



Technologies de l'information et développement des PME : des précautions à prendre

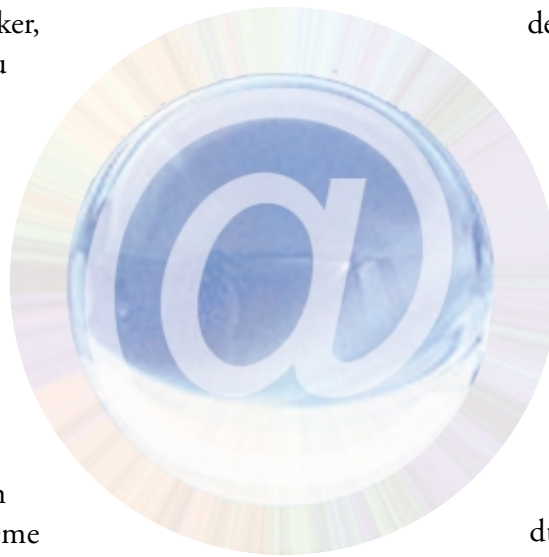
Valeur ajoutée stratégique de la compétitivité des entreprises depuis le développement des TIC, le système d'information peut se définir comme "tout moyen destiné à élaborer, traiter, stocker, acheminer, présenter ou détruire l'information".

Dans l'entreprise, il comprend l'ensemble des moyens matériels et logiciels qui assurent le stockage, le traitement et le transport des données sous format électronique.

Le système d'information est aujourd'hui "le système nerveux" de l'entreprise. L'explosion de l'économie numérique et de la société en réseaux et l'accroissement spectaculaire des échanges d'informations numérisées ont

démultiplié les opportunités de développement pour votre entreprise ; mais, ce nouvel environnement a également aggravé l'exposition de votre système d'information à de nouvelles menaces. Ces vulnérabilités requièrent la vigilance de chacun afin d'assurer la sécurité des systèmes d'information des entreprises françaises, qui est l'un des aspects d'une politique globale de sécurisation des informations.

Le Ministère de l'Economie, des Finances et de l'Industrie et l'Assemblée des Chambres Françaises de Commerce et d'Industrie se sont associés pour sensibiliser et mobiliser les entreprises sur cet aspect essentiel de la protection de leur patrimoine.



L'objectif de cette démarche est donc double :

- ✓ **créer un réflexe de vigilance pour sécuriser les systèmes d'information,**
- ✓ **informer sur les précautions utiles.**



Votre système d'information est vital

Le système d'information structure tous les aspects de votre activité.

Il contient l'ensemble des informations de votre entreprise :

- ✓ administratives (comptabilité, paye, achats, ressources humaines, etc),
- ✓ techniques (plans, procédés, etc),
- ✓ commerciales (liste de clients, factures, prix, prospects, propositions en cours, etc),
- ✓ stratégiques (nouveaux produits, contacts avec des partenaires, etc).

Ce système et les informations qu'il contient vous engagent dans vos relations avec l'extérieur :

- ✓ l'obligation de déclaration des fichiers de données personnelles à la CNIL¹,
- ✓ les données nécessaires aux déclarations fiscales,
- ✓ la sécurité des données et services qui vous sont confiés par vos donneurs d'ordre ou par vos prestataires extérieurs (plans de fabrication, nombre de pièces commandées, etc),
- ✓ la qualité du service à la clientèle (gestion de la relation client, site de commerce électronique, etc).



Mais votre système d'information est vulnérable

Voici des exemples, tirés de situations réelles :

- ✓ un seul et même incendie détruit le bâtiment contenant à la fois le système informatique et les sauvegardes,
- ✓ une entreprise tarde à s'apercevoir que certaines de ses données ont été corrompues, accidentellement ou intentionnellement. Leur reconstitution en est d'autant plus difficile,
- ✓ un ordinateur portable est volé : les informations stratégiques et commerciales qu'il contient sont récupérées, éventuellement par un concurrent...
- ✓ un consultant en sécurité commet diverses imprudences : le détail des protections mises en place sur le système d'information est accessible à des tiers,

