SÉCURITÉ INFORMATIQUE

numéro 33 février 2001

SÉCURITÉ DES SYSTÈMES D'INFORMATION

Ingrédients pour une bonne sécurité

éditorial

L'année dernière, environ trois cents millions d'internautes ont utilisé vingt millions de services disponibles par l'intermédiaire de près de quatre mille fournisseurs d'accès dans le monde. Chaque mois plus d'un milliard de messages sont échangés sur le réseau. Or Internet n'est pratiquement pas réglementé…, c'est la forêt de Bondy au XIX[e] siècle. La sécurité des communications est donc reportée au niveau des utilisateurs. Comprendre cela, c'est déjà avoir franchi une première étape… ; mais il faut aller plus loin : que doit-on protéger et contre quoi ? Doit-on protéger tout de la même manière et avec la même énergie ? Peut-on se contenter de courir derrière les problèmes que l'on détecte ou doit-on essayer de les anticiper ? On ne « fait pas de la sécurité » pour sacrifier à une mode mais parce que l'on cherche à atteindre des objectifs de sécurité. Ce sont ces objectifs qu'il nous faut définir, en apportant une réponse aux questions simples posées ci-dessus. C'est cette étape que je voudrais vous inviter à franchir : passer de l'ère du chasseur-cueilleur de sécurité à l'ère du cultivateur. Passer, en quelque sorte, dans ce domaine, du paléolithique au néolithique.

L'autre aspect sur lequel je voudrais insister, c'est la dimension fondamentalement humaine de la sécurité, la technique ne venant qu'après. De ce point de vue, la « démarche sécurité » est comparable à la « démarche qualité » : elle s'appuie sur une responsabilisation de l'ensemble des personnels. Ainsi, le premier niveau de responsabilité concerné est le niveau de direction. C'est à ce niveau que doivent être définis les objectifs de sécurité et les budgets au regard des priorités stratégiques. C'est également à ce niveau de responsabilité que les acteurs de la sécurité au quotidien doivent obtenir la reconnaissance de leur travail et l'appui indispensables pour asseoir leur crédibilité vis-à-vis des utilisateurs des systèmes d'information.

Le deuxième niveau est celui des administrateurs de réseau et des techniciens. C'est à eux qu'incombe la mise en œuvre des orientations retenues, en proposant pour le réseau de leur unité l'architecture, les équipements et les règles d'exploitation les mieux adaptés à l'importance de l'unité ainsi qu'à la nature de ses activités. C'est à eux, aussi, qu'il appartient de mener une action de sensibilisation permanente, tant vers l'échelon de décision que vers les utilisateurs. Enfin, derniers sans être les moindres, les utilisateurs. Leur contribution peut être déterminante par la rigueur dont ils font preuve dans le respect des consignes et par l'empressement qu'ils manifestent à rendre compte des dysfonctionnements.

Les « cyberdélinquants » peuvent disposer des technologies Internet dans les mêmes conditions que des dirigeants soucieux de bien-être et de prospérité et le duel opposant le glaive à la cuirasse n'est pas près de s'éteindre à l'ombre des arborescences de la société de l'information. La sécurité n'est jamais absolue et un niveau de sécurité jugé satisfaisant peut cesser de l'être rapidement. N'hésitons donc pas à remettre l'ouvrage sur le métier pour nous assurer de la bonne adéquation de nos objectifs et des ressources mises en œuvre pour les atteindre.

Alfred Schwenck
Fonctionnaire de défense

Pour une approche systémique de la sécurité

Comment assurer la sécurité des systèmes d'information dans ces entrelacs informationnels que sont nos laboratoires ? Ils donnent parfois l'impression d'un château de cartes : le moindre élément dérangé peut bouleverser l'ensemble. La sécurité ? Comment s'y prendre et par où commencer ? Face à cette complexité, l'attitude de certains administrateurs système varie du découragement (« de toute façon ça ne sert à rien ») à la paranoïa (blocage du système tout en laissant des brèches béantes). Certains sont tentés de chercher des solutions purement techniques (le fameux « garde-barrière » qui résout tout !) à des problèmes qui sont hors de leur portée, comme les problèmes de personnes ou d'organisation.

