Chapitre 1 : principes de base de sécurité

La sécurité informatique des systèmes d'information
A. Les objectifs de la sécurité
1. Disponibilité
2. Intégrité
3. Confidentialité
4. Traçabilité
B. Analyse complète des risques
1. Les composants du système d'information
2. Les menaces
3. Les parades
4. L'audit sécurité
C. Les attaques possibles
D. Les agresseurs potentiels
E. La détection d'intrusion
F. Bâtir une politique sécurité
G. La cyberguerre : la guerre pour l'information

1. Les objectifs de la sécurité

1.1. Disponibilité

Qualité d'une ressource informatique d'être utilisable à la demande.

Prévenir l'inaccessibilité des ressources

1.2. Intégrité

Qualité d'une ressource informatique de ne pouvoir être altérée,détruite par accident ou malveillance.

Prévenir les modifications non autorisées : fiabilité des données

Assurance que les données n'ont pas été modifiées pendant le transport. Cela permet par exemple au récepteur d'un message d'être raisonnablement assuré que le message reçu est le même que le message envoyé. Le contrôle de l'intégrité d'une donnée consiste à s'assurer que cette donnée n'a pas été altérée accidentellement ou frauduleusement.

1.3. Confidentialité

Qualité d’une ressource informatique de n'être connue que par les personnes autorisées.

Prévenir la divulgation d'informations.

Permet de garder secret le contenu de l'information aux personnes non autorisées. Seuls les destinataires prédéterminés doivent être capables de lire le contenu du message. La confidentialité permet de rendre la lecture de l'information inintelligible à des tiers non autorisés lors de sa conservation ou surtout de son transfert. Le chiffrement des informations constitue la technique la plus utilisée pour répondre à ce service.

1.4. Traçabilité

Journalisation et suivi des événements sur le réseau permettant le suivi des activités réseau.

2. Analyse complète des risques

2.1. Les composants du système d'information

Un inventaire permet de connaître son environnement et suppose un recensement exhaustif et précis.

- Le matériel
  - Les postes de travail
  - Les serveurs
  - Le (ou les) réseau(x)
  - Les routeurs
  - Les systèmes d'impression
  - Le PABX, les modems
  - Les lignes de transmissions

- Les logiciels
  - Les systèmes techniques
  - Les systèmes bureautiques
  - Les systèmes administratifs et de gestion
  - Les systèmes d'exploitation
  - Les systèmes de sécurité
  - Les systèmes de télécommunication

- Les données
  - Les données techniques
  - Les données de gestion
  - Les sauvegardes

- Le personnel
  - Les utilisateurs (identifiés)
  - Les administrateurs (informaticien ou équivalent)
  - Les prestataires de services
  - Les stagiaires
  - Les autres …

- La documentation
  - Les procédures d'installation
  - Les procédures de restauration
  - La politique sécurité de l'entreprise
  - Le plan de sécurité

…

2.2. Les menaces

2 types de menaces :

accidentelles

intentionnelles

qui peuvent être

d'origine interne (80% des attaques)

d'origine externe

Une menace se définit par rapport aux objectifs de sécurité de l'entreprise.

à Définir les objectifs sécurité de l'entreprise (Risque Maximal Tolérable). La survie de l'entreprise peut-elle être mise en jeu ?

à Faire une évaluation des menaces.

a) Destruction ou la corruption d'informations peut engendrer des pertes de temps considérables peut devenir catastrophique si les sauvegardes ne sont pas faites.

peut se caractériser par des modifications de logiciels par l'introduction de virus, vers et bombes logicielles.

Sabotage : Attentat, vandalisme, action malveillante conduisant à un sinistre matériel

à IMPORTANCE DES SAUVEGARDES

b) Déni de service (détérioration de la qualité du service).

perturbation des moyens de transmissions

peut entrainer une perte de confiance dans l'outil informatique et réseau de l'entreprise.

Appeler également "bactéries" ou "lapins", ces programmes, capables de se reproduire, ont pour vocation de consommer des ressources.

à IMPORTANCE DES RESEAUX INFORMATIQUES

c) "Vol" d'informations confidentielles.

Vol de fichiers magnétiques sur site ou en transit

l'espionnage technologique et économique est une réalité (perte de marchés , de contrats inexpliquée)

peut menacer l'existence de l'entreprise.

attention aux actions de maintenance (les disques durs partant en maintenance !)

