Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

Menaces sur les systèmes informatiques

GUIDE N° 650

Version du 12 septembre 2006

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 41 46 37 20 - Fax 01 41 46 37 01

Ce document a été réalisé par le bureau conseil de la DCSSI
(SGDN / DCSSI / SDO / BCS)

Les commentaires et suggestions sont encouragés et peuvent être adressés à l'adresse suivante :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau Conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP

conseil.dcssi@sgdn.pm.gouv.fr

Historique des modifications

Date	Objet de la modification	Auteur(s)	Statut
28/03/1994	Publication du guide N°650/DISSI/SCSSI "La menace et les attaques informatiques"	SCSSI	Validé
12/09/2006	Mise à jour du document suite au marché N°2002 001 29 00 215 075 01 "Fourniture d'une étude relative au développement de bases de connaissances de la sécurité des systèmes d'information" : - actualisation du texte (mise en cohérence avec les nouveaux éléments de langage, nouvelles références…), - mise en cohérence avec la structuration de la menace au sens ISO 15408, - mise en cohérence avec les bases de connaissances de la méthode EBIOS. Intégration des remarques des relecteurs	SGDN	Validé

Sommaire

1 Introduction

Les systèmes d'information (SI) reposent en partie sur des machines qui stockent, traitent et transmettent de l'information. Ces machines peuvent être, pour les plus sophistiquées, des ordinateurs mais aussi des périphériques informatiques, des téléphones, des télécopieurs, des télex… Elles sont majoritairement reliées par des réseaux locaux à l'intérieur de leur organisme d'appartenance, mais, dans de nombreux cas, elles permettent de communiquer avec l'extérieur. Certains SI offrent des services, parfois vitaux ou essentiels, sur lesquels repose l'économie des États et des entreprises. Ainsi de multiples informations, hier confinées, sont devenues accessibles de presque n'importe quel point du globe alors même que la dépendance vis-à-vis des services fragilise aussi bien leurs fournisseurs que leurs utilisateurs.

Les informations constituent une ressource stratégique, une matière première, elles sont un atout supplémentaire pour ceux qui les possèdent. La protection de ce patrimoine contre les malveillances doit par conséquent être un souci permanent d'organisation

1.1 Le périmètre : les menaces humaines intentionnelles sur les systèmes informatiques

Afin de décrire et d'illustrer de manière aussi complète que possible les notions associées aux menaces sur les systèmes informatiques, **le périmètre du présent document a été volontairement limité à la description des menaces sur les systèmes informatiques (matériels, logiciels, réseaux…) dont la cause est délibérée et le type est humain, interne au SI, ou environnemental (humain externe au SI)**.

1.2 La problématique : des menaces permanentes et multiformes

Les SI gèrent des informations qui peuvent être convoitées par des individus dont le spectre s'étale du simple potache qui cherche à occuper son temps, jusqu'au professionnel chevronné du renseignement en passant par le criminel de droit commun, isolé ou dans une organisation. En proposant de nouveaux services et en traitant toutes sortes d'informations les SI constituent de nouvelles cibles qui ne sont pas toujours l'objet d'attentions adéquates de la part de leurs propriétaires, qui vont parfois jusqu'à sous-estimer ou ignorer l'importance de leur capital.

La concentration des données et leur disponibilité sur un réseau permettent d'obtenir rapidement, dans la discrétion et parfois dans l'anonymat le plus complet, une grande quantité d'informations qu'il était auparavant difficile de se procurer. Pour leur part, les services offerts, facilitent les échanges entre les acteurs économiques et permettent de traiter des problèmes de façon plus efficace et plus sûre.

[Neumann & Parker 1989] proposent trois raisons qui permettent d'expliquer que les menaces qui pèsent sur les SI sont permanentes et ne peuvent descendre en dessous d'un seuil incompressible :

- il existe un fossé technologique entre ce qu'un système d'information est capable de faire et ce que l'on attend de lui,

- la loi, la réglementation et l'éthique ne sont pas toujours en cohérence avec la technique. Ceci vaut pour de nombreux domaines en dehors du traitement de l'information,

- les individus se comportent rarement comme on l'attend : un utilisateur jugé intègre par ses pairs peut dans certaines circonstances abuser de ses droits. Le comportement d'un individu confronté à des situations inhabituelles et critiques est imprévisible.

1.3 Origines et conséquences : des menaces aux risques

Une menace doit être décrite en citant le bien qui en est la cible, l'élément menaçant identifié et l'attaque. Les éléments menaçants devraient être caractérisés par des aspects tels que la motivation les ressources disponibles et l'expertise. Les attaques devraient être caractérisées par des aspects tels que l'opportunité, les méthodes d'attaque et toutes les vulnérabilités exploitées [ISO 15408].

Les éléments menaçants qui pèsent sur les SI sont de cause accidentelle ou délibérée et de nature interne ou externe. Au-delà de cette évidence, force est de constater l'évolution de la nature interne des éléments menaçants, longtemps considérée comme principale (70 à 80% des cas connus, ce phénomène s'expliquant par l'émergence de conduites déviantes, c'est-à-dire contraire aux intérêts d'une organisation, mais aussi par manque d'information, de sensibilisation, de formation. Il laisserait aujourd'hui une place prépondérante aux menaces de nature externe [CIGREF]. Cette tendance repose principalement sur la prolifération des attaques de type code malveillant tels que les virus informatiques propagés par messagerie électronique, et des attaques conduites par des individus qui n'ont pas un accès légitime au SI et qui essayent de briser les barrières de sécurité lorsqu'elles existent.

Bien que supplantées par les attaques utilisant l'Internet comme média, les menaces de nature interne représentent toujours une part significative. Quand ce type de menaces se matérialise par des attaques ou des fraudes, l'utilisateur agressif, qui possède déjà un accès légitime au SI et aux services qu'il offre, tente d'obtenir ou de falsifier des informations, de perturber le fonctionnement du SI, en abusant de ses privilèges ou en les augmentant.

Que les menaces soient internes ou externes, les informations et les services fournis par le SI peuvent subir des préjudices qui se traduiront par des pertes de disponibilité, d'intégrité ou de confidentialité [EBIOS]. Il peut en résulter une destruction, une modification ou une divulgation non autorisée des données ou encore une impossibilité d'obtenir une information ou un service. Par ailleurs, les effets induits et souvent non directement mesurables peuvent s'avérer catastrophiques pour l'entreprise ou l'organisme victime : atteinte à l'image de marque ou suppression d'emplois si le sinistre touche l'outil de production, l'outil de vente ou le produit vendu dans le cas d'un service par exemple.

1.4 Présentation du guide

Ce guide propose une description concrète de chaque composante de la menace intentionnelle sur l'informatique :

- les biens (chapitre 2),
- les éléments menaçants (chapitre 3),
- les attaques (chapitre 4).

2 Les biens : les éléments essentiels et les entités

Dans un SI, toutes les informations et tous les composants n'ont pas la même valeur. Celles et ceux qu'il est important de protéger parce qu'ils représentent un certain capital ou sont indispensables au bon fonctionnement d'un système ou d'un processus sont généralement désignés par le terme de biens (élément essentiel ou entité).

2.1 Les éléments essentiels : le patrimoine informationnel, porteur de besoins de sécurité

Les éléments essentiels sont les éléments à protéger par l'organisme. Ce sont eux pour lesquels l'organisme doit exprimer des **besoins de sécurité en terme de disponibilité, d'intégrité, de confidentialité…** Ils représentent le patrimoine immatériel et intellectuel, composé de toutes les informations et fonctions. Ils concourent à assurer les missions de l'organisme (données ou processus scientifiques, techniques, professionnelles, administratives…) dans le respect des lois, règlements et des codes d'éthique et de déontologie.

S'agissant de confidentialité, ces éléments essentiels à protéger peuvent relever d'une classification de défense ou non, tels que les éléments concernant :

- des informations nominatives (contractuelles, privées…),
- des informations administratives et financières,
- des informations professionnelles et / ou techniques (savoir-faire, recherche, projet métier),
- des informations commerciales,
- des informations scientifiques.

Dans le cas des menaces spécifiques d'espionnage[1], elle concerne particulièrement les informations stratégiques d'une nation, d'un organisme ou d'une entreprise. Les renseignements d'ordre militaire, diplomatique, mais aussi, économiques, industriels, technologiques, scientifiques, financiers et commerciaux seront recherchés en priorité.

2.2 Les entités : les composants du système d'information, porteurs de vulnérabilités

Le système d'information de l'organisme peut être présenté comme un ensemble d'entités sur lesquelles reposent des éléments essentiels (fonctions et informations) et sur lesquelles peuvent porter des menaces. Ici, nous ne considérerons que les menaces de cause délibérée (malveillante).