La sécurité est l'art de gérer le risque

La sécurité est l'état dans lequel « l'information est valide, les infrastructures garantissent l'intégrité des données et il est possible de détecter les actions malveillantes ». Malheureusement cet état, dans l'absolu, est le Saint Graal de Chrétien de Troyes, un idéal impossible à atteindre. Depuis la grande muraille de Chine construite pour arrêter les hordes mongoles jusqu'à la ligne de M. Maginot, beaucoup ont rêvé de pouvoir vivre tranquillement derrière des protections réputées infranchissables. Hélas, toutes les barrières sont faites pour être franchies – ou contournées – et tous les blindages sont faits pour être percés un jour ou l'autre. Il faut se faire à l'idée que, malgré la qualité et la vigueur des défenses, le « risque zéro » n'existe pas. Nous ne pouvons agir que sur le niveau résiduel du risque : plus nous voulons le diminuer, plus il faut faire d'efforts (et mettre de moyens). Gérer la sécurité, c'est donc gérer le risque ; c'est savoir où mettre le seuil au-delà duquel celui-ci est inacceptable et en dessous duquel, compte tenu de nos moyens, il va bien falloir l'accepter. *Le risque est le résultat de la rencontre de deux facteurs :*

- *les menaces :* elles existent indépendamment du système ;
- *les vulnérabilités* (c'est-à-dire ce qui rend le système sensible aux menaces), qui sont des données du système : c'est sur celles-ci qu'on interviendra.

La sécurité des systèmes d'information consiste donc à identifier les vulnérabilités – une combinaison d'événements fortuits peut aussi créer une vulnérabilité –, à évaluer les menaces et à déterminer le risque qu'une vulnérabilité permette à une menace donnée de se réaliser. Mais ce risque n'est pas statique, c'est un des aspects majeurs de la sécurité. La logique du défenseur n'est pas celle de l'attaquant : tandis que les premiers s'organisent pour contrer les attaques et ne

suite page 2

CNRS CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

peuvent que combler les failles connues, les attaquants, eux, en cherchent de nouvelles sur l'ensemble de l'espace ouvert : réseaux, systèmes, SGBD et applications. La sécurité doit donc être homogène sur l'ensemble du système d'information : il serait absurde de mettre en œuvre des solutions coûteuses si la sécurité peut être contournée par des attaques rudimentaires. Aussi faut-il savoir où agir en priorité.

Bref, la sécurisation d'un site est un problème complexe qui ne peut être appréhendé sans une approche systémique. Celle-ci commence par l'élaboration d'un « modèle » qui est la représentation qu'on se fait de la sécurité : quelles sont les menaces ? que doit-on protéger ? pourquoi ? C'est donc le modèle – c'est-à-dire la réponse à ces trois questions – qui donne un sens au mot sécurité. On en déduit ensuite la politique de sécurité : détermination du bon seuil en fonction des risques et des ressources disponibles, et chemin pour l'atteindre. Enfin, on spécifie les outils qui permettront de vérifier la pertinence de la politique (de préférence en temps réel, la réactivité étant fondamentale en sécurité) et de comprendre comment évoluent les menaces. Ceux-ci fournissent un ensemble d'indicateurs qu'on appelle « le tableau de bord ».

La plupart des approches méthodologiques répondent à ces caractéristiques, mais souvent de façon insuffisante.

Des améliorations possibles

Les techniques de détection de vulnérabilités (scanner), de détection d'intrusion (IDS), de traçage de flux, de filtrage, de vérification des fichiers système – quelques autres encore – constituent de puissants outils d'évaluation de la sécurité des systèmes. Ainsi rendent-elles l'élaboration de politiques de sécurité moins rigides et permettent-elles des solutions plus opérationnelles et pragmatiques. Voyons trois des améliorations majeures qu'elles offrent.