Divulgation : Utilisation non autorisée des ressources du système d'information, entraînant la divulgation à des tiers d'informations confidentielles.

d) Modifications de données d'importance capitale

savoir les détecter

peut nuire à l'image de marque à la réputation de l'entreprise.

e) "Mascarade d'identité"

L'intrus se fait passer pour quelqu'un d'autre et s'infiltrer pour diffuser ou collecter de fausses informations.

f) Rebonds

Attention à la multiplication des accès distants.

Responsabilité de l'entreprise favorisant le rebond.

g) Utilisation frauduleuse de ressources

Attaque logique : Utilisation non autorisée des ressources du système d'information, conduisant à un préjudice au moins qualitatif pour la victime, se traduisant essentiellement par une perte d'intégrité et/ou de disponibilité, entraînant le plus souvent un profit indirect pour le criminel et/ou le commanditaire éventuel (sabotage immatériel, infection informatique, programme "simple", bombe logique, cheval de Troie, sabotage "manuel", programme auto-reproducteur, ver, virus (système ou programme)).

Intrusion extérieure (ou intérieure) sur une machine sans autorisation et utilisation de ressources réservées (calcul, espace disque, logiciels, ...).

Responsabilité de l'établissement en cas d'utilisation de logiciels piratés, de stockage de contenus illicites, etc.

Attention à la divulgation des mots de passe

h) Vols et destructions des matériels

vols des équipements, incendie provoqué, sabotage, destruction de support magnétique.

destruction des liens physiques de communication

i) Fraudes

Utilisation non autorisée des ressources du système d'information, conduisant à un préjudice évaluable monétairement pour la victime, essentiellement formé par le détournement de biens au profit du criminel

j) Accidents / erreurs non malveillantes

Incendies, dégâts des eaux, pannes, dysfonctionnement, coupure électrique, mauvaise utilisation

2.3. Les parades

a) Les objectifs

Prévention
peut s'organiser à partir du précepte suivant : "Interdire tout ce qui n'est pas explicitement autorisé"

Protection
par contrôle d'accès contre l'usage non autorisé des ressources accessibles, en particulier pour les utilisateurs distants.

Détection

Identification
permet de distinguer un individu dans un ensemble connu

Authentification
Action de prouver l'identité. Elle est à la base des méthodes de contrôle d'accès., assure que la prétendue origine de l'information est bien la même que l'origine réelle. Facilite la détection d'intrusion et l'analyse des événements. Elle est indispensable pour l'audit.

Non répudiation
L'émetteur ne doit pas pouvoir nier avoir envoyé le message. S'appuie sur le mécanisme de notarisation. La non répudiation permet d'obtenir la preuve de l'émission d'une information ou la preuve de sa réception. L'émetteur ou le récepteur ne peut ainsi en nier l'envoi ou la réception.

b) Les différents types de parade

Physiques

Protection des zones sensibles

Alimentation électrique de secours,
redondance de certains équipements (serveurs,disques durs,...)

Logiques

Accès aux programmes et aux données

Accès aux réseaux (définition des routes autorisées et non autorisées) par l'utilisation de FireWall.

Le bourrage de trafic , mécanisme de protection contre l'analyse du trafic

Mise en place d'antivirus mis à jour régulièrement.

Organisationnelles

Organisation de la sécurité
Suivi des configurations,
Organisation de l'utilisation des systèmes
Responsabilité des agents
Traitement des incidents sécurité

2.4. L'audit sécurité

Définition par les dirigeants des gravités et priorités.

Analyse par les responsables informatiques des conséquences liées à chaque menace.

Cet analyse permet une identification des cibles.

Analyse des possibilités techniques de réalisation de la menace, évaluation des failles potentielles, mise en lumière des points faibles.

3. Les attaques possibles

Une attaque est une entrave volontaire portant atteinte aux ressources informatiques et résultant d'une activité humaine.(Tendance actuelle : Les outils d'automatisation d'attaques de hacking vont être de plus en plus utilisés. Ils sont de plus en plus nombreux et de plus en plus intelligents, sophistiqués.)

3.1. Destruction par virus, vers, bombes logicielles

3.2. Intrusion par Cheval de Troie

Il s'agit de placer un programme dans un système de façon à fournir un accès ultérieur privilégié et incontrôlable.

3.3. Intrusion par portes dérobées

Le concepteur d'un programme peut laisser un accès lui permettant de s'introduire dans son système à l'insu de tout contrôle.

