les causes diverses de dysfonctionnement d'un système d'information en précisant que le plus souvent elles étaient d'origines accidentelles ou avaient pour cause des défaillances techniques ou humaines. La SSI comporte donc une « composante sûreté de fonctionnement » dont l'objectif est d'agir sur les causes de ces dysfonctionnements et d'en réduire les conséquences. Mais nous avons vu que les menaces nouvelles, plus particulièrement celles liées à l'Internet, nous obligent à nous prémunir sur un autre plan : celui de la « protection contre la criminalité informatique ». C'est une préoccupation qui va croissante. Les statistiques sont parlantes. Elles montrent que la délinquance informatique est en forte hausse. Aux États-Unis (source : Ernst & Young), 42 % des sites informatiques ont signalé des attaques en 1997, contre moins de 16 % l'année précédente. Cette hausse signifie probablement aussi, une meilleure prise en compte de la sécurité (les sites signalent des piratages qu'ils ne voyaient pas auparavant). On remarque également une hausse significative de l'espionnage industriel : 38 % des attaques contre 6 % l'année précédente. D'autres études, réalisées à partir de simulations, ont montré que plus de 80 % des attaques ne sont pas détectées. Ces résultats sont significatifs de l'effort qui reste à accomplir en matière de sécurité.

En France, dans notre organisme en particulier, les statistiques fiables sur la délinquance informatique sont rares. Cette carence présente incontestablement un avantage, celui de masquer les problèmes et donc de permettre de les ignorer. Malheureusement, elle présente aussi l'inconvénient de laisser supposer que la situation n'est pas plus brillante qu'ailleurs. En particulier, pouvons-nous légitimement supposer que notre milieu universitaire est mieux loti ?

Mieux qu'un long développement théorique ou incantatoire, quelques anecdotes, tirées d'histoires vécues dans les laboratoires, feront comprendre la diversité des problèmes rencontrés.

Prêter, c'est donner !

Dans ce laboratoire, un gros effort avait été fait pour faciliter la connexion aux systèmes informatiques à partir de l'extérieur. Les chercheurs peuvent se connecter de chez eux sur leur station et travailler comme s'ils étaient à leur bureau. C'est pratique, d'autant que, en se faisant rappeler par le modem du labo, cela ne leur coûte que le prix d'une communication locale. La tentation est grande, cependant, de confier « à la famille » les mots de passe, et donc l'accès aux moyens informatiques de cet important laboratoire. Pour le gamin lycéen, c'est l'occasion de naviguer sur le web dans des conditions idéales et sans que les parents se fâchent à la réception des factures téléphoniques. Mais, très rapidement, les joies de la navigation sur le web s'affadissent, et, apprenant plutôt vite, le bambin passe à d'autres activités beaucoup moins innocentes. Le laboratoire travaille dans des domaines qui intéressent apparemment beaucoup de monde, car l'enfant se fait « contacter » par un groupe de pirates « internationaux » pour « échanger des informations ».

L'affaire est grave car elle touche à la sécurité de l'État. Que risque le gamin ? Le père est-il complice sans le savoir ? Quelle est la responsabilité du laboratoire ?

Receleur malgré soi !

Les sites warez, vous connaissez ? Il s'agit de sites sur lesquels des pirates internationaux déposent à travers l'Internet, à l'insu de l'administrateur du système, des logiciels piratés, des images pornographiques souvent pédophiles, des « documents » révisionnistes, etc. Les FTP anonymes en écriture libre (souvent le répertoire « *incoming* ») mal gérés sont l'une des cibles les plus fréquentes. Les sites warez servent de bourses d'échange entre pirates. Les victimes (de nombreux laboratoires CNRS en sont) sont ainsi transformées à leur insu en receleurs ou distributeurs de logiciels piratés, de photos pédophiles ou de textes révisionnistes. Ces délits peuvent se poursuivre pendant de longs mois avant que quelqu'un commence à se douter de quelque chose… C'est souvent pendant le week-end que les pirates mettent en place leur dispositif : le site warez est ouvert le vendredi soir vers minuit et refermé le lundi tôt dans la matinée. Tout le week-end, il a fonctionné à plein régime, mais le lundi matin, tout est redevenu « calme ». Une affaire grave a, il y a quelque temps, touché un grand laboratoire. Le soir du départ en vacances de Noël de l'ingénieur système, 700 Mo de photos pédophiles sont téléchargés dans le FTP anonyme du laboratoire. Elles vont y rester pendant les dix jours des vacances. Parallèlement, sur de nombreuses listes de diffusion, dans les forums de discussion, apparaît l'information : « Si vous êtes intéressé par des photos « hard-sex », allez sur… ». Pendant ces dix jours, le FTP du laboratoire a eu de très nombreux visiteurs… À la fin des vacances, les enregistrements journaliers de l'activité du site contenant les noms et les adresses de tous ceux qui ont extrait des photos pédophiles ont été récupérés par les pirates. Quel était leur but ? Se constituer un carnet de contacts « intéressants » ? Rechercher des noms de « personnalités » pour, éventuellement, exercer un chantage ? Compromettre le laboratoire ?

Détournement de sites

Un serveur web, quand il est administré par des personnes aux intentions malveillantes, peut servir à pirater les systèmes « clients » qui utilisent des navigateurs mal configurés. C'est la raison pour laquelle il faut être très prudent quand vous autorisez l'exécution d'applet Java, d'activeX ou même simplement qu'on vous demande de remplir un formulaire. Vous serez d'autant plus prudent que le site que « vous visitez » ne présente pas de garanties d'intégrité suffisantes. Mais lorsque le serveur est celui d'une « honorable institution » (comme un laboratoire), vous avez toute confiance et vous avez bien raison. Mais parfois… Nombreux sont les serveurs web qui se font pirater et sur lequel on retrouve des « sniffeurs » (dispositif permettant d'écouter les mots de passe). Pour installer un « sniffeur » sur une machine, il faut avoir les privilèges du super administrateur. Cela signifie que, outre que le pirate récupère tous les couples login/password qui circulent en clair (cas standard) sur le réseau, il a pris le contrôle total de votre machine serveur et qu'il pourra faire subir à vos « clients » tous les « derniers outrages à la mode ». Quelle est votre responsabilité juridique si la victime porte plainte ? Dans tous les

cas de figure, quelle est votre responsabilité morale, si vous n'avez pas pris toutes les mesures nécessaires pour prévenir ce type de délit ?

Histoire d'un courrier trop bien diffusé

Le courrier électronique, c'est facile, ce n'est pas cher… et ça peut coûter gros. Un cas récent le prouve une fois encore. La scène se déroule dans un laboratoire où campent de lourds conflits de personnes, malgré l'action énergique de son directeur qui essaye de reconstituer une dynamique d'équipe. Ce faisant, il est entièrement dans son rôle, mais il s'attire ainsi des rancœurs pugnaces. Certains n'ont pas hésité à espionner son courrier électronique et diffuser « pour information », « aux personnes concernées », des échanges de courriers confidentiels. But recherché : pourrir l'atmosphère du laboratoire. Objectif atteint ! Mais ces personnes qui se sont laissées entraîner par la dynamique de leur rancœur, savent-elles qu'elles ont commis un délit grave puni de trois ans de prison et 300 000 F d'amende (Art. 311-1 du nouveau code pénal) ? Si elles ont agi en groupe, la peine est encore aggravée au motif « d'association de malfaiteurs » (cinq ans et 500 kF) ! Que peut faire un directeur dans cette situation ? Comment peut-il la prévenir ?

Combien ça coûte ?

Le CNRS traite tous les ans plusieurs dizaines d'affaires de piratage ayant entraîné des dommages graves. Les cas courants sont ceux relatifs aux vols de « résultats de recherche » débouchant sur des produits industriels. Il est difficile de chiffrer le préjudice global – par manque de remontée d'informations –, mais tout laisse supposer qu'il est considérable… Un laboratoire constate des incursions de pirates sur une machine sensible, soupçonne une entreprise « aux mœurs légères », et, quelques jours après, retrouve dans la presse l'annonce d'un accord entre un grand éditeur de logiciel et l'entreprise en question sur la cession d'un produit très proche du leur. Montant de la transaction : 39 M$. Cette intrusion a coûté cher en « manque à gagner » ! Quant à vous, comment auriez-vous réagi ? Peut-on se faire aider ou conseiller ? Ne faut-il pas mieux « garder pour soi » l'incident ?

La confiance… oui, mais pas à n'importe quel prix !

De très nombreuses fois, lorsqu'une machine a été pénétrée dans un laboratoire, on retrouve, déposé par le pirate dans cette machine, un sniffeur. Ce programme qui tourne en permanence, écoute toutes les données qui transitent sur le réseau et en extrait les triplets nom/mot de passe/machine. Cette écoute inclut les connexions locales de machines à machines, mais aussi les connexions depuis ou vers l'extérieur qui ont transité par le réseau. Le pirate peut ensuite utiliser ces données pour pénétrer les machines distantes d'un autre site.
Une école d'ingénieur se fait attaquer par des pirates, les dégâts sont énormes : réinstallation du système sur les machines pouvant avoir été compromises (en fait, la plupart des machines), plusieurs mois de surveillance soutenue, des données importantes perdues, etc. L'école en question était bien protégée, la sécurité sérieusement prise en compte, le personnel compétent et bien formé, mais le pirate est

passé par un chemin détourné pour attaquer sa cible : il s'est servi d'un laboratoire « laxiste » comme rebond. Ce sont donc des collègues, par leur inconscience, qui ont ouvert les portes aux malfrats. Pourquoi investir dans la sécurité si des collègues moins rigoureux peuvent tout faire échouer ? Ne faut-il pas plutôt refuser les demandes de connexions venant de sites « à risque » ?

Ce que sauvegarder veut dire

Un brillant étudiant arrivait à la fin de sa thèse : trois ans d'un dur et passionnant travail ; des jours, des soirées, des week-ends passés en tête à tête avec son ordinateur. La rédaction était enfin terminée, il ne restait plus que quelques corrections de principe. Tout était sur le disque dur : les six chapitres, les annexes, les programmes, les calculs et les résultats soigneusement classés. Mais aussi tous les courriers électroniques : les avis critiques, les commentaires, les encouragements, les contacts pour un post-doc et les recommandations. Très prudent, il faisait ses sauvegardes soigneusement qu'il rangeait méticuleusement dans un tiroir de son bureau fermé à clé. Et pourtant… Un matin, quand il est arrivé à son laboratoire, on avait volé son ordinateur et forcé les tiroirs de son bureau pour voler les bandes de sauvegarde. La catastrophe, tout avait disparu !

Encore une mauvaise fiction ? Erreur ! Même si elle ne se termine pas toujours d'une manière aussi dramatique, cette histoire – avec de nombreuses variantes – arrive plusieurs fois par an. Le destin naturel d'un disque dur est de tomber en panne. Ce n'est qu'une question de temps… Circonstance aggravante, il tombe en panne toujours quand on s'en sert, c'est-à-dire quand on en a besoin ! Faire des sauvegardes est donc une précaution élémentaire. Élémentaire mais insuffisante, comme le montre l'histoire de cet étudiant. Dans combien de laboratoires, les micro-ordinateurs des secrétariats, sur lesquels il y a parfois toute la comptabilité ou d'autres informations tout aussi vitales, sont-ils sauvegardés correctement ?

2.2 Vulnérabilité et insouciance des laboratoires

Combien coûte la sécurité ?

On dit souvent « la sécurité, ça coûte cher », mais on oublie que l'absence de sécurité coûte plus cher encore. Ces quelques anecdotes le montrent amplement ! Tout l'art de la gestion du risque est de trouver le juste compromis entre « ce que ça coûte » et « ce que ça rapporte ». La SSI n'est donc pas une recherche mythique « du risque zéro », mais plutôt la recherche de l'organisation offrant la meilleure efficacité. Le bon niveau de sécurité, c'est celui au-delà duquel tout effort supplémentaire a un coût plus important que les avantages qu'on peut en attendre. Le coût de la prévention est donc à mettre en relation avec celui d'un éventuel incident de sécurité. Cette évaluation nécessite une claire conscience des dommages que peuvent causer les malveillances informatiques et des avantages qu'on retire d'une organisation adaptée.

Le « retour sur investissement » d'une politique de prévention est d'abord financier. Il s'évalue en dommages directs évités : pertes de données, de propriétés intellectuelles, de savoir-faire, d'informations…

Ces dommages sont souvent cités car leurs coûts sont visibles ; mais il ne faut pas oublier le coût en « organisation » des malveillances informatiques. Elles s'expriment par exemple en pertes de capacité et de productivité :

- indisponibilité des machines générant des pertes de temps (une intrusion peut « coûter » une coupure des services de plusieurs jours) ;
- immobilisation du personnel pour réparer ou pour attendre le retour à une situation normale (une intrusion coûte un quasi temps complet d'ingénieur système pendant près d'une semaine et un travail supplémentaire d'observation de l'activité pendant plusieurs mois).

C'est aussi une altération de l'image du laboratoire et, par contrecoup, de la confiance de partenaires industriels ou de collaborations de recherche, surtout si elles sont internationales. Les pertes d'image peuvent provoquer des ruptures de contrat, des pertes de crédit ou la mise en place, par les partenaires « inquiets », de procédures plus contraignantes de connexion sur leur site (dégradation de souplesse organisationnelle).

Sur l'Internet on voit aussi apparaître des « *black list* », liste des domaines avec lesquels il est risqué d'échanger du courrier électronique, des réseaux avec lesquels on ne doit plus communiquer. Un laboratoire peut être inclus dans ces listes noires par « dénonciation », si un de ses utilisateurs a émis trop de courriers publicitaires par exemple, ou si ses équipements sont mal configurés (comme le serveur de messagerie où la fonction relais n'est pas invalidée) et peuvent servir de tremplin à des pirates. Dès lors, ce laboratoire aura des difficultés de communication avec certains sites.

Ces pertes, souvent sous-estimées, parfois même ignorées, sont considérables prises globalement.
A contrario, une bonne politique de sécurité permet d'améliorer l'organisation, la recherche et les services. Le « retour sur investissement » s'évalue alors comme le prix qu'on est prêt à payer pour atteindre cet état.

Nos 100 millions d'«amis»

Nous sommes actuellement 100 millions d'internautes dans le monde : tous des amis ? Beaucoup de choses ont changé depuis l'ouverture d'Internet au « grand public », et c'est un euphémisme de dire que la « grande fraternité » des habitués du réseau n'est pas toujours bien respectée. C'est cette évolution que nous n'avons pas vu venir et qui nous dépasse encore très largement. Nous continuons à agir avec les règles qui étaient celles du temps où l'Internet était exclusivement le domaine de l'enseignement et de la recherche. Pourquoi des pirates s'en prendraient-ils à nos laboratoires ? Qui sont-ils ? Où voudraient-ils en venir ? Quels risques courrons-nous ?

Depuis quelque temps, les actes délictueux sont en forte augmentation et nous n'en détectons qu'à peine 10 % ! Ceux que nous repérons le plus facilement sont perpétrés par des pirates suffisamment maladroits pour laisser des traces flagrantes. Ils sont l'œuvre de non-spécialistes aux mobiles variés qui tentent leur chance à partir de « recettes » connues et publiées sur Internet.

Incursions dans les réseaux-passoires

« Le Figaro » a pu suivre le piratage de serveurs de sites sensibles. On y pénètre comme dans un moulin.

Christophe DORÉ

« Il y a des trous béants »

Nos hackers ouvrent d'abord un compte fictif chez un fournisseur d'accès à l'Internet. Faux nom, fausse adresse et, s'il le faut, faux numéro de carte Bleue. Sur son ordinateur, Julien compose le numéro du fournisseur d'accès. Quatre chiffres précédant le numéro d'appel normal camouflent l'origine de la communication. Puis les pirates choisissent leur cible. Ce soir, ils vont tester la vulnérabilité informatique d'un centre de recherche français.

Julien lance un programme qui va rechercher les références des ordinateurs mal protégés, suivant des critères définis à l'avance. Cela s'appelle un « scan ». Les lignes défilent sur l'écran : réseaux, sous-réseaux, ordinateurs... Des bons apparaissent avec d'autres adresses Internet comme le CEA ou l'Inserm, des universités américaines aussi... « Il y a des trous béants, c'est à peine croyable », commentent les deux informaticiens. En dix minutes, ils usurpent l'identité d'un utilisateur du réseau, M. Marco. De leurs ordinateurs, ils pilotent sa machine. Vingt minutes et des dizaines de lignes de programmation plus tard, ils sont « Root », autrement dit ils ont les pleins pouvoirs car le réseau les prend pour son responsable. Ils ont même la possibilité de lire les courriers électroniques des chercheurs. Un seul E-mail est ouvert pour vérifier. Ils ont aussi la possibilité d'entrer dans d'autres fichiers.

Volonté de nuire

Chaque manipulation sur le clavier de l'ordinateur ouvre un nouveau tiroir abritant d'autres documents comme s'ils avaient un passe pour ouvrir les portes de tous les bureaux du centre.

Certains documents ... rent des programmes ... cherche... On imagine ... concurrent direct don... beaucoup pour jeter un ... d'œil sur tout cela. Mais ... ne se fait pas », répon... plement Julien qui pr... peine d'effacer toutes ... de son effraction et se ... point d'honneur à ne rien ... rer sur le réseau qu'il ... sité.

Figure 1 : *Le Figaro* 20/03/98

On retrouve parmi ceux-ci :

- le mobile ludique : c'est celui des néophytes qu'on repère le plus fréquemment. Il aboutit parfois à des actes de malveillance, comme la destruction de données, pour tenter d'effacer les traces de l'intrusion ;
- le mobile de pure malveillance : la destruction des données est le but fixé. Cela peut être l'œuvre d'un collègue irascible ou jaloux, ou l'acte purement gratuit d'un malade qui cherche simplement à nuire (en hausse).

Les autres mobiles de la délinquance sont la recherche d'informations dans un but mercantile ou de concurrence et le piratage pour exploiter des ressources ou pour compromettre une machine (activité semble-t-il, en très forte hausse). Elles n'aboutissent pas, sauf maladresse de l'intrus, à la destruction des données.
D'autres types de piratage (les services spéciaux étrangers, les mafias, certains industriels…) laissent peu de traces visibles car ils sont l'œuvre de professionnels.
Le monde des réseaux a donc bien changé depuis quelques années et le « gentleman pirate » vanté par certains médias complaisants n'est qu'un mythe destiné à endormir notre méfiance. Nous devons nous protéger !

