SÉCURITÉ INFORMATIQUE
numéro 34 avril 2001
SÉCURITÉ DES SYSTÈMES D'INFORMATION

La sécurité des systèmes d'information, une priorité gouvernementale

éditorial

Dès les années 70, les développements de l'informatique avaient conduit à légiférer pour préserver les libertés individuelles et à créer la CNIL (Commission Nationale Informatique et Libertés). Au cours des années 80 une préoccupation nouvelle était apparue en matière de protection des systèmes d'information de l'État, lorsqu'il était devenu clair que les progrès continus en matière de technologies de l'information allaient conduire à une interpénétration profonde du chiffre et de la transmission. Créé en 1986, le Service central de la sécurité des systèmes d'information fut alors chargé d'apprécier le niveau de protection des systèmes d'information de l'État, de participer aux activités de recherche et de coordonner les études et développements faits dans le domaine de la SSI.

Mais il faudra attendre le discours d'Hourtin du 25 août 1997 et les travaux du Comité interministériel pour la société de l'information (CISI) pour que soit publié en janvier 1998, le Programme d'action gouvernemental pour l'entrée de la France dans la société de l'information (PAGSI) bientôt suivi, en août 1998, de la mise en place de la MTIC (Mission interministérielle de soutien technique pour le développement des technologies de l'information et de la communication dans l'administration). « L'administration électronique » devient alors un objectif majeur du gouvernement tandis que, cette même année, le SCSSI est pleinement intégré au sein du SGDN.

Ces orientations sont confirmées et renforcées une première fois à l'issue du CISI du 19 janvier 1999, lorsque le Premier ministre décide la création d'un centre d'alerte et de réponse aux attaques informatiques, pour l'administration. Il annonce également un accroissement significatif des moyens techniques et humains affectés à la sécurité des systèmes d'information, à la fois par le renforcement du SCSSI et par le développement des moyens techniques nécessaires aux services administratifs pour s'adapter à la diffusion accrue des outils cryptologiques.

Dans son discours d'Hourtin du 26 août 1999, le Premier ministre souligne à nouveau que le développement des nouvelles formes de criminalité fondées sur les technologies de l'information et la communication nécessitent une réflexion en profondeur sur les risques encourus par les infrastructures vitales du pays et sur la nécessaire adaptation de l'appareil gouvernemental. Celle-ci passe notamment par la création, au sein de la Direction générale de la police nationale, d'un Office central de lutte contre la criminalité liée aux technologies de l'information. Elle passe aussi par la modernisation et la montée en puissance du Secrétariat général de la défense nationale, avec en particulier trois ambitions : accroître l'expertise et le savoir-faire dans tous les secteurs concernés de la SSI ; accroître les capacités opérationnelles d'évaluation et de réaction face aux menaces ; préparer une adaptation des textes réglementaires et législatifs au nouveau contexte.

suite page 6

Le traitement des incidents informatiques

Malgré l'amélioration constante de la qualité de production des logiciels, tout système d'exploitation et tout logiciel, d'une manière générale, comportent des erreurs résiduelles liées aux outils employés (atelier de génie logiciel, compilateur, éditeur de lien, bibliothèque des fonctions système...) et parfois introduites volontairement.

On peut trouver sur l'Internet de nombreux sites qui permettent, en fonction d'un système d'exploitation ou du numéro de version d'un logiciel, de connaître l'ensemble des failles. On trouve également de nombreux sites qui proposent un ensemble d'outils tous prêts permettant d'exploiter ces failles, un hacker aujourd'hui n'a plus besoin de savoir programmer il lui suffit simplement « de faire son marché » sur les nombreux sites existants sur Internet et de les utiliser ensuite en fonction des failles qu'il a repérées (voir par exemple le site http://packetstorm.securify.com).

La seule manière de se protéger contre ce type d'attaque est de ne jamais installer une machine avec une « installation par défaut » (voir encadré) mais de toujours réfléchir à l'utilisation qui en est prévue, de n'installer uniquement que les processus strictement nécessaires et de les configurer en fonction des besoins associés. Il faut également connaître parfaitement l'état de son parc informatique :

– qu'est-ce qui est installé sur chaque machine ;
– quelles sont les versions du système d'exploitation et des logiciels installés ;

et suivre les avis et alertes publiant les failles découvertes ainsi que les parades associées et appliquer les correctifs proposés.

Enfin, il ne faut jamais oublier de sensibiliser l'ensemble du personnel aux aspects de la SSI (Sécurité des Systèmes d'Information).

Les CERTs ou CSIRTs

Création du premier CERT

La seconde moitié des années quatre-vingt vit le réseau « Arpanet », développé par le DoD (Département de la Défense américain), sortir de la phase de R&D pour devenir une réalité pratique, « Internet », sous l'impulsion du monde universitaire. L'efficacité et la constante amélioration des divers services, dont le courrier électronique, rendirent rapidement ce réseau indispensable pour de nombreux sites.