- Dans un logiciel, une porte dérobée (de l'anglais backdoor, littéralement porte de derrière) est une fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au logiciel.
  fr.wikipedia.org/wiki/Porte_dérobée
- Programme malicieux visant à détourner les fonctionnalités d'un service ou d'un système en ouvrant sur la machine touchée des canaux d'accès masqués et utilisés par une personne malveillante
  www.binarysec.fr/cms/docs/ressources/glossaire/p-s.html
- Menace de sécurité potentielle créée par un programme qui détourne les fonctionnalités du système dans le but d'ouvrir des accès utiles aux attaquants à fin de contrôler le système à distance. Ce programme est souvent installé par un cheval de Troie.
  securite.topnet.tn/index.php

3.4. Intrusion par Spoofing de paquets

Usurpation d'adresses IP autorisées

3.5. 5. Espionnage des liaisons ou analyse de trafic

La capture des données circulant sur le réseau permet d'intercepter les mots de passe.

3.6. 6. Intrusion par bogues logiciels

Les vulnérabilités des produits sont très vites connues.

3.7. 7. Exploitation d'accès non sécurisés

On ne compte plus les utilisateurs sans mot de passe ou très simple à deviner.

3.8. 8. Refus d'accès, Saturation de services (DENI de service)

Le "Distributed Denial of Service" (DDoS) consiste à rendre une ressource inaccessible par saturation ou par destruction.Cette attaque est souvent réalisée par un envoi massif de requêtes. Deux techniques d'attaques communément appelée "Smurf" et "Syn Flood" sont possibles. L'une comme l'autre consistent à inonder de demandes de connections l'ordinateur, appelé serveur, permettant d'accéder à un site internet. Dans la technique du "Syn Flood", ces demandes sont assorties d'une adresse d'origine qui est fausse, ce que les experts appellent le "spoofing", augmentant la confusion du serveur, suivi de son engorgement voire de son arrêt. Des programmes comme TFN, TFN2K, Trin00 ou Stacheldraht sont conçus spécialement pour réaliser ce type d'attaque et sont totalement disponibles sur Internet.

3.9. 9. Transparence excessive des annuaires

L'accès à l'annuaire de l'entreprise peut être l'étape préalable à une recherche des mots de passe. L'utilisation de dictionnaires, d'outils pour trouver des mots de passes se répand. On tente de se faire identifier en essayant des milliers de mots de passe jusqu'à trouver le bon.

3.10. 10. Surveillance des messageries d'entreprises

Le système d'information de l'entreprise est de plus en plus lié à la messagerie d'entreprise.

3.11. 11. Exploitation des fichiers de logs

L'analyse des fichiers de données révèle souvent de précieux renseignements. Certains de ces fichiers gardent des traces de l'activité réseau.

3.12. 12. Man in the Middle

Technique qui consiste à se placer entre deux clients pour intercepter, lire, modifier, effacer, les données qu'ils se transmettent.

4. Les agresseurs potentiels

4.1. Les saboteurs ou Crasher

Pirates dangereux qui détruisent pour le plaisir (?), pratique le vandalisme

4.2. Les chasseurs ou "les invisibles"

Hackers visitant les sites sans laisser de traces, pratiquement indécelables.

4.3. Les espions

Pirate payé par une entreprise ou un organisme concurrent pour récolter (de façon frauduleuse) des informations sur un domaine précis.

4.4. Les hackers

Initialement, programmeur informatique de génie capable de pénétrer les systèmes informatiques à distance (via un réseau). Seule la prouesse technique comptait. Progressivement et par simplification, le hacker a été associé au terrorisme informatique (pirate informatique). Le terme Cracker ("black hat hacker") a alors été inventé pour différencier les "bons" hackers ("white hat hacker") , des criminels informatiques.

4.5. Les lamers

les débutants, profanes de la piraterie informatique, littéralement les "boiteux"

4.6. Les scripts kiddies

Nouvelle génération de pirates informatiques (apparentée aux crackers) utilisant des utilitaires déjà existants. En général, laisse des traces pour marquer leur passage.

4.7. Les fraudeurs

Utilisation des ressources informatiques sans autorisation.

Phreaker : pirate spécialisé dans la fraude aux télécom, en contournant le réseau téléphonique pour ne pas payer la communication.
Coder : pirate spécialisé dans l'utilisation des codes de cartes bancaires.

4.8. Les voleurs

Vols d'informations ou de technologies.

4.9. Les maladroits

Utilisateur inconscient détruisant des informations dont il a accès sans le savoir…

4.10. Les corsaires

Pirate ayant un ordre de mission d'un Etat (qui le protège) et commettant des actes de cybercriminalité.

