



Le guide pratique du chef d'entreprise face au risque numérique

Version du 31 mars 2010



Préface

de Brice HORTEFEUX

Ministre de l'intérieur,
de l'outre-mer
et des collectivités territoriales

Parce qu'il constitue un des gisements essentiels de croissance durable pour notre économie, l'espace numérique représente aujourd'hui un enjeu fondamental pour la sécurité nationale. Les nouvelles technologies de l'information doivent être à la fois protégées et maîtrisées sous peine d'être infiltrées ou dévoyées et de devenir ainsi des menaces à la stabilité globale.

Parce que le capital d'une entreprise repose autant sur la sécurité de l'outil de production que sur la sécurité de son patrimoine d'information, l'entrepreneur doit bien discerner les risques et les opportunités au sein d'un univers numérique complexe et changeant. C'est au prix d'une vigilance permanente qu'il pourra faire grandir son entreprise en investissant les espaces numériques sans pour autant la rendre plus vulnérable.

Dans ce combat déterminant, l'entrepreneur reçoit le soutien sans faille de l'Etat qui se mobilise activement pour préserver la santé et la sécurité du tissu économique national. C'est dans cet esprit que la compétence de l'Agence nationale de sécurité des systèmes d'information (ANSSI), initialement réservée aux administrations et aux secteurs d'activité vitale, a été étendue aux PME et PMI.

Dans cet ouvrage conçu au terme d'une réflexion commune d'acteurs publics et privés, l'entrepreneur pourra prendre connaissance des risques que court son entreprise dans le domaine numérique, mais aussi découvrir les solutions qui sont à sa disposition. Sensibilisé aux dangers que fait encourir à son entreprise chaque faille dans le dispositif de sécurité numérique, il pourra élever son niveau de vigilance à la hauteur du niveau de la menace.

La connaissance permettant la vigilance, ce guide contribuera, j'en suis certain, à la sécurité globale dans le domaine de l'économie numérique.

Brice HORTEFEUX
Ministre de l'intérieur
de l'outre-mer
et des collectivités territoriales

Les raisons d'une nouvelle édition

Une mise à jour de la précédente édition s'avérait indispensable afin d'exposer les adaptations du dispositif français destiné à faire face à la menace cybercriminelle.

Ainsi, suivant les prescriptions du livre blanc pour la défense et la sécurité nationale, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est venue coiffer le dispositif national pour une plus grande efficacité.

De nouvelles fiches, toujours aussi opérationnelles, ont été ajoutées pour venir contrer des menaces grandissantes pour les entreprises ou pour adopter une posture permanente de vigilance.

L'évolution régulière de cet outil est une garantie de sa pertinence.

Chef d'escadron Dominique SCHOENHER
Commissaire général délégué
Forum International sur la Cybercriminalité

Pourquoi un guide de bonnes pratiques à destination des PME-PMI?

Dans un contexte de mondialisation et de développement des technologies numériques, la dépendance des entreprises à l'égard des technologies de l'information et de la communication (TIC) présente des risques potentiels que savent exploiter des délinquants et des criminels avertis et de plus en plus souvent organisés.

Résolument inscrite dans une démarche d'intelligence économique et de protection des patrimoines matériels et immatériels de l'entreprise, la quatrième édition du FIC mettra l'accent sur les axes de travail qu'il appartient aux autorités de suivre pour mener au mieux la protection des personnes et des biens dans le cyberspace et permettre ainsi tant le développement de l'économie numérique, le secteur le plus dynamique de l'économie mondiale, que le développement et la protection des PME-PMI.

Les différents ateliers proposés permettront notamment de :

- Contribuer à une lutte efficace contre la criminalité liée aux technologies numériques (pédophilie, terrorisme, blanchiment d'argent, contrefaçon...) en utilisant la détection, l'investigation et la poursuite, tant au niveau national qu'international, et en prévoyant des dispositions matérielles en vue d'une coopération internationale rapide et fiable.
- Intensifier la coopération entre les Etats liés à la Convention du Conseil de l'Europe d'avril 2001, les pays membres de l'UE et les candidats à l'accession.
- Structurer un partenariat sur une base transnationale, avec les entreprises et plus généralement avec les acteurs socio-économiques impliqués au quotidien dans le développement de l'économie de la connaissance et les acteurs concrets de la mutation de l'économie européenne.

L'actualisation et l'évolution du guide pratique à destination des chefs de PME-PMI lui permet de conserver toute sa pertinence et son attrait pour les décideurs et cadres en entreprise dans les services, les administrations, et les collectivités territoriales.

Colonel Régis Fohrer
Commissaire général
Forum International sur la Cybercriminalité

Remerciements
aux participants
des comités
scientifiques
et de rédaction.

*Au nom du Forum International
sur la Cybercriminalité, j'adresse
mes meilleurs remerciements
à l'ensemble des membres
et partenaires pour la qualité
des réflexions qui ont permis
de donner toute la pertinence
à ce guide, ainsi qu'au
comité de rédaction et de
relecture pour l'important travail
de synthèse et d'écriture fourni.*

Colonel Régis Fohrer

Commissaire général
Forum International sur la Cybercriminalité

Comité de rédaction pour la mise à jour 2010

Rédaction et coordination :

M. Eric LESTRINGUEZ,
Lieutenant-colonel de réserve, Gendarmerie Nationale
Correspondant IE AA-IHEDN (AR15)

Avec le concours de :

M. David CASSEL,
Enquêteur en technologie numérique, chef de la cellule
d'investigations criminelles d'Arras

Mme Nathalie FAVIER,
Commandant de Police - Chargée de Mission Coordination
au Centre Opérationnel de Sécurité des Systèmes
d'Informations (ANSSI)

M. Daniel GUINIER,
OSIA- Docteur ès Sciences, CISSP, ISSMP, ISSAP, MBCI,
Expert judiciaire honoraire, Expert devant la Cour Pénale
internationale, Lieutenant-colonel (RC), Gendarmerie Nationale.

M. Pascal LOINTIER,
Président du Club de la Sécurité de l'Information
Français, CLUSIF, conseiller sécurité de l'information,
CHARTIS

M. Jean-Paul PINTE,
Docteur en information scientifique et technique, maître
de conférences, expert en veille et intelligence compétitive
au sein du laboratoire d'ingénierie pédagogique,
Université Catholique de Lille
Lieutenant-colonel (RC), Gendarmerie Nationale

Mme Blandine POIDEVIN,
Avocate, Barreau de Lille et de Paris - Intervenante en
droit des nouvelles technologies à la faculté de Lille 2
Conférencière en France et à l'étranger sur les thématiques
IE et TIC - Tiers aviseur du CMAP (centre de médiation
et d'arbitrage de Paris) - Inscrite sur le liste des Expert
en Nouvelles technologies à la commission européenne.

Chef d'escadron Dominique SCHOENHER
Commissaire général délégué
Forum International sur la Cybercriminalité

Pour les illustrations

M. Dominique DAGUE,
Commissaire de Police,
Préfecture de Police de Paris

Liste des participants au comité scientifique de la première édition

INSTITUTIONS

M. Alain JUILLET,
Haut responsable chargé de l'intelligence
économique, SGDN

M. Cyril BOUYEURE,
Coordonnateur ministériel à l'Intelligence
Economique, MEIE

M. Philippe CLERC,
Directeur de l'Intelligence Economique et
des TIC, Assemblée des chambres fran-
çaises de commerce et d'industrie

M. Gwendal LE GRAND,
Chef du service de l'expertise
à la direction des Affaires juridiques, inter-
nationales et de l'expertise, CNIL

M. Pascal LOINTIER,
Président du Club de la Sécurité de
l'Information Français, CLUSIF, conseiller
sécurité de l'information, CHARTIS

M. Gérard PARDINI,
Chef du département Sécurité économique
et gestion de crise, Institut National des
Hautes Etudes de Sécurité.

M. Jean-Philippe VACHERON,
Ingénieur d'études, CRCI-ARIST Nord-Pas
de Calais, animateur de l'action «sécurité
des systèmes d'information»

M. Philippe VANDENBERGHE,
Chargé de mission défense et protection
civile, Direction Générale des Services de
la Ville de LILLE

UNIVERSITAIRES ET PROFESSION DU DROIT

M. Eric CAPRIOLI,
Avocat à la cour de Paris,
Associé du Cabinet Caprioli & Associés,
Docteur en droit

M. Jean Jacques LAVENUE,
Laboratoire IREENAT, Université de Lille 2

M. Jean-Paul PINTE,
Docteur en information scientifique et
technique, maître de conférences, expert
en veille et intelligence compétitive au sein
du laboratoire d'ingénierie pédagogique,
Université Catholique de Lille
Lieutenant-colonel (RC), Gendarmerie
Nationale

Mme Blandine POIDEVIN,
Avocate, Barreau de Lille et de Paris
- Intervenante en droit des nouvelles
technologies à la faculté de Lille II Confé-
rencière en France et à l'étranger sur les
thématiques IE et TIC - Tiers aviseur du
CMAP (centre de médiation et d'arbitrage
de Paris) - Inscrite sur le liste des Expert
en Nouvelles technologies à la commission
européenne.

Mme Myriam QUÉMÉNER,
Magistrat, Parquet général de la Cour
d'appel de Versailles, auteur de
«Cybermenaces, entreprises, internautes»
et co-auteur de «Cybercriminalité, défi
mondial»

M. Christophe ROQUILLY,
Professeur de droit, directeur du centre
de recherche LegalEdhec - performance
juridique, EDHEC Business School

FORCES DE SÉCU- RITÉ FRANÇAISES ET ÉTRANGÈRES

M. Luc BEIRENS,
Commissaire divisionnaire, Chef de la
Federal Computer Criminal Unit (FCCU),
Belgique

M. David CASSEL,
Enquêteur en technologie numérique, chef
de la cellule d'investigations criminelles
d'Arras

Colonel Joël FERRY,
Commandant de la Section de Recherche
de Versailles

M. Eric LESTRINGUEZ,
Lieutenant-colonel de réserve, Gendarme-
rie Nationale
Correspondant IE AA-IHEDN (AR15)

M. Alain PERMINGEAT,
Chef de la division lutte contre la
cybercriminalité au Service Technique de
Recherche Judiciaire et de Documentation
de la Gendarmerie Nationale

ENTREPRISES

M. Patrick DESCHAMPS,
GEN'ETIQ

M. Daniel GUINIER,
OSIA- Docteur ès Sciences, CISSP,
ISSMP, ISSAP, MBCI, Expert judiciaire
honoraire, Expert devant la Cour Pénale
internationale, Lieutenant-colonel (RC),
Gendarmerie Nationale.

M. Olivier VARLET,
Directeur du Pôle MAUD

REMERCIEMENTS AUX RÉDACTEURS

Colonel Régis FOHRER,
Forum International sur la Cybercriminalité

M. Pascal LOINTIER,
Président du Club de la Sécurité de l'Information Français, CLUSIF, conseiller sécurité de l'information, CHARTIS

• Groupe « *Le chef d'entreprise face au risque numérique - Risques identifiés et solutions proposées en 12 études de cas* »

Rédigé par M. Eric LESTRINGUEZ,
Lieutenant-colonel de réserve, Gendarmerie Nationale
Correspondant IE AA-IHEDN (AR15)
avec la participation de

- M. Eric CAPRIOLI,
Avocat à la cour de Paris,
Associé du Cabinet Caprioli & Associés, Docteur en droit
- M. David CASSEL,
Enquêteur en technologie numérique, chef de la cellule d'investigations criminelles d'Arras
- M. Daniel GUINIER,
OSIA- Docteur ès Sciences, CISSP, ISSMP, ISSAP, MBCI,
Expert judiciaire honoraire, Expert devant la Cour Pénale internationale, Lieutenant-colonel (RC), Gendarmerie Nationale.
- Mme Noëlle JEAN-PIERRE,
Cabinet CAPRIOLI & Associés, Juriste TIC
- Mme Blandine POIDEVIN,
Avocate, Barreau de Lille et de Paris - Intervenante en droit des nouvelles technologies à la faculté de Lille 2
Conférencière en France et à l'étranger sur les thématiques IE et TIC - Tiers aviseur du CMAP (centre de médiation et d'arbitrage de Paris) - Inscrire sur le liste des Expert en Nouvelles technologies à la commission européenne.
- M. Christophe ROQUILLY,
Professeur de droit, directeur du centre de recherche LegalEdhec - performance juridique, EDHEC Business School
- M. Dominique DAGUE
Commissaire de Police, illustrations humoristiques

• Groupe Etat des lieux « *Le chef d'entreprise face au risque numérique* » - recommandations « *approche institutionnelle* »

Rédigé par M. Jean-Paul PINTE,
Docteur en information scientifique et technique, maître de conférences, expert en veille et intelligence compétitive au sein du laboratoire d'ingénierie pédagogique, Université Catholique de Lille
Lieutenant-colonel (RC), Gendarmerie Nationale
avec la participation de

- Mme Nathalie FAVIER, Jean Philippe CHAPUT et Franck VEYSSET
SGDSN / ANSSI
- MM. Gabriel GOLDSTEIN et Pierre CROS,
Service de coordination à l'Intelligence économique, Bureau Dépendances Stratégiques, Ministère de l'Economie, de l'Industrie et de l'Emploi, Ministère du Budget, des Comptes Publics et de la Fonction Publique.
- M. Gwendal LE GRAND,
Chef du service de l'expertise à la direction des Affaires juridiques, internationales et de l'expertise, CNIL
- M. Gérard PARDINI,
Chef du département Risques et Crises de l'Institut National des Hautes Etudes de la Sécurité et de la Justice.

Les « avis d'expert » ont été rédigés par SPIE Communications et notamment :

- M. Arnaud FEIST
Consultant Direction Régionale Nord Est
- M. Yohan CAPLIER
Consultant Direction Régionale Nord Est
- M. David DELANNOY
Consultant Direction Régionale Nord Est
- M. Christian MEGARD
Marketing, Offre IRM (Informatique / Réseaux / Mobilité)
- M. Julien HOPPENOT
Marketing, responsable offre sécurité

Cet ouvrage
a pu être réalisé
grâce à la collaboration
active et engagée de

• Les enseignants chercheurs :



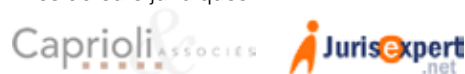
• Les acteurs de la sécurité :



• Les institutions :



• Les acteurs juridiques :



• Partenaires privés :



SOMMAIRE

PREFACE
de Brice HORTEFEUX, Ministre de l'Intérieur,
de l'outre-mer et des collectivités territoriales P 3

AVANT-PROPOS
du Chef d'Escadron Dominique Schoenher,
et du Colonel Régis FOHRER P 4

REMERCIEMENTS participants aux comités scientifiques P 6

PRÉSENTATION des partenaires P 9

DÉFINITIONS de la cybercriminalité en entreprise
et introduction P 11

CHAPITRE 1

Le chef d'entreprise face au risque numérique

Risques identifiés et solutions
proposées en 12 études de cas P 13

- Le comportement à risques du salarié P 14
- La fraude financière via la comptabilité P 16
- La divulgation de savoir-faire P 18
- Les téléchargements illicites et intrusion via le réseau sans fil P 20
- La défaillance de sauvegarde des données P 22
- Le vol d'ordinateur portable ou de PDA P 24
- Le sabotage interne d'une base de données P 26
- Le dysfonctionnement ou l'altération par programmes malveillants P 28
- La diffamation par courrier électronique P 30
- La défiguration de site web P 32
- Les Botnets P 34
- Le Cybersquatting P 36
- Les 5 réflexes messagerie P 38
- Les 5 réflexes Hotspot Wifi P 40

CHAPITRE 2

Etat des lieux « Le chef d'entreprise face au risque numérique »

Recommandations
des institutions P 46

Les entreprises
et la cybercriminalité P 47
- Un enjeu de coopération internationale P 48
- Analyse de la menace - Bilan P 48

La loi protège votre entreprise P 51
- Première réponse de l'Etat aux incidences
concrètes sur la vie quotidienne : la loi P 51
- Réponses françaises à la cybercriminalité P 52

Des services spécialisés
pour aider les entreprises P 53
- La création de services spécialisés
au sein de l'Etat P 53
- De nombreuses actions de prévention
et de sensibilisation des acteurs économiques P 56

Perspectives pour l'entreprise P 62
- Les Assises du numérique P 62
- Plan de continuité :
Essentiel à la protection d'activité P 62
- Annexes P 65

POSTFACE P 70

WEBOGRAPHIE P 72

LES SOUTIENS DE NOS PARTENAIRES P 74

Définition de la Cybercriminalité

Définition du Colonel de gendarmerie,
Commissaire général Régis FOHRER
La criminalité du XXI^{ème} siècle.

Faute d'une définition communément admise, la définition pertinente du terme « cybercriminalité » donnée par la communication n° 267 du 22 mai 2007 de la Commission européenne « Vers une politique générale en matière de lutte contre la cybercriminalité » a été retenue pour préparer les éditions successives du FIC. Aux fins de ce texte, « cybercriminalité » s'entend des « infractions pénales commises à l'aide des réseaux de communication électroniques et de systèmes d'information ou contre ces réseaux et systèmes ».

Ce terme englobe trois catégories d'activités criminelles.

- La première concerne les formes traditionnelles de criminalité, comme les fraudes ou les falsifications;
- La seconde concerne les infractions liées aux contenus illicites par voie électronique (violence sexuelle contre les enfants, incitation à la haine raciale...);
- La dernière connaît des infractions propres aux réseaux électroniques (attaques visant les systèmes d'information, déni de service, piratage...).

Ainsi la cybercriminalité constitue dans un monde globalisé l'une des nouvelles formes de criminalité et de délinquance transnationales dont les conséquences peuvent être particulièrement graves pour les citoyens, les personnes vulnérables et le secteur de l'économie de toutes les nations de la planète.

Quatre grands types de menaces concernent particulièrement les entreprises :

- Les vols de supports et de données;
- Les intrusions dans les réseaux;
- Les interceptions de communications ou de flux de données;
- La manipulation des employés et des partenaires, cette dernière menace étant plus connue sous le terme de « social engineering ».

Glossaire :

MAC: media access control
NAC: network access control
PDA: personnel digital assistant
SSID: service set identifier
RFID: radio frequency identification
SSL: secure sockets layer
USB: universal serial bus
WEP: wired equivalent privacy
Wi-Fi: wireless fidelity
WLAN: wireless local area network
WMAN: wireless metropolitan network
WPA: wifi protected access
WPAN: wireless personal area network

Introduction

par Pascal LOINTIER,
Président du Club de la Sécurité
de l'Information Français, CLUSIF
conseiller sécurité de l'information,
CHARTIS

Début des années 80, un grand constructeur américain lance un nouveau modèle d'ordinateur : le PC, pour Personal Computer. Ordinateur individuel... ce qui signifiait qu'on envisageait peut-être un emploi professionnel dans une PME ! Manifestement les choses ont évolué autrement et aujourd'hui non seulement la micro-informatique est complètement intégrée dans les systèmes d'information des entreprises de toutes tailles mais encore, l'individu est devenu à la fois un internaute et un citoyen muni d'une informatique embarquée : cartes de crédit, téléphones GSM avec fonctions d'assistant (PDA), navigateurs GPS...

Cette dépendance est une bonne chose car d'une part, elle accroît la productivité, fluidifie les échanges et d'autre part, facilite la sécurité des données au format électronique en terme de disponibilité et d'intégrité dans le temps. En effet, le rapport « France numérique 2012 », présenté par le gouvernement en octobre 2008 détaille nombre des avantages pour une entreprise quant à l'utilisation des technologies de l'information et de la communication (TIC) : « l'économie numérique est le principal facteur de gain de compétitivité des économies développées ».

Ainsi, l'informatique s'est installée un peu partout dans l'entreprise. Historiquement il s'agissait de l'informatique de management (comptabilité, etc.) puis les traitements externalisés (infogérance). Plus récemment, l'informatique industrielle s'est standardisée (TCP/IP, systèmes d'exploitation, etc.) et la téléphonie est devenue la voix sur IP (VoIP). Dernière innovation : les services généraux (climatisation, ascenseurs, caméras de surveillance, serrures) utilisent des équipements dont on peut prendre le contrôle à distance... Côté sécurité, les outils de sauvegarde, la délocalisation du lieu de conservation des dites sauvegardes permettent aujourd'hui, à moindre coût, d'organiser la disponibilité des données, c'est-à-dire, la pérennité de leur accès et de leur usage quelle que soit, ou presque..., la nature du dommage informatique.