La typologie proposée dans la méthode [EBIOS] identifie six grands types d'entités :

- les logiciels,
- les matériels,
- les réseaux,
- les sites,
- les organisations,
- les personnels.

Cette typologie permet notamment de distinguer le cadre organisationnel, l'environnement physique et humain dans lequel le SI est exploité et le système informatique.

Ainsi, par exemple, on distinguera :

- l'organisation du siège de l'organisme,
- son personnel,
- ses sous-traitants,
- son bâtiment, sa salle informatique et ses bureaux,
- ses réseaux d'énergie et de télécommunications,
- ses serveurs, postes de travail et supports de sauvegarde,
- son réseau informatique interne et ses accès Internet,
- son parc applicatif…

Dans notre périmètre, ce sont **essentiellement les logiciels, les matériels et les réseaux** qui sont concernés, et ce sont eux qui possèdent des vulnérabilités exploitables dans le cadre des attaques.

[1] Recherche systématique et très professionnalisées d'informations par tous moyens légaux ou non ciblant préférentiellement des informations protégées.

3 Les éléments menaçants : une typologie des attaquants

Les éléments menaçants se caractérisent par leur type et par leur cause.

Les aspects des menaces évoqués dans ce chapitre ne peuvent pas constituer une classification exhaustive, mais une description des aspects les plus courants. Les menaces ne sont pas liées à un seul facteur ; elles sont souvent composites comme l'illustre le cas tristement célèbre du Chaos Computer Club où certains agresseurs de SI (« pirates ») ont mis leurs talents au service d'organismes de renseignement avec des motivations à la fois ludiques et purement lucratives.

3.1 Les types : humain (interne) et environnemental (externe)

[EBIOS] et l'[ISO 15408] expliquent que les éléments menaçants peuvent être regroupés selon leur type, qui peut être :

- naturel,
- humain,
- environnemental (dans le sens : externe au SI).

Le périmètre de ce guide ne concerne que les éléments menaçants :

- **de type humain (personnes faisant partie du SI considéré),**
- **de type environnemental (personnes extérieures au SI).**

à l'exclusion des évènements naturels.

Les paragraphes qui suivent proposent une typologie de profils d'attaquants.

L'avidité et l'appât du gain sont les motifs principaux des actes des attaquants, mais il apparaît que les problèmes personnels ainsi que l'ego jouent un rôle primordial en influant sur les comportements socioprofessionnels.

Cependant, comme le présente le rapport du CIGREF [CIGREF], l'espionnage étatique ou industriel a une influence trop souvent sous estimée par les responsables des organismes.

Un élément également important concerne l'évolution du niveau de compétence des attaquants. En effet, comme le montre les rapports [CERT-CC], bien que la sophistication des attaques Internet augmente, la compétence technique des attaquants diminue. Une échelle de compétence est proposée au chapitre relatif à l'expertise.

Agresseurs
Nous proposons les deux profils d'agresseurs les plus souvent identifiés :

- ***hacker*** ou passionné : individu curieux, qui cherche à se faire plaisir. Pirate par jeu ou par défi, il ne nuit pas intentionnellement et possède souvent un code d'honneur et de conduite. En général il n'a pas conscience de la mesure de ses actes.
  Comme mentionné plus haut dans le rapport [CERT-CC], l'agresseur passionné est de moins en moins expérimenté.

- ***cracker*** ou casseur : plus dangereux que le *hacker*, cherche à nuire et montrer qu'il est le plus fort. Souvent mal dans sa peau et dans son environnement, il peut causer de nombreux dégâts en cherchant à se venger d'une société - ou d'individus - qui l'a rejeté ou qu'il déteste. Il veut prouver sa supériorité et fait partie de clubs où il peut échanger des informations avec ses semblables.

Fraudeurs
Le fraudeur bénéficiant souvent d'une complicité, volontaire ou non, chez ses victimes, il cherche à gagner de l'argent par tous les moyens. Son profil est proche de celui du malfaiteur traditionnel. Parfois lié au grand banditisme organisé ou non, il peut attaquer une banque, falsifier des cartes de crédit ou se placer sur des réseaux de transferts de fonds et, si c'est un particulier, il peut vouloir falsifier sa facture d'électricité ou de téléphone.

Employés malveillants
Le fraudeur interne : possédant de bonnes compétences sur le plan technique, il est souvent informaticien et sans antécédents judiciaires. Il peut penser que ses qualités ne sont pas reconnues, qu'il n'est pas apprécié à sa juste valeur. Il veut se venger de son employeur et chercher à lui nuire en lui faisant perdre de l'argent. Il peut répondre à un besoin matériel personnel qui induit des conduites de dépendances (jeux, sexe…). Pour parvenir à ses fins, il possède les moyens, qu'il connaît parfaitement, et qui ont été mis à sa disposition par son entreprise.

Militants
Motivés par une idéologie ou la religion, ils disposent de compétences techniques très variables. Leurs objectifs peuvent être limités à la diffusion massive de messages, comme ils peuvent s'étendre à des nuisances effectives sur les systèmes d'information des organismes en opposition avec leur idéologie.

Espions
Ils participent à la guerre économique. Ils travaillent pour un État ou pour un concurrent.
Ils sont patients et motivés. Ils savent garder le secret de leur réussite pour ne pas éveiller les soupçons et continuer leur travail dans l'ombre.
Ils agissent souvent depuis l'intérieur de l'organisme, soit en ayant trouvé un moyen d'y pénétrer, soit en soudoyant une personne ayant accès aux biens.
Ils ont pour but de voler des informations ou de détruire des données stratégiques (vitales) pour l'organisme.
Dans tous les cas, les espions ont un excellent niveau de maîtrise de soi, ainsi qu'une grande capacité d'adaptation aux environnements.

Terroristes
Souvent appelés les cyber-terroristes, moins courants, les terroristes sont aidés dans leur tâche par l'interconnexion et l'ouverture croissante des réseaux : très motivés, ils veulent faire peur et faire parler d'eux. Les actions se veulent spectaculaires, influentes, destructrices, meurtrières. Ce profil est pris de plus en plus au sérieux par les États depuis l'attentat du 11 septembre 2001. Ils considèrent qu'une cyber-attaque perpétrée par un terroriste pourrait gravement nuire aux infrastructures économiques et critiques d'un État devenu très dépendant de ses systèmes d'informations vitaux.

3.2 La cause : délibérée, avec des motivations, ressources et expertises variées

La cause d'un élément menaçant peut être :
- accidentelle (avec une exposition et des ressources disponibles données),
- délibérée (avec une motivation, des ressources disponibles et une expertise données).

Le périmètre de ce guide ne concerne que les éléments menaçants de **cause délibérée**.

3.2.1 Motivation d'un attaquant : du caractère ludique au stratégique

Parvenir à distinguer la motivation d'un attaquant, ainsi que son niveau de technicité (expertise), permet de déterminer son potentiel d'attaque et ainsi de mieux la contrer.

Les motifs de l'agresseur sont nombreux et variés ; ils évoluent dans le temps. Il n'est pas possible de dresser une liste exhaustive des motivations des criminels mais quelques exemples permettront de saisir la personnalité de quelques-uns uns d'entre eux. Les actes intentionnels, qui nous intéressent ici, comprennent : l'espionnage, l'appât du gain, la fraude, le vol, le piratage, le défi intellectuel, la vengeance, le chantage, l'extorsion de fonds.

De la même façon, peuvent être observés des comportements déviants dus à certaines pulsions incontrôlées ayant pour origine des états psychologiques douloureux non traités (frustration, sentiment d'exclusion, sentiment d'abandon, situation de divorce, dépendances à des drogues…).

L'exhaustivité ne peut être atteinte en raison également de l'évolution temporelle des composantes de la menace. Pour un système gouvernemental par exemple la menace change selon que l'on est en temps de paix, de crise ou de guerre. Les effets de mode peuvent aussi influer momentanément sur la prédominance d'une menace par rapport à une autre. Ajoutons que la menace est généralement composite ce qui rend plus difficile sa détermination pour le défenseur.

Les origines que nous proposons sont celles de la Fiche d'Expression Rationnelle des Objectifs de Sécurité [FEROS] que nous avons complété avec de nouveaux éléments. Nous présentons ainsi la motivation stratégique, idéologique, terroriste, cupide, ludique ou vengeur de la menace.

Étant hors du périmètre de ce document, cette liste devrait être complétée par celles des actes non intentionnels mais qui constituent une menace pour le SI : la négligence, la curiosité, l'ennui, la paresse, l'ignorance, l'incompétence, l'inattention...

Ajoutons que la menace a généralement des motivations plurifactorielles (par exemple à la fois pathologique, ludique et économique), ce qui rend plus complexe son repérage, son analyse et son traitement par le défenseur.