En novembre 1988, un étudiant de l'Université de Cornell lâcha sur ce réseau un programme qui se propageait et se répliquait tout seul. Ce programme, connu sous le nom de « ver Internet », exploitait diverses failles de sécurité du système Unix (le système d'exploitation de la majorité des ordinateurs connectés sur le réseau). Bien que programmé sans intentions malveillantes, ce premier virus informatique, se répandit rapidement tout en engorgeant les machines infectées par de multiples copies du ver. À cette époque, le réseau comprenait

suite page 2

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

..... Suite de la page 1 ....

environ 60000 ordinateurs. Avec seulement 3 à 4 % de machines contaminées, le réseau devint complètement indisponible pendant plusieurs jours jusqu'à ce que des mesures conservatoires soient prises (dont la déconnexion de nombreuses machines du réseau).
Pour éliminer le « ver Internet », une équipe d'analyse ad hoc fut créée avec des experts du MIT, de Berkley et de Purdue. Le code du virus fut reconstitué et analysé ce qui permit, d'une part, d'identifier et corriger les failles du système d'exploitation, et d'autre part, de développer et diffuser des mécanismes d'éradication. À la suite de cet incident, le maître d'ouvrage d'Arpanet, la DARPA (Defense Advanced Research Projects Agency), décida la mise en place d'une structure permanente, le CERT/CC (Computer Emergency Response Team/Coordination Center), semblable à l'équipe réunie pour résoudre l'incident, au sein de l'université de Carnegie-Mellon (www.cert.org). Le mot CERT étant sous un copyright de l'université de Carnegie-Mellon, c'est le terme CSIRT (Computer Security Incident Response Team) qui est souvent utilisé comme synonyme.
Depuis Internet n'a cessé de croître pour devenir le réseau que nous connaissons aujourd'hui, avec une multiplication rapide des machines connectées (plusieurs millions) et malheureusement des sources d'agression.

Rôle et mission d'un CERT

Les tâches prioritaires d'un CERT sont les suivantes:
- centralisation des demandes d'assistance suite aux incidents de sécurité (attaques) sur les réseaux et les systèmes d'informations: réception des demandes, analyse des symptômes et éventuelle corrélation des incidents;
- traitement des alertes et réaction aux attaques informatiques: analyse technique, échange d'informations avec les autres CERTs, contribution à des études techniques spécifiques;
- établissement et maintenance d'une base de donnée des vulnérabilités;
- prévention par diffusion d'informations sur les précautions à prendre pour minimiser les risques d'incident ou au pire leurs conséquences;
- coordination éventuelle avec les autres entités (hors du domaine d'action): centres de compétence réseaux, opérateurs et fournisseurs d'accès à Internet, CERTs nationaux et internationaux.

La coordination internationale

Le FIRST (Forum of Incident Response and Security Teams)

Peu après l'incident du « ver Internet », le DoE (Département de l'Énergie américain) créait son propre centre d'alerte, le CIAC (Computer Incident Advisory Capability), pour servir ses clients.
Durant les deux années qui suivirent, le nombre d'équipe continua à progresser de part le monde, chacune avec ses propres finalités et financements. Les difficultés de communication inhérentes (standards internationaux, langues, conventions) risquaient de compromettre l'intérêt premier d'un CERT: une coordination centralisée.
En octobre 1989, un autre incident majeur ayant affecté plusieurs nœuds du réseau SPAN (Space Physic Academic Network) révéla la nécessité d'un meilleur dialogue entre ces diverses structures. Le FIRST fut alors créé en 1990, et n'a depuis cessé de croître et de s'adapter en réponse aux besoins des CERTs et de leurs organismes d'appartenance; il permet de fédérer l'ensemble des équipes de réaction aux incidents concernant la sécurité des systèmes d'information (www.first.org).

Rôle et mission du FIRST

Les buts mis en avant par le FIRST sont:
- favoriser la coopération entre les équipes pour prévenir, détecter et rétablir un fonctionnement nominal en cas d'incident de sécurité informatique;
- fournir un moyen de communication commun pour la diffusion de bulletins et d'alertes sur des failles potentielles et les incidents en cours;
- aider au développement des activités de ses membres, en particulier la recherche et les activités opérationnelles;
- faciliter le partage des informations relatives à la sécurité, des outils, des méthodes et des techniques.

À ce jour, 86 CERTs sont membres du FIRST. Parmi ces 86 CERTs, on trouve 41 CERTs « publics » (15 CERTs gouvernementaux et 26 CERTs dans le domaine de l'enseignement et de la recherche) et 39 CERTs « privés » dont 11 appartiennent à des opérateurs de télécommunications ou à des ISPs.
Le FIRST organise une conférence annuelle internationale « Computer Security Incident Handling Conference » dont le thème principal est le traitement des incidents de sécurité et le partage de l'expérience et de l'expertise dans ces domaines. Cette conférence est destinée aux membres du FIRST, mais est aussi ouverte aux non-membres; la 13e conférence du FIRST se tiendra, cette année, du 17 au 22 juin 2001 à Toulouse.

La coordination européenne

Une coordination des CERTs européens se met actuellement en place: un secrétariat permanent est assuré et des réunions trimestrielles sont organisées. Cette coordination est assurée au travers d'une « task force » (TF-CSIRT) de TERENA (Trans-European Research and Education Networking Association).
Le TF-CSIRT (www.terena.nl/task-forces/tf-csirt/) regroupe actuellement une vingtaine de CERTs provenant de 15 pays (Allemagne, Autriche, Belgique, Danemark, Espagne, Finlande, France, Grande-Bretagne, Grèce, Italie, Norvège, Pays-Bas, Slovénie, Suède et Suisse), parmi lesquels on trouve deux organismes européens (CERN et DANTE).