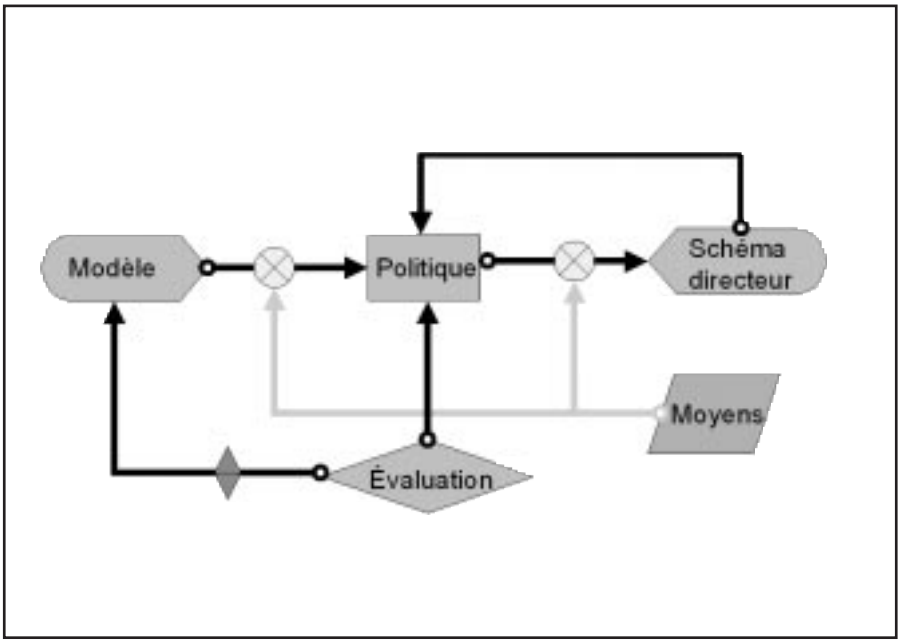
Récursivité de mise en œuvre de la sécurité

Quand les contraintes de sécurité le permettent – comme c'est souvent le cas dans notre organisme –, la politique de sécurité peut être construite par approches successives. On la définit d'abord à grands traits de façon à obtenir rapidement des résultats opérationnels. On l'ajuste ensuite récursivement, affinant contrôles, filtrages, mesures et sensibilité des alarmes. Enfin, on la pilote en fonction des modifications de l'environnement. Cette démarche permet d'appréhender la sécurité comme un processus continu, évolutif, qui tient compte de la réaction du milieu, non comme un « projet » qui établit une politique de sécurité une fois pour toutes.

Sécurité physique

Les moyens techniques sont au service d'un objectif et dans le cadre d'une organisation. C'est pourquoi, avant de penser « quelle technique ? », il faut penser « quelle organisation pour quel objectif ? ». La sécurité physique, qui est la dimension « organique » de la sécurité, doit être conçue dans ce cadre-là. Même si elle tend à devenir moins importante qu'avant dans des organismes comme les nôtres, elle demeure toutefois l'« ultima ratio regnum » :

- Contrôler les accès.
- Déconnecter les machines sensibles du réseau.
- Instaurer une « zone à accès limité » quand cela est nécessaire.
- Protéger physiquement les équipements (serveurs, câbles, équipement d'interconnexion de réseaux, …).
- Protéger le PABX.
- Avoir un plan de secours contre le feu, les inondations, la tempête, etc.



• La définition de la politique de sécurité est un processus récursif.

Mesures en temps réel du risque résiduel

Déterminer la politique de sécurité, c'est faire des choix qui doivent s'appuyer sur des mesures indépendantes des opérateurs. Les nouvelles technologies de détection de vulnérabilités et de détection d'intrusion, en donnant des valeurs statistiques, l'une sur le risque *réel*, l'autre sur les tentatives d'intrusion *réelles*, permettent d'évaluer en continu :

- le bien-fondé de la politique de sécurité,
- les écarts entre les objectifs visés et ceux qui sont atteints en réalité,
- l'évolution de l'environnement (nouvelles stratégies d'attaque, nouveaux moyens techniques, exploitation de nouvelles vulnérabilités, ...) ;

et de mettre en place les mesures correctives, sans lesquelles le système reste figé..., jusqu'à la prochaine mise à jour – souvent c'est plusieurs mois et même plusieurs années. Le filtrage des accès réseau et le traçage des flux – facilitant la détermination de la « matrice de flux » – complètent ces outils.

Rapports réguliers permettant à chacun de « suivre » la sécurité

L'adhésion des acteurs est un leitmotiv rabâché, mais, reconnaissons-le, elle n'est jamais obtenue autrement que d'une manière formelle. Les enjeux de sécurité leur paraissent le plus souvent comme très éloignés de leurs préoccupations quoti-

diennes. Les premiers de ces acteurs à convaincre sont les directeurs. Grâce aux tableaux de bord, à la production de mesures opérationnelles que génèrent ces nouveaux outils, ils peuvent lier un niveau de sécurité à un niveau de risque, définir des objectifs plus ou moins ambitieux et contrôler leur réalisation. La sécurité n'est plus ressentie comme un trou noir dans lequel s'engouffrent sans fin leurs crédits ; ce ne sont plus des dépenses obligatoires et stériles. Les directeurs peuvent maintenant contrôler l'efficacité de la politique et percevoir concrètement les enjeux de la sécurité. Ainsi, ils peuvent traiter la sécurité comme n'importe quel autre investissement.