Caractère stratégique
Pour un État, la menace stratégique s'intéresse par essence à toutes les informations concernant le secret de Défense et la Sûreté de l'État, mais également à celles appartenant au patrimoine national, qu'il soit d'ordre scientifique, technique, industriel, économique ou diplomatique ; la menace stratégique, peut également attenter à la disponibilité de systèmes d'information, dont le fonctionnement continu est nécessaire au fonctionnement normal des institutions.

Pour une entreprise ou une société, la menace d'origine stratégique aura pour but d'obtenir toute information sur les objectifs et le fonctionnement de celle-ci, pour récupérer des clients prospectés, des procédés de fabrication, des résultats de recherche et de développement et de porter atteinte à sa capacité de réaction. Elle sera principalement le fait de concurrents.

Caractère idéologique
Les motivations idéologiques peuvent être les moteurs d'actes les plus extrêmes. Le combat pour les idées est incessant.
D'autres idéologies, raciales ou religieuses, resurgissent à la faveur d'une situation économique tendue. Cette menace peut s'appliquer aux nombreux fichiers informatiques constitués dans le monde et comportant des informations à caractère privé sur les individus.
Enfin, il existe des courants de pensée qui mettent en avant le fait que l'information doit être libre et ne peut en aucun cas être la propriété d'une personne, d'un groupe, d'une organisation ou d'un État. Cette vision du monde est partagée par de nombreux pirates.

Caractère politique
La motivation politique consiste à créer un événement propre à alerter les médias pour les focaliser sur un évènement grave, en espérant provoquer une prise de conscience collective. Elle peut être proche du terrorisme.

Caractère terroriste
On définira la menace terroriste comme regroupant toutes les actions concourant à déstabiliser l'ordre établi ; les actions entrant dans cette catégorie peuvent avoir un caractère violent (destruction physique de systèmes) ou plus insidieux (intoxication et désinformation par détournement ou manipulation d'informations, sensibles ou non, perturbations engendrées dans un système et susceptibles de déclencher des troubles sociaux présents à l'état latent…).

Mais leurs auteurs recherchent en général un résultat spectaculaire et les effets médiatiques qui l'accompagnent. Ce mode d'action relève de la manipulation et peut être l'une des expressions de la guerre psychologique.
Les groupes, susceptibles de commettre ce genre de forfaits, disposent généralement de moyens financiers importants et de complicités au niveau international, leur permettant d'envisager pratiquement tous types d'attaque sur un système. Cette menace peut aussi être fomentée par un État qui veut mener une action de déstabilisation.

Caractère cupide
Cette nouvelle forme de délinquance, engendrée par l'apparition des procédés de traitement de l'information, et parfois dite en col blanc, peut avoir deux différents buts, parfois concomitants :

- le premier se traduit par un gain pour l'attaquant ; ce gain peut être financier (détournement de fonds), lié à un savoir-faire (vol de brevet, concurrence déloyale...), ou de tout autre ordre ;

- le second occasionne une perte pour la victime qui se traduira par un gain pour l'agresseur (parts de marché, accès au fichier des clients, à des propositions commerciales...) ; ce peut être la destruction de son système ou de ses informations, une perte de crédibilité ou de prestige (image de marque) vis-à-vis d'une tierce personne, etc.

Il est difficile de caractériser, même succinctement, le profil type du fraudeur, tant les applications susceptibles d'être attaquées sont multiples. Néanmoins, les statistiques à ce sujet permettent de souligner que dans un grand nombre de cas, la menace a été initiée et mise en oeuvre à l'intérieur même de l'organisme abritant le système et a été le fait d'employés, dont les antécédents ne permettaient pas de supposer qu'ils commettraient un forfait de ce type. Les victimes figurent en général parmi les organismes qui détiennent l'argent : banques, compagnies d'assurances, etc.

Pour sa part, le concurrent déloyal est plus facile à identifier : il figure parmi les concurrents, pour peu qu'ils soient parfaitement identifiés.

Nous ajouterons dans cette catégorie le crime organisé qui pourrait prendre de l'importance dans un futur proche s'il s'avère qu'il est plus facile - moins coûteux et moins risqué – de détourner les fonds de manière électronique qu'en pillant une banque.

Caractère ludique
Les nouvelles techniques de traitement de l'information (micro-ordinateurs, modem, minitel...) ont créé cette menace, qui procède d'avantage, dans l'esprit de ceux qui en sont les auteurs, d'un jeu ou d'un loisir que d'un réel forfait (intrusion dans des systèmes, développement de virus ou de vers informatiques...). Animés d'un désir de s'amuser ou bien d'apprendre, ces auteurs possèdent généralement de bonnes connaissances techniques.

Motivés par la recherche d'une prouesse technique valorisante destinée à démontrer la fragilité du système plutôt que par souci de nuire, ils sont recrutés parmi les personnes soucieuses de s'affirmer, et ses victimes dans les organismes à forte notoriété sur le plan technique ou réputés inviolables.

Caractère vengeur
La vengeance peut être la motivation de l'employé brimé, qui sent ses capacités peu ou mal utilisées, qui vient d'être licencié ou qui sait qu'il va être. Il faut alors craindre des actes destructeurs et souvent non corrélés avec leurs causes dans le temps.

Les résultats consécutifs à une vengeance se verront ou se comprendront parfois bien après qu'ils aient été initiés**.**

3.2.2 Ressources disponibles : des moyens modestes à très importants

La connaissance de l'origine de la menace est l'un des éléments qui va permettre au défenseur d'évaluer la force et les moyens de son agresseur potentiel. En comprenant les motivations de ce dernier, le défenseur pourra adapter sa politique de sécurité et anticiper les actes malveillants. Un SI sera d'autant plus menacé que les informations qu'il possédera auront une valeur et pour leur propriétaire et pour d'autres entités. Il ne faut pas pour autant conclure qu'un SI ne gérant pas d'information de valeur n'est sujet à aucune menace : son rôle peut être primordial pour assurer un service.
Les ressources requises vont de pair avec les compétences et dépendent des techniques utilisées. Un attaquant voulant s'emparer d'informations chiffrées disposera d'importants moyens de calcul, ou de complicités internes, pour ensuite briser l'algorithme de chiffrement.

Attaque "standard"
L'attaquant "standard" possédera probablement un ou des ordinateurs modestes associés à une connexion Internet, et puisera sa connaissance dans la documentation technique et la littérature ouverte. Il se procurera les logiciels nécessaires à l'accomplissement de ses méfaits sur des serveurs publics ou les développera lui-même.
L'utilisation de moyens relais est de plus en plus courante soit pour leur assurer l'anonymat, soit pour lancer de manière simultanée de très nombreuses attaques contre une cible unique.

Ils ont à leur disposition via l'Internet un outillage de plus en plus performant pour exploiter les failles d'implémentation ou d'installation des applications standard accessibles depuis l'internet.

Les moyens qu'ils utilisent pour l'attaque sont complétés par une connaissance du système visé qui leur permet d'augmenter l'efficacité de l'attaque.

Espionnage et terrorisme
Elle est généralement le fait d'organismes gouvernementaux ou para-gouvernementaux structurés et organisés pour la recherche du renseignement et disposant de moyens financiers et techniques très importants leur permettant d'envisager tous types d'attaque sur un système.

Dans le cas d'espionnage industriel, les concurrents utilisent des moyens qui peuvent être proches de ceux d'un État.

S'il est moins fréquent, mais surtout non avoué que des entreprises ou des sociétés aient recours à l'espionnage, cela représente un intérêt pour leur activités en gain de temps et d'investissement. Les techniques restent les mêmes et la différence se fera sur l'ampleur des moyens utilisés. Il est concevable de penser que des États utilisent leurs services de renseignement pour fournir des informations à leurs industriels. Il est aussi de notoriété publique que des sociétés privées offrent leurs services pour obtenir des renseignements.

Néanmoins, certains moyens utilisés restent simples. Ils exploitent la communication entre les employés ou des groupes de discussion auxquels ils participent. L'espion collecte leurs informations et les analyses pour en tirer une quantité importante d'informations supplémentaires, voire même des informations confidentielles.

3.2.3 Expertise : des compétences faibles, moyennes ou fortes

Le succès d'une attaque dépend en partie de la compétence et de l'entraînement de son auteur. Le niveau de l'attaquant varie de l'expert au novice. Les domaines de connaissances seront cependant presque toujours l'informatique en général et en particulier la programmation, les systèmes d'exploitation, les communications mais aussi le matériel (routeurs, commutateurs, ordinateurs...). Selon Neumann et Parker, nous pouvons classer les méfaits en trois niveaux pour la compétence requise :

- compétence technique faible ou nulle pour dénaturer une information, observer, fouiller physiquement, voler, abîmer un équipement, perturber un SI, entrer des données fausses, se mettre de connivence avec un étranger à l'organisation...