Les CERTs français

Il existe trois CERTs en France:
- le CERT-RENATER: c'est le plus ancien des CERTs français; il est dédié à la communauté des membres du GIP RENATER (Réseau National de Télécommunications pour la Technologie, l'Enseignement et la Recherche);

Un exemple typique d'incident

Le 23 juin 2000, une faille concernant le serveur WU-FTPd (démon FTP de l'Université de Washington) est publiée ainsi que l'outil permettant d'exploiter cette faille. Le 10 juillet 2000, un serveur est installé avec les options « par défaut ». Le 16 juillet 2000, l'administrateur de ce serveur constate un très grand nombre de requêtes de type finger vers son serveur et alerte immédiatement le CERT de son domaine.
Après analyse du serveur, il est constaté qu'une partie des traces avait été effacée, qu'un root-kit ainsi qu'un scanner, outils classiques des hackers, avaient été installés (le root-kit est un ensemble d'outils permettant d'obtenir les droits d'administration lors des connexions ultérieures, le scanner est un outil qui permet d'analyser un sous-ensemble d'Internet, qui interroge chaque machine connectée pour connaître le nom et la version de son système d'exploitation, les principaux services ouverts et les principaux logiciels installés. En comparant ces informations avec la liste des vulnérabilités connues, on peut immédiatement connaître la meilleure manière de compromettre cette machine).
Dans les traces laissées par le scanner, on trouve les résultats d'une analyse de tous les serveurs FTP de plusieurs classes B. L'analyse de ces informations permet de découvrir que:
– en 2 ou 3 jours, le scanner a analysé 68539 machines;
– parmi ces 68539 machines, 2013 (environ 3 %) utilisaient un serveur WU-FTPd;
– parmi les 2013 serveurs WU-FTPd, 296 avaient appliqué le correctif nécessaire.
Conclusion: 85 % des serveurs WU-FTPd étaient vulnérables soient 1717 machines.

– le CIRT-IST (Industrie, Services et Tertiaire): c'est un CERT privé qui a été créé à la fin de l'année 1998 par quatre partenaires: ALCATEL, le CNES, ELF et France Télécom;
– le CERTA: c'est le CERT dédié au secteur de l'administration française.

Les trois CERTs français essaient de maintenir des liens très étroits entre leurs trois entités, cela se traduit par: le partage du travail sur le traitement de certains incidents; la rédaction en commun de logiciels concourant à améliorer la sécurité: par exemple le CERTA et le CERT-IST ont proposé des améliorations de la libsafe, réalisée par la société Lucent, pour se protéger des débordements dans la pile; la participation commune à des conférences sur la sécurité.

Le CERTA

La création du CERTA (Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques) a été annoncée par le Premier ministre à l'issue du Comité Interministériel pour la Société de l'Information (CISI), le 19 janvier 1999:

« ... Renforcer la protection des réseaux de l'État contre les attaques.

« Afin de renforcer et de coordonner la lutte contre les intrusions dans les systèmes informatiques des administrations de l'État, le Gouvernement décide la création d'une structure d'alerte et d'assistance sur l'Internet, chargée d'une mission de veille et de réponse aux attaques informatiques. Placée auprès du Secrétariat Général de la Défense Nationale, elle travaillera en réseau avec les services chargés de la sécurité de l'information dans l'ensemble des administrations de l'État. Elle participera au réseau mondial des CERT (Computer Emergency Response Team).»

Rattaché à la sous-direction « Opérations » de la Direction centrale de la sécurité des systèmes d'information (DCSSI) au sein du Secrétariat général de la défense nationale (SGDN), le CERTA est chargé d'assister les organismes de l'administration à mettre en place des moyens de protection et à résoudre les incidents ou les agressions informatiques dont ils sont victimes. Il constitue le complément indispensable aux actions préventives déjà assurées par la DCSSI et qui se situent plus en amont dans la démarche de sécurisation des systèmes d'information.

Le CERTA a été mis en place au cours du dernier trimestre de l'année 1999 et il a été inauguré le lundi 21 février 2000 par Monsieur Jean-Claude MALLET, secrétaire général de la défense nationale, en présence de Monsieur Jean-Noël TRONC, conseiller technique pour les technologies de l'information et de la communication, auprès de Monsieur Lionel JOSPIN.

Les deux principaux objectifs du CERTA sont d'assurer la détection des vulnérabilités et la résolution d'incidents concernant la sécurité des systèmes d'information (SSI) ainsi que l'aide à la mise en place de moyens permettant de se prémunir contre de futurs incidents. Afin d'assurer ces deux objectifs, les trois missions suivantes doivent être menées en parallèle: assurer une veille technologique; organiser la mise en place d'un réseau de confiance; piloter la résolution d'un incident (si besoin en relation avec le réseau mondial des CERTs). Le CERTA est membre du FIRST depuis le 12 septembre 2000 et participe à la coordination européenne au sein du TF-CSIRT.

Les documents émis par le CERTA

Les documents émis par le CERTA sont de quatre types:

- les « Avis »: dans ce type de document on trouve une brève description de la vulnérabilité concernée, de ses conséquences et de la manière de s'en protéger (généralement une nouvelle version d'un logiciel ou un « patch » publié par l'éditeur);
- les « Alertes »: ce sont des Avis pour lesquels le moyen de se protéger n'a pas encore été publié (il peut s'agir d'un nouveau type d'attaque, d'une faille découverte dans un protocole…). Il est donc nécessaire de mettre en place des moyens de protection spécifiques à l'architecture du site. La première Alerte publiée par le CERTA, le 4 mai 2000, correspond à l'incident lié au virus ILOVEYOU. Les virus sont avant tout un phénomène médiatique auquel il convient de ne pas attacher trop d'importance, le CERTA publie de temps à autre des alertes sur des virus, non pas parce que ces virus présentent un intérêt particulier, mais parce c'est l'occasion de rappeler les règles de prophylaxie de base;
- les « Notes d'Information »: ce sont des notices plus documentées que les simples avis ou alertes, et qui donnent une explication complète d'un mécanisme. La première Note d'Information publiée par le CERTA a concerné les attaques en déni de service distribué (DdoS) du mois de février 2000;
- les « Recommandations »: ce sont des documents qui traitent plus particulièrement de méthodes d'organisation.