Le devoir de se protéger

Le besoin de sécurité augmente avec le rôle de plus en plus essentiel des systèmes d'information. Pourtant leur vulnérabilité va croissant et évolue de pair avec leur

complexité. Plus notre dépendance est grande vis-à-vis de ces systèmes, plus ils sont devenus fragiles :

– la technique avance plus vite que la sécurité ;
– la diversification des domaines d'application aboutit à une complexité accrue ;
– le « savoir-faire » et les moyens techniques se généralisent ;
– les mafias tentent d'organiser dans l'Internet des « zones de non-droit ».

Face à ces défis, il y a de grandes faiblesses : la méconnaissance des protections existantes, les comportements moutonniers, les effets de modes… Dans un passé encore proche, la menace principale contre les systèmes d'information était de nature physique. Aujourd'hui, avec l'augmentation des interconnexions, c'est une menace virtuelle et omniprésente à laquelle nous devons nous opposer.

Le réseau est notre outil de travail commun. Il est devenu indispensable à une recherche de qualité. Il ne dépend que de nous qu'il ne soit pas facile de porter atteinte à sa fiabilité, à ses performances, à l'intégrité et à l'accessibilité des informations transportées. Il ne dépend que de nous de refuser une dégradation de cet outil, notre outil, afin qu'il reste au service d'une bonne recherche et que nous ne soyons pas montrés du doigt par nos partenaires. La sécurité est ainsi un devoir collectif. Il revient à chacun de nous de se protéger pour ne pas mettre en danger la sécurité de tous.
Dans cet effort, les responsables, de tous niveaux, ont un rôle particulier à jouer.

2.3 La sécurité est une fonction de management

Un problème de généralistes qui agissent avec le soutien du directeur

La sécurité des systèmes d'information est une discipline transversale qui recouvre des aspects très variés. Elle est donc de la responsabilité de « généralistes » qui ont su acquérir plusieurs spécialités adaptées concrètement à l'installation dont ils ont la responsabilité. Ces « généralistes spécialisés » ne peuvent mener à bien leur mission qu'avec le soutien sans faille de leur directeur. Le directeur doit être informé des risques et des vulnérabilités de son système d'information ; il doit être conscient des enjeux pour qu'il puisse, avec l'aide de ces « hommes de l'art », définir la politique de sécurité du laboratoire et la faire appliquer.
Or qu'observons-nous dans notre organisme ? Peu de responsables, quel que soit leur niveau, savent si leur site a déjà été attaqué, si des données – les leurs peut-être – ont été volées. C'est un signe (qui ne trompe pas) de l'importance qu'ils accordent aux problèmes de sécurité. Mais comment peuvent-ils, dans ces conditions, désigner les menaces, mobiliser leur personnel, faire accepter à l'ensemble des acteurs la mise en place d'une politique de prévention et demander d'en vérifier l'efficacité ? Faut-il qu'ils attendent d'être confrontés à des situations pires encore que celles que nous venons de décrire pour qu'ils prennent la juste mesure des enjeux ?

C'est le directeur qui décide !

Certains directeurs croient que ce n'est pas dans leur rôle de connaître leur système d'information ou les risques qui pèsent sur lui, « pourvu que ça marche ». Qu'ils sachent que d'autres verront ce qu'ils ne veulent pas voir : ils prendront leur temps, mais ils le verront et sauront en profiter ! Qu'ils sachent aussi que personne d'autre qu'eux ne peut prendre les décisions d'organisation qu'implique la « sécurité ».

L'organisation est au service d'un objectif global. Les choix d'organisation exigent donc une intelligence d'ensemble. Le système d'information est l'épine dorsale de l'organisation, il est à son service, mais en même temps il la structure. Organisation et système d'information sont en étroite interdépendance. Faire des choix sur les structures, c'est placer les acteurs dans le système d'information. Inversement, agir sur le système d'information, c'est modifier, de fait, l'organisation.
La définition d'une politique de sécurité n'implique pas seulement des choix d'organisation, mais aussi de stratégie et de mobilisation du personnel. Il faut mettre en place des structures, distribuer des rôles («qui fait quoi ?») et fixer des objectifs. Il faut faire des arbitrages budgétaires, choisir le niveau du risque résiduel, juste compromis entre les vulnérabilités acceptées et les moyens qu'on est prêt à mettre pour les réduire. Est-ce la tâche du « généraliste spécialisé » dont nous avons parlé plus haut ? Non, car il n'a ni les perspectives globales, ni l'autorité nécessaire pour le faire. La définition de la politique de sécurité n'est pas un problème seulement technique, le rôle de « l'homme de l'art » est en aval : appliquer la politique qui a été définie, avec son conseil, par le directeur.

La sécurité des systèmes d'information est donc une fonction de direction, les aspects techniques ne venant qu'en second lieu. Sans l'implication personnelle du directeur, la sécurité va à vau-l'eau. Elle n'est plus alors, suivant les cas, qu'un discours incantatoire, une somme de vœux pieux répondant à des besoins hypothétiques ou une fuite en avant dans la recherche de solutions techniques à des problèmes de management.

C'est une démarche « qualité globale »

La sécurité est une partie de la sûreté de fonctionnement et réciproquement, suivant le point de vue que l'on adopte. Il faut l'aborder avec les mêmes méthodes. Par exemple, un système qui a été mal conçu (ou « monté au fil de l'eau ») ne fonctionnera pas bien ; il ne répondra pas correctement aux besoins et comportera des failles de sécurité plus ou moins béantes. Les problèmes de sécurité dégraderont davantage les conditions de fonctionnement qui agiront à nouveau sur la sécurité… et ainsi de suite. Un système d'information qui n'a pas été correctement conçu est impossible à sécuriser proprement. Une approche méthodologique doit donc être adoptée dès la phase de conception.
Cette nécessité d'une approche méthodologique rejoint un autre impératif, la « démarche qualité », rendue nécessaire par le caractère collectif de la recherche qui fait travailler ensemble des milliers de personnes, bien au-delà du laboratoire. La recherche n'est pas (l'a-t-elle jamais été ?) une entreprise solitaire et individua-

liste. Elle participe et dépend de la transmission des connaissances et des savoir-faire à travers les générations et par-delà les frontières.

La norme AFNOR NF X50120 définit la qualité comme « l'aptitude d'un produit ou d'un service à satisfaire les besoins des utilisateurs ». Cette conception exige non seulement une claire conscience de ces besoins, mais également une métrologie permettant d'apprécier le comportement du produit ou du service et de vérifier qu'il est conforme à ses spécifications. C'est ce qu'on appelle « le processus de contrôle de la qualité ». Il intervient de plus en plus en amont du « cycle de vie » des produits et services, ce qui impose une méthodologie dans leur conception et leur évaluation (méthodes formelles).

Le contrôle et l'évaluation de la qualité d'un système au sein d'une organisation partent de ces principes et ont donné lieu à des techniques spécifiques :

- élaboration de la politique de sécurité (règlement intérieur, chartes, définition des objectifs, utilisation des ressources…) ;
- élaboration du schéma directeur ;
- maîtrise de méthodes, techniques et outils utilisés pour la réalisation de projets (conduite de projet, AGL, gestion des configurations…) ;
- maîtrise des procédures d'exploitation ;
- etc.

La qualité des systèmes d'information participe de la « qualité globale » du processus de recherche, au sens de la norme ISO 9000. Cette norme s'imposera bientôt à tous. Ainsi est-il à prévoir, dans un avenir imminent, qu'elle intégrera réglementairement des contraintes de sécurité. On voit déjà émerger outre-Atlantique l'exigence d'une certification à un niveau de sécurité donné, comme pré-requis à toute collaboration, surtout lorsqu'il faut interconnecter des systèmes entre partenaires. Cette tendance se dessine très clairement dans les milieux de la recherche nord-américaine. C'est le cas, entre autres, du « *Stanford Linear Accelerator Center* ».

3
Sur quelles organisations s'appuyer ?

Qui, au CNRS, s'occupe de sécurité ? Que font-ils ? Quelle aide puis-je en attendre ? Au-delà de notre organisme, quelles sont les structures qui s'occupent de sécurité ? Ces questions ne sont pas sans intérêt car elles montrent qu'il y a une réelle mobilisation, d'abord dans notre organisme, mais aussi à l'échelle de l'État, pour prendre en considération la sécurité des systèmes d'information.

3.1 La sécurité dans l'organisation gouvernementale

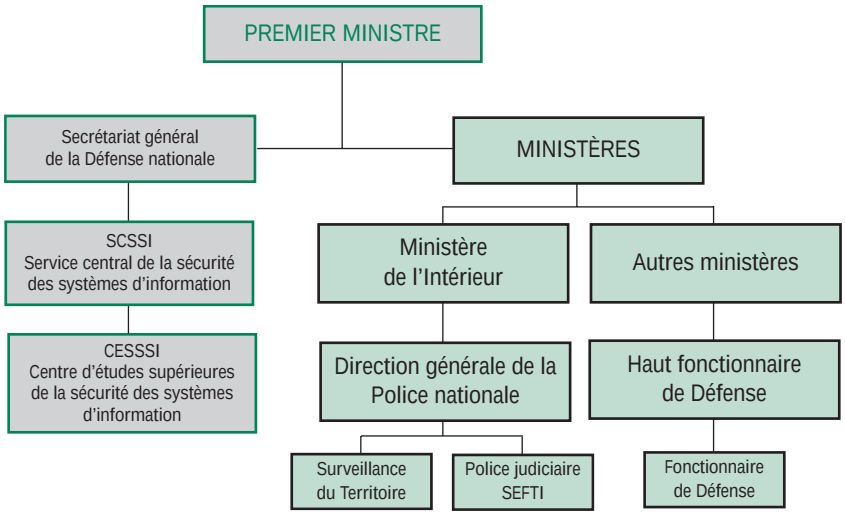


Figure 2

3.2 Protection du patrimoine scientifique et technologique au CNRS

Le Fonctionnaire de Défense du CNRS

La recherche publique française doit se nourrir d'échanges avec l'ensemble de la communauté scientifique internationale, mais elle doit simultanément protéger son patrimoine scientifique et technologique pour que la communauté nationale en soit le premier bénéficiaire.
C'est pourquoi, auprès du Directeur Général du CNRS comme auprès de tous les établissements publics scientifiques et techniques, se trouve un « Fonctionnaire de Défense », chargé de veiller qu'à l'occasion de coopérations internationales, de contrats, de missions hors de France ou d'accueils de chercheurs étrangers, ne se créent les conditions de transferts inopportuns de savoir, de savoir-faire ou de technologies.

Le patrimoine scientifique et technologique sensible

À l'origine, et dans un contexte mondial de guerre froide, les précautions à prendre concernaient principalement les domaines scientifiques susceptibles de débou-

cher sur des applications militaires et, plus particulièrement, sur la technologie des armes de destruction massive et de leurs vecteurs. Depuis dix ans, la menace d'une agression armée majeure contre le territoire national s'étant diluée au rythme où se mondialisaient les échanges, notre vigilance doit surtout s'exercer à l'égard des pays, potentiellement instables, qui cherchent à se doter d'armements nucléaires, biologiques et chimiques, ainsi qu'à l'égard de ceux qui les aideraient dans leur entreprise.

Ces « grandes oreilles » qui espionnent l'Europe

investi pour déjouer le « réseau Echelon », un système d'écoutes industrielles, financé par les États-Unis et la Gran

Comment le système Echelon contrôle les communications

Figure 3 : *Le Figaro* 10/04/98

Par les temps qui courent, c'est sur le terrain de l'économie et de la maîtrise des réseaux d'information que l'affrontement international devient le plus préoccupant. Les services de renseignement ont suivi cette évolution pour consacrer désormais 60 % de leurs activités à la recherche de l'information scientifique, économique et technologique. Parallèlement à l'apparition du concept d'intelligence économique se sont créées des entreprises privées, spécialisées dans le recueil, le traitement et la diffusion commerciale de telles informations.

Le patrimoine scientifique et technologique sensible d'un laboratoire est donc tout ce qui ne doit pas être mis à la libre disposition de tout un chacun, que ce soit pour des raisons stratégiques, économiques, voire dans le souci légitime de protéger la confidentialité d'informations nominatives.

Les vulnérabilités des laboratoires

Les méthodes traditionnelles de recueil (coopérations internationales, envoi de stagiaires et de visiteurs, photos et photocopies, vol de documents ou d'échantillons) gardent leur attrait et nous imposent de rester vigilants lorsque la relation entre le projet de recherche et la nationalité du « partenaire » présente une sensibilité particulière. C'est la raison pour laquelle un contrôle préalable est effectué sur les demandes de stages de chercheurs étrangers et sur les projets de coopération internationale.

Il est pourtant une manière bien plus discrète, rapide et efficace de s'approprier de l'information scientifique. Pourquoi se déplacer sur des milliers de kilomètres lorsque l'on peut, par les réseaux, pénétrer sur le système informatique d'un laboratoire et aller scruter la machine d'un chercheur particulier pour y consulter tout ce qu'il pense ingénument y avoir mis à l'abri. Si l'environnement des laboratoires de recherche publique (ouverture sur le monde, multiplicité des tutelles, nombreux utilisateurs non-permanents…) les rend particulièrement vulnérables aux attaques venues de l'extérieur, il ne faut pas pour autant baisser les bras.

3.3 L'organisation de la SSI au CNRS

Le CNRS a pris conscience progressivement des enjeux : c'est pourquoi il a mis en place des structures et désigné des responsables. Ces moyens sont mis en œuvre sur les trois niveaux traditionnels de notre organisme :

Au niveau central

Au niveau central existent une structure fonctionnelle et une structure opérationnelle. La structure fonctionnelle est constituée par le service du Fonctionnaire de Défense aidé de ses deux chargés de mission : un chargé de mission à la sécurité des systèmes d'information, Robert Longeon ; un chargé de mission pour la sécurité des réseaux (à mi-temps), Jean-Luc Archimbaud. Le Fonctionnaire de Défense participe aux travaux des instances chargées d'orienter la politique de l'Établissement en matière de systèmes d'information.
La structure opérationnelle est constituée au sein de l'UREC (Unité Réseaux du CNRS) d'une petite équipe animée par Jean-Luc Archimbaud, aidé de Nicole Dausque.

Au niveau régional

Au niveau régional a été mis en place un réseau de correspondants de sécurité informatique régionaux, en liaison étroite avec les correspondants sécurité des laboratoires. Ils ont été nommés sur la base du volontariat pour assumer, en plus de leurs tâches de service, un rôle de relais pour la diffusion de l'information et d'alarme en cas de problèmes, et organisent les formations sécurité dans leur région.

Au niveau des laboratoires

Au niveau du « terrain », le directeur de l'unité est responsable de la sécurité des moyens d'information de son unité. Il détermine la politique de sécurité de son laboratoire et les mesures à tenir en cas d'incidents. Il peut désigner parmi ses collaborateurs un agent chargé de la sécurité des systèmes d'information (ce qu'ont fait les unités d'une certaine taille) qui est alors correspondant sécurité du laboratoire. Les directeurs suivent, à leur prise de fonction, une formation qui comprend un module sur la protection du patrimoine scientifique.
Ces structures collaborent étroitement avec le CERT (*Computer Emergency Response Team*) Renater, cellule qui assure la coordination entre les membres de Renater et la liaison avec les réseaux étrangers dans la diffusion d'information, les alarmes, la recherche de l'origine des attaques et les mesures de préventions.

3.4 Les actions sécurité au CNRS

Plusieurs actions ont été menées et se poursuivent pour aider les laboratoires CNRS à améliorer leur sécurité.

La diffusion d'informations et de recommandations

La diffusion d'informations et de recommandations a été faite de manière variée. Citons pour mémoire :

- Le bulletin *Sécurité informatique*, bimestriel très largement diffusé dans les laboratoires et à l'extérieur du CNRS : (http://www.cnrs.fr/Infosecu/Revue.html).
- Des serveurs d'information de l'UREC (http://www.urec.cnrs.fr/securite/) et du Fonctionnaire de défense (http://www.cnrs.fr/Infosecu/accueil.html). Ces serveurs mettent en ligne des cours, des articles, des recommandations générales et officielles CNRS, des outils logiciels, et donnent différents pointeurs vers des serveurs spécialisés en sécurité.
- Des listes de diffusions électroniques fermées (140 correspondants sécurité de laboratoire) ou à accès contrôlé (sur les virus : http://www.services.cnrs.fr/Listes/liste.cgi?liste=sos-virus).
- L'organisation de différents cours en collaboration avec le SCSSI, les universités et la formation permanente du CNRS.

La diffusion d'antivirus

La diffusion d'antivirus (http://www.cnrs.fr/Infosecu/AVP.html) et de logiciels libres (http://www.urec.cnrs.fr/securite/outils/index.html).

L'édition de différentes recommandations

L'édition de différentes recommandations : charte utilisateur, installation et gestion d'un serveur WEB… (http://www.urec.cnrs.fr/securite/).

Les opérations sécurité

La mise en place d'opérations sécurité dans les délégations de Sophia, Marseille, Toulouse, Grenoble, Nancy, Gif et bientôt Orléans (*cf.* http://www.urec.cnrs.fr/securite/articles/ope.secu.html). Avec une méthodologie adaptée aux laboratoires, ces opérations ont pour but de sensibiliser les unités, les aider à faire un bilan de leurs vulnérabilités, à améliorer et organiser leur sécurité, à proposer des actions correctrices et des outils de sécurisation. Elles se poursuivront.

4
Quelques recommandations élémentaires

Aucune mesure qui permette d'améliorer la sécurité du système d'information du laboratoire ne doit être négligée, même si parfois elle paraît dérisoire par rapport à l'importance des besoins. Tout ne peut être fait en un jour. Une approche méthodologique nous aidera à déterminer le niveau de vulnérabilité accepté en même temps qu'elle nous permettra d'étaler dans la durée les investissements qu'exige la politique de sécurité. Bien souvent, quelques mesures élémentaires – qui ne coûtent que le mal qu'on se donne pour y réfléchir un peu – suffisent pour améliorer considérablement une situation qui paraissait désespérée : gérer le parc de matériel, gérer les comptes utilisateurs, mettre en place une architecture réseau adaptée...