5. La détection d'intrusion

5.1. Niveau Utilisateur

Connexions anormales (horaire,…)

Modification de données

Anomalies de messagerie

Anomalies de comptatibilité logicielle (message d'erreurs anormal,…)

5.2. Niveau Administrateur

Utilisation inhabituelle des ressources

Accès à des fichiers sensibles

5.3. Mesures élémentaires de protection

Eviter de rendre publics les numéros d'accès distants

Contrôler l'origine des appels

Ne fournir des informations qu'après l'authentification de l'utilisateur référencé.

Contrôler les mots de passe

Déconnexion automatique après plusieurs tentatives infructueuses

Déconnexion automatique après délai d'inactivité

5.4. Réaction en cas d'intrusion

Comportement face à l'intrus.
Il existe la possibilité de stopper l'attaque à sa source, c'est à dire directement sur le système émetteur, en utilisant un programme du type Zombie_Zapper. Mais attention, en France son utilisation pourrait être assimilée par la DST à une attaque de votre part.

Analyse des défaillances dans sa globalité

Mise à niveau du système incriminé : validation et installation des correctifs, la réinstallation du système doit être envisagée en cas de doutes.

Informer la Direction

Déposer une plainte (selon l'importance du cas)

6. Bâtir une politique sécurité

0. Sensibilisation des dirigeants

La prise de conscience des risques par les dirigeants est indispensable.

1. Nommer un responsable sécurité et organiser une équipe

Le responsable de la sécurité des systèmes d'information (RSSI) est chargé de définir et mettre en place une politique de sécurité.Si une entreprise n'a pas une politique de sécurité efficace, il est quasi-impossible pour elle de se protéger.
Sécuriser les serveurs est une chose. Mais sécuriser une société entière est beaucoup plus compliqué.
Vérification du respect des règles de sécurité.

2. Définir les périmètres de sécurité

3 zones possibles :

Intranet

Extranet

Internet

L'accès physique aux salles "sensibles" devra être protégé.

3. Analyser les vulnérabilités

Concerne les applications et les systèmes interconnectés.

4. Définir les niveaux de sécurité

Elle s'effectue en fonction des risques évalués pour chaque composant. La mesure des risques encourus s'effectue avec les différents responsables. Il faut définir quelles informations ont de la valeur et quels sont les systèmes à protéger. Puis, diviser le réseau de l'entreprise en entités et définir les sous-réseaux confidentiels. Dans la plupart des entreprises, toutes les machines se font confiance, et sans cloisonnement il est très difficile de protéger les capitaux.

5. Recherche des parades

Les parades peuvent être de nature techniques et organisationnelles. Elles réduisent le risque mais ne le suppriment pas complètement.

6.Estimation des ressources nécessaires

Concerne les charges humaines et budgétaires engendrées.

7. Mise en oeuvre de solutions incontournables

Installation d'un coupe-feu.
Installation d'un outil de détection d'intrusion temps réel. Ce type de système (IDS) permet d'identifier un trafic suspect sur votre réseau et d'alerter votre équipe technique en charge de l'exploitation.
Installation de détecteur d'invulnérabilités
Installation d'un serveur d'analyse de contenus de messagerie
Installation d'une plate-forme de gestion centralisée

8. Sensibiliser et informer les utilisateurs

Informer sur les réglementations en vigueur (lois, décrets,…)

Sensibiliser sur les enjeux de la sécurité pour l'entreprise, mettre en oeuvre un politique sérieuse d'éducation au sein de l'entreprise.

Faire appliquer les recommandations internes et responsabiliser le personnel.
Mettre au point une procédure de suivi des entrées/départs avec la Direction des Ressources Humaines.

6.1. Authentifier et chiffrer les transactions

Une étude doit définir une véritable stratégie dans le cadre d'échanges sécurisés, celle-ci doit permettre la maitrise du process de certification de ses utilisateurs (distants).

a) La signature

La signature numérique est une technique qui permet la mise en oeuvre à la fois de l'intégrité des données, de l'authentification et de la non répudiation. Seul son détenteur possède cette information secrète.

Prévoir un changement périodique des mots de passe.

b) Le chiffrement

Permet de transformer des données en clair en des données non intelligibles pour ceux qui ne sont pas autorisés.

c) Le déchiffrement

Opération permettant aux destinataires légitimes de reconstituer le message en clair.

d) Le décryptement

Opération qui consiste à essayer de déterminer le message en clair à partir d'un message chiffré sans information sur l'algorithme de chiffrement.