Veille technologique

C'est la base technique du CERTA. Afin de l'assurer correctement, il est nécessaire:
– de surveiller le plus grand nombre possible de sources d'information;
– de recouper ces différentes informations afin de s'assurer de l'existence réelle d'une faille et ne pas propager des rumeurs;
– de reproduire éventuellement cette faille sur une plate-forme de test pour en comprendre le mécanisme et les limites;
– d'élaborer ou tester la ou les parades associées;
– de diffuser un bulletin d'alerte (voir encadré) expliquant la faille et les moyens de s'en prémunir;
– d'inscrire cette faille et l'ensemble des éléments associés dans une base de connaissance pour en conserver la trace et faire croître le niveau d'expertise.

Réseau de confiance

Pour qu'un CERT soit efficace, il est nécessaire que l'information circule de manière sûre: il doit donc utiliser des moyens de communications de confiance avec ses correspondants. Il existe au moins deux flux d'information entre le CERTA et ses correspondants qui sont de natures très différentes: le sens CERTA vers administration, et le sens administration vers CERTA.

- CERTA vers administration: ce flux correspond essentiellement aux informations techniques qui sont produites par le CERTA. Pour que cette information soit exploitée le plus efficacement possible, il est nécessaire qu'elle arrive le plus rapidement possible aux personnes concernées, qu'elle soit largement diffusée, et que l'on puisse facilement authentifier l'émetteur et vérifier l'intégrité du message. Ce flux est constitué par de la messagerie Internet avec signature des messages.
- Administration vers CERTA: ce flux correspond essentiellement aux informations de type incident qui sont déclarées au CERTA. Pour que ces informations soient traitées rapidement et efficacement, il est nécessaire qu'elles soient validées, qu'elles soient de même nature (besoin de formats et d'outils normalisés), et qu'il y ait une garantie sur le traitement confidentiel de ces informations. Ce flux utilise donc un chemin sûr.

Résolution d'incident

Pour qu'un incident puisse être résolu le plus rapidement possible, il est nécessaire:
– d'être prévenu dès sa détection;
– de réunir l'ensemble des éléments significatifs permettant de le résoudre;
– d'estimer sa portée afin d'informer et/ou de travailler avec les autres CSIRTs à sa résolution;
– d'élaborer avec le correspondant une solution, qui sera ensuite appliquée par celui-ci pour traiter l'incident;
– d'alimenter la base de connaissance avec les éléments de l'incident.

Michel DUPUY
DCSSI/SDO/CERTA

Quelques remarques suite à un incident récent au niveau de l'émission d'un message électronique

Au cours de sensibilisations à la sécurité des systèmes d'information, un certain nombre de personnes voient s'ouvrir devant elles un gouffre béant: elles réalisent brutalement la réalité des faiblesses des outils de l'internet. L'absence de garanties quelconques en ce qui concerne l'origine des messages, la facilité avec laquelle il est possible de falsifier les adresses visibles d'émetteur, accompagnent l'extraordinaire capacité des réseaux de messageries à propager rumeurs, fausses informations voir actions, influence (dans ce cas, il n'y a pas de grande différence avec le téléphone portable).

Bien sûr, il est très facile avec n'importe quel navigateur d'envoyer un courrier dont le champ émetteur (From: universel dans les internets, extranets et intranets) contienne n'importe quoi, y compris une identité empruntée, voire celle d'une autorité[1].

Par contre, il existe déjà, au-delà des principes de droit qui engagent la responsabilité des personnes physiques bien avant celle des organisations – prévue par le code pénal et le code civil –, une jurisprudence condamnant le prêt d'identité[2], y compris sur le courrier électronique[3] sans besoin de recourir à un quelconque futur droit spécifique: un « techno-droit ».

De plus, on ignore trop souvent le fait que, si apparemment cette falsification d'origine du message est à la portée de tous, l'effacement complet de toute trace de la manipulation au moyen des outils spécialisés prévus n'est pas à la portée du premier venu:

- les comptes d'accès gratuit à l'internet sont soumis en fait à l'exigence d'un appel à travers une liaison identifiable (du point de vue de la responsabilité): numéro de téléphone autorisant l'affichage de son numéro à l'appel;
- les adresses IP numériques (« n.m.p.q ») et parfois symboliques (« ministere.gouv.fr ») sont présentes dans la partie cachée des en-têtes de messages[4];
- les journaux des commutateurs de messages et des dispositifs de gardes aux frontières des enclaves sécurisées contiennent des traces du trafic comprenant souvent des numéros uniques identifiant tous les messages[5];
- il existe, dans l'architecture des protocoles des réseaux internet, extranet, intranet (TCP-IP), des possibilités techniques d'effacer les indications d'origines – gênantes ou dangereuses pour la sécurité (par exemple donnant des informations sur le réseau interne) – en transférant la responsabilité de ce fait au gestionnaire du dispositif frontière qui en est alors comptable et garde une trace de ses actions. C'est sur ce principe que fonctionnent les anonymiseurs sur le réseau.
- Les médias (presse et électronique) ont propagé l'existence factice d'un anonymat sur les réseaux TCP-IP en restituant maladroitement la perplexité des experts devant la difficulté des reconstitutions de trace et la fragilité ordinaire des indices ainsi recueillis.

