Le programme national « Sécurité des systèmes d'information »

Le MINEFI/HFD (Haut Fonctionnaire de Défense) et l'ACFCI ont signé en 2002 une convention cadre pour sensibiliser et former à la sécurité des systèmes d'information les petites et moyennes entreprises.

Cette convention prévoyait deux phases ; la première concernait la rédaction d'une brochure d'information destinée aux PME-PMI sur les risques liés à l'utilisation des TIC et s'est achevée fin 2002.

La deuxième phase, qui débute, doit permettre de mettre en place dans les C(R)CI des cellules de sensibilisation aux menaces visant les systèmes d'information des PME-PMI et aux parades adéquates.

La région Picardie, par l'intermédiaire de la CRCI, fait partie des huit régions pilotes désignées pour organiser les premières actions de sensibilisation.

La Sécurité des Systèmes d'Information

Dans ce dossier, le Service d'Information Economique de la Chambre Régionale de Commerce et d'Industrie de Picardie se propose de présenter les systèmes d'information, les menaces dont ils sont l'objet et les risques encourus du fait d'incidents de sécurité.

Les évolutions récentes et rapides de l'informatique ont contribué à l'accélération des échanges d'informations. Les entreprises se trouvent désormais confrontées au contrôle efficace de la confidentialité, de l'intégrité et de la disponibilité de ces informations.

Véritable point névralgique, le système d'information est souvent la proie de multiples attaques qui menacent l'activité économique des entreprises et requièrent la mise en place d'une politique interne de sécurité.

Système d'information et sécurité des systèmes d'information

D'une manière générale le système d'information concerne l'ensemble des moyens (organisation, acteurs, procédures et systèmes informatiques) nécessaires à l'élaboration, au traitement, au stockage, à l'acheminement et à l'exploitation des informations.

Dans les faits, de nos jours, l'essentiel du système d'information est porté par le système informatique et la notion de sécurité informatique recouvre pour l'essentiel la notion de sécurité des systèmes d'information (SSI).

Le concept de SSI recouvre donc un ensemble de méthodes, techniques et outils chargés de protéger les ressources d'un système informatique afin d'assurer la disponibilité des services, la confidentialité et l'intégrité des informations.

Les échanges au travers notamment d'Internet ont rendu également nécessaire le développement de propriétés nouvelles comme l'authentification, la paternité et la traçabilité de l'information.

La sécurité fait donc appel à différentes techniques complémentaires dont :

- *le chiffrement de l'information (cryptologie)*
- *la protection contre les signaux parasites compromettants (sécurité électronique)*
- *la protection contre les intrusions dans les logiciels, mémoires ou banques de données (sécurité informatique).*
- *la protection contre les accidents naturels et les actes malveillants (sécurité physique)*

Quelles menaces ?

Bien que souvent invisibles, du moins tant qu'elles n'ont pas eu de conséquences directes, les menaces sont cependant bien réelles :

- ***Les menaces physiques***

Actes de délinquance (vols, détérioration) et accidents naturels sont des menaces physiques qui visent directement le matériel. Souvent ignorés, les évènements naturels, accidentels ou malveillants, représentent pourtant jusqu'à 8% des sinistres déclarés (source : étude 2003 du CLUSIF sur la sinistralité).

Quelle entreprise peut se prétendre totalement à l'abri d'une inondation, d'une tempête ou d'un incendie d'autant que, si le matériel peut être, le plus souvent, aisément remplacé il n'en va pas de même des données qu'il contenait ?

- ***Les menaces informatiques***

Bien plus connues et envisagées, dès lors qu'on parle de sécurité des systèmes d'informations, les menaces informatiques (virus, chevaux de Troie, spams...) n'en sont pas moins de réels dangers. En 2003 environ 18% des entreprises ayant répondu à l'enquête du CLUSIF (étude sur la sinistralité) ont déclaré avoir été infectées par un ou plusieurs virus et l'impact financier en a été jugé élevé dans 11% des cas.