L'adhésion de tous les acteurs est un objectif réaliste, même vis-à-vis de ceux qui n'ont pas un niveau d'expertise élevé, c'est seulement un problème de clarté de l'information. Ces nouveaux outils le permettent en apportant une « vision » de l'état de sécurité du système à chaque instant. Avec en plus un peu de pédagogie, on peut donner réellement à chacun les moyens de participer pleinement aux processus de sécurité.

Modèle, politique et mesures

Un modèle de sécurité

Le modèle de sécurité est la représentation qu'on se fait de la sécurité à partir d'une « vision du monde ». En effet, les menaces – et même l'appréciation des vulnérabilités – ne seront pas les mêmes suivant qu'on s'imagine des ennemis partout ou que l'on croit le monde « tout beau et tout rose ». Le modèle indique ce que l'on a à défendre (type et flux des informations), contre quoi (les menaces) et pourquoi (sensibilité de l'information). Il peut être plus ou moins complet, plus ou moins élaboré, mais dans tous les cas il fait ressortir peu ou prou les risques d'où l'on déduira une politique de sécurité. L'établissement d'un modèle de sécurité évite d'être perméable aux idées à la mode ou à l'argumentaire de commerciaux habiles qui, tout en proposant le « comment se protéger », disent en réalité le « quoi protéger » et le « contre qui ». Ils imposent ainsi un modèle stéréotypé.

Une politique de sécurité

Du modèle, on déduit la politique de sécurité : détermination du bon seuil de sécurité en fonction des risques et des ressources disponibles, et manière de l'atteindre. Toute politique de sécurité a pour but d'éliminer ou de réduire les vulnérabilités de façon à atteindre le niveau de risque choisi en fixant des règles à appliquer, des mesures à prendre, des structures et l'organisation à mettre en place. Elle met en évidence les éléments du système d'information sur lesquels agir à moindre coût. Elle est :
– *simple :* trop compliquée, elle est chère et elle sera contournée,
– *cohérente :* c'est le maillon le plus faible qui détermine la solidité de la chaîne ;
et s'appuie, autant que faire se peut, sur des standards, de façon à être plus facile à évaluer et à faire évoluer.

La politique de sécurité n'est pas seulement passive (mise en place d'un blindage du système), elle est aussi active : elle dit comment
– *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 ;
– *contrôler les défaillances* par des alarmes, des journalisations, des audits et le traçage des accès réseau.

Elle définit encore comment :
– mettre en place des leurres,
– faire les sauvegardes,
– mettre en place une procédure d'alerte,
– prévoir une procédure de repli et de remise en service après sinistre.

Le tableau de bord

Le tableau de bord est un ensemble d'indicateurs constituant une véritable métrique de la sécurité. Il permet de faire (de préférence en temps réel) l'évaluation de l'efficacité de la politique de sécurité, d'indiquer les modifications de l'environnement, d'alerter sur l'apparition de nouvelles faiblesses et de mesurer la vulnérabilité résiduelle du système.

La qualité de l'outil détermine la qualité de la mesure

Tous les outils de mesure ne sont pas équivalents. Par exemple, les scanners ont pour fonction d'identifier toutes les failles potentielles, parmi lesquelles les écarts par rapport à la politique de sécurité. Les IDS, quant à eux, ont pour fonction d'identifier en temps réel les tentatives d'effraction dans le système d'information. Mais ce sont des évaluations statistiques ; elles s'approcheront d'autant mieux de la réalité qu'elles pourront :

- Disposer de la base de connaissances et de tests la plus exhaustive et la mieux qualifiée possible : les utilisateurs rejetteront les produits si l'information n'est pas assez bien qualifiée ou si les produits manquent de pertinence. Lorsqu'une faille est mise en évidence, le produit doit donner les moyens d'obtenir les correctifs associés ; car, pour être responsables, les acteurs sur le terrain doivent avoir les moyens de « produire » la sécurité.

- Être déployées sur l'ensemble de la structure, pour avoir une vision complète des risques et associer l'ensemble des acteurs. L'architecture des produits doit donc permettre à la fois une distribution et une utilisation locale, ainsi que la consolidation centrale des informations.

- Fournir une information structurée, qui aide à la mise en place et permette le suivi d'une politique de sécurité. Cela va des rapports de synthèse – pour le directeur par exemple – jusqu'aux rapports de corrections détaillés pour les ingénieurs. Le produit doit enfin être capable de s'adapter à l'architecture existante et non l'inverse.

