Accompagner

Septembre
2006

Sécurité informatique

Guide de sensibilisation

MEDEF

Sommaire

GUIDE SSI

Guide de sensibilisation à la sécurisation du système d'information et du patrimoine informationnel de l'entreprise

Présentation

Fiches

Glossaire

Présentation

Guide de sensibilisation à la sécurisation du système d'information et du patrimoine informationnel de l'entreprise

Avertissement : *Le présent document a pour unique vocation de sensibiliser à la sécurisation des systèmes d'information. Le MEDEF décline toute responsabilité en ce qui concerne l'utilisation des solutions préconisées par ce guide. Ce guide ne peut aucunement se substituer aux conseils avisés de spécialistes techniques ou juridiques de la sécurité des systèmes d'information.*

Le besoin grandissant de communication a créé l'ère de l'informatique répartie et interconnectée au travers du réseau Internet. Non seulement l'entreprise ne peut plus se passer de l'informatique pour son fonctionnement interne, mais en plus son système d'information est accessible de l'extérieur pour lui permettre un travail en réseau avec ses fournisseurs, donneurs d'ordre, partenaires et l'administration. Ce besoin de communication tant interne qu'externe crée une vulnérabilité des systèmes internes de l'entreprise vis-à-vis d'attaques potentielles. La généralisation des outils nomades (téléphones mobiles, PDA, ordinateurs portables) accentue encore ces risques. Des mesures de protection homogènes sont donc indispensables.

La mise en œuvre d'un plan de sécurité des systèmes d'information, et des échanges, s'impose aujourd'hui à toutes les entreprises. La sécurité est liée à la fiabilité du système d'information comprenant le réseau, les systèmes, les applications, et le contenu.

Mais, encore trop souvent, la dotation de solutions de sécurité (produits ou services) est consécutive à des attaques majeures ayant occasionné de graves dégâts pour l'entreprise. Pourtant, les investissements nécessaires pour pallier ce risque sont de loin inférieurs aux conséquences financières de ces attaques.

Pourquoi êtes-vous concerné ?

Vous devez être conscient que protéger votre entreprise et ses actifs est de votre devoir, et que votre responsabilité peut être personnellement engagée (civilement et pénalement).

Quelles sont les catégories de risques ?

Les risques sont classés en quatre grandes catégories. Celles-ci peuvent être découpées en fonction des dix usages détaillés au paragraphe suivant « risques associés aux usages » :

- **Vol d'informations ;**
- **Usurpation d'identité ;**
- **Intrusions et utilisation de ressources systèmes ;**
- **Mise hors service des systèmes et ressources informatiques.**

Quelles sont les conséquences des risques ?

De la perte de temps en passant par la possible perte de confiance des clients et partenaires, une sécurité défaillante peut conduire à :

- **Une perte d'information et de données ;**
- **Une perte d'image ;**
- **Une mise en cause au plan légal ;**
- **Une remise en cause de vos assurances générales de perte d'activité ou spécifiques couvrant le risque de dommage post attaque.**

Selon le Gartner Group, 50 % des PME qui gèrent leur propre sécurité Internet font l'objet d'attaques diverses, et 60 % d'entre elles ignorent qu'elles ont été attaquées.

Quelles sont les conséquences financières directes ?

En France, dans 86 % des cas de sinistres du système d'information, l'impact financier est absorbé par la trésorerie courante de l'entreprise (Source : rapport 2002 du Clusif).

Selon l'étude TNS-Sofres (novembre 2003 et janvier 2004), les attaques virales ont touché 44 % des entreprises dont 50 % ont dû cesser leur activité pendant plusieurs heures (36 % ayant perdu des données).
On distingue trois catégories de coûts directs :

Coûts d'immobilisation

L'arrêt de l'informatique entraîne un ralentissement notable de l'activité, voire la paralysie de l'entreprise.

Coûts du temps passé

Recherche de l'origine de l'attaque, tentatives de réparation en interne, restauration des données, ressaisies de fichiers perdus, réorganisation, etc.

Coûts techniques

Remplacement d'un disque dur de micro-ordinateur, intervention d'un expert pour éradiquer un virus ayant contaminé l'ensemble du réseau, réinstallation d'un programme ou d'un serveur, etc.

Aux États-Unis, selon l'enquête réalisée en 2003 par le CSI (Computer Security Institute) et le FBI, de nombreuses sociétés consultées ont déclaré avoir subi des sinistres avec un impact financier significatif

Sinistre	% entreprises sinistrées *	Impact financier moyen
Usage abusif d'Internet	97 %	93 KUS$
Contamination par virus	90 %	45 KUS$
Vol de PC	69 %	87 KUS$
Accès à des données confidentielles via l'Internet	55 %	143 KUS$
Intrusion des Systèmes d'Information (SI)	31 %	103 KUS$
Vol informatique dans l'entreprise	26 %	1 848 KUS$
Fraude financière	14 %	1 477 KUS$

* Une même société subit généralement différents types de pertes ce qui explique un total supérieur à 100 %.

Les risques sont-ils dépendants des usages ?

Compte tenu de la diversité des risques et des systèmes d'information, il n'y a pas de solution toute faite, mais autant de réponses que d'usages :

- Votre entreprise stocke sur ses systèmes des données confidentielles et stratégiques pour son développement ?

- Vous échangez, via Internet, des données importantes avec vos clients ou prospects (par exemple gestion de commande, ou appel d'offres dématérialisés) en utilisant des moyens tels que mails, transferts de fichiers, site web, connexions Extranet ?

- Vous avez plusieurs établissements interconnectés ?

- Vous avez un site Web connecté ou non à vos systèmes ?

- Vous avez déployé un ou des réseaux Wi-Fi ?

- Vos collaborateurs peuvent consulter ces données depuis l'extérieur via Internet ?

- Vos collaborateurs, nomades ou non, disposent de leur propre connexion Internet par modem tout en étant connectés sur votre réseau ?

- Vos collaborateurs sont équipés de moyens mobiles de présentation et de communication (portables, assistants, tablettes, téléphones mobiles intelligents) ?

Si vous avez répondu OUI à au moins une de ces questions sans avoir pris de précautions particulières, vous êtes concernés par ce guide.

Quels sont les risques associés aux usages ?

Les informations détaillées ci-contre vous aideront à mieux cerner les risques associés aux usages. Les fiches associées ont été conçues pour vous permettre d'approfondir les solutions en fonction des risques et des usages.

Fiche 1 (voir page 17)

Point clés : Vous n'avez pas fait l'inventaire des biens à protéger et vous ne connaissez pas vos failles de sécurité éventuelles.

Votre sécurité n'est pas abordée comme un projet appelé « Politique de sécurité ». Vos actions ne sont pas coordonnées et suivies. Une politique de sécurité est illusoire sans évaluation régulière contre les nouvelles menaces et les changements d'organisation de l'entreprise.

Solution : Bâtir une politique de sécurité :

- Identifier et faire l'estimation des biens à protéger.
- Évaluer les usages Internet de l'entreprise et les risques associés.
- Sensibiliser vos salariés au respect des règles de base.
- Faire un état des lieux.
- Bâtir la politique de sécurité.

Fiche 2 (voir page 19)

Point clés : Vous n'avez pas connaissance de vos obligations légales.

Pourtant les lois, règlements et accords professionnels sont contraignants et peuvent engager votre responsabilité personnelle :

- Dommages causés aux tiers (responsabilité de l'employeur engagée du fait de son salarié en cas par exemple de consultation d'un site illicite, de violation du droit d'auteur, de fraude informatique).
- Dommages causés à l'entreprise (atteinte à la confidentialité ou modification des données comptables).

Solution : Connaître la législation en vigueur et la jurisprudence :

- Quel est le régime général de responsabilité qui vous est applicable ?
- Quelles sont les règles à respecter concernant l'utilisation des moyens de communication électronique ?
- Quelles sont les règles concernant les contenus informationnels ?
- Quelle est la responsabilité du chef d'entreprise quant à son activité sur l'Internet ?
- Alerter et déposer plainte.

Fiche 3 (voir page 22)

Point clés : Vos données confidentielles peuvent être interceptées.

Vos systèmes d'information et vos applications évoluent avec votre activité. Votre personnel change de fonction, de responsabilités. Dans chaque entreprise même non informatisée, il existe un accès différencié à l'information en fonction des niveaux de responsabilité des collaborateurs. Vous gérez les entrées et sorties au plan administratif, mais pensez-vous à changer vos mots de passe lorsqu'un collaborateur vous quitte, et plus encore lui avez-vous supprimé sa connexion/son mot de passe ? A défaut d'une bonne gestion des moyens d'identification et de sécurisation des échanges, les données sensibles (comptabilité, paye, fichier client et prospect, brevets, plans, …) peuvent être accessibles par des personnes non autorisées ayant accès au réseau en interne ou en externe.

Solution : Mettre en œuvre des moyens appropriés à la confidentialité des données :

- Contrôler l'accès aux données et applications (identification).
- Sécuriser les échanges sur Internet (protocoles sécurisés).
- Sécuriser les échanges de données confidentielles.
- Notions de base sur les certificats, la signature électronique et le chiffrement.

Fiche 4 (voir page 25)
Point clés : Vous n'avez pas associé vos collaborateurs à votre projet « Politique de sécurité ».
Vos collaborateurs ne peuvent adhérer au respect des règles de bonne conduite, sous la forme d'une charte d'utilisation. La plus grande partie des brèches de sécurité sont ouvertes par le fait des salariés, souvent par manque de formation/sensibilisation, quelquefois par intention frauduleuse. L'activité frauduleuse d'un pirate informatique peut être facilitée par une action préalable dite d'« ingénierie sociale » consistant à se présenter à vos salariés sous une fausse identité pour obtenir des informations confidentielles.
Solution : Sensibiliser vos salariés :
- Les 3 règles d'or de l'utilisateur formé.
- Mise en œuvre des 3 règles par la Charte d'Utilisation. Contenu et cadre juridique de la charte.

Fiche 5 (voir page 28)
Point clés : Vous n'avez pas prévu de plan de reprise d'activité, de plan de sauvegarde.
Pourtant une entreprise peut tarder à s'apercevoir que certaines données ont été corrompues, accidentellement, intentionnellement. Le temps perdu à reconstituer les données excèdera largement l'investissement dans la mise en œuvre de sauvegardes.
Solution : Mettre en œuvre un plan de sauvegarde :
- Politique de sauvegarde.
- Procédures de sauvegarde.
- Procédures de restauration.
- Maintenir la politique de sauvegarde.

Fiche 6 (voir page 30)
Point clés : Vous n'avez pas mis en œuvre les moyens minimums de sécurité.
Pourtant l'ordinateur utilisé pour se connecter est identifié par un numéro unique (adresse IP) et peut être vulnérable. Vous êtes visible depuis le monde Internet. Vous devenez une cible sans le savoir pour des attaques virales généralisées (virus, vers, spyware), et pour des attaques ciblées par un pirate informatique. Vos systèmes, sous contrôle de tiers, deviennent le réceptacle de « chevaux de Troie » qui serviront à neutraliser votre site, à pénétrer vos données, ou à utiliser vos systèmes pour attaquer des tiers vous mettant en situation légalement dangereuse.
Solution : Mettre en œuvre des moyens de défense minimums :
- Bloquer les attaques automatisées.
- Limiter les brèches ouvertes.
- Limiter la prolifération virale.
- Détecter les anomalies.

Fiche 7 (voir page 33)
Point clés : Vous avez déployé des connexions sans fil (connexions Wi-Fi, bientôt Wi-Max, liaisons Bluetooth, postes nomades…).
Ce mode de connexion, pourtant bien pratique, est susceptible, si aucune précaution supplémentaire n'est prise, de permettre un piratage beaucoup plus facile des informations que vous échangez.
Solution : Mettre en œuvre des moyens de défense minimums pour les connexions sans fil :
- Particularité des réseaux sans fil.
- Huit moyens de défense adaptés.

Fiche 8 (voir page 36)
Point clés : Vous n'avez pas envisagé de précautions supplémentaires lors de la mise en place d'un site Web ou de procédures de télétravail.
Pourtant un site web vous rend très visible depuis l'extérieur et vous expose à la curiosité. Votre site est un moyen d'échange. Le serveur Web est connecté à vos systèmes internes après filtrage par le pare-feu. Les pirates disposent d'outils sophistiqués (mais accessibles sur le Web) ou très simples pour tester vos moyens de défense et la faiblesse de vos applications. Si vos collaborateurs travaillent à distance et se connectent à vos systèmes internes, sans précautions supplémentaires, ils peuvent mettre en péril la confidentialité de vos données.
Solution : Établir une barrière entre les données externes et internes :
- Deux usages.
- Trois moyens de protection supplémentaires.

Fiche 9 (voir page 38)
Point clés : Vous pensez peut-être que la sécurité est établie une fois pour toutes.
Le défaut de maintenance est aussi dangereux que l'inconscience car il peut créer un sentiment de fausse sécurité.
Solution : Gérer et maintenir les politiques de sécurité :
- Les risques liés au changement.
- Maintenance minimum.
- Moyens.

Fiche 10 (voir page 39)
Point clés : Vous manquez de ressources en interne.
Vous considérez que la sécurité des systèmes d'information n'est pas votre métier et vous ne connaissez pas les opportunités et les risques de la sous-traitance.
Vous craignez de ne pouvoir y consacrer suffisamment de ressources et que par la suite la sécurité ne soit qu'illusoire (installer un pare-feu, un antivirus sans les maintenir pendant que vos structures évoluent et que les menaces se renouvellent sans cesse).
Solution : Externaliser la mise en œuvre et la maintenance de la politique de sécurité :
- Installation et configuration.
- Maintenance sur site.
- Externalisation.
- Les 10 points clé d'un contrat d'externalisation.

Combien ça coûte ?

La réussite de mise en place d'une politique de sécurité repose sur un équilibre entre les coûts des moyens mis en œuvre et les bénéfices obtenus. Le coût de mise en œuvre d'une politique de sécurité est extrêmement variable et peu de données comparatives sont disponibles.

Dans certains cas le coût peut être relativement bas pour un niveau de protection minimum. Par exemple, les mises à jour de sécurité de votre système d'exploitation sont en général gratuites ; les coûts d'un antivirus (attention à bien effectuer les mises à jour), anti-spam, pare feu de bonne qualité (attention à bien le faire configurer) sont à la portée de tous (jusqu'à quelques milliers d'euros).

Mais ce niveau minimum se révèlera rapidement insuffisant si vous souhaitez mettre en place un niveau d'authentification pour l'accès aux données sensibles de votre entreprise (liste et usages des clients, propositions concurrentielles, prospects, brevets, etc.).

Dans d'autres cas, si vous disposez par exemple de votre propre site web et qu'il communique avec vos données internes (par exemple par le biais de formulaires que vous demandez à vos prospects de remplir), la mise en œuvre d'une politique de sécurité peut se révéler plus complexe et donc plus coûteuse (quelques dizaines de milliers d'euros).

L'ordre de grandeur de cet investissement peut être mis en regard des coûts que pourrait vous causer une attaque aux biens matériels de l'entreprise (données à ressaisir, bases de données à reconstruire, applications à redéployer, …) et/ou aux biens immatériels (image, perte de confiance des clients ou perte de productivité des salariés).

L'investissement est préventif selon le même principe qu'une assurance.

La mise en œuvre d'une politique de sécurité peut apparaître comme complexe à certains. Ce guide et ses annexes (accessibles en ligne sur http://www.medef.fr) rend cette « complexité » accessible à chacun de nous et présente des solutions simples pour atteindre, en fonction des usages, un niveau de sécurité minimum.

Protection minimum

Il est de votre responsabilité de garantir un niveau minimum de protection de vos systèmes informatiques.

L'ensemble des actions peut être réalisé par vos soins ou par un prestataire externe (société spécialisée ou opérateur de télécommunications). Il existe des solutions mutualisées très abordables au plan financier.

Ces opérations doivent être réalisées régulièrement :

- certaines à un rythme hebdomadaire (mise à jour des signatures antivirus et des correctifs logiciels de sécurité disponibles, etc.).

- et d'autres au minimum tous les trimestres (vérification des versions du moteur antivirus, vérification des vulnérabilités, application de la politique de sécurité, configuration des firewalls, mise à jour du plan de sécurité, etc).

Recommandations

Mettre à jour régulièrement vos logiciels en téléchargeant les correctifs depuis le site de votre fournisseur, et vérifier (ou faire vérifier) régulièrement l'état des vulnérabilités potentielles de vos logiciels.
A titre d'exemple, sur 4.240.883 vérifications réalisées, 19 % des sites sont vulnérables (mises à jour non faites) et donc exposés à une attaque ayant 100 % de chance de réussite.

Installer sur chaque machine un antivirus et faire régulièrement les mises à jour intégrées au contrat de maintenance (couvrant en général une durée d'un an).
A titre d'exemple, sur 4.240.883 vérifications réalisées, 25 % des sites vérifiés ne sont pas protégés par un antivirus et 9 % des sites protégés par un antivirus n'ont pas une version à jour.

Veiller au strict respect de la confidentialité des identifications et authentifications.
A titre d'exemple, en 2004, 50 % des collaborateurs des entreprises françaises écrivent les mots de passe et 35 % les communiquent à un tiers.

Installer et configurer au moins sur chaque machine un « firewall » logiciel.
Si besoin (voir usages), installer et bien configurer un pare-feu sur le périmètre externe voire installer un pare-feu réseau (pour les applications).

Définir un plan de sauvegarde des données sensibles et/ou stratégiques de l'entreprise.

Sites et adresses utiles

Sites gouvernementaux

http://www.premier-ministre.gouv.fr
le site du Premier Ministre.

http://www.ssi.gouv.fr/fr/dcssi/
la Direction Centrale de la Sécurité des Systèmes d'Information, site thématique institutionnel du Secrétariat Général de la Défense Nationale (SGDN).

http://www.service-public.gouv.fr
le portail de l'administration française.

http://www.ladocfrancaise.gouv.fr
la direction de la documentation française.

http://www.legifrance.gouv.fr
l'essentiel du droit français.

http://www.internet.gouv.fr
le site du SIG (Service d'information du Gouvernement) à propos de l'entrée de la France dans la société de l'information.

http://www.adae.pm.gouv.fr
l'Agence pour le Développement de l'Administration Électronique.

http://www.telecom.gouv.fr
le site de la direction ministérielle chargée des télécommunications.

http://www.interieur.gouv.fr
l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.

http://www.cases.lu
site du Ministère de l'Économie et du Commerce Extérieur du Luxembourg, dédié à la sensibilisation aux risques informatiques et à la prévention de ces derniers.

Organismes publics ou privés

http://www.cnil.fr
la Commission nationale de l'informatique et des libertés.

http://www.renater.fr
le réseau de la Recherche, fournisseur d'accès pour les universités et les pouvoirs publics.

http://www.urec.cnrs.fr
l'unité réseau du CNRS.

http://www.cnrs.fr
le site du CNRS

http://www.clusif.asso.fr
le club de la sécurité des systèmes d'information français.

http://www.ossir.org
l'Observatoire de la sécurité des systèmes d'information et des réseaux.

http://www.afnor.fr
l'Association Française pour la Normalisation.

http://www.cigref.fr
le Club informatique des Grandes Entreprises Françaises.

http://www.adit.fr
l'Association pour la Diffusion de l'Informatique Technique.

http://www.medef.fr
le site du MEDEF où se trouve ce guide, les 10 fiches associées et le glossaire.

http://www.foruminternet.org
espace d'information et de débat sur le droit de l'Internet.

http://www.cert@cert-ist.com
le CERT-IST recueille et diffuse les alertes pour les entreprises de l'industrie des services et du tertiaire.

OCLCTIC
(Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication)
Compétence nationale :
11, rue des Saussaies - 75800 Paris
Tél. : 01 49 27 49 27 - Fax : 01 49 97 80 80

BEFTI
(Brigade d'enquêtes sur les Fraudes aux Technologies de l'Information)
Compétence sur Paris et la petite couronne :
163 avenue d'Italie - 75 013 Paris
Tél. : 01 40 79 67 50

Contributeurs

Ce guide a été rédigé par le groupe de travail Sécurité des Systèmes d'Information du MEDEF, présidé par Daniel Thébault, président d'Aliacom, président du MEDEF Midi-Pyrénées et membre du Conseil Exécutif du MEDEF.

Le rapporteur du groupe de travail est Catherine Gabay, directeur Recherche - Innovation - Nouvelles Technologies du MEDEF.

Ce groupe de travail fait partie du Comité Économie Électronique du MEDEF, présidé par Philippe Lemoine, président de LASER.

Ce Comité fait lui-même partie de la Commission Innovation – Recherche – Nouvelles Technologies du MEDEF, présidé par Charles Beigbeder, président de Poweo et membre du Conseil Exécutif du MEDEF.

Le groupe de travail est composé des sociétés et associations suivantes listées dans l'ordre alphabétique. Les contributions de leurs représentants, indiqués entre parenthèses, sont vivement remerciées.

ACE Europe (Luc Vignancour), ACFCI (Wanda Egger), AchatPublic (Dimitri Mouton), Adentis (Stéphane Madrange, AFNET (Youval Eched), Alcatel (Jean-Paul Bonnet), Aliacom (Daniel Thébault), Alliance TICS (Jean-Patrice Savereux), Altran (Vincent Iacolare), Axalto (Xavier Passard, Olivier Piou), Cabinet Alain Bensoussan (Benoit Louvet), Cabinet Caprioli et associés (Pascal Agosti, Eric Caprioli), Cabinet Itéanu (Olivier Itéanu), Cabinet S Soubelet (Sophie Soubelet-Caroit), Caisse d'Epargne (Jérôme Fanouillère), Cigref (Jean-François Pépin, Stéphane Rouhier), Cisco (Philippe Cunningham), Clusif (Julien Airaud, Marie-Agnès Couwez, Pascal Lointier), CNIL (Yann le Hegarat, Laurent Lim, Norbert Fort), Compuserve (Gérard Ollivier), EADS (Jean-Pierre Quemard, Gilles Robine), EDS (Etienne Busnel, Robert Stakowski), ENST (Michel Riguidel), e-MYP (Yves Léon), FFA (Bernard Bertier), FIEEC (Eric Jourde), Flowmaster (Marie-Christine Oghly), France Télécom (Philippe Bertran, Francis Bruckmann, Sylvie Burgelin, Philippe Duluc), Francis Behr, Gixel (Isabelle Boistard), Hervé Schauer Consultants (Hervé Schauer), HP France (Christophe Stener), IPP Technologies (B. Pourcines), La Poste (Monique Cosson, Brice Welti), Laser (Isabelle Felix, Philippe Lemoine), Lucent Technologie (Yannick Bourque, Alain Viallix), MEDEF (Eric Ingargiola, Richard Pernod, Philippe Dougier, Catherine Gabay), MEDEF Moselle (Gérard Pacary), MEDEF Périgord (Valérie Sibileau), Microsoft (Thaima Samman, Stéphane Senacq, Bernard Ourghanlian, Cyril Voisin), MINEFI/DiGITIP (Mireille Campana, Frédéric Tatout), MINEFI/HFD (Didier Lallemand, Jean-François Pacault, Daniel Hadot), NetSAS (Philippe Eyries), Pompiers de Paris (Gilles Berthelot), Qualiflow (C-P Jacquemin), Réseau Echangeur (Cécile Alvergnat), SAGEM (Nicolas Goniak), Secrétariat Général de la Défense Nationale (Henri Serres, Christophe Marnat, Stéphane Miège, Anne-Valérie Poteau), SFIB (Xavier Autexier, Benoit Le Mintier de Lehellec), Simavelec (Bernard Heger), Stéria (Eric Hayat, Thierry Harle), Société Générale (François Coupez), Sonilog (Aïda Demdoum), Supelec (Alain Bravo), Syntec Informatique (Sandra Oget, Pierre Dellis, Franck Populaire, Jean-Paul Eybert), Thalès (Henry Chaignot), UNIFA (Sandrine Puig-Roger), Université Paris 1 (Georges Chatillon).

Le Comité Économie Électronique du MEDEF tient à remercier plus particulièrement **Philippe Eyries** (NetSAS), **Vincent Iacolare** (Altran), **Francis Bruckmann** (France Télécom), **Jean-Pierre Quemard et Gilles Robine** (EADS), **Youval Eched** (Afnet), **Yann le Hegarat** (CNIL), **Benoît Louvet** (Cabinet Alain Bensoussan), **Cyril Voisin** (Microsoft), **Sophie Soubelet-Caroit** (Cabinet Soubelet-Caroit), **Pascal Agosti** (Cabinet Caprioli et Associés), **Sandra Oget** (Syntec Informatique), **Stéphane Madrange** (MEDEF Hauts de Seine Nord et Adentis) pour leur contribution exceptionnelle à la réalisation de ce guide et de ses annexes.

Lexique des principaux termes utilisés

Antivirus
Utilitaire capable de rechercher et d'éliminer les virus informatiques et autres « malwares ». La détection se fait par analyse de la signature des virus connus, ou par analyse heuristique de détection des virus inconnus à partir de leur logique de programmation ou comportement à l'exécution.

Authentification
Vérification visant à renforcer selon le besoin, le niveau de confiance entre l'identifiant et la personne associée (exemples : le mot de passe est un authentifiant faible, la carte à puce est un authentifiant fort…).

Chiffrement (Encryption)
Mécanisme de sécurité permettant d'assurer la confidentialité des données.

Clé (Key)
Elément sur lequel repose le secret, permettant de chiffrer et de déchiffrer un message. Il existe des clés secrètes (utilisées par les algorithmes symétriques, avec clés de chiffrement et de déchiffrement identiques) et des jeux de clés privée/publique (utilisées par les algorithmes asymétriques, avec clés distinctes).

Déni de service (DoS)
Attaque ayant pour but de bloquer le fonctionnement de machines ou de services, par saturation d'une ressource.

Faille de sécurité
Défaut dans un programme. Les « hackers » et/ou pirates informatiques et/ou « script kiddies » qui les découvrent peuvent créer des virus exploitant ces failles pour pirater un ordinateur.

Internet
Réseau interconnectant la plupart des pays du monde, indépendant du type de machine, du système d'exploitation et du support de transport physique utilisé.

Intrusion
Pénétration non autorisée d'un système ou d'un réseau, ayant pour but la compromission de l'intégrité, la confidentialité ou la disponibilité d'une ressource.

IP (Internet Protocol)
Protocole d'échange d'informations, dont l'usage s'est généralisé sur le réseau Internet et les réseaux d'entreprises.

IPsec (IP Security Protocol)
Protocole de sécurisation des échanges sur réseau IP, par établissement de tunnels, authentification mutuelle et chiffrement des données.

LAN
Réseau local interconnectant des équipements informatiques (ordinateurs, serveurs, terminaux…) dans un domaine géographique privé et limité, afin de constituer un système cohérent.

Log
Fichier texte tenu à jour par un serveur, dans lequel il note les paramètres liés à chaque connexion.

Pare-feu (Firewall)
Dispositif installé à une frontière du réseau, qui protège le réseau interne vis-à-vis de l'extérieur et interdit le trafic non autorisé de l'intérieur vers l'extérieur. Il assure les fonctions de passerelles applicatives (Proxy), d'authentification des appels entrants, d'audit et d'enregistrement de ces appels (log).

Pirate (Cracker/Hacker)
Terme générique désignant celui qui « craque » ou attente à l'intégrité d'un système informatique, de la simple duplication de données à l'accès aux ressources d'un centre de calcul (vol de programmes, de fichiers, …).

Pot de miel (Honeypot)
Serveur ou programme volontairement vulnérable, destiné à attirer et à piéger les pirates. Cet appât fait croire aux intrus qu'ils se trouvent sur une machine de production normale alors qu'ils évoluent dans un leurre.

Proxy
Service qui partitionne la communication entre le client et le serveur en établissant un premier circuit entre le client et le firewall, et un deuxième entre ce dernier et le serveur (Internet).

RPV (VPN)
Réseau privé d'entreprise multi sites utilisant les réseaux d'opérateur pour leur interconnexion.

SLA (Service level agreements)
Engagements de la part du fournisseur sur la qualité du service fourni. Ils déterminent le niveau d'indemnisation du client en cas de non atteinte d'un niveau minimum de disponibilité de service.

Signature électronique
Transformation électronique permettant d'assurer l'authentification du signataire et éventuellement celle d'un document signé par lui. Une signature numérique fournit donc les services d'authentification de l'origine des données, d'intégrité des données et de non répudiation.

Spam
Message intempestif envoyé à une personne ou à un groupe de personnes. Il faut prendre l'habitude de supprimer ce genre de messages sans les lire et sans cliquer sur aucun lien.

SSL (Secure Socket Layer)
Protocole de sécurisation des échanges sur Internet, intégré dans tous les navigateurs récents. Il assure authentification, intégrité et confidentialité.

Système d'information (SI)
Ensemble d'entités organisé pour accomplir des fonctions de traitement d'information.

Tiers de certification
Organisme chargé de gérer et de délivrer les clés publiques avec la garantie qu'elles appartiennent bien à leurs possesseurs reconnus.

Tiers de confiance
Organisme chargé de maintenir et de gérer, dans le respect des droits des utilisateurs, les clés de chiffrement ou d'authentification. Les tiers de confiance peuvent être des tiers de certification ou des tiers de séquestre.

Virus
Programme qui se répand à travers les ordinateurs et le réseau et qui est conçu pour s'auto-répliquer Les virus contiennent souvent des « charges », actions que le virus réalise séparément de sa réplication.

Vulnérabilité
Faiblesse d'une ressource d'information qui peut être exploitée par une ou plusieurs menaces.

Zone démilitarisée (DMZ : Demilitarized Zone)
Une DMZ contient un ou plusieurs services accessibles par Internet tout en interdisant l'accès au réseau privé.

WLAN (Wireless LAN)
Réseaux locaux sans fils, normalisés sous la référence IEEE 802.11.

Fiches

Fiche 1

Bâtir une politique de sécurité

Une politique de sécurité est un ensemble, formalisé dans un document applicable, d'éléments stratégiques, de directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du (des) système(s) d'information de l'organisme. Bâtir une politique de sécurité est un projet à long terme visant à mettre en œuvre une sécurité adaptée aux usages, économiquement viable et conforme à la législation en vigueur.

Le plus souvent, il s'agira de bâtir une politique de sécurité prenant en compte les risques aussi bien internes qu'externes, ainsi que la typologie du système d'information, la sécurité devant prendre en compte la spécificité de chaque type de communication. Avant tout, il conviendra de répondre à ces trois questions :
- Que dois-je protéger en priorité ? Quel est mon patrimoine informationnel ?
- Quels sont les risques que je cours (externes, internes) ?
- Quels sont les facteurs aggravants de ces risques ?

Que dois-je protéger ? Quel est mon patrimoine informationnel ?

Un État des lieux pour bâtir une politique de sécurité adaptée aux usages. Du réseau au contenu, en passant par les systèmes et les applications, la segmentation de la sécurité en fonction des usages, des risques potentiels et des composantes impliquées est la seule démarche qui garantisse la sécurité globale pour l'entreprise.

Pour bâtir une politique de sécurité adaptée aux besoins et usages, il faut, chronologiquement :

Identifier les biens à protéger

- **Les biens matériels et logiciels** : Les serveurs et les postes de travail (fixes et nomades), les équipements d'interconnexions (routeurs, commutateurs, modems), leur localisation ou leur titulaire, le type et la version des logiciels installés.

- **Les données sensibles** de l'entreprise (procédés de fabrication, codes sources, données commerciales et administratives, …)

- **Les services et applications** : Applications métiers internes et externes communiquant avec le monde extérieur (fournisseurs, site de commerce électronique), applications de gestion. Attention aux services et applications obsolètes et non maintenues mais toujours résidentes.

Découvrir les réseaux

Il s'agit de découvrir les interactions des différents matériels/logiciels (entre eux et avec le monde extérieur), d'identifier les vulnérabilités pouvant les affecter, d'identifier les applications qui résident dans les systèmes et qui transitent par le réseau. Cette phase permet, en outre, de comparer l'existant réel avec l'inventaire précédent.

- **Étape 1** : Lister les moyens d'accès au « réseau de l'entreprise » depuis « le monde extérieur ». Un point d'entrée unique (passerelle d'accès Internet) est plus facile à sécuriser mais il convient de porter une attention particulière aux diverses connexions établies temporairement en dehors de l'entreprise avec des équipements nomades, aux modems individuels (permettant la connexion directe à Internet en contournant les sécurités du point d'entrée principal) et aux réseaux locaux sans fils dont le périmètre d'écoute dépasse l'enceinte physique de l'entreprise.

- **Étape 2** : Détecter les vulnérabilités des systèmes et applications (outil ou service en ligne – voir fiche 6).

- **Étape 3** : Identifier les flux applicatifs circulant à l'intérieur du réseau de l'entreprise (applications métiers, gestion des stocks, paie…) et ceux communiquant avec le monde extérieur (messagerie, commerce en ligne, échanges

avec des partenaires, …). Cette étape permettra de découvrir l'usage des réseaux (internes ou externes) et de leur bande passante. Elle permettra aussi de découvrir comment les collaborateurs de l'entreprise utilisent les ressources mises à leur disposition pour remplir leurs tâches. Les outils d'analyse de flux utilisés seront par ailleurs très utiles pour détecter les applications (parfois non souhaitées) et juger de leur importance par le volume de leurs flux. Ils permettront aussi de faire le point sur la politique d'accès aux données (connexion et mot de passe par exemple) et de réfléchir à la mise en œuvre de moyens plus sophistiqués (authentification forte, chiffrement) pour les données les plus sensibles.