Le bon fonctionnement au quotidien du système informatique et le gain de productivité générés par un traitement numérique ne doivent pas faire oublier que la menace est « polymorphe » : les causes d'un arrêt ou d'une dégradation du fonctionnement du système sont potentiellement très variées. Classiquement, on peut classer les causes en deux grandes catégories : les événements accidentels et les actes de malveillance. Les accidents peuvent être divisés en deux origines, naturelles ou humaines (sans digression philosophique...) où dans le premier cas on considère des événements tels que les incendies, dégâts des eaux, perturbations électromagnétiques du fait de la nature ou d'une activité industrielle. Et dans le second cas, les erreurs de programmation, les erreurs de manipulation ou d'exploitation informatique.

Les malveillances où on pourrait distinguer le fait de programmes automatiques, virus, botnets, etc. où l'entreprise devient victime sans pour autant avoir été spécifiquement ciblée ; et la malveillance par l'agissement direct d'un individu. Pour cette dernière, et même si on médiatise beaucoup (trop) l'Internet et les hackers, les auteurs ou leurs actions les plus dommageables restent des employés de l'entreprise car leurs motivations sont les plus fortes et leur connaissance des faiblesses de sécurité souvent meilleure.

Cette variété des origines d'un arrêt du système et l'évolution des architectures informatiques, opportunités de nouvelles expositions aux malveillances, notamment, ne doivent certainement pas être interprétées comme un frein à l'emploi des TIC. Il faut garder à l'esprit que toute technologie (et pas seulement informatique) comporte intrinsèquement un risque et un emploi malveillant spécifiques. L'automobile « coûte » cher en terme de dommages corporels et matériels et la bande à Bonnot a pour la première fois utilisé le véhicule lors d'attaques de banques...

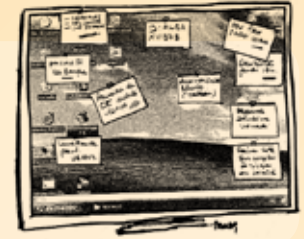
Il faut donc accueillir les nouvelles technologies mais toujours dans une posture de vigilance : savoir comment accroître son activité tout en limitant les nouveaux risques par des moyens raisonnables

C'est bien souvent l'insouciance et/ou la méconnaissance du risque qui permettent ou aggravent les conséquences d'un accident ou d'une malveillance informatique.

Le chef d'entreprise face au risque numérique :

risques identifiés
et solutions proposées
en 12 études de cas.

Le comportement à risques du salarié



- Une entreprise met en place un dispositif technique de gestion des accès basé sur un identifiant/mot de passe sans avoir sensibilisé les salariés aux règles de bon usage.
- Un salarié laisse un post-it sur son écran d'ordinateur avec ses identifiant et mot de passe.
- Un autre salarié utilise l'identifiant et le mot de passe pour accéder à l'ordinateur et en profite pour commettre des actes illicites : envoi de messages diffamatoires ou racistes, téléchargement de fichiers protégés par le droit d'auteur, etc...
- La personne physique ou morale subissant un préjudice dépose plainte contre l'entreprise et/ou contre l'expéditeur du message.

Impacts judiciaires

L'identifiant et le mot de passe servent à créer une présomption sur l'utilisateur des outils. Ainsi, si le salarié ne respecte pas la procédure mise en place dans l'entreprise ou s'il ne peut apporter la preuve que ce ne peut matériellement être lui, sa responsabilité pourra être retenue.

Gestion des accès et responsabilité de l'employeur - L'employeur sera tenu pour responsable des actes illicites commis sur le fondement de la responsabilité des commettants du fait de leurs préposés vis à vis des tiers (art. 1384 du Code civil).

Usurpation d'identité
En matière pénale : L'usurpation d'identité n'est pas un délit pénal en soi, mais seulement au sens de l'art. 434-23 du Code pénal. Une proposition de loi envisage toutefois d'ajouter un art. 323-8 au Code pénal concernant l'usurpation d'identité numérique avec une peine d'un an d'emprisonnement et de 15 000 € d'amende.

En matière civile : La responsabilité civile édictée par l'art. 1382 du Code civil, est applicable dès qu'il y a une faute, un préjudice subi par la victime et un lien de causalité entre cette faute et ce préjudice.

Définition :

L'usurpation d'identité correspond à l'emprunt temporaire ou définitif de l'identité d'une personne existante, par appropriation des identifiants de cette dernière, pouvant constituer un délit.

Impacts managériaux et humains

Ambiance délétère au sein de l'entreprise. Saisine des prud'hommes pour faute du salarié négligeant peu envisageable dans ces circonstances.

Le salarié victime des agissements ainsi que son employeur sont amenés à porter plainte contre X.

Impacts financiers

Frais de procédure et condamnation possible de l'entreprise au civil en cas de dommage causé à un tiers.

Impacts sur l'image

Répercussion possible sur l'image de l'entreprise en cas de contenu illicite ou diffamant.

Préconisations

Mettre en place et faire appliquer une politique efficace d'authentification et de gestion des accès, avec la participation des instances représentatives du personnel. Ces dispositions feront partie de la charte d'utilisation des moyens informatiques, et en tout cas devront être adossées au règlement intérieur de l'entreprise. Tous les employés devront être sensibilisés à cette nécessité et avertis des sanctions encourues.

LES POINTS CLES A RETENIR

L'authentification est une fonctionnalité de sécurité essentielle au contrôle d'accès. Les accès autorisés à l'information et aux ressources doivent être fonction du ou des rôles de chacun. Il est également nécessaire d'alerter les salariés sur les responsabilités découlant de l'utilisation de leurs identifiants et de les informer sur la procédure qu'ils doivent mettre en place en cas de perte de leur mot de passe ou identifiant.

AVIS D'EXPERT :

Les entreprises prennent généralement toutes les protections nécessaires à la sécurisation des accès extérieurs mais oublient bien souvent la menace interne. En effet, la confiance faite à l'employé présente une faille de sécurité considérable : transmission volontaire ou non de mot de passe, non verrouillage d'une session,

introduction de virus via l'utilisation de ressources externes à l'entreprise (clé USB, connexion privée, disque dur externe...) Toutes ces menaces nécessitent une politique de sécurité interne qui passe par la sensibilisation (charte...) et l'accompagnement des utilisateurs ainsi qu'un contrôle performant des accès et des activités.

La fraude financière via la comptabilité

- *Le chef-comptable, en poste depuis de nombreuses années, vient d'être mis en arrêt longue durée suite à un accident automobile.*
- *Un intérimaire est embauché d'autant plus rapidement que le bilan doit être clôturé prochainement.*
- *A l'occasion de rapprochements bancaires et stocks, ce remplaçant détecte une différence entre les factures payées à un fournisseur et les livraisons effectives de matériaux.*
- *En collusion avec un employé du fournisseur, le chef-comptable a détourné plusieurs centaines de milliers d'euros en moins de deux ans. Il apparaissait comme consciencieux, extrêmement zélé et d'ailleurs, ne prenait quasiment pas de congés.*
- *Une procédure judiciaire a été lancée mais la récupération des actifs détournés s'avère délicate. Ces derniers ayant été consommés ou investis dans des biens immobiliers dont la liquidation va prendre des mois.*

Impacts judiciaires

Le licenciement du salarié ne peut se faire tant que son contrat se trouve suspendu sauf faute grave ou lourde qui ne pourra être démontrée que par une expertise comptable ou une enquête pénale. Elles devront déterminer s'il a bénéficié de complicité. Une procédure d'expertise devra être lancée afin de déterminer le préjudice exact subi par l'entreprise. Des conséquences fiscales sont également envisageables du fait de l'absence de fiabilité des documents comptables.



Définition :

La fraude financière est un acte illicite délibéré, réalisé par des moyens plus ou moins subtils, avec la volonté de tromper dans le but de s'approprier un avantage. Elle peut prendre diverses formes qui nécessitent ou non des complicités, et conduit à un préjudice pour la victime.

Impacts managériaux et humains

Détection délicate a priori car tout le monde se connaissait dans l'entreprise et la suspicion d'une malversation semblait inimaginable. Dès la présomption fondée, le chef d'entreprise doit agir rapidement et discrètement en supposant l'existence de collusions internes.

Impacts financiers

Effets multiples : perte des actifs détournés et difficultés à venir pour récupérer les fonds détournés d'autant plus que la PME ne s'était pas assurée contre les fraudes financières.

Impacts sur l'image

Impact sur le sérieux de l'entreprise (rigueur dans les contrôles) et crainte de difficultés financières futures qui pourraient remettre en cause des contrats clients, voire d'autres fournisseurs...

Préconisations

Mettre en place des contrôles informatiques et des procédures : double ordonnancement, séparation des circuits paiements et achats, limitation de seuils, audit et inventaires aperiodiques.

LES POINTS CLES A RETENIR

Les mécanismes de détournements sont le plus souvent très simples à comprendre et parfois stupides de la part du commettant car la détection n'est qu'une affaire de temps (cf fraude dite « en cavalerie* »). Etudier des scénarios techniquement possibles (c'est à dire sans présumer de la bonne foi des salariés) et mettre en place des indicateurs qui permettront la détection des situations atypiques.

(*) : La fraude financière dite « en cavalerie » peut prendre diverses formes. L'une consiste à créditer artificiellement un compte par des chèques croisés de montants croissants pour maintenir la confiance, ce qui nécessite des complicités successives, sinon des complaisances.

AVIS D'EXPERT :

La traçabilité des activités et des interventions du personnel joue un rôle primordial pour la prévention des fraudes. En effet, les fraudes sont de plus en plus informatisées (création d'un compte fictif, modification de RIB...). Il est donc important de sauve-

garder l'historique des opérations critiques. Il existe par ailleurs une offre commerciale de logiciels aidant à la détection de ces atypismes dans les opérations comptables ou dans l'emploi des ressources.

La divulgation de savoir-faire



- *Un stagiaire, s'appuyant sur une technique « d'ingénierie sociale », l'appel à la compassion, a récupéré les droits d'accès de son tuteur de stage pour « faciliter son travail dans l'entreprise ».*
- *Ces droits lui permettent de détourner des informations confidentielles d'un autre service de l'entreprise, à savoir du laboratoire de recherche qui était sur le point de déposer un brevet.*
- *Une fois le stage terminé, il va même obtenir un prix d'une prestigieuse école européenne.*
- *Il sera engagé par une société concurrente étrangère qui développera le produit et déposera plusieurs brevets voisins.*

Impacts judiciaires

En matière pénale : Les faits peuvent être qualifiés d'abus de confiance au sens de l'art. 314-1 du Code pénal. Cette incrimination peut s'appliquer au collaborateur qui utilise frauduleusement les outils ou informations mis à sa disposition pour extraire des informations confidentielles, mais aussi d'atteinte au système de traitement automatisé de données (STAD) (Art. 323-1). Si ces informations présentent un caractère de secret de la défense nationale, le cas est traité à l'art. 413-9 du Code pénal, tandis que leur livraison à une puissance étrangère est du ressort de l'art. 411-6.

En matière civile : La responsabilité civile de celui qui commet un tel acte se réfère à l'art. 1382 du Code civil en cas de violation de la convention de stage. Enfin, au cas où des éléments relatifs à la vie privée interviennent, l'art. 9 du Code civil, dispose que chacun a droit au respect de sa vie privée. On relèvera peut-être par ailleurs des atteintes au droit de la propriété intellectuelle ou à la politique de confidentialité de l'entreprise.

Définition :

L'ingénierie sociale (en anglais «social engineering»), est une méthode d'exploitation de la crédulité humaine, par pression psychologique ou faisant appel à la compassion, pour disposer d'un bien ou d'informations.

Impacts managériaux et humains

Remise en cause tardive de l'organisation au regard des conséquences. Dévalorisation, voire licenciement, du tuteur de stage. Perte de chiffres d'affaires et de contrats à venir.

Impacts sur l'image

Influence sur l'image de la société causée par la fuite d'information.

Préconisations

Vérifier le contenu de la convention de stage et la rendre tripartite (étudiant, école, entreprise). Vérifier dans l'entreprise l'existence de charte éthique et en expliquer le contenu à chacun. Informer les salariés des risques consécutifs à la diffusion non contrôlée de droits d'accès.

Règles de classification, de marquage des données sensibles et contrôle des accès physiques et logiques (« besoin d'en connaître »). Procédure d'authentification forte pour les informations sensibles (contrôle biométrique ou par carte à puce ou mot de passe dynamique). Récupération et analyse rapides des traces d'accès horodatées, comme moyen de preuve.

LES POINTS CLES A RETENIR

La sensibilisation des personnels est primordiale : préserver les informations sensibles pour l'entreprise, réagir à tout phénomène atypique. L'ingénierie sociale est difficile à prévenir et à détecter car elle s'appuie sur des comportements humains normaux et quotidiens : solliciter une aide, faire état de la gêne occasionnée en l'absence de collaboration, nécessité de réagir dans l'urgence sans avoir le temps d'appliquer les procédures standards, etc...

AVIS D'EXPERT :

La protection des données sensibles et leur non divulgation nécessitent la mise en place d'une politique de sécurité globale dans laquelle devront apparaître 3 types de mesures. L'authentification forte ou la biométrie, une stratégie globale de contrôle de

données qui permettra d'installer les outils nécessaires pour que l'information reste dans l'entreprise, ainsi qu'une solution de gestion et de sauvegarde des logs pour tracer les contrevenants et établir les preuves en cas de fuites.

Les téléchargements illicites et intrusion via le réseau sans fil

- *L'entreprise Z s'est toujours positionnée originalement : historiquement installée dans ses vieux mais prestigieux locaux parisiens conservés comme à l'origine, elle est toujours à la pointe de la technologie.*
- *Ainsi, pour ne pas dénaturer ses bureaux et s'économiser le coût du câblage, elle a doté ses commerciaux d'ordinateurs portables avec une connexion Wi-Fi, les membres de l'équipe de direction ne peuvent plus travailler sans leur nouveau PDA avec une connexion Bluetooth.*
- *La plupart des accès au système d'information local se font via des technologies sans fil.*
- *Un beau matin, le PDG reçoit la visite de représentants de la force publique lui demandant de s'expliquer sur le téléchargement dans son entreprise de plusieurs giga octets de films et de musique piratés.*

Impacts judiciaires

La protection du droit d'auteur et des droits voisins dans la société de l'information relève de la loi n°2006-961 du 1er août 2006 (DADVSI). Il y a obligation pour l'entreprise de veiller à ce que son système d'information ne soit pas utilisé à des fins illicites (Arts. L226-17 du Code pénal, et 1384 al 5 du Code civil), voire à des fins de recel (Art. 321-1 du Code pénal). L'entreprise est responsable du comportement de ses salariés. Elle a l'obligation lors de la mise en place de ces outils d'informer ses salariés des limites d'utilisation et des contrôles possibles (rôle des chartes informatiques ou annexes au règlement intérieur).



Définition :

Les technologies sans fil correspondent aux réseaux sans fil de type :
- personnels (WPAN), tels : Bluetooth, RFID, etc.,
- locaux (WLAN) : Wi-Fi,
- métropolitains (WMAN),
en fonction de la portée.

Impacts managériaux et humains

Il règne dans l'entreprise un climat de suspicion et chaque collaborateur se sent atteint personnellement après avoir été auditionné par les enquêteurs.

Impacts financiers

Les enquêteurs conduisent les constatations de manière à ne pas engendrer un ralentissement dans le fonctionnement de l'entreprise. Pour ce faire, il leur arrive de cloner le(s) disque(s) dur(s) susceptible(s) de détenir la preuve numérique. Ils travaillent alors sur le(s) clone(s) et remettent le(s) disque(s) réel(s) au chef d'entreprise. C'est pourquoi l'entreprise peut être paralysée pendant plusieurs jours, voire plus.

Impacts sur l'image

Un des majors de l'industrie du film et de la musique porte le dossier en justice et l'affaire se trouve relayée par la presse spécialisée.

Préconisations

Masquer le nom du réseau (SSID : service set identifier). Mettre en place un chiffrement de type WEP ou mieux WPA avec une authentification complémentaire par la carte réseau Wi-Fi (adresse physique MAC). Mettre en place une charte informatique, effectuer des contrôles concernant l'intégrité du réseau, vérifier les déclarations CNIL. Dans un autre ordre d'idée, l'usage d'une connexion Wi-Fi libre d'accès dans un hôtel ou sur un lieu public peut présenter un risque d'interception de vos données (messagerie, fichiers téléchargés) si la communication n'est pas sécurisée. Il faut que les échanges entre votre ordinateur et l'entreprise soient effectués en mode chiffré (WEP puis SSL pour la partie Internet par exemple).

LES POINTS CLES A RETENIR

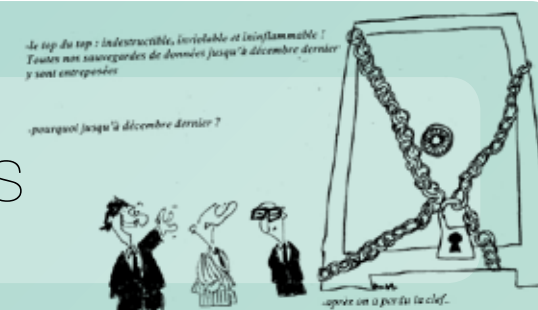
Un réseau sans fil doit être encore plus surveillé que les autres modes de connexion filaires au SI car le point d'entrée est difficile à identifier : la propagation des ondes hertziennes est très difficilement contrôlable. Toutefois, il existe des logiciels, y compris open source, permettant de surveiller les connexions (identification de l'adresse MAC).

AVIS D'EXPERT :

Pour sécuriser un réseau Wi-Fi, il existe différents mécanismes. WPA2, le mécanisme correspondant à la norme 802.11i, est à ce jour le plus abouti de ces mécanismes, il est basé sur l'authentification 802.1x (authentification forte par carte à puce, certificat, ...) et le chiffrement AES pour

assurer la confidentialité des informations transmises. L'emploi de WPA2 est formellement recommandé car WEP peut être « cassé » en quelques minutes et il existe aussi une offre de « cloud crackin » pour casser WPA...

La défaillance de la sauvegarde des données



- *Le responsable informatique de la société X a élaboré une procédure de sauvegarde incrémentielle de ses données : sauvegarde totale le dimanche et enregistrement tous les soirs des modifications faites dans la journée.*
- *La secrétaire est chargée de changer les supports magnétiques et une semaine sur 2 un jeu différent est utilisé.*
- *Le 25 novembre, une panne survient, endommageant le serveur sur lequel sont centralisées toutes les données sensibles et notamment comptables.*
- *Lors de l'opération de restauration des dites données, le support de mercredi de la première semaine ainsi que celle du jeudi du second jeu s'avèrent illisibles.*
- *La restauration est impossible. Il faut repartir d'une ancienne sauvegarde totale, vérifier l'intégrité des données enregistrées (conformité à la réalité) et rejouer toutes les opérations de mise à jour. L'activité économique est fortement dégradée et certains clients n'hésitent pas à porter l'affaire en justice.*

Impacts judiciaires

Outre les aspects contractuels et la responsabilité civile en cas de préjudice pour les clients, la loi sur la sécurité financière (LSF) n° 2003-706 du 1er août 2003 oblige à disposer des données qui découlent d'un contrôle interne de qualité, à ceci s'ajoute notamment le respect du livre des procédures fiscales au vu des arts. L169, L176 et L102 B. Il faudra veiller aux clauses de responsabilités contenues dans les contrats clients. Était-il imposé aux clients de sauvegarder eux-mêmes leurs données ? Une clause limitative de responsabilité existe-t-elle ? L'entreprise est-elle assurée ?

Définition :

On peut distinguer la sauvegarde de configuration qui concerne les programmes et leur paramétrage et la sauvegarde des données proprement dites. En fonction des emplois, on peut aussi distinguer une sauvegarde de production qui sera conservée sur site pour un accès et une remise en état plus rapide et la sauvegarde de recours, conservée hors site, pour gérer des événements majeurs (incendie, dégâts des eaux, etc...)

Impacts managériaux et humains

Le service commercial, le service client ainsi que la comptabilité sont paralysés. Il est nécessaire d'avoir recours à des mesures palliatives et de ressaisir les écritures.

Impacts financiers

La ressaisie entraîne un trouble de trésorerie et de production, et des frais supplémentaires. Certains clients décident de changer de fournisseur et refusent de payer leurs factures en cours.

Impacts sur l'image

Mauvaise image vis-à-vis des clients en attente de leur commande, qui sera retardée ou n'arrivera jamais. Impact sur la gestion de trésorerie avec des pénalités de retard, des intérêts non perçus et une communication de crise à financer.

Préconisations

Développer un plan de sauvegarde avec, par exemple, un cycle de sauvegarde quotidienne sur un mois, une sauvegarde mensuelle avec une rotation annuelle. Externaliser le support de fin de semaine ainsi que la sauvegarde mensuelle en dehors de l'entreprise ou, a minima, dans un autre bâtiment..