- compétence technique moyenne pour balayer un SI et chercher des informations, fouiller logiquement, inférer, faire des agrégats, surveille le trafic ou une activité, écouter, faire fuir de l'information, se faire passer pour quelqu'un d'autre, rejouer une transaction, abuser de ses droits, exploiter une trappe...

- compétence forte pour modifier le système, exploiter un cheval de Troie, fabriquer une bombe logique, un ver ou un virus, réaliser une attaque asynchrone, modifier le matériel, décrypter...

Ces compétences sont souvent présentes dans un organisme et parfois à l'insu des dirigeants qui connaissent mal les capacités de leur personnel. Cette méconnaissance peut aussi expliquer le nombre d'attaques internes, les politiques de sécurité étant inadaptées ou sous-estimant les agresseurs potentiels.

4 Les attaques

Les attaques devraient être caractérisées par les méthodes d'attaque, les vulnérabilités exploitées et l'opportunité [ISO 15408].

4.1 Les méthodes d'attaques : 15 moyens de porter atteinte à la sécurité du SI[2]

Des menaces différentes peuvent avoir les mêmes effets. Nous présentons les types d'attaques génériques retenus dans le périmètre du document [EBIOS], accompagnés de quelques exemples par ailleurs très connus. Remarquons à nouveau qu'il n'est pas toujours besoin d'être un spécialiste de l'informatique pour s'emparer de façon illicite d'informations intéressantes.

Les attaques informatiques délibérées peuvent porter entre autres sur les communications, les machines ou les traitements.

Nous proposons dans ce chapitre une typologie des principales méthodes d'attaques, néanmoins il faut envisager également les scénarios qui consistent à cumuler plusieurs types d'attaque. Deux types d'attaques multiples peuvent être menées :

- les attaques dont la conséquence permet d'obtenir des informations ou des privilèges pour mener un autre type d'attaque ; c'est le cas par exemple de la technique d'attaque par rebond, qui consiste à prendre le contrôle d'une machine du réseau interne de l'organisme visé, de s'approprier ses privilèges pour attaquer d'autres systèmes ;

- les attaques simultanées par collusion ou par coordination sur une cible unique ; dans le premier cas, il s'agit pour l'attaquant d'exploiter les résultats de nombreuses s'attaques menées de manière coordonnée (par exemple, analyse de cryptogrammes) ; dans le deuxième cas, il s'agit de coordonner une attaque utilisant de très nombreux systèmes pour saturer la cible.

4.1.1 Destruction de matériels ou de supports

Sabotage
Plus fort que la perturbation, le sabotage a pour but de mettre hors service un SI ou une de ses composantes.
Le sabotage porte atteinte à l'intégrité des informations mais surtout à la disponibilité des services.

4.1.2 Rayonnements électromagnétiques

Brouillage
Utilisée en télécommunication, cette technique rend le SI inopérant. C'est une attaque de haut niveau, car elle nécessite des moyens importants, qui se détectent facilement. Elle est surtout utilisée par les militaires en temps de crise ou de guerre.

4.1.3 Écoute passive

Écoute
L'écoute consiste à se placer sur un réseau informatique ou de télécommunication et à analyser et à sauvegarder les informations qui transitent. De nombreux appareils du commerce facilitent les analyses et permettent notamment d'interpréter en temps réel les trames qui circulent sur un réseau informatique.
Des protections physiques, pour les réseaux informatiques, ou le chiffrement (COMSEC, INFOSEC), pour tous types de réseau, offrent une protection adéquate pour faire face à ce type d'attaque.

Interception de signaux compromettants
L'attaquant va tenter de récupérer un signal électromagnétique et de l'interpréter pour en déduire des informations compréhensibles. L'interception peut porter sur des signaux hyperfréquences ou

[2] Voir également la note d'information N°CERTA-2006-INF-002 relative à la terminologie d'usage.

hertziens, émis, rayonnés, ou conduits. L'agresseur se mettra ainsi à la recherche des émissions satellites, et radio, mais aussi des signaux parasites émis par les SI, principalement par les terminaux, les câbles et les éléments conducteurs entourant les SI. Les techniques d'interception seront très variées pour les différents cas évoqués.

Pour se protéger, le défenseur pourra sécuriser ses transmissions (TRANSEC) en utilisant des appareils à saut de fréquence et diminuer le nombre et l'intensité des signaux parasites compromettants de ses SI (utilisation de matériels dits TEMPEST). Il devra en outre vérifier ses matériels pour éviter tout piégeage ou altération dans le temps. Pour cela, il lui faut avoir l'assurance que ses matériels sont conformes à ce qu'il en attend et vérifier que les procédures de maintenance ne viennent pas les altérer.

Cryptanalyse
L'attaque d'un chiffre ne peut se faire que lorsqu'on a accès aux cryptogrammes qui peuvent être interceptés lors d'une communication ou qui peuvent être pris sur un support quelconque. Cette attaque nécessite en général d'excellentes connaissances en mathématiques et une forte puissance de calcul, lorsqu'il s'agit d'algorithmes éprouvés. Elle est principalement le fait de services de renseignement.

4.1.4 Vol de supports ou de documents

Le vol, visible quand l'objet du délit est matériel, est difficile à détecter quand il s'agit de données et encore plus de ressources informatiques. En effet une simple copie suffit pour s'approprier une information. Cette opération n'est pas toujours facile à déceler.

Fraude physique
Elle peut consister à récupérer les informations oubliées ou non détruites par l'adversaire ou le concurrent. L'attaquant portera une attention particulière aux listages, aux supports physiques usagés (bandes magnétiques, disquettes, disques classiques ou optiques...), et s'intéressera aux armoires, aux tiroirs et aux dossiers des organismes visés.

Comme l'espionnage, la fraude physique va tenter d'enfreindre les mesures de sécurité qui protègent la confidentialité des informations.

4.1.5 Vol de matériels

Le vol de matériels passe généralement par une infraction aux mesures de sécurité protégeant la confidentialité des informations. Le vol de ressources est plus insidieux, car il se peut qu'il soit réalisé sans porter atteinte à la confidentialité, à l'intégrité ou à la disponibilité des informations et des services.

Vol de micro-ordinateur portable
Le vol des micro-ordinateurs portables est aujourd'hui pratique courante. De plus, l'utilisation croissante de ces micro-ordinateurs portables, souvent attribués à des hauts responsables de l'organisme a pour conséquence que de plus en plus d'informations sensibles se trouvent exposés sur ces machines attractives.
Or, bien que dans la majorité des cas de vol la motivation première ne soit pas l'exploitation du contenu, rien ne permet d'assurer le contraire.

4.1.6 Récupération de supports recyclés ou mis au rebut

Analyse de support mis au rebus
Les organismes sont la victime de deux types de scénarios fréquemment utilisés :

- l'un consiste à effectuer une fouille systématique des poubelles ou plus simplement le vol d'éditions oubliées sur les imprimantes partagées, accessibles dans les locaux "publics" de l'organisme ;

- l'autre exploite une lacune souvent présente dans la procédure de ré-attribution ou d'envoi en maintenance des postes de travail. Il consiste simplement à analyser le contenu des données stockées sur la machine par son précédent propriétaire.

4.1.7 Divulgation

Chantage
Soutirer de l'argent à un organisme ou à une personne est d'autant plus tentant que de nombreuses données concernant la vie privée des personnes ou les activités d'une organisation sont gardées sur des ordinateurs. Il est donc possible d'identifier les besoins et les faiblesses des personnes et de les manipuler. Le chantage peut aussi porter sur une menace de sabotage à l'encontre des installations d'une organisation. Le chantage peut mettre en cause aussi bien la confidentialité, l'intégrité, que la disponibilité des informations et des services.

Hameçonnage ou filoutage (*phishing*[3])
Cette technique désigne l'obtention d'informations confidentielles (comme les mots de passe ou d'autres informations privées), en se faisant passer auprès des victimes pour quelqu'un digne de confiance ayant un besoin légitime de l'information demandée. C'est une forme d'attaque informatique de type ingénierie sociale.

4.1.8 Informations sans garantie d'origine

Canular (*hoax*)
Il est transmis par courrier électronique et annonce la propagation d'un virus imaginaire dont les conséquences se trouvent être, en général, catastrophiques. Bien qu'il soit difficile de considérer ce type d'évènement comme une réelle attaque, elle contribue à la désinformation générale.

4.1.9 Piégeage du logiciel

Bombe
Une bombe est un programme en attente d'un événement spécifique déterminé par le programmeur et qui se déclenche quand celui-ci se produit. Ce code malicieux attend généralement une date particulière pour entrer en action. Les conséquences peuvent être bénignes comme l'affichage d'un message, d'une image ou d'un logo mais aussi dommageables, comme la destruction de données et plus rarement la destruction du matériel. Les effets visuels et sonores sont fracassants.