- ✓ un concurrent intercepte des données stratégiques de l'entreprise envoyées par voie électronique, à l'occasion, par exemple, d'une réponse à un appel d'offre en ligne,
- ✓ un collaborateur charge à son insu sur son poste un virus, qui diffuse sur Internet des fichiers stockés dans le système, ou un "cheval de Troie"² qui permet à un attaquant de fouiller son disque et d'attaquer les autres postes de travail,
- ✓ un pirate informatique pénètre les dispositifs de protection du système d'information de l'entreprise. Il peut provoquer des dégâts sur celui-ci ou s'en servir pour relayer une attaque vis-à-vis d'un tiers, qui se retournera contre l'entreprise,
- ✓ un salarié décide de lancer des attaques en utilisant sa connaissance des systèmes de l'entreprise,
- ✓ des attaques modifient la présentation et le contenu du site de l'entreprise ou en bloquent l'accès ; celle-ci perd la confiance de certains de ses clients.

L'analyse des dégâts sur les systèmes d'information illustre l'insuffisance de la réflexion et de l'anticipation vis-à-vis des risques encourus. Cette dernière révèle une double défaillance en termes :

- ✓ d'implication et de sensibilisation des dirigeants de l'entreprise,
- ✓ d'information des collaborateurs.

Les menaces pesant sur les systèmes d'information peuvent être définies en fonction :

- ✓ de l'origine de la menace, interne ou externe à l'entreprise,
- ✓ du caractère accidentel ou intentionnel de la menace,
- ✓ de la nature physique ou logique³ de la menace.



Vous pouvez réduire ces risques

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'entreprises.

Cependant, toutes les entreprises devraient respecter les principes de précaution suivants :

- ✓ mener une réflexion sur ce qu'il faut protéger et les risques acceptables. Elle nécessite un arbitrage par la direction générale (et non par le service informatique, par défaut) entre performances du système d'information, respect de la sécurité et coût,
- ✓ mettre en place une organisation adaptée, permettant de définir les règles à suivre et les modalités d'application (qui fait quoi ?), notamment en cas d'incident,
- ✓ impliquer chacun dans la sécurité des systèmes d'information, quel que soit son rôle dans l'entreprise,
- ✓ prendre en compte les menaces sur les systèmes d'information dans des contrats établis avec les prestataires extérieurs de confiance,
- ✓ mettre en place des produits de sécurité en adéquation avec les besoins.

Ce nouvel environnement nécessite de désigner un animateur de la fonction "sécurisation des systèmes d'information".



Prenez des précautions au quotidien

Face aux risques

d'accidents :

- ✓ sauvegarder régulièrement les serveurs, les postes de travail sur supports amovibles (disquettes, bandes...) et stocker les sauvegardes en lieu sûr, éloigné si possible des machines sauvegardées,
- ✓ examiner les contrats d'assurance au regard des garanties et des risques non couverts.

Chaque utilisateur est responsable de la sauvegarde de son travail, sur le serveur du réseau ou sur des supports amovibles (disquettes) conservés en lieu sûr, selon la sensibilité des informations.

d'intrusions physiques :

- ✓ limiter l'accès aux équipements du système en fonction de l'habilitation des personnels (lecteur de badges, par exemple).

Chaque utilisateur est responsable de l'accès à son poste de travail.

d'intrusions logiques :

- ✓ protéger l'ensemble du système d'information par un antivirus mis à jour,
- ✓ créer des mots de passe en prenant en compte les limites de cette sécurisation : certains logiciels disponibles en ligne permettent de casser ce type de code,
- ✓ surveiller l'importation de fichiers et en particulier de logiciels de provenance inconnue, pour limiter les risques d'infection par des virus,
- ✓ établir une veille des publications du CERTA⁴ et des sociétés de veille technologique qui rendent publiques les vulnérabilités des principaux logiciels ainsi que les remèdes.

Chaque utilisateur doit signaler toute anomalie constatée dans le fonctionnement de son poste de travail.