LES POINTS CLES A RETENIR

La sauvegarde des données est fondamentale. Elle ne concerne pas seulement les données de gestion/comptabilité mais aussi la configuration du système téléphonique et les données pilotant l'informatique industrielle (les machines-outils, la régulation et la logistique, etc...). Une fois la politique de sauvegarde élaborée, il est tout aussi fondamental de tester l'efficacité des enregistrements, c'est-à-dire, vérifier qu'on peut effectivement réinstaller les ressources et les données à partir des supports conservés hors site. L'assurance est un bon moyen d'être remboursé des coûts de remise en état et des préjudices économiques subits.

AVIS D'EXPERT :

Le Plan de Reprise d'Activité, PRA (ou encore appelé Plan de Continuité d'Activité ou des Services), constitue l'ensemble des procédures et moyens techniques et humains à mettre en œuvre pour faire face à une situation de crise.

Au sein de l'entreprise, c'est ce plan qui va permettre d'assurer le maintien des activités critiques. La sauvegarde - et ses processus ad-hoc - en est une composante obligatoire et essentielle.

Le vol d'ordinateur portable ou de PDA

- *Le directeur commercial de la société Y se rend en TGV à Francfort pour négocier un important contrat portant sur 500 pièces de sa dernière innovation.*
- *Il emporte dans ses bagages son PC portable dans lequel il a pris soin de stocker le contrat qu'il doit signer, le tableau des marges et le dernier tarif à donner aux commerciaux locaux, le fichier client et le dernier projet innovant de l'entreprise qui doit sortir l'année prochaine.*
- *En montant dans le taxi, il se rend compte que son ordinateur a disparu.*

Impacts judiciaires

L'employeur licencie son salarié pour faute lourde, à laquelle sera plus probablement retenue la négligence. Le salarié peut saisir les instances prudhommales et obtenir la requalification de son licenciement. L'entreprise ne pourra pas réclamer réparation de son préjudice à son salarié. L'assurance ne prendra en compte que le prix du matériel volé.

Impacts managériaux et humains

La société et son directeur commercial sont décrédibilisés auprès du client allemand. L'entreprise supporte la responsabilité encourue.



Définition :

Le vol matériel est la soustraction de la chose d'autrui, ici matérialisé par un matériel ou des supports de données, par opposition au vol immatériel de données.

Impacts financiers

Le marché qui aurait dû être signé est perdu. Un fabricant étranger sort peu après un produit de caractéristiques voisines mais à prix cassé.

Impacts sur l'image

La société allemande a des doutes sur la capacité de la PME française à protéger efficacement les informations confidentielles.

Préconisations

Mettre en place une protection par mot de passe ou biométrique pour l'accès physique à l'équipement portable. Chiffrer les données. Il existe maintenant des solutions simples et suffisamment robustes à la crypto-analyse, s'appuyant sur une offre commerciale ou « open source » (emploi libre).

Penser à faire une sauvegarde des données traitées pendant le déplacement. Le support (CD, clef USB) sera également chiffré. Déposer dans la mesure du possible immédiatement les éléments volés si des titres de propriété intellectuelle peuvent être obtenus afin de préserver l'antériorité de l'entreprise et vérifier que l'entreprise a bien fait signer des clauses de non-débauchage à ses co-contractants pour éviter que les informations récupérées par un tiers soient utilisées pour concurrencer sans peine l'entreprise.

LES POINTS CLES A RETENIR

Pour certains pays (Chine, Etats-Unis, Israël...), se renseigner avant déplacement sur les réglementations en vigueur (nature des moyens de chiffrement autorisés, autorisation légale d'accès pour des contrôles de sécurité intérieur, etc.). Pour les téléphones-PDA, penser à conserver par ailleurs, l'IMEI, le numéro de téléphone, le numéro de carte SIM, le carnet d'adresses et éventuellement l'agenda.

AVIS D'EXPERT :

En cas de vol, l'identification nécessaire pour ouvrir une session sur le portable sert uniquement à empêcher l'accès au PC. Cependant il n'est pas compliqué de récupérer le disque dur, et les données qui y sont stockées, en le connectant sur un autre ordinateur. De ce fait il est essentiel de chiffrer

les données sensibles sur l'ordinateur portable mais également sur les périphériques de stockage (CD, clés USB, disque dur externe, carte mémoire...). De manière générale, il est prudent de ne jamais se séparer de ses équipements, même pour quelques instants.

Le sabotage interne d'une base de données

- *L'administration organise annuellement sur le territoire national un concours. Celui-ci se déroule en deux phases : une première pour l'admissibilité, une seconde pour les oraux, en vue de l'admission.*
- *L'ensemble des résultats concernant l'admissibilité est communiqué à partir du site Internet de l'administration.*
- *Les candidats admissibles reçoivent alors chez eux une convocation à des examens oraux.*
- *Or, suite à un appel téléphonique d'un candidat qui n'avait pas reçu cette convocation, il est apparu que différentes informations du site Internet avaient été falsifiées par leur webmaster en cours de licenciement.*
- *En effet, une page mentionnant les résultats d'un étudiant non admissible a été modifiée, de telle sorte que ledit candidat apparaissait comme admissible.*

Impacts judiciaires

Ces faits sont clairement constitutifs des infractions visées aux arts. 323-1 et 323-3 du Code Pénal, du fait d'accéder et de se maintenir frauduleusement dans tout ou partie d'un système de traitement automatisé de données (STAD), et de modifier les données qu'il contient. De plus, si des données personnelles circulent sur Internet, le non-respect de l'obligation de sécurité et la divulgation des données personnelles par négligence constituent des infractions au vu des art. 226-17 226-22 du Code pénal.

*-19 en maths mon pater va avoir une syncope !
et 05 à pat pour mes CD pas rendus
-mets un 0 à la brindille ça lui apprendra à tourner autour de mon marc*



Définition :

L'intrusion se fonde sur le caractère frauduleux de l'introduction et du maintien en vue d'une récupération ou d'une modification, sinon d'une altération ou d'une destruction.

Impacts managériaux et humains

Des données personnelles circulent sur l'Internet.

Impacts financiers

Coût de réorganisation de l'épreuve dans sa totalité.
Possibilité de paiement de dommages et intérêts aux candidats.
Frais d'expertise et de procédures.
Frais de gestion des poursuites légales.

Impacts sur l'image

Le discrédit est jeté sur l'organisme victime de cette manipulation.

Préconisations

Nécessité de conserver l'ensemble des données de connexion au serveur et de les remettre aux autorités compétentes. Eviter toute remise en service ou réinstallation qui serait susceptible de supprimer ces traces. Prévoir lors de l'inscription que ce type d'évènements peut amener l'organisateur à annuler l'épreuve.

LES POINTS CLES A RETENIR

Le préjudice en termes d'image peut être considérable. Le contrôle d'intégrité et l'authentification relèvent de la prévention, et la sauvegarde des données de la protection. Le dispositif et la procédure d'alerte et la conservation des traces sont essentiels pour la suite.

AVIS D'EXPERT :

L'utilisateur reste le risque majeur pour la perte des informations. A fortiori lorsque celui-ci décide de venger un manquement à son égard (licenciement, refus d'une augmentation de salaire) par la destruction ou pire, l'altération de la base de données de l'entreprise. Dans ce cadre, l'entreprise doit être en mesure :

- d'assurer la protection de ces données,

*- de tracer les actions de l'inconvenant pour preuve,
- de reconstituer sans dégradation ces données.*

Les solutions adéquates consistent en l'authentification forte, la corrélation de logs et bien sûr les systèmes de sauvegarde de données ainsi qu'une gestion des identités efficace.

Le dysfonctionnement ou l'altération par programmes malveillants

- Les virus font désormais partie de l'environnement informatique. Plusieurs dizaines de malwares (malevolent software, programme malveillant) sont créés chaque jour.
- L'entreprise pensait être en sécurité, mais sa protection antivirale était inadaptée, certains postes n'étant pas protégés, d'autres n'avaient pas la mise-à-jour automatique activée.
- Lors de la consultation par un salarié d'un site d'e-commerce accidentellement contaminé, le réseau de l'entreprise est alors très rapidement infecté, notamment le serveur de messagerie, celui des fichiers et les postes utilisateurs ayant été connectés aux deux serveurs...



Impacts judiciaires

L'introduction d'un code malveillant constitue un délit.
En matière pénale :
une atteinte au système de traitement automatisé de données (STAD) (Art. 323-1, 323-2, 323-3-1 du Code pénal), résultant d'une modification, voire d'une atteinte au fonctionnement même du système à l'aide d'un programme.

En matière civile : celui qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé, à le réparer, aux termes de l'Art.1382 du Code civil, s'il existe des dommages liés à la contamination étendue à des systèmes appartenant à des tiers, à partir de ceux de l'entreprise.

Glossaire :

NAC : network access control

Définition :

Les codes malveillants (en anglais «malware») : virus, vers, chevaux de Troie, bombe logique, espioniciels etc., sont caractérisés par la présence de mécanismes de propagation, de déclenchement, et d'action, en général développés dans l'intention de nuire.

Impacts managériaux et humains

Le système d'information est totalement inutilisable : il faut arrêter le réseau pour éviter la propagation virale et nettoyer chacun des équipements. En premières conséquences, c'est une semaine d'inactivité avec chômage partiel de certains personnels, mais aussi l'usage de palliatifs pour les activités essentielles.

Impacts financiers

Perte de chiffre d'affaires et d'opportunités commerciales.
Coûts de décontamination, de réinstallation de l'ensemble des systèmes.
Dommages et intérêts et frais de procédure éventuels, en cas de contamination d'installations tierces.

Impacts sur l'image

Trouble chez les fournisseurs, les clients, et la banque, avec une nécessité de réduire l'incident.

Préconisations

Un dispositif pare-feu et anti-virus de qualité doit être installé et maintenu constamment à jour, il doit être vérifié dans son bon fonctionnement et dans l'étendue du parc d'équipements protégés, une fois les outils de sécurité et les procédures mis en place. Les journaux d'événements seront régulièrement examinés et conservés, et les alertes prises en compte.

LES POINTS CLES A RETENIR

Les programmes malveillants peuvent causer d'importants dégâts au sein d'une société. Ces programmes peuvent être introduits de différentes manières au sein d'un système d'information : consultation de sites Internet, messagerie, utilisation de données personnelles, ... Aucun dispositif technique n'est en mesure de bloquer les codes malveillants à 100 %. L'accès à Internet est concerné, en même temps que les serveurs, les postes de travail, mais aussi les différents supports : disques externes, clés USB, cartes mémoire, CD-ROM, DVD, PDA en synchronisation etc...

AVIS D'EXPERT :

Pour faire face à ces programmes il faut sécuriser au maximum tout accès vers et depuis l'Internet. Outre la mise en place de Firewall et d'antivirus, il existe également des solutions permettant de centraliser les accès Internet des utilisateurs et d'effectuer un contrôle d'accès au réseau (NAC) qui vérifie l'état d'un ordinateur avant de le

connecter au système d'information. Il est également judicieux de doubler les sécurités avec deux technologies différentes : un antivirus sur les postes de travail et un autre sur la passerelle de messagerie, doublés de deux pare-feux différents en série c.à.d. l'un après l'autre pour ralentir l'intrusion.

La diffamation par courrier électronique

- *Un cadre d'entreprise a reçu un courrier électronique à son adresse professionnelle présentant l'identité d'un de ses collègues, qui n'est pourtant pas à l'origine de cet envoi.*
- *L'adresse de courrier électronique de ce collègue a été créée par un service de messagerie gratuite*
- *Ce courrier a été adressé à d'autres personnes sans que chacun des destinataires n'ait connaissance des autres envois*
- *Le contenu du message porte atteinte à l'honneur et à la considération d'un autre collègue de l'entreprise*

Impacts judiciaires

Le contenu du message peut constituer une diffamation au sens de la loi du 29 juillet 1881 (art. 29), sinon une injure. Il y a aussi dans ce cas usurpation d'identité, du fait de l'usage de l'identité d'un tiers étranger à l'envoi du message. L'usurpation d'identité devrait prochainement être qualifiée de délit pénal.

En matière pénale : la diffamation qualifiée envers un particulier est punie, selon le contenu, jusqu'à un an d'emprisonnement et d'une amende de 12000 € à 45000 € (art.32).

En matière civile : une action en responsabilité civile pourrait être intentée sur les dispositions des arts. 1382 et 1383 du Code civil, en cas de préjudice subi.

En préalable, l'employeur alerté devra vérifier s'il dispose des moyens de contrôler les boîtes aux lettres internes sur ce motif selon sa charte informatique et le rôle dévolu à l'administrateur réseau.

Impacts managériaux et humains

La tension est montée entre les deux hommes avec un impact dans leur travail quotidien.

Impacts financiers

Perte de productivité et d'opportunités difficiles à chiffrer.

Impacts sur l'image

Répercussion possible sur l'image de l'entreprise en cas de contenu à caractère raciste ou sectaire.

Préconisations

Vérifier si des contrôles peuvent être menés sur les messageries de l'entreprise. Sur démarche de la victime et par injonction judiciaire à l'hébergeur de la boîte aux lettres de l'expéditeur, l'identité de la personne mise en cause sera établie et la pluralité des destinataires pourra être démontrée.

Il appartiendra à l'auteur apparent d'apporter la preuve de sa bonne foi, et à l'employeur de réagir dans le respect des règles puisque certains faits se déroulent sur le poste de travail de salariés. Si le nom de l'entreprise a été utilisé, cette dernière sera aussi compétente pour agir en justice.

LES POINTS CLES A RETENIR

L'action en diffamation se prescrit après 3 mois, à compter de la première émission de l'écrit qualifié de diffamatoire ou publication.

AVIS D'EXPERT :

Outil de communication, commun et répandu, la messagerie électronique peut être utilisée comme tous les médias de communication pour transmettre des informations erronées et agresser autrui. Ces messages diffamatoires doivent pouvoir

être tracés afin de fournir la preuve de la diffamation et identifier l'émetteur. Il s'agit donc de placer sur les réseaux internes des sondes de tracking et être capable de stocker sur les serveurs de messagerie les messages diffamatoires reçus et émis.



Définition :

La diffamation est l'allégation ou l'imputation de mauvaise foi d'un fait déterminé qui porte atteinte à l'honneur ou à la considération de la personne physique ou morale à laquelle ce fait est imputé.

La défiguration de site web

- *L'entreprise X est bien connue pour son catalogue en ligne d'articles de décoration.*
- *Son site Internet est le moteur de son activité commerciale et la société X ne se prive pas d'en vanter l'ergonomie et le nombre croissant de visiteurs.*
- *Le vendredi 13 décembre, la société X est obligée de mettre hors ligne son site. Sa page d'accueil a été modifiée, indiquant que la société a été rachetée par un groupe concurrent, et les liens menant aux sites de ce dernier. Les bases de données clients et les commandes sont altérées. L'attaque est menée par un groupe de jeunes hackers qui souhaitent faire un coup.*

Impacts judiciaires

Ces faits peuvent être qualifiés d'atteinte au système de traitement automatisé de données (STAD) (arts. 323-1 et 323-2 du Code pénal), résultant d'une altération des données contenues par suppression ou modification, voire d'une atteinte au fonctionnement même du système, suite à l'accès et au maintien frauduleux, à l'aide d'un programme (art. 46 de la LCEN, art. 323-3-1 du Code Pénal).

Impacts managériaux et humains

Une partie du personnel administratif, de la préparation de commande et de la logistique, est mise au chômage technique pendant 11 jours.

Glossaire :

IP : internet protocole

Définition :

La défiguration (de l'Anglais «defacement») est une action délibérée dirigée contre un site Web pour sa dégradation, sa modification ou sa destruction de pages web, le plus souvent la page d'accueil.

Impacts financiers

Le site n'a plus été en ligne durant 11 jours ce qui a entraîné une perte sèche d'exploitation immédiate, différé la livraison des commandes en cours et généré un important SAV pour certains clients qui avaient payé mais n'ont pas reçu leur colis. Les événements ayant eu lieu en pleine période de fêtes, l'entreprise a vu son plus gros mois d'activité amputé de 50 %.

Impacts sur l'image

L'image de marque de l'entreprise est mise à mal par la revendication et la médiatisation. Les clients expriment leur mécontentement sur un blog connu. Le chiffre d'affaires de l'entreprise a baissé et n'a pas encore repris le même essor qu'auparavant. Les internautes qui se connectaient sur ce site pour la première fois n'y retourneront plus.

Préconisations

S'assurer auprès du responsable ou du prestataire, de la mise à jour des correctifs du serveur Web. Mettre en place un contrôle régulier de l'intégrité des pages et des bases de données associées. Mettre en place et suivre l'efficience des dispositifs visant à prévenir la modification d'intégrité. Conserver toutes les adresses IP et logs de connexion d'une façon fiable et avant dépôt de plainte pour la restauration.

LES POINTS CLES A RETENIR

Les entreprises sont de plus en plus victimes de ce type d'attaque initialement tournée vers les sites institutionnels. L'entreprise doit supprimer les failles présentes sur le dispositif web et son système d'exploitation par une mise à jour au fur et à mesure via les correctifs appropriés.

AVIS D'EXPERT :

Outil de communication et de marketing incontournable, le site web est devenu une cible de choix des hackers, des mécontents, d'une concurrence malhonnête. De par son utilisation, il doit être accessible depuis tout utilisateur d'Internet, donc potentiellement de

personnes mal intentionnées. Ainsi l'accès et l'intégrité du site web doivent être surveillés et sécurisés, soit en mettant en place une infrastructure dédiée à cette sécurisation, soit en vérifiant les conditions effectives de sécurité lors d'un hébergement chez un prestataire.



Les botnets



• *Un courriel contenant une pièce jointe est envoyé à l'ensemble des salariés d'une entreprise. Dans le lot, au moins l'un d'eux exécute la pièce jointe. Dès lors une connexion sortante est créée qui permet alors au pirate de disposer d'un accès à l'intérieur de l'entreprise pour y dérober des données sensibles.*

• *Une banque étrangère est attaquée. Plusieurs millions d'euros sont détournés. Les policiers identifient une adresse IP d'un artisan français. Une perquisition est effectuée, le titulaire de la ligne internet est placé en garde à vue. L'analyse informatique établira que la machine de l'intéressé est compromise et a servi de rebond pour réaliser l'attaque.*

Impacts judiciaires

Lorsque le maître du botnet passe à l'attaque, il se cache derrière les machines compromises. Ainsi seules les adresses IP des connexions en rapport avec celles-ci apparaissent au niveau du serveur cible. C'est donc les propriétaires d'ordinateurs « zombies » qui sont les premiers inquiétés (perquisition, garde à vue, etc ...) et qui devront prouver leur innocence.

Glossaire :

Attaque par déni de service (denial of service attack) : attaque ayant pour but de rendre indisponibles un service ou l'accès à un service. (réseaux, sites internet, etc...)

Pare-feu (firewall) : logiciel ou matériel dont la fonction est de mettre en oeuvre la politique de sécurité du réseau d'une entreprise et des informations qui y transitent en cloisonnant notamment le réseau local et le réseau internet.

Définition :

Abréviation de rOBOTs en réseaux (NET) . Réseaux d'ordinateurs détournés à l'insu de leurs propriétaires. Les Botnets peuvent servir à paralyser un serveur, à diffuser du spam mais également à commettre des délits comme le vol de coordonnées bancaires et identitaires à grande échelle.

Impacts financiers

Paralyser un serveur d'entreprise par une attaque de type « déni de service » peut engendrer de grosses pertes financières. Ceci peut par exemple mettre hors service une interface de vente en ligne et ainsi, priver l'entreprise de nombreuses transactions financières, ou encore rendre inutilisable une boîte aux lettres et empêcher ainsi la société d'accéder à des informations importantes pour son fonctionnement.

Impacts sur l'image

Rendre le système d'information inutilisable ou faire l'objet d'une enquête judiciaire ternit inévitablement l'image de l'entreprise auprès des clients, fournisseurs, partenaires, opinions publiques ... Il en découle bien souvent des rumeurs plus ou moins fondées qui au final font les affaires de la concurrence.

AVIS D'EXPERT :

Les botnets sont de plus en plus puissants et sont désormais l'œuvre des groupes mafieux qui cherchent sans cesse à accroître la puissance de frappe en contaminant un nombre toujours croissant de machines afin d'augmenter la capacité de leur réseau.