Les personnes impliquées et les acteurs sous-estiment bien trop souvent les conséquences de leurs actes. Ceux-ci engagent de fait leur responsabilité dès lors que l'instrument est la communication informelle à caractère personnel utilisant l'internet et les réseaux locaux internes: ils s'imaginent que ce ne sont que des paroles (« verba volent, scripta manent »).

Il s'agit d'une très grave erreur: en effet, il s'agit bien d'écrit et qui plus est d'écrit indélébile comme a tenté de le formuler un jugement récent (souhaité par les protagonistes[6]), car il est probablement impossible d'en détruire l'ensemble des exemplaires et des traces disséminées ou archivées.

La volonté des personnes sensibilisées de contribuer de façon organisée à la maîtrise des outils techniques (et des conséquences de leur emploi) dont ils disposent soit à titre personnel, soit au titre de leur mission, reste encore très inégale et doit être suscitée, renforcée, entretenue et garantie par l'organisme ou l'entreprise – conduite du changement critique pour les TIC –.

En particulier, les rappels concernant déontologie et responsabilités sont utiles à formaliser, surtout dans le domaine du recours aux outils d'information et de communication.

L'appel à la responsabilité des personnes et des organismes est essentiel, et le rappel qu'au-delà de l'existence de traces, certes complexes et coûteuses à analyser et de preuves parfois fragiles[7], des cadres légaux (loi, codes, doctrine issue de la jurisprudence, réglementations) constitue le fil d'Ariane de la gestion de la répartition des responsabilités.

Sous forme de boutade-signature, un spécialiste des réseaux indique qu'« il est nécessaire qu'une personne agisse pour mettre du désordre, mais qu'il faut et il suffit de mettre en œuvre un [micro]-ordinateur pour que cela ait des conséquences catastrophiques ». ■

1. Attention, ceci n'est pas une erreur de la normalisation, mais bien une composante clé de l'architecture de sécurité TCP-IP destinée à permettre de communiquer vers l'extérieur d'une enclave sans risquer de mettre en péril le réseau interne comme indiqué dans le quatrième alinéa.
2. Voir le Code Civil.
3. Diffamation, recherche de l'auteur, usurpation d'une adresse email (France): Cariane c/ Stéphane A. et Pascal B., TGI Paris, 14 février 2000: http://www.juriscom.net/jurisfr/cariane.htm (Voir le jugement du tribunal de Lyon.)
4. RFC 822.
5. « Le système d'identification actuel des abonnés est pragmatique. Il repose sur une combinaison de coordonnées vérifiables et de données techniques comme les données de connexion. Il est adapté à la multitude de nouveaux éditeurs que sont les Internautes et permet au juge de retrouver l'auteur d'un contenu. La loi doit en tenir compte. En revanche, si la loi fait peser de lourdes incertitudes sur les responsabilités réelles de chacun, la réaction des Internautes français sera simple: bien que déjà identifiés en pratique, ils feront héberger leurs sites chez des prestataires étrangers, en Europe ou ailleurs, loin de la nouvelle économie à la française, bien loin de l'autorité du juge français. » Extrait d'un article paru dans le *Journal du Téléphone* de mai 2000, n° 104. sous le titre « Internet: une loi mal rédigée peut déstabiliser une industrie sans protéger les citoyens », par Jean-Christophe Le Toquin, Délégué Permanent de l'Association des fournisseurs d'accès et de services Internet (AFA).
6. T. Corr. Paris, 6 décembre 2000, Carl Yves L. c/ Thierry M., Raphaël M., association Réseau Voltaire (diffamation...): http://www.juriscom.net/txt/jurisfr/cti/tcorrparis20001206.htm
   Le tribunal s'est néanmoins prononcé sur une question de procédure soulevée par les prévenus, lesquels invoquaient l'exception de prescription prévue à l'article 65 de la loi de 1881 sur la liberté de presse. Les juges ont estimé que « les caractéristiques techniques spécifiques du mode de communication par le réseau Internet transforment l'acte de publication en une action inscrite dans la durée, qui résulte alors de la volonté réitérée de l'émetteur de placer un message sur un site, de l'y maintenir, de le modifier ou de l'en retirer, quand bon lui semble, et sans contraintes particulières » et que « le point de départ de la prescription se situe au jour ou l'activité délictueuse a cessé ». (*cf.* http://www.reseauvoltaire.net/actu/proces/proces4.htm).
   http://parodie.com/articles/doc_vie_privee.htm
   « De plus, certains juges considèrent que des propos diffusés sur le web sont imprescriptibles car ils considèrent qu'il y a acte de publication continue et que la prescription ne court pas à partir de la première diffusion de l'information. Ce débat de la durée de la prescription sur Internet est donc particulièrement critique depuis plusieurs années. Les acteurs attendent une précision législative à ce niveau. Voir affaire Front National contre le réseau Voltaire. »
   Alexandre Braun, Les infractions de presse commises sur Internet prennent un caractère continu, Juriscom.net, janvier 2000: http://www.juriscom.net/espace2/delit2.htm, commentaire sur une décision belge en date du 2 mars 2000 (M.O. c/ P-Y. L. et Skynet) (cas des forums).
   L'arrêt de la Cour d'appel de Paris dans l'affaire Costes: http://www.canevet.com/jurisp/991215.htm, cas d'un serveur Web.
7. Leur recueil peut être très difficile (cas de frontières à traverser), et reste en tout cas très encadré et échappe rapidement à la compétence des responsables de la sécurité des systèmes d'information (inviolabilité de la correspondance télématique) pour passer à celle des enquêteurs munis d'une commission rogatoire (CPP 100). Voir le jugement du 2 novembre du tribunal correctionnel de Paris condamnant des agents de sécurité des systèmes d'information [de l'ESPCI] « pour action illégale dans l'exercice de leur mission »: http://www.canevet.com/jurisp/textes/001102.htm

Vous êtes pénalement responsables de vos informations sensibles, le saviez-vous ?

La protection des informations et systèmes sensibles dans les administrations

La modernisation des services de l'État[1] et le recours aux technologies de l'information et de la communication, s'ils rendent les administrations et ses services, centraux, déconcentrés et territoriaux, plus efficaces, les exposent aussi à de nouvelles vulnérabilités tout en créant un *nouvel écheveau de responsabilités entrecroisées*[2].

La directive 4201 du premier ministre[3], relative à la sécurité des systèmes d'information, clarifie le cadre des actions nécessaires pour maîtriser les risques dans ce domaine : « Sécuriser l'information doit être un souci général. Sécuriser les systèmes d'information est une obligation nationale majeure. » Elle fonde la recommandation 901 du Premier ministre[4] du 2 mars 1994 pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense. Il convient donc, après avoir défini les rôles et les responsabilités des acteurs et fait l'inventaire des informations sensibles, après avoir choisi et pris les mesures de protection, mis en place des procédures de traitement des incidents, d'identifier les situations à risques pour mieux savoir les prévenir et les gérer[5].

En ce qui concerne la mise en place de procédures d'échanges d'informations *dématérialisées*, les solutions décentralisées qui ont l'avantage de la souplesse doivent néanmoins s'inscrire dans une politique de sécurité globale clairement définie afin que les informations sensibles restent protégées dans toute la chaîne d'échanges grâce à la prise de responsabilité sans équivoque de tous les acteurs soutenus par les moyens techniques appropriés.

Cette politique est bien celle qui est mise en œuvre dans le cadre du PAGSI, en particulier dans le cadre de la mise sur internet des formulaires administratifs[6] et des téléprocédures de façon à « garantir la qualité et la fiabilité des services offerts[7] ».

En pratique, chaque unité d'un organisme, est tenue, sous la responsabilité de l'autorité qualifiée pour la sécurité des systèmes d'information ou à défaut de l'autorité hiérarchique, de faire l'inventaire[8] structuré des informations et systèmes sensibles qui lui sont propres et, pour chacun d'entre eux, d'en exprimer la sensibilité en analysant l'impact des sinistres[9]. Des mesures de protection utiles et appropriées doivent être déterminées et prises une fois les nécessaires arbitrages rendus, par l'autorité hiérarchique responsable de l'organisme, entre coûts et sécurité[10]. L'autorité hiérarchique de l'unité est personnellement responsable de l'application des mesures résultant de la politique de sécurité interne (nota PSI) de l'organisme et des mesures particulières propres à son unité.

1. PAGSI, voir les sites : www.internet.gouv.fr/francais/textesref/sommaire.html et www.mtic.pm.gouv.fr
2. « Responsabilité des décideurs et systèmes d'information », *L'actualité juridique* - Droit administratif du 20 janvier 1999.
3. Directive interministérielle n° 4201/SG du 13 avril 1995 relative à la sécurité des systèmes d'information. http://www.scssi.gouv.fr/docs/4201/4201.htm
4. N° 901/DISSI/SCSSI : « Recommandation pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense » (article 4 pour la définition). http://www.scssi.gouv.fr/document/docs/901/901.htm
5. Pp. 114, 122 et suivantes dans *Responsabilité et déontologie, guide de référence pour les chefs de services et pour l'encadrement*, 207 pages, ISBN 2-85978-285-0, Presses de l'École Nationale des Ponts et Chaussées, janvier 1998. Ministère de l'Équipement, des Transports et du Logement, Direction du Personnel et des Services DPS/GA2, Tour Pascal B 92055 PARIS – La Défense CEDEX 04 – téléphone 0140816177.
6. La circulaire du 31 décembre 1999 (parue au *JO* du 7 janvier 2000 page 00279) : http://www.legifrance.gouv.fr/citoyen/jorf_nor.cgi?numjo=PRMX0003923C
7. Le communiqué le 7 janvier 2000 http://www.premier-ministre.gouv.fr/PM/070100.HTM
8. Guide n° 730/SCSSI du 13 janvier 1997 sur les systèmes d'information et applications sensibles.
9. Voir la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) mise en œuvre dans de nombreux organismes privés et publics, élaborée par le SCSSI et disponible à l'adresse suivante : http://www.scssi.gouv.fr/document/docs/EBIOS/ebios.html
   Les principes en sont très simples : • identifier les biens (informations) et services à protéger en fonction du contexte dont les contraintes légales et réglementaires et la mission de l'organisme ; • analyser les conséquences d'incidents sur ces biens et services pour déterminer des impacts et qualifier la nature et la priorité des besoins de sécurité ; • analyser, en parallèle, les vulnérabilités des architectures techniques pour déterminer les scénarios d'agressions possibles créant des incidents de sécurité sur les biens ; et • choisir les objectifs de sécurité adéquats pour minimiser les risques : c'est-à-dire minimiser les impacts compte tenu de l'intensité des menaces. Ces objectifs de sécurité (techniques et non techniques) seront mis en œuvre par le responsable du système.
10. Guide technique n° 150/SGDN/DISSI/SCSSI du 10 février 1991 Fiche d'expression rationnelle des objectifs de sécurité (FEROS) à faire approuver par l'autorité qualifiée. http://www.scssi.gouv.fr/document/docs/150/150.html
11. Ministère de la Défense, ministère de l'Équipement.
12. Confère l'affaire de l'hôpital d'Orléans « L'État est condamné pour la divulgation d'une note de l'Inspection des affaires sociales », quotidien *Le Monde* du 21 mai 1999, page 12, Jean-Yves Nau. Taille 4672 caractères. Le tribunal administratif d'Orléans a condamné l'État, mardi 18 mai, à verser 119000 francs, à voir... http://archives.lemonde.fr
13. Loi 83-634 du 13 juillet 1983 modifiée portant droits et obligations des fonctionnaires. http://www.legifrance.gouv.fr/textes/html/fic198307130634.htm ou http://www.admi.net/jo/loi83-634.html
14. *IGI* n° 1300/SGDN/SSD/DR du 12 mars 1982. Instruction générale interministérielle sur la protection du secret et des informations concernant la défense nationale et la sûreté de l'État.
15. Loi n° 78-753 du 17 juillet 1978 : « Mesures des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal » modifiée par la loi n° 79-587 du 11 juillet 1979 (voir l'article 6) complétée par la loi n° 2000-321 du 12 avril 2000 (*JO* page 05646) relative aux droits des citoyens dans leurs relations avec les administrations. NOR : FPPX9800029L http://www.legifrance.gouv.fr/citoyen/jorf_nor.ow?numjo=FPPX9800029L ou http://www.admi.net/jo/20000413/FPPX9800029L.html

Dans certains ministères[11], cette *recommandation n° 901* est devenue une *instruction*. Cette recommandation a la même force exécutoire qu'une circulaire ou une instruction. Certaines affaires récentes[12] montrent qu'il ne faut pas prendre ces questions à la légère et que la responsabilité de l'État peut être engagée[13] à la suite d'une méconnaissance des règles élémentaires de protection des informations *sensibles* et de la responsabilité des organismes et agents des administrations.

En effet, au sein de chaque ministère et des établissements sous tutelle, il existe des informations qui, sans devoir être classifiées de défense[14], nécessitent néanmoins d'être protégées, parfois avec autant – sinon plus – de précautions.

Par exemple, le non-respect de la confidentialité de telle ou telle information porterait atteinte au secret de la vie privée. Ou encore, est-il souhaitable qu'une note de la direction de l'administration centrale en direction du cabinet se retrouve à l'extérieur ?

La *confidentialité* est le facteur prédominant dans les sinistres visibles, mais la question de l'intégrité de l'information ou sa disponibilité peuvent jouer un rôle parfois plus important. De telles informations sont qualifiées d'*informations sensibles* et ont fait l'objet de la recommandation du Premier ministre le 2 mars 1994 mentionnée plus haut. Elles comprennent notamment :

- les informations vitales pour l'exercice de la mission de l'organisme,
- les informations protégées par la loi relevant du secret professionnel (secret statistique, secret médical, secret douanier...),
- les informations nominatives au sens de la loi informatique et libertés,
- les informations qui sont soumises à l'obligation de réserve ou de discrétion, professionnelle, notamment celles qui préparent une décision finalisée[15] laquelle est seule accessible avec ses motivations définitives,
- les informations constitutives du patrimoine scientifique, industriel et technologique,
- les informations concernant les appels d'offres et marchés des administrations,
- les informations permettant d'authentifier les actes dématérialisés, mettant ainsi en jeu la responsabilité des personnes qui les initient. ■

Suite de l'éditorial

Organisation de la Direction Centrale de la Sécurité des Systèmes d'Information

Conformément aux orientations annoncées, la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) est organisée en vue de remplir, sous l'autorité du Secrétaire général de la Défense nationale, les quatre fonctions suivantes :

- fonction de contribution à la définition interministérielle et à l'expression de la politique gouvernementale en matière de SSI ;
- fonction d'autorité nationale de régulation en matière de sécurité des systèmes d'information ;
- fonction opérationnelle de conseil et soutien au profit des administrations et des services publics ;
- fonction d'expertise/contre-expertise scientifique et technique dans les différentes disciplines concernées.

Organisation générale

L'organisation retenue comprend :

- une équipe de direction constituée du Directeur et de ses adjoints ;
- une cellule de communication et un centre de formation directement rattachés à l'équipe de direction ;
- trois sous-directions chargées respectivement d'assurer les activités de régulations, les fonctions opérationnelles et l'expertise scientifique et technique.

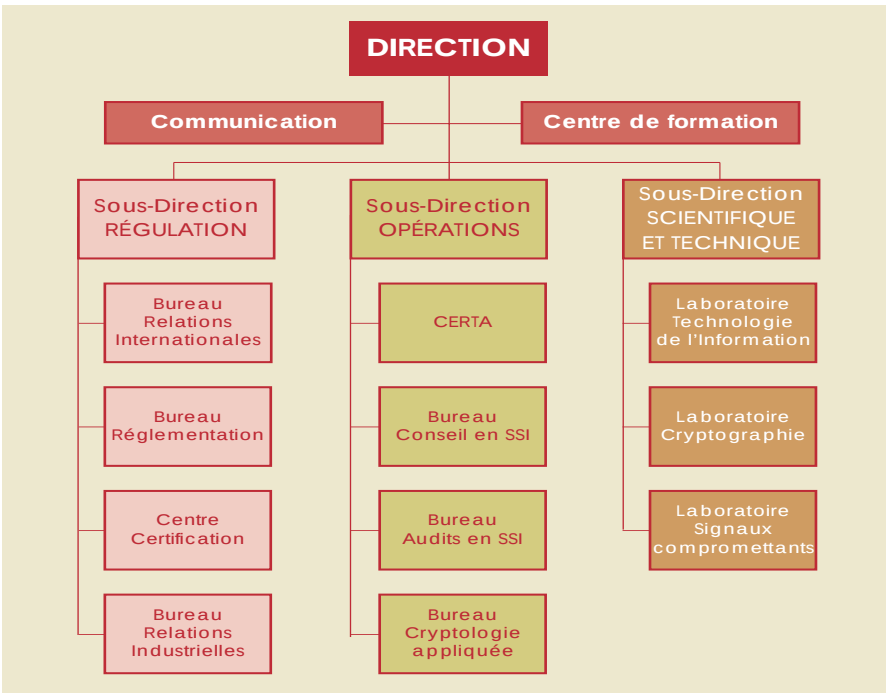
• **La Sous-direction Régulations** a pour mission :

- de conduire les travaux nécessaires à la mise en œuvre des fonctions d'autorité nationale de régulation en matière de SSI confiées au SGDN ;
- de participer à la formalisation de la politique nationale en matière de SSI, à sa mise en œuvre, à son évolution ;
- d'assurer les relations de la DCSSI avec ses homologues étrangers et de la représenter dans les instances internationales ;
- d'assurer les relations avec les industriels de la SSI.

• **La Sous-direction Opérations** appuie les administrations et services publics dans la mise en œuvre de la politique gouvernementale en matière de SSI. En particulier, elle doit :

- aider les administrations et les services publics à faire face aux incidents et aux attaques auxquels leurs systèmes d'information peuvent être soumis, en phases de détection, de résolution et de prévention ;
- conseiller les administrations pour tout problème auquel elles peuvent être confrontées en matière de SSI, au plan des méthodes de travail, de l'organisation, des procédures, des choix technologiques ;
- aider les administrations à évaluer la sécurité de leurs systèmes d'information ;
- assurer les prestations nécessaires aux administrations pour leurs fournitures cryptologiques.

• **La Sous-direction Scientifique et Technique** est chargée des études et recherches dans les disciplines essentielles de la SSI. Elle développe plus particulièrement le savoir-faire nécessaire au soutien technique des autres sous-directions. À l'appui de ses missions, elle collabore en tant que de besoin avec les services et les laboratoires extérieurs à la DCSSI. ■



La sécurité des systèmes d'information, un facteur de développement

La transformation du concept de sécurité des systèmes d'information d'une vision de protection et de défense, vers une vision d'outil de développement des nouvelles technologies et des nouvelles applications paraît donc une évolution tout à fait stratégique, partagée par le secteur public et le secteur privé.

Grâce au poids de ses entreprises dans la nouvelle économie, par la diffusion de ses compétences scientifiques et technologiques, par la créativité de ses ingénieurs, par la qualité et l'originalité de ses produits, la France s'est d'ores et déjà placée en position d'acteur majeur du cyberespace.

Mais si l'essor de ces nouvelles technologies de l'information et de la communication offre des potentialités d'enrichissement et d'épanouissement pour la collectivité et l'individu, elles se caractérisent également par de multiples vulnérabilités, provenant de nouvelles natures de risques et de nouveaux types de menaces émanant de tiers mal intentionnés.

Mais la recherche d'une meilleure sécurité et d'une plus grande confiance dans le cyberespace doit se faire dans le respect des libertés individuelles et de la protection de la vie privée des individus. Une grande vigilance s'impose face à certaines évolutions technologies et à certaines pratiques qui, mal maîtrisées ou trop faiblement régulées, pourraient aboutir à de graves atteintes à des principes fondamentaux d'un État de droit. Tout autant que la sécurité et la confiance dans le cyberespace, la France – et c'est là une de ses positions fortes dans la concertation internationale – souhaite favoriser l'émergence et la consolidation d'une cyberculture démocratique et citoyenne.

Henri Serres
DCSSI

SÉCURITÉ INFORMATIQUE
numéro 34 avril 2001
SÉCURITÉ DES SYSTÈMES D'INFORMATION

Sujets traités : tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité : 5 numéros par an.
Lectorat : toutes les formations CNRS.

Responsable de la publication :
ROBERT LONGEON
Centre national de la recherche scientifique
Service du Fonctionnaire de Défense
c/o IDRIS - BP 167. 91403 Orsay CEDEX
Tél. 01 69 35 84 87
Courriel : robert.longeon@cnrs-dir.fr
http://www.cnrs.fr/Infosecu

ISSN 1257-8819
Commission paritaire n° 3105 ADEP

Conseil et coordination : CNRS - DIST - Jacqueline Leclère • Conception et réalisation : La Souris 01 45 21 09 61