Pour la sécurité des communications

- ✓ mettre en place des procédures strictes pour les connexions des postes de travail à l'extérieur par modem : veiller à ce qu'une machine ainsi connectée à l'extérieur ne le soit pas simultanément au réseau interne,
- ✓ procéder systématiquement à la désinfection (par antivirus) de toute machine ayant été connectée à l'extérieur avant de la raccorder au réseau interne,
- ✓ réguler l'usage de pièces jointes aux messages (par exemple, sous Windows, des fichiers en .exe, .vbs, .bat se révèlent parfois être des virus),
- ✓ protéger le système de l'entreprise par un pare-feu (firewall), pour détecter et repousser les tentatives d'intrusion en provenance d'Internet. Face à la complexité particulière de ce type de logiciels, s'assurer des compétences techniques de la personne en charge,
- ✓ sensibiliser les personnels au paramétrage de leur navigateur Internet (applets Java et ActiveX⁵ dans les pages sans garantie, cookies⁶),
- ✓ utiliser la signature électronique certifiée pour vos messages importants.

Chaque utilisateur doit se méfier des messages de provenance inconnue, potentiellement porteurs de virus, des pièces jointes éventuellement dangereuses et utiliser de préférence les formats les plus basiques. Il doit consulter l'animateur de la Sécurisation des Systèmes d'Information en cas de doute.

Pour les ordinateurs portables

- ✓ un ordinateur portable ne doit pas rester sans surveillance,
- ✓ un portable emporté en voyage doit être préalablement purgé de ses données sensibles ou, si ce n'est pas possible, celles-ci doivent être chiffrées avec un logiciel éprouvé,
- ✓ un portable, confié successivement à plusieurs personnes, devrait être purgé de ses données sensibles entre chaque utilisateur. S'il a été connecté à un réseau, il est indispensable de le décontaminer complètement,
- ✓ s'assurer que les collaborateurs se connectant, de l'extérieur, au réseau de l'entreprise, maîtrisent les conditions de sécurité et veillent à leur application.

Pour les données les plus sensibles

- ✓ aucun système d'information n'est totalement sécurisable ; si vous avez des données sensibles, à vous de définir celles que vous ne mettez pas sur votre système,
- ✓ les données sensibles restent vulnérables avant leur chiffrement : renforcer les mesures de protection contre les intrusions physiques et logiques (accès aux données par carte à microprocesseur),
- ✓ s'assurer de la fiabilité du logiciel de chiffrement, que les données soient stockées sur le poste de travail, sur un serveur ou transmises à l'extérieur,
- ✓ si les données chiffrées doivent être transmises, utiliser une disquette, envoyée par courrier ou remise en main propre, pour faire parvenir la clé de déchiffrement. N'utiliser le courrier électronique que s'il est certifié par une signature électronique. <http://www.certa.ssi.gouv>

¹ Commission Nationale Informatique et Liberté. Elle garantit la protection des libertés individuelles en contrôlant toute base de données intégrant des informations personnelles sur les individus.

² Programme informatique caché dans un autre qui exécute des commandes sournoises, et qui généralement donne un accès à la machine sur laquelle il est exécuté.

³ Attaque logique : utilisant des programmes informatiques, sans intervention physique sur le système.

⁴ Organisme rattaché au Secrétariat Général de la Défense Nationale et chargé de la détection des vulnérabilités, de la résolution des incidents et de la mise en place de moyens de prévention dans le domaine des systèmes d'information au profit de l'ensemble de l'administration.

⁵ programmes exécutés automatiquement par un site Internet sur son ordinateur

⁶ programmes s'installant lors de la consultation d'un site Internet et mémorisant les adresses électroniques sur lesquels il navigue jusqu'à ce qu'il retourne sur le site consulté initialement.

L'ensemble des activités de l'entreprise exige une politique de sécurisation.

Elle est propre à chaque entreprise.

C'est donc à la direction de l'établir et de veiller à son application.

La sécurisation a un coût.

Il doit être proportionné aux enjeux et aux risques.

La sécurité de votre système d'information doit être réexaminée périodiquement.

**La sécurité est l'affaire de tous.
Son efficacité repose sur la mobilisation
et l'adhésion des personnels.**

Pour plus d'informations, consultez :