Préconisations

Il est nécessaire de sécuriser intelligemment l'entreprise. Pour cela il faut bien évidemment veiller à la mise à jour des différents logiciels afin de limiter les failles mais aussi se poser les bonnes questions pour mettre en place une politique de sécurité adaptée : Qu'avons-nous sécurisé? Par rapport à qui? Contre quoi? Pour combien de temps? Jusqu'à quel niveau d'attaque? La sécurité informatique ne peut se faire dans la généralité. Elle doit être adaptée au contexte.

LES POINTS CLES A RETENIR

Il est impératif d'activer la mise à jour automatique et de veiller à ce qu'elle soit appliquée à l'ensemble du parc informatique dans les délais les plus brefs. Il est aussi nécessaire de définir les logiciels utiles et nécessaires en y mettant obligatoirement un anti virus et un firewall. Le maillon faible reste les employés. Il faut les sensibiliser aux risques, à la richesse de l'information et au social engineering.

Les attaques touchent fréquemment les établissements financiers et les sites disposant d'une grosse activité sur le web (adossée à un fichier client souvent important). La finalité des pirates est d'obtenir un rançon en échange du retour à la normal dans le trafic de la société visée.

Le cybersquatting

- Une entreprise constate sur le net la présence d'un site dont l'adresse fait référence ou ressemble à une marque de la société. Ce site présente des images contraires à l'image du groupe et lui porte ainsi atteinte.
- Suite à une négligence, une entreprise ne renouvelle pas son nom de domaine dans les délais impartis. Un concurrent ou un opportuniste saisit l'occasion et le rachète pour, respectivement, le faire désormais pointer vers ses propres produits ou le revendre au prix fort.

Impacts juridiques

Il faudra à l'entreprise légitime du temps, de l'argent et des procédures judiciaires pour espérer récupérer le nom cybersquatté.

Toutefois, la jurisprudence a tendance à reconnaître des droits au premier exploitant du nom en question à partir du moment où le terme litigieux n'est pas, par ailleurs, utilisé en tant que marque, dénomination sociale, ou autre.

D'un point de vue juridique, il est donc important, d'une part, d'effectuer une veille régulière des noms de l'entreprise, et d'autre part, de vérifier qui est renseigné comme titulaire du nom de domaine sous la rubrique « registrant » et qui bénéficiera donc de la présomption de propriété de ce nom de domaine.

Glossaire :

AFNIC : Association Française pour le Nommage Internet en Coopération
CEMAP : Centre de Médiation et d'Arbitrage de Paris
OMPI : Organisation Mondiale de la Propriété Intellectuelle

Définition :

Le cybersquatting est un acte de parasitisme des activités de l'entreprise qui consiste à déposer un nom de domaine en usurpant le nom d'une entreprise ou celui de ses marques. Une variante est le typo-squatting qui repose sur une orthographe incorrecte en espérant que l'internaute saisisse le nom en commettant la faute d'écriture ou en se trompant de nom de domaine.

Impacts financiers

L'impact financier peut consister en un détournement de clientèle ou de prospect, voire le blocage du lancement d'une innovation ou d'une campagne de communication par un concurrent, faute de disposer du nom.

En cas d'échec de la procédure arbitrale ou judiciaire, l'entreprise risque même de devoir racheter au prix fort ce nom.

Ce type de comportement n'est pas rare car il est favorisé par la modicité du coût et la facilité d'enregistrement d'un nom de domaine dès lors qu'il n'a pas de titulaire à l'instant « t ».

Impacts sur l'image

En termes d'image, l'effet pour l'entreprise peut être désastreux dans la mesure où l'internaute a l'impression d'être sur le site réel de l'entreprise et non sur le site du cyber-squatteur. De fait, l'internaute peut se voir proposer un service de moindre ou faible qualité ou pire encore, être victime d'une escroquerie, etc...

Préconisations

Le premier réflexe peut être pour une entreprise de déposer les dénomination sociale, enseigne de son entreprise, de ses produits, mais également des noms proches : par exemple, pour le nom d'un produit, le déposer au pluriel, au singulier, avec ou sans tiret, en imaginant le terme sous un langage SMS, avec différentes extensions

AVIS D'EXPERT :

Le cybersquatting ne reste pas impuni. Divers recours sont possibles.

Par le biais judiciaire, il vous est possible d'engager des poursuites pour contrefaçon, et, selon les circonstances, pour concurrence déloyale ou parasitisme. Le tribunal sera notamment amené à prononcer la suppression du nom domaine litigieux au profit du légitime titulaire.

de premier niveau (.com, .net, .org) ou de niveau national (.fr, .be)...

Il peut être utile de renforcer les droits sur les noms par des dépôts en tant que marque. Il est également nécessaire d'avoir le réflexe, pour chacun de ces noms de domaine, de les mettre en exploitation réelle et non de se contenter d'une page d'attente, sachant que tous les noms de domaine peuvent renvoyer au même site.

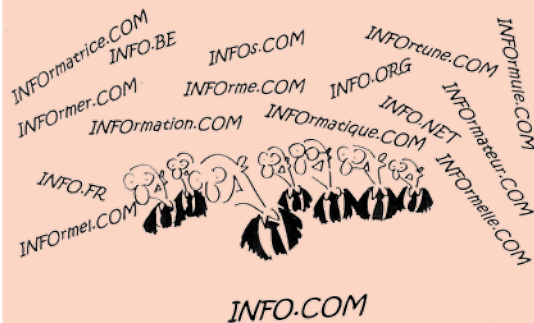
Enfin, il sera utile de mettre en place pour se défendre contre toute opération de cybersquatting, des procédures qui peuvent être soit des procédures judiciaires, soit des procédures alternatives de résolution des litiges. Ces procédures alternatives de résolution du litige peuvent être effectuées entièrement en ligne. Il en existe quatre à ce jour en France. Il s'agit par exemple de la procédure PARL du .fr et .re proposée par l'AFNIC, de la recommandation en ligne du CMAP, les centres de l'OMPI et le forum sur le droit sur l'Internet.

LES POINTS CLES A RETENIR

Il faut anticiper le dépôt des noms de domaines potentiellement intéressants pour la communication ou le développement de l'entreprise.

Selon la taille de l'entreprise et le nombre des noms de domaines à gérer, il conviendra peut-être de les faire surveiller par un organisme qui assurera le suivi de la péremption des droits, voire une veille des noms de domaine susceptibles de susciter ce type de problèmes.

Par le biais de procédures alternatives avec le recours aux règles de l'ICANN. Il s'agit de l'autorité internationale pour la régulation de l'Internet. Elle dispose d'un système d'arbitrage international en cas de conflit, avec de nombreux représentants au travers le monde. Par le biais de la médiation avec des démarches en ligne de l'AFNIC et le forum des droits sur Internet.



Les 5 réflexes à avoir lors de la réception d'un courriel

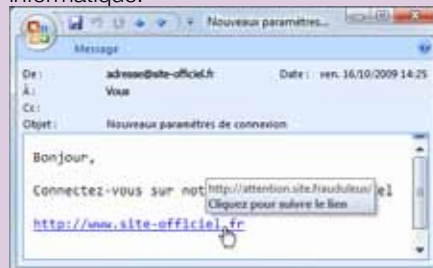


1 N'ayez pas une confiance aveugle dans le nom de l'expéditeur

N'importe qui peut vous envoyer un courriel en se faisant passer pour un autre! Cela n'est pas beaucoup plus compliqué que de mettre un faux nom d'expéditeur au verso d'une enveloppe. Soyez donc attentif à tout indice mettant en doute l'origine réelle du courriel, notamment si le message comporte une pièce jointe ou des liens : incohérence de forme ou de fond entre le message reçu et ceux que votre interlocuteur légitime vous envoie d'habitude, par exemple. En cas de doute, contactez votre interlocuteur pour vérifier qu'il est à l'origine du message. Et même si l'expéditeur est le bon, il a pu, à son insu, vous envoyer un message infecté. Vous devez admettre, que dans le domaine de la messagerie électronique, il n'existe pas d'expéditeur a priori de confiance.

3 Ne jamais répondre sans vérification à une demande d'informations confidentielles

Certaines demandes d'informations confidentielles ne sont jamais faites par courriel (mots de passe, code PIN, coordonnées bancaires, etc.). En cas de doute, là encore, demandez à votre correspondant légitime de confirmer sa demande. Car vous pouvez être victime d'une tentative de **filoutage, ou phishing**. Il s'agit d'une technique utilisée par des personnes malveillantes, usurpant généralement l'identité d'un tiers ou simulant un site dans lesquels vous avez a priori confiance (une banque, un site de commerce, etc.) dans le but d'obtenir des informations confidentielles, puis de s'en servir. Les messages du type chaîne de lettres, porte-bonheur ou pyramide financière, appel à solidarité, alerte virale, ou autres, peuvent cacher une tentative d'escroquerie. Evitez de les relayer, même si vous connaissez l'expéditeur. Consulter la fiche «**les canulars par messagerie**» sur le portail gouvernemental de la sécurité informatique.



2 Méfiez-vous des pièces jointes

Elles peuvent contenir des **virus** ou des **espioniciels**. Assurez vous régulièrement que votre anti-virus est activé et à jour. Si votre poste a un comportement anormal (lenteur, écran blanc sporadique, etc.), faites le contrôler.

4 Ne cliquez pas les liens proposés et soyez attentif à l'orthographe

En passant la souris au-dessus du lien proposé, vous pouvez repérer s'il pointe bien vers l'adresse du site annoncé dans le message. Si l'adresse est différente, soyez méfiant, et évitez de cliquer sur le lien. De manière générale, il est préférable de saisir manuellement l'adresse dans le navigateur. Dans la plupart des tentatives de **filoutage**, notamment lorsqu'elles viennent de l'étranger et que le texte a été traduit par un logiciel, l'orthographe et la tournure des phrases sont d'un niveau très moyen, et les caractères accentués peuvent être mal retranscrits. Soyez donc le plus vigilant possible lors de la réception de tels messages.



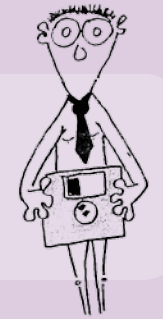
5 Bien paramétrer vos logiciels de messagerie

- Mettez à jour vos logiciels, si possible en activant la procédure de mise à jour automatique ;
- Paramétrez votre logiciel de messagerie pour désactiver la prévisualisation automatique des courriels ;
- Dans les paramètres de sécurité en options, interdisez l'exécution automatique des ActiveX, des plugins et des téléchargements, soit en les désactivant, soit en imposant de vous en demander l'autorisation ;
- Dans un environnement sensible, lisez tous les messages au format texte brut.

A SAVOIR

Des mesures de prévention et un guide de paramétrage des logiciels de messagerie sont disponibles sur le site du **Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques (CERTA)**, à l'adresse

<http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-002/index.html>



Les 5 réflexes à avoir lors de la connexion à un HotSpot wifi

1 Tout d'abord, vérifiez que vous êtes convenablement protégés

Les statistiques le démontrent, beaucoup trop d'ordinateurs sont encore aujourd'hui mal protégés contre les logiciels malveillants (virus, vers, espionciels...). C'est vrai des stations de travail, mais également pour les appareils mobiles qui évoluent dans un environnement plus risqué à l'extérieur de l'entreprise...

Un bon antivirus (étendu aux spyware et autres trojans), à jour bien évidemment, est d'abord est avant tout de mise, comme sur tout ordinateur... Il faudra également veiller à ce que le système d'exploitation et les applications soient à jour de leurs correctifs, afin que les failles de sécurité connues soient comblées. Enfin, un firewall (le plus souvent logiciel) permettra une protection contre tout accès extérieur, notamment de la part des autres utilisateurs du HotSpot Wifi...

2 Paramétrez convenablement votre ordinateur

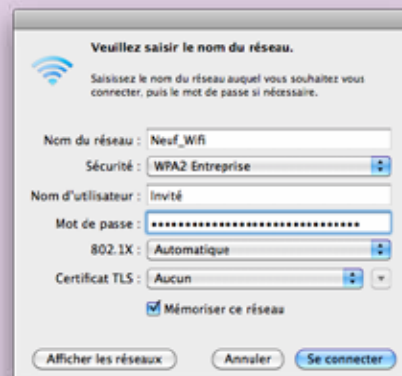
Tout d'abord, désactivez le partage de fichier dans les préférences de votre système d'exploitation afin de ne pas faciliter la tâche d'un internaute indélicat qui viendrait à vouloir regarder le contenu de votre appareil.

De même, désactivez le mode point à point (ou ad hoc) qui permet de créer facilement et directement un réseau entre

plusieurs appareils, sans point d'accès ni connexion physique à un réseau, parfois même sans que vous ne vous en rendiez compte

3 Au moment de la connexion, vérifiez bien l'authenticité du HotSpot Wifi

En effet, les pirates n'hésitent plus à mettre en place de faux hotspots reproduisant les caractéristiques de ceux les plus connus, pour intercepter vos login et mot de passe réseau et en faire une utilisation frauduleuse.



En cas de doute, vérifiez tout d'abord la présence d'un petit cadenas dans la barre de votre navigateur internet (qui signifie que la communication est sécurisée), et que le certificat est légitime, émanant bien d'une autorité reconnue. Malgré cela, il faut rester vigilant car certains sites de

pharming ou de phishing utilisent ces technologies pour avoir un aspect authentique. Le cas échéant n'hésitez donc pas à en demander la confirmation auprès du responsable du hotspot considéré.

Préférez au surplus un hotspot utilisant un protocole de cryptage pour la connexion, comme le WPA (WiFi Protected Access) ou mieux le WPA2.

Passer votre curseur au dessus des liens, faites attention aux caractères accentués dans le texte ainsi qu'à la qualité du français dans le texte ou de la langue pratiquée par votre interlocuteur

4 Protégez vos données sensibles

Tout d'abord sur le support sur lesquelles elles sont stockées en utilisant le cas échéant un logiciel approprié. C'est vrai pour votre disque dur, mais également pour les données stockées sur des supports amovibles telles les clefs USB. En effet, si malgré les précautions énoncées ci-dessus, une personne malintentionnée parvenait à accéder à vos données sensibles, elle ne pourra pas les utiliser sans les avoir préalablement déchiffrées. Ensuite, en chiffrant à leur tour les données que vous envoyez depuis votre appareil mobile, tels les e-mail suivant leur contenu.

Vous pouvez enfin utiliser un tunnel ou VPN (Virtual Private Network) pour y faire transiter les données destinées à~ ou provenant de~ votre entreprise.

Lors de vos déplacements, prenez l'ha-

bitude de n'emporter que le minimum de données destinées exclusivement à vos tâches en cours...

5 Protégez le matériel lui-même !

A quoi bon toutes ces précautions si vous n'adoptez pas les bons réflexes, tellement évidents, mais que d'aucuns oublient souvent ! Tout cryptage est inutile si vous ne prenez pas la peine de cacher vos login et mot de passe de la vue des tiers lors de leur saisie sur l'écran approprié !

De retour au sein de l'entreprise, vérifiez l'intégrité du matériel mobile avant sa reconnexion au réseau interne.

De même, le vol de votre appareil mobile même protégé, permettra à l'auteur de ce dernier surtout s'il est déterminé, d'avoir le temps de contourner toutes vos protections et d'accéder à vos données !

A SAVOIR

Les ordinateurs d'entreprises volés le sont de plus en plus pour les informations qu'ils contiennent, et non pas pour l'appareil lui-même.

Dans ce contexte de nomadisme toujours croissant, il faut développer une posture de vigilance adaptée. Le portail de la sécurité informatique propose un passeport de conseils qui présente des règles simples à mettre en œuvre pour réduire les risques et les menaces, ou en limiter l'impact à l'adresse:

http://www.securite-informatique.gouv.fr/IMG/pdf/Passeport-de-conseils-aux-voyageurs_janvier-2010.pdf

Mais encore ...

Les 12 scénarios de malveillance que vous venez peut-être de découvrir sont des cas très fréquemment rencontrés dans l'environnement PME-PMI.

Comme vous pouvez le constater, les risques sont variés de par leur nature et quant à leur impact. Une démarche de sécurité est donc une action dynamique, cyclique, qui doit mettre en œuvre une mise-à-jour périodique des moyens et procédures en place. Pour cela, une évaluation des risques et des enjeux par un consultant en sécurité des systèmes d'information permettra une meilleure harmonisation des plans de sécurité (sauvegarde, secours informatique, gestion des droits, antivirus et correctifs de sécurité, etc.) tout en ordonnant la mise en place de nouvelles solutions de sécurité.

Il y aurait également ...

• *Le déni de service*

Il s'agit d'une indisponibilité de la ressource ciblée sans, toutefois, altérer ou détruire les données sur le site. On distingue ainsi le déni de service distribué qui s'appuie sur un réseau de zombies (botnets) pour viser par exemple le site web. Mais il peut également s'agir de bombing par saturation d'une ressource telle que la messagerie électronique (envoi de milliers de messages avec pièce jointe) ou encore du standard téléphonique maintenant de plus en plus en VOIP (voix sur IP).

• *La carence de fournisseur*

La tendance commerciale à l'externalisation des traitements (infogérance) présente des avantages économiques certains, mais complique encore la mise en sécurité des données de l'entreprise. En effet, cette offre de service (traitement des données) ou d'hébergement se caractérise par une concentration de plus en plus massive des équipements dans de gigantesques centres informatiques. De fait, tout dysfonctionnement d'un service (climatisation, électricité, connexion Internet) perturbera l'activité de tous les clients hébergés sur le même site. Le fait initial peut être identique à un des scénarios présentés : sabotage de données, infection virale, etc. Mais comme il se produit chez un prestataire, l'entreprise a moins de facilités pour gérer la crise. D'autant plus qu'elle pensait être en confiance considérant la bonne renommée du prestataire ou qu'elle s'imaginait que les dispositions contractuelles (pénalités de retard et niveau de service qualité) ou un recours en responsabilité civile lui permettrait d'absorber le préjudice économique subi. Pour ce

qui est infogérance, hébergement, accès Internet, application service provider... il est fondamental que non seulement les informaticiens et les juristes valident le contrat de prestation mais aussi les réponses des « métiers et services » pour vérifier que les dispositions de reprises (délais) et compensations sont cohérentes avec les exigences de l'activité.

• *Les risques environnementaux*

De plus, même des données et des ressources dites immatérielles peuvent subir une destruction ou une altération consécutive à un dommage physique. Comme indiqué dans l'introduction, l'incendie, les dégâts des eaux, qu'ils soient d'origine naturelle ou industrielle, peuvent provoquer l'indisponibilité d'une ressource. Un risque d'environnement de type pollution ou un conflit syndical peuvent empêcher l'accès physique à la salle informatique et rendre impossible l'exploitation des ressources informatiques. C'est pourquoi, en complément du plan de sauvegarde des données, il est fondamental de mettre en place non seulement un « plan de secours informatique » pour assurer la redondance des serveurs mais encore un « plan de continuité d'activité » qui permettra aux utilisateurs d'accéder aux serveurs relocalisés pendant la durée de gestion de crise.

Toutefois, la sûreté de fonctionnement mise en avant par la redondance des équipements, le nombre de transformateurs, d'onduleurs, de groupes électrogènes... est remise en cause par la présence de plus en plus systématiques d'une « couche logicielle » pour le paramétrage et/ou l'administration de ces équipements. A l'aléa de la panne matérielle physique s'ajoute le risque d'un bug logiciel répliqué sur toutes les installations en redondance...

• *Les erreurs et les omissions*

Le comportement humain est très riche en matière de comportement à risques. Ainsi les erreurs de saisie, les mauvaises configurations des équipements, les cahiers des charges inadaptés, les conduites de projets non formalisées... sont autant de possibilités d'atteinte au bon fonctionnement du système d'information. L'omission et la négligence peuvent aussi générer des situations à risques !

• *La non-conformité réglementaire*

Enfin, l'impact et/ou le traitement judiciaire des actes malveillants présentés ne doit pas faire oublier une autre forme de risque pour l'entreprise : l'engagement de responsabilité pour non-conformité réglementaire. Que ce soit pour un défaut de déclaration, une conservation inadaptée, une divulgation accidentelle ou malveillante...

• *Un suivi lacunaire du matériel en fin de vie*

Au moment de la mise au rebut ou de la cession du matériel informatique (y compris imprimantes, photocopieurs, fax) et de tout support de données en général, il est important d'effacer l'ensemble des données stockées et donc de bien choisir la méthode de suppression. Formater un support n'est pas équivalent à l'effacer, des logiciels en accès libre permettent de récupérer des données après plusieurs formatages. Il importe de proportionner l'efficacité de la méthode d'effacement au degré de confidentialité des données potentiellement contenues sur le support. En outre, une bonne pratique consiste à assurer la traçabilité du matériel informatique en fin de vie (cession à un tiers ou certificat de destruction dans le respect des normes écologiques).