Virus
Nommé ainsi parce qu'il possède de nombreuses similitudes avec ceux qui attaquent le corps humain, un virus est un programme malicieux capable de se reproduire et qui comporte des fonctions nuisibles pour le SI : on parle d'infection. Le virus dispose de fonctions qui lui permettent de tester s'il a déjà contaminé un programme, de se propager en se recopiant sur un programme et de se déclencher comme une bombe logique quand un événement se produit.
Ses actions ont généralement comme conséquence la perte d'intégrité des informations d'un SI et/ou une dégradation ou une interruption du service fourni.

Ver
Un ver est un programme malicieux qui a la faculté de se déplacer à travers un réseau qu'il cherche à perturber en le rendant indisponible. Cette technique de propagation peut aussi être utilisée pour acquérir des informations par sondage.
Par exemple, le ver *MS-SQL Slammer*, qui le 25 janvier 2003 a provoqué une augmentation du trafic Internet telle qu'elle a ralenti, voire bloqué de manière perceptible, une partie des SI mondiaux.
Aujourd'hui ces deux derniers types d'attaque que sont les "Vers" et "Virus" se rapprochent, tel qu'il devient difficile d'en faire une distinction nette.
Parmi les plus célèbres nous pouvons citer :

- *Code Red*, apparu en août 2001, profitait d'une faille de certains serveurs web pour se propager,
- *Nimda*, apparu en septembre 2001, a utilisé plusieurs techniques de propagation pour infecter les systèmes et en laissant derrière lui des portes dérobées sur ces systèmes.

Piégeage
L'agresseur tentera d'introduire des fonctions cachées, en principe en phase de conception, de fabrication, de transport ou de maintenance, dans le SI. Seule une évaluation de la sécurité du SI donnera au défenseur une certaine assurance.

[3] d'après Wikipédia (http://fr.wikipedia.org).

Exploitation d'un défaut (*bug*)
De nombreuses failles sont présentes dans les logiciels commerciaux. Dès leurs découvertes par des pirates, elles font l'objet pour la plupart de publication sur l'Internet, accompagnée de la description des méthodes d'attaque à utiliser pour les exploiter. Ainsi, l'attaquant n'a plus besoin de compétence particulière pour mener des attaques parfois complexes. De plus, la "standardisation" des logiciels et le nombre croissant de failles découvertes rend les organismes de plus en plus vulnérables.

Canal caché
Ce type d'attaque est de très haut niveau et fait appel à l'intelligence de l'attaquant. Il permet de faire fuir des informations en violant la politique de sécurité. On peut classer les canaux cachés en quatre catégories :

- les canaux de stockage qui permettent de transférer de l'information par le biais d'objets écrits en toute légalité par un processus et lus en toute légalité par un autre ;

- les canaux temporels qui permettent à un processus d'envoyer un message à un autre en modulant l'utilisation de ses ressources système afin que les variations des temps de réponse puissent être observées ;

- les canaux de raisonnement qui permettent à un processus de déduire de l'information à laquelle il n'a pas normalement accès ;

- les canaux dits de "fabrication" qui permettent de créer de l'information en formant des agrégats qui ne peuvent être obtenus directement.

Ces attaques sont perpétrées dans le système ou les bases de données à plusieurs niveaux de confidentialité.

Cheval de Troie
Subterfuge employé par les Grecs pour prendre Troie, en informatique un cheval de Troie est un programme ou un fichier qui comporte une fonctionnalité cachée connue de l'attaquant seul. Elle lui permet de contourner des contrôles de sécurité en vigueur. Cependant un cheval de Troie doit d'abord être installé et ceci n'est possible que si les mesures de sécurité sont incomplètes, inefficaces ou si l'agresseur bénéficie d'une complicité.

Un cheval de Troie doit être attirant (nom évocateur) pour être utilisé, posséder l'apparence d'un authentique programme (un utilitaire par exemple) pour inspirer confiance et enfin ne pas laisser de traces pour ne pas être détecté. La simulation de terminal, dont le but est de s'emparer du mot de passer d'un utilisateur, est un cheval de Troie.
En conséquence, identifier la présence d'un cheval de Troie n'est pas aisée et une bonne connaissance du système et des applications installées est nécessaire.

Réseau de robots logiciels (*botnet)*
Réseau de robots logiciels (*bots*) installés sur des machines aussi nombreuses que possibles. Ces robots se connectent sur des serveurs IRC (*Internet Relay Chat*) au travers desquels ils peuvent recevoir des instructions de mise en œuvre de fonctions non désirées (envoi de *spam*, vol d'informations, participation à des attaques de saturation…).

Logiciel espion (*spyware*)[4]
Un logiciel espion est un logiciel malveillant qui infecte un ordinateur dans le but de collecter et de transmettre à des tiers des informations de l'environnement sur lequel il est installé sans que l'utilisateur n'en ait conscience.

4.1.10 Saturation du système informatique

Perturbation
L'agresseur va essayer de fausser le comportement du SI ou de l'empêcher de fonctionner en le saturant, en modifiant ses temps de réponse ou en provoquant des erreurs. L'agresseur veut désorganiser, affaiblir ou ralentir le système cible.
La perturbation va influer sur la disponibilité et l'intégrité des services et des informations d'un SI.

[4] d'après Wikipédia (http://fr.wikipedia.org).

Saturation
Cette attaque contre la disponibilité consiste à remplir une zone de stockage ou un canal de communication jusqu'à ce que l'on ne puisse plus l'utiliser. Il en résultera un déni de service.

Pourriel (*spam*)
Un *spam* est un courrier électronique indésirable, contenant ou non une pièce jointe, qui est transmis à une multitude de destinataires n'ayant sollicité aucune demande de la part de l'émetteur. Utilisé pour promouvoir des services ou des produits commerciaux, il est contribue à la pollution voir à la saturation des boîtes aux lettres électroniques.

4.1.11 Utilisation illicite des matériels

Détournement d'utilisation normale
L'attaque consiste à exploiter un défaut particulier d'implémentation. De nombreuses attaques ont ainsi été menées en utilisant la technique du *Buffer Overflow*. La technique consiste à exploiter une erreur de programmation de manière à faire exécuter à distance à la machine victime un code malveillant.
Cette technique est complexe et demande une forte compétence technique. Néanmoins, de nombreux outils sont disponibles sur l'Internet et permettent sans connaissance particulière de lancer de manière automatique ce type d'attaque.

Fouille
La fouille informatique, par analogie avec la fouille physique, consiste à étudier méthodiquement l'ensemble des fichiers et des variables d'un SI pour un retirer des données de valeur. Cette recherche systématique d'informations est en général grandement facilitée par la mauvaise gestion des protections classiques qu'il est possible d'attribuer à un fichier. Quand on se déplace dans les divers répertoires d'un système informatique, il est courant de constater que des fichiers et des répertoires ont des protections insuffisantes contre des agresseurs potentiels, uniquement par manque de connaissance, dû le plus souvent à l'insuffisance de formation, de l'utilisateur. Ainsi, est-il bien utile de donner un droit de lecture à ses fichiers pour l'ensemble des utilisateurs du système ?

Si l'attaquant est quelque peu entraîné, il aura recours à une attaque plus subtile. Pour s'emparer de certaines informations il va lire la mémoire, centrale ou secondaire, ou les supports de données libérés par les autres utilisateurs. Une parade efficace consiste à effacer physiquement toute portion de mémoire ou tout support libéré. En contrepartie, les performances du SI seront moindres.

Mystification
Dans ce cas, l'attaquant va simuler le comportement d'une machine pour tromper un utilisateur légitime et s'empare de son nom et de son mot de passe. Un exemple type est la simulation de terminal et le comportement d'une machine pour tromper un utilisateur légitime et s'emparer de son nom et de son mot de passe.
Un protocole d'authentification de la machine de destination permettra à un utilisateur d'être sûr de son interlocuteur.

Trappe
Une trappe est un point d'entrée dans une application généralement placé par un développeur pour faciliter la mise au point des programmes. Les programmeurs peuvent ainsi interrompre le déroulement normal de l'application, effectuer des tests particuliers et modifier dynamiquement certains paramètres pour changer le comportement original. Il arrive quelquefois que ces points d'entrée en soient pas enlevés lors de la commercialisation des produits et qu'il soit possible de les utiliser pour contourner les mesures de sécurité.

Un exemple connu est celui de l'exploitation du mode *debug* du programme *sendmail* utilisé par Robert T. Morris lors de son attaque par un ver sur Internet.