Que voyons-nous, quand on étudie les causes des vulnérabilités dans les laboratoires ? Citons pêle-mêle, parmi les plus importantes :

– l'absence de méthodologie de sécurité ;
– l'absence de structure de sécurité ;
– l'absence de plan de secours (ou s'il y en a, il n'a jamais été testé) ;
– l'absence de formation : « *Les utilisateurs savent…* » ;
– la méconnaissance de la réglementation.

S'attaquer à ces causes de vulnérabilité permettrait d'éviter au moins 80 % des problèmes. Cela signifie :

– Mieux organiser, mieux prévoir et mieux sensibiliser.
– Appliquer des procédures de gestion des ressources informatiques.
– Mettre en place des moyens de protection active.
– Avoir une approche méthodologique.
– Concevoir une architecture structurée et cohérente.

4.1 Organiser, prévoir et sensibiliser

La sécurité, c'est d'abord s'organiser. C'est aussi prévoir les incidents et c'est informer.

Les structures de sécurité

Le directeur doit diriger les hommes et gérer les moyens. Il agit en déléguant ses pouvoirs et en distribuant les responsabilités, desquelles on lui rend compte. Pour la sécurité, dont fonctionnellement il est le responsable, il nomme – quand c'est possible – un correspondant de la sécurité informatique et réseaux qui l'informera, le conseillera et fera appliquer ses directives. Ce correspondant a une délégation de pouvoir sur tout ce qui concerne la sécurité et il en rend compte au directeur. Il est l'interlocuteur, mandaté sur ce problème, du laboratoire auprès des autorités et des entités liées au système d'information : la Direction scientifique, la Délégation, l'UREC, le service du fonctionnaire de défense, Renater, … Il participe à l'information et à la sensibilisation des utilisateurs. En particulier, il fait connaître les consignes sur ce que chacun doit faire s'il est victime ou s'il est témoin d'un incident de sécurité. Pour mener à bien l'ensemble de cette mission, le correspondant sécurité doit être lui-même particulièrement motivé et correctement formé.

En cas d'incident, savoir que faire et le faire savoir !

Un incident de sécurité est toujours, *a priori*, un événement grave. Si un utilisateur découvre des traces permettant de suspecter une malveillance quelconque sur une machine, il doit d'abord, et avant toute chose, en informer le directeur. Mais ce n'est pas tout. Il faut aussi empêcher que le mal s'étende en prévenant ceux dont la charge est d'essayer de garder la sécurité au réseau. Il faut également isoler les

systèmes qui ont été violés, faire le bilan des dégâts et enregistrer tout ce qui peut permettre de retrouver l'origine de l'agression. Ce n'est qu'après tout cela que, finalement, on peut commencer à réparer.

En résumé, lors d'un incident, il faut :

1. Déconnecter du réseau, la ou les machines suspectées, ou mettre un filtre qui empêche tout accès de l'extérieur.
2. Effectuer une sauvegarde du système pour conserver les traces de l'incident.
3. Avertir le CERT Renater http://www.urec.fr/securite/chartes/fiche_suivi_incident.txt.
   et envoyer une copie à mayday@urec.cnrs.fr (message qui arrivera dans la boîte à lettres de N. Dausque, R. Longeon, et J.-L. Archimbaud)
4. Faire le bilan des dégâts :
   http://www.cru.fr/securite/Documents-generaux/Recommandations.html
   En particulier il faut vérifier toutes les machines du réseau et contrôler s'il y a un sniffeur installé. Si c'est le cas, changer les mots de passe de tous les utilisateurs sur toutes les stations.
5. Réinstaller le système et les comptes utilisateurs.
6. Ne donner aucune information sur l'incident à des tiers non habilités.

Si vous désirez déposer une plainte, contacter le Fonctionnaire de défense (p.schreiber@cnrs-dir.fr, tél. : 01 44 96 41 88).

Ne pas avoir honte de s'être fait pirater !

Certains hésitent à faire partager leur expérience d'un incident de sécurité par peur d'être mal jugés. C'est une erreur, car se faire pirater arrive aux meilleurs d'entre nous. Au contraire, ils peuvent être fiers de s'en être aperçus, c'est la marque d'un système bien géré ; si de surcroît ils font remonter l'information à ceux qui en ont besoin pour assurer la sécurité à l'échelle de l'organisme tout entier, ils rendent un service inestimable à la collectivité. Les mesures de sécurité qui sont prises par l'organisme dépendent de ces remontées d'incidents.

Les incidents de sécurité sont très nombreux dans nos laboratoires. Globalement, leurs coûts budgétaires, au niveau des unités comme au niveau de l'organisme, sont loin d'êtres négligeables. Mais le plus grave, c'est qu'ils compromettent également la qualité de la recherche, c'est-à-dire la raison d'être de notre organisme.

On évalue que moins de 10 % des incidents de sécurité sont actuellement détectés. Parmi ceux-ci, moins d'un tiers nous est signalé. Parmi ceux qui nous ont été signalés en 1997, nous avons considéré que près de cinquante cas présentaient un caractère gravissime, soit un cas sur deux. Trois plaintes, dont une avec constitution de partie civile, ont été déposées auprès des services de police compétents. Elles concernaient cinq unités propres du CNRS, travaillant sur des domaines sen-

sibles et victimes de pénétrations malveillantes. L'un des cas pourrait, si l'enquête de police le confirmait, couvrir une action d'intelligence économique menée depuis un pays étranger.

4.2 Procédures de gestion des ressources informatiques

Veiller au respect de la législation en vigueur

Parmi les règles élémentaires de bonne gestion, la première est de veiller à ce que les lois, le code général de la fonction publique et le règlement intérieur du laboratoire soient respectés scrupuleusement par chacun. Les textes législatifs les plus importants à connaître sont rappelés au chapitre 5.1.

Rappelons plus particulièrement qu'il est de la responsabilité du directeur de veiller à ce que :

- toutes les mesures soient effectivement prises, pour empêcher le piratage ou l'utilisation de logiciels piratés dans son laboratoire ;
- tous les fichiers nominatifs aient été déclarés à la CNIL suivant la procédure adéquate (*cf.* chapitre 8.1) ;
- les webs du laboratoire ne violent pas la législation sur la propriété intellectuelle, respectent les recommandations du « Comité web » du CNRS (*cf.* chapitre 5.2.) et ne portent pas atteinte à l'image du CNRS (pas de pages personnelles n'ayant rien à voir avec les missions du laboratoire par exemple) ;
- les moyens informatiques du laboratoire, en particulier le réseau qui est une ressource « rare et chère », ne soient pas exagérément détournés de leurs finalités professionnelles.

Pour que l'ensemble de ces contraintes – qui s'imposent à tous – soit bien clair et porté à la connaissance de chacun, il est indispensable de proposer à chaque utilisateur, une charte du « bon usage des moyens informatiques ». Elle doit être annexée au règlement intérieur (*cf.* annexe A et http://www.cnrs.fr/Infosecu/Charte.html).

Une gestion du parc informatique

L'administrateur système doit avoir la connaissance et la maîtrise de tous les équipements informatiques (même « personnels ») et réseaux. Il doit tenir à jour la liste des équipements (stations, routeurs, imprimantes…), des prises réseaux (localisation, utilisateur connecté sur cette prise). Il doit tenir la liste à jour des espaces disques, de leur type de montage, de leur protection et de leur affectation.
Dans les petites unités où il n'y a pas d'ITA, une personne du laboratoire doit néanmoins centraliser toutes les informations concernant ces équipements et faire office de responsable informatique même si ce n'est pas son travail de base.

Une procédure d'installation des nouvelles machines

Même s'agissant d'une « station personnelle » où l'utilisateur administre sa propre machine, il faut appliquer une procédure d'installation.

1. Faire une sauvegarde des fichiers de configuration et une empreinte du système en utilisant un logiciel tel que tripwire (*cf.* http://www.urec.cnrs.fr/securite/outils/index.html). Automatiser cette procédure pour pouvoir la refaire après les mises à jour ou l'installation de correctifs.

2. Tenir à jour la liste des logiciels (systèmes de base, applications, services…) avec leurs implantations, leur fournisseur et numéro de licence. Il est préférable que cette liste soit centralisée.

3. Supprimer les services réseaux déclarés et inutiles (demons).

4. Installer ce qui est nécessaire pour avoir des accès journalisés et contrôlés (tcpwrapper par exemple).

Installez les correctifs de sécurité ?

Dès qu'une faille de sécurité est annoncée par les CERT, elle est immédiatement exploitée. Il faut donc passer les correctifs (*patchs*) le plus tôt possible, car c'est alors une course poursuite entre l'administrateur système qui doit mettre à jour ses machines en permanence et les pirates qui espèrent, en utilisant la toute dernière faille, prendre en défaut un certain nombre de machines.

Cependant la plus grande prudence est de mise dans le choix du serveur lorsque vous voulez télécharger un logiciel. Certains sites piègent les logiciels qu'ils proposent (cheval de Troie, bombe logique, etc. *Cf.* chapitre 7). Alors ne faites confiance qu'aux sites connus et reconnus et vérifiez les « *signatures** ». Cette précaution est utile pour tous les « outils » de sécurité dont il faut se méfier *a priori*. Elle l'est plus encore pour les correctifs systèmes.

La gestion des comptes des utilisateurs

– Chaque compte doit appartenir à un utilisateur clairement identifié. Proscrire les accès banalisés (guest, visitor, invité…).
– Pour chaque nouvel utilisateur, mettre en service une procédure d'entrée : signature de la charte, attribution d'espace disque, machine, compte, ressources allouées.
– Vérifier régulièrement que tous les comptes ouverts sont encore d'actualité. Les comptes inutilisés depuis plus de trois mois doivent être fermés.
– Vérifier régulièrement la solidité des mots de passe (avec un logiciel tel que « crack » : *cf.* http://www.urec.cnrs.fr/securite/outils/index.html). Il

* Valeur permettant de vérifier si le contenu d'un fichier à été modifié.

est recommandé que les utilisateurs changent régulièrement leurs mots de passe (cela implique une procédure à mettre en place et à gérer).
– Créer une procédure de sortie de l'utilisateur : l'administrateur système doit être informé immédiatement du départ d'un utilisateur, les comptes provisoires (thésards, stagiaires, visiteurs) ne peuvent être laissés à vau-l'eau.

La gestion du libre-service

Le libre-service est géré, et les consignes impératives, telles que la déconnexion après usage, sont clairement affichées. Les stations en libre-service sont sur un sous-réseau particulier, avec des droits restreints et très contrôlés. Toute machine en libre-service doit être considérée comme aussi dangereuse qu'une machine externe au laboratoire.

4.3 Moyens de protection active

Contrôle des accès physiques dans certaines parties du laboratoire

Certains fichiers peuvent présenter un degré particulier de confidentialité. C'est le cas des fichiers nominatifs dans certaines recherches médicales par exemple. On trouve aussi cette particularité dans des collaborations industrielles où des clauses de confidentialité sont imposées par contrat, ou dans des laboratoires qui utilisent des matériels particuliers. Le responsable doit alors proposer des moyens spécifiques pour mettre en œuvre des mesures de sécurité particulières. Ce peut être des contrôles d'accès plus stricts, ou bien de chiffrement des données et/ou des communications ; ce peut être aussi la décision de ne pas connecter une machine « sensible » au réseau. Associé à un contrôle des accès, l'isolement d'une machine est le moyen le plus sûr que l'on connaisse pour protéger les données qu'elle contient. S'il faut que certains serveurs soient physiquement protégés et placés dans des locaux à accès sécurisés, il peut être judicieux de définir différentes zones dans le laboratoire : une zone à accès libre et une zone où l'accès est contrôlé.
Plus particulièrement, il ne faut pas perdre de vue qu'un ordinateur, surtout un PC, est une proie tentante pour les voleurs. Il n'y a guère d'autre moyen de le protéger que de fermer les portes des bureaux à clé et de contrôler les entrées dans le laboratoire.

Les sauvegardes

Il faut effectuer régulièrement des sauvegardes, on ne le dira jamais assez. Le mieux est d'édicter des règles précises qui permettent d'être sûr qu'elles sont faites correctement : qu'est-ce qu'on sauvegarde ? Avec quelle périodicité ? Avec quels recouvrements ? Ces règles définissent aussi où doivent être rangés les supports des sauvegardes, de façon que :
– en cas de sinistre ou de vol, elles ne soient pas perdues avec la (ou les) machine(s). Ne pas laisser la sauvegarde à proximité du système qu'elle est sensée protéger est une évidence… qui n'est pas toujours partagée ;

– elles ne soient pas à portée de main du premier venu, surtout si elles contiennent des fichiers confidentiels : rien ne sert de bien protéger son système si les sauvegardes sont en accès libre pour tous !

N'oubliez pas qu'il faut vérifier les sauvegardes. On sait d'expérience que des sauvegardes jamais testées en restauration révèlent de grosses surprises. Comme par hasard (mais est-ce vraiment un hasard ?), c'est le jour où on en a réellement besoin qu'on s'aperçoit des problèmes… et de la catastrophe que représente la perte d'un travail de parfois plusieurs mois.

Dans les secrétariats des laboratoires, domaine de la bureautique par excellence, il est très fréquent qu'il n'existe aucun moyen de sauvegarde. Il y a pour cela des raisons historiques : les documents importants étaient jusqu'à présent sauvegardés sur disquettes. Les disques durs des machines de bureau ont atteint aujourd'hui de telles capacités qu'il est devenu impossible de les sauvegarder par ce moyen. Il faut donc associer, aux machines de bureau, des dispositifs de sauvegarde spécifiques. Rappellerons-nous qu'un disque dur est destiné à tomber en panne un jour ou l'autre… même celui de votre secrétaire !

Détection des attaques

Une protection efficace ne peut se limiter à renforcer la « solidité » des systèmes. Il faut savoir que, tôt ou tard, il sera attaqué avec succès, souvent de façon totalement inattendue et avec des conséquences imprévues. Il faut être capable de détecter ces attaques, de les contrôler et d'assurer que les dommages seront réduits.

L'enregistrement de l'activité réseau anormale permet une première possibilité de détection :

– il faut installer des dispositifs de détection des tentatives d'intrusion au niveau des équipements d'entrée (alarmes générées par les filtres sur les routeurs) et des stations (messages de tcp_wrapper par exemple, *cf.* http://www.urec.cnrs.fr/securite/outils/index.html) ;
– il faut veiller à l'examen quotidien de ces alarmes.

Sur les stations :

– il faut veiller à ce que la comptabilité soit effectivement vérifiée afin de repérer les comptes qui ne consomment plus de ressources et les fermer, ainsi que ceux dont les consommations sont insolites ;
– il faut s'assurer que les systèmes sont vérifiés régulièrement de façon à détecter leurs modifications anormales. Ces vérifications doivent être faites plus attentivement en périodes d'alertes (annonces d'intrusions sur des sites avec lesquels on est en relation, par exemple).

Procédure d'alerte

Il faut définir la conduite à tenir en cas d'intrusion ou de malveillance informatique. Un utilisateur qui détecte un fait « anormal » doit avertir le correspondant

sécurité du laboratoire. Ce dernier doit coordonner, avec le directeur, les mesures à prendre en suivant les recommandations « Que faire en cas d'incidents ? » décrites chapitre 4.1.

Existence d'une procédure de repli et de remise en service après sinistre

Il n'y a rien de plus angoissant qu'un incident de sécurité lorsque vous ne savez pas quoi faire ; c'est pourquoi il faut avoir réfléchi à l'avance à la conduite à tenir. Il est bon d'avoir envisagé les conséquences de quelques incidents types et d'avoir étudié les réponses possibles. Dans certains laboratoires, les conséquences de dysfonctionnement peuvent être trop graves pour être négligées : il est parfois nécessaire de maintenir un certain niveau de service, même dégradé, pendant la phase de restaurations du bon fonctionnement du système. Cette question se pose, par exemple, pour les serveurs vitaux du laboratoire tels que les serveurs de fichiers ou de messagerie.

4.4 Avoir une approche méthodologique

Pour savoir « comment faire »

Bon nombre de responsables ne savent pas comment aborder « la sécurité ». N'ayant pas de méthode, ils procèdent au coup par coup, errant du « *de toute façon, ça ne sert à rien* », au « *vaut mieux en faire de trop que pas assez* ». Ainsi mal pensée, la sécurité aboutit tantôt au verrouillage complet du système – tout en laissant des vulnérabilités béantes –, tantôt à une démobilisation totale et à un laxisme irresponsable.

Une « approche méthodologique » consiste à élaborer des modèles, définir des procédures, caractériser les « cycles de vie »… Un système se construit toujours suivant des modèles. Quand il n'y en a pas, ils sont en réalité implicites. Alors chacun dans l'organisation projette inconsciemment les siens propres. Les décisions sont prises au coup par coup, d'une manière erratique en fonction des rapports de force, des humeurs du jour, des modes et souvent de la pression commerciale des constructeurs. En revanche, si les modèles sont explicites, les décisions sont cohérentes et raisonnées. Elles peuvent être mauvaises si la modélisation est fausse, mais on peut alors l'adapter, ce qu'on ne peut évidemment pas faire avec une « modélisation implicite ».

Pour savoir « ce qu'on veut »

Les modèles définissent, à chaque moment du cycle de vie du système d'information, des règles sur « les ressources », les « contraintes », les « fonctions » et les « produits ». Ils expriment :

– ce qu'on veut protéger et pourquoi,
– le niveau de protection dont on a besoin,

– contre quoi protéger,
– comment protéger,
– l'effort qu'on est prêt à faire pour assurer cette protection.

Pour savoir « où on va »

Nous avons vu au chapitre 2 que la qualité d'un produit est définie comme « l'adéquation de celui-ci à sa fonction » et que, dans la « démarche qualité globale », on fixe cet objectif dès la phase de conception, pour le système tout entier. Or une mauvaise appréciation des menaces (maladresse, malveillances, défaillances, accidents, sinistres…) est une cause majeure du dysfonctionnement des systèmes d'information dont l'origine se situe bel et bien dans la conception du système lui-même. C'est pourquoi la « sécurité d'un système » et la « qualité globale » sont deux approches similaires se confondant en bien des points de vue. En particulier, on cherchera à intégrer la sécurité dès la phase de conception d'un système, comme dans « l'approche qualité ».