Quels sont les risques externes ?

Attaques non ciblées

Toutes les entreprises sont concernées par la propagation des virus (ou vers) ou les attaques distribuées (déni de service) dont l'objectif est la prise de contrôle d'une machine pour l'utiliser à une attaque d'un site tiers.

Attaques ciblées

La probabilité de risque physique (vol ou destruction de matériel) et de risque logique (attaques distantes et ciblées pour veille, vol ou destruction) augmente avec la visibilité et les facteurs aggravants.

Quels sont les risques internes ?

La sécurité doit impérativement impliquer tous les collaborateurs qu'il faut former à la mise en œuvre des politiques de sécurité, car les plus grandes menaces pour la sécurité informatique des entreprises viennent des utilisateurs eux-mêmes.

Quels sont les facteurs aggravants de ces risques ?

Nomadisme et nouvelles technologies

Postes et équipements nomades (assistants numériques de poche, téléphones évolués, portables et autres PDA/Smart phones, réseaux sans fil).

Infrastructures, services et applications mal protégées

Serveurs et postes de travail non mis à jour (« non patchés ») et donc vulnérables, site web mal conçu, messagerie non protégée.

Plan de sauvegarde inexistant ou incomplet

L'approche des politiques de sécurité par segmentation

La connaissance acquise au cours de ces phases de découverte et d'inventaire permettra d'élaborer une politique de sécurité pour déployer les moyens de protection adaptés aux usages. La segmentation est la base des politiques de sécurité :

Réseau

La sécurité commence avec le contrôle d'accès appliquant une politique de sécurité personnalisée par site et par groupe de population, pouvant se compléter par une authentification simple ou renforcée.

Système

Les systèmes peuvent être hétérogènes ce qui complexifie leur gestion et leur mise à jour. Par ailleurs, la publication régulière de nouvelles vulnérabilités crée un risque permanent.

Application

Une application Web ouverte, par nature, au monde extérieur présente plus de risques potentiels qu'une application propriétaire (paie, comptabilité, gestion stock, client…) utilisée par une population limitée.

Contenu

La protection du contenu (fichier de données, image ou texte, programme exécutable, pièce jointe…) doit tenir compte de sa dangerosité potentielle, de sa confidentialité pour l'entreprise et des obligations légales.

Comme il est difficile de tout prévoir, faute de temps et de moyens, il conviendra au minimum de prévoir des sauvegardes et peut-être de considérer une couverture complémentaire pour les dommages résultant des attaques. Souscrire une assurance informatique impose de toutes façons un niveau de sécurité minimum.

La mise en œuvre

Plusieurs possibilités

- **Mise en œuvre par des ressources internes** avec acquisition des outils.

- **Sous-traitance** à un prestataire de service informatique qui pourra utiliser ses propres outils. Il faudra prévoir de le faire revenir régulièrement car les menaces évoluent sans cesse.

- **Utilisation des services mutualisés à distance** par des MSSP (« Managed Security Service Providers ») pour les tests de vulnérabilités, la découverte de vos flux applicatifs, la gestion des moyens de protection (équipements filtrants et antivirus) et la gestion des identifications/authentifications.

Fiche 2

Connaître la législation en vigueur et la jurisprudence

Quel est le régime général de responsabilité applicable ?

La responsabilité civile de l'entreprise (art. 1384 alinéa 5 du code civil)

L'employeur est civilement responsable du fait de l'activité de ses préposés, notamment en cas d'utilisation malveillante des moyens informatiques et de communications électroniques (ex : messagerie, forums).

La responsabilité pénale de l'entreprise

L'employeur peut être pénalement responsable du fait de ses préposés dès lors qu'ils commettent des infractions susceptibles d'engager la responsabilité pénale des personnes morales (ex : atteinte aux systèmes de traitement automatisé de données, contrefaçon…) et qu'elles ont été commises pour le compte de l'entreprise par ses « organes ou représentants » (article L. 121-2 du code pénal).

Quelles sont les règles concernant les contenus informationnels ?

Les règles en matière de données personnelles

La loi Informatique et Libertés du 6 janvier 1978 impose au chef d'entreprise de prendre le plus grand soin des données personnelles collectées auprès de clients comme de salariés. De façon générale, les droits garantis des personnes dont les données sont traitées sont :

- Le **droit à l'information préalable**

- Le **droit d'accès** aux données traitées qui les concernent

- Le **droit de rectification** de ces données

- Le **droit de s'opposer au traitement** de ces données (collecte, utilisation, diffusion)

Sauf cas particuliers, le chef d'entreprise a l'obligation d'effectuer une déclaration préalable de ces traitements auprès de la CNIL.

L'article 34 de la loi du 6 janvier 1978 précise que le responsable du traitement est tenu de prendre *« toutes précautions utiles »* pour protéger les données à caractère personnel sous sa responsabilité, notamment, pour *« empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès »*.

S'il ne respecte pas ces obligations, le chef d'entreprise s'expose à des sanctions pénales (art 226-16 à 226-24 du code pénal) et civiles.

Les reproductions ou représentations non autorisées d'un contenu informationnel protégé

La responsabilité du chef d'entreprise peut également être engagée si ses préposés utilisent dans le cadre de leur mission des logiciels « piratés ». De même, la responsabilité du chef d'entreprise peut être engagée dans l'éventualité où ses préposés utiliseraient les ressources informatiques de l'entreprise pour stocker et/ou rendre accessibles des contenus protégés (logiciels, musiques, films etc.).

Le secret des correspondances privées

Le chef d'entreprise doit veiller au respect du secret des correspondances privées, électroniques ou non au sein de son entreprise.

Précaution recommandée

Le chef d'entreprise doit prendre les plus grandes précautions en matière de surveillance par la mise en place d'une charte d'utilisation des moyens informatiques et des communications électroniques (voir fiche 4 et rapport Cyber-Surveillance sur les lieux de travail www.cnil.fr).

Quelle est la responsabilité du chef d'entreprise quant à son activité sur l'Internet ?

Identification de l'entreprise sur son site Internet

Sous peine de sanction pénale, le cybercommerçant est tenu d'assurer la mise à disposition du public d'« un accès facile, direct et permanent utilisant un standard ouvert », aux informations suivantes :

- **Coordonnées de l'entreprise et de ses responsables** : sa dénomination ou raison sociale ; l'adresse de son siège social ; un numéro de téléphone et une adresse de courrier électronique où il est possible de joindre la société ; son numéro d'inscription au registre du commerce ; son capital social ; le nom du directeur de la publication ; information sur les prix (frais de livraison) ;

- **Coordonnées du prestataire hébergeant le site sur l'Internet** : raison sociale, adresse et numéro de téléphone (ou mention que le site est hébergé sur les propres serveurs de l'entreprise) ;

- **Taxe sur la valeur ajoutée** : numéro individuel en application de l'article 286 ter du code général des impôts, numéro individuel d'identification ;

- **Profession réglementée** : la référence aux règles professionnelles applicables, son titre professionnel, l'Etat membre dans lequel il a été octroyé ainsi que le nom de l'ordre ou de l'organisme professionnel auprès duquel elle est inscrite ; si son activité est soumise à un régime d'autorisation, le nom et l'adresse de l'autorité ayant délivré celle-ci.

La publicité par voie de courrier électronique doit être identifiée

Le titre du message doit suggérer son caractère publicitaire, l'identité de la société émettrice doit être indiquée, le destinataire du message doit disposer de la possibilité effective de s'opposer à l'avenir à la réception de tels messages (droit d'opposition ou opt-out). L'entrepreneur en ligne doit recueillir le consentement préalable (opt-in) des personnes physiques qu'il compte prospecter directement par systèmes automatisés d'appel, télécopieurs ou messages électroniques sauf exceptions posées par la loi. Tout manquement au consentement préalable peut être pénalement sanctionné (à l'heure actuelle [juin 2005], 750 EUR d'amende par message).

La conclusion de contrats en ligne est soumise à l'article 1369-1 et suivants du Code civil

- L'offre doit présenter les étapes à suivre pour la conclusion du contrat ;

- L'offre doit préciser si le contrat est archivé et accessible après sa conclusion ;

- L'offre doit fournir les moyens de corriger les erreurs commises dans la saisie des données ;

- L'offre doit indiquer les langues proposées pour la conclusion du contrat ;

- L'offre doit préciser les règles professionnelles auxquelles l'auteur de l'offre entend se soumettre.

L'acceptation de l'offre par le client se manifeste par un geste électronique (le clic) ou par l'utilisation d'un procédé de signature électronique au sens de l'article 1316-4 du Code civil. Le législateur a posé une présomption de responsabilité à l'égard du commerçant en ligne concernant la bonne exécution des obligations résultant du contrat.

Que faire en cas d'attaque ?

L'entreprise peut être victime d'une « attaque » contre son système d'information (voir Guide et fiche 1).

Elle doit en ce cas :

Prendre toutes les mesures permettrant de conserver la preuve des faits dont elle est victime

- faire une copie physique du disque dur concerné (image) qui sera stockée sur un support différent ; isoler sur un autre support le fichier de journalisation (log) concerné, si possible après l'avoir daté et signé électroniquement ;
- faire procéder à un constat des opérations effectuées par un huissier de justice.

Alerter les instances de sécurité des réseaux

- Informer le CERT-IST
  (le CERT-IST recueille et diffuse les alertes
  pour les entreprises de l'industrie
  des services et du tertiaire)
  9, rue du Président Allende - 94 526 Gentilly Cedex
  Tél. : 05 34 35 33 88 - Fax : 05 34 35 33 89
  cert@cert-ist.com

- L'utilisation d'Internet ou l'attaque d'un système d'information à des fins d'espionnage, de terrorisme ou de pillage du patrimoine économique est de la compétence de la DST (Direction de la Surveillance du Territoire). Une cellule spécialisée dans cette criminalité informatique peut être jointe au 01 40 57 99 42.

Déposer une plainte pénale

- Des dispositions du Code pénal (articles 323-1 et 323-7) sanctionnent les atteintes aux systèmes de traitement automatisé de données (STAD) telles que par exemple l'intrusion dans le système d'information, l'altération de son fonctionnement…

- Prendre contact avec le **SRPJ** ou la **brigade de Gendarmerie** du lieu des faits objets de la plainte (par exemple lieu du serveur attaqué) ;

  ou **l'OCLCTIC** : (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication)
  Compétence nationale :
  11, rue des Saussaies - 75800 Paris
  Tél. : 01 49 27 49 27 - Fax : 01 49 97 80 80 ;

  ou le **BEFTI** : (Brigade d'enquêtes sur les Fraudes aux Technologies de l'Information)
  Compétence sur Paris et la petite couronne :
  163, avenue d'Italie - 75013 Paris
  Tél. : 01 40 79 67 50

Quelles sont les exigences de la loi de sécurité financière du 1er août 2003 (LSF) en matière de sécurité des systèmes d'information des entreprises ?

La LSF a introduit dans le code de commerce les articles L. 225-37 et L. 225-68 qui prévoient pour les sociétés anonymes, que leur président du conseil d'administration ou du conseil de surveillance doit rendre compte dans un rapport spécifique *« des conditions de préparation et d'organisation des travaux du conseil ainsi que des procédures de contrôle interne mises en place par la société »*.

Ce rapport annuel devra notamment exposer les procédures de contrôle interne concernant la sécurité du système d'information de l'entreprise, garantie notamment de l'intégrité des informations comptables qu'il traite. Aux termes de l'article L. 225-235 du code de commerce, le commissaire aux comptes devra, quant à lui, dans un rapport distinct de son rapport de certification des comptes annuels, présenter ses observations sur *« les procédures de contrôle interne qui sont relatives à l'élaboration et au traitement de l'information comptable et financière »* décrites dans le rapport spécifique du chef d'entreprise.

Il est à noter que des mesures du même ordre sont également prescrites par la loi américaine Sarbanes-Oxley du 29 août 2002 mais ne concerne que les entreprises cotées aux États-Unis.

Fiche 3

Mettre en œuvre des moyens appropriés à la confidentialité des données

Pour rappel, 80 % des dommages au patrimoine informatique ou informationnel de l'entreprise proviennent de malveillances internes, volontaires ou non. Certaines de vos données électroniques sont sensibles et font partie du patrimoine immatériel de l'entreprise. Elles doivent donc être protégées.

Contrôler l'accès aux données et applications

Identification et Profil

Une organisation des profils utilisateurs et des moyens d'identification de chacun d'entre eux est le minimum obligatoire pour éviter l'accès libre à vos informations (voir risque légal fiche 2).

Droits d'accès

À chaque profil doivent être associés des droits d'accès liés aux prérogatives du salarié. Certaines informations doivent pouvoir être accessibles en lecture seule, d'autres en mise à jour ou suppression selon les responsabilités de chacun.

Mots de Passe

Les mots de passe sont préférentiellement codés sur 8 caractères alphanumériques changés régulièrement (voir fiche 4).

Administration

Pour contrôler l'accès à votre réseau d'entreprise ou à chaque poste de travail, vous aurez recours à un minimum d'administration qui vous permettra, par exemple, de gérer aussi soigneusement les départs de personnels que les entrées (les codes d'accès d'un salarié qui quitte l'entreprise doivent être immédiatement bloqués).

Sécuriser les échanges

Risques

Si vous n'utilisez pas de solutions sécurisées, un tiers malveillant peut utiliser vos données sensibles à des fins frauduleuses et à vos dépens (usurpation d'identité ou de coordonnées bancaires, espionnage industriel…).

Échanges sur Internet

Dans le cadre d'une utilisation « standard » des moyens d'échanges électroniques de données sensibles (votre n° de carte bleue par exemple) la politique minimale des sites consiste à passer du mode standard sur Internet au mode sécurisé. Ce changement est visible par la mention « https » dans votre barre de navigation, accompagnée éventuellement d'un cadenas en bas à droite de votre navigateur. Le protocole https permet de chiffrer l'échange électronique pendant son transfert entre l'expéditeur et le destinataire, empêchant ainsi quiconque de le lire.

Échanges de données critiques et confidentielles (fiscales, juridiques, médicales, etc.) ou liées au secret professionnel

La loi sanctionne la violation du secret professionnel dans le cas où les solutions adéquates n'auraient pas été utilisées :

- La première solution consiste à utiliser des outils de chiffrement intégrés à votre messagerie électronique, couplés avec des certificats. Ces solutions sont peu onéreuses, mais leur mise en œuvre n'est pas aisée et ne vous donne pas de garantie absolue.

- La deuxième solution consiste à utiliser des services de messagerie sécurisée, commercialisés par des sociétés spécialisées. Il est bien entendu conseillé de privilégier les services d'une société reconnue et pérenne, afin d'avoir le maximum de garantie. Ces offres reposent sur le principe suivant :
  - connexion de l'émetteur du message à un site sécurisé et dépôt du message,
  - notification (via un e-mail) par le serveur sécurisé au destinataire qu'il a reçu un message,
  - téléchargement par le destinataire du message sur le serveur intermédiaire sécurisé. Toutes ces opérations et échanges se déroulent sous protocole d'échanges chiffrés https.

- La troisième solution consiste à utiliser des services de messagerie sécurisée, associés à des certificats de signature électronique. Cette solution permet non seulement une excellente sécurité au plan technique, mais assure également le caractère probant de l'échange grâce à la signature électronique.

Moyens existants

La « signature électronique »

Le mot « signature » est utilisé ici dans un sens élargi, mais il faut rappeler qu'en droit français, signature vaut identification.

- **Composantes**. La signature électronique est formée de trois composantes :
  - le document porteur de la signature,
  - la signature elle-même,
  - le certificat électronique authentifiant le signataire.

- **Technologie**. La signature électronique s'appuie sur une technologie appelée PKI (Public Key Infrastructure, ICP : Infrastructure à Clefs Publiques, en français).

- **Autorités**. Cette technologie nécessite la délivrance par des sociétés appelées Autorités de Certification (AC) de certificats de signature électronique.
  - L'autorité de certification (AC) définit une politique de certification, et la fait appliquer. L'autorité de certification est responsable vis à vis de ses clients, mais aussi de toute personne se fiant à un certificat qu'elle a émis, de l'ensemble du processus de certification et donc de la validité des certificats qu'elle émet. Certaines AC sont reconnues par les pouvoirs publics (Ministère des Finances, Minefi).
  - L'autorité d'enregistrement (AE) vérifie que le demandeur de signature électronique est bien la personne qu'il prétend être, et ce conformément aux règles définies dans la politique de certification. L'autorité d'enregistrement a un rôle essentiel d'identification.
  - L'opérateur de certification (OC) assure la fourniture et la gestion des certificats électroniques. Son rôle consiste à mettre en œuvre une plate-forme technique sécurisée, et ce dans le respect des exigences énoncées dans la politique de certification. Il assure les prestations techniques, en particulier cryptographiques, nécessaires au processus de certification.

- **Types de signatures (certificats)**. Il existe aujourd'hui, en droit français, 3 types de signature électronique :
  - La signature électronique (effectuée avec des certificats de classe 1) : elle permet de contrôler l'intégrité du document, mais pas l'identité du signataire (les certificats de classe 1 sont remis selon un processus de contrôle très léger).
  - La signature électronique sécurisée (effectuée avec des certificats de classe 2 et/ou 3) : elle permet de contrôler l'intégrité du document et d'assurer une authentification forte du signataire (par exemple : le Minefi accepte ce type de signature pour les déclarations de TéléTVA). Plus la classe est élevée, plus le lien entre la clé publique établie par le certificat électronique et la personne physique est « certain ».
  - La signature électronique sécurisée PSC (effectuée avec des « certificats qualifiés », voir arrêté du 26 juillet 2004.) : il n'existe pas aujourd'hui d'offres permettant de telles signatures électroniques mais les premiers PSC devraient être certifiés au printemps 2005 (dès approbation du référentiel du COFRAC préparé l'automne dernier avec la DCSSI et l'ADAE).

- **Exemples**. Les télé-procédures vous imposent de vous identifier ou de signer votre déclaration électroniquement. Dans le cas des télé-procédures, le risque est essentiellement réglementaire ou juridique. Il faut vous conformer aux exigences des procédures de dématérialisation des actes juridiques selon les modalités inscrites dans les textes de lois autorisant les déclarations et échanges administratifs par voie électronique (en principe ces exigences sont clairement indiquées sur le site Internet). Quelques exemples :
  - Télé-TVA est l'une des premières télé-procédures accessibles à l'ensemble des entreprises pour la déclaration de la TVA par voie électronique. Le site du Minefi donne toutes les précisions nécessaires, dont les AC (autorités de certification) agréées.
  - La sécurisation des échanges entreprises/acheteurs publics dans le cadre de la dématérialisation des procédures de commande publique nécessite l'utilisation de certificats, selon des modalités définies par l'entité publique acheteuse.
  - La facturation électronique est maintenant autorisée : elle pourra requérir l'usage d'un certificat de signature électronique sécurisée.

Le Chiffrement

Il consiste à traiter une information par un procédé mathématique, de sorte que seules les personnes possédant la clé appropriée puissent rétablir, lire et traiter ladite information.

- **Principe**. Le principe des techniques de chiffrement est d'utiliser un code pour chiffrer les messages et un code pour les déchiffrer. Ces techniques existent depuis l'antiquité (par exemple, Jules César utilisait des messages chiffrés pour communiquer avec ses généraux). En 1976, Diffie et Hellmann inventent le procédé de chiffrement à clé publique. L'idée est que la clé est séparée en deux parties, l'une pouvant être divulguée et l'autre devant rester confidentielle.

- **Catégories**. Il existe 2 grandes catégories de chiffrement :

  - Le chiffrement symétrique (aussi appelé chiffrement à clé privée ou chiffrement à clé secrète) consiste à utiliser la même clef pour le chiffrement et pour le déchiffrement.
    - Il faut prévoir que chacun utilise une clé différente pour communiquer avec chaque correspondant.
    - Le principal inconvénient d'un crypto-système à clefs secrètes provient donc de l'échange des clés : le chiffrement symétrique reposant sur l'échange d'un secret (les clés), se pose le problème de la distribution des clés.

  - Le chiffrement asymétrique (aussi appelé crypto-système à clés publiques), est basé sur le principe que les clés existent par paires (on parle souvent de bi-clés): une clé publique pour le chiffrement et une clé privée ou secrète pour le déchiffrement.
    - Ce qui a été chiffré par la clé publique ne peut être déchiffré qu'avec la clé privée et ce qui a été chiffré par la clé privée ne peut être déchiffré qu'avec la clé publique.
    - Les utilisateurs choisissent une clé aléatoire dont ils sont seuls connaisseurs (il s'agit de la clé privée). A partir de cette clé, les utilisateurs déduisent chacun automatiquement un algorithme (il s'agit de la clé publique). Les utilisateurs s'échangent cette clé publique au travers d'un canal non sécurisé.

- **Méthodes de chiffrement**. Dans les échanges électroniques des données, on emploie toute une série de méthodes de chiffrement, comme SSL ou PGP, consistant à crypter les données soit avant, soit pendant leur transfert :
  - SSL est un protocole de transfert de données qui permet de chiffrer l'échange électronique pendant son transfert entre l'expéditeur et le destinataire. Cette forme de transmission cryptée des données est surtout utilisée pour les services bancaires en ligne et pour le commerce électronique, par exemple pour la transmission de données confidentielles (mots de passe, numéros de cartes de crédit) entre un navigateur et un serveur.
  - PGP est un procédé de chiffrement hybride, qui sert à crypter des données au moyen d'une clé publique et à les déchiffrer à l'aide d'une clé privée. PGP est actuellement le système le plus employé pour le chiffrement du courrier électronique.

La Biométrie

C'est un moyen reconnu comme étant de plus en plus fiable pour vérifier l'identité électronique des personnes mais les textes n'en prévoient pas encore l'usage de manière explicite. C'est donc une technologie dont la montée en charge est à suivre dans les années qui viennent.

Fiche 4

Sensibilisation du personnel

La sécurité est l'affaire de chacun des employés. Une bonne politique de sécurité doit être partagée et comprise par tous. La plus grande partie des brèches de sécurité sont le fait des salariés par ignorance ou par intention frauduleuse (vol de données et transfert par Internet).

Comment se protéger ? Les 3 règles d'or de l'utilisateur

Ne pas faire confiance à un tiers

(pouvant être un manipulateur pratiquant l'« ingénierie sociale »), en n'hésitant pas à demander des justifications complémentaires et en mettant en pratique systématiquement le contre appel, même si tout laisse penser que ce tiers dispose de l'autorité nécessaire (usurpation fréquente d'identité).

Préserver son identification

Ne communiquer (ou laisser accessible) aucun mot de passe et code d'accès personnel.

Bien choisir le mot de passe (8 caractères alpha numériques sont recommandés, sans référence à l'état civil personnel ou de personnes proches) et veiller au renouvellement tous les trois à six mois. Mais la longueur et la complexification des mots de passe ne sont pas toujours positives, les utilisateurs sont en effet souvent amenés à les noter sur un papier ou les oublient tout simplement.

En France, contrairement aux autres pays, il a été constaté en 2004 une augmentation des utilisateurs qui notent leurs mots de passe.

En moyenne sur 100 personnes, 50 écrivent le mots de passe et 35 le communiquent à un tiers ! (source étude SafeNet 2004 portant sur 67000 entreprises en France, UK, Allemagne et USA).

Pratiquer librement l'autocensure

Réserver au seul usage professionnel les moyens informatiques et le réseau de la société et accepter de limiter l'accès à certains sites et le transfert de fichiers dangereux ou de taille importante.

- **Éviter les téléchargements et installation sans autorisation**. Faire valider toute installation de matériel/logiciel sur l'équipement bureautique.

- **Respecter les règles de connexion depuis l'extérieur**. Faire valider toute installation pouvant permettre de se connecter sur le réseau interne depuis l'extérieur du périmètre de l'entreprise.

Mise en œuvre des 3 règles La charte d'utilisation

Objectif

La mise en place d'une Charte assure la protection du système d'information, limite la responsabilité de l'entreprise et de ses dirigeants et s'applique à tous les utilisateurs.

Nature juridique

Cette charte a une valeur d'abord informative puis normative lorsqu'elle est acceptée par le salarié. La Charte d'utilisation sera au choix :

- Une annexe du Règlement Intérieur (la mise en place de la Charte et sa modification suivront la procédure applicable au Règlement Intérieur),

- Un document unilatéral qui peut prendre la forme d'une note interne et qui répond à une procédure d'information (collective et individuelle) et de consultation mais qui renverra dans tous les cas au Règlement Intérieur de l'entreprise pour les sanctions disciplinaires applicables en cas de violation.

Avis du comité d'entreprise

La Charte doit être soumise au Comité d'entreprise pour avis conformément à l'Article L. 432-2-1 alinéa 3 du Code du travail (ou conformément à l'Article L.122-36 du Code du travail lorsque la Charte est portée en annexe du Règlement Intérieur).

Contenu

La Charte définit clairement et de façon transparente les modalités et limites de l'utilisation des moyens informatiques mis à la disposition du salarié par l'entreprise.

- **Protection/sécurité et confidentialité du système d'information** dont les dispositions encadrant la cybersurveillance.
  - Accès au réseau sécurisé et protégé par des mots de passe accordés à un utilisateur ou à l'ensemble des utilisateurs du système d'information et confidentialité de ces derniers.
  - Mise en place de pare-feux et obligation qui incombe aux responsables de les mettre à jour régulièrement.
  - Obligation pour l'utilisateur d'effectuer des sauvegardes régulières afin de minimiser le risque de perte de données.
  - L'introduction de tout nouveau matériel, programme ou logiciel est interdite aux utilisateurs sans autorisation de l'employeur ou de l'administrateur du système d'information.

- **Mise à disposition et limites d'utilisation de la messagerie** par les salariés et les institutions représentatives du personnel (dont certaines dispositions encadrant la cybersurveillance).
  - Droit pour le salarié d'utiliser la messagerie électronique mise à sa disposition à des fins privées dans la limite du raisonnable,
  - Obligation pour l'utilisateur de distinguer les données professionnelles des données à caractère privé,
  - Possibilité pour l'employeur de sanctionner l'utilisation privée de la messagerie lorsqu'elle est abusive et compromet le fonctionnement normal de la messagerie professionnelle.
  - Limitation du format, du type et de la taille des messages électroniques. La taille des messages électroniques ne devra pas venir compromettre le bon fonctionnement du système d'information et notamment sa performance,
  - Possibilité pour l'employeur de modifier ces mesures par note de service.

- **Règles relatives à l'utilisation d'Internet**
  - Mesure dans laquelle la consultation d'Internet à des fins privées est permise au salarié (une consultation raisonnable est socialement admise, la Charte ne doit pas être abusive en édictant une interdiction absolue. Cette utilisation ne doit pas venir perturber le travail du salarié ou de ses collègues),
  - Interdiction de télécharger des œuvres protégées et rappel des règles selon lesquelles la responsabilité de l'employeur peut être engagée en cas de téléchargement par un utilisateur d'œuvres protégées sans l'autorisation des ayants droits (logiciel, fichiers mp3…),
  - Interdiction de consulter des sites illicites (liste exhaustive des sites que l'utilisateur est en droit de consulter ou exclusion des sites contraires aux bonnes mœurs tels que les sites activistes, pédophiles ou pornographiques),
  - Droit pour l'employeur, en cas de violation de cette disposition, de dénoncer l'utilisateur aux autorités compétentes,
  - Interdiction de participer à des forums sauf autorisation de la direction de la communication, ou de la personne en charge de la communication de la société, pour s'exprimer au nom de cette dernière.

- **Contrôle**
  - Droit d'accès de l'administrateur à l'ensemble des éléments du système d'information afin de le contrôler ou de le maintenir dans un souci de protection de ce dernier.
  - Définition des actes de contrôle ou de maintenance du système d'information (liste exhaustive ou exclusions).
  - Possibilité pour l'employeur ou l'administrateur d'exercer un contrôle sur la nature des sites visités par le salarié, la durée de connexion à Internet, les téléchargements…. Ce contrôle doit être justifié par un impératif de sécurité et de confidentialité.
  - Droit pour l'employeur de conserver l'historique de messagerie électronique pendant une durée fixée dans la Charte.

- **Sanctions** en cas de non-respect de la Charte (Tout ce que la Charte n'interdit pas reste autorisé). Modalités d'information du salarié et procédure contradictoire en cas de sanction disciplinaire (information par écrit des griefs retenus contre le salarié, convocation écrite à un entretien, possibilité de se faire assister, déroulement de l'entretien, motivation de la sanction).

Affichage et formalités - entrée en vigueur

Lorsque la Charte est portée en annexe du Règlement Intérieur, l'employeur devra respecter les obligations suivantes :

- Mise en ligne de la Charte sur l'Intranet de l'entreprise,

- Affichage de la Charte dans l'entreprise conformément à l'Article R. 122-12 du Code du travail,

- Communication à l'inspecteur du travail après avis du Comité d'entreprise (ou à défaut des délégués du personnel),

- Dépôt de la Charte au secrétariat au greffe du Conseil des prud'hommes du siège social de la société ou de l'établissement concerné,

- Fixation d'une date d'entrée en vigueur, au plus tôt un mois après l'accomplissement des formalités de dépôt auprès du secrétariat au greffe et d'affichage.

Litiges

Sous peine de voir la charte remise en question par les tribunaux, le contrôle prévu par la Charte, doit être loyal, transparent et proportionné :

- Respect du principe de proportionnalité. Lors de la rédaction de la Charte, l'employeur doit respecter certains principes (le respect de la vie privée ou encore le principe de proportionnalité), dans le cas contraire, sa responsabilité pourrait être engagée.

- Information du salarié et des institutions représentatives du personnel.

Assistance

- Information : Rapport de la CNIL, « La cybersurveillance sur les lieux de travail » mis à jour en février 2004 (www.cnil.fr) et Vade-mecum du MEDEF, « l'utilisation des nouvelles technologies dans l'entreprise », février 2003.

- Coûts de spécialistes. 3 jours d'expert (interne ou externe) dont 3 demi-journées avec l'ensemble des salariés clés suffisent à définir la charte et sensibiliser. 2 jours par an pour un diagnostic rapide et re-sensibiliser.

Fiche 5

Mettre en œuvre un plan de sauvegarde

Quelque soit la qualité des moyens de défense mis en œuvre (physiques ou logiques), les données peuvent être altérées sciemment ou accidentellement.

Les données et les applications informatiques doivent être disponibles « à tout moment » lorsqu'on en a besoin, et doivent être conservées (sauvegardées) afin de pouvoir être récupérées (restauration) le moment voulu.

Il convient par conséquent de :
- Définir une politique de sauvegarde ;
- Définir des procédures de sauvegarde ;
- Définir des procédures de restauration ;
- Maintenir ces politiques et procédures.

Politique de sauvegarde

Il n'y a pas de politique de sauvegarde universelle. Elle doit être définie en fonction du volume de données, de la quantité d'information que l'on accepte de perdre, et éventuellement de la durée « légale » de conservation de l'information.

- Définir les périmètres à sauvegarder (services, matériels, sites, utilisateurs, …)

- Définir le type de données sauvegardées (fichiers utilisateurs, fichiers serveurs, documents contractuels, emails, bases de données, …). Le contenu de la sauvegarde peut évoluer dans le temps avec l'ajout de nouvelles applications ou de données. Cette contrainte doit être prise en compte et il faut veiller à la complétude des sauvegardes régulièrement.

- Fréquence/périodicité de la sauvegarde, périodicité de la rotation des sauvegardes

- Principe de sauvegarde générique :
  - Le support de sauvegarde journalière du lundi au jeudi est doublé et utilisé par alternance toutes les deux semaines.
  - La sauvegarde mensuelle est conservée un an jusqu'au mois identique de l'année suivante.

- Principe de sauvegardes spécifiques : Des sauvegardes spécifiques peuvent être réalisées en parallèle pour des données sensibles comme les données financières de l'entreprise et conservées suivant les obligations légales (s'assurer que les applications ayant généré ces données soient également accessibles et que toutes les données soient bien identifiées, comme par exemple des petits outils de pilotage financier développés sous Excel en local, ou des fichiers sur les portables).

- Définir le(s) lieu(x) et moyens de stockage des sauvegardes (lieux différents, armoires ignifugées, …). Ne pas laisser les supports près de la machine. En cas de vol ou de sinistre, ces supports risquent en effet d'être également volés ou détériorés. Il est nécessaire de conserver les supports mensuels et annuels en dehors du site de l'entreprise. Conserver les supports hebdomadaires dans une localisation la plus éloignée possible de leur source et dans une armoire fermée (ignifugée de préférence).

Procédures de sauvegarde

Les différentes méthodes de sauvegarde

Sauvegarde complète

C'est une méthode de type « annule » et « remplace ». On écrase le contenu de sauvegarde par la nouvelle information. Méthode très sûre mais longue si le volume est important (par ex : la sauvegarde de gros volumes peut être supérieure à la durée de la nuit et empêcher le travail des utilisateurs le lendemain matin).

Sauvegarde différentielle

C'est une méthode qui sauvegarde toutes les informations qui ont été modifiées depuis la dernière sauvegarde complète.

Sauvegarde mixte

Une sauvegarde journalière différentielle

+ une sauvegarde complète le vendredi

+ une sauvegarde mensuelle gardée un an

+ à chaque intervention technique (mise à jour, …) sur un poste de travail ou un serveur, une sauvegarde complète (image de la machine) du poste ou du serveur réalisé par le prestataire.