Conclusion

Courir inlassablement boucher les trous de sécurité de son système les uns après les autres, appliquer des recettes toutes faites sans comprendre les menaces, sans connaître la sensibilité de ses informations et encore moins ses vulnérabilités, sans avoir déterminé la matrice des flux, penser que la technique s'occupera de tout, etc. est une approche de la sécurité qui date... du siècle dernier. La sécurité exige une approche systémique ! Les techniques sont maintenant assez mûres pour permettre aux méthodes actuelles de devenir plus opérationnelles, plus pragmatiques, et ainsi de définir des politiques de sécurité adaptatives.

Robert Longeon
Chargé de mission à la sécurité
des systèmes d'information
Robert.Longeon@cnrs-dir.fr

Enjeux de la sécurité

On parle souvent des coûts de la sécurité, mais on oublie de parler de ceux de l'insécurité. Il faut se rappeler que certaines économies peuvent coûter très cher... C'est pour cette raison qu'on déterminera le bon niveau de sécurité en mesurant les coûts de l'un à l'aune de l'autre. L'ennui vient de ce que ces coûts ne sont pas toujours comparables. Les coûts de la sécurité sont les plus faciles à appréhender, ce sont des coûts directs, c'est-à-dire « directement budgétisés ». Mais les coûts de l'insécurité sont plus pernicieux : ils ne se présentent pas toujours comme un débours immédiat, d'autant qu'ils se trouvent souvent supportés par la collectivité tout entière. C'est pourquoi il est préférable de parler d'enjeu de la sécurité plutôt que de coûts. Il reste que la conséquence de l'insécurité est un appauvrissement global.

Maintien de la performance de notre outil de travail

Tout incident de sécurité dégrade notre outil de travail en immobilisant des moyens et des savoir-faire. En cas d'intrusion, il faut déconnecter du réseau la machine concernée ou au moins installer des filtres pour bloquer les accès interactifs. Parfois, il faut même isoler complètement le réseau de l'extérieur, le temps de sauvegarder l'image des systèmes (pour garder des traces de l'agression) et de faire une évaluation des dégâts et certaines vérifications. Il y a aussi la défaillance de l'organisation et la diminution globale de l'efficacité dues à l'utilisation pirate des ressources.

Un administrateur système raconte son expérience de restauration des systèmes après une intrusion : « Il a fallu réinstaller complètement les serveurs et changer tous les mots de passe. Bilan : ça nous a coûté l'autre fois environ 1 000 heures, on doit en être facilement à l'équivalent de la moitié d'un poste IR de manière permanente sur la question. » Et il conclut : « Est-ce trop cher payer l'intrusion ou pas assez ? »

Maintien du niveau de notre recherche

Un laboratoire qui ne sait pas surveiller ses systèmes d'information risque de se voir voler ses résultats de recherche. Il en résulte une perte de compétitivité sur le plan international. Il y perdra son crédit auprès de ses partenaires, tant scientifiques qu'industriels. Les problèmes de sécurité, s'ils se répètent trop souvent, entraîneront une « perte d'image » qui aura inévitablement des incidences sur les collaborations et les contrats de recherche, et donc sur ses moyens de financement.

Protection de notre patrimoine scientifique

Le patrimoine scientifique est l'ensemble de nos moyens, de nos savoir-faire et de nos résultats de recherche. L'opportunité de leur transfert à l'étranger est appréciée par les autorités gouvernementales en fonction de nos intérêts fondamentaux. L'information scientifique à protéger est celle dont la diffusion incontrôlée pourrait compromettre :
– la liberté et la sécurité de nos concitoyens,
– la prospérité de notre économie,
– le respect de l'éthique scientifique,
– la protection de la vie privée.

Le monde d'aujourd'hui – comme celui d'hier – n'a rien d'angélique, il est composé d'intérêts contradictoires s'opposant parfois avec force. Nous ne sommes pas neutres dans cette compétition, tant comme citoyens (pouvons-nous être indifférents aux enjeux ci-dessus ?) que comme chercheurs (que serait notre recherche dans une économie en faillite ou sous dépendance ?). Nous ne travaillons pas seulement à augmenter la quantité d'articles publiés dans le monde, nous avons aussi un rôle social à jouer.

La sécurité, mais contre quoi ?