La sécurité se dégrade dans le temps ; on ne peut pas croire qu'on va « faire un coup » et s'en tenir quitte pour plusieurs années. L'effort doit être permanent ! La reconnaissance des « cycles de vie » d'un système permet, entre autres choses, d'appréhender son évolution et de planifier sur plusieurs années cet effort en moyens et en organisation.

Pour savoir « limiter le problème »

La sécurité, entend-on parfois, est « tout ce qui permet de rendre sans effet une menace sur des biens sensibles ». Mais la sécurité absolue n'existe pas et il faut souhaiter bon courage à ceux qui se fixent de tels objectifs ! Plus prosaïquement, l'approche méthodologique permet de déterminer le niveau de sécurité efficace, grâce à des critères qui permettent de faire des choix en comparant simplement des investissements à des rendements. Au fond, c'est bien le seul critère qui vaille, quand il faut gérer des moyens…

4.5 Les phases d'une méthode adaptée aux laboratoires

Les trois phases d'une approche méthodologique qui nous importent ici sont :
– l'élaboration d'un modèle ;
– l'élaboration d'une politique de sécurité ;
– l'élaboration d'un tableau de bord.

Toutes les méthodes ont leurs originalités, mais toutes partent d'un modèle qui est une manière de poser correctement le problème. Elles aboutissent toutes à ce qu'il faut faire (la politique de sécurité) et donnent les moyens de mesurer les écarts entre ce que l'on souhaite et ce que l'on a réellement (le « tableaux de bord »).

Dans la plupart des méthodes classiques, le modèle est formel ou semi-formel. Ce type de modélisation est bien adapté aux systèmes d'information qu'on appelle complexes, parce que les éléments y sont fortement dépendants (exemple : les grandes unités administratives). En revanche, il constitue, nous semble-t-il, un frein à l'adoption d'une approche méthodologique quand il faut l'appliquer à des structures plus simples comme celle d'un laboratoire. Pour ces organisations légères, nous préconisons « les modèles réels » dans lesquels le système physique est décrit sans formalisme, tel qu'il est perçu. Ce type de modélisation a ses limites : les interrelations « échappent » au modèle et restent donc implicites (les combinaisons de vulnérabilités par exemple). C'est le prix à payer pour conserver la simplicité, condition *sine qua non* pour qu'une méthodologie soit acceptée dans les laboratoires.

Concept de modèle réel

Ce type de modélisation permet de décrire précisément « ce que l'on veut » avec les moyens dont on dispose dans le cadre des contraintes existantes. Elle donne une « vision » (ou une mesure) des menaces, des risques et des vulnérabilités, ce qui permet de dégager des critères de « maîtrise de la sécurité » (gestion du risque) et d'éviter d'errer entre les deux attitudes extrêmes, intégriste ou laxiste, que nous avons vues précédemment.

Qu'est-ce qu'une menace ?

Une menace (M_i) est un danger qui existe dans l'environnement d'un système indépendamment de celui-ci : accident, erreur, malveillance. Une malveillance est l'action d'individus et/ou d'organisations qui exploitent des vulnérabilités dans les systèmes d'information. Une malveillance peut être :

– passive : elle ne modifie pas l'information et porte essentiellement sur la confidentialité ;
– active : elle modifie le contenu de l'information ou le comportement des systèmes de traitement.

La vulnérabilité

Une vulnérabilité (V_i) est une faiblesse du système qui le rend sensible à une menace :

– bogues dans les logiciels,
– mauvaises configurations,
– erreurs humaines,
– services permis et non utilisés,
– virus ou chevaux de Troie,
– saturation de la liaison d'accès à l'Internet,
– logiciels en mode « *debug* », …

Pour déterminer les vulnérabilités d'un système d'information, on vérifiera donc :

- si le système fait tout ce qu'il doit faire, s'il le fait correctement et s'il ne fait que ce qu'il doit faire,
- s'il est bien impossible au système de faire ce qu'il ne doit pas faire.

Il n'est évidemment jamais possible d'apporter des réponses sûres et complètes à ces questions. La difficulté vient de la complexité* des systèmes.

Le risque

Le risque est la probabilité qu'une menace particulière puisse exploiter une vulnérabilité donnée du système. Pour les habitués du formalisme mathématique, on pourrait écrire :

$$\text{Risque} = \Sigma^{i} \quad (M_i \times \Sigma^{j} \; V_i^j)$$

Traiter le risque, c'est prendre en compte les menaces et les vulnérabilités.

Une information présente une certaine vulnérabilité. On lui assure un niveau de protection, qui a un certain coût. L'écart entre la menace virtuelle et son niveau de protection correspond au risque (accepté ou résiduel).

Il y a des risques spécifiques dans les milieux de recherche, liés aux menaces de l'environnement expérimental des laboratoires : risque chimique, risque incendie, risque inondation (surtout pour le laboratoire de l'étage du dessous…), risque électrique, etc. Contre ce type de risque qui menace l'intégrité physique de nos systèmes d'information, la seule planche de salut, répétons-le, c'est une sauvegarde correctement effectuée et correctement stockée.

La politique de sécurité

Déterminer une politique de sécurité, c'est définir des objectifs (ce qu'il faut protéger), des procédures, une organisation en fonction de moyens. La démarche est récursive : après un problème de sécurité, la politique est ajustée. Les procédures, les moyens et parfois l'organisation sont adaptés. Parfois, il faut réviser à la baisse les objectifs.

Il est important de définir correctement les règles du modèle : ce qui est autorisé et ce qui ne l'est pas (il est interdit de lire le courrier de son voisin sans y être invité, même si celui-ci n'a pas su le protéger correctement…). Il est absurde – mais on le voit souvent – de vouloir verrouiller les entrées, définir des interdictions alors qu'on n'a pas su définir les règles auxquelles devraient se référer ces actions.

La politique de sécurité est élaborée à partir du modèle défini précédémment :

- analyse des menaces potentielles ou réelles ;
- identification et l'analyse des vulnérabilités (audit, contrôle qualité…) ;
- évaluation des risques et la détermination du niveau de risque admissible.

* Un système complexe est un système composé d'un très grand nombre d'éléments en interrelation les uns avec les autres.

Elle se réalise par :

– l'intégration d'outils et de services de sécurité système ou réseau (audit, contrôle d'accès, identification, logiciel antivirus, systèmes experts, noyau de sécurité…) ;
– la validation logiciel/système (techniques formelles, analyse qualimétrie, tests statiques et dynamiques, etc.) ;
– l'évaluation et la certification des systèmes et des produits.

La sécurité ne doit pas rester statique car toute défense peut être contournée ; c'est pourquoi une bonne politique de sécurité comprend toujours deux volets :

1. La sécurité *a priori* (politique dite « passive ») : c'est le blindage du système. Elle se caractérise par l'élaboration d'une politique de sécurité explicite, une organisation adaptée à cette politique, des procédures des méthodes de travail, des techniques et des outils…

2. La sécurité *a posteriori* (politique dite « active ») : c'est la défense « en profondeur »… Elle consiste par exemple à :
   – surveiller les moyens de protection pour contrôler leur efficacité (mais aussi l'efficacité de la politique de sécurité) ;
   – détecter les attaques et les mauvaises configurations en enregistrant les accès aux services sensibles, en mettant en place des automatismes de détection d'intrusion, etc. ;
   – répondre par des actions correctives : arrêt de session, reconfiguration dynamique des systèmes de contrôle d'accès, enregistrement des sessions ;
   – mettre en place des leurres.

Le tableau de bord

Il faut concevoir des indices statistiques afin de constituer des « tableaux de bord » qui permettent d'évaluer l'impact de la politique de sécurité sur la qualité de la recherche, l'organisation et le management. Ces tableaux de bord constituent une véritable métrique de la sécurité.

– Ils mesurent la vulnérabilité résiduelle d'un système d'information et permettent d'apprécier son évolution.
– Ils évaluent l'efficacité de la politique de sécurité.
– Ils indiquent les modifications de l'environnement.
– Ils alertent sur l'apparition de nouvelles faiblesses.

Cette métrique permet de « piloter » la politique de sécurité en mettant en évidence les adaptations qui s'avèrent nécessaires au fil du temps. Elles sont aussi des « aides à la décision » indispensables. En effet, ils donnent les moyens de faire de véritables « bilans » sur le bien-fondé des choix qui ont été faits et donc de justifier les investissements consentis en mettant en regard les gains réalisés. Sans eux, la sécurité ne peut être vue que comme une charge inutile par les « décideurs ».

4.6 La méthode de l'UREC

L'UREC (Unité Réseaux du CNRS) a élaboré une approche méthodologique de la sécurité adaptée aux laboratoires (http://www.urec.cnrs.fr/securite/articles/ope.secu.html). Elle a été d'abord expérimentée sur trois régions. Cela a permis de l'affiner et de confirmer son grand intérêt. Elle est maintenant rodée et est utilisée en moyenne sur une délégation régionale par trimestre, dans ce qui est appelé une « opération sécurité ».

Élaboration du modèle

Un groupe d'experts a établi *a priori* une liste (appelée liste de contrôles) de vulnérabilités techniques, structurelles (architectures, qui fait quoi ?…) et organisationnelles, adaptée à notre milieu de recherche. Cette liste a été élaborée en fonction de la connaissance des pratiques informatiques des laboratoires et des problèmes de sécurité qui sont remontés à l'UREC. Pour chaque vulnérabilité, une action correctrice est proposée, donnant ainsi au laboratoire les moyens de résorber ses vulnérabilités. Un petit ensemble d'outils à installer (contrôles d'accès, traces…) complète cette liste. Le document est assez succinct pour être appliqué pendant un temps raisonnable par l'administrateur système d'un laboratoire. Il est mis à jour après chaque utilisation et lorsqu'apparaissent de nouvelles attaques ou de nouveaux bogues qui touchent les laboratoires.

Procédure d'intervention

Une méthode d'intervention a aussi été spécifiquement élaborée pour ces opérations et se décline en cinq étapes :

Étape 1 Préparation de l'opération (généralement sur une douzaine de laboratoires dans une région) avec le Délégué régional et un coordinateur local de l'opération (ingénieur connaissant bien les laboratoires de la région) : liste des laboratoires à impliquer, des directeurs et des administrateurs informatiques, personnes externes à associer (universités), planning, … Chaque opération est adaptée à l'environnement : gros ou petits laboratoires, regroupés (campus universitaire/CNRS), dispersés, …

Étape 2 Intervention (2 jours) :
Sensibilisation et présentation de l'opération aux directeurs et aux administrateurs informatiques pendant une demi-journée. Interviennent le Délégué, l'UREC, le service du fonctionnaire de défense, la DST.
Pour les administrateurs informatiques : tour de table, présentation détaillée de la liste de contrôles, cours spécifiques si besoin.

Étape 3 Travail (20 jours) des administrateurs dans leur laboratoire pour appliquer cette liste de contrôle, ceci coordonné par le correspondant local (liste de diffusion électronique, …).

Étape 4 Bilan (un jour).

Étape 5 Rapport indiquant les principales lacunes (en personnel, organisation, techniques) relevées dans les laboratoires et les propositions d'actions correctrices.

Intérêt de la méthode

Cette méthode très pragmatique aide à la modélisation du système d'information d'une manière non formelle et permet d'élaborer toute la partie « sécurité passive » de la politique de sécurité du laboratoire et en partie la sécurité active (avec les outils installés). Elle permet en outre de créer une dynamique régionale et un groupe sur lequel pourra s'appuyer une organisation sécurité CNRS.
Point très important dans la démarche : elle n'est pas destinée à évaluer le niveau de sécurité des laboratoires, mais à les aider à améliorer leur sécurité.
Un développement testé actuellement consiste à ajouter *a posteriori* à cette méthode manuelle un outil automatique de tests de vulnérabilités par le réseau, outil de sécurité active qui permet la mise en place des indicateurs d'évaluation de la politique de sécurité et de l'évolution des vulnérabilités.

4.7 Une architecture structurée et cohérente

Les concepts

Le réseau du laboratoire est généralement connecté « au reste du monde » par un routeur, à travers un réseau de campus (ou un réseau d'établissement), raccordé à un point d'entrée de renater. Le réseau du laboratoire s'ouvre ainsi vers l'extérieur. Le laboratoire devient « branché ». Il peut communiquer plus largement, bénéficier de multiples services et travailler en coopération. Mais il s'offre aussi aux convoitises des prédateurs, comme nous l'avons vu précédemment.

Il faut alors mieux protéger encore l'accès aux informations du laboratoire, c'est-à-dire contrôler les flux venant de l'extérieur pour que les services (ordinateurs, réseaux, périphériques, applications…) et les informations (données, fichiers…) soient accessibles aux personnes autorisées quand elles en ont besoin… mais qu'elles ne le soient pas (ou le moins possible) pour « le reste du monde ». On aborde ainsi le concept d'architecture réseau de sécurité.

En effet toutes les architectures réseau ne sont pas équivalentes. Il y a des architectures recommandées parce qu'il est possible, à moindres coûts, d'y adapter des mesures de prévention et de sécurité active. D'autres ne le permettent pas d'une

manière réaliste. C'est le cas des réseaux dits « Ethernet à plat » où toutes les stations sont connectées sur un même réseau de diffusion. Cette architecture présente plusieurs inconvénients majeurs :

– Il est possible d'écouter, depuis n'importe quelle station, toutes les transactions sur le réseau. Un utilisateur malveillant peut ainsi découvrir très rapidement les mots de passe de tous les utilisateurs.
– Il n'est pas possible d'effectuer un quelconque tri en fonction du niveau de protection ou d'ouverture que l'on veut donner à une station. Certains serveurs nécessitent plus de protection que d'autres, certaines stations n'ont pas besoin d'être accessibles depuis l'Internet, …

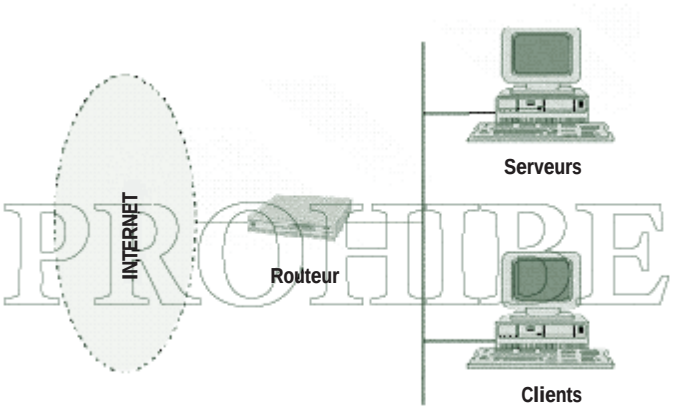


Figure 4 : un réseau à plat

Il faut ainsi préférer la commutation (éventuellement les concentrateurs sécurisés) qui limite les possibilités de l'écoute et le partitionnement (un sous-réseau par service, ou type d'activité, ou type de serveurs, ou…) qui est le début de la structuration.

Puisqu'on peut pénétrer également dans le laboratoire par le réseau, il va falloir mettre, là aussi, « une porte d'entrée ». Pour être utile, cette porte doit être pourvue de « serrures » permettant de restreindre les accès à ceux qui y sont autorisés, et il peut y avoir également un concierge qui veille sur « les entrées et les sorties » du laboratoire, note les noms des visiteurs étrangers et vérifie que les demandes de services sont bien conformes aux instructions qu'il a reçues.

Les concepts d'architecture réseau suivent l'offre commerciale qui est, elle-même, dépendante de l'évolution de la technique. Cette offre a véritablement explosé ces dernières années et a renouvelé complètement les concepts qui avaient encore cours au début des années 90. Il n'est pas possible, dans le cadre de ce guide, de passer en revue l'ensemble des matériels existant. Nous ne retiendrons donc que quelques solutions types permettant de réaliser ces trois fonctions :

– le filtrage des accès et des services (le concierge vérifie les entrées) ;
– la journalisation de l'activité (le concierge tient un registre) ;
– l'authentification forte (la serrure de la porte).

La séparation des trafics

1. Brins physiques et brins logiques

Une architecture réseau de sécurité est une architecture dans laquelle on a su séparer les différents flux d'information, au moins un sous-réseau physique (un brin ou un réseau virtuel) par type d'utilisation de machines : machines de services, machines d'enseignement, machines de recherche, machines de gestion. L'idéal est d'organiser les sous-réseaux en groupes de travail cohérents qui constituent autant de compartiments étanches en cas de piratage. Il faut associer ces sous-réseaux physiques à des sous-réseaux logiques IP (*cf.* figure 5 (c)).

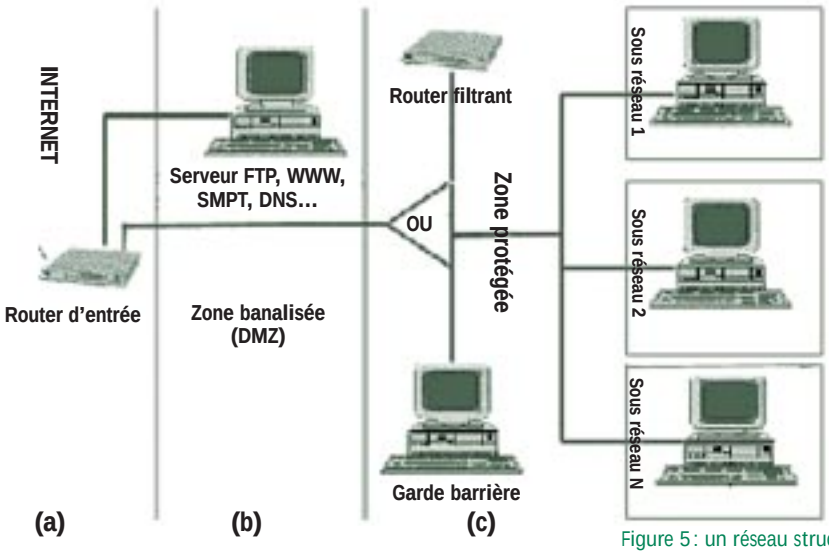


Figure 5 : un réseau structuré

2. Installer les services réseau sur des machines dédiées

Les services comme le DNS, la messagerie, le web, le FTP anonyme… sont les services les plus utilisés depuis l'extérieur. Il est plus prudent de les installer sur des machines dédiées, sur lesquelles il n'y a pas (ou très peu) de connexion interactive possible et surtout ne pas y installer de répertoires utilisateur. Regrouper ces machines dans un sous-réseau particulier (appelé parfois DMZ) isolé du réseau interne par un élément filtrant, routeur ou garde-barrière (*cf.* figure 5 (b)).