--> L'utilisation d'une clef de chiffrement à 40 bits est largement insuffisante !! 128 bits pour les clefs symétriques est - ce encore viable ? (-> Utiliser du triple DES)

10. Assurer une veille technologique et réglementaire

L'administrateur chargé du réseau et de la sécurité doit se tenir parfaitement informé des failles de sécurité découvertes, des corrections à appliquer. Sans cette vigilance, la défense du réseau est compromise.
Lecture des listes électroniques de diffusion
Suivi des journaux officiels (lois, décrets,...).

11. Auditer régulièrement

Activation des programmes d'audit.

Vérification des droits d'accès.

Surveillance permanente des accès physiques.
La journalisation des traces permet une surveillance en temps différé et peut être un outil capable de localiser une attaque.

12. Une méthode d'analyse des vulnérabilités : Le test d'intrusion

Avertir l'organisme officiel concerné avant d'entreprendre une telle action.

Mettre au point une convention entre l'entreprise et le prestataire chargé de l'intrusion en exigeant confidentialité, expérience, non altération et non destruction des données. Définir éventuellement les adresses IP autorisées à effectuer des attaques (pour différencier les tests, des vrais attaques !)

Définition du périmètre réseau avec l'inventaire des points d'accès

Détection des failles potentielles (failles connues, erreurs de configuration classiques)

Récupération des informations disponibles sur le périmètre concerné.

Recherche des machines les plus vulnérables.

Attaques progressives et systématiques.

Rédaction d'un rapport détaillé sur les actions effectuées et les résultats obtenus.

Propositions pour pallier aux failles répertoriées.

7. La Cyberguerre : la guerre pour l'information

Les réseaux deviennent une arme dans la recherche de l'information et de son contrôle. Le monde est en guerre économique ; un affrontement virtuel qui fait des victimes bien réelles. L'économie et l'information sont les maîtres mots de la très incontournable société de l'information. Les implications sont colossales pour les États, les entreprises et les particuliers. Le cyberespace est un véritable champ de bataille. Les fusils, les balles et le barbelé y sont remplacés par les ordinateurs, les paquets de données et les logiciels de filtrage.

Intrusions : firewall, proxy

Sécurité logique, virus et intrusions

Le fait de s'introduire et de se maintenir dans un système informatique sans autorisation est un délit puni par la loi. En cas d'incident, il ne faut pas hésiter à porter plainte. Pour éviter d'être dans cette situation, il est possible de prendre un minimum de précautions classiques.

Les attaques

Le **cheval de Troie** est un petit programme malveillant d'apparence anodine (jeu, petit utilitaire...) qui, une fois installé dans un ordinateur, peut causer des dégâts comme un virus classique, ou permettre de prendre le contrôle à distance de la machine.
La **backdoor** (porte arrière) est un point d'entrée dans un programme ou un système, plus ou moins secret. C'est généralement une sécurité pour débloquer un code d'accès perdu ou pour contrôler les données lors du debuggage. Malheureusement, c'est aussi l'un des points d'entrée des hackers, lorsqu'ils en découvrent l'existence. Le hacker peut également créer lui-même cette porte pour l'utiliser dans un deuxième temps.
Le **sniffing** : c'est écouter une ligne de transmission par laquelle transitent des données pour les récupérer à la volée. Cette technique peut-être utilisée en interne pour le débuggage ou de manière abusive par un pirate cherchant, par exemple, à se procurer des mots de passe.

Le **spoofing** : c'est une technique d'intrusion consistant à envoyer à un serveur d'une entreprise, des messages (paquets) semblant provenir d'une adresse IP connue par le firewall (adresse interne existante autorisée). Pour que la communication ne s'établisse pas avec la machine possédant réellement cette adresse, le hacker doit dans le même temps rendre cette machine injoignable pour avoir le temps d'intercepter les codes de communication et établir la liaison pirate.
L'**attaque par rebond** est menée via un autre ordinateur qui se trouve involontairement complice et qui expédie les messages d'attaque à la victime, masquant ainsi l'identité du véritable agresseur.
Dans l'**attaque par le milieu** le hacker se place entre deux ordinateurs en communication et se fait passer pour un afin d'obtenir le mot de passe de l'autre. Dès lors, il peut se retourner vers le premier avec un mot de passe valide et l'attaquer réellement.
Le **déni de service** est une attaque cherchant à rendre un ordinateur hors service en le submergeant de trafic inutile. Par exemple, un serveur entièrement occupé à répondre à des fausses demandes de connexion.
Plusieurs machines peuvent être à l'origine de cette attaque (généralement à l'insu de leur propriétaire).
Dans le cas des réseaux Wi-Fi, le **war-driving** consiste à circuler dans la ville avec un ordinateur portable ou un PDA équipés d'une carte Wi-Fi pour repérer et pénétrer dans les réseaux locaux mal protégés.