Asynchronisme
Ce type d'attaque évoluée exploite le fonctionnement asynchrone de certaines parties ou commandes du système d'exploitation. Les requêtes concernant de nombreux périphériques sont mises en file dans l'ordre des priorités puis traitées séquentiellement. Des tâches sont ainsi endormies puis réveillées lorsque les requêtes sont satisfaites. A chaque fois qu'une tâche ou qu'un processus est ainsi endormi, son contexte d'exécution est sauvegardé pour être restitué en l'état lors du réveil. En outre de nombreux processus s'exercent sur les périodes très longues. Pour éviter de perdre le bénéfice des calculs effectués depuis le début de l'application en cas de panne, il est nécessaire de définir des points de reprise sur incident. Les sauvegardes de contexte contiennent donc des informations propres à l'état du système et un attaquant averti peut les modifier afin de contourner les mesures de sécurité.

Souterrain
La technique du souterrain est un type d'attaque qui évite de s'attaquer directement à une protection mais qui tente de s'en prendre à un élément qui la supporte. Une telle attaque exploite une vulnérabilité d'un système qui existe à un niveau d'abstraction plus bas que celui utilisé par le développeur pour concevoir et/ou tester sa protection. Nous retrouvons ce type d'attaque dans le cas ou un détenu veut s'évader de prison : il préférera creuser un souterrain dans la terre plutôt que tenter de percer un mur d'enceinte en béton.

Par exemple, un accès non autorisé qui correspond au vol des données d'identification/authentification d'une personne afin de s'en arroger les droits ou en contournant les contrôles d'accès (porte dérobée).

Salami
La technique du salami permet à un attaquant de retirer des informations parcellaires d'un SI afin de les rassembler progressivement et de les augmenter de façon imperceptible. Cette technique est utilisée par de nombreux fraudeurs pour détourner subrepticement des sommes d'argent soit en s'appropriant de faibles sommes sur de nombreux comptes, soit en faisant transiter d'importantes valeurs sur des périodes courtes mais sur des comptes rémunérés leur appartenant.

Inférence sur les données
L'établissement d'un lien entre un ensemble de données non sensibles permet, dans certains cas, de déduire des données sensibles.

4.1.12 Altération des données

Interception
L'interception est un accès avec modification des informations transmises sur les voies de communication. Les quatre types d'interception sont :

- la destruction de messages,
- la modification de messages (modification de l'information; réagencement de l'information à l'intérieur des messages ou réagencement de la suite des messages),
- l'insertion de messages,
- refus de service (décalage dans le temps d'un message).

Balayage (*scanning*)
Le balayage consiste à envoyer au SI un ensemble d'informations de natures diverses afin de déterminer celles qui suscitent une réponse positive. L'attaquant pourra aisément automatiser cette tâche et déduire par exemple les services fonctionnant sur les machines, le type dudit système et pourquoi pas le nom de certains utilisateurs ainsi que leur mot de passe. Cette technique est analogue à celle qui consiste à balayer une gamme de fréquences pour trouver un signal porteur.

4.1.13 Abus de droit

L'abus de droit est le fait d'un utilisateur à qui a été attribué des privilèges systèmes et/ou applicatifs élevés et qui les utilise pour effectuer une opération malveillante. Par exemple, un opérateur de sauvegarde n'ayant pas le besoin d'en connaître sur le contenu à sauvegarder à la possibilité technique d'abuser de ses droits de lecture pour fouiller les fichiers sauvegardés.

4.1.14 Usurpation de droit

Les accès illégitimes
Cette menace est le fait d'une personne qui se fait passer pour une autre en usurpant son identité. Elle vise tout particulièrement l'informatique.
Les accès illégitimes portent atteinte à la confidentialité des informations.

Déguisement
Forme d'accès illégitime, il s'agit d'une attaque informatique qui consiste à se faire passer pour quelqu'un d'autre et obtenir les privilèges ou les droits de celui dont on usurpe l'identité.

Un utilisateur est caractérisé par ce qu'il est, (empreintes, digitales ou palmaires, rétiniennes, vocales, ou toute autre identifiant biométrique), ce qu'il possède (un badge, une carte magnétique, à puce, un jeton, un bracelet...) et ce qu'il sait (un mot de passe, sa date de naissance, le prénom de ses parents...). Pour se faire passer pour lui, un agresseur doit donc s'emparer d'un ou plusieurs éléments propres à l'utilisateur. Si le contrôle d'accès au SI se fait par mot de passe, l'attaquant tentera de le lire quand l'utilisateur le rentrera au clavier ou quand il le transmettra par le réseau. Si le contrôle d'accès se fait avec une carte à puce, l'attaquant cherchera à en dérober ou en reproduire une.
Sans arriver à des solutions lourdes et coûteuses, le défenseur pourra combiner des méthodes d'identification et d'authentification comme carte et mot de passe pour renforcer sa sécurité.

Rejeu
Le rejeu et une variante du déguisement qui permet à un attaquant de pénétrer dans un SI en envoyant une séquence de connexion effectuée par un utilisateur légitime et préalablement enregistrée à son insu.

Substitution
Ce type d'attaque est réalisable sur un réseau ou sur un SI comportant des terminaux distants. L'agresseur écoute une ligne et intercepte la demande de déconnexion d'un utilisateur travaillant sur une machine distante. Il peut alors se substituer à ce dernier et continuer une session normale sans que le système note un changement d'utilisateur.

Un cas bien connu est celui des ordinateurs sur un réseau local qui ne sont déclarés que par leur adresse réseaux. Un attaquant peut alors attendre qu'une machine soit arrêtée pour se faire passer pour elle en usurpant l'adresse de la machine éteinte.
Les techniques et outils de détection d'intrusion pourront contribuer à identifier ce type d'attaque.

Faufilement
Par analogie avec le faufilement physique où une personne non autorisée franchit un contrôle d'accès en même temps qu'une personne autorisée, on dira qu'il y a faufilement électronique quand, dans le cas où des terminaux ou des ordinateurs ne peuvent être authentifiés par un SI, un attaquant se fait passer pour le propriétaire de l'ordinateur ou du terminal.

4.1.15 Reniement d'actions

Le reniement (plus usuellement la répudiation) correspond pour une entité impliquée par exemple dans le cadre d'un échange d'informations, au fait de nier avoir participé à tout ou partie de la communication, de nier avoir reçu ou émis un message ou document déterminé, ou au fait de prétendre avoir émis ou reçu un message ou un document différent. Cette menace s'applique à de nombreuses actions réalisées sur les SI.

4.2 Les vulnérabilités : elles permettent la réalisation des méthodes d'attaque

Les vulnérabilités représentent les failles ou faiblesses des entités qui composent ou interagissent avec le système informatique. Elles sont susceptibles d'être exploitées par des éléments menaçants, utilisant une méthode d'attaque pour consulter, détruire, usurper ou modifier un bien.

Les moyens de protection sont mis en œuvre en vue "d'agir" sur les vulnérabilités pour réduire ou supprimer les risques en diminuant les vulnérabilités ou en rendant leur exploitation impossible (risque maîtrisé) ou seulement difficile (risque résiduel). La notion de vulnérabilité est donc essentielle dans le cadre de la gestion des risques.

4.2.1 Présentation générale

Pour arriver à son objectif, un attaquant va, en général, mener plusieurs attaques élémentaires coordonnées qui vont exploiter des vulnérabilités successives afin de constituer un chemin lui permettant de parvenir à ses fins. Les vulnérabilités exploitées ne sont pas toujours indépendantes les unes les autres car l'exploitation d'une vulnérabilité constitue souvent une nouvelle opportunité pour en exploiter d'autres. Il faut donc éviter particulièrement l'effet "château de carte" déclenché à partir d'un maillon faible et, si possible, mettre en œuvre des mesures dans un souci de défense en profondeur. Dans le cas d'une attaque élémentaire d'origine délibérée, elle ne pourra être exploitée par l'attaquant que si l'environnement dans lequel se trouve l'entité le lui permet. Dans ce chapitre, les vulnérabilités sont donc indiquées en supposant qu'il existe une telle opportunité d'attaque.

Une vulnérabilité est une propriété intrinsèque d'une entité. Une même vulnérabilité peut exister pour plusieurs entités, en général de type similaire (par exemple : une vulnérabilité de télémaintenance liée à la fonction de prise en main à distance des équipements, systèmes d'exploitation et application). À contrario, une vulnérabilité peut s'appliquer seulement à une entité donnée, voire à un exemplaire particulier d'une entité (exemple : une vulnérabilité de type *buffer overflow* dans un logiciel XXXX en version n). Enfin, on note qu'une même vulnérabilité peut être exploitée dans le cadre de plusieurs méthodes d'attaque.

Dans ce document, les vulnérabilités des différentes entités sont regroupées par types, à partir d'une classification qui a pour but de faciliter la compréhension.