Mettre des filtres et des alarmes sur le routeur d'entrée

Un routeur, équipement qui initialement avait pour seule fonction l'interconnexion de réseaux, intègre maintenant de plus en plus les fonctions de sécurité qui sont devenues indispensables. Il est recommandé d'installer un équipement de ce type à la porte Internet de chaque laboratoire et d'en faire assurer l'administration par son propre personnel afin de toujours rester maître de sa sécurité (*cf.* figure 5 (a)).

Sur ce routeur d'entrée, il vaut mieux interdire (sauf pour des besoins spécifiques) les services suivants : bootp, tftpd, syslog, sunrpc, snmp, xdmcp, rlogin, rsh, lpr, openwin, imap, nfs, x11, irc, netbios, sqlserver, ipx, wins, ica et ica browser, rdp, back orifice, netbus. Ce sont actuellement des services à problème potentiel : certains ont des versions boguées, d'autres sont très dangereux quand ils sont mal configurés sur les stations. Mais cette liste ne sera jamais à jour. Le mieux est donc d'avoir une politique de filtrage où « tout ce qui n'est pas explicitement autorisé est interdit ». On ne laisse alors passer que les services que l'on utilise (exemple : SMTP, protocole de messagerie, entrant uniquement vers le serveur de messagerie).

L'installation d'un système de journalisation sur le routeur d'entrée, transmettant à une station protégée toutes les alarmes qu'il génère, en particulier l'activation d'un filtre, est le complément indispensable pour surveiller l'activité réseau.

Structurez vos réseaux

Les gardes-barrières et routeurs filtrants permettent de partitionner le réseau (*cf.* figure 5 (c)). Le garde-barrière (*firewall*) permet de concentrer la sécurité en un point (normalement le point d'entrée dans un réseau ou un sous-réseau) et de contrôler tout le trafic. Le routeur filtrant permet de filtrer les paquets, les demandes de service réseau, et d'enregistrer les traces dans un but de vérifications, de diagnostics des incidents et éventuellement d'établissement de preuves en cas de piratage. Plus complets, les gardes-barrières applicatifs, qui intègrent des fonctions de relayage d'applications, permettent d'authentifier les utilisateurs, de contrôler tous les accès, de journaliser l'activité d'un sous-réseau et, éventuellement, d'intégrer des systèmes de chiffrement ou de faire un contrôle antivirus du flux entrant. En revanche, le routeur filtrant permet d'absorber des débits beaucoup plus importants que les gardes-barrières qui constituent très rapidement un goulet d'étranglement.

Il faut être très attentif dans le choix des solutions : avant d'acheter un matériel, il faut faire une étude technique, organisationnelle et financière. Une configuration facile à base d'icônes cliquables n'est pas une assurance de fonctionnalités ni de robustesse ! Outre ces critères fonctionnels ou financiers (il y a des gardes-barrières à tous les prix), le critère qu'il ne faut jamais oublier c'est le critère « humain » : quelle personne s'occupera du matériel et aura-t-elle une formation suffisante ? Il vaut mieux ne pas installer un garde-barrière applicatif si on ne sait pas comment il sera administré. Ce type d'équipement ne peut être laissé « dans un placard » sans que personne n'en ait explicitement la charge. N'oubliez pas : une sécurité illusoire est pire que pas de sécurité du tout !

Interdire les connexions modem «sauvages»

Les connexions modem «sauvages» (non contrôlées par l'administrateur informatique) sont de véritables calamités du point de vue de la sécurité, car elles contournent toutes les mesures «officielles». Il ne faut donc accepter les connexions par modem *via* le réseau téléphonique que dans le cadre de procédures bien contrôlées.

Contrôle d'accès et journalisation de l'activité réseau sur les serveurs

Nous avons vu qu'il fallait contrôler et enregistrer les activités réseau. On doit le faire sur le routeur d'entrée, il faut aussi le faire sur chaque serveur.

Le problème des serveurs (NT ou Unix) est qu'ils sont souvent livrés avec de nombreuses applications réseaux lancées en mode serveur, applications inutiles et dangereuses. La première chose à faire est donc de faire du ménage (dans /etc./inetd.conf par exemple sous Unix) et ne garder que ce qui sert.
Il existe un logiciel libre tcp_wrapper qui permet de journaliser les connexions réseau et de les filtrer (*cf.* http://www.urec.cnrs.fr/securite/outils/index.html). Celui-ci est à installer sur tous les serveurs.

L'authentification forte par carte à puce

Le mot de passe n'est pas une technique fiable d'authentification. Il peut être écouté sur le réseau, il peut être découvert, il peut être facilement «prêté»… Une technique d'authentification plus forte est la carte à puce. C'est une technique qui tend à se développer. Son coût reste (à la date d'avril 1999) encore élevé : environ 350 F par machine + le logiciel de gestion sur le serveur. C'est certainement le meilleur produit en rapport qualité/prix pour la fonction d'authentification (peut-être est-ce la raison de son utilisation comme moyen de paiement par le milieu bancaire). Par contre, elle nécessite la connexion d'un lecteur sur chaque poste utilisateur.

Les autres aspects de la sécurité

Il y a d'autres aspects de la sécurité comme la confidentialité des données, l'intégrité, la non-répudiation. Il existe des solutions simples pour assurer ces services à base de produits de chiffrements. On étudie actuellement les moyens de les déployer d'abord dans des cercles restreints puis, plus tard, dans les laboratoires.

5
Les règles de bon usage

Les réseaux donnent le moyen de diffuser n'importe quelle information sur la planète entière en un instant. Cette extraordinaire capacité impose à chacun d'entre nous le respect de certaines règles et un peu d'autodiscipline. Un comportement responsable est essentiel pour que notre organisme garde cohérence et crédibilité. Ces règles s'appliquent à toute personne qui utilise les moyens informatiques d'un laboratoire directement, à distance, ou en cascade.

5.1 Respect des règles écrites et non écrites

Respecter la loi !

L'observance des règles commence en tout premier lieu par le respect des lois. Toute personne se trouvant sur le territoire français est tenue de respecter la législation en vigueur. Par exemple si, dans l'accomplissement de son travail, un utilisateur est amené à constituer des « fichiers nominatifs » relevant de la loi « Informatique et Libertés », il devra auparavant faire une demande d'autorisation, sous couvert de son directeur de laboratoire, auprès de la CNIL. Cette autorisation n'est valable que pour le traitement défini dans la demande et pas pour le fichier lui-même.

D'une manière générale, on peut trouver sur le web les textes des lois qui se rapportent plus ou moins directement à la sécurité informatique :
– la loi du 6/1/78 dite « informatique et liberté » (*cf.* http://www.cnil.fr/) ;
– la loi du 5/1/88 relative à la fraude informatique, complétée par la loi du 22/7/92 dite « loi Godfrain »
(*cf.* http://www.legifrance.gouv.fr/citoyen/code.cgi
et http://www.cnrs.fr/Infosecu/10godfr1.html) ;
– la législation relative à la propriété intellectuelle
(*cf.* : http://www.legifrance.gouv.fr/citoyen/code.cgi
et http://www.sg.cnrs.fr/internet/droitauteur.htm
ou http://www.cnrs.fr/Infosecu/10droits.html) ;
– la loi du 04/08/1994 relative à l'emploi de la langue française,
(*cf.* http://www.culture.fr/culture/dglf/) ;
– la législation applicable en matière de cryptologie
(*cf.* http://www.telecom.gouv.fr/francais/activ/techno/crypto0698_1.htm) ;
– Web SCSSI : http://www.scssi.gouv.fr/
– liste des derniers décrets et arrêtés sur la cryptologie ainsi que les liens vers les documents complets à :
http://www.internet.gouv.fr/francais/commerce/textesref.htm#1 ainsi qu'à http://www.internet.gouv.fr/francais/textesref/cryptodecret99199.htm et http://www.internet.gouv.fr/francais/textesref/cryptodecret99200.htm ou encore à http://www.clusif.asso.fr/rubriques/crypto/crypto.htm

Respecter les autorisations d'accès aux fichiers

Un utilisateur ne peut accéder aux informations d'un système (fichiers, journalisations, bases de données…) que si elles lui appartiennent ou sont publiques. Ceci signifie concrètement qu'il n'a pas le droit :

– d'utiliser ou essayer d'utiliser des comptes autres que le sien ;
– de tenter de lire, modifier, copier ou détruire d'autres fichiers que les siens.

En particulier, il lui est interdit de modifier le ou les fichiers contenant des informations comptables ou d'identification ou bien de prendre connaissance d'infor-

mations détenues par d'autres utilisateurs sans leur consentement explicite, quand bien même ceux-ci ne les auraient pas (ou les auraient mal) protégées. Cette dernière règle s'applique également aux correspondances privées de type « courrier électroniques » dont l'utilisateur n'est destinataire ni directement, ni en copie. Toutefois, dans le cadre de sa responsabilité sur l'utilisation des moyens mis à la disposition du laboratoire, le directeur à un droit de contrôle et peut l'exercer en cas d'incident particulier ou d'enquête.

La sécurité et le bon usage sont à la charge de tous !

Chaque utilisateur est responsable de l'emploi des ressources informatiques et du réseau du laboratoire, et il a pour devoir de contribuer, à son niveau, à la sécurité générale. Il doit :

- appliquer les recommandations de sécurité du laboratoire et signer la charte désormais obligatoire ;
- choisir des mots de passe sûrs, gardés secrets, et ne les communiquer en aucun cas à des tiers ;
- s'engager à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux à travers des matériels dont il a l'usage ;
- assurer la protection de ses informations pour lesquelles il est responsable des droits qu'il donne aux autres utilisateurs ;
- signaler toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater.

L'installation des logiciels doit suivre les règles en vigueur dans le laboratoire. En particulier, il est interdit d'installer un logiciel pouvant mettre en péril la sécurité ou pour lequel aucun droit de licence n'a été concédé.

Ces règles de bons usages, que rappelle opportunément la « Charte utilisateur pour l'usage de ressources informatiques et de services Internet » parue au *Bulletin Officiel du CNRS* (on peut la consulter en format pdf : http://www.cnrs.fr/Infosecu/Charte.pdf ou en format html : http://www.cnrs.fr/Infosecu/Charte.html) sont le reflet, au fond, du désir de chacun de pouvoir travailler dans les meilleures conditions possibles. Une société sans règle n'est-elle pas aussi une société sans droit ? La charte énonce les devoirs de chacun pour assurer les droits de tous.

5.2 Le bon usage des moyens de communication

Quand Guillaume Martin, chercheur au CNRS ou Alexandra Dupuis, thésard au laboratoire de « Genèse des particules », s'expriment en tant que tel sur le réseau, ils engagent leur laboratoire, mais aussi l'ensemble de l'organisme. Ils n'expriment pas une simple « opinion personnelle », ils expriment des idées que cautionnent leur titre et leur fonction dans l'organisme. Quand ils le font à partir du site de leur unité (site web, ftp, courrier électronique…), ils participent à l'image que donne

notre Centre National et dont dépend la confiance qu'on lui accorde. Ils engagent sa responsabilité juridique. Il n'est donc pas possible de faire n'importe quoi :

– ne pas confondre serveur web et tribune de débats sur le sexe des anges ;
– rester modéré et courtois dans ses propos ;
– observer le devoir de réserve qui s'impose à tout fonctionnaire en particulier sur le plan politique.

Tout laxisme sur ce sujet aboutirait tôt ou tard à des dérives incontrôlables qui mettraient en cause l'existence même de notre organisme.

Accès aux ressources informatiques et réseau

L'utilisation des ressources informatiques partagées du laboratoire et la connexion d'un équipement sur le réseau ne sont pas des droits, mais sont soumises à l'autorisation du directeur. Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Elles ne valent que pour des activités conformes à la législation en vigueur et dans le cadre exclusif de l'activité professionnelle de leurs bénéficiaires. L'application de ces règles est soumise à l'appréciation, au cas par cas, du responsable de l'unité qui a à répondre de la bonne utilisation de ces moyens.

Ces autorisations peuvent être retirées à tout moment. Toute autorisation prend fin lors de la cessation, même provisoire, de l'activité professionnelle qui l'a justifiée.

Accès aux sites Internet

Les connexions aux sites distants doivent se faire en respectant les règles du bon usage traditionnelles des réseaux et, bien entendu, dans le respect de la législation en vigueur.

– Il est interdit de rentrer (ou de tenter de le faire) dans des systèmes, sans en avoir les autorisations explicites.
– Il est interdit de se livrer à des actions mettant sciemment en péril la sécurité ou le fonctionnement d'un site. En particulier, les opérations de représailles, quelles qu'en soient les raisons, ne doivent pas être tolérées.
– Toutes tentatives d'usurpation d'identité et d'interception de communications entre tiers doivent être sanctionnées.
– La plus grande correction est de mise dans les échanges électroniques par courrier, forums de discussions…
– Un utilisateur ne doit pas ouvrir ou déposer des documents sur un serveur du laboratoire sans autorisation du directeur responsable administrativement de son contenu.

Création, administration et gestion des serveurs FTP anonymes

Les répertoires « ouverts en écriture » des ftp anonymes, installés dans des systèmes mal configurés, peuvent être utilisés dans les tentatives de pénétration du réseau

des laboratoires. Ils peuvent également servir à des provocations, à paralyser les systèmes d'information en saturant les serveurs, à diffuser des documents illicites, ou plus simplement, à exploiter indûment des ressources informatiques du CNRS.

C'est pourquoi l'attention des directeurs de laboratoires et des gestionnaires de serveur est attirée sur quelques points importants de la gestion des serveurs ftp.

1. Il est recommandé, dans la mesure du possible, d'éviter la mise en place, dans un ftp anonyme, d'un répertoire ouvert à tous en écriture. L'expérience montre que cela est souvent possible. Si l'utilisation d'un tel répertoire est incontournable, l'administrateur doit vérifier chaque jour son contenu. Ce répertoire doit être systématiquement fermé lorsque cette vérification quotidienne n'est pas – ou n'est plus – possible.

2. Pour l'administration d'un serveur ftp anonyme, il est recommandé de suivre les mêmes règles de saine gestion que pour un serveur web : désignation d'un administrateur, contrôle du contenu, journalisation des transactions, etc.

3. Il est rappelé qu'un serveur ftp doit toujours être administré. Pendant les absences de l'administrateur régulier, l'unité de recherche peut soit nommer un administrateur de remplacement, soit interrompre ce service.

Installation et gestion d'un serveur web

Rappelons les 12 recommandations du Comité web du CNRS sur cette question.

1. Le directeur de l'unité est responsable de l'information délivrée par le serveur de son laboratoire. Comme pour une publication traditionnelle, un serveur doit avoir « un directeur de publication » qui assure la responsabilité de l'information qui est accessible sur le serveur. Cette fonction ne peut être assurée que par le directeur du laboratoire.

2. Ne déposer sur le serveur que les informations que l'on a le droit d'y mettre. Un serveur doit respecter les lois sur la presse et tous les moyens de diffusion plus classiques. Il faut notamment faire très attention :
   – aux informations nominatives (déclaration à la CNIL),
   – aux contrats comportant des clauses de confidentialité,
   – aux droits d'auteurs (copyright) sur les textes, images, sons, vidéos…

3. Ne mettre sur le serveur que des informations qui valorisent l'image du laboratoire. Les informations doivent être opportunes, claires, attrayantes, et mises à jour autant que de besoin. Le serveur ne doit pas être librement utilisé par le personnel pour y satisfaire ses hobbies propres ou pour y introduire des données qui n'ont strictement rien à voir avec l'activité de l'unité.

4. Ne pas omettre de préciser, dans la page d'accueil du serveur, l'appartenance au CNRS. Cette précision est importante pour votre organisme et vos interlocuteurs.

5. Veiller à déclarer l'existence du serveur auprès du CNRS.
Cette déclaration consiste en un simple dépôt à l'adresse électronique : webinfo@cnrs-dir.fr. Veillez également à informer de l'existence du serveur :
– le directeur de département scientifique dont relève le laboratoire ;
– le délégué régional.

Important : cette déclaration est complémentaire et ne se substitue pas à celle effectuée auprès de l'Internet.

6. Désigner un « responsable de web » chargé du fonctionnement du serveur et de la surveillance de ce qu'il contient. Cet agent, proche du directeur de l'unité, distinct de l'administrateur du réseau mais éventuellement assisté par une petite équipe nommément désignée, est chargé de contrôler, valider et installer tous les fichiers (informations) sur le serveur. Il faut veiller à ce qu'aucune autre personne de l'unité n'installe librement des données sur le serveur.

7. Installer ce service sur une machine où il n'y a pas de données sensibles (au sens large). En effet, la machine qui héberge ce service est de fait connue et accessible par tout l'Internet. C'est donc la première cible pour les pirates qui, si la machine est mal configurée, pourront rapidement accéder à toutes les données qu'elle contient. Il ne faut donc pas mettre le serveur sur l'ordinateur principal du laboratoire, mais lui dédier une petite station de travail. Cela permet aussi de faciliter les mesures de contrôle d'accès qui peuvent être installées à l'entrée du réseau (garde-barrière ou filtre dans le routeur).

8. Les fichiers et les répertoires doivent y être en « lecture seule ».
L'accès en écriture doit être strictement réservé au responsable de web. Nul ne doit pouvoir introduire des modifications ou des informations nouvelles sans passer par lui.

9. Journaliser les transactions.
Outre l'avantage de pouvoir vérifier la pertinence de l'information, la journalisation permet *a posteriori* de reconstituer et d'expliquer certaines intrusions.