Impact et occurrence des risques en entreprise

Il vous est proposé une grille pour mesurer l'évaluation de la probabilité et l'impact des menaces évoquées dans les fiches. L'évaluation dépend toutefois de la situation de chaque entreprise, mais aussi de la sensibilisation et de la connaissance de celui qui l'exprime, en fonction de deux facteurs indépendants qui sont la possibilité d'occurrence et l'impact.

Niveaux d'exposition

Pour faciliter l'estimation, il est également proposé les échelles suivantes :

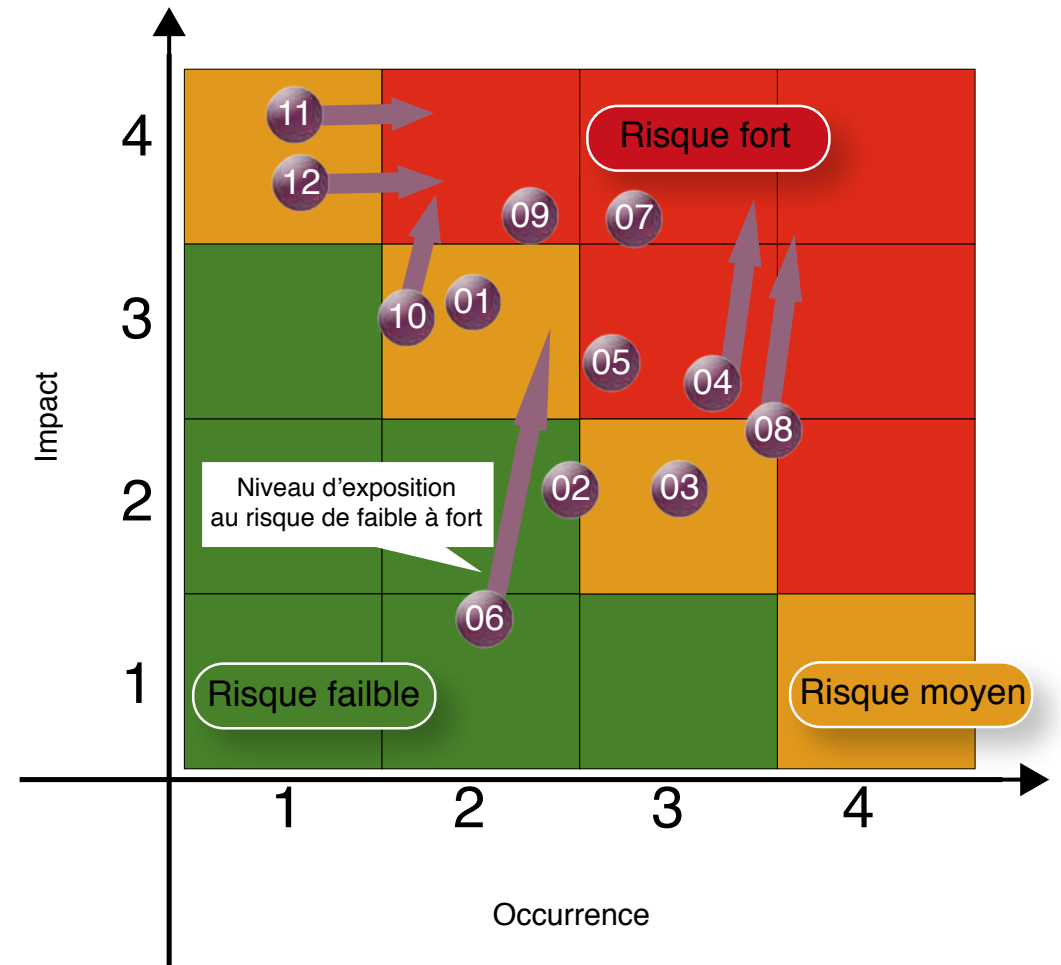
Impact du risque : 1 léger, 2 moyen, 3 sérieux, 4 catastrophique,

Occurrence du risque : 1 légère, 2 modérée, 3 forte, 4 très forte,

et trois couleurs pour qualifier arbitrairement le niveau d'exposition au risque de faible, moyen et fort.

Risques étudiés

- Le comportement à risques du salarié **01**
- La fraude financière via la comptabilité **02**
- La divulgation de savoir-faire **03**
- Les téléchargements illicites et intrusion via le réseau sans fil **04**
- La défaillance de la sauvegarde des données. **05**
- Le vol d'ordinateur portable ou de PDA **06**
- Le sabotage interne d'une base de données **07**
- Le dysfonctionnement ou l'altération par programmes malveillants **08**
- La diffamation par courrier électronique **09**
- La défiguration de site web **10**
- Les botnets **11**
- Le cybersquatting **12**



Etat des lieux “le chef d’entreprise face au risque numérique”

Recommandations des institutions.

Les entreprises et la cybercriminalité

Bien que la sécurité informatique soit de plus en plus une réalité, un élément incontournable et une condition à la survie des entreprises, il apparaît que le cheminement vers une prise de conscience du risque numérique ne soit pas encore totalement parcouru aujourd’hui.

En effet, la cybercriminalité gagne du terrain dans une économie mondialisée. L’enjeu de souveraineté nationale pour l’Etat est de garantir la sécurité de ses propres infrastructures, essentielles pour le développement des activités socioéconomiques de la nation et la protection des entreprises et des citoyens. Par ailleurs les entreprises doivent prendre des dispositions pour se préserver de la concurrence et de la malveillance.

Le terme de cybercriminalité a été inventé à la fin des années quatre-vingt-dix, alors qu’Internet se répandait en Amérique du Nord. Lors du Sommet de Lyon (27-29 juin 1996), les pays du G8 ont constitué un groupe de travail chargé d’étudier les nouveaux types de criminalité encouragés par, ou migrant vers Internet.

Dans un même temps, et à l’initiative des membres du groupe de Lyon, le Conseil de l’Europe a rédigé un projet de « Convention sur la Cybercriminalité » (1). Il s’agissait d’harmoniser les législations des Parties contractantes en la matière. A cet effet, cette convention, rendue publique pour la première fois en 2000, prévoyait de compléter l’arsenal juridique des Etats en matière procédurale, afin d’améliorer la capacité des services de police à mener en temps réel leurs investigations et à collecter

des preuves sur le territoire national avant qu’elles ne disparaissent. Cependant, elle n’a pas fourni de définition claire de cette nouvelle forme de criminalité : le terme englobait tout un ensemble de nouveaux problèmes auxquels se trouvaient confrontées la police et les agences de renseignement, et découlant des performances toujours meilleures des ordinateurs, de la baisse du coût des communications, et du phénomène Internet.

La majeure partie a traité du droit et des conventions internationales : il s’agissait de définir les outils (coopérations internationales renforcées, nouveaux modes de preuve,...) susceptibles de fonder des poursuites efficaces à l’encontre des cybercriminels. C’est ainsi que l’on envisagea pour la première fois la mise en place de procédures de contrôles sur le réseau des réseaux : injonctions de conservation rapide de données stockées, mandats électroniques, recueil de données en temps réel, archivage des données relatives au trafic.

Un peu plus tard, le 25 février 2005, un rapport présenté par Thierry Breton, Ministre de l’Economie, des Finances et de l’Industrie au Ministre de l’Intérieur, de la Sécurité Intérieure et des Libertés Locales évoque un chantier de lutte contre la cybercriminalité (2).

Le rapport définit la cybercriminalité comme un nouveau domaine pour le droit pénal et la procédure pénale tout en mesurant l’émergence d’un corpus législatif et réglementaire et en intégrant sa dimension au niveau international.

Il est aussi question d’une prise en compte

1/ Cf : <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=FRE>
2/ www.telecom.gouv.fr/fonds_documentaire/rapports/cybercriminalite.pdf

de la cybercriminalité par la police et la gendarmerie comme un champ d'action renouvelé et ouvert.

Ce même rapport a permis de mettre en avant un certain nombre de mesures à savoir :

- une meilleure connaissance statistique de la cybercriminalité ;
- un doublement des capacités d'investigation spécialisées des services de police et des unités de gendarmerie avec le renforcement de l'OCLCTIC, le doublement du nombre des enquêteurs spécialisés, la mise en place de référents ;

- le développement d'actions de formation communes ;
- un renforcement des capacités juridiques d'investigation ;
- un renforcement de la veille technologique et de la recherche et développement (R&D) ;
- un meilleur contrôle des contenus illicites véhiculés par Internet ;
- une meilleure protection des mineurs ;
- une politique de prévention ;
- la définition d'un certificat «citoyen» des fournisseurs de services de l'Internet.

Un enjeu de coopération internationale

La Convention sur la cybercriminalité du Conseil de l'Europe, adoptée en 2001, reste le seul cadre juridique de référence au niveau international.

Afin de renforcer la coopération européenne et à l'initiative de la France, le conseil européen a décidé, fin 2008, de créer une plate-forme européenne de signalement de contenu illicite. Hébergée à Europol, elle centralise les signalements des plateformes nationales pour une plus grande réactivité dans le traitement des sites illicites. Le programme de Stockholm, adopté en décembre 2009, fixe pour les cinq années à venir, l'ambition de renforcer la coopération policière et judiciaire européenne pour contrer la cybercriminalité notamment en développant l'action d'Europol et en clarifiant les règles s'appliquant sur le cyberspace européen.

Analyse de la menace. Bilan

Ces dernières années ont été particulièrement riches en événements, ont permis d'identifier de nouveaux risques majeurs, de constater que les attaquants développaient continuellement de nombreux outils ou techniques d'attaque afin de déborder les outils de sécurité mis en place et la vigilance des utilisateurs, mais aussi que des menaces que l'on pensait contrôlées pouvaient encore entraîner de nombreux dégâts.

L'année 2009 notamment a été marquée par une augmentation particulièrement significative du nombre d'attaques traitées, augmentation qui peut être imputée, d'une part aux échanges internationaux plus riches, et donc des renseignements sur les attaques ou tentatives plus fournis, mais aussi à l'augmentation des attaques informatiques dans le monde.

Les codes malveillants, méthode d'attaque visant la récupération de données sensibles

L'utilisation de codes malveillants, de type Chevaux de Troie, destinés à réaliser des attaques dans le but de dérober des informations sensibles ne se limite pas au champ des activités secrètes ou sensibles des Etats. Elles touchent l'ensemble des activités dans lesquelles la concurrence existe. Les entreprises sont ainsi une cible de choix pour les attaquants. Au même titre, la récupération de données à caractères personnels est toujours en forte croissance. Les attaques par filoutage (Phishing), maintenant rédigées dans un français de bonne qualité, sont monnaie courante. En période de crise, les arnaques proposant des gains d'argent sont toujours alléchantes. Ainsi, le ministère des finances a vu une recrudescence de courriels dits « de remboursement de trop perçu » ayant pour objectif d'obtenir les coordonnées bancaires des internautes crédules.

L'année 2009 restera aussi tristement célèbre en raison de la propagation du ver Conficker. En octobre 2008, une faille critique a été corrigée par Microsoft. Malheureusement, la criticité de cette faille a été largement sous estimée. Quelques mois plus tard, de nombreux codes malveillants ont envahi nos réseaux, entraînant des infections massives, des indisponibilités... La capacité de ce ver à se propager via des médias amovibles (clés mémoire USB) a décuplé ses capacités d'infection, lui permettant de pénétrer et d'infecter des réseaux normalement déconnectés de l'internet. Début 2010, la menace est toujours présente.

La multiplication des attaques ciblées au plan mondial

Depuis 2005, le nombre d'attaques ayant délibérément ciblé des systèmes sensibles et utilisant des codes malveillants spécifiquement conçus à cet effet est en très forte augmentation. La France n'a pas été épar-

gnée. Le modus operandi de ces attaques consiste en l'envoi d'un message électronique semblant provenir d'un interlocuteur habituel ; ce message est accompagné d'une pièce jointe infectée qui installe un code malveillant ayant pour but de récupérer des informations sensibles lorsque le destinataire tente de l'ouvrir. Du fait de la difficulté à les détecter et du ciblage préférentiel des autorités, ces attaques ciblées constituent une menace particulièrement insidieuse. De nombreuses vulnérabilités dans les formats bureautiques usuels ont amplifié la menace. Citons les formats PDF particulièrement exploités sur 2009.

Plusieurs pays étrangers sont maintenant parfois cités comme étant impliqués, ou participants à ces récupérations d'informations.

Les vulnérabilités qui favorisent les attaques

Il s'avère que ces différentes menaces s'expliquent par des vulnérabilités diverses dont les plus importantes sont exposées ci-dessous :

Les premières sont les vulnérabilités liées aux applications, à savoir une qualité médiocre du code d'un logiciel qui permet alors au pirate d'en exploiter des failles pour conduire ses attaques. Il s'agit d'erreurs de conception ou d'implémentation. La réponse apportée par l'Etat pour les organismes gouvernementaux vient du CERTA sur la base de ses publications. On ne rappellera jamais assez que la mise à jour des applications et de leurs correctifs constitue la première ligne de défense des systèmes d'information.

L'autre vulnérabilité mise en cause concerne les conditions d'emploi. Il peut s'agir de l'environnement du travail et du paramétrage de l'installation. On constate que ces incidents sont souvent liés à une mauvaise mise en œuvre de la PSSI. Les exemples sont diversifiés et nombreux et vont de l'hébergement mutualisé de sites sur un serveur propice à la propagation des codes malveillants, à la suppression de la protection apportée par

les pare feux, en passant par des erreurs de configuration des droits ou la fuite d'informations circulant par des technologies rayonnantes, de type wifi ou bluetooth.

Enfin, il est un élément qu'on ne peut ignorer, puisqu'il participe à sa façon au système d'information : les vulnérabilités introduites par les utilisateurs. Elles résultent d'une mauvaise manipulation par les utilisateurs finaux du système d'information, et s'expliquent par la faible qualité des mots de passe, l'ingénierie sociale, le phénomène de filoutage, l'utilisation de supports amovibles sans contrôle...

Conclusion - Etude de cas

Fin mars 2009, une administration française a été la cible d'une attaque en déni de service distribué (ou DDoS). Cette attaque par saturation a consisté en un envoi massif de données en provenance de nombreux pays étrangers, vers les structures de l'administration, entraînant une paralysie de ses moyens de communication avec Internet. Bien que la motivation des attaquants reste encore à déterminer, la volonté de nuire ne fait aucun doute. Depuis l'incident dont a souffert l'Estonie en mai 2007, ce type d'attaque a été de plus en plus médiatisé, amenant les différents pays et des groupes de réflexion à chercher activement les moyens de s'en prémunir.

Dès le début de l'attaque l'administration victime a rapidement identifié le dysfonctionnement. Le CERTA s'est déplacé au centre informatique afin de soutenir l'équipe de crise mise en place. L'intervention a alors consisté à analyser les éléments techniques disponibles afin de proposer des parades à l'attaque.

L'attaque a pu être endiguée, avec un retour à la normale au bout de 24 heures, grâce à un travail conjoint du CERTA, de l'administration visée et du fournisseur d'accès Internet. Dans ce type d'attaque, il convient de réagir très vite, et de savoir impliquer les bonnes personnes ayant une maîtrise suffisante de l'infrastructure, ainsi que la capacité de prendre les bonnes décisions.

En parallèle, une procédure policière a été diligentée, et de nombreux éléments ont été collectés dans le cadre d'accords internationaux visant à la sauvegarde des données. Ces données récupérées sur les ordinateurs ayant participé à l'attaque ont permis de déterminer que les machines attaquantes avaient elles-mêmes été compromises et participaient à l'insu de leurs propriétaires à ce déni de service distribué.

Ce cas n'est malheureusement pas isolé, les attaques par déni de service étant maintenant monnaie courante sur l'Internet (nuisance provoquée par un concurrent, motif politique, propagande...). Dans tous les cas, il convient de traiter ces attaques sérieusement, en l'occurrence par un dépôt de plainte d'une part, et par une demande d'assistance technique si besoin d'autre part.

Il n'existe pas de solution simple car aujourd'hui, les logiciels malveillants peuvent s'attaquer à tous les utilisateurs d'Internet, des entreprises aux particuliers, en passant par les gouvernements. **La sécurité est donc bien l'affaire de tous, qu'il s'agisse des Etats, des entreprises ou des particuliers. Neuf grands principes permettent de structurer une démarche globale :** sensibilisation, responsabilité, réaction, éthique, protection des libertés, évaluation des risques, conception et mise en œuvre de la sécurité, gestion de la sécurité, réévaluation. La prise en compte de cette chaîne permet de s'engager dans une démarche cohérente face à un problème universel. La réponse à ce défi passe également par l'approfondissement des connaissances par les différents groupes (gouvernements, entreprises, utilisateurs ou acteurs techniques). Coopération et partage doivent également fédérer ces acteurs. Toute solution appliquée par l'un sans être partagée par les autres sera inefficace. L'encouragement de bonnes pratiques doit associer, dans une démarche convergente, approche réglementaire, répression, solutions techniques, actions d'éducation et de sensibilisation et enfin coopération internationale.

La loi protège votre entreprise

Première réponse de l'Etat aux incidences concrètes sur la vie quotidienne : la loi

Dans la mesure où la protection des citoyens et des entreprises dans le cyberspace entre dans le champ des compétences régaliennes de l'Etat, il apparaît clairement que ce dernier a pu identifier des risques et des menaces. La première réponse, assez précoce finalement, de l'Etat français a donc été de légiférer en la matière. Les domaines concernés sont parfois abordés par les mêmes textes de loi, ce qui explique les redites ci-après.

Informatique et libertés

Le premier principe a consisté à dire que « l'informatique doit être au service de chaque citoyen (...) Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ». Ce principe correspond en fait au tout premier article de la loi Informatique et Libertés, du 6 janvier 1978, modifiée par la loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données personnelles, l'une à caractère général, l'autre relative à la pro-

tection de ces données dans les réseaux. La commission européenne a contribué au principe de protection de la vie privée et des libertés individuelles au travers des deux textes suivants :

- directive européenne 95/46/CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;
- directive européenne 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

Cybercriminalité

Nouveau domaine pour le droit pénal, la cybercriminalité recouvre deux grandes catégories d'infractions :

- les infractions directement liées aux technologies de l'information et de la communication, à savoir les atteintes aux systèmes de traitement automatisés de données, la diffusion de programmes malveillants, les infractions à la loi Informatique et Libertés sanctionnées au pénal, les infractions aux moyens de paiement et les infractions à la législation sur la cryptologie ;
- les infractions dont la commission a été facilitée ou liée à l'utilisation de ces technologies, à savoir la diffusion de contenus illicites (pédopornographie, racisme, ...),

les escroqueries par faux moyens de paiement pour une transaction en ligne, et certaines autres formes d'escroqueries, mais aussi les contrefaçons de logiciels et autres atteintes à la propriété intellectuelle.

Pour couvrir l'ensemble de ces domaines, les principales lois qui ont été adoptées sont :

- la loi du 5 janvier 1988, dite loi Godfrain (accès frauduleux aux systèmes d'information) ;
- la loi sur la sécurité quotidienne du 15 novembre 2001 (conservation des données de connexion par les opérateurs, cryptologie, cartes de paiement) ;
- la loi pour la sécurité intérieure du 18 mars 2003 (perquisition dans un système d'information, préservation des données par les opérateurs) ;
- la loi pour la confiance dans l'économie numérique du 21 juin 2004 (conservation des données par les hébergeurs de contenus, saisie des données informatiques, renforcement de la loi Godfrain, cryptologie) ;
- la loi relative au droit d'auteur et aux droits voisins dans la société de l'information, du 1er août 2006.

D'autres textes sont venus compléter cet arsenal :

- l'article 163-4 du Code Monétaire et Financier (CMF) sanctionne la fabrication, la détention, et la cession de moyens informatiques permettant d'attaquer les cartes bancaires ;
- l'article 39 de la loi 2001-1062 modifiant le CMF crée un Observatoire de la sécurité des cartes de paiement.

Au niveau européen, il convient de signaler :

- la décision cadre 2005/222/JAI du 24 février 2005 relative aux attaques visant les systèmes d'information ;

- la directive 2006/24/CE du 15 mars 2006 sur la conservation de données dans le cadre de la fourniture de services de communications électroniques.

Par définition, le cyberspace ne connaît pas de frontières physiques. Il a donc fallu prendre en compte des dimensions internationales au-delà de l'Union Européenne : cela a été fait au travers du traité de Budapest (Convention du Conseil de l'Europe) sur la cybercriminalité en date du 23 novembre 2001 et de son protocole additionnel du 7 novembre 2002. Des travaux dans le domaine de la cybercriminalité sont également conduits par le G8.