Parler de sécurité n'a aucun sens si on ne sait pas définir le danger dont on veut se protéger. Dans les ouvrages traitant de l'art de la guerre, une place privilégiée est toujours réservée à la connaissance de l'ennemi, de ses moyens, de ses tactiques et de ses habitudes. Les nouveaux pirates ne sont plus les quelques illuminés d'antan, rodés au développement en « langage C ». Ce sont de plus en plus souvent des collectionneurs de boîtes à outils, récoltées sur le réseau,

..... suite page 5 ...►

Qu'est-ce que la SSI ?

La sécurité des systèmes d'information, c'est la protection de l'information, des systèmes et des services contre les sinistres, les erreurs et les malveillances, de façon à diminuer leur probabilité et la gravité de leurs conséquences. Reste à définir ce qu'est une « information », un « système d'information » et l'action de « protéger » ?

Qu'est-ce que l'information ?

- C'est ce qu'on transmet (les messages).
- C'est ce qu'on stocke (les données).
- C'est ce qu'on traite (les connaissances).

Qu'est-ce qu'un système d'information ?

Un système d'information est « tout moyen destiné à élaborer, traiter, stocker, acheminer, présenter ou détruire l'information ». Il est maintenant habituel de confondre les notions de « systèmes et réseaux informatiques » et celle de « systèmes d'information ». On dit 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 » (IGI n°900/SGDN).

Qu'est-ce que la sécurité ?

Le concept de sécurité des systèmes d'information recouvre l'ensemble des méthodes, techniques et outils, chargés de protéger les ressources d'un système d'information. On le définit au moyen de ce qu'on appelle « les services de sécurité ». On entend par service de sécurité « tous les aspects relatifs à la définition, à la réalisation, et au maintien de la confidentialité, de l'intégrité, de la disponibilité de l'imputabilité et de l'authentification » (source : ISO TR 13335-1).

Référence ISO TR 13335-1

- *Confidentialité :* « propriété qu'une information ne peut être accédée ou divulguée par des personnes, entités ou processus non autorisés ».
- *Intégrité des données :* « propriété qui garantit qu'une donnée ne peut être altérée ou détruite d'une façon non autorisée ».
- *Intégrité des systèmes :* « propriété qui garantit qu'il sera exécuté la fonction attendue de façon complète sans manipulation non autorisée volontaire ou accidentelle ».
- *Authentification :* ce service permet de s'assurer de l'origine d'un message.
- *Non-répudiation* (ou imputabilité) : ce service assure la preuve de l'authenticité d'un acte, d'une communication ou d'une transaction.
- *Disponibilité :* ce service permet d'assurer l'accessibilité des informations.

suite de la page 4

Vulnérabilités

Les vulnérabilités du système d'information sont des défauts de la qualité et de l'efficacité du processus de production, c'est pourquoi on dit souvent que la SSI s'intègre à une démarche qualité. À l'origine de ces vulnérabilités, on constate le plus souvent :
– une faible sensibilisation du personnel ;
– une absence de méthodologie de sécurité ;
– une faiblesse des structures de sécurité ;
– une absence de plan de secours (ou, s'il y en a, il n'a jamais été testé) ;
– une formation insuffisante des utilisateurs : « les utilisateurs savent… » ;
– une méconnaissance de la réglementation.

Ce sont des problèmes de management et d'organisation !

Les méthodes les plus utilisées pour nous attaquer sont d'une grande banalité :
– logiciels d'écoute des mots de passe sur les réseaux, souvent sur des sites externes au CNRS ;
– mauvaise gestion des comptes utilisateurs : mots de passe triviaux, comptes restés ouverts après le départ de la personne du laboratoire ;
– mauvaise configuration du système ou accès réseaux non contrôlés ;
– utilisation de trous de sécurité connus sur les systèmes : les correctifs n'ont pas été installés.

Ce type d'attaque distingue clairement la petite délinquance.

à la recherche d'excitations nouvelles, des organisations mafieuses, des groupes politiques extrémistes, des agences gouvernementales étrangères, voire un simple agent estimant qu'un serveur « planté » est un bon moyen de régler des comptes avec ses collègues.