Heureusement la plupart des entreprises ont désormais saisi l'importance et l'intérêt des outils destinés à se prémunir de ces attaques (antivirus, firewall) et ces dernières voient leur efficacité reculer d'années en années.

- ***Les menaces internes***

Bien moins identifiées, les menaces internes sont plus souvent liées à la négligence et à l'ignorance du personnel de l'entreprise ; il s'agit plus d'inconscience que d'une réelle volonté de nuire.

En général ces menaces correspondent à un usage personnel du matériel informatique de l'entreprise avec d'une part le risque d'infection par virus (surtout dans le cas des ordinateurs portables confiés aux employés) et d'autre part un risque pénal par le téléchargement de programmes ou de fichiers pirates (films, musiques) qui sont incompatibles avec les applications professionnelles ou utilisés en dehors du cadre légal (licences d'exploitation).

Les cas d'espionnage industriel sont plus rares mais restent néanmoins un danger bien réel qui pèse sur les entreprises oeuvrant sur des marchés stratégiques. La sécurité des systèmes d'information passe aussi par la mise en place d'une politique efficace de protection visant à empêcher toute possibilité d'action malveillante par du personnel temporairement affecté à l'entreprise (stagiaires...)

Quels risques ?

Les risques sont tout aussi multiples et doivent être pris au sérieux. Nombre de personnes ne jugent ces risques que sous l'angle de l'entreprise agressée et peu savent ou même imaginent que leur propre responsabilité est engagée.

- *Les risques financiers*

En 2003, selon une étude publiée par KPMG, les dégâts occasionnés par des incidents de sécurité génèrent des pertes qui peuvent se chiffrer, en Europe, entre 0,2 et 0,5 % du chiffre d'affaires.

S'il est assez facile de mesurer la perte financière représentée par la destruction, le vol et le remplacement du matériel informatique, la perte que représente le vol ou la destruction d'un fichier clients, par exemple, est beaucoup plus difficile à mesurer mais bien réelle. Certaines entreprises n'ayant pas prévu de plan de redémarrage de leur activité en cas de problèmes informatiques graves ne sont pas à même de faire face rapidement et à moindre frais à une telle catastrophe.

- *La responsabilité pénale*

La loi relative à l'informatique, aux fichiers et aux libertés, oblige toute personne ordonnant ou effectuant un traitement d'informations nominatives à prendre toutes les précautions pour préserver la sécurité de ces informations et empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés.

Les risques encourus en cas de violation de cette loi sont très lourds : 5 ans d'emprisonnement et 300 000 € d'amende.

- *La responsabilité civile de l'employeur*

Le code civil énonce que chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence. L'absence de moyens de sécurisation du serveur de l'entreprise est susceptible de constituer une faute donnant lieu à responsabilité.

Si un collaborateur de l'entreprise venait à introduire un virus sur le serveur de l'entreprise et si le système informatique de clients ou partenaires venait à être infecté par un virus émanant de ce serveur, ces derniers pourraient engager la responsabilité pénale du salarié mais aussi la responsabilité civile de l'employeur qui est responsable des dommages causés par ses collaborateurs.

Les contacts

CRCI Picardie
Vincent Becquet
Documentaliste
Téléphone : 03.22.82.80.57
Télécopie : 03.22.82.80.65
Mél : v.becquet@picardie.cci.fr

CCI Aisne
Sara Jankovsky
Chargée de mission TIC
Téléphone : 03.23.06.02.08
Télécopie : 03.22.06.02.30
Mél : s.jankovsky@aisne.cci.fr

CCI Oise
Mathieu Callais
Chargé de mission
Téléphone : 03.44.79.80.45
Télécopie : 03.44.79.80.20
Mél : callais@cci-oise.fr

CCI Péronne et CCI Abbeville-Picardie Maritime
Jean-Louis Rayez
Responsable informatique
Téléphone : 03.22.73.36.36
Télécopie : 03.22.73.36.37
Mél : jl.rayez@peronne.cci.fr