Security Expert
EXENOS

Responsabilités en matière de sécurité informatique

Sommaire

- ✓ Présentation Exenos
- ✓ Introduction
- ✓ Les responsabilités
  - ✓ de l'entreprise, du dirigeant, du responsable informatique
  - ✓ des salariés
  - ✓ des contrevenants
- ✓ Comment se protéger ?
- ✓ Conclusion

Présentation EXENOS

- ✓ Société spécialisée en sécurité informatique
- ✓ Conseil, Audit, Formation
- ✓ Les points forts :
  - ✓ haut niveau de compétence en sécurité
  - ✓ impartialité = pas de revente de matériel ou logiciel
  - ✓ qualité des relations clients = volonté d'accompagner les clients sur les problématiques sécurité
- ✓ www.exenos.com

Introduction

La tendance

- ✓ Volonté des tribunaux de responsabiliser de plus en plus l'entreprise et donc ses responsables sur les problèmes de sécurité
- ✓ On ne s'intéresse pas seulement à la faute mais aussi aux personnes qui auraient pu l'empêcher

Exemple

Juin 2003 :

- ✓ Un employé est condamné par le tribunal de Marseille pour avoir mis en ligne et administré un site web à caractère diffamatoire depuis son poste de travail
- ✓ Son entreprise est, elle aussi, condamnée car la faute a été commise pendant l'exercice de ses fonctions et donc sous la responsabilité de l'entreprise

Les Responsabilités
1. L'entreprise

Qui est réellement concerné ?

- ✓ L'entreprise est représentée par son ou ses dirigeants
- ✓ Par délégation, le responsable informatique ou responsable sécurité peut être mis en cause (faute professionnelle)

Responsabilité de l'entreprise?

- La responsabilité peut être engagée :
  - si des manquements techniques ou organisationnels ont mis en péril la pérennité de l'entreprise
  - si la loi sur la protection de la vie privée est enfreinte
- L'entreprise est responsable civilement par rapport aux agissements des ses employés pendant les heures de travail (art 1383 du code civil)
- Dans certains cas, en cas de propagation de virus ou intrusion à partir du réseau de l'entreprise

Données nominatives

- loi du 6 janvier 1978 prévoit que les entreprises qui hébergent des données nominatives « s'engagent à protéger ces données contre toute déformation, communication à des tiers non autorisés »
  - responsabilité pénale: 300 000 € d'amende, 5 ans prison
- la directive du 24 oct 1995 complète ces obligations:
  - l'entreprise doit mettre en oeuvre les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel
  - tient compte de l'état de l'art de la sécurité et des coûts de mise en oeuvre pour l'entreprise
- cette loi peut être utilisée par des employés, clients ou internautes si un préjudice de la sorte est constaté

Responsabilité civile

- Art 1382, 1383, 1384 alinéa 5 du code civil peuvent être appliqués
  - Absence de moyens de sécurisation susceptibles de constituer une faute civile (art 1383) = faute par abstention
  - Le chef d'entreprise est responsable des dommages causés par leurs préposés dans les fonctions auxquelles ils les ont employés (art 1384 alinéa 5)
    - la jurisprudence considère que si le salarié agit pendant son temps de travail, sur son lieu de travail, il exerce sa fonction
  - l'employeur peut ensuite se retourner contre le fautif mais sans certitude d'avoir gain de cause

Les Responsabilités

2. Les salariés

De quoi sont-ils responsables ?

- ✓ Du bon usage de l'outils informatique mis à leur disposition
  - ✓ respect de la charte informatique si elle existe
  - ✓ usage de l'outils non frauduleux
- ✓ La responsabilité pénale de l'employé est engagée en cas de détournement des moyens informatiques (téléchargement illégal, installation de logiciels sans licence, intrusion ou altération du système) = Loi Godfrain
- ✓ Diffusion d'un secret de fabrique
- ✓ Diffusion de fausses informations ou informations diffamatoires

Les Responsabilités

3. Les contrevenants

Pour quels actes ?

- ✓ Contrevenant = personne qui commet des actes illégaux (particulier ou salarié dans l'exercice de ses fonctions)
- ✓ Quels actes sont condamnés ?
  - ✓ diffusion de vers, virus, chevaux de Troie, bombes logiques
  - ✓ Intrusion ou accès sur un système, serveur, une machine, un réseau sans autorisation
  - ✓ Introduction frauduleuse de données ou modification frauduleuse de données
- ✓ Loi Godfrain prévoit jusqu'à 50 000 € d'amende et 3 ans de prison

Comment se protéger ?

La charte informatique

- ✓ Doit être intégrée au règlement intérieur, signée par les employés avec le contrat de travail
- ✓ Elle précise ce que l'employé peut faire ou ne pas faire avec l'outil informatique mis à sa disposition
- ✓ Déresponsabilise l'entreprise en cas de manquement à un article de la charte
- ✓ Peut être une clause du contrat de travail pour les administrateurs réseau, responsables informatique,...

Cyber-surveillance ?

- ✓ les règles à respecter :
  - ✓ principe de transparence = les salariés doivent être avertis de façon officielle des éléments de logs, limitations,...
  - ✓ principe de discussion collective = mettre les représentants du personnel dans la discussion en cas d'intégration d'éléments de sécurité
  - ✓ principe de proportionnalité = mettre en place des restrictions proportionnelles au but recherché
- ✓ un minimum de surveillance est un devoir pour veiller à la sécurité de l'entreprise (divulgation de secret de fabrique ...)

Cybersurveillance ?

- ✓ Rôle de l'équipe informatique :
  - ✓ l'administrateur doit pouvoir avoir accès aux données personnelles mais se doit de garder la confidentialité des informations y compris vis-à-vis de la direction (CNIL)
- ✓ La nouvelle loi sur la protection des personnes physiques à l'égard des traitements de données à caractère personnel prévoit la nomination d'un correspondant dans l'entreprise chargé du respect de cette loi
- ✓ Attention au respect de la vie privée (arrêt Nikon du 02/10/2001)

Les moyens reconnus

- Pour ne pas être accusée de négligence, l'entreprise doit avoir pris des dispositions dans les domaines:
  - sécurité du système d'informations : alarmes, climatisation, sauvegardes, procédures de reprise, maintenance régulière
  - lutte contre la malveillance interne ou externe : politique de sécurité, mot de passe, contrôle d'accès, firewall, anti-virus

Les moyens recommandés

- ✓ Audit de sécurité : il fait valider par une société externe les moyens et procédures en place
- ✓ Procédures de gestion des moyens (sauvegardes, mise à jour, maintenance, ...)
- ✓ Assurances : couvrent les pertes financières possibles

Actualité juridique

- ✓ Projet de réforme du droit des fichiers : nomination d'un responsable des données personnelles
- ✓ Loi sur l'économie numérique
  - ✓ responsabilité des hébergeurs
  - ✓ responsabilité des vendeurs e-commerce
  - ✓ spam
  - ✓ signature numérique
- ✓ Lutte contre la cyber-criminalité
  - ✓ aggravement des peines Loi Godfrain
  - ✓ précision sur la nature des actes répréhensibles (diffusion intentionnelle de virus,...)

Conclusion