Il existe de nombreux logiciels conçus plus à cet effet qu'à un usage normal d'analyse de son propre réseau.

Prévention des attaques

Indispensable :

- disposer d'une bonne sauvegarde de toutes ses données.
- faire un audit des portes inutilement ouvertes (modems installés à demeure, logiciels de transmissions permanents…).
- lorsqu'ils existent, vérifier que les comptes d'administration ont des mots de passe sécurisés.
- supprimer les comptes utilisateurs non utilisés (notamment à la suite de chaque départ).
- désactiver les services non utilisés sur les machines (serveur Internet par exemple).
- supprimer les partages de fichiers non nécessaires

Souhaitable

- mettre à jour systèmes et logiciels (serveurs et serveurs Web principalement) à l'aide des patchs de sécurité officiels fournis pour fermer les brèches logicielles découvertes.
- installer un FireWall (boîtier électronique ou logiciel), qui sert d'intermédiaire lors des transmissions et bloque ainsi les attaques directes.
- structurer les réseaux en zones étanches par activité et sensibilité (VLAN). Instituer un système de mots de passe. Bien isoler les serveurs Internet.
- s'abonner aux newsletters de sécurité des différents fournisseurs.

Plus sophistiqué

- créer une zone tampon (DMZ) pour isoler fortement les serveurs Internet de l'informatique interne
- faire établir un audit de sécurité (analyses des points faibles, tentatives d'intrusion volontaires…).

Firewall, proxy, DMZ

Le **Firewall** est un ordinateur, un boîtier ou même un logiciel qui sert à protéger et isoler les réseaux les uns des autres, notamment pour protéger des pirates pénétrant par les connexions Internet. Il assure généralement les fonctions suivantes :

- examen détaillé de chaque paquet reçu,
- filtrage de contenu d'applications,
- authentification/autorisation d'applications,
- cryptage/décryptage,
- traduction d'adresses de réseau ou NAT (Network Address Translation), qui rend les utilisateurs non visibles de l'extérieur en leur attribuant une adresse IP différente pour l'extérieur.

La **DMZ** (DeMilitarized Zone) désigne une zone de sécurité située entre l'accès à Internet et le réseau interne de l'entreprise et dans laquelle on peut placer les serveurs Web accessibles depuis l'extérieur. Un firewall isole cette zone du réseau interne qui bénéficie ainsi d'une sécurité supérieure aux systèmes les plus exposés.

Dans la pratique, les boîtiers firewall disposent parfois d'une sortie DMZ pour connecter les serveurs Web sans autres connexions complexes.

Le **proxy** est un dispositif (ordinateur, logiciel...) qui stocke les pages Internet les plus demandées pour accélérer le trafic (cache). En s'interposant entre l'utilisateur et le réseau Internet, le proxy peut aussi servir de filtre de sécurité (firewall) et interdire certains types de malveillances, comme la prise de contrôle à distance de l'ordinateur client.

Autres protections

Un **IDS** (Intrusion Detection System) est un dispositif de sécurité détectant les tentatives d'intrusion ou les événements suspects similaires sur un système informatique.
Ce type de produit est principalement proposé par Cisco et ISS. Il peut s'agir d'un logiciel ou d'un boîtier externe (appliance).
Un **HIDS** (Host based IDS) surveille les intrusions sur un serveur,
un **NIDS** (Network based IDS) surveille l'activité des machines sur le réseau en capturant les trames échangées.

Organismes de sécurité

Un **CERT** (Computer Emergency Response Team) est une organisation d'administrateurs systèmes qui se charge de recenser les failles logicielles et de les publier.
Il existe une petite centaine de CERT au monde, dont 3 en France :

- CERTA (administrations)
- CERT-RENATER (recherche et éducation
- CERT-IST (Industrie, Services, Tertiaire)

Le FIRST (Forum for Incident Response and Security Teams) se charge de diffuser la liste des CERT.