

mai
2005

GUIDE SSI

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.

Accompagner

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). 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, intervention d'un expert pour éradiquer un virus ayant contaminé l'ensemble du réseau, réinstallation d'un programme ou d'un serveur, etc.

Aux Etats-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 connecté 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-dessous 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.

Les dix points clés	Les dix solutions
<p>Vous n'avez pas fait l'inventaire des biens à protéger et vous ne connaissez pas vos failles de sécurité éventuelles.</p> <p>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. (Fiche 1)</p>	<p>Fiche 1 : Bâtir une politique de sécurité</p> <ul style="list-style-type: none">→ Identifier et faire l'estimation des biens à protéger.→ Evaluer 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
<p>Vous n'avez pas connaissance de vos obligations légales.</p> <p>Pourtant les lois, règlements et accords professionnels sont contraignants et peuvent engager votre responsabilité personnelle :</p> <ul style="list-style-type: none">■ Dommages causés aux tiers (responsabilité de l'employeur engagée du fait de son salarié en cas par exemple en cas 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) (Fiche 2)	<p>Fiche 2 : Connaître la législation en vigueur et la jurisprudence</p> <ul style="list-style-type: none">→ 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.

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 / 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. **(Fiche 3)**

Fiche 3 : 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.

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, quelque fois 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. **(Fiche 4)**

Fiche 4 : 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.

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 de mise en œuvre de sauvegardes. **(Fiche 5)**

Fiche 5 : Mettre en œuvre un plan de sauvegarde :

- Politique de sauvegarde
- Procédures de sauvegarde
- Procédures de restauration
- Maintenir

Vous n'avez pas mis en œuvre les moyens minimum 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. **(Fiche 6)**

Fiche 6 : Mettre en œuvre des moyens de défense minimum :

- Bloquer les attaques automatisées.
- Limiter les brèches ouvertes.
- Limiter la prolifération virale.
- Détecter les anomalies

Vous avez déployé des connexions sans fil (connexions Wi-Fi, bientôt Wi-Max, liaisons Bluetooth, postes nomade...).

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. **(Fiche 7)**

Fiche 7 : Mettre en œuvre des moyens de défense minimum pour les connexions sans fil :

- Particularité des réseaux sans fil
- Huit moyens de défense adaptés

Vous n'avez pas envisagé de précautions supplémentaires lors de la mise en place d'un site Web ou de procédures de télé travail.

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, ils peuvent, sans précautions supplémentaires, mettre en péril la confidentialité de vos données. **(Fiche 8)**

Fiche 8 : Etablir une barrière entre les données externes et internes :

- Deux usages
- Trois moyens de protection supplémentaires

<p>Vous pensez peut-être que la sécurité est établie une fois pour toutes.</p> <p>Le défaut de maintenance est aussi dangereux que l'inconscience car il peut créer un sentiment de fausse sécurité. (Fiche 9)</p>	<p>Fiche 9 : Gérer et maintenir les politiques de sécurité :</p> <ul style="list-style-type: none"> → Les risques liés au changement → Maintenance minimum → Moyens
<p>Vous manquez de ressources en interne.</p> <p>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.</p> <p>Vous craignez de ne pouvoir y consacrer suffisamment de ressources et que par suite la sécurité ne soit qu'illusoire (installer un pare-feu, un anti-virus sans les maintenir pendant que vos structures évoluent et que les menaces se renouvellent sans cesse). (Fiche 10)</p>	<p>Fiche 10 : Externaliser la mise en œuvre et la maintenance des politiques de sécurité</p> <ul style="list-style-type: none"> → Installation et configuration, maintenance sur site → Externalisation → Dix points-clés d'un contrat d'externalisation de la mise en œuvre et de la maintenance des politiques de sécurité

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 anti-virus (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 révélera 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 qui 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 de 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 politique de sécurité, configuration des firewalls, mise à jour du plan de sécurité, etc).

Il est recommandé de :

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 anti-virus 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 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 Electronique
- <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 liées aux technologies de l'information et de la communication
- <http://www.cases.lu> : Site du Ministère de l'Economie 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 trouvera ce guide et les 10 fiches associées.
- <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 Economie Electronique du MEDEF, présidé par Philippe Lemoine, président de LASER.

Ce Comité fait lui-même partie du Groupe de Propositions et d'Actions (GPA) Recherche – Innovation – Nouvelles Technologies du MEDEF, présidé par Eric Hayat, président fondateur de Stéria 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 Coupe), Sonilog (Aïda Demdoun), 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 Economie Electronique 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** (Afnét), **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

Anti-virus	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)	Élément 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.
Faible 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.