Direction Innovation, Recherche et Nouvelles Technologies

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

Contact : cgabay@medef.fr

Contact : Catherine Gabay, Directeur - Innovation, Recherche et Nouvelles Technologies, MEDEF, cgabay@medef.fr

Introduction

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 sécurité des systèmes d'information, et au-delà la sécurité des échanges, est une obligation qui concerne aujourd'hui toutes les entreprises. La sécurité est liée à la fiabilité du système d'information comprenant le réseau, les systèmes, les applications, les procédures d'accès des utilisateurs et de maintenance.

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.

- La France n'est pas épargnée par ces pertes. Selon l'étude TNS-Sofres (réalisée entre 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).

- Aux Etats-Unis, selon l'enquête réalisée en 2003 par le CSI (Computer Security Institute) conjointement avec le FBI, de nombreuses sociétés consultées ont déclaré avoir subi des sinistres :

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%.

Contact : Catherine Gabay, Directeur - Innovation, Recherche et Nouvelles Technologies, MEDEF, cgabay@medef.fr

◈ Pourquoi êtes-vous concerné ?

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

◈ Pourquoi vous protéger ?

De la perte de temps aux pertes financières lourdes, en passant par la possible perte de confiance des clients et partenaires, une sécurité défaillante peut conduire à la faillite de l'entreprise.
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).

Votre entreprise s'expose à un risque financier important lié à l'absence d'une politique sécurité :

- 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.

◈ Quels sont les risques liés aux technologies de l'information ?

Ils sont de quatre types :

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

Ces risques impliquent une menace potentielle pouvant être exploitée par une personne malveillante, qui au travers d'une faille de votre système, remettra en cause l'intégrité de votre système d'information.

Ces risques sont aussi bien internes qu'externes, et exploitent des vulnérabilités d'ordre technique, mais aussi humaines.

Contact : Catherine Gabay, Directeur - Innovation, Recherche et Nouvelles Technologies, MEDEF, cgabay@medef.fr

Comment se protéger ?

Mettre en œuvre un ensemble de bonnes pratiques, que l'on appelle une **« politique de sécurité »**, est indispensable pour réduire ces risques. 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 de l'entreprise. Cependant, 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 ?
- ✓ Vos salariés peuvent consulter ces données ?
- ✓ Vos salariés disposent de leur propre connexion Internet par modem tout en étant connecté sur votre réseau ?
- ✓ Vous échangez, via Internet, des données importantes avec vos clients ou prospects (par exemple gestion de commande, de stock, ou appel d'offres dématérialisés) en utilisant des moyens de communication modernes (mails, site web, connections extranet) et/ou vous faites du commerce en ligne ?
- ✓ Vos collaborateurs sont équipés de moyens mobiles de présentation et de communication (portables, assistants, tablettes, téléphones mobiles intelligents) ?
- ✓ Vous avez plusieurs établissements connectés ?

Si vous avez répondu OUI à au moins une de ces questions sans avoir mis en place une politique de sécurité, vous êtes concernés par ce guide.

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 sécurisation 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 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 qui communique de surcroît avec vos données internes (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**).

Contact : Catherine Gabay, Directeur - Innovation, Recherche et Nouvelles Technologies, MEDEF, cgabay@medef.fr

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.

Comment se protéger tout en maîtrisant les coûts?

Le tableau ci-après vous aidera à définir pour chaque usage-type, les différents éléments risques-menaces / conséquences-impacts / solutions-antidotes associées. Il vous permettra dans chaque cas d'approfondir le sujet au travers de fiches détaillées :

- **Fiche 1 : Bâtir une politique de sécurité ;**
- **Fiche 2 : Connaître la législation en vigueur et la jurisprudence ;**
- **Fiche 3 : Mettre en œuvre des moyens appropriés à la confidentialité des données ;**
- **Fiche 4 : Sensibiliser vos salariés ;**
- **Fiche 5 : Mettre en œuvre un plan de sauvegarde des données et des applications ;**
- **Fiche 6 : Mettre en œuvre des moyens de défense minimum ;**
- **Fiche 7 : Mettre en œuvre des moyens de défense minimum pour les connexions sans fil ;**
- **Fiche 8 : Etablir une barrière entre les données externes et internes ;**
- **Fiche 9 : Gérer et maintenir les politiques de sécurité ;**
- **Fiche 10 : Externaliser la mise en œuvre et la maintenance des politiques de sécurité.**

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.

Quelle que soit la complexité de votre installation, il est préconisé de mettre en œuvre de manière régulière et programmée (par exemple tous les trois mois), sur chacun de vos postes de travail, une action de protection minimale décrite plus loin dans ce document.

Pour une sécurité optimum, le travail de mise à niveau devra être réalisé dans certains cas avec l'aide de prestataires externes.

Contact : Catherine Gabay, Directeur - Innovation, Recherche et Nouvelles Technologies, MEDEF, cgabay@medef.fr

Usages - Risques - Menaces- Conséquences – Impacts	Solutions antidotes

Vous avez un système d'information connecté à l'extérieur.

Internet fait partie des usages habituels de votre société. **Vous échangez des mails, vous vous connectez sur le web, votre entreprise fait partie d'un Extranet (plateforme d'achat, de sous-traitance) par lequel vous collaborez avec des fournisseurs, partenaires, clients.** Vous êtes sans le savoir la cible d'attaques généralisées (propagation de virus par exemple) ou ciblées (un pirate informatique s'intéresse à votre activité par défi ou par intérêt). Dans tous les cas, si vous restez passif, vous risquez : - Une perte d'information et de données ; - Une perte d'image ; - Une perturbation voire l'arrêt temporaire de l'activité ; - 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.	La **fiche 1,** vous donnera des informations pour **bâtir votre politique de sécurité :** ❶ **Faire l'estimation des biens à protéger**. ❷ **Evaluer les besoins et les usages Internet de l'entreprise.** ❸ **Prévoir la protection de tous les canaux d'entrée, notamment les connexions par modem.** ❹ **Sensibiliser vos salariés au respect des règles de base**. Si vous disposez d'une politique de sécurité, il vous sera alors possible de souscrire efficacement une assurance complémentaire pour les dommages résultant des attaques. La **fiche 2** vous permettra de mieux **connaître la législation en vigueur et la jurisprudence :** Tous les pays ont un arsenal législatif sophistiqué pour lutter contre la fraude informatique. Les tribunaux ont eu à juger de nombreuses affaires et une jurisprudence commence à se faire jour. Le principe de précaution (basé sur la gestion en « bon père de famille » de la sécurité des entreprises) est une des pierres angulaires dans l'estimation des responsabilités respectives (attaquant, attaqué, complice passif de l'attaquant). Que faire si cela vous arrivait ? Dépôt d'une plainte : comment, chez qui ? ❶ **Quel est le régime général de responsabilité qui vous est applicable ?** ❷ **Quelles sont les règles concernant les contenus informationnels ?** ❸ **Quelle est la responsabilité du chef d'entreprise quant à son activité sur l'Internet ?** ❹ **Alerter et déposer plainte.**

Contact : Catherine Gabay, Directeur - Innovation, Recherche et Nouvelles Technologies, MEDEF, cgabay@medef.fr

Votre entreprise stocke et échange des données confidentielles ou stratégiques.

Dans chaque entreprise même non informatisée, il existe un accès différencié à l'information en fonction des niveaux de responsabilité de ses collaborateurs. Dans les systèmes d'information, il en est de même, sauf que, sans précautions préalables, 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. Enfin, l'identité des destinataires des données peut avoir été usurpée (tout comme celle de l'émetteur) ou les données reçues / envoyées peuvent être lues et copiées depuis l'extérieur dans les systèmes mal protégés. Le détournement ou le vol de données (depuis l'intérieur vers l'extérieur ou depuis l'extérieur vers l'intérieur) peuvent être critiques pour l'entreprise en terme de perte financière ou même d'image.	La **fiche 3** vous donnera des informations pour **mettre en œuvre des moyens techniques appropriés à la confidentialité des données :** ❶ Protéger **l'accès à vos données et à vos applications**. ❷ Votre entreprise doit accéder à des **échanges sécurisés, confidentiels ou certifiés.** ❸ Assurer la **sécurité des téléprocédures** ❹ Protéger **l'accès à vos données et à vos applications** ❺ **Echanger des données confidentielles**. ❻ Notions de base sur les **certificats, la signature électronique et le chiffrement.**

Vos salariés ont accès à des données confidentielles

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 (vol de données et transfert par Internet). L'activité frauduleuse d'un pirate informatique peut être facilitée par une action préalable dite d'« ingénierie sociale » consistant à parler à vos salariés en se présentant sous de fausses identités. Ces contacts sont souvent bénéfiques pour remplir leur objectif de découverte de mot de passe par exemple.	La **fiche 4** vous indiquera comment vous pouvez **sensibiliser vos salariés** La sécurité est l'affaire de tous les salariés. Une bonne politique de sécurité doit être partagée et comprise par tous. ❶ Comment se protéger contre des salariés négligents ou indélicats et les **faire adhérer** aux fondamentaux de la sécurité et à quels coûts ❷ Etre préparé à l'**Ingénierie sociale** ou la manipulation humaine : le cycle de manipulation, les plans de sensibilisation des salariés, les populations visées ❸ Généraliser les **Mots de passe** : à quoi ça sert, Les principes de mise en place et renouvellement, exemples de mots de passe simples ❹ Mettre en place une **Charte d'utilisation** : Le contenu de la charte, le cadre juridique de la charte.

Contact : Catherine Gabay, Directeur - Innovation, Recherche et Nouvelles Technologies, MEDEF, cgabay@medef.fr

Vos données sont stockées sur vos ordinateurs personnels ou sur les serveurs de l'entreprise

Une entreprise peut tarder à s'apercevoir que certaines données ont été corrompues, accidentellement ou intentionnellement. Leur reconstitution en est d'autant plus difficile en cas d'attaque ou d'incident technique.	La **fiche 5** vous donnera des éléments pour **mettre en œuvre un plan de sauvegarde des données et des applications.** **❶ Politique de sauvegarde** **❷ Procédures de sauvegarde** - les différentes méthodes de sauvegarde - La sous-traitance à un prestataire (la sauvegarde à distance) - Test des sauvegardes - Vérification des sauvegardes **❸ Retours d'expérience sauvegarde** - sur la périodicité - sur l'exhaustivité es sauvegardes - sur la localisation des supports de sauvegarde - sur l'évolution de la sauvegarde - sur les coûts **❹ Protéger l'accès à vos données et à vos applications** Mettre en place un plan de sauvegarde périodique des données ET des applications :

Contact : Catherine Gabay, Directeur - Innovation, Recherche et Nouvelles Technologies, MEDEF, cgabay@medef.fr

Vous utilisez la messagerie électronique notamment pour des messages importants et confidentiels (commande, contrat, données commerciales)
Vous accédez à Internet sur votre lieu de travail (recherche d'informations ou relations inter-sociétés et relations avec des tiers)
Vous avez une connexion permanente (Internet haut débit)
Vous utilisez un ordinateur portable (ou tout autre type de terminal connectable sur Internet puis sur votre réseau)

L'ordinateur utilisé pour se connecter est identifié par un numéro unique (adresse IP).

Vous êtes visible depuis le monde Internet. Vous devenez une cible :

1. **pour des attaques virales (virus ou vers) ou une attaque potentielle d'agressions marketing (spam, qui peuvent d'ailleurs véhiculer des virus) ou le réceptacle de chevaux de Troie** (qui serviront à attaquer votre site et vos systèmes et donc vos données ultérieurement ou encore à utiliser vos systèmes pour attaquer des tiers vous mettant ainsi en situation légalement dangereuse).

2. **Pour des attaques ciblées par un pirate informatique.** Pour s'introduire dans un ordinateur ou un système, le pirate a besoin que l'entreprise soit connectée.

Cette vulnérabilité aux attaques est aggravée si les postes de travail sont connectés en permanence (ADSL par exemple).

La **fiche 6** détaillera les éléments pour **mettre en œuvre des moyens de défense minimum** du type :

❶ Protection réseau grâce aux **pare-feu**.

Un **pare-feu d'entreprise** situé entre votre réseau d'entreprise et l'Internet servira à filtrer le trafic entrant et sortant afin d'éviter les attaques et les abus d'utilisation de la connexion à Internet. Les **pare-feu personnels** activés sur les machines de votre réseau constituent un second rempart contre les attaques réseau.

❷ Protection par **installation des mises à jour de sécurité de vos logiciels**.

Les logiciels que vous utilisez comportent des vulnérabilités qui font l'objet de mises à jour périodiques lorsqu'elles sont découvertes. Vous pouvez les télécharger sur Internet puis les déployer pour vous prémunir d'attaques contre ces vulnérabilités connues de tous, en particulier des attaquants.

Vous pouvez ensuite contrôler l'efficacité de votre gestion des mises à jour de sécurité grâce à l'utilisation périodique d'outils de tests de présence de vulnérabilités (réseau et applications).

❸ Protection antivirale par **l'utilisation de logiciels anti-virus**.

Ceux-ci peuvent être placés sur la passerelle Internet, sur la passerelle de messagerie ainsi que sur les postes de travail. Les messages ou contenus infectés ou malveillants peuvent être détruits systématiquement.

Ne pas oublier de mettre en place un système efficace de maintien à jour régulier des signatures antivirales.

A ces 3 moyens de protection classiques s'ajoute la **détection des anomalies des systèmes** afin de détecter d'éventuelles compromissions ou intrusions.

Contact : Catherine Gabay, Directeur - Innovation, Recherche et Nouvelles Technologies, MEDEF, cgabay@medef.fr

Vous utilisez des connexions sans fil

Les connexions sans fil (connexions WIFI, mobiles, liaisons bluetooth, …) sont susceptibles de permettre un piratage beaucoup plus facile des informations que vous échangez. L'entreprise a mis en œuvre des moyens de défense (voir ci-dessus) et croît être protégée. Mais les collaborateurs se déplacent avec leur portable, se connectent sur Internet chez eux ou ailleurs et reviennent se connecter dans votre réseau, porteurs de menaces potentielles.	La **fiche 7** vous indiquera comment **mettre en œuvre des moyens de défense minimum pour les connexions sans fil.** ❶ Qu'appelle-t-on **réseau sans fil ?** - ❷ Les réseaux sans fil sont des **cibles** ❸ Les **principaux risques encourus** ❹ La mise en œuvre de la **sécurisation du sans fil**

Vous souhaitez ouvrir une partie de votre système informatique vers l'extérieur

Vous avez un site web (site internet, extranet, ..)

Vous échangez des données informatiques
- avec des établissements secondaires
- avec des sociétés extérieures
- avec du personnel nomade

Un site web permet de communiquer mais rend très visible depuis l'extérieur et expose l'entreprise 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 sue le Web) ou très simples pour tester vos moyens de défense (scan) et la faiblesse de vos applications Web visibles depuis l'extérieur. **Vous êtes connectés avec les personnes à l'extérieur (clients, partenaires, fournisseurs, employés) pour échanger des données.** L'information, quelquefois confidentielle, transite sur Internet. Sans précautions, cette information peut être lue par d'autres personnes que les véritables destinataires.	La **fiche 8** vous expliquera comment **mettre en place des barrières de sécurité entre votre réseau d'entreprise, vos utilisateurs, les personnes habilités … et le reste du monde** ❶ Se **protéger** en définissant une "zone démilitarisée", testant les applications web exposée, s'appuyant sur des liaisons sécurisées ❷ Mettre en place une zone tampon entre l'interne et l'externe, appelée **"zone démilitarisée" ou DMZ**. Plusieurs solutions possibles : DMZ pour protéger les services offerts aux internautes, Protéger les services offerts aux internautes via son fournisseur d'accès à internet, DMZ avec relais des services internes ❸ Mettre en place un **réseau privé virtuel (RPV ou VPN)**, conduit (tunnel) sécurisé entre deux ordinateurs ou deux réseaux en utilisant l'infrastructure Internet en général: Comment faire simplement? Par une solution avec service de chiffrement intégré.

Contact : Catherine Gabay, Directeur - Innovation, Recherche et Nouvelles Technologies, MEDEF, cgabay@medef.fr

Votre métier évolue,
vous changez vos systèmes et vos applications,
vous embauchez,
vous débauchez

Vos systèmes d'information et vos applications évoluent avec votre activité. Votre personnel change de fonction, de responsabilités. Vous embauchez (CDD ou CDI) ou vous débauchez. Tous ces facteurs de changements doivent être maîtrisés au risque que votre sécurité soit illusoire. 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 ?	La **fiche 9** vous indiquera comment **gérer et maintenir les politiques de sécurité** ❶ **Valider régulièrement la configuration de vos pare-feu et autres systèmes de protection** ; ❷ **Tester ponctuellement la vulnérabilité de tous les composants logiciels** de votre système d'information aux attaques potentielles ; ❸ **Gérer les authentifications**.

Vous préférez vous consacrer votre métier
et confier la mise en œuvre et la gestion de la sécurité
à des prestataires de service.

Vous manquez de ressources en interne ou vous considérez que la sécurité des systèmes d'information n'est pas votre métier. Vous craignez de ne pouvoir y consacrer suffisamment de ressources pour que la sécurité ne soit qu'illusoire (installer un pare-feu, un anti-virus et les oublier, pendant que vos structures évoluent et que les menaces se renouvellent sans cesse).	La **fiche 10** vous donnera des conseils pour **externaliser la mise en œuvre et la maintenance des politiques de sécurité.** Vous devez : ❶ Négocier un **niveau de service** (SLA : « service level agreement ») conforme à vos attentes ; ❷ Mettre en œuvre des **indicateurs pour apprécier la qualité de service de ces prestataires.** En annexe : **10 points-clefs d'un contrat d'externalisation de la mise en œuvre et de la maintenance des politiques de sécurité**

Contact : Catherine Gabay, Directeur - Innovation, Recherche et Nouvelles Technologies, MEDEF, cgabay@medef.fr

Protection minimale

Il est de votre responsabilité de garantir le niveau de protection de votre entreprise.

L'ensemble d'actions qui en résulte 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, au minimum tous les trimestres.

Il est recommandé de :

- **Définir un plan de sauvegarde des données sensibles ou stratégiques de l'entreprise** ;

- **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 réalisés, 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)** – voir fiche 6;

A titre d'exemple, sur 4.240.883 vérifications réalisés, 25% des sites vérifiés ne sont pas protégés par un anti virus et 9% des sites protégés par un anti virus n'ont pas une version à jour.

- **Installer sur chaque machine un «firewall » logiciel**, en faisant bien attention à sa configuration (ce qui garantira son efficacité en cas de tentative d'intrusion) ; et faire régulièrement les mises à jour intégrées au contrat de maintenance (couvrant en général une durée d'un an) – voir fiche 6.

Contact : Catherine Gabay, Directeur - Innovation, Recherche et Nouvelles Technologies, MEDEF, cgabay@medef.fr

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 leur comportement à l'exécution.
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…).
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 clés publiques (utilisées par les algorithmes asymétriques, avec clés distinctes).
Déni de service	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 » qui les découvrent peuvent créer des virus exploitant ces failles pour infecter 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 (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.
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 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).

Contact : Catherine Gabay, Directeur - Innovation, Recherche et Nouvelles Technologies, MEDEF, cgabay@medef.fr

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'accés au réseau privé.
WLAN (Wireless LAN)	Réseaux locaux sans fils, normalisés sous la référence IEEE 802.11.

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.foruminternet.org/ » : espace d'information et de débat sur le droit de l'internet.

Contact : Catherine Gabay, Directeur - Innovation, Recherche et Nouvelles Technologies, MEDEF, cgabay@medef.fr

- « http://www.adae.pm.gouv.fr » : l'Agence pour le Développement de l'Administration Electronique
- « http://www.cnil.fr » : la Commission nationale de l'informatique et des libertés
- « 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.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.

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, co-président du groupe Galeries Lafayette et 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)	Hervé Schauer Consultants (Hervé Schauer)
AchatPublic (Dimitri Mouton)	HP France (Christophe Stener)
Adentis (Stéphane Madrange)	IPP Technologies (B. Pourcines)
AFNET (Youval Eched)	La Poste, (Monique Cosson, Brice Welti)
Alcatel (Jean-Paul Bonnet)	Laser (Isabelle Felix, Philippe Lemoine)

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)

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)

Contact : Catherine Gabay, Directeur - Innovation, Recherche et Nouvelles Technologies, MEDEF, cgabay@medef.fr