L'Internet s'est largement ouvert sur le vaste monde depuis quelques années, offrant aux délinquants des opportunités et un champ nouveau d'activité. Des bandes s'organisent pour écumer ces « grands chemins » modernes mal protégés qu'on appelle « routes de l'information ». Différentes affaires dont nous avons été victimes ces dernières années nous ont permis de dresser une typologie de cette délinquance. Il ressort essentiellement trois catégories :

Le piratage juvénile

Il constitue un groupe responsable de plus de 80 % des incidents de sécurité repérés dans nos laboratoires. Parfois on distingue parmi ces pirates les plaisantins, les ludiques, les vandales, les politiques, etc. Mais ces subdivisions paraissent arbitraires dans la mesure où les pirates sont d'abord des opportunistes : c'est « l'occasion qui fait le larron ». Cette délinquance est le fait de « débutants », « jeunes » (tout au moins en âge mental) ; qui se présentent comme animés par un idéal libertaire ; ils rêvent d'exploits ; ils voudraient être admirés. Mais en réalité, ils sont peu expérimentés et utilisent des recettes toutes prêtes. Ils surestiment généralement leurs capacités et commettent des erreurs grossières ; ils font parfois beaucoup de dégâts sans toujours le vouloir. Ils sont facilement manipulables, et souvent manipulés par ceux des deux autres groupes, mais ce sont eux qui se font prendre.

Le piratage économique

Cette deuxième catégorie est composée de mercenaires dont la seule motivation est l'argent : ils se vendent au plus offrant. De véritables bandes mafieuses s'organisent, constituant des filières où il est possible de « passer un contrat » pour détruire un site informatique qui déplaît, empêcher un marché de se réaliser, faire une « veille technique » sur l'activité d'un concurrent, établir des « organigrammes » détaillés d'entreprises « adverses », etc. Ce sont des prédateurs absolus : le réseau est leur territoire de chasse, les sites informatiques leurs gibiers.

Les organes étatiques

Dans cette dernière catégorie, nous avons affaire à des « pros » de la guerre économique. Depuis la fin de la guerre froide, le recyclage des différents « services d'information et de documentation » vers des activités de « guerre économique » constitue une préoccupation majeure des responsables de la sécurité des systèmes d'information. Cette préoccupation est d'autant plus forte que ces organisations, dans le cas de certains pays, possèdent à la fois des compétences de premier ordre et des moyens quasiment illimités.

Conclusion

La sécurité est partie intégrante du processus de production : c'est une dimension essentielle de la qualité de notre recherche.

R. L.

Menaces

Une menace est un danger qui existe dans l'environnement d'un système indépendamment de celui-ci. Il y a d'abord la délinquance sous les formes que nous connaissons. Pour elle, toute occasion (une vulnérabilité) est bonne à saisir pour lancer une attaque. C'est la préoccupation permanente de la SSI, mais cet aspect du problème ne doit pas nous cacher que d'autres menaces pèsent aussi sur nos systèmes d'information : accidents, pannes, erreurs humaines (dont les plus fréquentes sont les erreurs de conception), catastrophes naturelles ont parfois des conséquences dramatiques. Elles doivent être appréhendées dans le cadre d'une vision globale de la sécurité et le plus tôt possible dans la phase de conception, à la fois sous l'angle de leur prévention (sécurité incendie, plan de sauvegarde, organisation, …) et sous celui de leur traitement (essentiellement sous la forme de plan de secours).

Malveillances

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.

Le risque

Le risque est la probabilité qu'une menace particulière puisse exploiter une vulnérabilité donnée du système. Traiter le risque, c'est prendre en compte les menaces et les vulnérabilités.

La sécurité des systèmes d'information au CNRS

La complexité des systèmes d'information des entreprises s'accroissant sans cesse, s'est accrue aussi leur fragilité. Parallèlement, la délinquance informatique a été favorisée par l'ouverture des réseaux, la diminution des coûts des matériels, la facilité de connexion, la diffusion à large échelle d'outils de piratage. Elle atteint maintenant un niveau qui pose un réel défi à tous les États, à toutes les organisations, à toutes les entreprises.

Notre organisme de recherche ne fait pas exception. La sécurité des systèmes d'information est devenue un enjeu majeur pour nous comme pour l'économie tout entière. Sur ce nouvel échiquier – développement de la délinquance –, les administrateurs systèmes et tous les acteurs de la sécurité semblent quelque peu dépassés : hétérogénéité des systèmes, ouverture et connexion entre les réseaux et l'extérieur, multiplication des applications, des versions, des correctifs et des « services packs » ... Ils doivent s'imprégner des connaissances des pirates et soumettre mentalement les réseaux qu'ils doivent défendre à leurs principaux scénarios d'attaque. Ils doivent assimiler le fonctionnement des principaux systèmes de défense : garde-barrière, relais applicatifs, systèmes d'authentification et chiffrement. Une technique est à peine assimilée qu'il faut passer à la suivante ... Il faut changer d'approche ! Qui ne voit que le maillon le plus faible est le plus souvent les acteurs du système eux-mêmes ? Nombreux à intervenir dans les systèmes d'information, ils contribuent à la force ou à la faiblesse de l'ensemble. Il est clair que l'aspect humain et organisationnel prime le technique.