Réponses françaises à la cybercriminalité

La France a ratifié la Convention du Conseil de l'Europe.

La loi n° 2005-493 du 19 mai 2005 a approuvé la Convention du Conseil de l'Europe sur la cybercriminalité et le protocole additionnel à cette Convention relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (J.O., n° 116, 20 mai 2005, p. 8729). Les décrets permettant la publication de la Convention et du protocole ont été adoptés le 23 mai 2006. Il s'agit du décret n° 2006-580, J.O., n° 120, 24 mai 2006, p. 7568 et du décret n° 2006-597, J.O., n° 122, 27 mai 2006, p. 7937.

La prise en compte croissante de la menace représentée par la cybercriminalité s'est traduite par la mise en place d'un dispositif dédié au sein du ministère de l'Intérieur.

Ainsi, le plan d'action du ministère de l'Intérieur, présenté le 14 février 2008, définit quatre cibles principales : l'usurpation d'identité, l'escroquerie en ligne, les

contenus pédopornographiques, racistes ou antisémites, les incitations aux terrorismes.

Pour accomplir ces nouvelles missions, de nouveaux moyens sont consacrés à la lutte contre la cybercriminalité :

- Mise en place d'une plate-forme de signalement automatique de toutes les formes de malversation, escroquerie, incitation à la haine raciale ou pédopornographie constatées sur Internet (3) ;
- Doublement du nombre d'enquêteurs spécialisés en criminalité informatique, au

sein de la direction centrale de la police judiciaire, et d'enquêteurs en technologie numérique de la gendarmerie ;

- Création de cursus à vocation technologiques au sein de la police nationale, comme il en existe dans la gendarmerie.

La loi d'orientation et de programmation pour la performance de la sécurité intérieure viendra compléter le dispositif juridique national pour permettre aux forces de l'ordre de mieux sécuriser le cyberspace.

3/ www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action

Des services spécialisés pour aider les entreprises

Disposer d'outils, aussi performants soient-ils, ne suffit pas pour autant, encore faut-il pouvoir les mettre en œuvre. Pour cela, la France s'est dotée de services spécifiques. La réponse, sur le plan pénal et judiciaire, s'est concrétisée par la création de services spécialisés au sein de l'Etat.

La création de services spécialisés au sein de l'Etat

L'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC) a été créé en 2000 (la première entité constituée remonte toutefois à 1996). Il est intégré au sein de la Direction Centrale de la Police Judiciaire (Ministère de l'Intérieur) et a pour vocation de lutter contre la cybercriminalité sur l'ensemble du territoire national. Il compte dans ses rangs à la fois des gendarmes et des policiers qui mettent en commun leurs compétences. Il est épaulé pour ce faire par la Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information (BEFTI) constituée en septembre 1994, placée quant à elle sous la direction de la Préfecture de Police de Paris.

Cette brigade, composée de policiers uniquement, a les mêmes compétences techniques, mais est limitée de plein droit quant à sa compétence territoriale à Paris et sa petite couronne.

La Direction Centrale du Renseignement Interieur (issue de la fusion entre la DST et la DCRG) dispose elle aussi d'enquêteurs spécialisés en criminalité informatique, dont le domaine de compétence concerne les services gouvernementaux, les établissements à régime restrictif ou encore tout ce qui concerne les données classifiées de défense, et plus généralement le domaine de la sécurité intérieure.

La gendarmerie pour sa part a créé dès 1998, au sein du service technique de recherches judiciaires et de documentation (STRJD), une division de lutte contre la cybercriminalité. Ses enquêteurs recherchent les infractions sur Internet (pédopornographie, vente de contrefaçons, recettes d'explosifs, haine raciale, etc.) et sont même autorisés depuis avril 2009 à conduire des cyberinfiltrations pour tromper la vigilance des pédophiles. Cette division conseille et aide aussi les unités territoriales confrontées à des affaires en relation avec Internet.

Il est utile de préciser que nombre d'autres services peuvent être amenés à participer à la lutte contre la cybercriminalité sans toutefois que ce soit leur objectif principal. Leur liste est trop importante pour être citée, et pourrait consister en l'annuaire complet des services de police et de gendarmerie, répartis sur le territoire national.

Il convient également de citer l'Institut de Recherches Criminelles de la Gendarmerie Nationale (IRCGN), reconnu pour son expertise grâce aux capacités mises en œuvre dans sa division « Ingénierie et numérique » ainsi que la Direction de la Police Technique et Scientifique de la police judiciaire, qui interviennent régulièrement en support technique de l'ensemble des autres services et dont les travaux permettent souvent de comprendre des technologies et techniques émergentes.

La formation des enquêteurs constitue une priorité du ministère de l'Intérieur qui abrite désormais les deux grandes directions que sont la DGPN et la DGGN. Les enquêteurs spécialisés en criminalité informatique (ICC : investigateur en Cyber Criminalité) sont aujourd'hui disséminés au sein de bon nombre de services sur l'ensemble du territoire national alors que pendant très longtemps les personnels des services parisiens ont été privilégiés pour bénéficier de telles formations.

Pour autant, l'Etat a compris également que de disposer de services chargés de la répression ne suffisait pas à assurer sa sécurité. Il s'est donc doté de services préventifs.

La menace sur les systèmes d'information et les moyens destinés à y faire face ont été pris en compte et exposés dans le Livre blanc sur la défense et la sécurité nationale, approuvé par le Président de la République en juin 2008.

Face à cette menace croissante et toujours plus insidieuse, le Livre blanc a souligné les défis à relever : doter notre pays d'une capacité de défense informatique active, apte à détecter et contrer les attaques ; étendre les réseaux sécurisés et résilients pour assurer la gestion des crises ; développer une offre de produits de très haute sécurité totalement maîtrisés pour protéger les secrets de l'Etat, et de produits et de services labellisés pour assurer la protection des domaines sensibles ; assurer la résilience d'Internet, désormais classé comme infrastructure vitale ; disposer d'une expertise de haut niveau dans tous les domaines des technologies de l'information, apte à conseiller les administrations et les opérateurs d'importance vitale ; enfin, participer à la diffusion de la sécurité dans la société de l'information.

C'est dans ce cadre et à cette fin qu'a été créée le 7 juillet dernier l'Agence nationale de la sécurité des systèmes d'information, l'ANSSI (héritière de la DCSSI). L'objectif est bien de concentrer les compétences les plus poin-

tues dans une agence unique à compétence nationale, pour mener à bien l'ensemble de ces projets. Un comité stratégique, constitué de responsables de haut niveau de l'administration, a été institué par le même décret pour préparer la stratégie de l'Etat en matière de cybersécurité.

De nombreux projets sont d'ores et déjà lancés, certains sont opérationnels, notamment le plus emblématique d'entre eux, qui a mobilisé d'importants moyens au second semestre 2009, la création d'une capacité centralisée de détection des attaques informatiques.

Le catalogue des produits de confiance labellisés par l'agence, (www.ssi.gouv.fr/labels) s'est fortement développé, avec le succès notamment de la certification de sécurité de premier niveau (CSPN). Il constitue un outil essentiel pour les acheteurs. De nombreux autres produits sont en cours d'évaluation.

L'ANSSI doit aussi relever deux grands défis prioritaires, qui mobiliseront des équipes de projets dans les années à venir, l'amélioration de la résilience des réseaux, notamment de l'Internet, et la sécurisation des infrastructures d'importance vitale.

Le Livre blanc appelait également une démarche de communication plus active, tournée vers la société de l'information. Vous avez sans doute pu noter une plus grande présence de l'agence dans les forums et les médias, ainsi que l'enrichissement de nos sites internet, notamment le portail gouvernemental de la sécurité informatique (www.securite-informatique.gouv.fr).

D'autres projets tout aussi ambitieux et passionnants vont suivre, dotant notre pays d'un dispositif adapté au défi majeur qu'il doit relever face aux menaces qui pèsent sur les systèmes d'information de l'Etat et des entreprises, et plus globalement, sur la société de l'information.

Pour mener à bien ses missions, l'ANSSI s'est structurée en quatre sous-directions :

- le centre opérationnel de la sécurité des systèmes d'information (COSSI), qui assure un service permanent de veille, de détection et d'alerte en cas d'incident ou de vulnérabilité susceptible d'affecter la sécurité des systèmes d'information ;

- la sous-direction stratégie et réglementation (SR), qui coordonne la mise en œuvre de la fonction d'autorité nationale dans le domaine de la sécurité des systèmes d'information ;

- la sous-direction assistance, conseil et expertise (ACE), qui apporte son concours et son expertise aux administrations et aux opérateurs d'importance vitale pour la sécurisation de leurs systèmes d'information, et élabore les recommandations générales, les référentiels techniques et les méthodes dans les domaines de compétence de l'agence ;

- la sous-direction systèmes d'information sécurisés (SIS), qui est chargée de la conception, de la réalisation et des évolutions des systèmes d'information sécurisés dont l'Etat a besoin.

L'agence comporte en outre un centre de formation, destiné à préparer les agents de la fonction publique, qu'ils soient informaticiens, experts en sécurité des systèmes d'information ou simplement utilisateurs, à assurer, chacun à leur niveau, la sécurité des systèmes d'information de l'Etat.

Pour diffuser les règles, les bonnes pratiques et les outils mis au point par l'ANSSI sur l'ensemble du territoire, et assurer la remontée des besoins et des difficultés rencontrés sur le terrain, des observatoires zonaux de la sécurité des systèmes d'information (OZSSI) ont été créés en 2009, en liaison avec le ministère de l'Intérieur, qui en assure le pilotage, à Paris, à Lille, à Rennes, à Bordeaux, à Marseille, à Lyon et à Metz, couvrant ainsi chacune des sept zones de défense métropolitaines.

Outre l'ANSSI, en France, d'autres organismes assure au profit de divers secteurs d'activités des services de prévention des risques et d'assistance aux traitements d'incidents : il convient de citer le CERT IST dédié au secteur de l'Industrie, des Services et du Tertiaire, créé fin 1998, mais aussi le CERT RENATER, en activité depuis 1995, dédié à la communauté de l'Enseignement et de la Recherche). Il existe d'autres CERTs français, privés.

De nombreuses actions de prévention et de sensibilisation des acteurs économiques

La politique de répression contre la cybercriminalité s'accompagne également de la mise en place d'un volet préventif, destiné à sensibiliser les acteurs économiques à cette menace.

Une préoccupation affichée des instances européennes et atlantiques

Cette nécessité a été soulignée par la Commission européenne dans une Communication au Conseil, au Parlement européen, au Comité économique et social et au Comité des régions : créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité (4). Le texte encourage les entreprises à mener directement des actions contre la criminalité informatique.

En mars 2004, un programme pluriannuel Safer Internet Plus (2005-2008), succédant au plan d'action Safer Internet (1999-2004), est doté d'un budget de 45 millions d'euros afin de lutter contre les contenus internet illicites et préjudiciables et de promouvoir une utilisation plus sûre d'internet et des nouvelles technologies en ligne, particulièrement pour les enfants. Les activités menées au titre du programme sont réparties selon plusieurs lignes d'action : lutte contre les contenus illicites, traitement des contenus non désirés et préjudiciables, promotion d'un environnement plus sûr, sensibilisation des consommateurs, protection des données et sécurité des informations et des

4/ Cf.: COM(2000) 890 final - Non publié au Journal officiel

réseaux (virus, spams, etc.).

L'Agence Européenne pour la Sécurité des Réseaux (ENISA), créée le 10 mars 2004 par un règlement du Parlement européen et du Conseil, est chargée de renforcer la capacité d'anticipation, d'examen et de résolution des problèmes rencontrés par les Etats-membres, les institutions communautaires et les entreprises en matière de sécurité des réseaux et des informations.

Lors de la réunion ministérielle de l'OCDE sur le futur de l'économie d'Internet, en juillet 2008, l'Organisation a affirmé sa volonté de travailler avec les pays développés et en développement ainsi que les organisations internationales pour améliorer les politiques à l'égard de l'économie Internet et accroître la coopération internationale sur des questions comme la cybercriminalité et la sécurité. Cette volonté se traduit, en particulier, par la rédaction de rapports, comme celui sur la menace des logiciels malveillants publié en juin 2008.

L'Organisation du Traité de l'Atlantique Nord (OTAN) s'est dotée, en avril 2008, d'une agence de recherche dédiée à la cyberdéfense « Cyber Defence Management Authority ». Basée à Bruxelles, la CDMA est chargée de coordonner les moyens de défense dans et entre les différents pays membres, qui veulent se protéger des attaques cybernétiques.

Une préoccupation intégrée par les pouvoirs publics

La prise en compte par les pouvoirs publics de la nécessité de mettre en œuvre une politique de sensibilisation des entreprises contre la cybercriminalité apparaît avec l'analyse des bouleversements introduits par Internet dans le monde de l'entreprise.

Ainsi, en 2002, le rapport Yolin inclut dans les adaptations juridiques nécessaires à l'usage d'Internet comme facteur de compétitivité des petites et moyennes entreprises la mise en place de moyens juridiques aptes à

5/ Rapport Yolin 2002 p : 256 Lien Internet : <http://www.ensmp.net/pdf/2001/&1028mirage2001.pdf>

6/ Cf. lien : http://www.lasbordes.fr/IMG/pdf/26_novembre_doc_definitif.pdf

7/ Cf. le site Internet du CLUSIF : <http://www.clusif.asso.fr/fr/production/ouvrages/type.asp?id=CYBER-CRIMINALITE>

lutter contre la cybercriminalité (5).

Le rapport du député Lasbordes (6), en date du 26 novembre 2005, et intitulé « La sécurité des systèmes d'information - Un enjeu majeur pour la France » traite des vulnérabilités qui affectent la sécurité de systèmes d'information des entreprises et des administrations, du fait de la malveillance d'acteurs économiques indelicats mais également celle induite par les NTIC.

Ce constat le conduit à écrire : « L'environnement lié aux technologies de l'information et de la communication est la cible de nombreuses menaces. L'ouverture des réseaux et leur complexité croissante associant des acteurs aux multiples profils, ont renforcé la vulnérabilité des systèmes d'information. Détruire, altérer, accéder à des données sensibles dans le but de les modifier ou de nuire au bon fonctionnement des réseaux, les motivations sont diverses et fonction de la nature des informations recherchées et de l'organisme visé. ». Soulignant que la sécurité des systèmes d'information est un véritable défi, à la fois technologique et économique, il formule 6 recommandations détaillées dans l'annexe n°2.

Une préoccupation relayée par les associations professionnelles

Les associations professionnelles se sont, dans le même temps, fortement impliquées dans la sensibilisation des entreprises à la prévention de la cybercriminalité. Ainsi, le Club de la Sécurité de l'Information Français, le CLUSIF, qui a pour mission d'agir pour la sécurité de l'information en direction des entreprises et des collectivités publiques, publie chaque année, d'une part, un « Panorama sur la Cybercriminalité »(7) recensant les grandes tendances de ce phénomène ainsi que ses nouvelles formes, et, d'autre part, un rapport sur « les menaces informatiques et les pratiques de sécurité en France »(8),

qui analyse les nouveaux risques informatiques, leur sinistralité, ainsi que les mesures permettant de les circonscire. Toutefois et au-delà d'un simple constat, le Club met à la disposition des entreprises différents outils pour améliorer la sécurité de leur système d'informations :

- des fiches pratiques pour les TPE-PME ;
- des recommandations abordant des questions aussi diverses que le retour sur investissement en matière de sécurité de l'information ou la sécurisation d'un Intranet ;
- des méthodes d'analyses de risque mise à jour annuellement, comme MEHARI.

Le Club Informatique des Grandes Entreprises Françaises, le CIGREF, accorde, de son côté, une place importante à la sensibilisation des entreprises dans la lutte contre la cybercriminalité : en 2008, ce Club a publié un rapport sur « Protection de l'information : Enjeux, gouvernance et bonnes pratiques ». Il propose une définition élargie de la protection de l'information comme « une démarche consciente visant à protéger, au sein de l'entreprise étendue, ce qui vaut la peine d'être protégé, tant au niveau des données que des supports d'information », impliquant « un système de gestion, une identification des informations sensibles, une analyse de risques, des acteurs, avec des rôles et responsabilités et un programme de réduction des risques » (9).

Dans ce document, les objectifs assignés à une politique de protection de l'information en entreprises sont les suivants :

- Protéger les actifs immatériels de l'entreprise ;
- Définir les orientations générales et les priorités ;
- Développer, mettre en œuvre et maintenir un référentiel de protection de l'information (politiques, rôles et responsabilités, processus, normes) ;

- Sensibiliser et éduquer le management/ les employés à tous les niveaux ;
- Identifier et traiter les faiblesses prioritaires ;
- Assurer la conformité et contrôler.

Une préoccupation prise en compte par les instances de normalisation

Au niveau européen, la Commission européenne a présenté, le 6 juin 2001, une communication proposant, notamment, un soutien des projets de normalisation et de certification orientés vers les besoins du marché.

La mise en œuvre de cette politique s'est notamment traduite par la création de l'European Telecommunications Standards Institute (ETSI), c'est-à-dire de l'Institut européen des normes de télécommunications. Basé à Sophia-Antipolis, cet institut est l'organisme de normalisation européen du domaine des télécommunications qui travaille actuellement sur la sécurité des réseaux, en coopération avec le Comité européen de normalisation (CEN) et le Comité Européen de la Normalisation Electrotechnique (CENELEC).

Cette volonté a été relayée par la prise en compte de la prévention de la cybercriminalité dans la normalisation de l'AFNOR. Le Référentiel des bonnes pratiques de l'AFNOR, d'août 2002, aborde la problématique de la sécurité des informations stratégiques – qualité de la confiance. Il propose 12 principes (10) destinés à préserver la confidentialité des informations, abordant la nécessité de délimiter un périmètre d'informations stratégiques à protéger, d'exploiter l'information librement disponible sur les marchés et la concurrence, de s'assurer un réseau de fournisseurs de confiance, de mettre en place des dispositifs de protection efficace reposant sur un personnel qualifié et sensibilisé, et d'analyser et d'exploiter tout incident éventuel (Cf. annexe n°1).

Quelques exemples d'actions prévues par le plan numérique 2012

- **Action 44** : Améliorer la confiance dans les services de communication et de partage en ligne en luttant contre les usages délictueux ou abusifs de ces services.
- **Action 45** : Missionner la CNIL pour qu'elle émette une recommandation au sujet de la protection des données liées aux plateformes, ainsi qu'à la suppression de vidéos atteignant à l'intégrité de la personne ou à caractère diffamatoire.
- **Action 76** : Déployer à partir de 2009, la carte nationale d'identité électronique, sur la base d'un standard de signature électronique fortement sécurisé, pour atteindre, à terme, un objectif de 100 % de citoyens titulaires d'une carte nationale d'identité électronique.
- **Action 78** : Développer l'usage de l'authentification pour le grand public.
- **Action 82** : Promouvoir la protection des données personnelles au plan international.

Le Plan Numérique 2012 vient asseoir le développement de l'économie numérique.

Ce plan, porté par le Secrétariat d'Etat chargé de la prospective, de l'évaluation des politiques publiques et du développement de l'économie numérique a été adopté en octobre 2008 (11).

154 actions regroupées dans quatre chapitres et une annexe s'intéressent aux fléaux numériques, aux architectures et technologies de sécurité (pourriel (spam), phishing, archivage, carte nationale d'identité, authentification forte et signature électronique (Transparence et confidentialité, droits d'auteur, pertinence,

- **Action 103** : Créer un référentiel des métiers du numérique

- **Action 114** : Développer le télétravail dans le secteur public

- **Action 124** : Prévoir et assurer l'archivage électronique des données et documents numériques.

- **Action 125** : Faciliter l'accès aux services de l'usager

- **Action 126** : Assurer l'interopérabilité entre administrations

- **Action 127** : Assurer l'accessibilité des sites de l'administration

- **Action 133** : Développer les services de télésanté et de bien-être

- **Action 154** : Fédérer nos partenaires européens autour d'une structure de gestion européenne de l'Internet des Objets (ou "racine ONS") et mettre en commun les programmes de R&D nécessaires à la création d'une architecture distribuée pour l'Internet des Objets en Europe.

etc...)). Ce document se veut être une démarche créatrice de confiance.

Les travaux de l'OCDE sur la sécurité de l'information et la vie privée

Un rapport a été rédigé au cours de l'année 2007 par le Groupe de travail sur la sécurité de l'information et la vie privée (WPISP, Working Party on Information Security and Privacy) de l'OCDE en partenariat avec le Groupe de pilotage sécurité et prospérité (SPSG, Security and Prosperity Steering Group) du Groupe de travail des télécommunications et de l'information (GTTEL) de la Coopération économique Asie-Pacifique (CEAP).