Sauvegarde incrémentale

C'est une méthode qui ne sauvegarde que les informations qui ont été modifiées depuis la dernière sauvegarde enregistrée sur le support.

Synchronisation d'équipements

C'est une première méthode à mettre en place entre des équipements nomades et des postes fixes d'un utilisateur donné. Elle peut inclure autant les données d'agenda, de carnets d'adresses que de simples fichiers (fonction porte document) et s'active souvent manuellement.

Pour des postes de travail en réseau, il existe des outils simples et efficaces de duplication automatique

(fonction « miroir ») vers un autre disque (serveur sur réseau par exemple) mais cette duplication ne garantit que les pertes dues à des pannes matérielles et ne protège pas contre les risques de virus.

Test des sauvegardes

La procédure doit prévoir, avant de passer en mode de fonctionnement continu, de tester la bonne récupération des données afin de s'assurer du bon fonctionnement des sauvegardes.

Vérification des sauvegardes

La procédure doit inclure le contrôle régulier d'un journal des sauvegardes afin de vérifier qu'aucune anomalie n'ait perturbé le bon fonctionnement des sauvegardes (support saturé par exemple).

La mise en œuvre et les coûts

Mise en œuvre par des ressources internes avec acquisition des outils

A titre d'exemple, pour une sauvegarde par poste, 1 disque dur externe sur port USB mobile de poste en poste (environ 300 €) ou 1clé USB par poste (environ 100 €/poste) ou pour un système de sauvegarde en réseau de 20 postes, 2 serveurs (environ 5 000 €).

Sous-traitance à un prestataire de service informatique pour assistance et mise en œuvre

A titre d'exemple, 2 jours d'expert (interne ou externe) avec la direction pour définir politique et procédures et 1/2 jour par an pour un audit du processus de sauvegarde.

La sous-traitance à un prestataire (la sauvegarde à distance)

Cette solution offre l'avantage de ne plus avoir à gérer le support physique des sauvegardes, ni la charge de travail associée car ils sont externalisés à un prestataire via un réseau haut débit. Il est nécessaire de bien définir la politique de sauvegarde et le contrat de prestation (s'assurer de la bonne adéquation de la prestation en cas de problème ; de la présence d'un cryptage adapté, les données se trouvant chez le prestataire ; de la santé financière de ce prestataire stratégique ; etc.).

Fiche 6

Mettre en œuvre des moyens de défense minimums

La mise en œuvre de moyens de défense minimums permet de :
- bloquer les attaques automatisées,
- d'éviter de laisser des brèches ouvertes,
- de limiter la prolifération virale,
- de détecter les anomalies (les événements pouvant affecter la sécurité du système d'information).

Pour être exhaustifs, ces moyens seront complétés par les mesures suggérées dans les fiches 3 (mettre en œuvre les moyens adaptés à la confidentialité des données), 5 (mettre en œuvre un plan de sauvegarde) et 7 (mettre en œuvre les moyens de défense minimums pour les connexions sans fil).

Bloquer les attaques automatisées : les firewalls (pare-feu)

Rôle

Le rôle des pare-feu est de protéger le réseau de l'entreprise des intrusions extérieures. Ils filtrent la couche IP (Internet Protocol) qui sert à transporter les données circulant sur l'Internet, inspectent et/ou examinent chaque paquet IP afin de détecter les flux illicites, et les bloquent avant qu'ils n'atteignent le réseau de l'entreprise (pare-feu périmétriques et pare-feu applicatifs) ou du poste de travail (pare-feu personnel). Ils peuvent prendre une forme logicielle ou une forme de boîtiers appelés « appliances ».

Critères de choix

La réflexion préalable au choix d'une solution pare-feu ne s'effectuera qu'après avoir établi une politique de sécurité minimum et portera sur les points suivants :

- **Liés au niveau de sécurité requis**. Les pare-feu se différencient essentiellement par la finesse du contrôle qu'ils autorisent et leur capacité à traiter des flux élevés et à gérer un nombre important d'utilisateurs :
  - Simple contrôle sur les services et sur les adresses IP autorisés pour les pare-feu simples,
  - Contrôle sur la validité des protocoles et des flux applicatifs pour les pare-feu dit applicatifs (Plus de 75 % des attaques portent sur l'exploitation des faiblesses applicatives). Attention au choix de ce type de pare-feu (white list, black list, ou les dernières génération basées sur les principes de l'intelligence artificielle) plus ou moins facile à mettre en œuvre et à administrer.
  - Mise en œuvre de services associés tels que translation d'adresse, Proxy, passerelle antivirus, serveur DHCP (Dynamic Host Configuration Protocol), service VPN (s'assurer que l'autre extrémité du lien VPN est compatible avec la technologie VPN incluse dans le pare-feu sélectionné), services IDS (Intrusion Detection System) ou IPS (Intrusion Prevention System).

- **Liés à l'architecture des systèmes**
  - Caractéristiques de la connexion Internet,
  - Dimensionnement du réseau local (nombre d'utilisateurs).

- **Liés aux compétences internes**. Quels sont les moyens d'administration disponibles ? Un pare-feu, quel qu'il soit, doit être administré. Toutefois la technicité nécessaire pour installer et configurer avec soin un pare-feu logiciel open source par exemple sera bien supérieure à celle requise pour brancher et configurer un boîtier pare-feu ADSL via une interface Web. Le choix de la technologie pare-feu devra donc prendre en compte les compétences dont dispose ou souhaite se doter l'entreprise. Un pare-feu n'a d'intérêt que s'il est configuré en accord avec la politique de sécurité établie. Si, par exemple, seuls les flux Web et e-mail sont autorisés depuis l'Internet, l'ensemble des autres flux devra être interdit. La configuration du pare-feu peut être très fine en attribuant des droits diffé-

rents selon les catégories d'utilisateurs, elle peut également mettre en œuvre une politique variable suivant les plages horaires ou les jours d'ouverture de l'entreprise afin de limiter la consommation de bande passante durant les périodes de charge.

- **Le coût**. Le plus souvent les pare-feu sont facturés en fonction du nombre d'utilisateurs, des flux et des services associés.

Limiter les brèches ouvertes : se protéger des vulnérabilités

Les logiciels, comme toute réalisation humaine, contiennent des erreurs, appelées vulnérabilités, dont certaines menacent la sécurité. Ces vulnérabilités peuvent être exploitées manuellement ou par des programmes développés spécifiquement qui le plus souvent permettent à leur utilisateur de contrôler des ordinateurs sans légitimité.

Comment se protéger

Mettre en œuvre un processus de gestion des mises à jour de sécurité de tous les logiciels présents dans l'entreprise afin de pouvoir éliminer les vulnérabilités connues et bénéficier au passage des dernières améliorations en matière de sécurité. Les derniers systèmes d'exploitation et les dernières applications intègrent des fonctionnalités de mise à jour automatique, dont il faut s'assurer qu'elles sont activées. Les administrateurs du système d'information suivront classiquement la démarche suivante :

- Audit automatisé des configurations installées, et/ou à défaut veille permanente minimum sur les vulnérabilités des systèmes d'exploitation et applications installées (ww.cert.org),

- Test des nouvelles mises à jour,

- Déploiement des correctifs de sécurité en commençant par colmater les failles les plus critiques sur les machines les plus sensibles,

- Application des correctifs, grâce à des outils spécialisés, en prenant soin de gérer la non régression des systèmes.

Exemples d'outils de mise à jour

- Un service de mise à jour automatique, Windows Update, est intégré à Windows 2000 et Windows XP. Il permet aux consommateurs et aux petites entreprises d'installer automatiquement les mises à jour dès qu'elles sont disponibles.

- MBSA est un outil gratuit d'inventaire des mises à jour manquantes pour les machines Windows
www.microsoft.com/france/technet/themes/secur/infombsa.html

- Software Update Services (SUS) peut être téléchargé gratuitement sur le site Web de Microsoft. Ce service est conçu pour simplifier le processus de mise à jour des systèmes Windows. SUS permet aux administrateurs de déployer rapidement et en toute sécurité les mises à jour importantes sur leurs serveurs Windows 2000, ou Windows XP Professionnel.
www.microsoft.com/france/securite/outils/sus.asp

- Les autres plateformes offrent des possibilités similaires (Linux, Unix, Mac…)

Exemples d'outils de test de vulnérabilités

Les outils de test peuvent être utilisés à des fins d'audit préalable et/ou pour tester les mises à jour effectuées.

- **Outils gratuits**. Nessus est un outil gratuit de recherche de vulnérabilités (www.nessus.org). L'installation et la mise en œuvre sont réservées à des utilisateurs confirmés.

- **Outils payants**. Ces outils existent pour tous les types de plateformes. Ils peuvent être installés dans l'entreprise ou être actionnés à distance, un rapport complet étant alors transmis de façon totalement sécurisée à l'entreprise. Ils peuvent être, dans un premier temps, testés à distance gratuitement puis par abonnement. Il est vivement recommandé de procéder au moins à un test gratuit pour établir un état des lieux rapide du niveau de vulnérabilité des systèmes (offres multiples disponibles).

Limiter la prolifération virale : les antivirus

La prolifération des virus (des vers, des spams et autres chevaux de Troie) impose l'adoption de logiciels antivirus pour éviter une contamination rapide des systèmes. Comment choisir ? La bonne question n'est pas tant la marque que leur positionnement et leur nombre.

Trois solutions

Un antivirus disposé sur la passerelle d'accès Internet

Le principe est de réaliser un filtrage applicatif sur l'ensemble des flux en clair (c'est-à-dire communications non chiffrées) qui transitent par la passerelle Internet. En particulier cet antivirus analysera les flux Web à la recherche de logiciels malveillants. Ceci peut s'avérer intéressant dans le cas d'utilisation de service de courrier Web. En pratique, il est admis que ce niveau de filtrage est aujourd'hui à lui seul une garantie insuffisante pour se prémunir de l'ensemble des codes malveillants.

Un antivirus disposé sur le serveur de messagerie

Le point névralgique de la communication d'entreprise est le serveur de messagerie d'entreprise. Le choix de traiter la lutte antivirale à ce niveau présente donc de nombreux avantages : relative simplicité de mise en œuvre, efficacité maximale sur les infections par e-mail, ressources matérielles associées généralement limitées. L'inconvénient majeur est que l'ensemble des flux n'est pas traité par l'usage exclusif de cet antivirus.

Un antivirus équipant les postes personnels

La nécessité de disposer d'un antivirus à jour sur chaque poste de travail de l'entreprise s'impose : d'une part les protections antivirales réseau ne sont pas infaillibles (les fichiers chiffrés par exemple ne pourront jamais être analysés), d'autre part les usages personnels des ordinateurs sont par définition incontrôlables (insertion de CD, utilisation d'une connexion à domicile, …).

En pratique, ce déploiement indispensable peut impliquer une remise à niveau du réseau et du parc informatique :

- le système doit permettre la mise en place de l'antivirus mais aussi la mise à jour régulière des bases de signatures, sans laquelle l'efficacité de la détection est compromise ;

- les systèmes d'exploitation doivent être suffisamment homogènes pour autoriser un déploiement uniforme de l'antivirus.

L'usage est de combiner plusieurs de ces solutions, en essayant autant que possible de choisir deux fournisseurs distincts pour favoriser les chances de détection de nouvelles souches. La solution minimum est probablement le déploiement de l'antivirus personnel, mais il sera raisonnable et confortable d'ajouter rapidement un dispositif antivirus sur le serveur de messagerie.

Détecter les anomalies

Identifier une activité anormale

Il faut au préalable :

- définir ce que doit être une activité normale, c'est-à-dire les types de flux autorisés ainsi que les configurations associées. Cette action peut être menée par l'utilisation d'outils automatisés (voir fiche 1).

- détecter les flux contraires aux règles ou les modifications de configuration indues.

Sans ces deux démarches, les intrus pourront d'une part s'introduire sur le système sans risque d'être détectés, et d'autre part, et c'est plus grave encore, se maintenir sur le système à demeure avec un accès de plus en plus large à l'ensemble des ressources informatiques.

Surveiller les traces des systèmes sensibles

Les équipements de sécurité mais aussi l'ensemble des serveurs du réseau d'entreprise génèrent des traces (logs) permettant de retracer une partie de l'activité du système. La surveillance de ces traces, rébarbative, est souvent négligée. Elle est pourtant essentielle pour détecter les incidents de sécurité en l'absence de dispositifs spécifiques de détection ou de prévention d'intrusion. Il faudra donc mettre en place une procédure simple de consultation de certaines traces sur les machines sensibles ou exposées, en s'aidant par exemple d'outils dédiés facilitant ce travail.

Détecter les modifications de configuration

Très souvent une agression sur un système d'information se caractérise par la modification de paramètres de configuration ou de fichiers système sans autorisation. Ces opérations indues peuvent être détectées facilement par le contrôle régulier et automatisé de l'intégrité de fichiers spécifiés. Le logiciel open source Tripwire permet par exemple de réaliser ce type de contrôle. Il sera essentiel de limiter l'usage du contrôle d'intégrité à un nombre réduit de fichiers sensibles pour conserver l'efficacité du dispositif.

Détecter les intrusions

De nombreuses sondes de détection d'intrusion ou de prévention d'intrusion sont proposées, parfois incluses dans des équipements de réseaux du type pare-feu. Elles peuvent constituer un complément efficace aux dispositifs présentés précédemment, toutefois la mise en œuvre et l'exploitation parfois délicates de ces outils incitent à un usage modéré.

Fiche 7

Mettre en œuvre des moyens de défense minimums pour les connexions sans fil

Cette fiche est complétée par la fiche n° 6 sur les moyens de défense minimums dans le cas des connexions fixes.

Qu'appelle-t-on « réseau sans fil » ?

C'est un moyen de connecter un terminal à un réseau (d'entreprise, Internet) sans utiliser de câblage physique.

Ces technologies sont également utilisées pour faire communiquer localement plusieurs terminaux entre eux sans avoir à créer de réseau permanent.

On classe les technologies sans fil selon leurs usages

Les réseaux sans fil personnels

Ils permettent une connectivité entre appareils électroniques proches les uns des autres. Cet usage est aujourd'hui dominé par la technologie Bluetooth (portée typique de plusieurs mètres) ;

Les réseaux sans fil d'entreprise

Ils se substituent aux réseaux câblés d'entreprise classiques. La technologie la plus répandue est aujourd'hui le « Wi-Fi » (portée typique de quelques dizaines de mètres), utilisée soit intra-entreprise soit pour couvrir les zones d'affaires (« Hot-Spots »).

Les réseaux sans fil métropolitains

Ils permettent une couverture large (plusieurs dizaines de kilomètres) et sont utilisés le plus souvent pour proposer une connectivité à Internet en complément du câble ou de l'ADSL. Plusieurs technologies coexistent, parmi lesquelles le « WiMAX », soutenue par Intel qui l'intègrera dans sa future génération de microprocesseurs.

Les réseaux sans fil nationaux

Déployés par les opérateurs de téléphonie mobile, et dont les générations successives permettent de plus en plus de débit : GSM, GPRS, EDGE, UMTS. Ces deux dernières technologies, en cours de déploiement, amèneront des débits compatibles avec de véritables échanges de données d'entreprise.

Cette fiche envisage l'étude des deux technologies les plus répandues en entreprise aujourd'hui : le Bluetooth pour les réseaux sans fil personnels et le Wi-FI pour les réseaux sans fil d'entreprise.

Les vulnérabilités des réseaux sans fil

Les réseaux sans fil du type Wi-Fi ou Bluetooth offrent de multiples avantages : simplicité et coût modique d'installation, facilité d'usage, mobilité étendue. En contrepartie, ils sont par nature plus vulnérables aux attaques informatiques que les réseaux filaires.

Les principales vulnérabilités de ces réseaux sont les suivantes :

Les intrusions sur les réseaux ou les équipements connectés

Par définition, le cœur du réseau est accessible de l'extérieur par les équipements sans fil (ordinateurs équipés d'une interface radio, PDA ou téléphones portables dans le cas du Bluetooth). Il est extrêmement difficile de garantir que seules les personnes autorisées y auront accès. Ainsi une borne d'accès Wi-Fi porte en environnement dégagé à plus de 100 mètres, ce qui la rend le plus souvent atteignable bien au-delà du strict périmètre physique de l'entreprise.

La sécurité reposera donc fondamentalement sur la qualité du contrôle d'accès logique mis en place.

L'interception des données échangées par voie hertzienne

Puisque les données sont transmises par voie radio, elles peuvent être écoutées par l'ensemble des personnes présentes dans la zone d'émission, ce qui peut permettre de capter des informations précieuses, mais surtout donner des renseignements utiles pour mettre en œuvre une attaque plus dangereuse : une intrusion sur le système d'information par exemple.

Les protocoles sans fils intègrent maintenant quasi systématiquement des moyens de chiffrement des communications permettant de se prémunir de ce type d'attaques.

Toutefois à ce jour cette vulnérabilité est accentuée par le fait que certaines technologies sans fil contiennent des failles de sécurité et que la fonction de chiffrement n'est pas toujours activée.

Les perturbations de services

Le but de ces attaques dites « en deni de service » est de perturber durant un certain temps le bon fonctionnement du système. Il peut s'agir de rendre la borne d'accès à un réseau sans fil indisponible ou – plus grave – de paralyser le réseau.

La plus simple et la plus efficace des attaques consiste simplement à brouiller au niveau physique le spectre utilisé pour parasiter les communications. La source est cependant aisément identifiable, et peut être neutralisée.

Une menace plus importante réside en une sollicitation indue de l'équipement sans fil – des demandes de connexion multiples par exemple – qui peut saturer les entrées et ainsi interdire tout accès aux utilisateurs légitimes, mais aussi engendrer d'autres dysfonctionnements sur les réseaux connectés. La parade résidera dans l'architecture de sécurité mise en place derrière les points d'accès Wi-Fi, et la bonne configuration des équipements.

Si la disponibilité des services est la principale exigence de sécurité, le choix du sans fil n'est sans doute pas le plus judicieux.

La mise en œuvre de la sécurisation du sans fil

Les équipements sans fil étant accessibles le plus souvent au-delà du périmètre physique sécurisé de l'entreprise, il est indispensable de les sécuriser dès leur installation. De fait, la mise en œuvre d'un réseau Wi-Fi nécessite un niveau sécurité minimal, sans quoi l'entreprise sera une cible facile et privilégiée des pirates informatiques ou de la concurrence. Les principes généraux sont décrits ci-dessous pour deux environnements spécifiques : Bluetooth et Wi-Fi.

Sécurité des réseaux sans fil personnels (Bluetooth)

Bluetooth est une technologie de « souplesse ». La sécurité du protocole Bluetooth est – dans sa version actuelle – insuffisante pour garantir une résistance aux attaques évoluées. On évitera donc d'utiliser cette technologie pour connecter des équipements supportant ou donnant accès à des informations d'une importance stratégique pour l'entreprise.

Par extension, il est fondamental de ne pas utiliser cette technologie pour des équipements du type PDA communiquant reliés eux-mêmes à des réseaux sensibles.

D'une façon générale, pour se prémunir des intrusions et du vol de données sur les réseaux personnels utilisant Bluetooth, il convient de configurer correctement les équipements :
- en inhibant le mode découverte et appariement ;
- en activant la reconnaissance d'équipements répertoriés (par liste d'appareils « amis » autorisés) ;
- en activant le chiffrement des données ;
- en activant le mode invisible.

De plus, pour les équipements nomades (téléphone mobile ou PDA) intégrant une interface Bluetooth, les fonctions de liaison sans fil doivent être désactivées par défaut pour être réactivées lors d'un usage ponctuel. Ceci permet en particulier de se prémunir de certaines contaminations virales du type « ver bluetooth ».

Sécurité des réseaux sans fils d'entreprise (Wi-Fi)

La sécurité d'un réseau local sans fil de type Wi-Fi est plus complexe et peut être réalisée à différents niveaux. Elle intègre l'ensemble des préconisations de sécurité valables pour un réseau filaire (c.f. fiche 6) plus un ensemble de préconisations spécifiques au sans fil.

Compte tenu de la difficulté pour restreindre l'accès à un réseau sans fil, il est indispensable d'associer à son déploiement une procédure spécifique de sécurité.

Au-delà de la formation et de la sensibilisation des utilisateurs cette étape comprend a minima :
- la configuration des couches liaison et transport ;
- la gestion des accès ;
- les mises à jour logicielles ;
- l'audit périodique et la surveillance active de son réseau.

Tableau récapitulatif de la démarche minimum de sécurisation d'un réseau Wi-fi

- Sécuriser les points d'accès, les clients Wi-Fi et le compte administrateur et utiliser une liste d'accès d'appareils autorisés.
- S'assurer que les mécanismes de sécurité intégrés et normalisés sont bien activés (authentification, chiffrement WPA (Wi-Fi Protected Access) ou WPA2, liste d'équipements autorisés). La conservation de la configuration par défaut des équipements Wi-Fi est aujourd'hui la principale cause de compromission ; elle est donc à bannir.
- Mettre à jour le logiciel des équipements Wi-Fi (nouvelles versions logicielles qui corrigent les failles de sécurité).
- Étendre (et compléter) les services de sécurité déjà déployés sur le réseau filaire (exemple par VPN, firewall…).
- Mettre en œuvre les outils et règles d'authentification et les politiques de sécurité.
- Différencier les utilisateurs Wi-Fi une fois qu'ils sont connectés.
- Informer et former les utilisateurs. Pour les appareils en mobilité, les fonctions de liaison sans fil Wi-Fi doivent être désactivées par défaut et réactivées pour un usage ponctuel.
- Auditer le réseau : Un audit physique (s'assurer que le réseau sans fil ne diffuse pas d'informations dans des zones non désirées et qu'il n'existe pas de réseau sans fil non désiré dans le périmètre à sécuriser) et un audit informatique (s'assurer que le degré de sécurité obtenu est bien égal à celui désiré).
- Surveiller le réseau : surveillance au niveau IP avec un système de détection d'intrusions classique et surveillance au niveau physique (sans fil) avec des outils dédiés.

Fiche 8

Établir une barrière de sécurité entre les données externes et internes

Deux usages

L'entreprise a ouvert une partie de son système d'information vers l'extérieur, via un site web ou par échanges de données informatiques.

Par nature et destination, un site web rend très visible l'entreprise depuis l'extérieur. Le serveur web est connecté aux systèmes internes après filtrage par le pare-feu. Les pirates disposent d'outils sophistiqués ou très simples pour tester les moyens de défense (scan) et la faiblesse de vos applications web. Plus de 75 % des attaques utilisent ces faiblesses.

Lorsque l'échange de données parfois confidentielles avec les personnes à l'extérieur de l'entreprise (clients, partenaires, fournisseurs, employés nomades) transite sur Internet, le contenu peut, sauf précautions, être lu par des tiers non autorisés.

Ces deux usages nécessitent un surcroît de précautions, en plus des moyens de protection minimums décrits dans les fiches 3 (mettre en œuvre des moyens appropriés à la confidentialité des données) et 6 (mettre en œuvre des moyens de protection minimums).

Trois moyens de protection supplémentaires

La mise en œuvre d'un site Web, parce qu'il met l'entreprise particulièrement en évidence, peut nécessiter la mise en place d'une DMZ et dans tous les cas le test des applications Web avant déploiement.

- **Définir une DMZ** (Demilitarized Zone, zone démilitarisée) et la protéger.

Ce terme vient du vocabulaire militaire pour désigner une zone tampon entre deux ennemis.

La DMZ est un sous réseau qui se positionne entre un réseau interne de confiance et l'Internet public.

Objectif

Les éléments suspects (les flux transitant vers le réseau interne et depuis le réseau interne), découverts par les équipements filtrants (firewalls, outils de détection et de filtrage de contenu), seront redirigés dans la DMZ (« quarantaine ») pour analyse.

Architecture

Les serveurs installés sur la DMZ permettent de fournir des services au réseau externe, tout en protégeant le réseau interne contre des intrusions possibles sur ces serveurs :

- **Les serveurs Web** (http), **serveurs de fichiers** (ftp), **serveurs d'e-mails** (SMTP) et **serveurs de noms** (DNS)… : services offerts par l'entreprise au monde Internet ?
- Les serveurs relais permettant d'assurer une communication indirecte entre le réseau local et le monde Internet (proxies, relais SMTP, antivirus, …).

Mise en œuvre. La DMZ est généralement créée par l'emploi d'un pare-feu, composé de trois interfaces réseau (Internet, réseau interne, DMZ).

Trois solutions

Pas de DMZ

Les serveurs sont placés entre le routeur et le pare-feu. Chaque serveur doit être parfaitement sécurisé ; tous les services et ports inutiles doivent être fermés ; la mise à jour des trous de sécurité détectés sur les logiciels et systèmes d'exploitation doit être très fréquente.

DMZ pour flux entrants uniquement

Pour une protection du système d'information des services, aucun flux ne doit aller d'Internet au réseau interne sans passer par la DMZ. Les serveurs sont sur la DMZ. Ils sont protégés par le pare feu et l'exploitation se révèle moins lourde. Les flux dans le sens Internet vers le réseau interne passent par la DMZ. Les flux dans le sens réseau interne vers Internet ne passent pas par la DMZ. Cette configuration est très répandue, et concilie l'investissement et un bon niveau de sécurité. En employant un relais de messagerie ou un service antivirus de messagerie, ce dernier sur la DMZ permet au serveur de messagerie d'être dans le réseau local. Les mails des utilisateurs stockés sur le serveur sont protégés.

DMZ pour flux entrants et sortants

Les serveurs sont sur la DMZ. Ils sont protégés par le pare-feu. Des serveurs relais (mail ou antivirus mail, Proxy FTP, HTTP, …) sont placés sur la DMZ, et permettent aux flux du

réseau interne vers Internet de passer par la DMZ. Les flux dans le sens Internet vers le réseau interne passent par la DMZ. Cette configuration est très sécurisée.

Mutualisation

La mise en place d'une telle solution peut être assurée par le fournisseur d'accès à Internet, qui se charge de mettre en place et de gérer sur son infrastructure le pare-feu et les services relais. Ces services sont mutualisés ce qui permet de réduire l'investissement et les contraintes d'exploitation de l'entreprise. Ce type d'offre convient pour les besoins standards d'utilisation et de protection d'Internet (proxies mail et web, filtrage antivirus et anti-spam par exemple).

- **Tester les applications web exposées**
  - Les applications Web sont des applications visibles depuis l'extérieur (elles sont conçues pour communiquer). Le site Web est une application Web. Les applications Web ne sont pas exemptes de faiblesses liées à leur conception et réalisation. Ces applications peuvent être d'autant plus dangereuses qu'elles peuvent être connectées à vos applications critiques (récupération de données venant de formulaires par exemple).
  - Les hackers disposent d'un arsenal impressionnant pour les exploiter. Les scenarii d'attaques sont même disponibles sur Internet à l'usage des apprentis hackers. Ces scripts se renouvellent sans cesse et deviennent de plus en plus sophistiqués. En exploitant les faiblesses des applications et les systèmes d'exploitation sur lesquels elles reposent, ces scripts permettent soit de rendre le site indisponible pour plusieurs heures à plusieurs jours (DOS), ou de prendre le contrôle des systèmes en s'arrogeant les droits d'administrateur (TOS).
  - Tester les applications Web est donc indispensable avant tout déploiement (y compris les mises à jour). Les sociétés spécialisées d'audit (« pentest » pour penetration testing) disposent d'outils spécifiques. Leur mise en œuvre exhaustive peut prendre de 2 à 3 journées dépendant de la complexité et de la nature du site (site d'information avec ou sans formulaires ou site de commerce en ligne). Un test rapide ne prendrait que quelques heures pour mettre en évidence les faiblesses les plus répandues. Ces tests permettent, en outre de valider la configuration et la pertinence du pare-feu applicatif retenu.

- **Mise en œuvre de liaisons sécurisées**

L'échange de données confidentielles implique la mise en œuvre de liaisons sécurisées, virtuelles (VPN) ou physiques (lignes louées spécialisées).

Réseau Privé Virtuel (VPN pour Virtual Private Network)

- **Objectif**. C'est un tunnel privé de communications chiffré entre l'entreprise et les entités ou personnes dénommées avec qui elle échange des données (coût réduit mais qualité de service liée à l'accès Internet).
  - Fournir un accès distant après authentification aux nomades/télétravailleurs. Selon les solutions, un logiciel spécifique est à déployer sur les postes nomades, ou bien le cryptage est réalisé par les couches standard Windows.
  - Interconnecter plusieurs sites entre eux, tout en offrant une ouverture sécurisée SSL) vers l'Internet.

Trois types de solutions

- Intégrée comme service du pare-feu ;
- Systèmes autonomes placés devant le pare-feu ;
- Systèmes autonomes placés derrière le pare-feu (solutions logicielles).

Pour une **PME**, la seule solution viable consiste à mettre en œuvre une solution avec service de chiffrement intégré. Les protocoles IPsec et SSL/TLS sont utilisés pour assurer la confidentialité et l'authentification mutuelle des échanges (voir fiche 3). Le chiffrement des données peut s'avérer difficile à concilier avec certains trafics multimédia temps réel (par exemple, Voix sur IP, visioconférence).

Lignes louées

L'échange de données entre deux sites distants appartenant à la même entreprise (bureaux-usine par exemple) peut aussi être effectué en louant à un opérateur une liaison spécialisée ou dédiée. Cette solution permet de s'affranchir de toutes les incertitudes liées à l'utilisation d'Internet, mais représente un coût non négligeable de l'ordre de 2K€/mois.

Fiche 9

Gérer et maintenir la politique de sécurité

Les risques liés au changement

Les systèmes d'information évoluent périodiquement. Les changements, souhaités ou subis, peuvent avoir des conséquences sur le niveau minimum de sécurité défini lors de la mise en œuvre de la politique de sécurité :

Changement de responsabilité des collaborateurs
Leur niveau d'accès aux données et applications critiques doit être géré en permanence.

Embauches
Le niveau d'accès aux données et applications critiques des nouveaux collaborateurs doit être défini (voir Charte).

Départs
Supprimer connexions et mots de passe des collaborateurs quittant l'entreprise.

Évolutions
Tester les nouvelles applications, nouveaux postes de travail, nouveaux réseaux, nouvelle version du site web, …

Renouvellement des menaces
Le système d'information doit faire face à des menaces externes sans cesse renouvelées (nouveaux virus ou vers, nouvelles vulnérabilités…).

Une politique de sécurité n'est valable dans le temps que si elle est évaluée régulièrement contre les nouvelles menaces et les changements d'organisation ou de périmètre de l'entreprise.

Maintenance minimum

Mise à jour périodique de la Charte d'Utilisation
L'entreprise se dote de nouveaux moyens de communication, déploie de nouvelles applications, les droits et devoirs des collaborateurs évoluent et doivent impliquer une mise à jour de la Charte.

Gestion des niveaux d'accès
Vous avez choisi un moyen d'authentification (voir fiche 4). Il vous faudra impérativement en assurer un bon suivi. Cette tâche est relativement complexe ; elle dépend des moyens utilisés, des effectifs et du nombre de sites de l'entreprise. Les outils d'administration permettent d'assurer la pérennité des moyens déployés.

Gestion des moyens de protection minimums
Certains moyens de protection sont aujourd'hui incontournables pour une sécurité minimum. Il ne suffit pas de les installer ou de les configurer une fois pour toutes, encore faut-t-il veiller à ce qu'ils soient activés et mis à jour en permanence.

Valider régulièrement la configuration de vos pare-feu
- Pour être efficaces, vos pare-feu ont été configurés au moment de leur mise en place en ligne avec vos politiques de sécurité (voir fiche 1).
- Pour rester efficaces, leur configuration doit être testée périodiquement et les alertes générées contrôlées et corrélées.
- Pour mieux maîtriser ces changements et affiner la configuration de vos firewalls, vous devez connaître les flux applicatifs. Cette connaissance vous permettra en outre de savoir ce que les utilisateurs font des moyens de communication que vous mettez à leur disposition.

Valider les mises à jour correctives régulièrement et tester périodiquement les vulnérabilités de tous les composants logiciels de votre système d'information.

Veiller à l'activation permanente de vos antivirus (et éventuellement anti-spam, anti-spyware). Les antivirus peuvent être désactivés par mégarde ou volontairement, en particulier lorsqu'ils sont déployés sur chaque poste de travail.

Gestion des procédures de sauvegarde
Le contenu de la sauvegarde peut évoluer avec le temps avec l'ajout de nouvelles applications ou de données. Cette contrainte doit être prise en compte et il faut veiller à la complétude des sauvegardes régulièrement.

Moyens

La maintenance (des pare-feu, VPN, antivirus, mises à jour correctives, moyens d'authentification, sauvegarde, gestion des flux applicatifs) peut être réalisée :
- Par les ressources propres de l'entreprise et/ou avec sous-traitance à une société de service qui délèguera du personnel qualifié sur votre site (voir contrats fiche 10).
- Par un prestataire de services ou un Opérateur (appelé MSSP – Managed Security Service Provider) qui gère la sécurité à distance à partir d'un centre mutualisé (SOC - Security Operation Centre) :
  - Gestion du trafic en temps réel 24/24 et 7/7 ;
  - Gestion des incidents en temps réel et conseils d'intervention ;
  - Mise à jour permanente des éléments de protection et des mises à jour correctives ;
  - Gestion des « logs » (archives des anomalies) ;
  - Reconnaissance et enregistrement des attaques ;
  - Rapports journaliers et assistance sur leur interprétation à la demande ;
  - Garantie de service et procédures de support ;
  - Corrélation et interprétation des alertes ;
  - Plan de continuité incluant les procédures de sauvegarde.