Le CNRS, c'est 1 300 unités de recherche fédérées par « une système administratif et de gestion » : le siège central, la DSI et les délégations régionales. Dans chaque laboratoire les systèmes informatiques sont interconnectés en réseaux locaux administrés souvent indépendamment. Ces réseaux sont connectés par RENATER aux réseaux d'autres unités de recherche (CNRS, universitaires et autres EPST) dont on ignore généralement le niveau de sécurité. L'ensemble est ouvert par l'Internet au monde entier.

Pour terminer ce tableau, il faut ajouter que la SSI s'appréhende différemment suivant le laboratoire : d'un grand laboratoire possédant des moyens financiers et humains importants, une culture et un savoir-faire en système et réseau, à une petite unité de recherche qui a constitué son informatique par accumulations successives, sans plan, sans connaissance préalable et sans personnel technique associé, en passant par les différentes unités dans leurs diversités, le panorama est vaste et le tout présente une grande variété de structures et de cultures qui se côtoient.

Des difficultés spécifiques

- Comment définir le « périmètre de sécurité » quand l'imbrication de divers organismes de recherche, de diverses structures et de divers pôles de responsabilité ou de compétence a atteint une telle complexité ?
- Comment intégrer la notion de « protection du patrimoine » dans chaque projet sans appauvrir la créativité de la recherche ?
- Comment la sécurité peut-elle être l'affaire de tous lorsqu'une proportion importante du personnel est « temporaire » (stagiaires, étudiants, visiteurs, ...) ?
- Comment faire en sorte que les individus œuvrent ensemble à l'amélioration de la sécurité alors que chacun peut légitimement mettre en avant la spécificité de sa recherche ?

Éléments d'évaluation de notre niveau de sécurité

La sécurité est pareille à toute chose, elle n'a de réalité scientifique que si l'on est capable de l'évaluer. On peut toujours penser qu'un laboratoire est « sécurisé » parce qu'il a suivi telle recommandation ou telle idée à la mode. Mais tant qu'on en reste là, ce n'est qu'une impression personnelle et rien d'autre. Nous avons besoin d'indicateurs (une métrique) qui nous renseignent d'une manière objective sur notre niveau réel de sécurité et sur son évolution. À l'échelle de notre organisme, l'essentiel sur ce point reste à faire : les seules données dont nous disposions sont établies grâce à des extrapolations de statistiques obtenues dans des organismes comparables au nôtre. Ces estimations sont les suivantes (dans une version optimiste) :

– un millier d'attaques par semaine,
– 90 % des attaques réussissent à pénétrer le réseau,
– 4 % des attaques sont détectées,
– à peine la moitié des attaques détectées sont remontées au niveau de l'organisme.

On a tout lieu de penser que ces chiffres, même tirés d'extrapolations, sont proches de la réalité. Ils amènent deux commentaires :

– une attaque qui a réussi à contourner les défenses du laboratoire a toutes les chances de rester non détectée ;
– les laboratoires craignent trop souvent d'en référer aux instances supérieures, comme s'ils se sentaient coupables d'avoir été agressés. Pourtant cela arrive même aux meilleurs. En revanche, s'en apercevoir est la marque d'un vrai professionnalisme. Le faire savoir, c'est permettre à la communauté scientifique de profiter de son expérience.

Conclusion

Il devient urgent d'enseigner la sécurité dans notre organisme, non pas comme des incantations ou des recettes, mais comme une méthodologie qui intègre la mesure de la sécurité. Des indicateurs doivent pouvoir permettre à nos organes de direction de mieux mesurer notre niveau de sécurité, et donc d'apprécier les coûts qu'elle génère tant à l'échelle de notre organisme qu'à celle de la nation elle-même.

R. L.

LES VIRUS ATTAQUENT :
• Plus de 50 000 virus connus en août 2000.
• 800 nouveaux virus analysés chaque mois,
– dont environ 60 à l 'état actif.
• 1 à 5 alertes de nouveaux virus actifs par jour…

La tendance est à l'accélération. Aussi faut-il mettre à jour aon antivirus quotidiennement

SÉCURITÉ INFORMATIQUE
numéro 33 février 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
La reproduction totale ou partielle des articles est autorisée sous réserve de mention d'origine

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