10. Se méfier des rebonds.
L'utilisation de pointeurs sur d'autres serveurs pour accéder à de plus larges informations doit se faire avec de grandes précautions, notamment lorsque l'on offre ainsi la possibilité d'accéder à des informations externes au CNRS ou bien si l'on risque de violer un quelconque copyright.

11. Prévoir des restrictions d'accès en lecture.
    Sur un serveur, il est possible de restreindre à certains groupes de machines l'accès à une partie des informations (concrètement, par des masques sur les adresses IP ou les noms de domaine). Si certaines informations ne doivent pas être accessibles à tout l'Internet mais rester disponibles pour le personnel de l'unité, il est possible de les mettre dans un répertoire particulier et de n'en donner accès qu'à votre réseau IP ou à votre nom de domaine.

12. Développer le serveur en français.
    En effet, une des missions de notre organisme est le développement de l'information scientifique en favorisant l'usage de la langue française. Naturellement, vous pouvez parallèlement traduire le serveur dans les langues étrangères de votre choix.

Gestion des listes de diffusion

Rappelons les points essentiels des recommandations du Comité web sur les listes de diffusion :

1. Les listes de diffusion rentrant dans le cadre de ces recommandations sont celles à portée large, généralement connues et gérées par un logiciel spécifique ; les alias de messagerie qui permettent, sur une petite échelle, de faire de la diffusion à quelques personnes ne rentrent pas dans ce cadre.

2. Toute liste nouvelle doit préciser clairement :
   – son objet et le thème exacts sur lequel doivent porter les questions et les discussions ;
   – le nom, les coordonnées et l'organisme de rattachement de l'administrateur qui gère la liste. Il doit pouvoir être joint facilement par chacun de ses membres ;
   – la durée de vie de la liste, illimitée, ou limitée – quand elle est attachée à un événement particulier (manifestation scientifique, projet de recherche coordonnée, collaboration industrielle, etc.) et, dans ce cas, la date précise de son échéance.

3. Lorsqu'une liste est prévue pour une durée limitée, chacun de ses abonnés doit en être informé au moment de son adhésion. La liste ne doit pas être laissée à l'abandon ; elle doit être supprimée dès qu'arrive son échéance et les participants doivent être informés de cette suppression.

4. Une liste peut être hébergée « physiquement » sur une machine administrée par un site, et être gérée par un administrateur depuis un autre site distant pouvant appartenir à un autre organisme.

5. Les créateurs de liste sont mis en garde contre le danger que représente une prolifération anarchique des listes de diffusion sur des serveurs d'unités de recherche ou d'organismes extérieurs ne possédant ni les équipements informatiques, ni les moyens humains indispensables à leur bonne et saine gestion. Il est nettement préférable de les faire héberger par un site homologué.

L'ensemble des textes du Comité web du CNRS peut être consulté sur l'URL suivante : http://www.cnrs.fr/Gazette/Comite/comite.html

6
La vulnérabilité des autocommutateurs

Les systèmes d'information ne sont pas uniquement constitués des systèmes informatiques et des réseaux d'ordinateurs ; il faut se rappeler que les téléphonies (téléphones, télécopies, portatifs...) en font aussi partie et sont également très fragiles, en particulier parce que les autocommutateurs ne sont pas toujours bien gérés : il faut connaître ces vulnérabilités, comme utilisateurs afin de ne pas se « laisser piéger », ou comme responsable de site afin de prendre les mesures qui s'imposent.

Les autocommutateurs téléphoniques privés (PABX) des campus, des laboratoires, des directions ou des services administratifs sont les éléments centraux des systèmes d'information. Ils en sont aussi des éléments très fragiles. Cette fragilité est d'autant plus dangereuse qu'elle est trop souvent ignorée. Pourtant un piratage peut avoir des conséquences désastreuses : détournement de trafic, piégeage de lignes téléphoniques, écoutes, blocage des communications, etc.

Il faut se rappeler que le piratage aux États-Unis a commencé par le téléphone, et plus précisément par le piratage des centraux téléphoniques. Cette délinquance, maintenant ancienne, a pris une ampleur considérable ; elle y a complètement achevé sa dérive du ludique au lucratif. Il existe des sites Internet et des forums de discussion particulièrement actifs et bien documentés spécialisés dans ce domaine. C'est donc un problème qu'il faut prendre très au sérieux.

6.1 Les responsabilités

Les fabricants

Les fabricants, pour faciliter les tâches de maintenance, proposent « en standard » sur leur matériel un mot de passe « administrateur » unique, toujours le même d'un client à l'autre. Ces mots de passe, qui permettent de configurer (ou de reconfigurer) une installation, sont maintenant très largement connus des milieux pirates. Cette vulnérabilité est d'autant plus inquiétante qu'elle s'associe à d'autres déficiences liées aux exigences de la télémaintenance : modem connecté en permanence, ligne de télémaintenance sur le MIC du PABX.

L'ensemble de ces « prestations » rend le piratage des PABX aisé. Le pirate, avec un simple minitel, peut se retrouver maître du système. Il peut tout faire, y compris « repatcher » le logiciel système pour lui attribuer des « fonctionnalités non documentées », dont sa victime serait consternée d'apprendre l'existence. Le pirate n'a pas besoin de connaître sa victime : de chez lui, parfois du bout du monde, connecté par une simple ligne téléphonique, il a pris possession de son « système de communication ». Il va l'utiliser ou le détourner pour son plus grand profit. La plupart du temps, il ne laissera aucune trace de ses mauvaises actions, car la journalisation dans les PABX laisse beaucoup à désirer.

L'organisation

La Direction des établissements a parfois aussi une large responsabilité :

- en n'instaurant pas un contrôle d'accès de la salle où est installé le PABX : une personne mal intentionnée, qui a un accès « physique » à la machine, pour peu qu'elle connaisse le mot de passe décrit ci-dessus peut tout faire, y compris modifier la « configuration matérielle » ;
- en négligeant la tâche d'administration : on voit trop souvent des situations où aucun responsable n'a été nommé, où il n'existe pas de

remplaçant pour suppléer les absences du responsable en titre. Il n'est donc pas rare qu'un PABX reste de longues périodes sans être surveillé.

6.2 Recommandations d'administration

Pour le PABX

1. Il est important que tous les PABX soient administrés, c'est-à-dire que quelqu'un soit nommé responsable. Il assurera le contrôle des entrées et la gestion des postes téléphoniques, mettra en place des systèmes d'archivage des accès, contrôlera les journaux des accès et éduquera les utilisateurs « des nouveaux usages ». Il est l'interlocuteur autorisé de la Direction vis-à-vis des fournisseurs.

2. Le mot de passe « administrateur » doit être systématiquement changé après l'installation. En aucun cas, il ne faut laisser celui du fabricant. Cette position exige parfois « une rude négociation » avec les services de maintenance du revendeur, mais il ne faut pas transiger sur ce point.

3. Déconnecter tout modem (il y en a toujours un sur les PABX modernes, mais il est parfois bien caché…). Une intervention de maintenance, même préventive, ne peut se faire à l'insu de l'administrateur. Les services de maintenance doivent pouvoir l'appeler sur une « ligne directe » pour l'informer de la nature de l'opération et lui demander de brancher le modem. Cette opération est enregistrée – ainsi que ses résultats – sur un cahier de maintenance. Le modem est à nouveau arrêté à la fin de l'opération.

4. Le modem ne doit pas être connecté sur une voie MIC du PABX, mais sur une ligne directe possédant un numéro différent du groupe de numéros affectés. Cette précaution, outre qu'elle permet de se protéger contre les pirates cherchant le numéro du modem par balayage des numéros non affectés, permet aussi de pouvoir se faire dépanner par télémaintenance en cas d'incident sur le MIC.

Pour être complètes, ces recommandations doivent être accompagnées de « conseils de bonne utilisation » des services qu'offrent les PABX.

Pour une bonne utilisation des services de téléphonie

Certaines fonctionnalités des PABX sont peu connues et peu utilisées. Les plus importantes, pour le sujet qui nous occupe, sont les protections.

- Il est possible de faire attribuer des communications téléphoniques à un poste distant (renvoi d'appels). Pour éviter cette fraude, il est recommandé

d'utiliser le code confidentiel clavier (cadenas) qui permet d'empêcher l'accès à un poste localement ou à distance. Ce verrouillage est le seul moyen d'empêcher le piratage de trafic.

- L'accès à la messagerie vocale est possible par n'importe qui depuis n'importe quel poste intérieur ou extérieur. Il est donc recommandé à chaque utilisateur de protéger sa messagerie par un code confidentiel.

Les PABX d'aujourd'hui proposent un grand nombre de services de téléphonie. Ils y associent souvent (toujours ?) un ensemble de protections qu'il faut connaître et utiliser, sans quoi ces services sont de véritables gouffres de sécurité. C'est le rôle de l'administrateur de faire connaître les protections en service.

7
Virus informatiques et autres malignités

Dans les ordinateurs pullule une faune bizarre : virus, vers, cheval de Troie. Que recouvrent ces vocables imagés ? Peut-on se prémunir contre de tels méfaits ? Que faut-il faire quand on en est victime ? Autant de questions qui tourmentent tous ceux qui ont eu affaire un jour à ce type de malveillance. Quelques connaissances rudimentaires suffisent, la plupart du temps, pour y répondre et se mettre ainsi à l'abri.

7.1 Un peu de vocabulaire

Qu'est-ce qu'un ver ?

Un ver est un programme qui possède la faculté de s'auto-reproduire et de se déplacer au travers d'un réseau (*cf. Le ver Internet* de Robert Morris de 1988). Il se déplace de manière autonome en exploitant des mécanismes système ou réseau (rpc, rlogin, etc.). Un ver est un virus réseau.

Qu'est-ce qu'une bombe logique ?

Les bombes logiques sont des lignes de codes programmés insidieux, cachés dans des programmes, avec un mode de déclenchement différé. Ce mode exploite principalement des informations comme la date système, le lancement d'une procédure, l'entrée d'une chaîne de caractères.

Qu'est-ce qu'un cheval de Troie ?

Les chevaux de Troie se présentent généralement sous la forme de programmes à caractère utilitaire ou ludique. Ces programmes comportent, en plus des fonctions déclarées, un mécanisme caché qui s'exécute de façon illicite en parallèle des actions connues de l'utilisateur. Par exemple, un cheval de Troie, en plus de ses fonctions normales, enverra des informations à un pirate ou créera dans le système une entrée secrète qui permet d'entrer sur le système en mode administrateur sans mot de passe.

Qu'est-ce qu'un virus ?

Pour la plupart des utilisateurs, un virus est un programme qui, à leur insu, exerce une action nuisible à son environnement : modification ou destruction de fichiers, effacement du disque dur, allongement des temps de traitement, manifestations visuelles ou sonores plus ou moins inquiétantes, etc. Cette action peut être continue, sporadique, périodique, ou n'avoir lieu qu'à une date précise ou selon la conjonction d'événements extérieurs fortuits. Le virus Michelangelo, par exemple, ne se déclenche que le 6 mars.

Mais on sait moins que les virus peuvent aussi servir à crocheter les systèmes les plus secrets en créant des vulnérabilités « cachées » qu'un autre processus exploitera ultérieurement. Ces virus ont pour mission de se disséminer afin de propager ces vulnérabilités et de « marquer » les systèmes atteints pour qu'ils puissent être détectés par des programmes de balayage de l'Internet. Ils doivent rester le plus silencieux possible pour ne pas se faire repérer. Contrairement aux autres virus, ils ne perturbent pas le système et ne détruisent pas de données. Ces virus-là sont les plus dangereux, même s'ils paraissent ne pas gêner. Sur une machine ainsi contaminée, votre système d'information est un livre ouvert. Il n'est plus question alors de parler de sécurité !

On voit ici que les virus s'attaquent à tous les aspects de la sécurité définie dans la trilogie : confidentialité, intégrité, continuité de service. On les caractérisera donc par leur mode de propagation, plutôt que par leur capacité de malfaisance, trop générale.

En informatique, on appelle virus « tout programme d'ordinateur capable d'infecter un autre programme d'ordinateur en le modifiant d'une façon qu'il puisse, à son tour, se reproduire ».

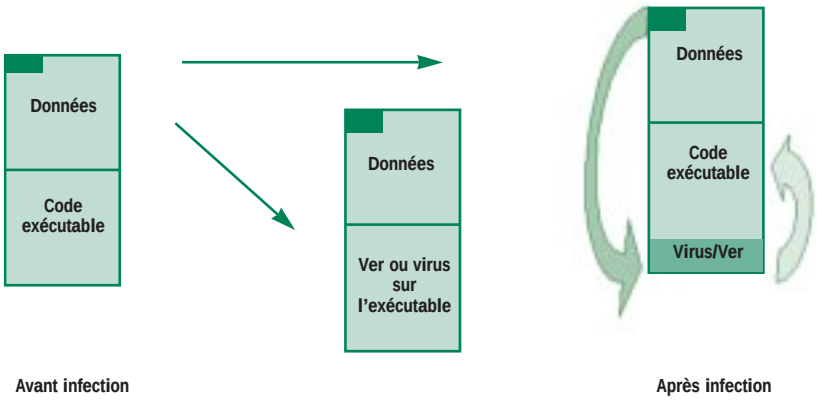


Figure 6 : contamination par un virus ou un ver informatique

On admet généralement qu'il existe deux classes principales de virus :

– les infecteurs de fichiers qui s'attachent aux programmes et exercent une action directe ou indirecte ;
– les virus du système qui s'attaquent à certains fichiers vitaux du disque dur, tels le *boot-sector* (premier secteur lu à l'amorçage du disque), la FAT (qui est la table d'allocation du disque) ou les répertoires (les tables des matières des fichiers). Ces virus ne font pas dans la broderie. Une fois ces zones critiques modifiées ou détruites (et cela demande peu de temps), le contenu du disque peut être considéré comme perdu. À moins qu'une sauvegarde intelligente n'ait été effectuée en temps opportun.

Certains virus sont capables d'effectuer ces deux types de dommages. Pour en savoir plus, voir l'historique des virus en http://www.cnrs.fr/Infosecu/VirHisto.zip.

7.2 La prévention

La détection de l'ennemi

Il existe une catégorie de détecteurs de virus qui opèrent sur une collection de signatures. Les virus les plus simples comportent tous, en effet, une suite d'ins-

tructions caractéristique, propre à chacun, mais parfaitement identifiable et qu'on appelle leur signature. On peut en établir un catalogue qui ira en grossissant au fur et à mesure qu'apparaîtront de nouveaux virus. Les programmes qui exploitent cette méthode s'appellent des *scanners*. Ils ne donnent que très peu de fausses alarmes, mais ils sont naturellement inefficaces pour les virus polymorphiques puisque ceux-ci ont la faculté de modifier leur apparence.

L'inconvénient de cette méthode est la nécessité de remise à jour périodique du catalogue, ce qui impose à l'utilisateur de souscrire un abonnement et procure au distributeur et à l'éditeur de l'antivirus une appréciable source de revenus.

Une autre méthode existe, qui a l'avantage de ne pas nécessiter de mise à jour. Elle se base sur des algorithmes heuristiques pour soupçonner dans certaines successions d'instructions la possibilité d'un virus. La probabilité de fausses alarmes est plus forte qu'avec les scanners, mais l'efficacité est permanente. Tout au moins jusqu'à l'apparition de nouveaux concepts d'attaque.

La prévention contre les virus

Nous recommandons, pour se protéger des virus :

- de contrôler toutes les nouvelles applications à installer ;
- de verrouiller les supports de stockage quand ils n'ont pas besoin d'être en écriture ;
- d'avoir un antivirus à jour.

Les unités du CNRS ont à leur disposition des aides et des outils afin de les encourager à améliorer l'efficacité de leur protection antivirus :

- la liste de diffusion « sos-virus » permet d'échanger les questions et les expériences (http://www.services.cnrs.fr/Listes/liste.cgi?liste=sos-virus) ;
- un site de téléchargement de mises à jour de logiciels F-Prot, Sam, AVP, TBAV ;
- la distribution gratuite de ces logiciels.

Les canulars

Sur l'Internet, la diffusion d'information est facile, gratuite, et difficilement contrôlable : aussi la dérive de lancer de fausses alertes est-elle vite apparue. C'est ce qui se produit avec les canulars («*myths, hoaxes, urban legends* ») qui se présentent faussement comme une alerte de sécurité.

Cette pratique a été inaugurée avec la fausse annonce d'un prétendu « nouveau virus » « GOOD TIME », présenté comme très dangereux. Cette fausse annonce continue, plusieurs années après son baptême, à circuler sur l'Internet, parfois avec quelques variantes (Penpal Greetings, AOL4FREE, PKZIP300, etc.). Elle a toujours autant de succès ! Plus généralement, des manipulations de ce genre affectent de nombreux thèmes couvrant la sécurité des systèmes et des réseaux, ce qui a amené les organismes de sécurité comme les CERT à signer leurs messages.

Il est facile de vérifier qu'une alerte virus est un canular en consultant au choix l'un des sites suivants :

http://ciac.llnl.gov/ciac/CIACHoaxes.html
http://www.symantec.com/avcenter/hoax.html
http://www.stiller.com/hoaxes.htm
http://kumite.com/myths/
http://www.nai.com/services/support/hoax/hoax.asp
http://urbanlegends.miningco.com/msubvir.htm?pid=3D2733&cob=3Dhome

On trouve également aux adresses ci-dessous les archives des canulars et autres mythes qui courent sur Internet :

http://www.snopes.com/
http://snopes.simplenet.com/message/
http://www.urbanlegends.com/

En règle générale, il ne faut faire confiance qu'aux sources « authentifiées » et ne jamais prendre pour « argent comptant » des informations qui vous arrivent par le courrier électronique. Dans tous les cas, vérifiez l'information avant de propager le message, surtout dans une liste de diffusion. Si vous êtes crédule, vous participez à votre insu à la malveillance.