4.2.2 Types de vulnérabilités

Différentes classifications sont proposées pour les vulnérabilités dans la documentation ouverte. Parmi celles-ci on trouve des classifications par origine (intentionnelle ou non), par moment de leur introduction (réalisation, installation, environnement), par faiblesse technique, etc. Aucune ne se révèle universelle car bien souvent elle ne s'adapte qu'à un seul type d'entité. Il est proposé ici de définir les différentes vulnérabilités en se plaçant du point de vue de leur origine, celle-ci déterminant souvent des mesures protectrices similaires, partant d'une même logique.

On distinguera donc les grands types de vulnérabilités suivants :

- les vulnérabilités de conception qui résultent d'un choix initial du concepteur (choix d'une technologie par exemple) ; ces vulnérabilités ne peuvent pas être supprimées sans remettre en cause l'entité elle-même ;

- les vulnérabilités de réalisation qui résultent des principes de fabrication (mauvais codage par exemple) ; ces vulnérabilités peuvent être diminuées ou supprimées par des opérations correctrices à la charge du réalisateur ;

- les vulnérabilités liées aux conditions d'emploi des entités, qu'il s'agisse de leur environnement ou de leur processus d'installation (mauvais paramétrage par exemple) ; ces vulnérabilités peuvent être diminuées ou supprimées par des opérations correctrices à la charge de la mise en œuvre ;

- les vulnérabilités liées à l'usage des entités et qui peuvent être diminuées ou supprimées par une action au niveau des utilisateurs, encore que d'autres mesures permettent de les limiter.

4.2.3 Principales vulnérabilités

S'il l'on se place du point de vue d'un attaquant, en fonction de l'objectif qu'il s'est fixé et des vulnérabilités de l'entité ou des entités à attaquer, il va utiliser une méthode d'attaque qui exploitera les vulnérabilités. Il est donc pratique d'associer les vulnérabilités des entités aux méthodes d'attaques pertinentes.

Il est à noter, que dans le cas des logiciels connus, les vulnérabilités de conception et de réalisation sont diffusées, par des organismes de type CERT (*Computer Emergency Response Team*), sous la forme d'avis (vulnérabilité découverte) et d'alerte (vulnérabilité exploitée) et font l'objet de bases de connaissances.

Vulnérabilités de conception
Les vulnérabilités de conception concernent tous les types d'entité. Elles peuvent être connues au moment du choix de l'entité et doivent faire l'objet d'un risque accepté ou de mesures de protection permettant de supprimer ou limiter l'opportunité de l'exploiter. Lorsqu'elles sont révélées après la mise en service, les mesures à prendre devront agir sur l'environnement pour interdire l'exploitation de la vulnérabilité voire même prévoir le remplacement de l'entité.

Les principales vulnérabilités de conception concernent :

- la définition de l'entité elle-même (un matériel portable est plus vulnérable au vol qu'un matériel non portable mais le rendre non portable n'a pas de sens) ;

- le choix de la technologie utilisée (exemples : vulnérabilité d'un protocole, technologie privilégiant le débit au détriment du contrôle d'intégrité) ;

- le choix des caractéristiques principales du produit (en général une limitation des capacités liés à un choix de type coût/efficacité comme la sensibilité au rayonnement par exemple).

Les méthodes d'attaques pour exploiter ce type de vulnérabilité ne nécessitent pas ou peu de connaissances particulières de l'environnement des entités et donc de reconnaissance préalable importante. Il suffit d'en connaître l'existence.

Vulnérabilités de réalisation
Les vulnérabilités de réalisation concernent principalement les entités de type logiciel et système en raison de leur mode de réalisation :

- il s'agit d'une œuvre de l'esprit qui est ensuite dupliquée en autant d'exemplaires que nécessaire ; en cas d'erreur, celle-ci va donc se retrouver dans tous les exemplaires (ceci permet de mettre au point des méthodes d'attaque ciblées mais aussi de faire profiter à tous des avis et alertes pour prendre les mesures protectrices nécessaires) ;

- les tests ne sont pas, en général, exhaustifs car ils s'attachent à vérifier que l'entité est conforme aux spécifications mais non qu'elle peut être utilisée dans d'autres conditions.

Les vulnérabilités de réalisation des matériels résultent en général des limitations économiques liées à leurs possibilités ou aux méthodes de fabrication qui les rendent plus ou moins sensibles aux agressions (exemples : sensibilité au rayonnement par manque de mesures de protection, usure engendrant une fiabilité insuffisante face à une agression). De surcroît, ils peuvent être piégés ou présenter des vices cachés (mauvaise fiabilité des composants par exemple).

Les vulnérabilités de réalisation des réseaux sont consécutives principalement à leur architecture, la technologie étant bien maîtrisée. Cette architecture peut être plus ou moins sensible à des attaques sur la disponibilité (redondance de liaisons), l'intégrité (présence ou absence de contrôles) et à la confidentialité car ils sont faits, par définition, pour communiquer. Les vulnérabilités de réalisation des réseaux vont donc concerner soit les techniques permettant la communication (leur exploitation a pour effet de gêner, interdire, modifier le flux) soit le contenu lui-même (leur exploitation a pour effet une atteinte à la confidentialité ou à l'intégrité). Il est à noter que les solutions visant à supprimer les vulnérabilités pesant sur le contenu doivent également prendre en compte les vulnérabilités des logiciels et des matériels présents aux extrémités.

Les principales vulnérabilités de réalisation des logiciels sont produites par l'utilisation, en développement, de techniques qui, bien que répondant au résultat attendu (le logiciel passe donc les tests d'acceptation), permettent de faire "autre chose" que ce qui est prévu (par exemple de tester le code du produit).
Les principales vulnérabilités concernent donc :

- la possibilité d'utiliser l'entité à autre chose que ce pour quoi elle est prévue (exemples : possibilité d'introduire un code permettant d'utiliser une machine comme "rebond", outils de détection d'attaque utilisable comme outil offensif) ;

- la possibilité d'utiliser l'entité à ce pourquoi elle est prévue mais lorsque l'on n'en possède pas le droit ; cette vulnérabilité correspond alors à une faiblesse dans les moyens d'accès (par exemple, possibilité de *buffer overflow*) ou à une possibilité de fraude.

Les méthodes d'attaques permettant d'exploiter de telles vulnérabilités vont résulter de l'analyse fine des produits logiciels dans le but de découvrir une fonctionnalité cachée, une erreur dans le logiciel, une faille. Elles nécessitent donc une phase exploratoire simple pour identifier la cible. Ces vulnérabilités seront ensuite exploitées en poursuivant un autre objectif (vol d'informations, prise de main, utilisation illégale…).

Vulnérabilités de mise en œuvre
Les vulnérabilités de mise en œuvre concernent toutes les entités mais pas toutes de la même manière. En effet, il faut considérer deux types de vulnérabilités de mise en œuvre : celles résultant de l'entité elle-même, indépendamment de son environnement, et celles résultant de l'entité interagissant avec d'autres entités.
Il est à noter qu'elles ont une importance particulière lorsque l'entité est accessible à des tiers non identifiés ou plus généralement à un large public (Internet).

Les vulnérabilités de mise en œuvre des matériels concernent en général les matériels eux-mêmes et leur dimensionnement pouvant entraîner des vulnérabilités dans leur fonctionnement en terme de disponibilité et d'intégrité (bien que ce dernier point soit devenu maintenant moins important qu'auparavant), lorsqu'ils sont mis en œuvre en dehors des conditions prévues par le fournisseur (dysfonctionnement par exemple suite à l'utilisation avec des périphériques non préconisés ou dans des conditions de température limite).

Les vulnérabilités de mise en œuvre des réseaux sont dues principalement à une mauvaise adaptation des conditions d'acceptation des flux par rapport aux besoins réels en raison souvent de leur méconnaissance (obligation d'accepter des flux illicites faute de connaître les flux licites soit en raison d'études insuffisantes soit par non cloisonnement des différents types). La vulnérabilité intrinsèque de chaque composant se double alors d'une vulnérabilité globale de l'ensemble le rendant plus sensible au maillon faible. Il est à noter que l'on rejoint dans ce cas la vulnérabilité de conception d'un réseau qui reporte toute la protection à la périphérie.

Les vulnérabilités de mise en œuvre des logiciels et des systèmes sont principalement à la conséquence d'erreurs ou de négligences de configuration (paramétrage inadapté, par défaut trop permissif, services ouverts mais non utiles…). Ces vulnérabilités entraînent souvent la possibilité d'exploiter des vulnérabilités d'autres types, c'est-à-dire de réalisation et d'utilisation.

Les méthodes d'attaques permettant d'exploiter des vulnérabilités de mise en œuvre nécessiteront en général une phase préparatoire permettant de déterminer les conditions de la mise en œuvre. Elles seront alors adaptées aux conditions du ou des défauts relevés dans la mise en œuvre.