8/ Cf. le site Internet du CLUSIF : <http://www.clusif.asso.fr/fr/production/sinistralite/index.asp>

9/ Cf. site du CIGREF : http://cigref.typepad.fr/cigref_publications/2008/10/2008---protect.html

10/ Ces principes figurent en annexe de ce chapitre.

11/ <http://www.francenumerique2012.fr>

Ce document de 115 pages vise principalement « l'économie du maliciel » et recommande la mise en place d'une stratégie globale pour lutter contre les programmes informatiques malveillants («malware» en anglais), en passe de devenir une «menace sérieuse pour l'économie de l'internet». L'activité malveillante affecte selon le rapport tous les utilisateurs d'Internet, des entreprises au gouvernement ne passant par les simples internautes mais fait encore l'objet d'une «réponse locale fragmentée», estime l'Organisation de coopération et de développement économique (OCDE). Elle est aussi devenue « une industrie criminelle mondiale multi-millionnaire agissant dans l'ombre » souligne encore le rapport.

Selon l'OCDE, la «coopération internationale» est par conséquent «essentielle» pour lutter contre ce fléau, qui pourrait devenir «une menace sérieuse pour l'économie de l'internet et la sécurité nationale». Une large panoplie d'acteurs a un rôle à jouer dans le combat» contre

la cybercriminalité, assure l'organisation, et les rôles et responsabilités de chacun doivent être mieux définis.

«Alors que les gouvernements se reposent toujours plus sur internet pour fournir des services aux citoyens, ils sont confrontés à des défis complexes» pour protéger leurs systèmes et réseaux informatiques d'une attaque ou d'une intrusion.

Les Etats-Unis ainsi que plusieurs pays européens ont ainsi signalé l'an dernier avoir été la cible d'attaques par internet, en provenance de Russie ou de Chine. Le grand public et les entreprises sont aussi visés par ces menaces en ligne, qui vont du simple blocage d'accès à des ressources jusqu'au vol d'information et d'identité en passant par l'espionnage, voire l'extorsion d'argent (rançons). (Cf. Fig.1 ci-dessous). L'OCDE propose également plusieurs pistes d'action, parmi lesquelles une meilleure sensibilisation des

internautes, l'attribution de ressources plus importantes pour poursuivre les cybercriminels ou encore l'établissement d'un code de bonnes pratiques.

La Commission Nationale Informatiques et Libertés (CNIL) joue un rôle de conseil et de formation

La Commission Nationale de l'Informatique et des Libertés (13), autorité administrative indépendante est chargée d'assurer le respect des dispositions de la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004.

Cette loi impose un certain nombre d'obligations aux responsables de fichier, et notamment aux chefs d'entreprises.

- Notifier la mise en œuvre du fichier et ses caractéristiques à la CNIL, sauf cas de dispense prévus par la loi ou par la CNIL.
- Mettre les personnes concernées en mesure d'exercer leurs droits en les informant.
- Assurer la sécurité et la confidentialité des informations afin qu'elles ne soient pas déformées ou communiquées à des tiers non autorisés.
- Se soumettre aux contrôles et vérifications sur place de la CNIL et répondre à toute demande de renseignements qu'elle formule dans le cadre de ses missions.

l'application de la loi.

Les entreprises et les administrations recourent de façon croissante aux moyens informatiques pour gérer leurs ressources humaines. L'ensemble du secteur des RH est concerné : recrutement, gestion des carrières et des compétences, le suivi du temps de travail, etc....

Simultanément, les dispositifs de contrôle des salariés liés aux nouvelles technologies se multiplient : vidéosurveillance, cybersurveillance, applications biométriques, géolocalisation, etc.... Ces applications enregistrent de nombreuses informations à caractère personnel sur les salariés. La loi Informatique et Libertés fixe un cadre à la collecte et au traitement de ces données afin de les protéger, dans la mesure où leur divulgation ou leur mauvaise utilisation est susceptible de porter atteinte aux droits et libertés des personnes, ou à leur vie privée. Le respect, par les entreprises et administrations des règles de protection des données à caractère personnel est un facteur de transparence et de confiance à l'égard des salariés. C'est aussi un gage de sécurité juridique pour les employeurs qui sont responsables de ces traitements informatiques et de la sécurité des données personnelles qu'ils contiennent. Ils peuvent ainsi voir leur responsabilité, notamment pénale, engagée en cas de non-respect des dispositions de la loi.

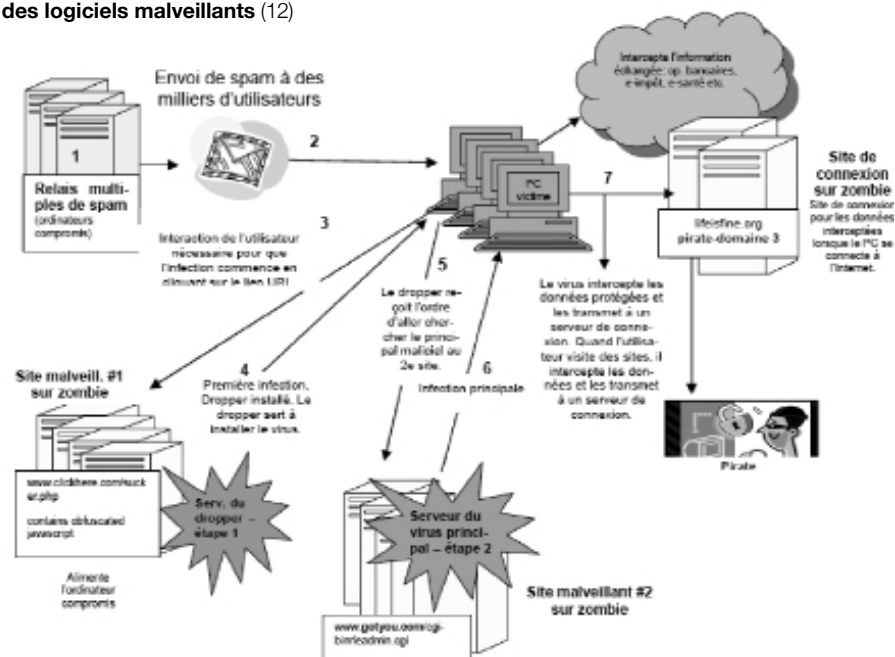
C'est pourquoi la CNIL est chargée de veiller au respect de ces principes et souhaite informer les salariés des droits dont ils disposent, ainsi que les employeurs, en les conseillant sur les mesures à adopter pour se conformer à la loi. Un guide (14) a pour vocation de leur donner les clés pour bien utiliser ces outils et les fichiers mis en œuvre en matière de gestion des ressources humaines. C'est aussi le but du « correspondant informatique et libertés », interlocuteur privilégié de la CNIL dont la désignation permet, au-delà de l'exonération de déclaration, d'intégrer pleinement la problématique de la protection des données personnelles.

En outre, les traitements les plus « sensibles » sont soumis à une autorisation de cette commission. Le non-respect de ces formalités par les responsables de fichiers est passible de sanctions administratives ou pénales.

Outre sa mission de contrôle, la CNIL conseille et renseigne les personnes et les organismes qui envisagent de mettre en œuvre des fichiers informatiques, que ce soit par téléphone, par courrier ou par ses publications. Elle s'est dotée d'un service d'orientation et de renseignement afin d'apporter une réponse rapide aux requêtes des particuliers comme des professionnels sur

12/ Source OCDE
13/ www.cnil.fr
14/ http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL_GuideTravail.pdf

Figure 1 :
Système de vol d'identité en ligne utilisant des logiciels malveillants (12)



Perspectives pour l'entreprise

Les Assises du numérique

Avec les Assises du numérique, qui se sont déroulées en juin 2008 (15), la France s'est dotée d'un cadre d'action de la politique publique en matière de lutte contre la cybercriminalité à l'horizon 2012. Son élaboration a associé les pouvoirs publics, les entreprises et plus généralement les différents acteurs du numérique, autorisant ainsi une approche globale de la criminalité sur Internet.

La lutte contre la cybercriminalité, avec neuf actions mêlant les approches répressive, pédagogique et de sensibilisation, est définie comme un domaine essentiel de l'action de l'Etat dans le secteur du numérique (Cf. Annexe n° 3). Les actions concernent la lutte contre la contrefaçon et les escroqueries sur Internet, l'accroissement des moyens affectés à la lutte contre la criminalité informatique, l'adaptation du droit à l'évolution de la fraude sur Internet, et des actions de prévention à l'égard des Internauts ainsi qu'une coopération renforcée entre les différentes administrations au niveau national et entre les différents Etats membres de l'Union européenne. **Les Assises du numérique font de la lutte contre la cybercriminalité une condition essentielle du succès de l'économie numérique française.**

15/ <http://francenumerique2012.fr/>

Plan de continuité : Essentiel à la protection d'activité

La capacité à garantir la continuité de leur activité est fondamentale pour les entreprises, mais aussi pour leurs clients et partenaires. Elle reste un problème récurrent, pas assez pris en compte et négligé en période de crise économique. Il s'agit pourtant d'un enjeu vital, au vu des systèmes d'information et des infrastructures correspondantes. En effet, une catastrophe majeure ne laisserait que 7% de chances de survie à l'entreprise non préparée, ayant eu la tentation de défier le hasard, pensant être en mesure de «se débrouiller» le moment venu, comme près de la moitié des PME!

Argumentaire

Depuis quelques années, des événements exceptionnels se succèdent en rappelant les vulnérabilités face à des catastrophes ou des sinistres de grande ampleur, dont les conséquences sont désastreuses au plan économique. Des cyber-attaques massives ont été vécues au niveau d'entreprises, mais aussi de nations entières, avec pour but essentiel : la déstabilisation, rappelant que les flux d'informations sont indispensables pour

l'activité, et que la concurrence est forte sur la scène mondiale.

Dans un contexte d'interdépendance, et par manque de diversité, les vulnérabilités sont communes et nombreuses. Par ailleurs, les risques à grande échelle sont sous-estimés, et la gestion des crises est délicate, en particulier en cas de scénario imprévu. Aussi, un dispositif de continuité est attendu. Sans être ni une «usine à gaz», ni une solution toute faite, il devra être adapté à l'entreprise et à son environnement, et assez souple pour faire face à l'imprévu, prendre des décisions et réagir très vite, alors que l'information est souvent incomplète et non vérifiée en cas de sinistre.

Le contexte paradoxal

Si la dépendance des organismes envers leur système d'information est largement reconnue, puisque 75% des répondants soulignent qu'elle est forte, avec des conséquences graves sur l'activité en cas d'indisponibilité jusqu'à 24 heures, il existe pourtant des disparités et incohérences dans la gestion de la continuité d'activité, tandis que 42% des entreprises n'ont toujours pas le moindre dispositif. Les motifs tiennent, soit à une surestimation de la complexité et du coût de mise en œuvre, soit à une sous-estimation ou un manque d'analyse du risque.

PRA versus PCA

«Plan de reprise» et «plan de continuité» ne sont pas des vocables interchangeable pour désigner approximativement une même chose. Ces appellations répondent à des besoins différenciés et sont à distinguer au regard de leur but. Un plan de reprise d'activité (PRA) (BRP-Business Resumption Plan) décrit la façon de reprendre les opérations dans les délais convenus jusqu'au retour à une situation normale, tandis qu'un plan de continuité d'activité (PCA) (BCP-Business Continuity Plan) décrit la poursuite

des opérations essentielles sans aucune interruption, par une disponibilité constante et en toutes circonstances de l'ensemble des ressources : techniques, infrastructures, information, compétences, etc. De fait, il y a lieu de réserver un PCA à un service ou un domaine qui nécessite des exigences très fortes, et un PRA à l'entreprise toute entière, sauf nécessité impérieuse, ou cas particulier.

Le dispositif est de la responsabilité de la direction générale et des cadres dirigeants, et pas uniquement de la direction des systèmes d'information (DSI). En outre, la gestion de la continuité est un principe structurant de la politique de sécurité du SI. Elle relève à la fois des activités et des opérations métiers, et des ressources en SI. Les DSI et les RSSI (Responsables de la sécurité des SI) auront un rôle stratégique mais également pédagogique pour changer les comportements et les croyances.

Le besoin de méthode

Il apparaît aussi que la vision reste réduite à la sauvegarde des données et aux moyens de secours informatiques au lieu de s'étendre aux domaines d'activité de l'entreprise, ce qui est impropre aux risques inédits et à grande échelle. De plus, les plans existants sont peu à jour, et mis à mal par des événements imprévus. En fait, la gestion d'un sinistre inédit présente certains aspects qu'il reste à expérimenter en pleine crise, laquelle pourrait être susceptible à l'extrême d'interdire l'accès au site pendant des jours, voire des semaines ou plus..., et de toucher un certain nombre de personnes-clés.

D'un côté, il existe des caractéristiques communes à prendre en compte : le caractère brutal avec pertes de repères, les défaillances multiples simultanées et les phénomènes en cascade. De l'autre, les pires scénarii sont très souvent écartés, jugés imprévisibles. Il faut donc se recentrer sur ce qui touche à l'activité et avoir une

approche systémique fondée sur les processus et leurs interactions, en s'appuyant sur une méthode, et en référence aux standards actuels.

Les standards actuels

Les standards actuels sont liés à la norme BS 25999 publiée par le British Standard Institute. Elle relève d'un besoin pressenti de standardisation des processus de management de la continuité d'activité. Elle s'adresse à toutes les entreprises, et pas seulement à celles opérant dans des environnements stratégiques à haut risque, tels que la finance, les télécommunications, et le secteur public. Elle comporte deux parties. La première est un guide de bonnes pratiques formulant des recommandations, et la seconde liste les exigences requises pour un système de gestion de la continuité basé sur ces pratiques.

Conclusion

La capacité de continuité d'activité ou de retour à une situation antérieure à un sinistre nécessite un dispositif éprouvé. Il s'agit d'éviter la faillite, en gardant en mémoire que la puissance d'une catastrophe majeure est sans rivale, avec peu de chances de survie s'il n'existait aucun plan à cet effet. Un tel dispositif de gestion de continuité est maintenant rendu obligatoire pour certaines entreprises. Il constitue la principale mesure de protection et reste un impératif pour toutes, qui auront à construire leur propre solution, en fixant leurs objectifs de continuité ou de reprise d'activité, ceci en menant également des actions préventives, en fiabilisant les processus et le système d'information lui-même.

Références

- Clusif (2003) : Plan de continuité d'activité – Stratégies et solutions de secours du SI, dossier technique, 58 p.
- Clusif (2006) : Politiques de sécurité des systèmes d'information et sinistralité en France. Bilan de l'année 2005, 58 p.
- Guinier D. (1995) : Catastrophe et management - Plans d'urgence et continuité des systèmes d'information. Ed. Masson, Paris, 336 p.
- Guinier D. (2007) : PRA/PCA : une obligation légale pour certains et un impératif pour tous. Legalis.net, Ed. des Parques, n° 2, ISSN 1626-7680, pp. 5-18

<http://www.bsigroup.com>
<http://www.thebci.org>
<http://www.drii.org>

Annexe n°1 :

Les 12 clés de la sécurité selon l'AFNOR

(D'après le Référentiel de bonnes pratiques de l'AFNOR - Août 2002 Sécurité des Informations Stratégiques – Qualité de la confiance. Comment préserver la confidentialité des informations)

- 1) Admettre que toute entreprise possède des informations à protéger (plans de recherche, prototypes, plans marketing, stratégie commerciale, fichiers clients, contrats d'assurance,...) ;
- 2) Faire appel à l'ensemble des capacités de l'entreprise (chercheurs, logisticiens, gestionnaires de personnel, informaticiens, juristes, financiers,...) pour réaliser l'inventaire des informations sensibles, des points faibles, des risques encourus et de leurs conséquences ;
- 3) Exploiter l'information ouverte sur l'environnement dans lequel évolue l'entreprise, observer le comportement des concurrents, partenaires, prestataires de service, fournisseurs, pour identifier les menaces potentielles ;
- 4) S'appuyer sur un réseau de fournisseurs de confiance pour ceux d'entre eux qui partagent ou accèdent à des informations sensibles ;
- 5) Ne pas chercher à tout protéger : classer les informations et les locaux en fonction des préjudices potentiels et des risques acceptables ;
- 6) Mettre en place les moyens de protection adéquats correspondant au niveau de sensibilité des informations ainsi classifiées, s'assurer qu'ils sont adaptés et, si besoin, recourir à des compétences et expertises extérieures ;
- 7) Désigner et former des personnes responsables de l'application des mesures de sécurité ;
- 8) Impliquer le personnel et les partenaires en les sensibilisant à la valeur des informations, en leur apprenant à les protéger et en leur inculquant un réflexe d'alerte en cas d'incident ;
- 9) Déployer un système d'enregistrement des dysfonctionnements (même mineurs), et analyser tous les incidents ;
- 10) Ne pas hésiter à porter plainte en cas d'agression ;
- 11) Imaginer le pire et élaborer des plans de crise, des fiches « réflexe » afin d'avoir un début de réponse au cas où... ;
- 12) Evaluer et gérer le dispositif, anticiper les évolutions (techniques, concurrentielles,...) et adapter la protection en conséquence en se conformant aux textes législatifs et réglementaires en vigueur.

Annexe n°2 :

6 recommandations du Rapport Lasbordes

Les six recommandations proposées correspondent à une double ambition : renforcer la posture stratégique de l'Etat en matière de TIC et de SSI et assurer la mise en œuvre opérationnelle des politiques et des décisions de l'Etat en matière de SSI. Certaines d'entre elles figuraient déjà dans le Plan de Renforcement de la Sécurité des Systèmes d'Information de l'Etat élaboré en 2004.

Axe 1 : Sensibiliser et former à la sécurité des systèmes d'information

- Organiser une grande campagne de communication s'inscrivant dans la durée à destination de tous ;
- Mettre en place un portail Internet pour mettre à la disposition des utilisateurs – citoyens, administrations et entreprises - des informations d'actualité, des guides de bonnes pratiques, des contacts, des alertes sur les menaces,...
- Proposer au système éducatif - du primaire à l'enseignement supérieur – et au système de formation continue, des canevas modulaires de formation en SSI ;
- Informer l'utilisateur : à l'instar du port de la ceinture pour l'utilisation d'un véhicule automobile, imposer que la documentation utilisateur qui accompagne les produits personnels de communication mentionne les risques principaux encourus vis-à-vis de la protection des informations, les points de vigilance pour l'utilisateur et les recommandations types à mettre en œuvre (exemple : activer un pare-feu, protéger et changer régulièrement son mot de passe,...).

Axe 2 : Responsabiliser les acteurs

- Etablir de manière obligatoire des chartes à l'usage des utilisateurs, annexées au contrat de travail – public et privé - ou aux règlements intérieurs des entreprises ;
- Labelliser les entreprises fournisseurs de produits ou services de SSI qui respectent un cahier des charges à établir.

Axe 3 : Renforcer la politique de développement de technologies et de produits de SSI et définir une politique d'achat public en cohérence

- Identifier les maillons des systèmes d'information qui exigent des produits qualifiés ;
- Etablir et tenir à jour un catalogue des produits de sécurité nationaux qualifiés et des produits européens adaptés aux différents niveaux de sécurité à assurer ;
- Développer les financements publics de R&D ;
- Favoriser le développement des PME innovantes dans la SSI et renforcer les fonds d'investissement en capital développement ;
- Développer la politique de certification et de qualification par une augmentation des produits certifiés et qualifiés et une réduction des délais et des coûts de certification ;
- Accroître la présence et l'influence française dans les groupes de standardisation et les comités de normalisation ;
- Définir et mettre en œuvre une politique d'achat public, fondée sur le principe d'autonomie compétitive. Inciter les grandes entreprises à travers le pacte PME à faire confiance aux PME certifiées en SSI.

Axe 4 : Rendre accessible la SSI à toutes les entreprises

- Inciter les entreprises à assurer leur SSI par la mise en place d'aides publiques ;
- Créer un centre d'aide et de conseil dans une logique de guichet unique ;
- Diffuser aux PME sous une forme adaptée les informations de veille, d'alerte et de réponse disponibles au niveau des CERT nationaux ;
- Initier et animer des forums thématiques publics – privés favorisant la circulation d'informations, les retours d'expériences, le partage des bonnes pratiques,...