Un nouveau danger : les macrovirus

Il est possible de rencontrer des macrovirus chaque fois qu'un produit offre à l'utilisateur la possibilité d'écrire des macro-commandes permettant une écriture sur disque. La plate-forme qui comporte le plus de macrovirus est Microsoft Word pour Windows. Les virus se propagent facilement dans cet environnement car les fichiers .DOC contiennent à la fois le texte et toutes les macros associées. Microsoft Excel est également touché.
La fabrication d'un macrovirus, contrairement aux souches anciennes où il fallait maîtriser la programmation système, est à la portée d'un néophyte. Cette facilité attire les vocations malsaines et tous les jours il se crée une quantité innombrable de nouveaux macrovirus. La procédure ancienne de rafraîchissement tous les six mois du fichier des « signatures virus » sur l'antivirus ne suffit donc plus. Faites donc régulièrement des mises à jour (au minimum une par mois) et rappelez-vous qu'un macrovirus peut bloquer partiellement un laboratoire pendant plusieurs jours.

7.3 Principes de lutte contre les macrovirus

Comment se fait la contamination ?

Word devient infecté dès la lecture d'un fichier contaminé. Le macrovirus se propagera alors à tous les fichiers ouverts avec ce Word contaminé et qui sera sauvegardé («Enregistrer», « Enregistrer sous… », ou réponse « OK » à l'invite de sauvegarde au moment de la fermeture du fichier).

Quelques précautions

Un récapitulatif complet est disponible sur le site http://www.cnrs.fr/Infosecu/MVirus.zip. Les trois méthodes exposées ci-dessous sont les plus courantes :

1. Empêcher la modification NORMAL.DOT

Une première méthode de lutte contre la propagation des macrovirus consiste à empêcher la modification du fichier NORMAL.DOT.

Interdire la modification du fichier NORMAL.DOT

• Soit en protégeant par un mot de passe le fichier NORMAL.DOT : voir la procédure dans http://www.cnrs.fr/Infosecu/Virus.html

• Soit en protégeant le fichier NORMAL.DOT en écriture : dans le menu « Outils », choisissez la rubrique « Options… ». Dans la boîte qui apparaît, sélectionnez l'onglet « Général ». Cochez « Protection contre les virus contenus dans les macros ». Fermez la boîte de commande.

Avec cette protection, à chaque fois que vous ouvrirez un document contenant des macros commandes, vous serez prévenu par une boîte de dialogue qui vous demandera si vous voulez activer ou non les macros contenues dans le document.

• Soit en forçant l'option « Confirmer l'enregistrement de NORMAL.DOT » de Word. Cliquez sur « Outil », puis sur « Options ». Choisissez ensuite l'onglet « Enregistrement ». Parmi les options d'enregistrement affichées, sélectionnez « Confirmer l'enregistrement de NORMAL.DOT ».

Vous pouvez naturellement appliquer toutes ces protections à la fois ! Plusieurs précautions valent mieux qu'une ; cependant beaucoup de virus actuels savent très bien contourner ces lignes de défense.

2. On peut aussi désactiver le lancement des macros au démarrage

Désactivation des macros de type AUTO

Lancez Word ou ouvrez un document en gardant la touche <majuscule> enfoncée. Cette opération permet d'empêcher l'exécution des macros automatiques de type AUTO, ce qui interdit au virus l'utilisation des AutoOpen ou AutoExec pour se propager. D'une manière similaire, l'activation de ce contrôle à la sortie de Word fait obstacle à l'exécution de la macro AutoClose.

3. On peut enfin faire désactiver les macros par Word

Si vous n'utilisez jamais les macros, préférez la fonction de Word « DésactiverMacroAuto » qui a exactement le même rôle que la technique précédente, mais opère une désactivation globale et systématique (voir la procédure dans http://www.cnrs.fr/Infosecu/Virus.html).

Malheureusement, il existe d'autres macros que celles de type AUTO. Cette méthode n'est efficace que dans la mesure où les macrovirus ont « l'amabilité de bien vouloir n'utiliser que celles-là ».

7.4 Que faire en cas d'infection par un virus ?

La meilleure protection contre les virus et les macrovirus est un antivirus à jour. Le reste est du pis-aller. Cependant, si vous vous êtes laissé prendre au piège, voici quelques conseils utiles.

Connaître son virus

Si vous pensez être infecté par un virus dont vous connaissez un des noms ou alias (un même virus porte plusieurs noms suivant les éditeurs antivirus), procédez de la manière suivante :

1. Récupérez la liste des noms ou alias de ce virus sur
   http://www.virusbtn.com/VGrep/search.html
2. Consultez une base de description de virus sur l'un des sites suivants :
   http://www.Europe.DataFellows.com/vir-info/
   http://www.drsolomon.com/vircen/enc/
   http://www.avp.ch/avpve/findex.stm
   http://vil.mcafee.com/villib/alpha.asp
   http://www.symantec.com/avcenter/vinfodb.html

Comment fabriquer une disquette de démarrage sur PC (Win9x) :

Pour les opération suivantes, il faut utiliser un ordinateur qui n'a pas été infecté.

1. Mettre une disquette vierge dans le lecteur
2. Lancer MS-DOS et rentrer les instructions suivantes :
   FORMAT A: /S /U
   COPY C:\WINDOWS\HIMEM.SYS A:\
   COPY C:\WINDOWS\EMM386.EXE A:\
   EXIT
3. Copier avec Notepad les trois lignes suivantes et les sauvegarder sur la disquette sous le nom de CONFIG.SYS
   DEVICE=A:\HIMEM.SYS
   DEVICE=A:\EMM386.EXE NOEMS
   DOS=HIGH,UMB
4. Protéger la disquette en écriture.

Désinfecter son PC sous Win9x sans disquette de démarrage :

Vous êtes contaminé. Normalement, il vous faudrait redémarrer votre ordinateur en partant d'une disquette « propre »… mais vous n'avez pas pensé à en préparer une quand il le fallait ! Pour l'instant (avril 99), seul AVP permet de travailler avec un système contaminé.

Comment désinfecter son PC

Téléchargez la version DOS d'AVP sur votre PC. Décompactez-la (unzip) et placez-la dans un nouveau répertoire, par exemple AVP.

1. Faites repartir votre PC en mode MS-DOS.
2. Vous devez récupérer un prompte du type "C:\>" ou "C:\WINDOWS>", tapez les commandes suivantes :
   CD \AVP
   AVPLITE * \-
3. Quand le programme a fini de désinfecter le disque, n'oubliez pas de vérifier aussi TOUTES vos disquettes.

Désinfecter une contamination par macrovirus

Quand l'antivirus n'a pas su détecter un nouveau macrovirus (versions Word 6 et ultérieures pour Mac et PC), alors « quelques gestes qui sauvent » sont profitables à connaître :

D'abord commencez par « nettoyer » Word lui-même

1. Lancez Word.
2. Dans le menu « Outils », choisissez la rubrique « Modèle et compléments… »
3. Prenez soigneusement note de tous les « modèles » lancés au démarrage, ainsi que de leur chemin d'accès : il suffit de sélectionner le modèle pour que son chemin d'accès apparaisse en bas de la boîte de dialogue.
4. Sortez de Word et jetez-les.
5. Trouvez le fichier NORMAL.DOT (il est en général dans « c:\Program Files\Microsoft Office\ Modèles ») qui est chargé au démarrage. Jetez-le.
6. Relancez Word sans ouvrir de document, activez la protection de Word contre les macros et mettez un mot de passe au fichier NORMAL.DOT comme indiqué ci-dessus.

Puis nettoyez les documents contaminés

1. Assurez-vous que le fichier NORMAL.DOT est verrouillé et que la protection antivirus est activée.
2. Pour chaque document Word contaminé, ouvrez-le avec « WordPad » et faites un « Copier/Coller » sur « Nouveau Document » de Word. Puis, jetez le document contaminé et enregistrez le nouveau document Word sous son ancien nom.

Si, après avoir effectué ces opérations, cela ne va pas mieux, c'est que vous avez oublié de décontaminer un document : recommencez au début.

7.5 Où trouver antivirus et documentation ?

AVP

Un accord de licence entre le CNRS et AVP* a été contracté. Les agents CNRS ou travaillant dans un laboratoire associé au CNRS peuvent acquérir ce logiciel. Consulter : http://www.cnrs.fr/Infosecu/AVP.html

Autres antivirus

Des antivirus sont disponibles GRATUITEMENT pour les laboratoires du CNRS et de l'Université. Ils sont diffusés – ainsi que leur « mise à jour » – par les Centres de Ressources en Informatique (CRI) des Universités. Contactez le correspondant de votre CRI (http://www.cnrs.fr/achats/da7.html) et veillez bien à disposer en permanence de la toute dernière version du fichier des signatures virus. Vous pouvez également consulter le site http://www.cnrs.fr/Infosecu/viruscrp.html#Ou

Documentation

Une documentation sur les listes de diffusion vous est proposée sur le site
http://www.cnrs.fr/Infosecu/viruscrp.html#Doc

Vous pouvez vous informer sur les alertes virus sur les sites suivants :
http://www.attac.net/virdesc.htm
http://www.drsolomon.com/vircen/index.cfm
http://www.symantec.com/avcenter/vinfodb.html
http://www.trendmicro.fr/infos.htm
http://www.virusbtn.com/VirusInformation/
http://www.datafellows.com/v-descs/

Une information complète sur les virus sur :
http://www.virusbtn.com/ (le célèbre Virus Bulletin)
http://www.westcoast.com/
http://www.uta.fi/laitokset/virus/
http://agn-www.informatik.uni-hamburg.de/vtc/en9810.htm

Une bonne encyclopédie virus :
http://www.avpve.com/

* Éditeur du logiciel antivirus du même nom.

8
Les aspects juridiques de la SSI

On entend souvent dire qu'un vide juridique régnait sur l'Internet. Rien n'est plus faux ! Sous prétexte de liberté d'expression, l'Internet n'échappe pas aux lois et règlements actuels qui régissent les activités humaines et qui ont été définis depuis longtemps pour tout ce qui a trait à la propriété intellectuelle, aux contrefaçons et au respect de la vie privée. Or « nul n'est censé ignorer la loi »... et tout le monde doit connaître ce qui est légal et ce qui ne l'est pas.

8.1 Les traitements automatisés d'informations nominatives

La déclaration à la CNIL

On appelle « informations nominatives » toutes informations permettant, directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent.

La loi du 6 janvier 1978 impose à toute personne mettant en œuvre un traitement automatisé de données nominatives d'en faire une déclaration préalable auprès de la Commission Nationale de l'Informatique et des Libertés. La procédure est alourdie pour les administrations qui doivent, quant à elles, faire une demande d'avis préalable. Cette loi confère en outre aux personnes faisant l'objet du traitement un certain nombre de droits : droit d'information préalable, droit d'accès, droit de rectification.

Les fichiers comportant des informations nominatives doivent êtres déclarés à la CNIL

Commission Nationale
de l'Informatique et des Libertés

21, rue Saint-Guillaume 75340 Paris Cedex 07
Téléphone : 01 53 73 22 22
Télécopie : 01 53 73 22 00
http://www.cnil.fr

Il existe plusieurs formes de déclarations :

- Demande d'avis : c'est la demande d'avis préalable à tout traitement de données nominatives dans des services de l'Etat.
- Déclaration simplifiée : le fichier est strictement conforme à une norme prédéfinie, la procédure est alors allégée.
- Déclaration de modification : c'est une demande d'avis pour une modification d'un traitement de données nominatives déjà déclarée ou par rapport à une norme simplifiée.
- Déclaration de suppression d'archivage lorsqu'on détruit des archives.

Exemples de normes simplifiées

- Norme simplifiée n° 9 (mai 1980) relative à la gestion de prêts de livres, de supports audiovisuels et d'œuvres artistiques.
- Norme simplifiée n° 23 (juillet 1981) relative à la gestion des membres des associations régies par la loi du 1er juillet 1901.
- Norme simplifiée n° 40 (décembre 1994) concernant la mise en œuvre d'autocommutateurs téléphoniques sur les lieux de travail.

Modèles déjà déposés

Un certain nombre de modèles types de déclaration ont été soumis à la CNIL, qui les a validés.

– Pour les Universités, il s'agit pour l'instant essentiellement des fichiers associés aux services des annuaires et des listes de diffusion. (voir : http://www.cru.fr rubrique juridique).
– Pour le CNRS : modèle type de création d'annuaires web dans nos unités propres ou mixtes (CNRS 11/07/96) et annuaires EUDORA (CNRS 2/08/96).

Recommandations de la CNIL pour les traitements accessibles sur l'Internet

– Information préalable et consentement éclairé des personnes objet du traitement.
– Mention de l'interdiction de capture pure et simple des informations nominatives à des fins commerciales ou publicitaires.
– Accès, par lien hypertexte, aux dispositions légales applicables (loi de 1978…).

Vous pouvez faire appel au service juridique du CNRS pour avoir tous les conseils nécessaires concernant les déclarations CNIL.

8.2 Quelques éléments de droit à se rappeler

Droits d'auteur

« L'auteur d'une œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous. »
(Art. L.111-1. du Code de la propriété intellectuelle).

– Toute utilisation faite sans son consentement est considérée comme illicite et sanctionnée pénalement.
– La seule exception : le droit de courte citation qui permet de reproduire partiellement une œuvre à condition d'en indiquer clairement l'auteur et la source.

Les articles L.112-1.et L.112-2. du même code précisent que sont protégées toutes les œuvres de l'esprit, quels qu'en soient le genre, la forme d'expression, le mérite ou la destination, et notamment :

– les livres, brochures et autres écrits littéraires, artistiques et scientifiques ;
– les conférences, allocutions, sermons, plaidoiries et autres œuvres de même nature ;
– les œuvres de dessin, de peinture, d'architecture, de sculpture, de gravure, de lithographie ;
– les œuvres graphiques et typographiques ;

– les œuvres photographiques et celles réalisées à l'aide de techniques analogues à la photographie ;
– les œuvres des arts appliqués ;
– les illustrations, les cartes géographiques ;
– les plans, croquis et ouvrages plastiques relatifs à la géographie, à la topographie, à l'architecture et aux sciences ;
– les logiciels, y compris le matériel de conception préparatoire ;
– …

La mise sur le réseau d'un document faisant l'objet d'un droit de propriété intellectuelle (texte, photographie, dessin…) doit être opérée avec une extrême prudence. Il est impératif d'être titulaire des droits sur ce document ou pour le moins d'être autorisé à le reproduire sur le réseau.

Intrusions informatiques

Art. 323-1. Le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 100 000 F d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 200 000 F d'amende.

Art. 323-2. Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 300 000 F d'amende.

Art. 323-3. Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, ou de supprimer ou de modifier frauduleusement des données qu'il contient est puni de trois ans d'emprisonnement et de 300 000 F d'amende.

À qui appartiennent les logiciels réalisés dans les unités ?

Le CNRS est titulaire des droits sur les logiciels créés dans ses unités.

Art. L. 113-9. Sauf dispositions statutaires ou stipulations contraires, les droits patrimoniaux sur les logiciels et leurs documentations créés par un ou plusieurs employés dans l'exercice de leurs fonctions ou d'après les instructions de leur employeur sont dévolus à l'employeur qui est seul habilité à les exercer. (…)
Les dispositions du premier alinéa du présent article sont également applicables aux agents de l'État, des collectivités publiques et des établissements publics à caractère administratif.

L'utilisation de la langue française

« Dans la désignation, l'offre, la présentation (…) d'un bien, d'un produit ou d'un service, (…) l'emploi de la langue française est obligatoire. Les mêmes dispositions s'appliquent à toute publicité écrite, parlée ou audiovisuelle. » Article 2 de la loi du 4 août 1994 sur l'emploi de la langue française.

En outre, rappelons que l'emploi de la langue française s'impose à la fonction publique et dans tout document à caractère administratif ou émanant d'un service de l'État.

Conclusion

La sécurité dépend de tous, et tous les facteurs interagissent entre eux. La qualité des hommes – compétence, motivation, formation – est importante ; il faut y porter un effort constant. Les techniques et les moyens financiers sont vitaux et ne doivent pas être négligés. Mais de tous les facteurs et acteurs qui interviennent dans les systèmes d'information et contribuent à la force ou à la faiblesse de l'ensemble, les directeurs d'unité jouent le rôle essentiel. La sécurité des systèmes d'information est une fonction de Direction. Cela ne veut pas dire que les directeurs doivent mettre une casquette et contrôler les identités. Cela signifie simplement qu'ils mettent en place une organisation et ont un style de direction qui favorise ou non la prise en charge de cette question ; que ce sont eux, qui déterminent la politique de sécurité de leur laboratoire, et que ce sont eux qui la font appliquer. Il n'y a qu'eux qui peuvent le faire, et rien ne se fera s'ils ne sont pas personnellement convaincus de l'importance de cette tâche.

De même, à l'autre bout de la chaîne, l'utilisateur final a la charge de l'exécution de tous les actes élémentaires de sécurité. S'il ne voit ces mesures que comme une somme de contraintes mises en place pour lui gâcher la vie, la partie est perdue d'avance. D'où l'importance des recommandations de sécurité et des chartes informatiques qui, accompagnées des explications nécessaires, sont avant tout un moyen de sensibilisation. Bien présentées, elles deviennent le « règlement intérieur du club des utilisateurs » ; elles sont alors facilement acceptées et la vie collective du laboratoire y gagne en qualité.

Image symétrique du laxisme, le rigorisme est une autre déviance des conceptions de la sécurité. Opposé en apparence, cet autre excès aboutit au même résultat : le blocage du système d'information. Il faut donc rappeler que la sécurité n'est pas une fin en soi. Il ne s'agit pas de partir à la quête de l'absolu ou de construire une nouvelle ligne Maginot réputée infranchissable, mais de déterminer un seuil de vulnérabilité acceptable en fonction de contraintes et d'objectifs, et d'en contrôler les défaillances par des alarmes, des audits, l'enregistrement des accès réseau.
Enfin, il existe une autre manière de nier la sécurité : appliquer, sans les comprendre

et sans considération des circonstances, des règles toutes faites. La politique de sécurité doit respecter les spécificités fortes qui caractérisent notre milieu, faute de quoi elle subirait inévitablement un rejet. Ces spécificités sont principalement l'ouverture, l'imbrication des structures et le modèle organisationnel :

1. L'ouverture des laboratoires sur le monde extérieur est une exigence obligatoire de l'activité de recherche : stagiaires et chercheurs viennent du monde entier, les coopérations sont la plupart du temps internationales, les réseaux sont interconnectés…

2. L'imbrication étroite des structures de divers organismes – très souvent Université et CNRS – induit une dispersion des responsabilités. Cette situation est encore accentuée par l'organisation administrative régionale en liaison étroite – mais découplée – de la structure opérationnelle qu'est le laboratoire.