Fiche 10

Externaliser la mise en œuvre et la maintenance de la politique de sécurité

La plupart des entreprises font appel aujourd'hui à des prestataires pour leur besoin d'évolution et de maintenance de leur système d'information. Il en va de même pour la sécurité, partie intégrante du système d'information.

Peu d'entreprises disposent des ressources internes pour remplir ces tâches relativement complexes.

La mutualisation permet de réduire les coûts et de s'assurer du maintien permanent d'un niveau acceptable de sécurité.

Installation et configuration

Par un (des) prestataire(s) de services agissant comme un sous-traitant sur votre site.

Ce prestataire installera et configurera les moyens de protection en conformité avec les politiques de sécurité.

Un autre prestataire pourrait contrôler si cet ensemble de tâches a été mené dans les règles de l'art (comme dans d'autres domaines avec le recours à des organismes de certification et de contrôle).

Maintenance sur site

Par un (des) prestataire(s) de services agissant comme un sous-traitant qui se rendra périodiquement sur site pour contrôler que ces moyens de défense répondent aux besoins.

Il est aussi envisageable de faire appel ponctuellement au prestataire en cas de modification des politiques de sécurité (à la suite de conditions imposées par exemple par une client ou un fournisseur, voire par une législation nouvelle).

Un autre prestataire pourrait contrôler si cet ensemble de tâches a été mené dans les règles de l'art (il peut s'agir simplement d'un contrôle très léger, pouvant d'ailleurs être réalisé à distance pour un coût assez faible).

Externalisation

L'externalisation de fonction consiste à confier à un partenaire spécialisé une fonction essentielle à la vie de l'entreprise, mais extérieure à son cœur de métier.

Principes

L'externalisation des systèmes d'information ou de leur gestion prend aujourd'hui des formes très diverses.

Il est difficile de s'y retrouver dans l'univers prolixe de l'externalisation, entre infogérance et tierce maintenance applicative, entre ASP (Application Service Provider) et BSP (Business Service Provider), MSS (Managed Security Services).

Beaucoup d'entreprises ont recours à l'externalisation de la paie voire de la comptabilité. Dans ce cas, l'entreprise transmet les données brutes au fournisseur de service et reçoit en contrepartie les documents de synthèse (déclarations sociales, fiscales, bilans et compte d'exploitation).

Dans le domaine de la sécurité, il existe un service équivalent pour la maintenance totale ou partielle des politiques de sécurité en permettant l'accès à distance aux systèmes en toute sécurité à une société spécialisée, dénommée « Managed Security Services Provider » (MSSP). Ce prestataire peut être votre fournisseur d'accès (Fournisseur d'Accès à Internet [FAI] ou Opérateur de télécommunication) ou une filiale spécialisée de société de service informatique. ▶▶

Accès à ce type de services

L'externalisation de la maintenance des politiques de sécurité semble être une solution particulièrement adaptée pour les PME/PMI, qui ne disposent généralement pas des moyens de veille nécessaires avec des ressources financières et humaines par nature très contraintes.

L'externalisation peut porter sur l'ensemble de la maintenance des politiques de sécurité (voir fiche 9) mais il semblerait opportun de voir apparaître sur le marché une offre spécifique pour les PME/PMI qui porterait au moins sur les moyens de défense minimums (voir fiche 6).

Cette offre adresserait :

- la configuration des pare-feu,
- la gestion des mises à jour des versions correctives (ou veille au minimum),
- la détection des vulnérabilités
- le contrôle des mises à jour de signatures pour les antivirus.

Une telle offre mutualisée pour PME/PMI devrait pouvoir être offerte à un coût acceptable, sous forme d'un abonnement annuel de l'ordre de quelques centaines d'euros pour les plus petites entreprises.

Ces différentes briques prises individuellement font d'ores et déjà partie du catalogue des offres de FAI ou d'Opérateurs.

Une offre globale et accessible financièrement, portant sur la gestion des moyens minimums, serait souhaitable.

Les 10 points

Afin de limiter le nombre de litiges, il conviendra de s'assurer que les documents contractuels (conditions générales et/ou particulières, proposition technique et financière, devis, ...) traitent clairement des 10 points suivants :

clé d'un contrat d'externalisation

Document contractuel
Le contrat mentionne-t-il la liste de l'ensemble des documents qu'il comprend (annexe, cahier des charges, proposition du prestataire…) et les hiérarchise t-il ?
Il est nécessaire de déterminer les documents qui engagent l'entreprise et le prestataire et, en cas de conflit entre ces documents, celui qui prévaudra.

Description des prestations
Les prestations sont-elles précisément décrites ?
Cela permet à l'entreprise de connaître précisément les prestations auxquelles s'engage le prestataire.

Régime de l'obligation du prestataire
Le contrat précise-t-il si le prestataire, ou telle ou telle de ses prestations, est soumis à une obligation de moyens ou à une obligation de résultats ?
L'obligation de résultats portera sur le respect de délais fermes, et/ou d'indicateurs de performance (mesurables). Ces délais et indicateurs devront être stipulés au contrat. Attention en cas d'obligation de moyens, l'entreprise supporte normalement la charge de la preuve de la défaillance du prestataire. Lorsqu'il est possible, le régime de l'obligation de résultats offre plus de sécurité à l'entreprise quant à la bonne exécution des prestations.

Prix des prestations
Est-il prévu que le prix puisse évoluer (hausse ou baisse) ? Notamment, si le prestataire baisse ses tarifs, s'engage-t-il a en faire bénéficier l'entreprise en cours de contrat ?
S'agissant de prestations qui s'inscrivent dans un environnement technologique et un marché qui évoluent vite, il faut que l'entreprise ait l'assurance que son contrat « colle au marché », ce d'autant plus que la durée du contrat sera longue (> 1 an).

Pénalités
Est-il prévu des pénalités en cas de non ou de mauvaise exécution du contrat, en terme de délai et/ou de non-respect de certaines performances (cf. obligation) ?
Elles sont normalement plafonnées (généralement à hauteur de 15 % du montant du contrat). Le contrat doit prévoir l'articulation des pénalités avec les dommages et intérêts que l'entreprise doit pouvoir réclamer par ailleurs. Les pénalités visent à indemniser de manière forfaitaire l'entreprise du fait du retard ou de la non performance. Elles ont en même temps un effet dissuasif pour le prestataire.

Statut des matériels et logiciels
Le contrat devra préciser la propriété et le statut des matériels et des logiciels utilisés par le prestataire dans le cadre de l'exécution du contrat. Seront-ils fournis par l'entreprise ou par le prestataire ? Dans le dernier cas, restent-ils ou pas la propriété de ce dernier ? Seront-ils placés dans l'entreprise ou chez le prestataire ? L'entreprise devra t-elle souscrire ou pas une licence ?
Ce point aura un impact sur la responsabilité de l'entreprise concernant ces matériels et logiciels. Si l'entreprise en est propriétaire ou s'ils sont placés dans ses locaux, elle devra les faire couvrir par ses polices d'assurance.

Étendue de la responsabilité
Le contrat contient-il une clause limitant la responsabilité du prestataire à certains types de préjudice ou en excluant certains autres ?
Le prestataire n'est en principe pas tenu d'indemniser l'entreprise de ses préjudices indirects (notamment de ses pertes d'exploitation), sauf à être expressément prévu au contrat. L'exclusion, par contrat, de certains préjudices directs ou indirects pré qualifiés peut réduire voire supprimer l'indemnisation à laquelle l'entreprise pourra prétendre.

Limitation du préjudice réparable
Le contrat prévoit-il une limitation du montant de la réparation à laquelle l'entreprise pourra prétendre en cas de dommage, tous chefs de préjudice confondus ?
Attention : un plafonnement drastique du montant des dommages et intérêts que pourra réclamer l'entreprise aboutit quasiment à « neutraliser » la responsabilité du prestataire en cas d'inexécution de sa part du contrat.

Cession des droits
Dans le cas où le contrat comporte, à la charge du prestataire, la réalisation ou le développement de tout ou partie d'un logiciel, prévoit-il la cession (autant qu'elle est nécessaire à l'entreprise) de ces créations ?
Attention, en l'absence d'une clause de cession conforme à l'exigence du Code de la propriété intellectuelle, le prestataire reste titulaire des droits d'auteur sur celles-ci. Permet à l'entreprise de s'assurer, autant que de besoin, de la propriété des logiciels qu'elle aura commandé.

Juridiction compétente
Le contrat désigne t-il la juridiction compétente en cas de litige, notamment au plan géographique ? N'est-elle pas trop éloignée du siège de l'entreprise ?
En cas de litige, il est plus facile de plaider près de chez soi que dans la ville, parfois éloignée, du siège du prestataire.

Glossaire

Les termes techniques

5_4_3
5_4_3
Règle 5-4-3. Elle est utilisée quand on parle de répéteurs. On peut connecter 5 segments réseaux à l'aide de 4 répéteurs mais seuls 3 des segments peuvent comporter des ordinateurs ou clients.

802.11i
802.11i
Norme de sécurité sur les liaisons wi-fi. Cette norme tend vers l'utilisation de TKIP pour aboutir à la standardisation de l'algorithme AES.

802.1x
802.1x
Norme définie par l'IEEE concernant l'authentification d'équipements et de postes sur un réseau.

A5
A5
Algorithme secret utilisé en Europe pour le chiffrement dans les téléphones portables.

AAL
AAL
ATM Adaptation Layer
Couche d'adaptation entre les données à transmettre dans le réseau et la couche ATM, par segmentation. Il existe plusieurs types d'AAL : AAL1 pour des flux voix ou vidéo en temps réel et à débit constant, AAL2 pour des flux voix ou vidéo compressées en temps réel et à débit variable, AAL3 ou AAL4 pour des transferts de fichiers, AAL5 pour l'interconnexion de réseaux locaux.

ABR
ABR
Available Bit Rate
Débit disponible. Classe de service définie par l'ATM Forum utilisant la bande passante disponible et garantissant une qualité de service ; applications : trafic LAN sur TCP/IP (ATM).

Acceptation du risque
Risk acceptance
Décision d'accepter un risque traité selon les critères de risque.

ACID
ACID
Logiciel de chiffrement développé par la DGA pour sécuriser tout type de fichiers et répertoires, par un cryptage fort.
- développé à destination de la Défense ou des Administrations.

ACK
ACK
Acknowledgement
Accusé de réception. Il confirme que les données envoyées ont bien étés reçus par le destinataire.

ACL
ACL
Access Control List
Liste de noms d'utilisateurs, de noms de machines ou d'autres entités qui sont, ou ne sont pas, autorisés à accéder à certaines ressources. Ensemble de sélections d'adresse IP source, adresse IP destination, protocole, port source, et port destination, afin de sélectionner des trafics particuliers : exemple « access-list » sur Cisco.

Ad-Hoc
Ad-Hoc
Mode de communication point à point entre stations wifi permettant de se connecter sans passer par un point d'accés.

Adresse IP
IP address
Adresse Internet Protocol. Adresse unique (codée sur 4 octets en IPv4 et 16 en IPv6) permettant d'identifier un ordinateur sur l'Internet, ou un équipement informatique utilisant le protocole TCP/IP (exemple : 192.156.112.123). Indispensable aux échanges d'informations entre les différentes machines, l'adresse IP peut être fixe, c'est-à-dire attribuée pour une durée indéterminée à un même ordinateur, ou bien dynamique, c'est-à-dire attribuée à chaque nouvelle connexion (cas de la majorité des fournisseurs d'accès grand public). Enregistrée dans les fichiers log des serveurs visités, l'adresse IP permet généralement de remonter jusqu'à l'identité physique de l'internaute par le biais de son fournisseur d'accès, dans le cadre d'une procédure judiciaire.

Adresse MAC
MAC address
Numéro unique qui identifie une carte réseau. C'est une adresse de 6 octets de long. les 3 premiers octets définissent le constructeur. Les 3 derniers sont le numéro de série. On l'appelle aussi adresse physique, adresse ethernet ou adresse matérielle.

ADSL
ADSL
Asymetrical Digital Subscriber Line
Technologie de transmission numérique offrant jusqu'à 6 Mb/s sur la paire de cuivre arrivant chez l'abonné. Le débit descendant vers l'abonné est plus important que le débit montant vers le réseau, d'où la terminologie asymétrique.

Advertising
Advertising
Définit l'envoi d'informations régulier sur l'état du réseau entre les routeurs.

Agent
Database agent collector
Ordinateur qui collecte des informations techniques sur le réseau à partir d'une base de données (MIB en environnement SNMP).

AES
AES
Advanced Encryption Scheme
Algorithme de chiffrement symétrique de données.

Agrément
Agreement
Reconnaissance formelle que le produit ou système évalué peut protéger des informations jusqu'à un niveau spécifié dans les conditions d'emploi définies.

Terme technique
English
Signification de l'acronyme
Description

Agrément d'un laboratoire
Laboratory agreement
Reconnaissance formelle qu'un laboratoire possède la compétence pour effectuer des évaluations d'un produit ou d'un système par rapport à des critères d'évaluation définis.

Algorithme cryptographique
Encryption algorithm
Procédé ou fonction mathématique utilisée pour le chiffrement et le déchiffrement. Dans la cryptographie moderne, l'algorithme est souvent public et le secret du chiffre dépend d'un paramètre appelé clef privée.

Analyse de trafic
Traffic analysis
Observation des caractéristiques extérieures du trafic transitant sur un réseau afin de tenter d'en tirer des informations : fréquence des transmissions, identités des tiers communicants, quantités de données transférées. Associées à des informations de nature différente (date de rendez-vous, actualité…) ces éléments peuvent permettre aux adversaires de faire des déductions intéressantes.

Analyse du risque
Risk analysis
Utilisation systématique de données pour l'identification des origines des attaques et l'estimation du risque.

ANT
ANT
ADSL Network Termination
Terminaison de réseau ADSL. Boitier assurant l'interface entre le client de l'opérateur télécom et le central téléphonique.

Anti-Spam
Anti-Spam
D'une manière générale, il ne faut jamais donner suite à un spam. Il faut au contraire prendre l'habitude de supprimer le courrier non sollicité dès sa réception et sans cliquer sur aucun de ses liens.
A titre d'exemples de spam :
- la fausse réponse, envoyée avec comme titre « Re : [phrase accrocheuse] ». Elle tente de se faire passer pour une réponse à un message qui n'a bien sûr jamais été envoyé ;
- le faux message égaré, faisant croire à un message mal adressé. Cordial voire familier, l'expéditeur vante les mérites d'un service ou d'un produit pour lequel il fournit le lien ;
- le faux message de confirmation d'abonnement à une newsletter. Généralement très bref, il fait en réalité la promotion d'un site dont il indique l'adresse ;
- l'adresse surprise, de la forme http://%59%38%36%33.%74%6b qui pique la curiosité et que le spam propose de visiter ;
- le message envoyé avec de véritables adresses emails en copie, ou avec comme adresse d'expéditeur votre propre adresse email afin de passer la barrière psychologique de l'expéditeur inconnu… et les filtres anti-spams ;
- le message au format HTML dont le contenu est une image, afin d'éviter toute présence de texte analysable par les logiciels anti-spam. Il faut rester méfiant vis à vis de ce genre de message dont le but est d'orienter vers un site dont la page est piégée par un virus ou par l'exploitation d'une faille du navigateur. Enfin, les victimes de spamming pourront filtrer le courrier reçu avec les fonctionnalités antispam éventuellement disponibles du logiciel de messagerie : dans Outlook c'est l'onglet « Outils » puis « Assistant Gestion des messages » qui permet de définir une règle de filtrage pour que les messages comportant une expression donnée (par exemple « .kr » pour les victimes de spams coréens) soient redirigés vers un répertoire poubelle. Ne pas hésiter à les dénoncer à l'adresse abuse@serveur « d'envoi ».

Antispyware
Antispyware
Utilitaire capable de rechercher et d'éliminer les espiogiciels. Il s'agit le plus souvent d'un scanner à la demande utilisant une analyse par signatures pour identifier les espiogiciels connus et les désinstaller. Un antispyware est utile pour s'assurer qu'aucun espiogiciel n'est présent sur un ordinateur, ou pour éliminer un espiogiciel récalcitrant lorsque l'utilisateur ne souhaite plus utiliser le logiciel associé. Par contre, l'utilisation de certains antispywares qui permettent de bloquer ou de neutraliser un spyware tout en continuant à utiliser son logiciel associé est assimilable à du piratage, les contrats de licence faisant généralement du spyware une contrepartie obligatoire à l'utilisation gratuite du logiciel associé.

Antivirus
Antivirus
Utilitaire capable de rechercher et d'éliminer les virus informatiques et autres malwares. La détection se fait selon deux principes : une analyse par signatures qui permet de détecter avec d'excellents résultats les virus connus pour peu que les définitions de virus soient régulièrement mises à jour, ou une analyse heuristique qui permet de détecter avec des résultats variables les virus inconnus à partir de leur logique de programmation et le cas échéant de leur comportement à l'exécution. Les antivirus fonctionnent eux-même selon deux principes : un scanner qui permet à l'utilisateur de lancer une analyse d'un disque ou d'un fichier lorsqu'il le souhaite (« on demand »), ou un moniteur qui surveille le système en temps réel (« on access ») et empêche l'utilisateur d'ouvrir un fichier infecté.
La plupart des antivirus comportent un scanner et un moniteur, mais il existe des produits analysant seulement « à la demande » (ex. : antivirus en ligne) voire ne disposant que d'un moniteur (ex. : antivirus génériques).

API
API
Application Program Interface
Collection de fonctions, d'objets de programmation permettant de déployer des applications en masquant des fonctionnalités sous-jacentes accessibles dans un système d'exploitation.

Appl@too
Appl@too
Plate-forme sur laquelle reposent les services de sécurité Cert@too.

Applet
Java applet
En français Appliquette.

Appliquette
Java applet
Petit programme, souvent accompagné de données plus volumineuses que lui, et conçu pour être téléchargé via un réseau à chaque fois qu'on veut l'utiliser, en particulier par un navigateur, qui se chargera de l'exécuter.
Terme surtout utilisé dans la communauté Java.

Terme technique
English
Signification de l'acronyme
Description

Appréciation du risque
Risk assessment
Ensemble du processus d'analyse du risque et d'évaluation du risque.

Architecture
Architecture
La notion d'architecture a plusieurs sens dépendant du contexte (d'après la traduction de la définition IEEE STD 610.12)
1- structure des composants, leurs interrelations, et les principes et règles régissant leur conception et leur évolution dans le temps ;
2- structure organisationnelle d'un système.

ARP
ARP
Address Resolution Protocol
Protocole de recherche d'adresses, liant une adresse « logique » IP avec une adresse « physique » MAC ; contenu dans IP (couche réseau).

ARP poison
Arppoisoning
L'arp poison est une attaque par déni de service dont le but est de duper des postes sur le même réseau ethernet en falsifiant des adresses ARP (MAC) pour des adresses IP données : on fournit à l'outil d'attaque une adresse IP source (un des postes cible de l'attaque) ainsi que son adresse MAC, on fournit ensuite l'adresse IP d'un autre poste cible de l'attaque et une adresse MAC falsifiée (n'importe laquelle), le 1er poste ciblé par l'attaque mettra à jour sa table ARP avec une fausse adresse MAC et ne pourra plus communiquer avec l'autre poste.

ASIC
ASIC
Application Specific Integrated Circuit
Circuit Intégré (« puce ») stockant la table de filtrage d'adresses MAC sur les commutateurs.

Association de sécurité
Security association (SA)
Connexion simplexe (unidirectionnelle) créée pour sécuriser des échanges. Tout le trafic qui traverse une SA se voit appliquer les mêmes services de sécurité. Une SA correspond donc à un ensemble de paramètres, qui caractérisent les services fournis au travers de mécanismes de sécurité comme AH et ESP.

ASP
ASP
Application Service Provider
Fournisseur de services applicatifs délivrés à travers le réseau.

Assurance
Insurance
Propriété d'une cible d'évaluation permettant de s'assurer que ses fonctions de sécurité respectent la politique de sécurité de l'évaluation.

Asynchrone
Asynchronous
Caractéristique d'une liaison dans laquelle l'émetteur et le récepteur ne sont pas synchronisés au préalable. Chaque mot ou caractère possède sa propre synchronisation, le plus souvent à l'aide de bits de « start » et de bits de « stop ».

ATM
ATM
Asynchronous Transfer Mode
Technique de transfert de l'information sous forme de paquets de petite taille constante par multiplexage asynchrone avec répartition temporelle, cherchant ainsi à lier les avantages de la commutation de paquets et de la commutation de circuits. Cellule ATM : élément fondamental du trafic ATM. Sa taille fixe (53 octets) assure la vitesse de transmission des messages et permet au réseau, grâce au mécanisme SAR (Segmentation and reassambly), de gérer simultanément plusieurs types de trafic ou une commutation de paquets classique…).

Attaque
Attack
Exploitation d'une ou plusieurs vulnérabilités à l'aide d'une méthode d'attaque avec une opportunité donnée.
On distingue divers types d'attaque :
- les attaques cryptologiques qui exploitent les failles, mais demandent une bonne connaissance du système (ou la compromission des personnes concernées) ;
- les attaques tempest qui analysent les signaux parasites émis par un matériel électronique ;
- les attaques par piégeage d'équipements qui utilisent la réémission des signaux vers des équipements d'écoute, le brouillage ou la saturation des télécommunications ;
- les attaques informatiques qui mettent en œuvre le contournement des contrôles effectués par un logiciel ou un mécanisme quelconque ainsi que l'usurpation d'identité offrant des privilèges accrus ;
- les attaques par virus, vers, chevaux de troie, bombes logiques qui correspondent toutes à des « contaminations » par programmes ;
- les attaques de réseau qui utilisent les faiblesses connues d'un système pour attaquer un système différent connecté au premier par un réseau ;
- les attaques sur les systèmes de conception qui visent l'implantation de fonctions cachées ;
- les attaques physiques qui relèvent du banditisme et se traduisent par le vol de supports d'informations avec menaces de divulgation ou de destruction des informations.

Attaque active
Active attack
Attaque informatique qui consiste à altérer des informations stockées, en cours de traitement ou transitant sur un réseau, ce qui en compromet l'intégrité. Les perturbations du service dont les manifestations les plus graves peuvent être la saturation d'un réseau, l'insertion de messages parasites, la destruction volontaire ou l'altération d'informations, la réinsertion, le détournement de sessions en cours ou de programmes téléchargés, constituent des exemples d'attaques actives.

Attaque analytique
Analitical attack
Analyse cryptographique qui consiste à étudier l'algorithme de chiffrement afin d'en trouver les failles et d'en déduire la clé de chiffrement utilisée pour produire un cryptogramme.
(Voir aussi Brute-force attack).

Attaque logique
Logic attack
Utilisation non autorisée des ressources d'un système d'information.

Attaque passive
Passive attack
Attaque informatique qui consiste soit à enregistrer, généralement grâce à l'écoute électronique, les informations transitant sur un réseau ou en cours de traitement, soit à copier des informations stockées, ce qui compromet la confidentialité des unes et des autres.
L'indiscrétion, l'analyse de trafic, la copie de fichiers ou de programmes sont les trois manifestations les plus caractéristiques d'une attaque passive.

Attestation de reconnaissance de responsabilité
Established responsability recognition
Attestation ayant pour objet de faire prendre conscience au titulaire d'une décision d'admission ou d'agrément des responsabilités particulières qui viennent s'ajouter à ses responsabilités administratives du fait de l'autorisation d'accès aux informations classifiées.

Attributs de sécurité
Security attributes
Informations (telles que l'identité, le niveau d'habilitation, le besoin d'en connaître, etc.) relatives à un utilisateur autorisé, permettant d'établir ses droits et privilèges.

Audit
Audit
Examen méthodique d'une situation relative à un produit, un processus, une organisation, réalisé en coopération avec les intéressés en vue de vérifier la conformité de cette situation aux dispositions préétablies, et l'adéquation de ces dernières à l'objectif recherché.

Auditabilité
Auditability
Garantie de la maîtrise complète et permanente sur le système, et en particulier de pouvoir retracer tous les événements au cours d'une certaine période.

Audité
Listened
Personne physique ou groupe de personnes ayant en charge le système soumis à audit.
Il assure les deux fonctions suivantes :
- responsable du système,
- responsable de la sécurité du système. Il est l'interlocuteur privilégié de l'auditeur.

Auditeur
Listener
Intervenant (personne seule ou groupe d'individus) responsable de la mission d'audit.

AUI
AUI
Attachment Unit Interface
Équipement de rattachement au support réseau local ; nom donné au câble reliant un coupleur Ethernet au transceiver.

Authenticité
Authenticity
Fait de ne pas permettre, par la voie de modifications autorisées, une perte du caractère complet et juste de l'information.
Consiste à assurer à la fois l'intégrité et l'authentification de l'origine des données.

Authentification
Authentication
Vérification visant à renforcer selon le besoin, le niveau de confiance entre l'identifiant et la personne associée (exemples : le mot de passe est un authentifiant faible, la carte à puce est un authentifiant fort…)
On distingue deux types d'authentification :
1- l'authentification d'un tiers : c'est l'action qui consiste à prouver son identité. Ce service est généralement rendu par l'utilisation d'un « échange d'authentification » qui implique un certain dialogue entre les tiers communicants.
2- L'authentification de l'origine des données : elle sert à prouver que les données reçues ont bien été émises par l'émetteur déclaré. Dans ce cas, l'authentification désigne souvent la combinaison de deux services : authentification et intégrité en mode non connecté. Ces deux services n'ont en effet pas de sens séparément et sont souvent fournis conjointement.

Autorité de certification
Certification authority
Dans une ICP, tierce partie de confiance chargée d'assurer la génération, la signature et la publication des certificats, et leur révocation.

Backdoor
Backdoor
Moyen non documenté permettant d'obtenir des droits privilégiés dans une application ou un ordinateur.
Dans le cas d'une application, la backdoor est souvent un bout de code ajouté par les développeurs pour contourner toute procédure de sécurité et faciliter ainsi les tests ou le dépannage : présente dans la version finale du programme, elle permet à qui en a connaissance d'exécuter l'application sans autorisation voire de s'introduire dans le système. Dans le cas d'un ordinateur, la backdoor est un petit programme installé automatiquement par un virus ou manuellement par une personne malveillante : à l'insu des utilisateurs, elle permet de prendre le contrôle à distance du système, ou lors d'une intrusion de revenir ultérieurement sans avoir à en forcer à nouveau la sécurité. Les antivirus pouvant assez facilement être pris en défaut par les backdoors, le meilleur moyen pour s'en prémunir reste de ne pas exécuter les logiciels ou fichiers joints douteux et d'installer un pare-feu afin de surveiller les entrées/sorties.

Backpressure
Backpressure
Schéma de résolution de blocage qui consiste à repousser les cellules vers les mémoires tampon qui sont placées à l'entrée du système.

Banyan
Banyan
Structure de commutation spatiale définissant un schéma d'interconnexion avec une seule voie d'accès entre les entrées et les sorties. Cette topologie est en général réalisée à partir d'éléments de commutation 2 x 2 et sa complexité est fonction de N log N (N, nombre d'entrées et de sorties).

BAS
BAS
Broadband Access Server
Concentrateur d'accès à haut débit qui collecte le trafic en provenance des DSLAM des clients ADSL pour l'injecter dans le réseau IP de l'Opérateur.

Terme technique
English
Signification de l'acronyme
Description

Beacon
Beacon
Type de trame envoyé périodiquement sur par un point d'accés ou carte 802.11 permettant de découvrir des équipements wi-fi et de donner l'autorisation de parler à une station sur le média.

Besoin de sécurité
Need to security
Définition précise et non ambiguë des niveaux correspondant aux critères de sécurité (disponibilité, confidentialité, intégrité…) qu'il convient d'assurer à un élément essentiel.

BGP
BGP
Border Gateway Protocol
Protocole de routage externe et de dialogue routeur-routeur.

Bi-clé
Key pair
Couple clé publique, clé privée (utilisées dans des algorithmes de cryptographie asymétriques).

Bien
Property
Toute ressource qui a de la valeur pour l'organisme et qui est nécessaire à la réalisation de ses objectifs. On distingue notamment les éléments essentiels et les entités qu'il convient de protéger.

Blowfish
Blowfish
Algorithme de chiffrement inventé et conçu par Bruce Schneier comme remplaçant du DES. Il supporte des clefs d'une taille allant jusqu'à 448 bits. Soumis à aucun brevet, il a été intégré à bon nombre de logiciels.

Bluetooth
Bluetooth
Technique de transmission sans-fil sur de courtes distances (environ 10 métres). Son but est du supprimer les fils entre le poste de travail et ses périphériques. Normalisation IEEE802.15.

Bombe logique
Logic bomb
Antiprogramme à déclenchement différé, qui ne se reproduit pas, activé soit à une date déterminée par son concepteur, soit lorsqu'une condition particulière se trouve vérifiée, ou un ensemble de conditions réunies, et qui, dès lors, produit l'action malveillante pour laquelle il a été conçu.

BOOTP
BOOTP
Bootstrap Protocol
Protocole permettant à un hôte de récupérer son adresse IP.

Brasseur
Digital crossconnect
Commutateur ATM gérant uniquement les numéros de conduits VP.

Broadcast
Broadcast
Diffusion générale d'information à destination de toutes les stations de réception.

Browser
Browser
Logiciel de navigation, « fouineur » d'informations disponibles sur les documents accessibles sur Internet.

Brute-force attack
Brute-force attack
Analyse cryptographique qui consiste à essayer systématiquement toutes les clés de chiffrement possibles ayant pu être utilisées pour produire un cryptogramme.

BS7799-1
BS7799-1
Norme BS7799
Désigne un guide, développé en Grande-Bretagne par le British Standards Institution (BSI), des meilleures pratiques sécuritaires appliquées aux systèmes d'information, applicables à toute entreprise, indépendamment des technologies employées. Publié en février 1995 avec le soutien de son gouvernement et amélioré de manière significative en mai 1999, la norme BS7799 aimerait devenir la référence pour le développement d'une certification « sécurité » en Europe. ISO 17799.

BS7799-2
BS7799-2
Norme BS7799
Ce deuxième volet de la norme BS7799 constitue le référentiel nécessaire pour une certification de la sécurité des systèmes d'information. Il n'existe pas, pour le moment, d'équivalent disponible auprés de l'ISO mais des travaux sont en cours.

Buffers
Buffers
Mémoires tampon utilisées pour stocker les cellules faisant simultanément appel à une même ressource. Leur position (internally buffered, externally buffered) influe sur l'architecture globale du commutateur et sur le type de mécanisme d'arbitrage.

Bump-in-the-stack
Bump-in-thestack
Une implémentation est dite de type bump-inthe-stack si elle s'intercale entre deux couches de la pile de protocole (par exemple, entre PPP et le modem). La logique ainsi insérée est perçue par la couche de rang n comme étant celle de rang n-1 et réciproquement.

CA
CA
Certifying Authority
Organisation ou personne de référence pour la création et la gestion de certificats. On parle aussi de « tiers de confiance ».

CAPI
CAPI
Cryptographic API
Générique de services cryptographique de Microsoft. Les services cryptographiques disponibles dans les programmes Windows (authentification, chiffrement, etc.) sont fournis au moyen de différentes techniques : cartes à puce, périphériques USB, logiciels, etc. Pour ajouter une nouvelle technique, on installe sur l'ordinateur un module répondant à la spécification CAPI. Lorsque Windows aura besoin d'accéder à une technique cryptographique précise, il passera par le l'implémentation de CAPI correspondante.

CBR
CBR
Constant Bit Rate
A débit constant. Classe de Service ATM offrant un débit constant garanti, permettant de transporter des flux (tels que la vidéo ou la voix) nécessitant un contrôle strict de synchronisation et de hautes performances en qualité de service. S'utilise aussi dans le monde des médias pour qualifier un encodage numérique audio ou vidéo à débit constant par opposition à variable (VBR).

CC
CC
Critères Communs
(Voir Critères Communs).

CDMA
CDMA
Code Division Multiple Access
Mode d'accès aux réseaux sans fil, utilisant une même bande de fréquences pour des centaines d'appels simultanés.

CE
CE
Customer Edge router
Routeur d'extrémité installé sur le site du client par le fournisseur d'accès.

Cellule
Cell
Unité de donnée de protocole mise en forme dans le format ATM (cellules de 53 octets : 5 pour l'en-tête, 48 pour les données). L'en-tête comporte notamment un VCI et un VPI.

Certificat
Digital certificate
Objet informatique qui associe une entité à sa clé publique ou à des attributs. Le lien est créé par la signature de l'ensemble des données du certificat par la clé privée de l'autorité qui émet le certificat. Document électronique qui renferme la clef publique d'une entité, ainsi qu'un certain nombre d'informations la concernant, comme son identité. Ce document est signé par une autorité de certification ayant vérifié les informations qu'il contient.

Certification
Certification
Outil de confiance qui conciste en une procédure par laquelle une tierce partie donne l'assurance écrite qu'un processus, une personne, un produit, un service, une organisation… est conforme à des exigences préalablement établies.

CHAP
CHAP
Challenge Handshake Authentification Protocol
Protocole d'échange de données chiffrées d'identification/authentification standardisé par l'IETF. Méthode d'authentification sur un réseau PPP utilisant un système de défi-réponse.

Chapeau blanc
White hat
Désigne un individu qui cherche à pénétrer des systèmes d'information par le biais d'internet, sans intention réelle de nuire. On peut l'assimiler à un « fouineur ».

Chapeau noir
Black hat
Désigne un individu qui cherche à pénétrer des systèmes d'information par le biais d'internet, avec des objectifs clairs de piratage. (Voir aussi Cracker).

Chat
Chat
Service qui permet d'établir des discussions interactives entre des groupes d'usagers (Internet).

Cheval de Troie
Trojan
Programme apparemment inoffensif mais qui facilite une attaque ultérieure par un virus. Antiprogramme qui, introduit dans une séquence d'instructions normales, prend l'apparence d'un programme valide contenant en réalité une fonction illicite cachée, grâce à laquelle les mécanismes de sécurité du système informatique sont contournés, ce qui permet la pénétration par effraction dans des fichiers pour les consulter, les modifier ou les détruire.

Chiffrement
Encryption
Transformation cryptographique d'un ensemble de données (clair) en vue de produire un ensemble chiffré (dit cryptogramme). Le chiffrement est un mécanisme de sécurité permettant d'assurer la confidentialité des données.

Chiffrement de bout en bout
End to end encryption
Chiffrement de données à l'intérieur ou au niveau du système extrémité source, le déchiffrement correspondant ne se produisant qu'à l'intérieur, ou au niveau du système extrémité de destination.

Cible d'étude
Target
Système d'information ou partie de celui-ci qui est soumis à l'étude de sécurité EBIOS.

Cible de sécurité
Security target
Spécification de sécurité d'un produit ou d'un système qui contient la description des fonctions dédiées à la sécurité, les objectifs de sécurité, les menaces qui pèsent sur ces objectifs ainsi que les mécanismes particuliers qui sont employés.

Cible d'évaluation
TOE
Target of Evaluation
Système d'information ou produit qui est soumis à une évaluation de la sécurité. Le commanditaire qui souhaite faire évaluer son produit, doit préciser sa cible d'évaluation : les menaces qui peuvent peser sur son produit dans les conditions d'emploi qu'il précisera, ainsi que les fonctions de sécurité qu'il mettra en œuvre dans son produit.

CIDR
CIDR
Classless Inter-Domain Routing
Méthode d'adressage IP permettant de libérer des adresses IP, ce qui en rend autant de disponibles, en attendant la mise en place d'IPv6.

Terme technique
English
Signification de l'acronyme
Description

CIR
CIR
Commited Information Rate
Débit minimum de transfert d'information que le réseau du Fournisseur s'engage à assurer dans des conditions normales pour chaque CVP.

Circuit
Line
Canal de communication bidirectionnel entre deux entités d'un réseau.

Circuit virtuel
Virtual circuit
En commutation par paquets, voie de communication logique (X25 ou FR par exemple).

Classe
Object class
En programmation par objets, ensemble d'objets ayant les mêmes propriétés.

Classe de débit
Data rate class
Débit maximum du trafic agrégé que l'équipement ATM du Client pourra émettre sur l'accès ATM du réseau du fournisseur.

Clé
Key
Élément d'un codage, sur lequel repose le secret, permettant de chiffrer et de déchiffrer un message.
On distingue deux types de clés :
1- les clefs secrètes, utilisées par les algorithmes symétriques, pour lesquels les clés de chiffrement et de déchiffrement sont égales.
2- bi-clés (couple clé publique, clé privée), utilisées par les algorithmes asymétriques, pour lesquels clé de chiffrement et clé de déchiffrement sont distinctes.

Clé de base
Database key
Clé utilisée pour chiffrer/déchiffrer les clés de trafic transmises sur le réseau ou mémorisées dans les moyens de cryptophonie.

Clé de chiffrement
Encryption key
Série de symboles commandant les opérations de chiffrement et déchiffrement.

Clé de chiffrement de clés
Encryption master key
Clé utilisée exclusivement pour chiffrer d'autres clés, afin de les faire parvenir à un interlocuteur. Une clé de chiffrement de clé a généralement une durée de vie assez longue, par opposition aux clés qu'elle sert à chiffrer.

Clé de session
Session key
Clé cryptographique utilisée seulement pour une durée limitée. Généralement, une clé de session est transportée dans le réseau, chiffrée par une autre clé, et provient par dérivation ou différentiation d'une clé principale.

Clef maîtresse
Master key
Clé servant à générer d'autres clés.

Clé privée
Private key
Dans une infrastructure à clé publique, clé qui n'est connue que de son propriétaire et d'un tiers de confiance. Elle est associée à une clé publique pour former un bi-clé. Ce dernier doit remettre cette clé aux autorités judiciaires ou de la défense nationale en cas de demande.

Clé publique
Public-key
Clé communiquée publiquement. Son intégrité et son authenticité peuvent être assurées par un processus de certification.

Clé secrète
Secret-key
Clé volontairement non publiée nécessaire à la mise en œuvre d'un moyen ou d'une prestation de cryptologie pour des opérations de chiffrement ou de déchiffrement. Dans un système à clés secrètes (ou symétriques), les clés de chiffrement et de déchiffrement sont identiques.

Client
Customer
Système (programme ou ordinateur) accédant à des ressources éloignées, en se branchant via un réseau sur un serveur. Un client « léger » se contente de gérer l'affichage des informations.

CLIR
CLIR
Caller Line Identity Restriction
« Restriction d'identification de la ligne appelante ».
Grâce au CLIR, l'utilisateur qui le désire peut interdire l'affichage de son numéro de téléphone sur l'écran (fixe ou mobile) de la personne appelée.

CLIP
CLIP
Calling Line Identification Presentation
Présentation du numéro qui permet à l'appelé de voir sur l'écran de son téléphone (mobile ou fixe), le numéro des personnes qui l'appellent.

CLP
CLP
Cell Loss Priority
Champ du 4e octet de l'en-tête de la cellule ATM qui indique la priorité de la cellule dans les mécanismes d'arbitrage.

CMIP/CMIS
CMIP/CMIS
Common Management Information Protocol/Services
Protocoles ISO pour l'administration de réseaux.

CMOT
CMOT
Common Management Open Transport
Protocole de liaison entre CMIP/CMIS et TCP/IP.

CAM
CAM
Code d'Authentification de Message
Résultat d'une fonction de hachage à sens unique à clé secrète. L'empreinte dépend à la fois des données et de la clé ; elle n'est donc calculable que par les personnes connaissant la clé. Adjointe aux données sur lesquelles elle a été calculée, elle permet de vérifier leur authenticité (authentification + intégrité).

Communication relative au risque
Interprocess risk communication
Échange ou partage d'informations concernant le risque entre le décideur et d'autres parties prenantes.

Commutation ATM
ATM communication
Schéma d'interconnexion à voie unique, avec un degré d'interconnexion fonction de N2 (N, nombre d'entrées et de sorties).

Condensat(ion)
Data compression
ou Hash
Fonction de compression de données à sens unique, utilisée dans les mécanismes de signature électronique.

Confidentialité
Privacy protection
Propriété d'une information ou d'une ressource de n'être accessible qu'aux utilisateurs autorisés (création, diffusion, sauvegarde, archivage, destruction). Le mécanisme qui permet d'obtenir ce service est généralement le chiffrement des données concernées à l'aide d'un algorithme cryptographique. On parle aussi de confidentialité du trafic lorsqu'on désire empêcher l'analyse du trafic en cachant les adresses source et destination, la taille des paquets, la fréquence des échanges…

Confidentiel Défense
CD
Mention réservée aux informations qui ne présentent pas en elles-mêmes un caractère secret mais dont la connaissance, la réunion ou l'exploitation peuvent conduire à la divulgation d'un secret intéressant la Défense nationale et la sûreté de l'État. [décret du 12/05/81 relatif à l'organisation de la protection des secrets et des informations concernant la Défense Nationale et la sûreté de l'État].

Congestion
Congestion
État dans lequel le réseau ne peut plus assurer tout ou partie de ses engagements de service (QoS, débit…) vis à vis de ses clients.

Connection
Connexion
Relation logique établie entre deux entités. Chaque couche réseau fournit aux couches supérieures un certain nombre de services dont certains sont dits sans connexion et d'autres orientés connexion. Dans un service sans connexion, chaque message est considéré comme totalement indépendant des autres et peut être envoyé à tout moment, sans procédure préalable et sans que le destinataire final soit nécessairement présent à ce moment. C'est le cas par exemple de IP, qui n'offre qu'un service de type remise de datagrammes. Dans un service orienté connexion, l'initiateur de la communication doit d'abord établir un lien logique avec l'entité avec laquelle il désire communiquer. Cette procédure est appelée ouverture de la connexion et implique généralement de se mettre d'accord sur un certain nombre d'options.

Connecté
On-line mode
Mode connecté : un chemin virtuel est réservé pendant tout le temps de la connexion.

Contrôle d'accès
Accesscontrol
Capacité d'autoriser un utilisateur à accéder à une information ou à une ressource à partir de ses droits et des contrôles appropriés exercés sur ses droits (en particulier, identification/authentification). Ce service a pour but d'empêcher l'utilisation d'une ressource (réseau, machine, données…) sans autorisation appropriée.

Cookie
Cookie
Données inscrites par un serveur sur l'ordinateur du client. Elles permettent à ce serveur de se configurer en fonction du client qui l'appelle, de mémoriser des informations spécifiques à la session ou de conserver des informations permanentes.

COPS
COPS
Computer Oracle and Password System
Logiciel permettant de tester les failles de sécurité (notamment les mots de passe) d'une machine Unix.

CORBA
CORBA
Common Object Request Broker Architecture
Standard de gestion d'objets distribués, défini par l'OMG (Object Management Group), association de professionnels de l'informatique orientée objet.

Correctif
Patch
Les éditeurs de logiciels cherchent souvent à améliorer leurs produits pour les doter par exemple de nouvelles fonctionnalités. Le nom d'un logiciel ne change pas pour autant mais il est suivi d'un numéro incrémentiel qui identifie la version du produit parmi celles déjà distribuées ou en cours de développement (ex. : Internet Explorer 6.0 est une version plus récente du navigateur Internet Explorer 5.5). Pour connaître le numéro de version d'un logiciel, il suffit généralement de regarder dans son menu « Aide » ou « ? », puis de choisir « A propos de » ou « Version » : il se présente sous la forme X.XX ou X.XX.xxxxxx. Il est indispensable de connaître le numéro de version de ses principaux logiciels afin de savoir s'ils sont concernés lors de l'annonce d'une faille, ou bien pour appliquer une mise à jour ou un correctif de sécurité correspondant à la bonne version du programme. Lorsque plusieurs versions d'une même application sont disponibles, il est généralement recommandé de ne pas opter pour la toute dernière si celle-ci est très récente, du fait d'un nombre de bogues potentiellement plus importants, ni pour les plus anciennes, pour lesquelles il n'est généralement plus publié de correctif, voire dont les failles ne sont plus même plus annoncées.

CoS
CoS
Classes of Service
Classes de service. Permettent d'assurer un traitement différencié des datagrammes IP transportés sur le réseau, en fonction des exigences de qualité de service de l'application. L'affectation des classes de service aux datagrammes IP issus des applications est assurée par le routeur installé et géré par le Fournisseur sur le site du Client.

COSINE
COSINE
Corporation for Open Systems Interconnexion Networking in Europe
Projet européen (Eurêka) visant une infrastructure de communication avancée à l'échelle de l'Europe.

Terme technique
English
Signification de l'acronyme
Description

Couche
Layer
Concept de base du modèle OSI.

CPL
CPL
Courants Porteurs en Ligne
Technologie de transmission par courants porteurs en ligne, permettant de véhiculer des données numériques et vocales sur les câbles électriques en utilisant les infrastructures existantes.

Cracking
Cracking
(Voir Craquer).

Craquer
Crack, to
Pénétrer illicitement dans un réseau en forçant les contrôles d'accès, par ex. les mots de passe ; ~ déplomber ; angl. : to crack.

CRC
CRC
Cyclic Redundancy Check
Algorithme implémenté dans certains protocoles afin de vérifier la validité des trames ou paquets reçus.

Critères Communs
Common criteria
Intitulé utilisé historiquement pour la norme à la place de l'intitulé officiel de l'ISO : « Critères d'évaluation de la sécurité des technologies de l'information ». Le but de ces critères est de répondre au besoin d'harmonisation au niveau mondial de critères d'évaluation des fonctions de sécurité de produits et de systèmes.
Les CC comprennent 3 parties :
- partie 1 : Introduction et modèle général
- partie 2 : Éxigences fonctionnelles de sécurité
- partie 3 : Éxigences d'assurance de sécurité.

Critères de risque
Risk criteria
Termes de référence permettant d'apprécier l'importance des risques.

Critère de sécurité
Security criterion
Caractéristique d'un élément essentiel permettant d'apprécier ses différents besoins de sécurité.

CRL
CRL
Certificate Revocation List
Liste de certificats révoqués, c'est-à-dire invalidés avant leur terme.

CRM
CRM
Customer Relation Management
Gestion informatisée de la relation client.

Cryptage
Encryption
Terme dérivé de l'anglais to encrypt et souvent employé incorrectement à la place de chiffrement. C'est l'action consistant à obtenir un texte chiffré à partir d'un texte en clair sans connaître la clé. Un exemple concret pourrait être de signer un texte choisi en reproduisant un chiffrement avec la clé privée de la victime. Mais on préfère parler dans ce cas de contrefaçon.

Cryptanalyse
Cryptanalysis
Analyse d'un système cryptographique, et/ou de ses entrées et sorties, pour en déduire des variables confidentielles et/ou des données sensibles. [ISO 7498-2]

Cryptogramme
Cryptogram
Transformé d'un message par une opération de chiffrement.

Cryptographie
Cryptography
Science permettant d'assurer la sécurité des systèmes de traitement de l'information. Discip line incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur modification passe inaperçue et/ou d'empêcher leur utilisation non autorisée. [ISO 7498-2]

Cryptographie asymétrique
Asymmetric cryptography
Système de cryptographie à clé publique. Chaque intervent possède une clé secrète S et une clé publique P. La clé P, dérivée de S par une fonction à sens unique, est publiée.

Cryptographie symétrique
Symmetric cryptography
Système de cryptographie à clé privée (ou secrète), reposant sur le partage de cette clé entre tous les intervents.

Cryptologie
Cryptology
Étude scientifique de la cryptographie et de la cryptanalyse.

Cryptopériode
Cryptoperiod
Période de temps pendant laquelle les clés d'un système restent inchangées.

C-SET
C-SET
Chip - Electronic Secure Transaction
Extension française de la norme SET développée par le GIE Cartes Bancaires en vue de standardise le paiement en ligne en France.

CSMA/CA
CSMA/CA
Carrier Sense with Multiple Access/Collision Avoidance
Méthode d'accés qui écoute si la ligne n'est pas utilisée avant un envoi de signal. Si elle est utilisée, la station attend puis réemet. Les collisions sont évitées avant l'envoi de données selon un algorithme de calcul. Utilisé dans les réseaux sans-fils.

CSMA/CD
CSMA/CD
Carrier Sense with Multiple Access/Collision Detection
Méthode d'accés qui écoute si la ligne n'est pas utilisée avant un envoi de signal. Si elle est utilisée, la station attend puis réemet. Elle détecte la collision (l'envoi de deux signaux simultanés provenant de deux stations différentes).
Cette méthode d'accés est utilisé sur Ethernet.

CVC
CVC
Circuit Virtuel Commuté
Circuit virtuel établi à travers le réseau du Fournisseur par une communication commutée.

CVP
CVP
Circuit Virtuel Permanent
Circuit virtuel établi en permanence entre deux Matériels à travers le réseau du Fournisseur.

Cyberwoozle
Cyberwoozle
(Syphonnage des données)
Dispositif visant à récupérer des informations sur une entreprise en se servant des paramètres fournis par les navigateurs internet.

Datagramme
Datagram
Bloc d'information (données, adresses source et destination) transmis « en vrac », nécessitant un dispositif de réassemblage à l'arrivée. Ce sont donc des paquets totalement indépendants les uns des autres et circulant en mode non connecté. Par exemple, les paquets IP ou UDP sont des datagrammes. Chaque paquet de type datagramme transite à travers le réseau avec l'ensemble des informations nécessaires à son acheminement, et notamment les adresses de l'expéditeur et du destinataire. Le routage étant effectué séparément pour chaque datagramme, deux datagrammes successifs peuvent donc suivre des chemins différents et être reçus par le destinataire dans un ordre différent de celui d'émission. En cas de problème dans le réseau, des datagrammes peuvent être perdus. Le destinataire doit donc ré-ordonner les datagrammes pour reconstituer les messages et contrôler qu'aucun datagramme n'est perdu.

DEA
DEA
Data Encryption Algorithm
Algorithme de DES.

Déchiffrement
Decryption
Opération inverse d'un chiffrement réversible.

Décryptage
Decryption
Tentative de retrouver un message clair à partir d'un cryptogramme dont on n'est pas le destinataire, en « cassant » le chiffrement d'un texte de façon à retrouver le texte en clair sans connaître la clé.

DDOS
DDOS
Distributed Denial Of Service
Également appelée SCA (Saturation Computer Attack), c'est une attaque informatique qui consiste à envoyer des milliers de messages depuis des dizaines d'ordinateurs, dans le but de submerger les serveurs d'une société, de paralyser pendant plusieurs heures son site Web et d'en bloquer ainsi l'accès aux internautes. Cette technique de piratage, assez simple à réaliser, est possible grâce à certains logiciels qui donnent l'instruction à des dizaines de serveurs d'inonder de messages des sites Web, souvent des sites commerciaux connus, pour provoquer un blocage du système informatique, appelé refus de service ou déni de service. Ces cyber-attaques, jugées comme de la pure malveillance, ne font que bloquer l'accès aux sites, sans en altérer le contenu.

Deep inspection
Deep inspection
Technique récente de firewalling permettant la détection d'attaques via la fragmentation de paquets.

Deflection
Deflection
Mécanisme de résolution du blocage qui consiste à dévier les cellules concurrentes vers les mémoires tampon sur un chemin autre que la voie la plus courte entre le point de blocage et l'entrée ou la sortie.

Déguisement
Impersonation
Acte de prétendre être une autre entité dans le but d'accéder aux ressources de celle-ci ; angl : masquerade.

Délai de Transit
Round Trip Delay
Le délai de transit correspond au temps de transmission Aller-Retour d'un datagramme IP de 128 octets, entre 2 points donnés du réseau de l'Opérateur. Ces points peuvent être des PE ou des CE. Dépassé ce délai, les collisions ne sont plus détectées.(En Ethernet 10Mb/s, il est de 51,2µs. En Fast-Ethernet 100Mb/s il est de 5,12µs).

Déni de service/DoS
Denial of service
Attaque ayant pour but de bloquer le fonctionnement de machines ou de services, par saturation d'une ressource. Impossibilité d'accès à des ressources pour des utilisateurs autorisés ou introduction d'un retard pour le traitement d'opérations critiques. [ISO 7498-2]. Exemple : ICMP flood, Smurf, …

DES
DES
Data Encryption Standard
Algorithme symétrique de chiffrement de données.

Désimlockage
Unblocking SIM
Les téléphones des packs sont liés à leur carte SIM d'origine. Le désimlockage se fait grâce à un code fourni par l'opérateur et permet à votre mobile de fonctionner avec une autre carte SIM. Cette opération est gratuite 6 mois après l'achat.

Détournement d'appels
Call splashing
Procédé qui consiste, pour un fournisseur indépendant de services téléphoniques, à acheminer un appel interurbain, d'un endroit différent de celui à partir duquel il est émis, et qui a pour conséquence d'en augmenter le coût. Exemple fictif : vous téléphonez de Bordeaux par l'opérateur X, mais les installations du fournisseur indépendant sont à Londres, ce dernier achemine donc votre appel vers le réseau que vous avez choisi, mais à partir de Londres. Ne pas confondre avec la Déviation d'appel (Call deflection) qui est un complément de service téléphonique qui permet de faire acheminer un appel reçu d'un terminal vers un autre avant même que toute communication soit établie.

Terme technique
English
Signification de l'acronyme
Description

Détournement informatique
ADP embezzlement
Automatic Data Processing emblezzlement
Action de soustraire à son profit des biens informatiques auxquels un accès a été accordé. Le détournement n'implique pas de modification des fichiers, ni ne se manifeste par aucune appropriation illégale d'un bien matériel.

Disponibilité
Availability
Propriété d'accessibilité dans des conditions définies d'horaires, de délais et de performances des informations et des fonctions par les utilisateurs autorisés.

Distribution
Distribution system
Délivrance par une autorité de distribution aux parties communicantes des clés à mettre en œuvre pour chiffrer ou déchiffrer des informations, y compris, le cas échéant, des éléments propres à d'autres abonnés.

DMZ
DMZ
Demilitarized Zone
Zone Démilitarisée - Une DMZ contient un ou plusieurs services accessibles par internet tout en interdisant l'accés au réseau privé.

DNS
DNS
Domain Name Service
Serveur de Nom de Domaine, effectuant la traduction du nom alphanumérique d'une machine (ex : machine1@francetelecom.com) en son adresse IP (ex : 194.156.178.12) ; donc convertit des noms explicites en adresses IP.

Domaine
Domain name system
Entité logique définie par l'administrateur du réseau local lui permettant de gérer plusieurs serveurs physiquement distincts.

Domaine de diffusion
Multicast domain
Ensemble de nœuds affectés par une même trame broadcast.

Domaine de collision
Collision domain
Ensemble de nœuds affectés par une collision commune.

Domain Name
Domain Name
(Voir Nom de Domaine).

Dongle
Hardware key
Périphérique disposant de fonctions cryptologiques et se connectant sur un port USB.

DR
Narrowcast
Diffusion restreinte
Des informations, non classifiées, qui concernent le patrimoine scientifique, technique, industriel, économique ou diplomatique, sont du domaine de la diffusion restreinte.

DRM
DRM
Digital Right Management
Méthode de gestion et de création des droits d'utilisation.

DSL
DSL
Data Subscriber Line
Ensemble de techniques de transmission utilisant la paire torsadée téléphonique.

DSLAM
DSLAM
Digital Subscriber Line Access Multiplexer
Équipement de collecte des clients ADSL, connecté au réseau IP via un BAS.

DSU/CSU
DSU/CSU
Data Service Unit/Channel Service Unit
Équipement reliant la ligne de l'opérateur au routeur de l'entreprise. Elle sert de synchronisation avec le routeur de l'entreprise et celui de l'opérateur.

EAI
EAI
Enterprise Application Intergration
Ensemble de technologies qui permet aux logiciels d'une entreprise de communiquer et de travailler de concert.

EAL
EAL
Niveau de certification en matière de sécurité, attribué à différents types de périphériques (carte à puce par exemple). Ces niveaux sont déterminés par une norme ISO internationale et attribués en France par la DCSSI.

EAP
EAP
Extensible Authentification Protocol
Protocole d'authentification par mot de passe ou clés publiques. C'est une extension du protocole PPP.

ebXML
ebXML
electronic business XML
Version de XML adaptée aux contenus de n'importe quel métier.

EBIOS
EBIOS
Expression des Besoins et Identification des Objectifs de Sécurité
Méthode d'analyse des risques en SSI permettant de rédiger différentes formes de cahier des charges SSI (FEROS, profils de protection…) et de contribuer à l'élaboration du référentiel SSI d'un organisme (schéma directeur SSI, politique de sécurité des systèmes d'information, tableaux de bord SSI…). Elle constitue un outil indispensable à la gestion des risques SSI. La méthode EBIOS se décompose en 4 étapes :
- l'étude du contexte
- l'expression des besoins de sécurité
- l'étude des risques
- l'identification des objectifs de sécurité.

Écoute
Wiretapping
Interception passive, donc sans altération, d'une information transitant sur une ligne de télécommunications ; l'écoute constitue une violation de la confidentialité.

EDI
EDI
Échange de Données Informatisées/
Electronic data interchange
Permet l'échange par le réseau de documents commerciaux normaliséstels que factures ou bons de commande.

EIGRP
EIGRP
Enhanced Interior Gateway Routing Protocol
Protocole de routage hybride combinant un routage par état de lien et à vecteur de distance.

EIR
EIR
Equipment Identity Registrer
Base de données qui regroupe les caractéristiques des téléphones mobiles volés, perdus ou n'ayant pas été homologués dans le monde entier. Chaque mobile possède un numéro d'identifiant (l'IMEI). Ce numéro commence par le code du pays, suivi par deux chiffres identifiant le fabricant, le numéro de série et un chiffre aléatoire. Cette base permet aux opérateurs d'identifier les utilisateurs de mobiles volés et ainsi d'empêcher les possesseurs frauduleux de ces mobiles d'accéder à leur réseau.

Élément essentiel
Critical element
Information ou fonction ayant au moins un besoin de sécurité non nul.

Élément menaçant
Sensitive element
Action humaine, élément naturel ou environnemental qui a des conséquences potentielles négatives sur le système. Elle peut être caractérisée par son type (naturel, humain, ou environnemental) et par sa cause (accidentelle ou délibérée). Dans le cas d'une cause accidentelle, elle est aussi caractérisée par une exposition et des ressources disponibles.
Dans le cas d'une cause délibérée, elle est aussi caractérisée par une expertise, des ressources disponibles et une motivation.

Empreinte
Digest
Aussi appelé condensé. Chaîne de taille fixe obtenue par application d'une fonction de hachage à un ensemble de données.

Émulateur
Emulator
Logiciel ou dispositif électronique permettant de faire fonctionner un système à la façon d'un autre, par exemple un navigateur web à la façon d'un terminal.

Encapsulation
Encapsulation
Technique qui consiste à inclure un paquet muni d'un protocole à l'intérieur d'un autre paquet muni d'un autre protocole afin que ce dernier transporte le premier paquet. L'intérêt peut être soit de rendre possible l'utilisation du protocole encapsulé sur une liaison possédant le protocole encapsulant, soit de faire profiter le protocole encapsulé des services rendus par le protocole encapsulant. La façon la plus « logique » d'utiliser l'encapsulation est d'encapsuler un protocole de niveau supérieur dans un protocole de niveau inférieur, mais il est également possible de faire l'inverse.

Enjeu
Stakes
Ce que l'on peut gagner ou perdre dans une entreprise, un domaine d'activité ou un projet. L'enjeu peut être financier, commercial, organisationnel, technique… (exemples : gains financiers, améliorations de l'image de marque, remplir les obligations de service public, accroissement des avances technologiques…).

Entité
Entity
Bien qui peut être de type organisation, site, personnel, matériel, réseau, logiciel, système.

Équilibrage de charge
Load Balancing
Fonctionnalité sur des serveurs ou équipements identiques permettant de se partager mutuellement la charge des opérations à effectuer.

ERP
ERP
Enterprise Resource Planning
Progiciel de gestion intégré, permettant de gérer l'ensemble des processus d'une entreprise.

Estimation du risque
Risk assessment
Processus utilisé pour affecter des valeurs à l'opportunité et aux pertes qu'un risque peut engendrer.

Ethernet
Ethernet
Topologie de réseau informatique utilisant la norme bande de base 802.3, la méthode d'accès CSMA/CD et pouvant atteindre des débits théoriques de 1 à 1000 Mb/s.
Conçu par Intel, Xerox et Digital.

Ethernet commuté
Switched Ethernet
Technique de commutation de trames Ethernet.

Évaluation
Security assessment
Estimation de la sécurité d'un produit ou d'un système par rapport à des critères d'évaluation définis.

Évaluation du risque
Risk bench
Processus de comparaison du risque estimé avec des critères de risque donnés pour déterminer l'importance d'un risque.

Exigence d'assurance de sécurité
Must security insurance
Spécification d'assurance des fonctions de sécurité à mettre en œuvre pour participer à la couverture d'un ou plusieurs objectifs de sécurité, et portant généralement sur l'environnement de développement du système.

Terme technique
English
Signification de l'acronyme
Description

Exigences de sécurité
Security requierements
Expression de besoins de sécurité et de contrôle associés à une information ou à une ressource. Elles sont spécifiées en terme de : confidentialité, intégrité, disponibilité, imputabilité, nonrépudiation et de contrôle d'accès.

Expertise
Skills-based level
Niveau attendu de compétence technique d'un élément menaçant dont la cause est délibérée. Ce niveau peut être caractérisé par des compétences techniques faibles, moyennes ou fortes.

Exposition
Exposure
Niveau d'exposition naturelle d'un système-cible face à un élément menaçant dont la cause est accidentelle. Ce niveau peut être caractérisé par une exposition faible, modérée ou forte.

FAI
ISP
Internet service provider
Fournisseur d'Accès Internet.

Faille
Failure
Trou de sécurité.

Fail-over
Fail-over
Technique permettant de « passer au-dessus » des pannes. Ce n'est pas de la tolérance aux pannes, mais cela y ressemble. Ici, on fait en sorte de pouvoir continuer à fonctionner en mode dégradé.

FAR
FAR
False Accept Rate
Pourcentage relatif au fait qu'un utilisateur invalide est incorrectement traîté (acceptance) dans une procédure d'authentification par détection biométrique.
On parle d'erreur de « Type 2 ».

Faux négatif
False negative
On désigne par ce terme l'absence de détection d'une vulnérabilité ou le non déclenchement d'une alerte d'intrusion. L'IDS ou l'outil de détection de vulnérabilités idéal ne devrait jamais créer de faux négatifs. En cas de doute, on préfère obtenir un faux positif qui réclamera une investigation plus poussée, même si elle est inutile.

Faux positif
False positive
On désigne par ce terme une alerte d'intrusion ou la détection d'une vulnérabilité non avérée. La génération de faux positifs par les IDS ou les outils de contrôle de failles est inévitable. Pour diminuer leur pourcentage, on recommande de corréler les informations obtenues par différentes sources.

FCS
FCS
Frame Check Sequence
Séquence qui vérifie l'intégrité de l'en-tête de la trame.

FDDI
FDDI
Fiber Distributed Data Interface
Structure normalisée de réseau MAN à double anneau en technologie optique, à jeton circulant.

FEROS
FEROS
Fiche d'Expression Rationnelle des Objectifs de Sécurité
Dans le cadre d'une démarche sécurité, document définissant les objectifs de sécurité que doit rendre le système ou le service à développer.

FIFO
FIFO
First In First Out
Méthode de coordination d'un flux de données dans une file d'attente. Les données reçues en premier sont les premières à ressortir.

FIREWALL
FIREWALL
(Voir Pare-Feu).

Fonction
Facility
Traitement ou ensemble de traitements contribuant au fonctionnement d'une activité d'un organisme, qui crée, modifie, détruit ou transport des informations.

Fonction à sens unique
Irreversible function
Une fonction à sens unique est une fonction facile à calculer mais difficile à inverser. La cryptographie à clef publique repose sur l'utilisation de fonctions à sens unique à brèche secrète : pour qui connaît le secret (i.e. la clé privée), la fonction devient facile à inverser.

Fonction de hachage
Hash coding
Fonction qui transforme une chaîne de caractères en une chaîne de caractères de taille inférieure et fixe. Cette chaîne est appelée empreinte (digest en anglais) ou condensé de la chaîne initiale. Cette fonction satisfait deux propriétés. Il est difficile pour une image de la fonction de calculer l'antécédent associé. Il est difficile pour un antécedent de la fonction de calculer un antécédent différent ayant la même image.

Fonction de hachage à sens unique
Irreversible hash coding
Fonction de hachage qui est en plus une fonction à sens unique : il est aisé de calculer l'empreinte d'une chaîne donnée, mais il est difficile d'engendrer des chaînes qui ont une empreinte donnée. On demande généralement en plus à une telle fonction d'être sans collision, c'est-à-dire qu'il soit impossible de trouver deux messages ayant la même empreinte.

Fonction de sécurité
Security function
Mesure technique, susceptible de satisfaire un objectif de sécurité.

FR
FR
Frame Relay
Relais de Trame - Protocole normalisé de transmission de données de haut débit, de niveau 2, fondé sur une version allégée de la norme X25.

FRAD
FRAD
Frame Relay Access Device
Concentrateur permettant de se raccorder à un réseau Frame Relay et offrant différents types de services (FR, Voix sur FR, X.25, IP etc.). Équipement assimilable à un routeur spécialisé.

Fragmentation
Compartmentalization
Découpage en plusieurs morceaux d'un paquet si les données à envoyer dépassent le MTU.

Fraude informatique
Computer fraud
Délit informatique qui consiste à utiliser ou à falsifier des données stockées, en traitement ou en transit, afin d'en retirer des avantages personnels ou des gains financiers. Les fraudes informatiques se répartissent en trois grandes catégories :
a) la falsification des états financiers ;
b) le détournement d'actifs ;
c) la vente ou la divulgation d'informations. Le système informatique sert d'instrument dans la préparation, l'exécution et le camouflage de la fraude.

FTP
FTP
File Transfer Protocol
Protocole de transfert de fichiers (utilisé avec TCP) ; application régissant ces transferts de fichiers (Internet).

Géolocalisation
Position determination technology
Système qui permet d'être localisé géographiquement par le biais de son téléphone mobile afin de recevoir des informations propres à l'endroit où l'on se trouve.

Gestion du risque
Risk management
Activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque. La gestion du risque inclut typiquement l'appréciation du risque, le traitement du risque, l'acceptation du risque et la communication relative au risque.

GFC
GFC
Generic Flow Control
Protocole de la couche ATM s'assurant que chacun des nœuds ATM peut transmettre.

GIX
GIX
Global Internet eXchange
Nœud d'interconnexion internet, où les opérateurs internet s'échangent du traffic selon une logique de peering.

GOST
GOST
(GOsudarstvennyi STandard Soyuza SSR/ Standart gouvernemental de l'URSS)
Algotithme de chiffrement par bloc, à clef symétrique. GOST fonctionne à la manière du DES sauf qu'il utilise, entres autres, une clef de 256 bits et non pas 56.

GPRS
GPRS
General Packet Radio Service
Service de radiocommunication. Technologie en mode paquet permettant d'accéder aux services Internet/Intranet à l'aide de multiples canaux radio qui sont attribués à un utilisateur ou partagés par plusieurs utilisateurs.

GRE
GRE
Generic Routing Encapsulation
Méthode d'encapsulation de données permettant de faire passer du flux d'un type de réseau sur un autre type de réseau. On parle de tunnel GRE. Développé par CISCO.

GTR
Time to repair warrenty
Garantie de Temps de Rétablissement
Engagement contractuel du fournisseur à rétablir, en un temps déterminé après sa prise en compte, le fonctionnement d'un service dont bénéficie le Client.

GSS
GSS
Generic Security Service
Interface d'application générique de sécurité pour les applications distribuées. Les bibliothèques GSS fournissent des services de sécurité aux applications communicantes d'une façon générique. Les API (Application Programming Interface) GSS supportent plusieurs mécanismes de sécurité (Kerberos, SESAME, DCE), cachent à l'utilisateur final la complexité des mécanismes mis en œuvre, sont complètement indépendantes des protocoles de communication mis en œuvre. Elles permettent d'établir un contexte de communication sûr avec une entité distante, après traitement d'un ou plusieurs jetons d'authentification par le module de sécurité, et liaison par une signature cryptographique de ce contexte avec l'identification d'une voie logique ou physique (channel bindings) et permettent en particulier la signature et vérification de messages.

Habilitation
Authorization
Procédure par laquelle une entité autorise formellement un individu à exercer une série de prérogatives. La notion d'habilitation répond à un besoin de confidentialité.
On distingue :
- la diffusion personnalisée réservée aux documents stratégiques et qui demande contrôle d'accès, identification et authentification forte des destinataires, traçage des opérations réalisées ;
- la diffusion contrôlée qui impose de connaître les détenteurs successifs de l'information, mêmes contraintes que précédemment sans traçage ;
- la diffusion interne qui concerne tout le personnel et ne demande qu'un contrôle d'accès avec identification et authentification faible des destinataires ;
- la diffusion libre destinée au grand public donc sans contrôle.

Hacker
Hacker
(Voir Pirate).

Handshake
Handshake
(Voir Négociation).

Terme technique
English
Signification de l'acronyme
Description

Hash(ing)
Hash(ing)
(Voir Condensat(ion)).

HDLC
HDLC
High Level Data Link Control
Protocole synchrone de liaison de données (niveau 2), permettant d'améliorer le rendement des supports utilisés. Le contrôle de redondance des informations transmises est assuré par un Code Cyclique ; X25 niveau 2 et FR sont basés sur HDLC.

Hearth-beat
Hearth-beat
Lien physique (généralement un cable croisé) entre deux firewalls qui sont configurés en mode haute-disponibilité afin de connaître leur état respectif.

Hiperlan
Hiperlan
High Performance Radio LAN
Standard de WLAN de l'ETSI.

Hoax
Hoax
Canulars : ils prétendent décrire un virus extrêmement dangereux, ils utilisent un langage pseudo-technique pour rendre impressionnant les faits relatés, ils prétendent que le rapport a été issu ou confirmé par une entreprise bien connue, ils demandent de faire suivre cette alerte à tous vos amis et collègues.

Homologation
Agreement
Autorisation d'utiliser, dans un but précis ou dans des conditions prévues, un produit ou un système (en anglais : accreditation). C'est l'autorité responsable de la mise en œuvre du produit ou du système qui délivre cette autorisation, conformément à la réglementation en vigueur.

Honey Pot
Honey Pot
De façon littérale : « Pot de miel ». Dans le domaine de la sécurité informatique, par boutade, c'est ainsi que l'on désigne un serveur chargé d'attirer des pirates dans le but d'étudier leurs méthodes d'attaques. La machine qui sert de leure doit être suffisamment attractive pour éveiller l'intérêt mais elle ne doit receler aucune information confidentielle réelle ! Le pirate est assimilé à un gros ours balourd comme ont les rencontre parfois dans les dessins animés. :-)

Horodatage
EDR
Electronic date recognition
Service qui associe de manière sûre un événement et une heure afin d'établir de manière fiable l'heure à laquelle cet événement s'est réalisé.

Hotspot
Hotspot
Appellation désignant une zone de couverture permettant à tout possesseur d'ordinateur équipé Wi-Fi de se connecter à internet sans fil.

HSDPA
HSDPA
High Speed Downlink Packet Access
Évolution du standard UMTS permettant la transmission de données en mode paquets dans le sens station de base vers abonné à un débit maximal de 10 Mb/s.

HSRP
HSRP
Protocole propriétaire CISCO permettant à un routeur d'être en secours d'un autre routeur situé sur le même réseau Ethernet, sur la base d'une adresse IP virtuelle commune. Protocole inspiré du protocole normalisé VRRP.

HTML
HTML
HyperText Markup Language
Langage de marquage de documents hypertexte, dérivé de SGML ; langage devenu standard de fait pour la conception de « pages » sur l'Internet.

HTTP
HTTP
HyperText Transfer Protocol
Protocole de transfert de données Internet utilisé pour gérer le dialogue (requêtes-réponses) entre browsers et serveurs Web.

Hypertexte
Hypertext
Système généralisé de manipulation et de navigation interactive dans les documents textuels, grâce à des liens.

Hypothèse
Hypothesis
Postulat, posé sur l'environnement opérationnel du système, permettant de procurer les fonctionnalités de sécurité attendues.

IAPRP
IAPRP
Inter-Acess Point Roaming Protocol
Protocole utilisé par les points d'accés wi-fi pour faire de l'itinérance (roaming).

ICMP
ICMP
Interface Control Message Protocol
Protocole d'envoi de messages de contrôle et d'information. Les messages ICMP sont transportés dans la partie données des paquets IP. Utilisé par la commande ping. Protocole de niveau 3 intégré à IP qui permet de connaître l'état d'un nœud ou d'un réseau.

ICP
ICP
Infrastructure à clés publiques - en anglais PKI
Ensemble de composants, fonctions et procédures dédiés à la gestion de clés et de certificats. Une ICP offre en général les services suivants : contrôle de validité de demandes de certificats, fabrication et signature de certificats, publication de certificats dans un annuaire, révocation de certificats, publication des révocations.

ICV
ICV
Integrity Check Value
« Valeur de vérification d'intégrité ». Cette valeur est calculée par l'expéditeur sur l'ensemble des données à protéger.

L'ICV est alors envoyée avec les données protégées.
En utilisant le même algorithme, le destinataire recalcule l'ICV sur les données reçues et la compare à l'ICV originale.
Si elles se correspondent, il en déduit que les données n'ont pas été modifiées.

Identification
Identification
Propriété permettant d'établir un lien avec une personne physique à qui on associe un identifiant (exemple : nom, code alliance, numéro de sécurité sociale…).

IDS
IDS
Intrusion Detection System
Système de détection d'intrusion basé sur un équipement de type « sonde réseau » (ou « sonde système ») permettant de détecter en temps réel les tentatives d'intrusion sur un réseau (ou sur un système). Terme générique faisant référence aux équipements ou logiciels chargés de détecter des intrusions. Les IDS permettent de garder une trace d'évènements anormaux, de signaler en temps réel des opérations jugées illégales et même de réagir sur la base de signatures d'attaques ou l'analyse de comportements (heuristique). On distingue deux types d'IDS : les NIDS (Network Intrusion Detection Systems) pour les réseaux et les HIDS (Host-based Intrusion Detection Systems) pour les serveurs.

IGP
IGP
Interior Gateway Protocol
Nom générique des protocoles de routage utilisés dans les réseaux sous même entité administrative.
Exemple : RIP, OSPF, IS-IS.

IGRP
IGRP
Interior Gateway Routing Protocol
Protocole de routage link-state spécifique au constructeur Cisco.

IMEI
IMEI
International Mobile Equipment Identity
Numéro d'identification unique à chaque téléphone mobile. Il peut être utilisé afin de bloquer un appareil volé. Il est donc conseiller de le noter au préalable. Ce code à 15 chiffres est présenté sous la forme de quatre nombres séparés par -, /, ou des espaces (par exemple : 449176/08/005766/1) ou d'un seul nombre à 15 chiffres (exemple : 332167404758456). Il se trouve au dos du mobile sous la batterie, ainsi que sur l'étiquette du coffret d'emballage. Il est également consultable directement depuis son mobile en composant : *#06# sur le clavier.

Impact
Impact
Conséquence sur l'entreprise de la réalisation d'un risque ou d'une menace.

Imputabilité
Accountability
Capacité de pouvoir attribuer, avec le niveau de confiance exigé, une action sur une information ou une ressource à un utilisateur déterminé.

IMS
Maximum service interruption
Interruption Maximale de Service
Temps maximal pendant lequel un site du Client est indisponible. Un site Client bénéficiant du service de secours de bout en bout est considéré comme indisponible lorsqu'il ne peut communiquer ni par le lien nominal ni par le lien de secours.

Information
Information
Élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, un enregistrement ou un traitement.

Infrastructure
Infrastructure
Le terme infrastructure a une signification différente selon le contexte. Fréquemment, l'infrastructure désigne le matériel ou a un rapport direct avec lui, et la plupart du temps le terme inclut les logiciels et les télécommunications.

Intégrité
Integrity
Propriété d'exactitude et de complétude des informations et des fonctions de l'information traitée. Celles-ci ne doivent pouvoir être modifiées que par un acte volontaire et légitime. Dans le cadre de communications, ce service consiste à permettre la détection de l'altération des données durant le transfert.
On distingue deux types d'intégrité :
1- l'intégrité en mode non connecté permet de détecter des modifications sur un datagramme individuel, mais pas sur l'ordre des datagrammes.
2- l'intégrité en mode connecté permet en plus de détecter la perte de paquets ou leur réordonnancement.
L'intégrité est très liée à l'authentification de l'origine des données, et les deux services sont souvent fournis conjointement.

Internet
Internet
Réseau interconnectant la plupart des pays du monde. Fondé sur le protocole de communication TCP/IP indépendant du type de machine, du système d'exploitation et du support de transport physique utilisé. Internet fonctionne de manière décentralisée, et les routes empruntées par les paquets d'informations ne sont pas figées.

Intrusion
Intrusion
Pénétration non autorisée d'un système ou d'un réseau.
On distingue deux types d'intrusion :
1- l'intrusion passive, qui affecte la confidentialité des informations et consiste à écouter ce qui transite sur un réseau.
2- l'intrusion active qui cherche à modifier ou détruire des informations ou d'attenter à la continuité de service du système ou du réseau.

IOS
IOS
Internetwork Operating System
Nom du système d'exploitation des machines CISCO.

Terme technique
English
Signification de l'acronyme
Description

IP
IP
Internet Protocol
Protocole Internet. Agissant au niveau 3 du modèle OSI, il traite des informations d'adressage et quelques fonctions de contrôle permettant aux paquets d'être routés. IP appartient à la suite de protocoles TCP/IP. IPv4 utilise des adresses de 32 bits, IPv6 utilise des adresses de 128 bits.

IPBX
IPBX
IP Branch eXchange
Autocommutateur d'entreprise en technologie IP.

IPSEC
IPSEC
IP Security protocol
Protocole de sécurisation des échanges sur réseau IP, par établissement de tunnels, authentification mutuelle et chiffrement des données. IPsec fait appel à deux mécanismes de sécurité pour le trafic IP : les mécanismes AH (Authentication Header) et ESP (Encapsulating Security Payload). L'AH est un en-tête conçu pour assurer l'intégrité et l'authentification des datagrammes IP sans chiffrement des données. Son but est d'ajouter aux datagrammes IP classiques un champ supplémentaire permettant, lorsqu'ils arrivent à destination, de vérifier l'authenticité des données incluses dans le datagramme. L'ESP a, quant à lui, pour objectif d'assurer la confidentialité des données. Il peut aussi être utilisé pour garantir leur authenticité. À partir d'un datagramme IP, l'ESP génère un nouveau datagramme dans lequel les données — et éventuellement l'en-tête original — sont chiffrés. AH et ESP utilisent tous les deux un certain nombre de paramètres (algorithmes de chiffrement, clés, mécanismes sélectionnés…) sur lesquels les équipements doivent s'entendre afin d'être sûrs de pouvoir communiquer. Ces paramètres sont gérés grâce à la Security Association (SA), une base de données où sont stockées les informations décrivant l'ensemble des paramètres associés à une communication donnée. Cette base de données contient donc la clé utilisée pour le cryptage des données. IPsec spécifie en outre une méthodologie pour la gestion des clés : il s'agit de l'Internet Key Exchange (IKE). Cette méthodologie décrit une série d'étapes afin de définir les clés utilisées pour l'encryption et pour le décryptage des données. Il s'agit en fait de définir un langage commun afin que les deux parties puissent s'entendre.

IP spoofing
IP spoofing
Technique qui consiste à usurper l'identité d'un autre utilisateur du réseau, en utilisant son adresse IP, ce qui permet de faire croire que la connexion provient d'un compte d'utilisateur autorisé. Lors d'une attaque par saturation, par exemple, l'adresse IP source des requêtes envoyées sera falsifiée pour éviter de localiser la provenance de l'attaque. L'ordinateur d'où provient l'attaque n'est alors pas identifiable.

ISAKMP
Internet Security Association and Key Management Protocol
Standard (RFC 2408) des procédures et formats des paquets pour l'établissement, la négotiation, la modification, l'arrêt ou la destruction d'échange de clés utilisées dans les solutions IPSec. Les formats employés ne sont pas liés à un algorithme de chiffrement ou un mécanisme d'authentification particulier.

ISO 17799
OSI 17799
La norme ISO 17799, issue de la norme anglaise BS7799, constitue un code de bonnes pratiques pour la gestion de la sécurité de l'information. Elle fait l'objet en Grande Bretagne d'un schéma de certification (C:Cure) qui permet aux entreprises anglaises d'être référencées par rapport à cette norme. La norme propose plus d'une centaine de mesures possibles réparties en 10 chapitres : Politique de sécurité, Organisation de la sécurité, Classification des informations, Sécurité du personnel, Sécurité de l'environnement et des biens physiques, Administration, Contrôle d'accès, Développement et maintenance, Plan de continuité, Conformité légale et audit de contrôle.

Isochrone
Synchronous
Caractéristique d'une liaison qui n'admet pas de retard dans la transmission : les extrémités travaillent au même rythme. Un retard perturbe la transmission.

ISP
ISP
Internet Service Provider
(Voir FAI).

JAVA
JAVA
Langage interprété de génération d'applets pour les applications client-serveur (Internet). Inventé par SUN.

Jepi
Jepi
Joint Electronics Payement Initiative
Système permettant l'universalité du paiement, autant pour le vendeur que l'acheteur, quelque soit son mode. Soutenu par Commerce Net et le World Wide Web Consortium.

Jeton
Token
Information particulière circulant en permanence sur un réseau, et signifiant une invitation à émettre. Par extension, mot de passe non rejouable émis par une personne ou un dispositif électronique, et permettant notamment son authentification.

JPEG
JPEG
Joint Photographic Experts Group
Technique de compression d'images fixes, développée pour des applications de stockage ou de télécommunications.

L2TP
L2TP
Layer 2 Tunnelling Protocol
Protocole permettant de créer un tunnel de « niveau 2 », supportant des sessions multiprotocoles PPP, sur architectures IP, Framerelay ou ATM. Il permet de normaliser les fonctionnalités de tunneling et de garantir une interopérabilité entre les équipements.

LAC
LAC
L2TP Access Concentrator
Point de départ des tunnels L2TP (généralement le NAS ou BAS). Concentrateur en entrée de tunnel chargé de transmettre les paquets d'un client PPP pour établir une connexion sur un serveur LNS.

LAN
LAN
Local Area Network
Réseau local interconnectant des équipements informatiques (ordinateurs, serveurs, terminaux…) dans un domaine géographique privé et limité, afin de constituer un système cohérent.

LDAP
LDAP
Lightweight Directory Access Protocol
Protocole de gestion d'annuaires de réseau, adaptation allégée du standard X.500.

LDP
LDP
Label Distribution Protocol
Protocole utilisé par MPLS pour distribuer des étiquettes (labels) servant à la commutation de paquets.

LER
LER
Label Edge Router
Routeur MPLS de périphérie, situé à l'entrée du réseau de l'opérateur, permettant d'étiquetter les flux IP pour être transportés sur un réseau MPLS.

LIFO
LIFO
Last In First Out
Méthode de coordination d'un flux de données dans une file d'attente, par opposition à la méthode FIFO. Les données reçues en dernier sont les premières à ressortir.

LIR
LIR
Local Internet Registries
Entité chargé de recevoir et gérer les demandes d'adresses IP sur Internet. Le fournisseur d'accés internet fait office de LIR généralement.

Log
Log
Fichier texte tenu à jour par un serveur, dans lequel il note les paramètres liés à chaque connexion.

Loss
Loss
Dans le mécanisme de résolution de la concurrence, les cellules sont supprimées à l'endroit même où le blocage survient.

LNS
LNS
L2TP Network Server
Point de terminaison des tunnels L2TP du client et aggrégeant l'ensemble des sessions.
Serveur en fin de tunnel traitant les sessions PPP envoyées par le LAC transportées par L2TP.

Loopback
Loopback
Test permettant d'effectuer un diagnostic de la ligne. Il compare le signal envoyé et le signal retourné après avoir traversé tous les composants de la ligne du réseau.

LSP
LSP
Label Switched Path
Tunnel suivi par un paquet MPLS pour arriver à destination.

LSR
LSR
Label Switch Router
Routeur MPLS en cœur de réseau.

MAC
MAC
Medium Access Control
Partie de la couche liaison de données (niveau 2) qui assure la gestion de l'accès au support physique.

MAC
MAC
Message Authentication Code
(Voir CAM).

MAC Address
MAC Address
(Voir Adresse MAC).

Mailbomb
Mailbomb
Message envoyé en de multiples exemplaires lors d'une opération de mailbombing. Il s'agit d'un courrier électronique vide, revendicatif voire injurieux, souvent accompagné d'un fichier joint volumineux afin d'encombrer plus rapidement la boîte aux lettres de la victime. Ce fichier joint peut être un virus, ce qui est surtout symbolique car face à un bombardement de messages par centaines le destinataire comprend en général instantannément qu'il est la cible d'une attaque.

Mailbombing
Mailbombing
Attaque basique qui consiste à envoyer des centaines, des milliers voire des dizaines de milliers de messages appelés « mailbombs » à un unique destinataire dans un but évidemment malveillant. Ce dernier va du simple encombrement de boîte aux lettres, avec possibilité de perte de données en cas de saturation de la capacité de stockage, jusqu'au crash machine ou déni de service. Comme en cas de spamming, il est éventuellement possible d'identifier l'agresseur et de porter plainte, mais les fournisseurs d'accès peuvent également spontanément détecter de telles attaques par la hausse d'activité suspecte voire la dégradation de performance qu'elles entraînent. Le mailbombing est illégal et sévèrement puni par la loi : le 24 mai 2002, un internaute français a été condamné à quatre mois de prison avec sursis et 20 000 euros de dommages-intérêts pour avoir voulu ainsi se venger d'un rival amoureux.

Malware
Malware
Contraction de « malicious software », le terme malware désigne les programmes spécifiquement conçus pour endommager ou entraver le fonctionnement normal d'un système, tels que les virus, les vers, les chevaux de Troie, ainsi que certains javascripts ou applets java hostiles. Cette famille ne doit pas être confondue avec les spywares (espiogiciels), autre famille de logiciels dont le fonctionnement est également contestable mais dont le but premier n'est pas de nuire à l'intégrité

Terme technique
English
Signification de l'acronyme
Description

d'un système. Les antivirus détectent et éliminent une grande partie des malwares sans toutefois pouvoir jamais atteindre 100 % d'efficacité 100 % du temps : il reste donc indispensable de n'exécuter un programme ou un fichier joint que si sa sûreté est établie avec certitude, le doute profitant toujours aux malwares.

MAN
MAN
Metropolitan Area Network
Réseau métropolitain, d'une portée géographique à l'échelle d'une ville, chargé d'interconnecter des LAN.

Man in the middle
Man in the middle
L'attaque « Man In The Middle » ou « Attaque de l'homme au milieu » porte bien son nom. Il s'agit d'un type d'attaque où une tierce personne s'interpose de manière transparente dans une connexion pour écouter sans se faire remarquer. Le type courant d'attaque « Man In The Middle » pour le réseau repose sur plusieurs attaques d'ARP poison vers des postes ciblés. Le but de cette attaque est de remplacer les tables ARP des victimes afin de mettre le poste attaquant en position d'écoute entre les cibles. (Voir ARP poison).

MARION
MARION
Méthode d'Analyse des Risques Informatiques et Optimisation par Niveaux
Méthodologie d'audit, qui permet d'évaluer le niveau de sécurité d'une entreprise au travers de questionnaires pondérés dans différents thèmes de la sécurité :
- le niveau de sécurité est évalué suivant 27 indicateurs répartis en 6 grands thèmes, chacun d'eux se voyant attribuer une note de 0 à 4, le niveau 3 étant le niveau à atteindre pour assurer une sécurité jugée correcte ;
- les thèmes sont : sécurité organisationnelle, sécurité physique, continuité de service, organisation informatique, sécurité logique et exploitation, sécurité des applications.

Mascarade
Spoofing
Usurpation d'identité
Acte de prétendre être une autre entité dans le but d'accéder aux ressources de celle-ci ; incident au cours duquel un tiers non autorisé prétend être le véritable utilisateur.

Masque de sous-réseau
Netmask
Le masque permet d'intégrer une station dans un réseau et de séparer plusieurs réseaux selon les entités de l'entreprise par exemple.

MAU
MAU
Multistation Access Unit
Point de connexion central sur un réseau Token-Ring.

MBS
MBS
Maximum Burst Size
Représente le nombre de cellules ATM que peut émettre le Matériel Client au débit crête, et qui seront considérées par le réseau du Fournisseur conformes au contrat de trafic de la connexion concernée.

Mécanisme de sécurité
Mecanism
Logique ou algorithme qui implémente par matériel ou logiciel une fonction particulière dédiée à la sécurité ou contribuant à la sécurité.

MEHARI
MEHARI
MEthode HArmonisée d'Analyse du Risque
Méthode d'analyse du risque développée par le CLUSIF. Le but de la méthode d'approche top-down est de mettre à disposition des règles, modes de présentation et schémas de décision. L'objectif de la méthode est de proposer, au niveau d'une activité comme à celui d'une entreprise, un plan de sécurité qui se traduit par un ensemble cohérent de mesures permettant de pallier au mieux les failles constatées et d'atteindre le niveau de sécurité répondant aux exigences des objectifs fixés.
Le modèle de risque MEHARI se base sur 6 facteurs de risque indépendants : 3 sur la potentialité du risque et 3 sur son impact ; 6 types de mesures de sécurité (structurelle, dissuasive, préventive, de protection, palliative, de récupération).
Les phases de MEHARI sont :
- phase 1 : établissement d'un plan stratégique de sécurité (global) ;
- phase 2 : établissement de plans opérationnels de sécurité réalisés par les différentes unités de l'entreprise ;
- phase 3 : consolidation des plans opérationnels (global).

Menace
Threat
Potentialité d'une action ou d'un événement sur une information ou une ressource susceptible de porter un préjudice. La menace peut être intentionnelle ou accidentelle. Une menace intentionnelle est réalisée par un agresseur qui a des motivations, elle nécessite des moyens (financiers et techniques) et du temps. L'autre type de menace, survient à la suite d'une erreur ou d'un accident.

Message
Message
Dans le monde des réseaux, un message est une suite de données binaires formant un tout logique pour les tiers communicants. Lorsqu'un message est trop long pour être transmis d'un seul bloc, il est segmenté et chaque segment est envoyé séparément dans un paquet distinct.

Mesure de sécurité
Administrative security measure
Moyen destiné à améliorer la sécurité, spécifié par une exigence de sécurité et à mettre en œuvre pour la satisfaire. Il peut s'agir de mesures de prévision ou de préparation, de dissuasion, de protection, de détection, de confinement, de « lutte », de récupération, de restauration, de compensation…

Méthode
Security method
Outil permettant d'analyser, de concevoir, d'évaluer ou de contrôler, ensemble ou séparément, la sécurisation des systèmes d'information.

Méthode d'attaque
Attack method
Moyen type (action ou événement) pour un élément menaçant de réaliser une attaque.

Métrique
Metric routing
La métrique définit dans un protocole de routage le nombre de sauts à réaliser pour atteindre l'extrêmité ou le réseau distant. Il peut se baser sur le nombre de routeurs traversés, sur la bande passante ou sur un coût de transmission.

MGCP
MGCP
Media Gateway Control Protocol
Protocole défini pour gérer le passage des signaux vocaux d'un réseau téléphonique traditionnel vers un réseau utilisant le protocole TCP-IP.

MHEG
MHEG
Multimedia and Hypermedia Experts Group
Norme de structuration et de représentation fonctionnelle d'applications multimédia ; conception orientée objet.

MIB
MIB
Management Information Base
Zone mémoire d'un équipement contenant son état ; base de données d'informations sur l'administration de réseaux.

MIE
ADM
Multiplexeur à Insertion-Extraction/Add-drop multiplexer
Équipement permettent l'insertion ou l'extraction reconfigurable d'une partie des flux synchrones.

MIME
MIME
Multipurpose Internet Mail Extension
Standard utilisé par la messagerie pour coder des fichiers binaires et intégrer tout type de données (son, images, programmes). Des extensions MIME ont été développées pour corriger les limitations initiales de la messagerie Internet, et en particulier pour être indépendantes de la machine émettant, transmettant ou recevant le message.

MIR
MIR
Maximum Information Rate
Débit maximum en entrée du réseau du Fournisseur que peut atteindre un CVP.

Mot de passe dynamique
Dynamic password
Mot de passe changé automatiquement à intervalle régulie ou à chaque connexion. Un module d'identification (carte, calculette, …), synchronisé avec le serveur, fournit la partie variable du mot de passe.

Motivation
Grounds
Motif d'un élément menaçant. Elle peut avoir un caractère stratégique, idéologique, terroriste, cupide, ludique ou vengeur et diffère selon qu'il s'agit d'un acte accidentel (curiosité, ennui, …) ou délibéré (espionnage, appât du gain, volonté de nuire, idéologie, jeu, fraude, vol, piratage, défi intellectuel, vengeance, chantage, extorsion de fonds…).

MPEG
MPEG
Moving Pictures Experts Group
Technique normalisée de compression d'images animées.

MPLS
MPLS
MutiProtocol Label Switching
Protocole de l'IETF permettant de créer et de gérer des réseaux privés virtuels totalement sécurisés, en utilisant le réseau privé du Fournisseur. Associé au protocole DiffServ, MPLS permet également de transporter les flux de façon différenciée grâce aux Classes de Services (CoS).

MPLS-VPN
MPLS-VPN
Adaptation de la technologie MPLS pour construire des réseaux privés virtuels au dessus d'un réseau IP partagé.

MPOA
MPOA
Multiprotocol over ATM
Protocole autorisant le transport de protocoles classiques routés sur un réseau ATM.

MSS
MSS
Maximum Segment Size
Indicateur de la taille maximale d'un segment TCP non fragmenté. Le MSS est déterminé en fonction du MTU.

MTBF
MTBF
Mean Time Between Failures
Durée moyenne entre deux pannes.

MTS
Synchronous final multiplexer
Multiplexeur Terminal Synchrone
Équipement terminal synchrone, placé chez le client.

MTTR
MTTR
Mean Time To Repair
Durée moyenne de réparation.

MTU
MTU
Maximal Transmission Unit
Détermine la taille maximale des paquets de niveau 3 en fonction du niveau 2 (Ethernet, FDDI, Token Ring, …).

MUA
MUA
Mail User Agent
Terme technique définissant le client de messagerie (Outlook, Eudora, Sylpheed, Mail).

Multicast
Multicast
Diffusion restreinte. Principe identique au broadcast mais vers un nombre restreint de destinataires, utilisé par exemple par les outils de conférence.Type d'opération qui consiste à envoyer un seul message à plusieurs destinataires, et dont l'application la plus répandue est la vidéoconférence.

Terme technique
English
Signification de l'acronyme
Description

Multilink PPP
Multilink PPP
C'est un protocole autorisant l'utilisation de plusieurs connexions PPP afin de répartir la charge de traffic entre deux équipements connectés en PPP.

Multiplexage
Multiplexing
Technique de mélange permettant de faire passer plusieurs communications sur un même canal de transmission.

NACK ou NAK
NACK ou NAK
Not Acknowledged
Bit indiquant que les données n'ont pas été reçues par l'équipement.

NAPT
NAPT
Network Address Port Translation
Sur un routeur NAT, une seule adresse IP publique est utilisée. Les clients privés utilisent un port TCP associé à l'adresse IP publique qui est définie par le routeur.
C'est le type de NAT le plus répandu.

NAS
NAS
Network Access Server
Concentrateur permettant aux utilisateurs d'accès commutés RTC, RNIS ou GSM de se connecter au réseau Transpac. Équivalent au BAS pour l'Internet commuté. Il peut inclure un mécanisme de sécurité (Firewall ou antivirus) ou disposer d'un OS embarqué pour assurer une fonctionnalité de serveur.

NAT
NAT
Network Address Translation
Protocole de translation d'adresse permettant de traduire une adresse IP (ou une plage d'adresses) provenant de machines se trouvant à l'intérieur d'un réseau privé, en une autre adresse « publique » pour aller sur l'Internet. Terme connu aussi sous le nom de mascarade IP (« IP-masquerading »). Mécanisme utilisé pour attribuer au poste de travail d'un intranet une adresse IP différente lorsqu'il sort sur le réseau internet. Pour les routeurs, c'est une technique simple permettant un accés internet simultané à plusieurs PC avec seulement une adresse IP fixe disponible.
Pour les firewalls, c'est un moyen de garder secret la véritable adresse IP des postes situés dans l'intranet et donc les protéger d'attaques directes.

Négociation
ATS
Alternative Trading System
Séquence d'échange d'information entre deux nœuds avant l'envoi de données.

NetWare
NetWare
Système d'exploitation possédant des fonctionnalités-réseau développé par Novell.

Nom de Domaine
Domain name
Nom délivré et enregistré par les autorités compétentes de l'Internet en France ou à l'étranger. Ce nom officiel identifie internationalement les réseaux et machines auxquels les adresses sont rattachées.

Non-rejeu
Non-replay
Garantie qu'un adversaire ayant intercepté des messages au cours d'une communication ne pourra pas les faire passer pour des messages valides en les injectant soit dans une autre communication, soit plus tard dans la même communication.

Non-Répudiation
Non-repudiation
Impossibilité pour un utilisateur de nier sa participation à un échange d'information ; cette participation porte tant sur l'origine de l'information (imputabilité) que sur son contenu (intégrité)

NTP
NTP
Network Time Protocol
Protocole permettant de synchroniser l'horloge des stations avec une très grande précision.

Objectif de sécurité
Security objective
Expression de l'intention de contrer des menaces ou des risques identifiés (selon le contexte) et/ou de satisfaire à des politiques de sécurité organisationnelles et à des hypothèses ; un objectif peut porter sur le système-cible, sur son environnement de développement ou sur son environnement opérationnel.

OCSP
OCSP
Online Certificate Status Protocol
Protocole permettant à une personne de vérifier la validité d'un certificat, en particulier s'il a été révoqué.

OFDM
OFDM
Orthogonal Frequency Division Multiplexing
Technique de modulation de signaux pour les technologies ADSL ou 802.11a.

Opportunité
Capabilities occur
Mesure de la possibilité de survenance d'une attaque.

OSI
OSI
Open System Interconnection
Modèle d'architecture pour l'interconnexion des systèmes informatiques élaboré par l'ISO. Il distingue sept « couches », depuis l'infrastructure physique de transport jusqu'aux applications (téléphonie, fax, … L'internet ne suit pas exactement ce modèle.

OSPF
OSPF
Open Shortest Path First
Protocole de routage intra-domaine, permettant également l'acheminement multi voies.

OUI
OUI
Organizationally Unique Identifier
Identifiant composé des trois premiers octets d'une adresse MAC. Il définit le fabricant de la carte réseau.

Overhead
Overhead
Données utilisées pour la gestion administrative d'un paquet.

PABX
PABX
Private Automatic Branch eXchange
Autocommutateur privé d'entreprise et relié aux réseaux publics de télécommunication. Ses interfaces-réseau fonctionnent en commutation de circuits.

PAP
PAP
Password Authentification Protocol
Protocole d'échange de données d'identification/authentification par mot de passe afin de sécuriser une session sur un réseau PPP. Standardisé par l'IETF.

Paquet
Data packet
Un paquet est une suite de données binaires ne pouvant pas dépasser une longueur fixée. Il est obtenu en découpant un message en plusieurs segments et en ajoutant à chaque segment un en-tête contenant un certain nombre d'informations utiles à l'acheminement de ce paquet sur le réseau (options, destinataire…). La taille maximale d'un paquet dépend du réseau ; un paquet peut correspondre à un message entier si celui-ci est court, mais en général il ne forme pas un tout logique pour le destinataire.
Les paquets sont acheminés séparément jusqu'au destinataire, qui attend la réception de tous les paquets pour pouvoir reconstituer le message.

Pare-Feu
Firewall
Dispositif installé à une frontière du réseau qui protège un réseau interne vis-à-vis de l'extérieur et interdit le trafic non autorisé de l'intérieur vers l'extérieur. Il assure les fonctions de passerelles applicatives (proxy), d'authentification des appels entrants, d'audit et enregistrement de ces appels (log).

Passerelle de sécurité
Security gateway
Une passerelle de sécurité est un système intermédiaire (par exemple un routeur ou un firewall) qui agit comme interface de communication entre un réseau externe considéré comme non fiable et un réseau interne de confiance. Elle fournit, pour les communications traversant le réseau non fiable, un certain nombre de services de sécurité.
Dans IPsec, une passerelle de sécurité est un équipement sur lequel sont implémentés AH et/ou ESP de façon à fournir des services de sécurité aux hôtes du réseau interne lorsqu'ils communiquent avec des hôtes externes utilisant aussi IPsec (soit directement soit par l'intermédiaire d'une autre passerelle de sécurité).

PAT
PAT
Port Address Translation
Translate un flux de données provenant d'une adresse IP publique vers une adresse IP privée en fonction du port TCP/UDP de destination.

Payload
Payload
Données utiles d'un paquet.

PDH
PDH
Plesiochronous Data Hierarchy
Hiérarchie numérique plésiochrone, dans laquelle chaque conduit possède son propre rythme ; tend à être remplacée par SDH.

PE
PE
Provider Edge
Routeur du backbone Internet.

Peer to Peer
Peer to Peer
Station à station : communication directe entre deux stations.

Perfect Forward Secrecy/PFS
Perfect Forward Secrecy/PFS
Propriété d'un protocole d'échange de clef selon laquelle la découverte, par un attaquant, du ou des secrets à long terme utilisés ne permet pas de retrouver les clefs de sessions.

Piégeage
Trapping
Action délibérée qui consiste à introduire un piège dans un système informatique.

Pigtail
Pigtail
Câble permettant de relier du matériel Wifi (Carte, point d'accés, …) à une antenne.

PIN
PIN
Personal Identification Number
Numéro d'identification personnel. Le code PIN est un code de sécurité à 4 chiffres défini par l'utilisateur qui protège la carte SIM de toute utilisation frauduleuse en cas de perte ou de vol du téléphone. Après 3 essais erronés, votre carte sera bloquée.

Ping
Ping
Packet INternet Groper
Programme de recherche et de vérification de la présence d'une machine (IP). Utilitaire TCP/IP permettant de connaître l'état d'un nœud sur le réseau.

Piratage téléphonique
Phreaking
Action de pirater les réseaux téléphoniques via Internet, avec l'intention de frauder et d'en retirer des avantages personnels ou des gains financiers. Cette fraude consiste principalement à « craquer » les systèmes téléphoniques afin de téléphoner gratuitement. Le terme phreaking vient de phone freak. Dans le jargon des pirates informatiques, la substitution des lettres d'un mot est obligatoire.
Phone devient fone et freak devient phreak, puis phreaking.

Pirate
Cracker
Terme générique employé pour désigner celui qui craque ou attente à l'intégrité d'un système informatique, de la simple duplication de données à l'accès aux ressources d'un centre de calcul (vol, pillage de programmes, de fichiers, …).
Les pirates ont l'habitude d'être classés en 3 groupes :

Terme technique
English
Signification de l'acronyme
Description

1- les white Hat qui œuvrent pour une diffusion de l'information sur les vulnérabilités du web (le full disclosure) et la prévention des risques informatiques ;
2- les black Hat qui œuvrent à la mise au point d'applications permettant d'exploiter les vulnérabilités du web, mais ne soumettent généralement pas leur découverte au « public » (no-disclosure) ;
3- les grey Hat qui se situent à mi-chemin entre white et black hat.

PKCS
PKCS
Public Key Cryptography Standards
Ensemble de standards de chiffrement traitant des questions relatives aux clef publiques, sur une initiative de la société RSA Data Security. Par exemple, PKCS#3 décrit l'échange de clef selon Diffie-Hellman, PKCS#8 définit le format des clefs privées, ou encore PKCS#10 établit la syntaxe d'une demande de certificat.

PKI
PKI
Public Key Infrastructure
(Voir ICP).

PKIX
PKIX
Public Key Infrastructure - X.509
Groupe de travail de l'IETF visant à faciliter la genèse d'ICP fondées sur la norme X.509 pour des applications Internet. Sous cette dénomination, l'IETF tente d'harmoniser les différents composants des infrastructures à clés publiques (PKI) comme les protocoles de gestion des clés et d'échanges de certificats, les formats de certificats, les requêtes dans les listes d'annuaires avec la sécurité comme base commune de développement (notamment, intégration de S/Mime).

Plésiochrone
Plesiochronous
Technique de multiplexage qui uniformise la longueur des trames, en insérant ou supprimant des bits.

Politique de sécurité
Security policy
Ensemble des critères permettant de fournir des services de sécurité.

Politique de sécurité de système d'information
Computer security policy
Ensemble formalisé dans un document applicable, des éléments stratégiques, des directives, procédures, codes de conduite règles organisationnelles et techniques, ayant pour objectif la protection du (des) système(s) d'information de l'organisme.

Policy Server
Policy Server
Terme propre au logiciel CheckPoint Firewall-1. Il sert d'identification, d'authentification aux ACL pour les utilisateurs se connectant via un lien VPN.

Pollupostage
Spamming
(Voir Spamming).

Polluriel
Spam
Équivalent français de email spam. (Voir Spamming).

PoP
PoP
Point Of Presence
Point de Présence du réseau du FAI.

Port
Port
Interface d'ordinateur pouvant être branché à un modem pour communiquer avec un terminal distant ;
adresse du point d'accès au service sur UDP et TCP.

Post-Routing
Post-Routing
Utilisé dans la terminologie firewall pour spécifier les opérations à effectuer après décision de routage. Exemple : connexion à internet de plusieurs clients d'un réseau privé sur internet avec une seule adresse IP publique.

Pourriel
Junk e-mail
Nom générique — contraction de « poubelle » et de « courriel » — désignant les courriers électroniques inopportuns voire intempestifs qui finissent à la poubelle dès réception. D'après l'OQLF, le pourriel comprend les courriels envoyés par spamming (essentiellement les publicités sauvages) et par mailbombing (notamment les messages infectés par certains virus capables de s'envoyer en plusieurs dizaines d'exemplaires aux mêmes internautes en un temps réduit). On peut également y ajouter les hoax, ces « canulars du web » qui devraient constituer la prochaine bête noire des internautes.
Pourriel est utilisé comme synonyme français de spam quelque peu abusivement. (Voir Spamming).

PPP
PPP
Point to Point Protocol
Protocole d'échange de données liaison, utilisé en particulier pour la liaison entre un ordinateur isolé et un provider, afin d'accéder à Internet. Standardisé par l'IETF.

PPPoA
PPPoA
Point to Point Protocol over ATM
Protocole d'échange de données liaison utilisant la technologie ATM.

PPPoE
PPPoE
Point to Point Protocol over Ethernet
Protocole d'échange de données liaison utilisant la technologie Ethernet. Protocole permettant de combler un manque dans le protocole PPP, c'est-à-dire la reconnaissance des adresses MAC (Medium Access Control) permettant ainsi de faire passer du PPP sur Ethernet.

PPTP
PPTP
Point To Point Tunneling Protocol
Protocole de cryptage de connexions point à point défini par Microsoft.

Préjudice
Injury
Conséquence sur l'entreprise de la réalisation d'un risque.

Pre-Routing
Conditional routing
Utilisé dans la terminologie firewall pour spécifier les opérations à effectuer avant décision de routage. Exemple : port forwarding.

Principe
Principle
Les principes de sécurité sont à la fois l'expression de contraintes (lois, règlements, environnement technique) et d'orientations de sécurité pour l'élaboration d'une politique. Les principes doivent permettre l'élaboration de règles.

Prise de risque
Risk acceptation
Acceptation de la charge de la perte d'un risque particulier.

Prise réseau
Handshake
La « Prise » matérialise l'accès du client au réseau de l'Opérateur. Elle comprend un routeur installé et géré par le Fournisseur sur le site du Client, et la liaison d'accès au réseau.

PRN
PRN
Random Number
Code numérique défini dynamiquement (par exemple, changeant à fréquence fixe). Le PRN est habituellement associé à un PIN pour fournir un code d'accès hautement sécurisé.

Profil de protection
Protection profil
Introduit par les Critères Communs, un Profil de Protection (PP) permet de définir un ensemble d'objectifs et d'exigences de sécurité pour une catégorie de Target Of Evaluation (TOE) ou cible d'évaluation donnée. Un PP a donc l'avantage d'exposer les exigences de sécurité nécessaires à la satisfaction des objectifs de sécurité, mais il doit d'abord subir lui-même une évaluation sécurité selon les Critères Communs pour être déclaré « complet, cohérent et techniquement correct ».

Protocole
Protocol
Description d'un ensemble de règles à respecter dans l'utilisation d'équipements réseaux.

Proxy
Proxy
Service qui partitionne la communication entre le client et le serveur en établissant un circuit entre le client et le firewall, et un deuxième entre ce dernier et le serveur (Internet).

Proxy applicatif
Application proxy
Type de firewall laissant passer des données d'applications spécifiques selon des règles de filtrage définis.

PTI
PTI
Payload Type Indicator
Champ de l'en-tête d'une trame qui identifie le type et la classe du trafic.

QoS
QoS
Quality of Service
Techniques permettant de prioriser des flux sur un réseau IP, en fonction des contraintes des applications qu'ils supportent.

RADIUS
RADIUS
Remote Authentication Dial-In User Service
Équipement informatique (matériel et logiciel) fonctionnant à ce standard, et assurant les vérifications d'identification et authentification des utilisateurs du client. Il peut appartenir au client qui l'a installé sur son site ou être souscrit auprès du fournisseur d'accès. RADIUS est un standard Internet qui décrit un serveur d'authentification centralisé et le protocole des échanges mis en œuvre pour l'authentification d'utilisateurs distants. L'intérêt de cette solution réside dans l'unicité de la base des données des utilisateurs (base centralisée).
Le serveur RADIUS partage avec l'utilisateur un mot de passe – éventuellement une clé secrète – et avec le serveur de contrôle d'accès (NAS) un secret. Ainsi l'utilisateur saisit son mot de passe. Il est récupéré par le NAS (utilisation de MD5). Ce dernier génère un aléa (valeur aléatoire de lutte contre le rejeu) et le concatène avec le secret qu'il partage avec RADIUS avant de calculer le condensé de l'ensemble. Il calcule le « XOR » de ce condensé et du mot de passe utilisateur pour obtenir la valeur « Request Authenticator (RA) » qu'il envoie à RADIUS qui effectue le contrôle d'authentification.
Si le serveur RADIUS et l'utilisateur partagent une clé secrète (à la place du mot de passe), RADIUS met en œuvre un mécanisme d'authentification par question/réponse. Dans ce cas, lorsque le NAS envoie le message « RA », RADIUS répond en envoyant un aléa à l'utilisateur via le NAS. L'utilisateur effectue un calcul sur l'aléa avec sa clé secrète et envoie sa réponse à RADIUS via le NAS pour authentification.
Une authentification peut aussi être effectuée en employant le protocole CHAP entre l'utilisateur et le NAS, c'est alors le NAS, à la place de RADIUS, qui fournit l'aléa à l'utilisateur.

RAI (FT)
Réseau d'Alerte et d'Intervention
Terminologie FT. Réseau téléphonique complètement indépendant du réseau public et utilisant ses propres commutateurs. Dimensionné pour accepter le trafic de gestion des crises majeures. Supporte un service d'audioconférences grâce à des ponts dédiés.

RARP
RARP
Reverse Address Resolution Protocol
Protocole de recherche d'adresse IP (couche réseau), utilisé par les machines sans disque pour leur propre compte.

Redondance
Redundancy
Concept de duplication d'équipements-réseau assurant la continuité de service en cas de défaillance de l'un d'eux.

Réduction du risque
Minimize risk
Processus visant à minimiser les conséquences négatives et les opportunités d'une menace.

Registrar
Registrar
Entité chargée de la gestion des noms de domaines utilisés sur internet. Pour être un registrar, il faut être membre d'un registre.

Terme technique
English
Signification de l'acronyme
Description

Registre
Register
Entité chargée de la gestion des TLD (Top Level Domain) sur internet. Exemple de TLD : .fr ; .uk ; .es ; .fi

Règle de sécurité
Security Rule
Les règles expriment dans un environnement et un contexte donné, les principes de sécurité, sous une forme permettant la mise en place de moyens et de comportements adaptés. La définition des règles doit prévoir le contrôle de leur mise en œuvre.

Rejeu
Replay
Attaque contre un système cryptographique, consistant à stocker et réutiliser ultérieurement un message en plus d'un autre ou à la place d'un autre. Action consistant à envoyer un message intercepté précédemment, en espérant qu'il sera accepté comme valide par le destinataire.

Répudiation
Répudiation
Fait de nier avoir participé à des échanges, totalement ou en partie.

Ressources disponibles
Available ressources
Moyens attendus d'un élément menaçant. Ce niveau constitue son potentiel d'attaque et peut être caractérisé par des ressources faibles, modérées ou élevées.

Reverse-proxy
Reverseproxy
Il sert de relais à un client qui souhaite se connecter à un serveur distant afin de protéger son propre serveur contre les attaques externes. De l'extérieur on voit l'adresse IP du relais inverse mais pas celui du serveur. Il sert d'accélérateur (server accelerator) et peut faire de l'équilibrage de charge (load balancing).

Révocation
Revoked key
Annonce qu'une clé privée a perdu son intégrité. Le certificat de la clé publique correspondante ne doit plus être utilisé.

Rijndael
Rijndael
Contraction du nom de ses auteurs (Rijmen et Daemen)
Cet algorithme travaille sur des blocs entiers de 128 bits en utilisant des clés de 128, 192 ou 256 bits. On le désigne souvent comme le successeur du DES et Triple DES.

RIP
RIP
Routing Information Protocol
Protocole de routage de type vecteur de distance.

Risque
Risk
Combinaison de la probabilité et de l'impact découlant de l'exploitation d'une vulnérabilité par une menace sur une information ou une ressource.

Risque résiduel
Residual risk
Risque subsistant après le traitement du risque.

Routage
Routing
Mécanisme utilisé pour diriger les cellules dans le réseau. Il existe deux types de routage : externe, pour la transmission des cellules entre différents points du réseau, et interne, pour diriger les cellules à l'intérieur même d'un commutateur multivoies.

Route
IP routing
Chemin emprunté dans l'acheminement d'un datagramme IP entre deux sites du Client.

Routeur
IP router
Équipement de niveau 3 OSI chargé de trouver le meilleur chemin à prendre pour atteindre une autre machine, par exemple dans un réseau IP. Chaque paquet de données reçu par le routeur est ainsi transmis au nœud suivant approprié pour suivre son chemin vers la machine visée.

Routeur filtrant
Screening router
Routeur pourvu de fonctions de filtrage de niveau 4 sur les ports TCP/UDP de destination.

RFC
RFC
Request For Comment
Littéralement, « Appel à commentaires ». C'est en fait un document décrivant un des aspects d'Internet de façon relativement formelle (généralement, spécification d'un protocole). Ces documents sont destinés à être diffusés à grande échelle dans la communauté Internet et servent souvent de référence. On peut les trouver sur la plupart des sites FTP.

RPV
VPN
Réseau Privé Virtuel
Réseau privé d'entreprise multi-sites utilisant les réseaux d'opérateur pour leur interconnexion. Dans le cadre de la sécurité des échanges, réseau composé par un ensemble d'hôtes et d'équipements qui utilisent des protocoles spécifiques pour sécuriser leurs communications.

RSA
RSA
Rivest, Chamir, Adleman
Système de chiffrement asymétrique à clé publique dont le nom est constitué par les initiales de ses inventeurs.

RTD
RTD
Round Trip Delay
(Voir Délai de Transit).

SAML
SAML
Security Assertion Markup Language
Basé sur XML, intégrant les notions de profil et droits d'accès, ce langage devrait s'imposer à l'avenir pour propager les niveaux de protection entre applications réseau.

SAR
SAR
Segmentation And Reassembly
Technique de « cellularisation » des messages utilisée par exemple sur réseau ATM : les trames de longueurs variables en provenance d'un émetteur non ATM sont hachées en paquets de dimension fixe auxquels sont rajoutés les entêtes ATM ; au niveau du récepteur, les cellules appartenant à une même trame sont reconstituées grâce aux informations contenues dans l'en-tête.

SATAN
SATAN
System Administrative Tool for Analysing Networks
Outil librement distribué, développé par Dan Farmer et Wieste Venema, dont l'objectif est d'aider les administrateurs réseau à corriger les faiblesses bien connus de leur environnement. Les experts en sécurité ont souvent décrié ce logiciel car des pirates s'en sont également servi à leur profit (mais n'y a-t-il pas plutôt un conflit d'intérêt à la base ?).

Scan
Scan
Action réalisée par un programme pour parcourir la configuration d'un système dans le but de détecter des vulnérabilités.

Scellement
Integrity locking
Mécanisme de sécurité permettant d'assurer l'intégrité et l'authentification de l'origine des données.

SD
EO (eyes only)
Secret Défense
La mention « secret défense » est réservée aux informations dont la divulgation est de nature à nuire à la Défense nationale et à la sûreté de l'État.

SDA
Sélection Directe à l'Arrivée
Service d'accès direct à un poste téléphonique derrière un autocommutateur d'entreprise sans passer par le standard.

SDH
SDH
Synchronous Digital Hierarchy
Nouvelle hiérarchie numérique synchrone européenne pour le multiplexage de réseaux fibre optique ; permet des débits beaucoup plus grands que la PDH. Normalisée par l'UIT-T. Son débit de base est de 155Mb/s.
Elle est compatible avec la hiérarchie SONET utilisée aux USA et au Japon.

SDSL
SDSL
Symmetric Digital Subscriber Line
Technologie de transmission numérique sur paire de cuivre arrivant chez l'abonné semblable à l'ADSL, mais à débits montant et descendant égaux.

SecurID
SecurID
Il s'agit d'un produit commercial de Security Dynamics, largement diffusé dans le monde, se présentant sous la forme d'une « calculette » au format carte de crédit, permettant de sécuriser un login. Son principe est de combiner l'heure à un mot de passe pour générer un mot de passe dynamique valide pendant seulement 60 secondes. Ce dernier est ensuite vérifié et traîté par un serveur d'accès dédié.

Sécurité
Security
État de protection, face aux risques identifiés, qui résulte de l'ensemble des mesures générales et particulières prises pour satisfaire aux exigences de sécurité concernant l'information et les ressources associées. Ces mesures peuvent se décliner en fonction du contexte (sécurité du système d'information, sécurité des biens physiques, sécurité des personnes…). Mesures de prévention et de réaction mises en œuvre pour faire face à une situation d'exposition résultant de risques accidentels, qu'il soient le fait de l'homme, de la machine ou de la nature.

Servlet
Servlet
Appliquette destinée à être exécutée sur le serveur et non pas chez le client.

Session
Session
Intervalle de temps entre le début d'un échange ou d'une communication et sa fin.

SET
SET
Protocole élaboré conjointement par Mastercard et Visa dans le but d'assurer un haut degré de sécurisation aux transactions financières en ligne nécessitant l'utilisation d'une carte de crédit.

SHDSL
SHDSL
Symmetric High bitrate Digital Subscriber Line
Accès DSL symétrique à haut débit.

Signature d'attaque
Attack signature
Signature servant à identifier en temps réel une tentative d'attaque sur un réseau, qui, une fois reconnue par le système de détection d'intrusion, fonctionne comme un coupe-feu et permet de bloquer les accès non autorisés au serveur.
On peut classer les outils de détection d'intrusion selon deux modes de fonctionnement : l'un se basant sur les signatures d'attaques et l'autre sur les anomalies du système (analyse heuristique). Un système de détection d'intrusion ne peut détecter que les attaques dont il possède la signature. De ce fait, il est nécessaire de faire des mises à jour quotidiennes. Ainsi, le système de détection est aussi bon que l'est la base de signatures. Si les signatures d'attaques sont erronées ou incorrectement conçues, l'ensemble du système est inefficace. Il est possible, à l'aide d'un assistant de définition de signature d'attaque personnalisée, de construire ses propres signatures d'attaques pour protéger les applications ou les environnements internes et ainsi en réduire la vulnérabilité.

Signature numérique
Digital signature
Transformation électronique permettant d'assurer l'authentification du signataire et éventuellement celle d'un document signé par lui. Données ajoutées

Terme technique
English
Signification de l'acronyme
Description

à une unité de données, ou transformation cryptographique d'une unité de données, permettant à un destinataire de prouver la source et l'intégrité de l'unité de données et protégeant contre la contrefaçon (par le destinataire, par exemple). [ISO 7498-2]. Une signature numérique fournit donc les services d'authentification de l'origine des données, d'intégrité des données et de nonrépudiation. Ce dernier point la différencie des codes d'authentification de message, et a pour conséquence que la plupart des algorithmes de signature utilisent la cryptographie à clé publique.
La signature peut prendre deux formes :
1- « transformation chiffrée » : un algorithme cryptographique modifie directement le message (par exemple chiffrement du message avec une clé privée).
2- « données annexées » : des données supplémentaires sont adjointes au message (par exemple une empreinte, chiffrée avec une clef privée).

SLA
SLA
Service Level Agreement
Engagements de la part du fournisseur sur la qualité du service fourni. Ils déterminent le niveau d'indemnisation du client en cas de non atteinte d'un niveau minimum de disponibilité de service.

Slamming
Slamming
Type de pratique frauduleuse en téléphonie qui consiste à changer le fournisseur d'appels interurbains d'un client sans son consentement.

SLIP
SLIP
Serial Line Internet Protocol
Protocole utilisé pour les connexions séries point à point.

SMDS
SMDS
Switched Multimegabit Data Service
Technologie haut-débit à commutation sur des réseaux WAN.

SMHD
SMHD
Service Multisite Haut Débit
Service d'infrastructure offert par FT aux clients multi-sites, par déploiement d'une boucle optique à très haut débit (jusqu'à 2,5 Gb/s) installée sur un périmètre restreint (ville…).

S/MIME
S/MIME
Secure MIME
Extension sécurisée de MIME (provenant de la société RSA Data Security) intégrant des services d'authentification par signature digitale (MD5, SHA-1) et confidentialité par chiffrement (RSA, RC2, DES). S/MIME traite également des aspects certificat ANSI X.509 et du tranfert par internet.

SMTP
SMTP
Simple Mail Transfert Protocol
Protocole application de courrier électronique.

SNA
SNA
Systems Network Architecture
Architecture de réseau d'finie par IBM.

SNAT
SNAT
Source NAT
Technologie de NAT modifiant l'adresse IP source d'un paquet. Toujours utilisé en Post-Routing.

Sniffer
Sniffer
Analyseur de trames - Logiciel permettant de consulter le contenu des trames circulant sur le réseau.

SNMP
SNMP
Simple Network Managment Protocol
Protocole d'administration à distance permettant de superviser les équipements réseau par accès à la MIB de chacun d'eux.

SOA
SOA
Services Oriented Architecture
Architecture orientée services, à la base des services web.

SOAP
SOAP
Simple Object Access Protocol
Protocole de communication assurant l'interopérabilité des applications à travers le web.

Social engineering
Social engineering
Pratique consistant à abuser de la confiance d'un ou de plusieurs personnes, dans le but de récupérer des informations confidentielles : le social engineering ou comment se servir de la faille humaine pour obtenir des codes confidentiels, des informations sensibles, des numéros de modems de télémaintenance, etc.

Socket
Socket
Mécanisme de communication (structure logicielle définissant une connexion entre deux hôtes sur le réseau) utilisé en programmation d'application réseaux, qui fait apparaître le réseau comme un fichier que l'on peut écrire ou lire. Les protocoles sous-jacents sont masqués au programmeur. Toute une bibliothèque de fonctions de programmation est associée à ce mécanisme.

Somme de contrôle
Checksum
Condensé d'un ensemble de données, calculé par l'expéditeur avant l'envoi des données et recalculé par le destinataire à la réception pour vérifier l'intégrité des données transmises.

SONET
SONET
Synchronous Optical NETwork
Normalisation SDH américaine.

Spam
Spam
Message intempestif envoyé à une personne ou à un groupe de personnes lors d'une opération de spamming. Il faut prendre l'habitude de supprimer ce genre de messages sans les lire et sans cliquer sur aucun lien (y compris le lien de désabonnement), afin de ne pas encourager cette pratique et ne pas en recevoir soi-même davantage. Spam est également

couramment employé pour désigner le seul polluriel (email spam).

Spamming
Spamming
Le spamming consiste en des pratiques de multipostage abusif : Excessive Multi-Posting (EMP), Excessive Cross Posting (ECP) ; mais peut aussi correspondre à une indexation abusive dans les moteurs de recherche. On parle alors de spamdexing ou encore d'engine spamming. L'envoi en nombre de messages électroniques est qualifié de spamming en référence au caractère non sollicité du message. Celui-ci comporte le plus souvent un objet publicitaire qui transforme l'envoi en un message promotionnel non sollicité par son destinataire. Le second critère de définition du spamming en matière de courrier électronique réside dans le transfert de charges qu'il occasionne au détriment du destinataire (cost-shifting). Cette situation est analogue à celle rencontrée avec l'envoi de fax à des fins commerciales. Cette pratique a été depuis lors interdite dans de nombreux pays ou bien soumise au consentement préalable (opt-in) des personnes visées comme l'a notamment imposée la directive européenne 97/66 du 15 décembre 1997 (article12 alinéa 1er et 2).

Spanning Tree
Spanning Tree
Algorithme et protocole permettant aux ponts de détecter des boucles dans le réseau et d'inhiber ces boucles.

SPF
SPF
Shortest Path First
Algorithme du plus court chemin. Appelé aussi algorithme de Dijsktra.

SPI
SPI
Security Parameter Index
Bloc de 32 bits qui, associé à une adresse de destination et au nom d'un protocole de sécurité (par exemple AH ou ESP), identifie de façon unique une association de sécurité (SA). Le SPI est transporté dans chaque paquet de façon à permettre au destinataire de sélectionner la SA qui servira à traiter le paquet. Le SPI est choisi par le destinataire à la création de la SA.

Spyware
Spyware
Logiciel exécuté sur un ordinateur à l'insu de son propriétaire, et conçu dans le but de collecter des données personnelles (adresse IP, URL consultées, mots de passe, numéros de cartes de crédit, …) et de les renvoyer à son concepteur via internet, sans autorisation préalable dudit utilisateur. Un spyware (ou espiogiciel, mouchard) est un logiciel espion contenant un programme qui, par Internet, peut recueillir et transmettre les données personnelles d'un internaute à une régie publicitaire, notamment sur ses intérêts, ses habitudes de téléchargement et de navigation. Tout cela dans un but exclusivement commercial. Ces mouchards présents dans de nombreux logiciels gratuits (freewares) ou en version de démonstration (sharewares) s'installent lors du téléchargement et ne sont pas détectables par l'utilisateur.

SSH
SSH
Secure Shell
Protocole permettant de se connecter sur une autre machine pour y exécuter des commandes et pour déplacer des fichiers d'une machine à l'autre. SSH offre une authentification forte et des communications sécurisées sur des canaux non sûrs.

SSI
ISS
Sécurité des Systèmes d'Information
Protection des systèmes d'information, et en particulier des éléments essentiels, contre toute atteinte des critères de sécurité non autorisée, qu'elle soit accidentelle ou délibérée.

SSL
SSL
Secure Socket Layer
Protocole de sécurisation des échanges sur internet, développé par Netscape. Il est intégré dans tous les navigateurs récents. Il assure authentification, intégrité et confidentialité Il repose sur un algorithme RSA. Il vise à sécuriser les échanges entre un serveur et un client sur Internet en offrant des mécanismes de chiffrement, de négociation de clés de chiffrement, d'intégrité de message (MAC), d'authentification du serveur et, en option, du client. La non-répudiation n'est pas offerte. Le protocole est indépendant du niveau applicatif, il peut donc être utilisé de façon transparente avec HTTP (HyperText Transfer Protocol), FTP (File Transfer Protocol) et Telnet notamment. Il repose sur un protocole de transport fiable (par exemple TCP). Le protocole SSL propose 54 choix possibles de mécanismes de sécurité avec le support des algorithmes RSA, DSS, Diffie-Hellman , Skipjack, SHA, MD5, DES, triple DES, IDEA, RC2 et RC4.A noter que 3 « types » de clés Diffie-Hellman sont distinguées dans SSL : les clés DH sont signées par l'autorité de certification, les clés DHE (Diffie-Hellman Ephemeral) sont signées par une entité disposant d'un certificat signé par l'autorité de certification, les clés DH anonymous sont des clés DH échangées sans authentification préalable des partenaires.

SSO
SSO
Single Sign On
Fonction permettant de disposer d'une identification unique, quelque soit le service applicatif.

Stéganographie
Steganography
La stéganographie est l'art de cacher des données dans d'autres données : cacher un texte dans une image, une image dans un fichier musical, une image dans une autre image, …

Sûreté
Reliability
Mesures de prévention et de réaction mises en œuvre pour faire face à une situation d'exposition résultant de menaces ou d'actions malveillantes.

Sûreté des biens physiques
Physical asset reliability
Ensemble des mesures de protection contre les évènements malveillants. Ces mesures portent notamment sur les contrôles d'accès physiques aux sites (protection périphérique), aux bâtiments (protection périmétrique), aux locaux et aux matériels (protection intérieure), en mode nominal et en mode dégradé ou en crise.

Terme technique
English
Signification de l'acronyme
Description

SYN
Synchronus
Bit de synchronisation dans les communications TCP/IP.

Synchrone
Synchronus
Mode de transmission dans lequel l'émetteur et le récepteur fonctionnent au même rythme, calés sur une même horloge.

Syslog
Syslog
Fichier servant à enregistrer les évènements d'un système. (Voir Log).

Système d'Information (SI)
IS
Ensemble d'entités organisé pour accomplir des fonctions de traitement d'information. Tout moyen dont le fonctionnement fait appel à l'électricité et qui est destiné à élaborer, traiter, stocker, acheminer, présenter ou détruire l'information (c.f.[901/DISSI/DCSSI]

SWIFT
SWIFT
Society for Worldwide
Interbank Financial Telecommunication
Réseau bancaire mondial ouvert en 1977 dans plus de 190 pays par les banques, permettant les échanges électroniques entre plus de 7 000 institutions financières.

TACACS
TACACS
Terminal Access Concentrator Access Control Server
Protocole d'authentification par question/réponse, uniquement point à point. Protocole d'échange entre un serveur d'accès distant et un serveur d'authentification pour vérifier si l'utilisateur a le droit ou non de se connecter au réseau protégé.

TCP - IP
TCP - IP
Transmission Control Protocol over Internet Protocol
Norme de communication entre systèmes hétérogènes, et définissant un ensemble de protocoles d'échange d'information. Elle repose sur la transmission par paquet et contrôle la transmission entre machines connectées. TCP est le protocole qui achemine les messages sans découpage ni regroupement, avec garantie de bon port. IP est le protocole qui assure le routage, ainsi que la fragmentation et le réassemblage des paquets.

TDMA
TDMA
Time Division Multiple Access
Accès multiple à répartition dans le temps (AMRT) ; multiplexage temporel partageant une même ressource entre plusieurs utilisateurs ; technique adoptée par la norme GSM.

TDP
TDP
Tag Distribution Protocol
Protocole propriétaire CISCO utilisé par MPLS pour distribuer des étiquettes (labels) servant à commuter les paquets.

TELNET
TELNET
TELecoms NETwork
Protocole application de connexion à distance (remote login). Protocole faisant parti de TCP/IP permettant de se connecter sur un hôte distant. Ce protocle n'est pas sécurisé sans l'utilisation de Kerberos.

Tempest
Tempest
Le terme « TEMPEST » regroupe l'ensemble des mesures prises ou à prendre pour éviter que la connaissance par écoute ou interception de certains des signaux parasites émis par un matériel électronique quelconque ne permette de remonter aux informations qui sont à l'origine de leur création ; les rayonnements dits « compromettants » dont il est question se propagent :
- par rayonnement dans l'atmosphère, avec une portée de l'ordre de quelques dizaines de mètres.
- par induction puis conduction dans des matériaux métalliques situés à proximité des équipements en cause, les distances pouvant alors être de plusieurs centaines de mètres.

Tiers de certification
Certification authority
Organisme chargé de gérer et de délivrer les clés publiques avec la garantie qu'elles appartiennent bien à leurs possesseurs reconnus.

Tiers de confiance
Trusted third party
Organisme chargé de maintenir et de gérer, dans le respect des droits des utilisateurs, les clés de chiffrement ou d'authentification. Les tiers de confiance peuvent être des tiers de certification ou des tiers de séquestre.

Tiers de séquestre
Trusted authentication authority
Organisme chargé de garder les clés secrètes de chiffrement, et de les remettre si nécessaire aux autorités de justice.

TKIP
TKIP
Temporal Key Integrity Protocol
Protocole destiné à fournir des clefs de chiffrements temporaires dans le cadre d'un échange réseau de données (par exemple WPA). Algorithme de cryptage utilisé par le WPA générant de nouvelles clés dynamiques par tranche de 10Ko de données transmises.

TNT
Digital directto-home television
Télévision Numérique Terrestre
Projet français de déploiement d'un système terrestre de diffusion de la télévision par techniques numériques.

ToIP
ToIP
Telephony Over IP
Concept regroupant l'ensemble mixable des technologies permettant de fournir un service de téléphonie sur la couche IP : PABX IP, PABX standard associé à un routeur IP, Centrex IP, et interconnectable au travers d'un réseau de transport IP.

Token
Token
(Voir Jeton).

Token Ring
Token Ring
Technique et méthode d'accès d'une catégorie de réseau en anneau ; le jeton est renvoyé après retour de la trame émise. Normalisée 802.5.

Topologie
Topology
Configuration physique des nœuds réseaux au sein d'une entreprise.

Traçabilité
Security audit trail
Suivi régulier de la qualité offerte par audits et rapports d'activité réguliers.

Traceroute
Traceroute
Utilitaire TCP/IP permettant d'indiquer les routeurs traversés pour atteindre une station.

Traitement du risque
Risk processing
Processus de sélection et de mise en œuvre des mesures visant à modifier le risque, ce qui signifie une réduction du risque, un transfert du risque ou une prise de risque.

Transfert du risque
Risk transfer
Partage avec une autre partie de la charge de la perte d'un risque particulier.

TSD
Très secret Défense
La mention TSD est réservée aux informations dont la divulgation est de nature à nuire gravement à la Défense nationale et à la sûreté de l'État, et qui concernent les priorités gouvernementales en matière de Défense.

TTL
TTL
Time To Live
Compteur utilisé par IP pour définir le nombre de sauts maximum qu'un paquet peut réaliser durant son acheminement. Il est décrémenté de 1 à chaque traversée de routeur. Quand le TTL est à 0 le paquet est détruit.

Tunneling
Tunneling
Technique consistant à créer un « tunnel » entre deux points du réseau en appliquant une transformation aux paquets à une extrémité (généralement, une encapsulation dans un protocole approprié) et en les reconstituant à l'autre extrémité.

UDDI
UDDI
Universal Description, Discovery, Integration
Protocole visant à contituer un annuaire mondial en ligne référençant l'ensemble des services web disponibles.

UDP
UDP
User Datagram Protocol
Protocole non structuré, rapide, utilisé pour transmettre des paquets d'information sur un réseau. Il est l'un des 2 mécanismes de transport du protocole TCP/IP. Protocole de niveau 4 fonctionnant en mode « non connecté » (Pas de négociation avant envoi) sur la pile TCP/IP.

UMTS
UMTS
Universal Mobile Telecommunication System
Concept de réseau mobile de troisième génération dans les travaux de l'ETSI.

Unicast
Unicast
Terme désignant l'envoie de données vers un seul nœud.

URL
URL
Uniform Resource Locator
Système d'identification des documents Internet et Intranet.

USB
USB
Universal Serial Bus
Interface universelle de connexion de périphériques externes, à bus série et connecteur normalisé.

Utilisateur
User
Personne ou chose qui utilise les services d'une organisation.

Utilitaire de désinfection
Eradication software
Petit programme permettant de rechercher et d'éliminer un nombre limité de virus. Il s'agit exclusivement d'un scanner à la demande utilisant une analyse par signatures et dont les définitions de virus ont été limitées à un seul voire quelques virus. Mis à disposition par les éditeurs d'antivirus, principalement lors des épidémies importantes, il permet aux utilisateurs ne possédant pas d'antivirus ou dont l'antivirus aurait été rendu inutilisable de tout de même désinfecter leur ordinateur. Ne disposant pas de moniteur pour surveiller le système en temps réel, l'utilitaire de désinfection est incapable d'empêcher une recontamination si l'utilisateur exécute à nouveau un fichier contaminé ou s'il ne comble pas la faille logicielle possiblement utilisée par le virus pour s'exécuter automatiquement.

VBR
VBR
Variable Bit Rate
Niveau de débit variable. Classe de service ATM utilisée pour faire de l'IP ou du FR sur ATM.

VCI (et VPI)
VCI (et VPI)
Virtual Channel Identifier (et Virtual Path Identifier)
Identité du canal virtuel et de la voie virtuelle.

Vecteur d'initialisation
Initialization Vector
Bloc de valeur quelconque servant à initialiser un chiffrement avec chaînage de blocs, et donc à faire en sorte que deux messages identiques donnent des cryptogrammes distincts.

Terme technique
English
Signification de l'acronyme
Description

Ver
Worm
Forme de virus ayant la propriété de se dupliquer au sein d'une machine, voire de se copier d'une machine à l'autre à travers le réseau.

Virus
Virus
Un virus est un programme qui se répand à travers les ordinateurs et le réseau. Les virus sont conçus pour s'auto-répliquer (c'est-à-dire se copier tout seuls). Ils s'auto-répliquent généralement sans que l'utilisateur n'en ait connaissance. Les virus contiennent souvent des « charges », actions que le virus réalise séparément de sa réplication. Les charges peuvent aller de l'ennui (par exemple, le virus WM97/Class D, qui affiche de façon répétée des messages tels que « I think that 'nom de l'utilisateur' is a big stupid jerk ») au désastre (par exemple, le virus CIH, essayant de réécrire le Flash BIOS, qui peut provoquer des dommages irréparables sur certaines machines). On dénombre 3 grandes catégories de virus, en fonction de la cible visée dans l'ordinateur :

1- les virus d'applications, notamment les virus de démarrage (Parity Boot) et les virus dits parasites, qui infectent les fichiers exécutables, c'est-à-dire les programmes (.exe, .com ou .sys). Pour simplifier, disons que le virus remplace l'amorce du fichier, de manière à être exécuté en premier, puis il rend la main au programme sollicité, camouflant ainsi son exécution aux yeux de l'utilisateur.
2- les virus macro qui infectent uniquement les documents (Word, Excel…). Ces virus se propagent rapidement et peuvent causer de grands dégâts (formatage du disque dur par exemple).
3- les virus de mail, également appelés vers. Ces virus se servent des programmes de messagerie (notamment Microsoft Outlook) pour se répandre à grande vitesse. Leur premier effet est de saturer les serveurs de messagerie, mais ils peuvent également avoir des actions destructrives pour les ordinateurs contaminés. Particulièrement redoutables.

VLAN
VLAN
Virtual LAN
Réseau local virtuel ; concept désignant la réunion de groupes d'utilisateurs physiquement séparés géographiquement, en un seul réseau apparent.

VoIP
VoIP
Voice Over IP
Technologie permettant de fournir un service de téléphonie en mode IP.

VP
VP
Virtual Path
Conduit virtuel ATM, composé d'un ou plusieurs VC.

VPN
VPN
Virtual Private Network
(Voir RPV).

VRF
VRF
VPN Routing and Forwarding
Tables construites et maintenues au niveau des routeurs PE de rattachement. Elles sont consultées par les paquets émis par un site faisant parti du VPN client.
Les VRF contiennent les routes reçues des routeurs CE clients directements connectés ainsi que des autres routeurs PE. La distribution des routes est contrôlée via des protocoles de routages dynamiques qui s'appuient sur des attributs permettant d'identifier l'ensemble des tables VRF d'un routeurs PE, ainsi que les sites autorisés à lui fournir d'autres routes.

VRRP
VRRP
Virtual Router Redundancy Protocol
Protocole d'élection permettant de faire fonctionner plusieurs routeurs avec la même adresse IP, l'un d'eux étant le chef. Si celui-ci tombe en panne, les autres prennent le relais.

Vulnérabilité
Vulnerability
Faiblesse d'une ressource d'information qui peut être exploitée par une ou plusieurs menaces. Elle peut être introduite pendant la conception ou l'exploitation de cette ressource d'information.
Un système d'informations étant composé de manière indissociable de matériels et de personnels effectuant des traitements données, la vulnérabilité s'adresse :
- aux personnels qui sont amenés à commettre des erreurs mais sont aussi susceptibles de commettre des actes de malveillance (divulgation, nuisances) ;
- à l'organisation qui connaît des dysfonctionnements (de procédure, de savoirfaire), du laxisme ;
- aux matériels soumis à des défaillances, à des perturbations du milieu ambiant ;
- aux logiques imparfaites de traitement, de cohérence ;
- aux systèmes de communication (écoute, brouillage, saturation, intrusion).

WAN
WAN
Wide Area Network
Réseau à grande distance, en général interurbain, par opposition au LAN (réseau local).
Permet entre autres d'interconnecter les réseaux locaux.

Wardriving
Wardriving
Le Wardriving est une forme de piratage qui consiste à rechercher les réseaux sans fils détectables sur la voie publique. Pour cela, un wardriver est équipé d'un terminal mobile, avec une antenne et éventuellement un mobile GPS. Il n'a alors plus qu'à se balader tranquillement pour capter les réseaux sans fils existants dans les parages et les cartographier.
Deux sortes d'attaques :
- détourner une connexion réseau à son avantage, et éventuellement pouvoir surfer sur Internet gratuitement ;
- écouter ce qui se passe sur le réseau pour voler des informations notamment.

Les wardrivers utilisent les vulnérabilités du chiffrement WEP ainsi que la verbosité naturelle des protocoles mis en œuvre dans 802.11b (Wifi aka Wireless Fidelity).

Warshalking
Warshalking
Le terme Warshalking désigne le fait de « tagger » les lieux où les réseaux WiFi ont été découverts par wardriving.

WDM
WDM
Wavelength Division Multiplexing
Technique de multiplexage de plusieurs canaux sur une même fibre optique par assignation d'une longueur d'onde propre à chaque canal.

WEP
WEP
Wired Equivalent Privacy
Protocole développé pour le chiffrement des trames 802.11, s'appuyant sur un chiffrement symétrique RC4 dont la longeur des clefs (définies statiquement) varient généralement de 64 à 128 bits (2048 bits maximum). Censé fournir aux réseaux sans fils une intimité/protection comparable aux réseaux cablés, le WEP a déjà montré de nombreuses faiblesses et de nouvelles solutions devraient le remplacer à plus ou moins court terme (se reporter à « WPA »).

Wi-Fi
Wi-Fi
Wireless Fidelity
Technologie hertzienne normalisée (norme 802.11) permettant d'assurer une connectivité sans fil, avec un débit max. de 11 Mb/s en version 802.11b et de 54 Mb/s en 802.11g. Sa portée est de 30 m environ en environnement bureau et jusqu'à 400 m en environnement ouvert.
Cette technologie permet de se connecter à internet et intranet sur les mêmes principes qu'un réseau classique.

WLAN
WLAN
Wireless LAN
Réseaux locaux sans fils, normalisés sous la référence IEEE 802.11.

WPA
WPA
Wi-Fi Protected Access
Standard développé par la Wi-Fi Alliance et visant à améliorer la sécurité des réseaux sans fil par introduction de mécanismes d'authentification, de confidentialité, d'intégrité et de gestion de clés robustes. Alternative au WEP, proposée par la Wi-Fi Alliance (3Com, Lucent, HP, Nokia, Sony, etc.). Basé sur TKIP, on protège les transferts sur le réseau sans fil en chiffrant chaque paquet de 10 Ko avec une nouvelle clef (mais l'algorithme de chiffrement demeure le même que pour le WEP).

WSDL
WSDL
Web Services Description Language
Protocole décrivant l'interface les services Web.

WWW
WWW
World Wide Web
Littéralement « toile d'araignée mondiale », est le réseau à interface graphique d'Internet. Composé de centaines de milliers de serveurs à travers le monde, c'est un système distribué d'accès à l'information qui s'appuie sur les principes de l'hypertexte, du routage avec protocole IP et qui supporte les documents multimédias.

WYSIWYG
WYSIWYG
What You See Is What You Get
« Ce que vous voyez est ce que vous obtenez ».
Technique permettant de reproduire l'image exacte de la représentation écran.

X.25
X.25
Recommandation de l'UIT définissant des mécanismes de transmission de données à commutation de paquets. Elle consiste à découper les données en blocs assez courts pour les acheminer de la source à la destination à travers un lien virtuel unique appelé circuit virtuel (commuté ou permanent). Bidirectionnel, ce qui permet un contrôle de flux sur l'ensemble de la chaîne de transmission.

X509
X509
Norme de l'UIT-T spécifiant un cadre de travail pour la certification de clefs publiques, et définissant entre autres un format de certificat.

xDSL
xDSL
x Digital Subscriber Line
Techniques numériques sur ligne téléphonique en cuivre (utilisation de fréquences au-delà des fréquences vocales), permettant d'augmenter le débit de transmission.

XKMS
XKMS
XML Key Management Specification
Défini par l'IETF et le W3C, ce standard traite des services de gestion des clés et certificats utilisés par les applications lors d'échanges par messages XML.

XML
XML
eXtensible Markup Language
Langage permettant de décrire le contenu d'une page Web indépendamment de sa présentation.

ZIP
ZIP
Zone Information Protocol
Protocole sur les réseaux appletalk établissant une coresspondance entre le nom d'un réseau et un nom de zone.

ZKP
ZKP
Zero knowledge proofs
Démarche où un demandeur prouve au vérificateur qu'il connait certaines information sans avoir à les révéler.

Terme technique
English
Signification de l'acronyme
Description

Les organismes

3GPP
Third Generation Partnership Project
Groupe de normalisation de l'UMTS

ADAE
Agence pour le Développement de l'Administration Électronique
Service interministériel placé auprès du premier ministre pour favoriser le développement de systèmes d'information permettant de moderniser le fonctionnement de l'Administration.
Ses missions principales :
- contribuer à la promotion et à la coordination des initiatives, assurer leur suivi, procéder à leur évaluation ;
- apporter son appui aux administrations pour l'identification des besoins, la connaissance de l'offre, la conception des projets.

AFNOR
Association Française de NORmalisation
Cette association s'occupe de gérer tout ce qui est normalisation en France.

AFNIC
Association Française pour le Nommage de l'Internet en Coopération
Organisme officiel de gestion et d'attribution des noms de domaine « .fr ».

AFUTT
Association Française des Utilisateurs du Téléphone et des Télécommunications
Représente les utilisateurs de produits et services de télécommunications, est un interlocuteur des pouvoirs publics en charge des télécommunications et des opérateurs.
Elle est présente sur tous les terrains concernant les télécommunications, au niveau national et international.

ARPA
Advanced Research Project Agency
Agence pour les projets de recherche avancée du DoD américain.

ART
Autorité de Régulation des Télécommunications
Organisme de régulation des services de télécommunication en France. Mise en place le 5 janvier 1997 en France après l'ouverture du secteur des télécommunications à une concurrence totale (loi du 26 juillet 1996), l'ART est une institution indépendante qui dispose de compétences propres et qui en partage d'autres avec le ministre chargé des télécommunications. La régulation consiste en l'application, par l'autorité compétente, de l'ensemble des dispositions juridiques, économiques et techniques qui permettent aux activités de télécommunication de s'exercer librement.
Elle travaille sur des grands chantiers tels que : le développement des services mobiles ainsi que sur la concurrence effective et durable sur les marchés de la Boucle Locale et de l'accès à Internet.

ATM-Forum
Consortium de normalisation ATM, qui regroupe tous les constructeurs réseau concernés par ATM. Organisme de plus en plus complexe et politisé.

BCRCI
Brigade Centrale de Répression de la Criminalité Informatique
Le BCRCI a compétence pour mener des enquêtes judiciaires sur tout le territoire national. Au plan international, elle gère le « Bureau central national » d'Interpol (BCN) pour la fraude informatique, constitue le « point de contact central national » d'Interpol et participe aux travaux du Groupe de travail européen sur la criminalité informatique.
101, rue des Trois Fontanot
92000 Nanterre
Tél. : 01 40 97 87 72, 01 40 97 83 12

CCI
CyberCrimInstitut
Association à but non lucratif qui a vocation à :
- Étudier toutes les formes de criminalité et les utilisations déviantes des nouvelles technologies de l'information et de la communication au sens le plus large ;
- Informer et sensibiliser tous les acteurs des risques, menaces et vulnérabilités engendrés par les NTIC ;
- Former les utilisateurs aux meilleures pratiques pour faire face ;
- Communiquer et diffuser les informations disponibles dans ce domaine ;
- Assurer la promotion des concepts et outils garantissant un meilleur environnement de sécurité ;
- Participer à l'amélioration du niveau de confiance et de sécurité et contribuer à parcourir le chemin vers une culture de sécurité globale de la société de l'information.

CDEE
Club de Défense Économique des Entreprises
Club rassemblant les Directeurs de la Sécurité d'environ 50 grandes entreprises. FT y adhère depuis peu.

CELAR
Centre Électronique de l'Armement
Centre de compétence de la DGA pour tout ce qui a trait aux technologies de l'Information et de la Communication
CEN Comité Européen de Normalisation : organisme de normalisation dont les décisions ont valeur d'obligation au sein de la CEE ; traite les mêmes domaines que l'ISO.

CERT / A
CERT pour l'Administration
Centre de reporting à destination des administrations françaises (dépendant de la DCSSI), le CERTA est chargé d'assister les organismes de l'administration à mettre en place des moyens de protection et à résoudre les incidents ou les agressions informatiques dont ils sont victimes. Il constitue le complément indispensable aux actions préventives déjà assurées par la DCSSI et qui se situent plus en amont dans la démarche de sécurisation des systèmes d'information.
Afin d'assurer ces deux objectifs, 3 missions sont menées en parallèle :
- assurer une veille technologique ;
- organiser la mise en place d'un réseau de confiance ;
- piloter la résolution d'un incident (si besoin en relation avec le réseau mondial des CERTs).

Organisme
Signification de l'acronyme
Description

CERT / CC
CERT Coordination Center
Centre mondial de reporting des problèmes de sécurité Internet.
Créé à l'initiative de la DARPA.

CHEAr
Centre des Hautes Études de l'Armement
Institut d'études, rattaché à la DGA.

CICREST
Commission Interministérielle de Coordination des Réseaux Et des Services de Télécommunications pour la défense et la sécurité publique
Cette commission élabore et propose les règles dont il doit être fait application lorsqu'il y a lieu de tenir compte, pour la définition et la réalisation des réseaux et des services, d'une part, et pour la fourniture des prestations de télécommunications aux départements ministériels ainsi qu'aux entreprises ou organismes publics placés sous leur tutelle, d'autre part, des besoins de la défense nationale et de la sécurité publique. Les exploitants de réseaux ouverts au public autorisés en application de l'article L. 33-1 du code des postes et télécommunications, les fournisseurs du service téléphonique au public autorisés en application des dispositions de l'article L. 34-1 et les fournisseurs de services de télécommunications au public autorisés en vertu des dispositions des articles L. 34-2, L. 34-3 et L. 34-4, premier alinéa, du code des postes et télécommunications apportent, en tant que de besoin, dans le cadre des missions inscrites à leur cahier des charges, leur concours aux études et aux travaux de la CICREST.

CIGREF
Club Informatique des Grandes Entreprises Françaises
A pour mission de promouvoir l'usage des systèmes d'information comme facteur de création de valeur et de compétitivité pour l'entreprise.

CISSI
Commission Interministérielle pour la Sécurité des Systèmes d'Information
A pour vocation d'harmoniser la conception des programmes d'équipements et de proposer des solutions nouvelles.
Elle est présidée par un délégué et rassemble des représentants des membres de différents ministères.
Au nombre de ses missions :
- Fait apprécier le niveau de sécurité des systèmes en service, évalue leur vulnérabilité et recommande les limites de leur utilisation ;
- Est informée, sous contrôle des ministres responsables, des opérations relatives à la protection des systèmes d'information en projet dans les départements ministériels ;
- Oriente les recherches, études et travaux lancés en France en vue de répondre aux besoins exprimés par les départements ministériels ;
- Inventorie les organismes sous tutelle et s'efforce d'identifier les entreprises ou organismes privés dont l'activité justifierait, dans l'intérêt national, que leurs systèmes d'information soient protégés.

CLUSIF
Club de la Sécurité Informatique des Systèmes d'Information Français
Association ayant pour but de sensibiliser les entreprises françaises face au problème de la sécurité informatique en organisant notamment des séminaires autour de ce sujet.
2, rue de la Chaussée d'Antin - 75009 Paris
Tél. : 01 42 47 92 28

CNCIS
Commission Nationale de Contrôle des Interceptions de Sécurité (Autorité Administrative Indépendante)
Est chargée de procéder à une appréciation de la légalité des motifs de demande d'interceptions, et aussi d'autoriser ou de refuser les écoutes de lignes téléphoniques demandées par la police hors de tout cadre judiciaire pour lutter contre le terrorisme, le crime organisé, défendre la « sécurité nationale » ou combattre l'espionnage.
Une écoute téléphonique doit, depuis la loi no. 91-646 du 10 juillet 1991, passer par un juge et être examinée par la Commission des interceptions de sécurité (CNCIS).
Messagerie éléctronique pas concernée.

COG
Component Obsolescence Group
Association gérant les obsolescences de composants électroniques.

DARPA
Defense Advanced Research Project Agency
Nouveau nom du projet ARPA, conjoint aux ministères de la Défense et de l'Éducation (USA).

DCSSI
Direction Centrale de la Sécurité des Systèmes d'Information
Direction du SGDN chargée de la politique gouvernementale dans le domaine de la Sécurité des Systèmes d'Information.
Principales missions :
- Contribuer à la définition interministérielle et à l'expression de la politique gouvernementale en matière de sécurité des systèmes d'information ;
- Assurer la fonction d'autorité nationale de régulation pour la SSI en délivrant les agréments, cautions ou certificats pour les systèmes d'information de l'État, les procédés et les produits cryptologiques employés par l'administration et les services publics, et en contrôlant les centres d'évaluation de la sécurité des technologies de l'information (CESTI) ;
- Évaluer les menaces pesant sur les systèmes d'information, donner l'alerte, développer les capacités à les contrer et à les prévenir (CERTA) ;
- Assister les services publics en matière de SSI ;
- Développer l'expertise scientifique et technique dans le domaine de la SSI, au bénéfice de l'administration et des services publics.
- Former et sensibiliser à la SSI (Centre de formation à la sécurité des systèmes d'information - CFSSI).

Fort d'Issy les Moulineaux
18, rue du Docteur Zamenhof
92131 Issy-les-Moulineaux Cedex
Standard : 01 41 46 37 00

DDSC
Direction de la Défense et de la Sécurité Civiles
Coordination des fonctions étatiques dans les domaines de la Défense et de la Sécurité civiles.
Une des Direction du MISILL.

Organisme
Signification de l'acronyme
Description

DG XIII
Direction Générale n°13
Direction Générale chargée des télécoms et de la sécurité informatique. Corps de police à échelle européenne.
Rue de la loi 200 BU 29 4/68
B 1049 Bruxelles
Tél. : 32 2 296 85 35 ou 32 2 296 35 91

DGA
Délégation Générale pour l'Armement
Organisme du Ministère de la Défense chargé du développement des programmes d'armement, au profit des forces armées.

DoD
Department of Defence (USA)
Ministère de la Défense américain.

DSN
Direction de la Sûreté Nationale
Par rapport à la BCRCI, ce service du Ministère de l'Intérieur n'a pas vocation de faire de la procédure judiciaire mais plutôt de la prévention et du conseil en cas d'incident. C'est un service spécialisé dans l'étude et le conseil en matière de risque informatique.

DSSI
Directoire de la Sécurité des Systèmes d'Information
Chargé de proposer au premier ministre la politique à suivre en matière de sécurité des systèmes d'informations et d'en contrôler l'application. Il était présidé par le secrétaire général du gouvernement et est composé de représentants des grands ministères.

DST
Direction de la Surveillance du Territoire
Elle a pour mission de rechercher et prévenir sur le territoire français les activités inspirés, engagés et soutenus par des puissances étrangères et de nature a menacer la sécurité du pays. Elle dispose d'une section informatique chargée des enquêtes judiciaires lorsque les attaques attentent à la sécurité nationale ou aux secteurs de pointe de l'industrie française. La DST a eu également un rôle de sensibilisation auprès des entreprises ou dans les grandes écoles d'informatique.
1, rue Nélaton
75015 Paris (métro Bir Hakeim)
Depuis juillet 1985.
Tél. : 01 40 57 55 34

ETSI
European Telecommunications Standard Institute
Organisme européen de normalisation pour les télécommunications (Sophia Antipolis).

Eurescom
European institute for Research and Strategic Studies in telecommunications
European institute for Research and Strategic Studies in telecommunications.

FCC
Federal Communications Commission
Organisme de régulation des services de télécommunication aux USA.

GIC
Groupement Interministériel de Contrôle
Considéré comme le « central » d'écoute du gouvernement.
51, Bd Latour-Maubourg
à Paris dans l'hôtel des Invalides.

GITEP
« Groupement des Industries de Télécommunications et d'Électronique Professionnelle »
Syndicat professionnel rassemblant les entreprises de droit français exerçant leurs activités dans le domaine des Technologies de l'Information, de la Communication et des Services associés (TICS). Le domaine des TICS recouvre les réseaux, systèmes, matériels et logiciels : de télécommunication y compris la radio ainsi que de transmission, diffusion, traitement de l'information, et les services afférents. Membre de l'EICTA (European Information, Communications and Consumer Electronics Technology Industry Association) et de la FIEEC (Fédération des Industries Électriques, Électroniques et de Communication). Le GITEP TICS a pour mission de fédérer les positions de l'Industrie des télécommunications.
17, rue Hamelin
75783 Paris Cedex 16
Tél. : 01 45 05 70 64

GITSIS
Groupement Interprofessionnel des Techniques de Sécurité des Informations Sensibles

HCFDC
Haut Comité Français pour la Défense Civile
Association loi 1901 participant à la réflexion sur la doctrine, l'organisation et les techniques de la France en matière de défense et de sécurité civiles. FT y adhère depuis 2003.

IANA
Internet Assigned Number Authority
Organisme attribuant l'adressage IP et les protocoles TCP/UDP sur internet.

IEEE
Institute for Electrical and Electronics Engineers
Association d'ingénieurs américains ayant conduit la normalisation des LAN, MAN.

IETF
Internet Engineering Task Force
Organisme chargé du développement des protocoles d'interconnexion de réseau basés sur TCP/IP, dont Internet.

IHEDN
Institut des Hautes Études de la Défense Nationale
Institut d'études, rattaché aux services du Premier Ministre, placé sous la tutelle du Premier Ministre qui en fixe les missions :
- donner dans des sessions nationales ou régionales, à des personnalités françaises des différents secteurs d'activité, une information approfondie sur les grands problèmes qui intéressent la Défense ;
- soutenir, dans ces domaines, l'activité de ces personnalités devenues anciens auditeurs ;
- conduire ou susciter des études ou des recherches concernant la Défense ;

- apporter son concours, dans les domaines de la Défense, aux universités et organismes ayant vocation à l'enseignement, à l'information, aux études et aux recherches ;
- recevoir les Instituts et Collèges étrangers en vue de les informer sur la politique de Défense de la France.

IHESI
Institut des Hautes Études de la Sécurité Intérieure
Institut d'études, rattaché au MISILL. Son travail :
- Identifier les différentes formes de risques ou de menaces, évaluer leur impact sur l'opinion, analyser les réponses publiques a pour mission de réunir des responsables de haut niveau appartenant à la fonction publiqueet aux autres secteurs d'activité de la nation, en vue d'approfondir leurs connaissances en matière de sécurité intérieure par l'étude en commun des problèmes qui se posent dans ce domaine ;
- Conduire des études et des recherches concernant la sécurité intérieure et coopèrer, à cet effet, avec les universités, les établissements d'enseignement supérieur et de recherche, ainsi qu'avec les organismes concourant à la sécurité.

Département Ingénierie et conseil
Tél. : 01 53 68 20 07 - 01 53 68 20 08

INTERNIC
INTERnet Network Identification Center
Organisme officiel de gestion et d'attribution des noms de domaine de types génériques (« .com », « .net », « .org », …).

ISO
International Standard Organization
Organisation de normalisation regroupant 3 comités : TC (Technical Comittee), SC (Sub comittee), et de WG (Working Group).

NSA
National Security Agency
« No Such Agency » et pourtant la NSA existe.
Créée en 1952, cette agence est chargée de l'espionnage des télécommunications et de la mise au point des systèmes de codage et de cryptage destinés à garantir la confidentialité des messages du gouvernement, des diplomates et des militaires américains. Elle a également développé un réseau d'interception radioélectrique mondial baptisé Échelon s'appuyant sur un maillage électronique planétaire, supervisé par le NMCC (National Military Command Center). Le réseau Echelon dispose d'ordinateurs nommés Dictionaries qui n'utilisent pas de listes de mots-clés, mais des textes d'exemples dont ils extraient des n-grammes (suite de n caractères) significatifs et des relations mathématiques entre ces n-grammes, qui les rendent indépendants du langage et du vocabulaire.

MISILL
Ministère de l'Intérieur, de la Sécurité Intérieure et des Libertés Locales
Nouveau nom du Ministère de l'Intérieur français.

OASIS
Oganization for the Advancement of Structured Information Standards
Forum de standardisation des technologies du commerce électronique.

OCLCTI
Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la communication
Cet office, rattaché à la sous-direction des Affaires économiques et financières de la direction centrale de la Police Judiciaire, est chargé d'animer et de coordonner la mise en œuvre opérationnelle de la lutte contre les auteurs d'infractions spécifiques à la criminalité liée à ces nouvelles technologies et de procéder, à la demande de l'autorité judiciaire, à tous actes d'enquête et de travaux techniques d'investigations en assistance aux services chargés d'enquêtes de police judiciaire sur les infractions dont la commission est facilitée par ou liée à l'utilisation des technologies de l'information et de la communication, sans préjudice de la compétence des autres offices centraux de police judiciaire.

OSSIR
Observatoire de la Sécurité des Systèmes d'Information & des Réseaux
L'OSSIR est une association du type loi 1901 existant depuis 1996 qui regroupe les utilisateurs intéressés par la sécurité des systèmes d'information et des réseaux informatiques. Thèmes :
- sécurisation du poste de travail, antivirus et firewall personnels ;
- gestion des mises à jour, gestion de parc ;
- journalisation, tableau de bord, gestion de la sécurité ;
- solution globale antivirus (client, serveur, infrastructure) ;
- protection du périmètre de l'entreprise ;
- intégration de solution antivirus dans la messagerie ;
- gestion des accès distants, des utilisateurs nomades ;
- organisation de gestion de crise (moyens et procédures), expérience vécue ;
- spywares, chevaux de Troies, fuite d'information ;
- enjeux sociétaux, juridiques, économiques des infections informatiques ;
- techniques d'infection et conséquences, propagation des vers, polymorphisme…

RIPE NCC
Réseaux IP Européens - Network Coordination Center
Organisme officiel d'attribution et de gestion des adresses IP en Europe.

RIR
Regional Internet Registries
Désigne les 4 autorités (ARIN, APNIC, LACNIC, RIPE NCC) qui gèrent l'adressage IP sur Internet dans le monde.

SEFTI
Service d'Enquête sur les Fraudes aux Technologies de l'Information
Service spécialisé à la lutte contre la criminalité informatique dépendant de la Police judiciaire de la Préfecture de Police de Paris.
163, avenue d'Italie
75013 Paris
Tél. : 01 40 79 67 50

SGDN
Secrétariat Général de la Défense Nationale
Organisme dépendant du Premier Ministre, chargé de la Politique et de la Sécurité de Défense. Dans le cadre de la politique définie par le Gouvernement, il veille à la cohérence des actions entreprises en matière de sécurité des systèmes d'information. Pour ce faire,

Organisme
Signification de l'acronyme
Description

il dispose du service central de la sécurité des systèmes d'information.
51, boulevard de Latour-Maubourg
75007 Paris
Tél. : 01 44 18 80 11

SIMAVELEC
Syndicat des Industries des Matériels Audiovisuels Électroniques
Syndicat français regroupant les contructeurs de matériels audiovisuels.

SIOTEL
Syndicat International des Opérateurs en TELécommunications
Étude et défense des droits et des intérêts matériels et moraux tant collectifs qu'individuels des opérateurs et sociétés de télécommunications. Le Siotel fournit à ces opérateurs et sociétés le moyen de se consulter et de collaborer entre eux.

SPOTI
Services des Programmes d'Observation, de Télécommunications et d'Information
Service de la DGA pilotant tous les programmes réseaux et télécom.

UIT
Union Internationale des Télécoms
Organisme de normalisation, regroupant les opérateurs de télécommunications au niveau mondial ; délivre des recommandations (avis) ; jusqu'en 1993, était composé de deux entités distinctes (CCITT et CCIR) aujourd'hui regroupées au sein de l'UIT (UIT-R Radiocommunications et UIT-T Télécommunications).

W3C
WorldWide Web Consortium
Oganisme officiellement chargé de la normalisation de tout ce qui concerne le Web (Internet).

WECA
Wireless Ethernet Compatibility Alliance
Organisme chargé de maintenir l'interopérabilité entre les matériels 802.11.

WS-I
Web Services Interoperability Organization
Forum de normalisation des services Web.