Vulnérabilités d'utilisation
Les vulnérabilités d'utilisation concernent toutes les entités et ont une importance particulière dans la mesure où, par définition, la protection vis-à-vis des utilisateurs est moindre que celle vis-à-vis de tiers non identifiés (en dehors des systèmes publics). Ces vulnérabilités seront encore plus cruciales lorsque les utilisateurs auront, de part leur fonction, des droits importants.

Les vulnérabilités d'utilisation des matériels concernent principalement le fait que, par définition, ils sont physiques et qu'à ce titre ils ont une valeur marchande, peuvent s'altérer, émettre des rayonnements, peuvent être détournés de leurs usages par exemple.

Les vulnérabilités d'utilisation des réseaux concernent soit l'usage qui peut en être fait (détournement d'usage, utilisation pour une attaque interne par contournement de procédure d'accès) soit la possibilité d'accès accrue permettant des actions de l'intérieur (utilisation d'un outil de surveillance pour intercepter le contenu par exemple).

Les vulnérabilités d'utilisation des logiciels proviennent du fait que ces derniers interagissent avec les utilisateurs de qui en font soient des causes de vulnérabilité, soient des attaquants privilégiés exploitant d'autres vulnérabilités :

- le non respect des mesures de sécurité associées à l'exploitation d'un produit (par exemples l'utilisation d'un mot de passe non "robuste", le non respect de règles de discrétion) est une cause de vulnérabilité aggravante de la moindre faiblesse d'une entité ; le fait que l'utilisateur est souvent le seul capable de déceler des infractions à la sécurité est une vulnérabilité particulière en raison d'un manque de fiabilité (l'erreur humaine) ;

- le fait que l'utilisateur est "propriétaire" de l'information c'est-à-dire que, dans les limites fixées, c'est lui est chargé de la validation finale (saisie de données illicites, divulgation ou modification d'information utilisant ses privilèges d'utilisateur pour en tirer un pouvoir ou commettre une fraude).

Les méthodes d'attaques permettant d'exploiter des vulnérabilités d'utilisation visent à détourner l'usage de l'entité soit pour réaliser une opération non souhaitée (utilisation personnelle, copie illicite, accès à distance à des systèmes non autorisés) soit pour l'exploiter en détournant son usage (génération d'un paiement valide à destination d'un comparse, revente d'information autorisées, etc.) soit pour usurper l'identité ou s'arroger les droits d'un autre utilisateur (par exemple un accès en mode privilégié pour des travaux d'exploitation permettant de consulter de l'information confidentielle).

4.3 L'opportunité : la notion d'incertitude de la menace

L'opportunité d'une attaque délibérée se définie comme sa faisabilité. Dans le cas d'une menace de cause non délibérée, la probabilité d'occurrence de l'attaque est souvent utilisée.

D'une manière générale, elle représente le niveau de la(des) vulnérabilité(s) exploitée(s), c'est-à-dire le fait qu'elle(s) est(sont) plus ou moins avérée(s).

5 Conclusion

Notre société est confrontée à des mutations sociales et technologiques constantes. Le domaine du traitement de l'information est particulièrement sujet à des bouleversements. Les États et les entreprises confient leurs informations à des systèmes de plus en plus performants et complexes. Leurs qualités dues principalement à la miniaturisation et à l'abaissement des coûts des équipements s'améliorent au détriment de la sécurité en partie à cause d'une grande ouverture pour faciliter les échanges, d'une grande hétérogénéité des matériels et des procédures et de la complexité croissante des produits.

Pour un SI donné, la menace n'est pas unique mais le plus souvent composite du fait de la diversité des systèmes et des informations gérées. Il en va de même pour les attaques. Un agresseur utilisera généralement plusieurs techniques, ou des combinaisons, pour arriver à ses fins en exploitant les vulnérabilités d'un SI.
Nous avons déjà dit que la concrétisation d'une menace peut se traduire par une perte de confidentialité, d'intégrité ou de disponibilité pour les informations et les services. Les pertes peuvent être, partielles ou totales avec les conséquences qui en découlent : divulgation d'informations stratégiques pour un État ou une entreprise, avec éventuellement mise en cause de son avenir pour cette dernière, perte d'argent, de marché...

De son côté, le défenseur doit être capable de déterminer ce qu'il veut protéger et contre qui. Connaissant ses propres vulnérabilités, une analyse de risque lui permettra d'identifier les scénarii d'attaques réalistes et par conséquent de mettre en place les parades nécessaires à la protection de ses informations.

6 Références bibliographiques

[ACM 1994] Landwehr, C.E., Rull, A.R., McDermott, J.P., Choi, W.S., *A Taxonomy of Computer Program Security Flaws, with Examples*, ACM Computing Surveys (1994).

[Bishop & Bailey 1996] Bishop, M., Bailey, D., *A Critical Analysis of Vulnerability Taxonomies*, CSE (1996).

[Bishop 1995] Bishop, M., *A Taxonomy of UNIX System and Network Vulnerabilities*, CSE (1995).

[CERT-CC] *Overview of Attack Trends*, et *Overview Incident and Vulnerability Trends*, CERT –Coordination Center.

http://www.cert.org/present/cert-overview-trends/

[Chen 2002] Chen, S., *Comments on Taxonomies of Security Vulnerabilities and Possible Ways to Find Security-related Topics*, CRHC, UIUC (2002).

[CIGREF] *Rapport du CIGREF* – CIGREF (2002)

[CMU] *Tracking and Tracing Cyber-Attack : Technical Challenge and Global Policy Issues* – CMU/SEI (2002).

[CS 6262] *Security Threats and Vulnerabilities* - CS 6262 Spring 02 (2002).

[EBIOS] *Expression des Besoins et Identification des Objectifs de Sécurité* – SGDN – version 2 (2004).

[FEROS] *Fiche d'Expression Rationnelle des Objectifs de Sécurité des systèmes d'information (FEROS)* – SGDN (1991).

[G 650v1] *La menace et les attaques informatiques* – SGDN (1994).

[ISO 13335] *Information technology – Security techniques – Guidelines for the management of IT security (GMITS)* – International Organization for Standardization (ISO) (2001).

[ISO 15408] *Critères Communs pour l'évaluation de la sécurité des Technologies de l'Information* – International Organization for Standardization (ISO) – version 3 (2005).

[MITRE 1999] Baker, D.W., Christey, S.M., Hill, W.H., Mann, D.E., *The Development of a Common Enumeration of Vulnerabilities and Exposures*, MITRE (1999).

[Neumann & Parker 1989] Neumann, P.G., Parker, D.B., *A Summary of Computer Misuse Techniques*, Proceedings of the 12th National Computer Security Conference (1989).

[Piessens 2002] Piessens, F., *A Taxonomy (with Examples) of Cause of Software Vulnerabilities in Internet Software*, Report CW346 (2002).

[PSSI] *Guide d'élaboration de politiques de sécurité des systèmes d'information* – SGDN (2004).

Formulaire de recueil de commentaires

Ce formulaire peut être envoyé à l'adresse suivante :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
conseil.dcssi@sgdn.pm.gouv.fr

Identification de la contribution
Nom et organisme (facultatif) : .....
Adresse électronique : .....
Date : .....

Remarques générales sur le document
Le document répond-il à vos besoins ? Oui ☐ Non ☐

Si oui :

Pensez-vous qu'il puisse être amélioré dans son fond ? Oui ☐ Non ☐

Si oui :

Qu'auriez-vous souhaité y trouver d'autre ?
.....
.....

Quelles parties du document vous paraissent-elles inutiles ou mal adaptées ?
.....
.....

Pensez-vous qu'il puisse être amélioré dans sa forme ? Oui ☐ Non ☐

Si oui :

Dans quel domaine peut-on l'améliorer ?
- lisibilité, compréhension ☐
- présentation ☐
- autre ☐

Précisez vos souhaits quant à la forme :
.....
.....

Si non :

Précisez le domaine pour lequel il ne vous convient pas et définissez ce qui vous aurait convenu :
.....
.....

Quels autres sujets souhaiteriez-vous voir traiter ?
.....
.....

Remarques particulières sur le document

Des commentaires détaillés peuvent être formulés à l'aide du tableau suivant.

"N°" indique un numéro d'ordre.

"Type" est composé de deux lettres :

La première lettre précise la catégorie de remarque :

- O Faute d'orthographe ou de grammaire
- E Manque d'explications ou de clarification d'un point existant
- I Texte incomplet ou manquant
- R Erreur

La seconde lettre précise son caractère :

- m mineur
- M Majeur

"Référence" indique la localisation précise dans le texte (numéro de paragraphe, ligne…).

"Énoncé de la remarque" permet de formaliser le commentaire.

"Solution proposée" permet de soumettre le moyen de résoudre le problème énoncé.

N°	Type	Référence	Énoncé de la remarque	Solution proposée
1				
2				
3				
4				
5				

Merci de votre contribution