3. L'organisation des laboratoires par projets ou par thèmes de recherche favorise les structures « en râteau » aux liaisons organiques et hiérarchiques faibles et encourage une dilution de l'autorité. Les comportements individualistes, spécifiques à certains de ces milieux, sont également à prendre en compte.

Chaque laboratoire est un cas particulier. La SSI ne s'appréhende pas de la même façon suivant qu'il s'agit d'un grand laboratoire possédant des moyens financiers et humains importants ainsi qu'une culture et un savoir-faire en système et réseau, ou d'une petite unité de recherche qui a constitué son informatique par accumulations successives sans plan, sans connaissances préalables et sans personnel technique associé. Les différentes unités dans leurs diversités présentent un vaste panorama et une grande variété de structures et de cultures qui se côtoient. Il ne saurait y avoir, par conséquent, de schéma préétabli qu'il suffirait d'appliquer « à la lettre ». C'est pourquoi ce livret ne s'intitule pas « Sécurité, mode d'emploi », mais plus modestement « guide ». Sa vocation est de vous aider à fixer VOTRE politique de sécurité, non de la faire à votre place.

Les systèmes informatiques et les réseaux, qui étaient naguère l'outil d'une certaine élite, sont maintenant au cœur de tous les systèmes. Ce développement technique a permis d'accroître considérablement nos capacités de traitement, de stockage et de transmission de l'information ; mais il a rendu en même temps les systèmes d'information beaucoup plus fragiles. La gravité des accidents, des maladresses, des erreurs ou des malveillances est bien plus grande qu'auparavant : c'est souvent la perte de plusieurs jours, parfois de plusieurs semaines de travail. Ces pertes peuvent être même irréparables. Parallèlement, les techniques et les savoir-faire se sont généralisés. Il y a vingt ans, attaquer un système informatique centralisé demandait une certaine « technicité » qu'il n'est plus nécessaire de posséder aujourd'hui. On trouve sur Internet les « boîtes à outils » toutes prêtes permettant d'attaquer n'importe quel site, surtout s'il est mal administré.

Même Internet a changé. Il y a quelques années, c'était un réseau limité à des personnes d'une même communauté, celle de la recherche et de l'enseignement. Les malveillances étaient rares, car il était facile de connaître l'identité d'un l'interlocuteur. Maintenant l'Internet est un réseau ouvert et anonyme que certains voudraient transformer en zone de non droit. Nos habitudes d'utilisation des services de ce « réseau planétaire », ainsi que l'organisation de nos systèmes d'informations qui datent de cette époque révolue, doivent changer eux aussi. Cela prendra du temps car la tâche est immense. Raison de plus pour commencer maintenant.

La charte utilisateur

Charte utilisateur pour l'usage de ressources informatiques et de services Internet

DEC 99 8407 DCAJ portant approbation de la charte utilisateur pour l'usage de ressources informatiques et de services Internet

Ce texte, associé au règlement intérieur des entités, est avant tout un code de bonne conduite. Il a pour objet de préciser la responsabilité des utilisateurs en accord avec la législation afin d'instaurer un usage correct des ressources informatiques et des services Internet, avec des règles minimales de courtoisie et de respect d'autrui*.

1. Définitions

On désignera de façon générale, sous le terme « ressources informatiques », les moyens informatiques de calcul ou de gestion locaux ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade à partir du réseau administré par l'entité.

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

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

On désignera sous le terme « entité » les entités administratives créées par le CNRS pour l'accomplissement de ses missions, telles que les unités de recherche ainsi que les services et directions administratives.

2. Accès aux ressources informatiques et services Internet

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

* Pour tout renseignement complémentaire, vous pouvez vous adresser à votre correspondant sécurité.

L'activité professionnelle est celle prévue par les statuts du GIP RENATER auquel est lié le CNRS, à savoir : les activités de recherches, d'enseignements, de développements techniques, de transferts de technologies, de diffusion d'informations scientifiques, techniques et culturelles, d'expérimentations de nouveaux services présentant un caractère d'innovation technique, mais également toute activité administrative et de gestion découlant ou accompagnant ces activités.

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

L'entité pourra en outre prévoir des restrictions d'accès spécifiques à son organisation : (Carte à puce d'accès ou d'authentification, filtrage d'accès sécurisé…)

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

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

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

En particulier :

– il doit appliquer les recommandations de sécurité de l'entité à laquelle il appartient ;
– il doit assurer la protection de ses informations et il est responsable des droits qu'il donne aux autres utilisateurs, il lui appartient de protéger ses données en utilisant les différents moyens de sauvegarde individuels ou mis à sa disposition ;
– il doit signaler toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater ;
– il doit suivre les règles en vigueur au sein de l'entité pour toute installation de logiciel ;
– il choisit des mots de passe sûrs, gardés secrets et en aucun cas ne doit les communiquer à des tiers ;
– il s'engage à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux, à travers des matériels dont il a l'usage ;
– il ne doit pas utiliser ou essayer d'utiliser des comptes autres que le sien ou de masquer sa véritable identité ;
– il ne doit pas tenter de lire, modifier, copier ou détruire des données autres que celles qui lui appartiennent en propre, directement ou indirectement. En particulier, il ne doit pas modifier le ou les fichiers contenant des informations comptables ou d'identification ;
– il ne doit pas quitter son poste de travail ni ceux en libre-service sans se déconnecter en laissant des ressources ou services accessibles.

4. Conditions de confidentialité

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, et ceux qui sont publics ou partagés. En particulier, il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées. Cette règle s'applique également aux conversations privées de type courrier électronique dont l'utilisa-

teur n'est destinataire ni directement, ni en copie. Si, dans l'accomplissement de son travail, l'utilisateur est amené à constituer des fichiers tombant sous le coup de la loi Informatique et Libertés, il devra auparavant en avoir fait la demande à la CNIL en concertation avec le directeur de l'entité et la Direction des Contrats et des Affaires Juridiques du CNRS et en avoir reçu l'autorisation. Il est rappelé que cette autorisation n'est valable que pour le *traitement* défini dans la demande et pas pour le *fichier* lui-même.

5. Respect de la législation concernant les logiciels

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

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

6. Préservation de l'intégrité des systèmes informatiques

L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes informatiques et des réseaux que ce soit par des manipulations anormales du matériel, ou par l'introduction de logiciels parasites connus sous le nom générique de virus, chevaux de Troie, bombes logiques… Tout travail de recherche ou autre, risquant de conduire à la violation de la règle définie dans le paragraphe précédent, ne pourra être accompli qu'avec l'autorisation du responsable de l'entité et dans le strict respect des règles qui auront alors été définies.

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

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

En particulier :

– il ne doit pas se connecter ou essayer de se connecter sur un serveur autrement que par les dispositions prévues par ce serveur ou sans y être autorisé par les responsables habilités ;
– il ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède ;
– il ne doit pas usurper l'identité d'une autre personne et il ne doit pas intercepter de communications entre tiers ;
– il ne doit pas utiliser ces services pour proposer ou rendre accessible aux tiers des données et informations confidentielles ou contraires à la législation en vigueur ;
– il ne doit pas déposer des documents sur un serveur sauf si celui-ci le permet ou sans y être autorisé par les responsables habilités ;
– il doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques par courrier, forums de discussions…
– il n'émettra pas d'opinions personnelles étrangères à son activité professionnelle susceptibles de porter préjudice au CNRS ;
– il doit s'imposer le respect des lois et notamment celles relatives aux publications à caractère injurieux, raciste, pornographique, diffamatoire.

L'entité ne pourra être tenue pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se sera pas conformé à ces règles.

8. Analyse et contrôle de l'utilisation des ressources

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

9. Rappel des principales lois françaises

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

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

10. Application

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

Elle sera annexée, à titre d'information, aux contrats de travail conclus avec les agents contractuels qui auront accès au système informatique de leur entité.

Elle sera en outre signée par toutes personnes accueillies au CNRS et ayant accès au dit système.

Vocabulaire abrégé des techniques de piratage

PIRATAGE D'UN SITE INFORMATIQUE

Contournement du point d'entrée (Back door)
: Branchement clandestin d'un modem à une station du réseau local, de manière à se connecter directement de/vers l'extérieur.

Découverte du numéro de séquence (TCP sequence number guessing)
: Calcul du numéro de séquence TCP afin d'agir « en aveugle ».

Espionnage du réseau (Sniffeur)
: Écoute des paquets pour déterminer la topologie et les comptes utilisés.

Fragmentation des paquets (IP fragmentation)
: Modification de l'offset de fragmentation pour obtenir un recouvrement des données.

Intrusion sur le routeur (Router hacking)
: Utilisation du compte administrateur pour modifier les tables de routage.

Routes par défaut (Source routing)
: Détournement des paquets IP vers une station pirate.

Saturation du réseau (TCP denial of service)
: Atteinte à la disponibilité du réseau par envoi d'un grand nombre de demandes de connexion.

Table de conversion d'adresse (DNS hacking)
: Modification des tables du serveur de nom.

Usurpation d'adresse (IP spoofing)
: Utilisation d'une adresse IP interne depuis l'extérieur.

Usurpation de nom de domaine (DNS spoofing)
: Détournement des requêtes DNS vers une station pirate.

Vol de connexion (TCP connection hacking)
: Utilisation d'une connexion après authentification de l'utilisateur autorisé.

PIRATAGE D'UN SERVEUR OU D'UNE STATION

Applet JAVA (JAVA applet)
: Récupération d'informations privées, voire d'exécution de programmes, sur la station de l'utilisateur.

Bogue du serveur (Server bug)
: Exploitation d'unebogue du serveur pour lancer des commandes système.

Bogue du système d'exploitation. (O.S. bug)
: Exploitation d'un bogue du système pour lancer des commandes avec des droits usurpés.

Bombe E-mail (Email bomber)
: Saturation de la boîte aux lettres d'un utilisateur.

Cheval de Troie (Trojan horse)
: Récupération d'un cheval de Troie déclenchant une action non autorisée sur le système.

Fonction JavaScript (JavaScript command)
: Récupération d'informations privées sur la station de l'utilisateur grâce aux fonctions JavaScript.

Module ActiveX (ActiveX code)
: Récupération d'informations privées, voire d'exécution de programmes, sur la station de l'utilisateur.

Mystification (User mystification)
: Utilisation de l'identité d'un utilisateur autorisé pour échanger des messages et récupérer des informations.

Outil d'analyse réseau (SATAN, ISS)
: Exploitation d'un service réseau non contrôlé pour accéder au système.

Profil de consultation (User profile)
: Récupération du profil d'un utilisateur par analyse des consultations effectuées afin de mieux le connaître, voire de le désinformer.

Script CGI (CGI script)
: Envoi vers le serveur de commandes système récupérées comme paramètres par le script CGI.

Utilisation des ressources (Use of resource)
: Ajout de pages personnelles à consulter ou de fichiers personnels à télécharger dans la base du serveur.

Virus informatique
: Récupération d'un virus infectant le système.

Vol de compte utilisateur
(Name and password guessing)
: Découverte d'un mot de passe associé à un compte utilisateur pour usurper l'identité de ce dernier et agir sur le serveur.

Serveurs d'informations utiles

- UREC : unité réseaux du CNRS : recommandations CNRS, cours, articles, outils de base, pointeurs vers autres serveurs. Informations ciblées pour les laboratoires CNRS. http://www.urec.fr/securite

- Service du Fonctionnaire de défense du CNRS : protection du patrimoine, recommandations CNRS, virus, bulletin sécurité informatique. Informations ciblées pour les laboratoires CNRS. http://www.cnrs.fr/Infosecu/accueil.html

- Service juridique du CNRS : l'Internet et la législation. Informations ciblées pour les laboratoires CNRS. http://www.sg.cnrs.fr/internet/legislation.htm

- Comité Réseaux des Universités (CRU) : énormément de références sur tout ce qui a trait à la sécurité, une des références françaises, très complète. http://www.cru.fr/Securite/index.html

- CNIL : Informatiques et Libertés mais aussi des conseils et des informations liés à l'Internet. http://www.cnil.fr

- SCSSI : Le site du Service Central de la Sécurité des Systèmes d'Information. http://www.scssi.gouv.fr/

- COMMUNICATION: Dernières informations gouvernementales liées à l'Internet (réglementation française en matière de cryptologie, nom de domaine…). http://www.telecom.gouv.fr/francais.htm

- OSSIR : association avec groupes de travail Unix, réseaux et Windows NT. http://www.ossir.org/

- CERT-CC : CERT avec logiciels de sécurité, documents, notes d'information… ftp://info.cert.org/pub

- CIAC : CERT avec logiciels de sécurité, documents, notes d'information… http://ciac.llnl.gov:80/ciac/

- FTP : de l'« Eindhoven University of Technology » ftp://ftp.win.tue.nl/pub/security/

Bibliographie thématique abrégée

INTERNET

Internet and tcp/ip security for Unix administrators. PABRAI.
Mac Graw Hill USA. ISBN 0-07-048215-2 (11/1996), 320 p. (320 FF)
Computer networks and Internet. (2e éd.). COMER.
Prentice Hall. ISBN 0-13-084222-2 (02/1999), 580 p. (320 FF)
Internet: complete reference, millenium edition. YOUNG.
Mac Graw Hill USA. ISBN 0-07-211942-X (04/1999), 992 p. (365 FF)

SÉCURITÉ UNIX

Security in computing. (2e éd.). PFLEEGER.
Prentice Hall. ISBN 0-13-185794-0 (07/1997), 574 p. (350 FF)
Practical Unix and Internet security. (2e éd.). GARFINKEL.
O'Reilly. ISBN 1-56592-148-8 (05/1996), 971 p. (339 FF)
Cookbook for serving the Internet Unix version. BOURNE.
Prentice Hall. ISBN 0-13-519992-1 (07/1997), 250 p. (235 FF)
Linux configuration & installation. (4e éd.). VOLKERDING.
Transworld publishers ltd. ISBN 0-7645-7005-6 (10/1998), 554 p. (300 FF)

SÉCURITÉ WINDOWS NT

Guide pratique de la sécurité sous Windows NT. SHELDON.
Vuibert. ISBN 2-7117-8623-4 (07/1998), 588 p. (320 FF)
Windows NT 4.0 Registry professional reference. THOMAS.
Mac Graw Hill USA. ISBN 0-07-913655-9 (01/1998), 764 p. (470 FF)
Windows NT 4.0 server: security guide. GONCALVES.
Prentice Hall. ISBN 0-13-679903-5 (01/1999), 400 p. (380 FF)

ADMINISTRATION DES RÉSEAUX

Heterogeneous Internetworking. SINGH.
Prentice Hall. ISBN 0-13-255696-0 (05/1999), 672 p. (325 FF)
Sécurité réseaux. STANG.
Dunod. ISBN 2-10-002108-7 (11/1996), 652 p. (298 FF)

VIRUS

Du virus à l'antivirus, guide d'analyse. LUDWIG.
Dunod. ISBN 2-10-003467-7 (05/1997), 720 p. (398 FF)

ROUTEURS ET GARDES-BARRIÈRES

Firewalls and Internet security. (2e éd.). CHESWICK.
Addison Wesley. ISBN 0-201-63466-X (04/1999), 340 p. (330 FF)
Firewalls complete. GONCALVES.
Mac Graw Hill USA. ISBN 0-07-024645-9 (05/1998), 635 p. (390 FF)
Building Internet firewalls. CHAPMAN.
O'Reilly. ISBN 1-56592-124-0 (10/1995), 515 p. (279 FF)
Introduction to Cisco router configuration. CHAPPELL.
MTP. ISBN 1-57870-076-0 (12/1998), 900 p. (455 FF)

CRYPTOLOGIE

Cryptographie appliquée. (2e éd.). SCHNEIER.
ITPS. ISBN 2-84180-036-9 (11/1996), 896 p. (355 FF)
Handbook of applied cryptography. MENEZES.
CRC Press. ISBN 0-8493-8523-7 (01/1997), 816 p. (656 FF)
Internet cryptography. SMITH.
Addison Wesley. ISBN 0-201-92480-3 (08/1997), 356 p. (250 FF)
Basic methods of cryptography. LUBBE.
Cambridge University Press. ISBN 0-521-55559-0 (03/1998), 243 p. (230 FF)

WEB

WWW security: How to build a secure World Wide Web. MAC GREGOR.
Prentice Hall. ISBN 0-13-612409-7 (03/1997), 224 p. (300 FF)
Protecting your website with firewalls. GONCALVES.
Prentice Hall. ISBN 0-13-628207-5 (07/1997), 500 p. (340 FF)

D'INTÉRÊT GÉNÉRAL

Menace sur Internet. DESTOUCHE.
Édition Michalon. ISBN 2-84186-101-5 (100 FF)
Knowledge power: quality information and knowledge. LEE.
Prentice Hall. ISBN 0-13-010141-9 (03/1999), 400 p. (285 FF)
Cyberwars espionnage on the Internet. GUISNEL.
Plenum. ISBN 0-306-45636-2 (08/1997), 295 p. (250 FF)
Intelligence stratégique sur Internet. REVELLI.
Dunod. ISBN 2-10-003621-1 (04/1998), 212 p. (185 FF)
Du renseignement à l'intelligence économique. BESSON.
Dunod. ISBN 2-10-003220-8 (11/1996), 224 p.
Sécurité et qualité des systèmes d'information. GUINIER.
Masson. ISBN 2-225-82686-2 (01/1992), 300 p. (319 FF)
Droit à l'épreuve du numérique. CATALA.
PUF. ISBN 2-13-049357-2 (05/1998), 352 p. (138 FF)


UN DISQUE DUR QUI S'EFFACE C'EST 200 BIBLIOTHÈQUES QUI BRÛLENT...

Coordination et conseil technique

Jacqueline Leclère

CNRS-DIST

Conception graphique et réalisation

La Souris

Dessins

Loïc Faujour

Centre National de la Recherche Scientifique
3, rue Michel-Ange
75794 Paris Cedex 16

Téléphone : 01 44 96 41 84
Télécopie : 01 44 96 49 95

Courriel : robert.longeon@cnrs-dir.fr
http://www.cnrs.fr/Infosecu

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE