

# *Fiche de l'AWT*

## *La sécurité*

### *informatique*

La sécurité informatique est essentielle pour l'entreprise, particulièrement dans le contexte de l'e-business: définition, dangers, coûts, outils disponibles

Créée le 15/04/00  
Modifiée le 15/04/00

# 1. Présentation de la fiche

---

*La sécurité informatique est essentielle pour l'entreprise, particulièrement dans le contexte de l'e-business: définition, dangers, coûts, outils disponibles*

**Parmi les craintes les plus souvent avancées par les entreprises concernant l'informatique en général et le commerce électronique en particulier, figure notamment la problématique de la sécurité.**

Si la notion de sécurité des systèmes informatiques et des données qu'ils traitent n'est pas nouvelle, il est évident que le développement extraordinaire des réseaux et singulièrement de l'Internet en a fait une priorité absolue pour les entreprises. Il ne se passe pas un mois sans que les médias évoquent des cas de piratages informatiques commis par les désormais célèbres crackers.

**L'objectif de cette fiche est de situer clairement la place que doit occuper la sécurité informatique dans l'entreprise et de présenter les différentes solutions existantes.**

## 1.1. Autres fiches à consulter

---

- **Qu'est-ce qu'un Intranet?**  
Présentation d'une ressource technologique indispensable aux entreprises: définition, utilité, composants, facteurs de réussite et schéma explicatif  
création le 15/04/00 | dernière modification le 13/04/00
- **Contrat d'accès à l'Internet**  
Définition et enjeux de ce type de contrats. Objet et prestations liées au contrat. Les différentes obligations pour les parties  
création le 24/11/00 | dernière modification le 24/11/00
- **La communication via le réseau Internet**  
Comment se déroule une communication d'informations sur le réseau Internet?  
Descriptions des éléments logiciels et matériels, présentation des différentes couches et rôle des ISP  
création le 28/11/00 | dernière modification le 27/02/03
- **Sites dynamiques et bases de données**  
Les pages dynamiques et l'accès aux bases de données sont des technologies indispensables au développement d'un site web d'e-business  
création le 18/04/01 | dernière modification le 03/01/02
- **Signature électronique**  
La reconnaissance juridique de la signature électronique constitue la pierre angulaire pour assurer la sécurité et la fiabilité des échanges en ligne. Présentation des aspects techniques et juridiques  
création le 24/04/01 | dernière modification le 19/07/01
- **Cadre juridique des relations inter-entreprises**  
Du point de vue juridique, les stratégies e-business inter-entreprises (B2B) s'organisent en un ensemble de contrats tenant lieu de loi entre les parties  
création le 02/05/01 | dernière modification le 02/05/01
- **Les différents modes de connexion à Internet**  
PSTN, RNIS, ADSL, SDSL, câble, ligne louée ou encore accès mobile: l'offre de connexion à l'Internet s'est considérablement diversifiée. Comment choisir un type de connexion en fonction de ses besoins? C'est le sujet traité par cette fiche  
création le 14/05/03 | dernière modification le 27/11/03

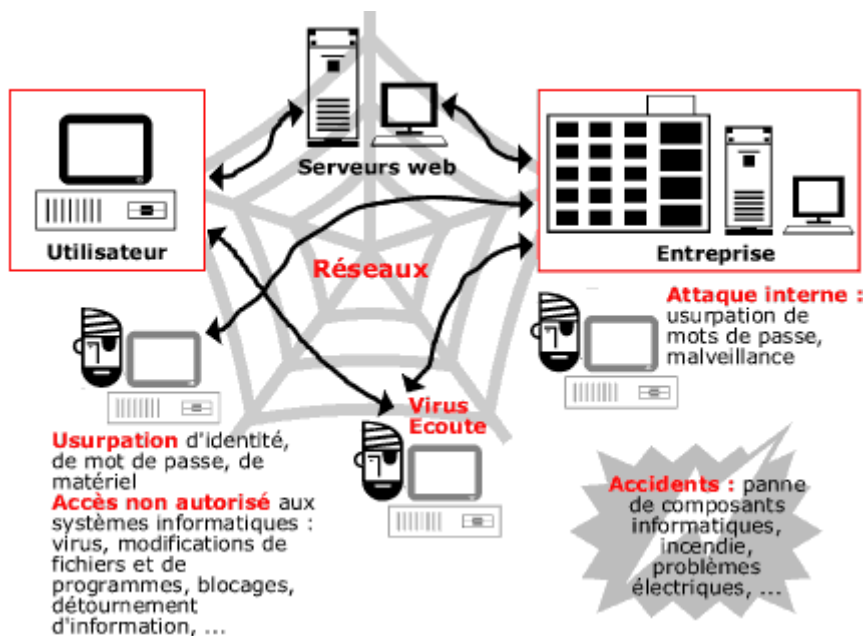
## 2. Définition, dangers potentiels et domaines relevant de la sécurité

Définition et portée de la sécurité informatiques. Quels sont les dangers potentiels (schéma explicatif)? Quels sont les domaines concernés (authentification, intégrité, autorisation, protection physique, etc.)?

### 2.1. Définition

La sécurité est la situation dans laquelle un système informatique, connecté ou non à un réseau externe de télécommunications, est protégé des dangers internes ou externes.

### 2.2. Quels sont les dangers potentiels?



## 2.3. Les domaines relevant de la sécurité

Domaines	Exemples de question de la part		Problèmes potentiels
	de l'utilisateur externe	du fournisseur de services et d'informations	
<b>Authentification détermination de l'identité de l'interlocuteur</b>	Le serveur est-il réellement celui qu'il dit être?	L'utilisateur est-il bien celui qu'il prétend être?	Usurpation d'identité
<b>Intégrité l'assurance que l'information stockée ou transmise n'est pas altérée</b>	L'information reçue est-elle identique à celle émise? Mes fichiers sont-ils corrompus? L'information est-elle fiable?		Modification accidentelle ou intentionnelle de l'information hébergée ou des transactions électroniques
<b>Confidentialité la connaissance de l'information par un groupe restreint de personnes ou de systèmes</b>	L'information n'est-elle connue que de l'émetteur et du récepteur? L'information stockée est-elle accessible uniquement aux personnes autorisées?		Détournement de l'information, appropriation non autorisée d'informations
<b>Autorisation la permission de faire ou d'accéder à quelque chose</b>	Qui peut accéder à mon ordinateur pendant mon absence?	L'utilisateur distant accède-t-il uniquement aux services et informations pour lesquels il a obtenu une autorisation?	Accès non autorisé à des ressources ou informations
<b>Non répudiation protection contre la négation d'une action accomplie</b>	Le fournisseur de services peut-il faussement prétendre qu'il n'a pas reçu ou effectué la transaction?	L'utilisateur peut-il faussement prétendre qu'il n'a pas effectué une transaction?	Nier avoir passé une commande électronique ou avoir effectué un achat
<b>Traçabilité garder un historique des événements</b>	Qui a fait quoi, utilisé quoi et quand?		Impossibilité de reconstituer les étapes qui ont conduit à un incident
<b>Intrusion accès non autorisé</b>	Comment protéger mon système personnel?	Comment détecter les intrus? Comment protéger le serveur?	Accès non autorisés et actions malveillantes (introduction de virus ou de mouchards, modification de contenu, blocage des accès, etc.), accès non souhaités (e-mail publicitaire)
<b>Protection physique protection contre les accidents ou sabotage</b>	Garder l'intégrité des informations en cas de panne de courant, dégâts des eaux, incendie, etc.		Interruption non prévue de l'opérationnel et impossibilité de redémarrage rapide, dégâts irréversibles du matériel, de données
<b>Gestion des procédures, des ressources humaines et machines</b>		Que doit-on faire? Qui fait quoi, qui est responsable de quoi, qui met à jour quoi? Qui peut entrer en salle machine?	Pas de contrôle, manque de rigueur dans la gestion des mots de passe, des mises à jour des fichiers d'autorisation d'accès, des fichiers d'audit, de la configuration des routers et firewalls, etc.

### 3. Coûts, portée et facteurs de réussite d'un projet de sécurité

*Quel est le coût d'une stratégie de sécurité informatique? Analyse de la portée d'une telle stratégie, des facteurs de réussite d'un tel projet et des ressources nécessaires à sa mise en oeuvre*

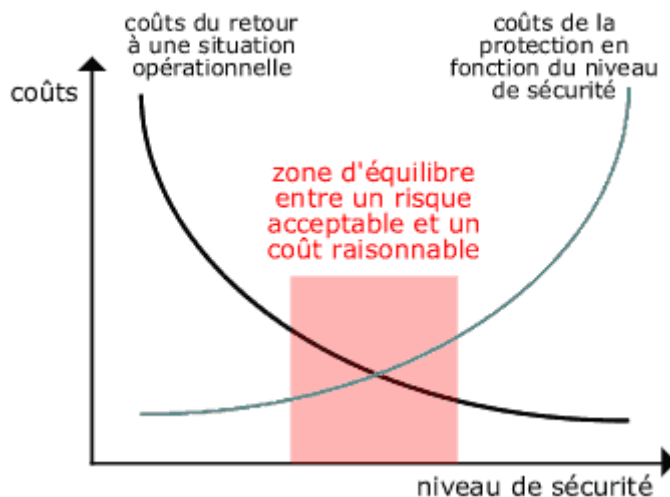
#### 3.1. Quel est le coût de la sécurité?

**Ne rien protéger ne coûte rien dans le poste sécurité.** Il faut dans ce cas évaluer le risque d'un incident, c'est-à-dire les coûts tangibles des ressources utilisées pour revenir à un état normal (par exemple reconstruire un fichier) ainsi que les coûts intangibles (par exemple la perte de clientèle).

**Se protéger de tout est impossible et exigerait un coût extrêmement élevé.** Le coût d'une protection à 99% (100 % est impossible) dépasserait probablement le coût des éléments à protéger.

**Chaque entreprise doit donc définir les solutions à adopter en fonction:**

- des éléments à protéger et contre qui,
- de la valeur de ces éléments ou de leur reconstruction,
- de la probabilité d'occurrence,
- de la perte potentielle,
- des coûts de protection ou de non-protection associés.



## 3.2. Portée de la sécurité et ressources nécessaires

---

**Une solution de sécurité comprend une suite d'éléments: mots de passe, cryptage, firewall, etc.** De même qu'une chaîne est aussi résistante que le plus faible de ses maillons, une solution de sécurité sera aussi efficace que le point le plus faible (single point of failure). **La solution de sécurité choisie doit donc être complète pour la zone d'équilibre choisie.**

**La sécurité doit être assurée vis à vis de l'extérieur de l'entreprise, mais également vis-à-vis de l'intérieur de l'entreprise. La majorité des problèmes trouvent leur origine à l'intérieur de l'entreprise** (par exemple un firewall mal configuré).

**Implémenter un projet de sécurité est un projet en soi, qui exige des ressources humaines et matérielles.** On y retrouve les phases traditionnelles:

- d'analyse et d'évaluation des risques;
- de conception, de développement, de tests;
- de gestion (contrôle, mesure, mise à jour).

## 4. Les outils de sécurité

*Examen des différents moyens d'assurer sa sécurité informatique (encryption, signature électronique, certificats, authentification, autorisation, firewall, VPN, etc.)*

**Le système de sécurité d'une entreprise se construit à l'aide de nombreux outils complémentaires et techniques existant sur le marché.** Un seul ne suffit pas: la sécurité est assurée par une utilisation correcte d'un ensemble d'outils à choisir, paramétrer et/ou développer en fonction de l'objectif de sécurité fixé.

### 4.1. Encryption, signature électronique et certificats

**L'utilisation des techniques d'encryption, de signature électronique et des certificats sont la base d'un commerce électronique sécurisé:**

- **l'encryption:** elle consiste à transformer les informations électroniques au moyen d'un algorithme mathématique afin de les rendre inintelligibles, sauf pour celui qui possède le moyen (une clé) de les décoder. L'encryption des informations qui transitent par le réseau est utilisée pour assurer la confidentialité, l'intégrité et l'authenticité des transactions et du courrier électronique. A titre d'exemple, le logiciel d'encryption gratuit Pretty Good Privacy (PGP) est très largement employé pour protéger le courrier électronique;
- **la signature électronique:** c'est un code digital (une réduction du document électronique à envoyer) qui, associé aux techniques d'encryption, garantit l'identité de la personne qui émet le message et assure la non-répudiation et l'intégrité de l'envoi;
- **le certificat:** document électronique (carte d'identité) émis par une autorité de certification. Il valide l'identité des interlocuteurs d'une transaction électronique, associe une identité à une clé publique d'encryption et fournit des informations de gestion complémentaires sur le certificat et le détenteur.

### 4.2. L'authentification et l'autorisation

**Une personne peut être authentifiée par la combinaison d'une identification et d'un mot de passe** (code secret personnel). Le mot de passe doit posséder certaines caractéristiques: non trivial, difficile à deviner, régulièrement modifié, secret, etc. Des outils logiciel ou hardware de génération de mots de passe existent.

**L'authentification précède généralement l'autorisation. L'autorisation définit les ressources, services et informations que la personne identifiée peut utiliser** et dans quelle mesure (par exemple consulter ou mettre à jour des données).

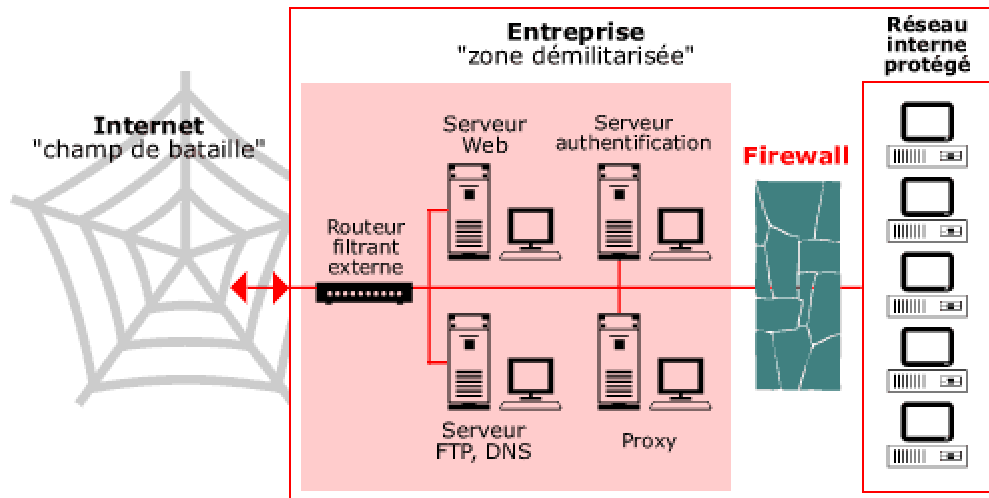
Les techniques d'encryption et de certificats utilisés conjointement à celle des mots de passe ajoutent un très haut degré de sécurité dans le domaine de l'authentification des utilisateurs.

### 4.3. Le firewall

**Le firewall est un ensemble informatique du réseau d'entreprise comprenant du matériel hardware (un ou des routers, un ou des serveurs) et des logiciels (à paramétrer ou à développer). Son objectif est de protéger le réseau interne contre les accès et actions non autorisés en provenance de l'extérieur, en contrôlant le trafic entrant. Le firewall peut également contrôler le trafic sortant.**

Le firewall est localisé entre le réseau externe et le réseau interne. Pour être efficace, le firewall doit être le seul point d'entrée-sortie du réseau interne (pas de modem sur un serveur ou pc pour accéder à l'extérieur sans passer par le firewall) et surtout doit être correctement configuré et géré en fonction des objectifs spécifiques de sécurité. Sans ces précautions, un firewall ne remplit pas son rôle et est complètement inutile.

**Le firewall est un élément de la sécurité, il ne couvre pas tous les risques** (par exemple le firewall n'assure pas la confidentialité des informations, n'authentifie pas l'origine des informations, ne vérifie pas l'intégrité des informations, ne protège pas contre les attaques internes).



**Il existe plusieurs types de techniques de firewall:**

- **la technique de filtrage des paquets:** chaque paquet d'information entrant ou sortant est accepté ou rejeté selon des règles établies par l'utilisateur;
- **la technique des serveurs proxy** qui empêchent l'extérieur de connaître les adresses internes du réseau d'entreprise;
- **la technique des passerelles** qui fournissent des systèmes de sécurité pour établir des connexions TCP/IP entre l'extérieur et l'intérieur ou pour certains services comme FTP et Telnet.

## 4.4. Les fichiers historiques

---

**Des outils de traçabilité (logging) doivent être mis en oeuvre pour garder une trace des événements,** comme par exemple:

- qui est venu, quand, quelle a été la durée de la transaction?
- qu'a-t-on consulté ou modifié?
- quelles on été les ressources utilisées?

**La consultation régulière des fichiers historiques constitués doit notamment permettre de vérifier les anomalies dans le trafic des transactions** (par exemple les message répétitifs en provenance d'une même adresse extérieure et rejetés par le firewall peuvent être un signe d'essai d'intrusion).

## 4.5. Les copies de sauvegarde

---

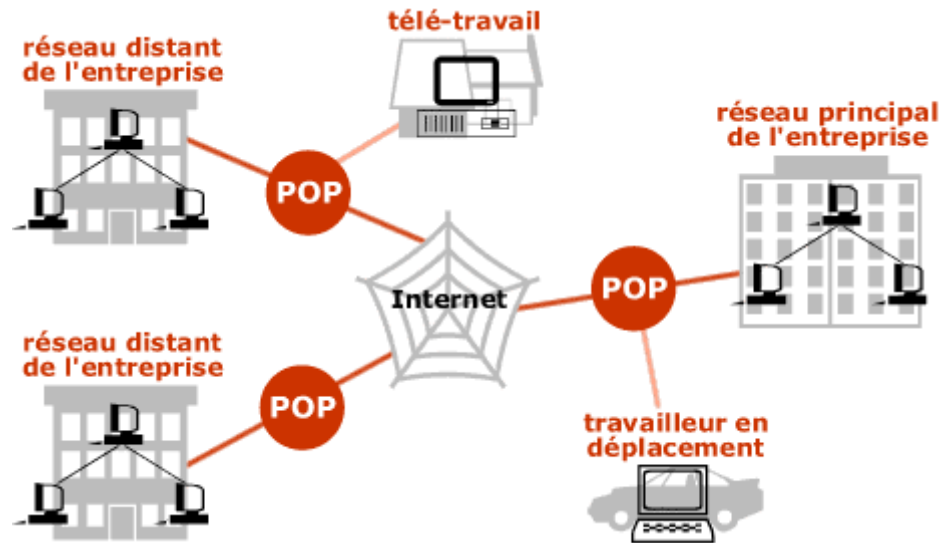
**Les copies de sauvegarde (back-up) créées régulièrement et stockées dans des endroits sécurisés permettent de protéger les informations essentielles pour l'entreprise** et permettent également de redémarrer rapidement en cas de problème.

## 4.6. Réseau Privé Virtuel

---

**Le VPN (Virtual Private Network) est un service disponible chez les fournisseurs de services Internet (ISP) qui permet d'établir des connexions sécurisées privées (un réseau privé) sur un réseau public comme l'Internet.** Le VPN est réalisé avec les techniques d'encryption et d'authentification, en assurant la qualité de services requise. Le VPN permet l'économie de connexions directes coûteuses entre les différentes implantations de l'entreprise, l'accès Internet lui servant à la fois pour la consultation classique de sites web et pour son réseau privé.

**Voici un exemple de VPN:**



© Agence Wallonne des Télécommunications  
Avenue de Stassart 16 à 5000 Namur - Belgium  
[www.awt.be](http://www.awt.be) - [info@awt.be](mailto:info@awt.be)