Axe 5 : Accroître la mobilisation des moyens judiciaires

- Reconnaître la spécificité des contentieux liés aux systèmes d'information ;
- Aggraver les peines prévues au Code pénal en matière d'atteinte à la SSI ;
- Introduire une exception au principe d'interdiction de la rétro-conception dans le Code de la Propriété intellectuelle pour des motifs de sécurité ;
- Assurer la sensibilisation des magistrats et des forces de sécurité par la formation initiale et continue ;
- Constituer un pôle judiciaire spécialisé et centralisé de compétence nationale ;
- Renforcer les coopérations internationales.

Axe 6 : Assurer la sécurité de l'Etat et des infrastructures vitales

- Mettre à jour les politiques de SSI et les schémas directeurs de chaque ministère et les valider par une autorité centrale ;

- Conseiller en amont les maîtrises d'ouvrage de l'Etat pour des projets sensibles tels que par exemple la carte nationale d'identité ou le dossier médical ;
- Confier à une autorité centrale le rôle d'approuver formellement le lancement de ces projets sensibles ;
- Faire contrôler par une autorité centrale l'application de ces prescriptions par des inspections sur site et des tests d'intrusion sans préavis ;
- Mettre en place et animer une filière SSI transverse dans laquelle la mobilité sera organisée, tant à l'intérieur de la fonction publique qu'au travers de passerelles avec les entreprises et les centres de recherche ;
- Définir les profils de postes des responsables SSI. Renforcer leur autorité et leur responsabilité ; ils devront être indépendants des directions des systèmes d'information ;
- Pour les opérateurs d'infrastructures vitales : valider la politique de sécurité par l'autorité centrale et conduire des inspections et des tests d'intrusion ;
- Pour les entreprises sensibles, faire à la demande des audits et des tests d'intrusion.

Annexe n°3 :

Les Assises du numérique

Lutter contre toutes les formes de cybercriminalité

La France doit se donner les moyens de lutter contre toutes les formes de cybercriminalité, que ce soit celle de l'atteinte aux réseaux (piratage, intrusions sur les sites...) ou celle de l'utilisation des réseaux (contre-façon, escroquerie, pédopornographie, incitation à la haine raciale, propagande terroriste...).

Des efforts de coordination et de mutualisation, tant au niveau national qu'international, en matière de moyens mis à disposition et d'investigations effectuées dans ces domaines par la police et la gendarmerie nationales, ainsi que par les douanes ont déjà été initiés. Ces moyens doivent être renforcés et adaptés. La coordination internationale doit être accrue.

Ainsi, en termes d'organisation, les prérogatives de certains organismes pourront être revues et étendues pour prendre en compte de nouvelles formes de cybercriminalité, comme la multiplication des délits de contrefaçon sur Internet. Par ailleurs, la France doit jouer un rôle moteur dans la coordination internationale des moyens de lutte contre la contrefaçon, en particulier sur Internet et prendre une initiative forte dans ce domaine à l'occasion de la présidence française de l'Union européenne.

Action n°83 : Accentuer la lutte contre la contrefaçon vendue sur Internet.

Adopter dans le cadre de la présidence française de l'Union européenne un plan intégré européen de lutte contre la contrefaçon, comprenant la lutte contre la contrefaçon vendue sur Internet, décliné au plan national à compter du 1^{er} janvier.

Action n°84 : Créer un groupe spécialisé sur les escroqueries sur Internet,

assurant la centralisation opérationnelle des enquêtes et moyens, au sein de l'Office central de lutte contre la criminalité liée aux technologies de l'information (OCLCTIC). De même, les outils statistiques de pilotage et de suivi, utilisés par la police et la gendarmerie nationale, doivent désormais prendre en compte les infractions constatées sur Internet.

Action n°85 : Développer, dans le cadre du projet Ardoise (Application de recueil de la documentation opérationnelle et d'informations statistiques sur les enquêtes), un outil de connaissance des statistiques

des infractions relevant de la "cybercriminalité". Enfin, parce que le volume des infractions constatées progresse d'année en année, il convient d'affecter plus d'effectifs à la lutte contre la cybercriminalité.

Action n°86 : Doubler d'ici à 2012 le nombre d'enquêteurs spécialisés en criminalité informatique dans la police nationale, la gendarmerie nationale et les services des douanes. Sur le plan juridique, la France doit également continuer à se doter d'outils adaptés, en matière de définition des délits et ou de sanctions.

Action n°87 : Introduire à l'occasion de la loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI) :

- Un délit d'usurpation d'identité sur les réseaux de communications électroniques ;
- Une disposition permettant, en accord avec les fournisseurs d'accès Internet, de bloquer sur signalement des sites pédopornographiques ;
- Des peines alternatives d'intérêt général pour les hackers condamnés sans intention de malveillance. Ces moyens juridiques et policiers renforcés doivent par ailleurs s'accompagner d'une meilleure information du cybernaute de la loi et des risques encourus et aussi informer le public sur les moyens d'éviter tous ces risques.

Action n°88 : Créer d'ici à la fin de l'année, un site Internet de conseils pédagogiques dédié aux utilisateurs pour prévenir les infractions commises sur Internet.

Internet ne connaissant pas de frontières, la coopération internationale, notamment avec les partenaires européens de la France, doit être un pilier majeur de la lutte contre la cybercriminalité. Elle est déjà une réalité par l'har-

monisation progressive qui s'opère au niveau Européen, sur le plan législatif comme sur celui de la formation des forces de police des pays membres, en matière de lutte contre la cybercriminalité. Dans le cadre de la Présidence française de l'Union européenne, la France pourra proposer de mutualiser les efforts dans la lutte contre la cybercriminalité.

Action n°89 : Créer d'ici à 2009, une plate-forme européenne d'échanges d'informations sur la cybercriminalité et les sites illicites

dans le cadre d'Europol, à l'image de la plate-forme française d'harmonisation, de recueil, d'orientation des signalements (PHAROS), qui sera opérationnelle fin 2008. L'action publique doit s'appliquer à rendre les plus jeunes conscients des risques associés aux outils de communication de l'Internet. C'est l'objectif des campagnes de sensibilisation et de pédagogie que le gouvernement a mis en œuvre, à l'instar de l'initiative de la Délégation aux Usages de l'Internet, qui a créé en 2003 un site Internet destiné à prévenir les mineurs contre les risques de l'Internet. Ces campagnes de sensibilisation menées souvent par différents ministères, bénéficieraient d'une meilleure coordination.

Action n°90 : Coordonner des campagnes de sensibilisation portées par les différents ministères en lien avec la direction du développement des médias (DDM), le secrétariat général de la Défense nationale (SGDSN) et la délégation aux usages de l'Internet (DUI).

Au-delà des campagnes d'information, la protection la plus efficace consiste à former, très tôt, les plus jeunes aux nouvelles technologies, à les accompagner et à les aider à développer leur esprit critique dans l'utilisation du net. C'est d'ailleurs l'un des objectifs du brevet informatique et Internet (B2I), qui atteste de la capacité de l'élève à utiliser,

avec esprit critique, les outils multimédias et Internet. Cette dynamique doit être consolidée par un effort de formation plus important à destination des plus jeunes, notamment des enfants de moins de 12 ans. Il s'agit notamment d'améliorer la formation des jeunes à la citoyenneté sur Internet à travers les modules du brevet informatique et Internet (B2I).

L'Internet doit demeurer libre pour continuer de s'enrichir. Ceci implique aujourd'hui la présence de nombreux contenus à caractère choquant pour les publics non avertis. L'accès de tous à Internet porte la promesse d'un accès inconditionnel à la connaissance et à l'information. Il est donc nécessaire que les plus jeunes puissent consulter l'Internet en toute quiétude.

Les moyens de communication se développent à une célérité qui met à mal l'efficacité du législateur. La concertation en amont entre les différents acteurs est indispensable à l'établissement d'une situation optimale et équilibrée. Pour poursuivre pleinement ses objectifs, l'État doit donc favoriser l'auto-régulation des acteurs de l'Internet : par des chartes d'engagement, par une "softlaw" plus souple et plus apte à s'adapter aux incessantes évolutions technologiques, une ligne de conduite commune peut être dessinée, au profit d'un Internet respectueux de tous les internautes.

Action n°91 : Améliorer la lutte contre les spams.

Les opérateurs seront invités à travailler avec les pouvoirs publics pour améliorer les conditions dans lesquelles ils pourraient s'engager à limiter l'accès aux numéros et SMS surtaxés correspondant à des services frauduleux ainsi que la réception des messages ou appels provenant de ces numéros et les versements financiers associés.

POSTFACE

par Pascal LOINTIER,

Président du Club de la Sécurité de l'Information Français, CLUSIF
conseiller sécurité de l'information, CHARTIS

Après lecture de ce guide sur le risque numérique, vous n'êtes plus dans la méconnaissance des risques et des enjeux de continuité qu'ils constituent pour votre entreprise. Vous pouvez, toutefois, rester insouciant face au danger : un raisonnement probabiliste était d'usage avant 2001 ! Depuis, ces événements - New-York, Toulouse, les accidents aériens en série - ont provoqué une modification des comportements et la question posée est désormais la suivante : le scénario d'incident a-t-il un impact vital/critique pour mon entreprise ? Si la réponse est positive, il faut alors identifier une solution pour en réduire les conséquences : il s'agit bien de la survie de votre activité.

Agir au plus tôt, ce qui ne signifie pas dans l'urgence

L'incident, accident ou acte de malveillance, peut survenir à tout moment. Il n'y a donc aucune justification à retarder une action de réflexion quant à sa politique de sécurité. Insistons sur ce point car la dernière étude diligentée par le Clusif « Menaces Informatiques et Politiques de Sécurité en France » fait d'abord état d'un paradoxe : 73 % des PME interrogées estiment avoir une dépendance forte par rapport au système d'information... mais 39 % d'entre elles n'ont pas réalisé une analyse globale des risques auxquelles on pourrait ajouter 30 % ayant effectuées une étude partielle, donc potentiellement incorrecte ou négligeant un facteur de risque critique !

Faire un point de situation sur le niveau de sécurité

La première étape consiste bien à faire un point de situation sur l'état opérationnel des moyens déployés et l'application effective des procédures de sécurité et d'organisation. Quelle que soit la taille de l'entreprise et son allocation initiale de ressources, une analyse de risques est possible et doit être engagée. Pour cela, une PME peut se faire assister d'un consultant en sécurité des systèmes d'information (SSI). Il est important que cette « photographie » du système soit réalisée par un professionnel ayant une vision transversale des atteintes possibles et des scénarios d'incident. Un « intégrateur », fournisseur historique, un revendeur de produit de sécurité peut être très bon dans son domaine (serveurs performants, antivirus, pare-feu, moyen de sauvegarde) mais la sécurité du système d'information déborde largement la seule installation de produits. Il faut d'une part, prendre en considération tous les facteurs de sécurité ou toutes les déclinaisons de politiques de sécurité : sauvegarde, secours informatique, continuité des services, gestion des droits en interne et en télé-accès, départ du personnel stratégique, etc. et d'autre part, identifier les bonnes procédures de travail. En effet, la sécurité n'est pas systématiquement couteuse ou trop couteuse. Par une réorganisation du travail, on augmente considérablement son niveau de sécurité. Redisons-le car les mesures

sont insuffisamment appliquées par les PME, une politique de sauvegarde composée de cycle journaliers, hebdomadaires et mensuels garantit une meilleure intégrité des données. La conservation hors site des supports de sauvegarde, c'est-à-dire sur un autre site, garantit une meilleure disponibilité suite à un incendie ou un dégât des eaux. Le consultant SSI peut, en quelques jours et à la suite d'entretiens préparés avec les différents acteurs de l'entreprise, réaliser une telle analyse. On citera ainsi les actions de sensibilisation organisées par les Chambres de Commerce et d'Industrie en collaboration avec des prestataires régionaux. A l'issue de ce point de situation, un plan d'action, on parle de schéma directeur de la SSI, peut alors identifier les priorités d'action et la cohérence de déploiement des outils et surtout des procédures d'emploi.

Le tableau de bord d'impact, aide à l'évaluation des besoins

Une fois cette analyse des facteurs de risques ou des scénarios de dysfonctionnement, l'étape suivante concerne l'appréciation des enjeux ou des conséquences. Là encore, l'étude CLUSIF fait état d'une situation qu'on pourrait presque qualifier d'affligeante : 72 % ne procèdent pas à l'évaluation de l'impact financier des incidents de sécurité et, corollaire, 75 % n'ont pas de tableau de bord de sécurité informatique. On pourrait avancer des éléments d'explication (et non de justification...) : réaction psychologique et volonté d'amnésie suite à un événement déstabilisant, absence de savoir-faire quant aux poste de remboursement à mesurer. Pourtant, le tableau de bord, qu'il soit d'impact (suite à une crise) ou de sécurité (dans l'exploitation courante) présentera plusieurs avantages. D'une part, c'est un début d'appréciation du RoSI, le retour sur investissement de sécurité, pour analyser comment la sécurité a contribué au maintien de la productivité de l'entreprise. D'autre part, il permet d'identifier le montant

de capital garanti dans le cadre d'une assurance du système d'information. A ce titre, il est important de comprendre qu'une couverture d'assurance n'est pas une alternative à une politique de sécurité ou à la mise en place de moyens et procédures. Elle doit s'analyser comme un financement des frais de remise en état du système et un remboursement possible des préjudices économiques subits (pertes d'exploitations, frais supplémentaires, etc.)...

Gérer le comportement humain et non le facteur humain

On l'a vu, une bonne politique insiste sur des procédures adaptées non seulement aux exigences du métier (nature des équipements, délai de disponibilité, traçabilité réglementaire, etc...) mais aussi à l'environnement humain. Cyniquement, on pourrait mettre en avant la paresse humaine, cette propension naturelle à ne pas systématiquement respecter des mesures perçues comme rébarbatives ou encore les erreurs ou omissions dans l'exécution des dites procédures. C'est pourquoi, la règle, même formalisée, ne se suffit à elle-même. Il est très important de prendre en considération les habitudes initiales de travail, la perception des enjeux et les avantages à gagner pour l'utilisateur quant il respectera ces nouvelles mesures. En clair, une note de service, une charte de bonne conduite informatique ne sauraient suffire : il faut motiver / intéresser les utilisateurs (y compris les directeurs...) au respect des usages édictés. La psychosociologie est là pour nous démontrer comment l'individu, et sa prise de décision, est susceptible d'interagir ou d'être orienté par des informations transmises par son environnement son groupe d'activité. On découvre alors que l'être individu n'est pas un être de raison, de rationalité et que des techniques permettent l'orientation du comportement...

Mettre en place une dynamique

L'adaptation des moyens, la cohérence des pratiques et l'adhésion de l'utilisateur aux bonnes pratiques ne peuvent malheureusement suffire... l'entreprise évolue et son système d'information aussi. Une dépendance ou un impact plus fort suite à l'accroissement d'activité, une évolution des architectures informatiques avec de nouvelles menaces à prendre en compte et enfin, les rotations de personnels font qu'une démarche cyclique doit être mise en place. Nouvel audit pour apprécier l'augmentation du niveau de sécurité, reconfiguration des équipements et installation de correctifs de sécurité et sensibilisation des nouveaux salariés... toutes ces actions sont nécessaires pour que « numérique » soit associé à gain de production et non à risques...

Webographie

E-Sources :

ANSSI :

www.ssi.gov.fr

CIGREF :

www.cigref.fr

CNIL :

www.cnil.fr

La mission de la Délégation Interministérielle à l'Intelligence Economique :

www.intelligence-economique.gov.fr

INHESJ :

www.inhesj.fr

www.cahiersdelasecurite.fr

Portail de la sécurité informatique :

www.securite-informatique.gouv.fr

www.nouvellesmenaces.eu

Portail du CLUSIF :

www.clusif.fr

Documentation

<http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=FRE>

www.telecom.gouv.fr/fonds_documentaire/rapports/cybercriminalite.pdf

<http://assembly.coe.int/default.asp>

[www.internet-signalement.gouv.fr/PortailWeb/planets/AccueilInput.action](http://internet-signalement.gouv.fr/PortailWeb/planets/AccueilInput.action)

http://cigref.typepad.fr/cigref_publications/2008/10/2008---protecti.html

www.clusif.asso.fr/fr/production/sinistralite/index.asp

www.clusif.asso.fr/fr/production/ouvrages/type.asp?id=CYBER-CRIMINALITE

www.clusif.fr/fr/production/ouvrages/pdf/PanoCrim2k8-fr.pdf

Rapport Yolin 2002 p 256

<http://www.ensmp.net/pdf/2001/&1028mirage2001.pdf>

Rapport Lasbordes - La sécurité des systèmes d'information Un enjeu majeur pour la France - novembre 2005

www.lasbordes.fr/article.php3?id_article=166

www.lasbordes.fr/IMG/pdf/26_novembre_doc_definitif.pdf

Plan de développement de l'économie numérique

www.francenumerique2012.fr

Guide pour les entreprises et les salariés - CNIL

www.cnil.fr/fileadmin/docume...blications/CNIL_GuideTravail.pdf

Autres sites pour en savoir plus :

Guide de l'Intelligence économique en Suisse occidentale

<http://campus.hesge.ch/areso/files/guide.pdf>

DCRG - Intelligence économique défensive :

Physionomie nationale du risque financier - novembre 2006

www.intelligence-economique.gouv.fr/IMG/pdf/Physionomie_nationale_du_risque_financier.pdf

Les normes de sécurités :

<http://www.iso.org/iso/fr/home.htm>

et notamment les normes suivantes :

ISO 13335 Gestion de la sécurité des TIC

ISO 15408 Evaluation de la sécurité des TIC

ISO 27001 Certification de la qualité des pratiques

ISO 27002 Code de bonne pratique pour la gestion de la sécurité de l'information, etc.

Blog de Jean-Paul Pinte

Jean-Paul Pinte vous invite à suivre l'actualité sur son blog :

<http://cybercriminalite.wordpress.com/>

Les soutiens de nos partenaires

Les services de Gendarmerie

Plusieurs dispositifs cohabitent au sein de la Gendarmerie pour la lutte contre la cybercriminalité : IRCGN, STRJD, SR, N-Tech. Bien qu'ils semblent nombreux, ils ont chacun leur spécialité et travaillent en collaboration.

IRCGN (Institut de Recherches Criminelles de la Gendarmerie Nationale)

Implanté à Rosny-Sous-Bois depuis 1987, l'IRCGN est un laboratoire de police scientifique. Ses deux missions : l'expertise scientifique (toxicologie, incendie, biométrie...) et la mise à disposition de spécialistes dans le cadre d'enquête; puis surtout l'anticipation des futures évolutions de la criminalité et la façon de les contrecarrer. Depuis 1992, la structure accueille le département Informatique & électronique divisé en quatre unités :

une de recherche et développement, et trois unités d'expertises (traitement de l'information, réseaux & télécommunications, et électronique).

STRJD (Service Technique de Recherches Judiciaire et de Documentation)

Créée en 1976 et implanté à Rosny-Sous-Bois, le STRJD met en corrélation tout les événements trouvés au cour de différentes enquêtes afin de les accélérer. Cinq divisions composent le STRJD, dont la DLCC (Division de Lutte Contre la Cybercriminalité) créée en 1994 qui regroupe deux départements principaux : la DSI (Département de Surveillance de l'Internet) et le DRAMI (Département de répression des atteintes aux mineurs sur Internet) dont le CNAIP (Centre National d'Analyse des Images Pédo-pornographiques) répertorie 24h/24 toutes les images pédo-pornographiques. Les autres divisions travaillant en relation avec la criminalité numérique coopèrent donc toujours avec la DLCC.

SR (Section de Recherche)

Les sections de recherche (SR) apportent expertises techniques et scientifiques (recherche de preuves) dans le cadre d'enquêtes. Depuis l'avènement d'Internet le nombre de leurs missions s'est réellement accru et leurs expertises sont demandées surtout en matière de criminalité numérique (analyse de disques durs ...).

N-Tech

Depuis 2001, des enquêteurs des sections et brigades de recherche sont formés aux nouvelles technologies au CNFPJ (Centre National de Formation de Police Judiciaire), à l'IRCGN et à l'université. Ils apprennent à décortiquer les disques durs, les données, la programmation, la cryptologie etc. Leur rôle est d'assurer l'expertise et l'analyse de la criminalité numérique au niveau régional. Leurs missions se recentrent autour des affaires de pédopornographie à l'échelle régionale (prérogatives initiales), comme à l'échelle nationale, voire dans des affaires internationales. Leurs enquêtes proviennent souvent de commission rogatoires, ou de demandes d'expertise. Néanmoins, les N-Tech effectuent un travail de veille avec des logiciels spécialisés comme l'IRCGN et le STRJD, ce qui leur permet parfois de lancer des enquêtes d'initiative, après bien sûr avoir retransmis l'information auprès des services de l'IRCGN, du STRJD et de l'OCLCTIC.

Pour satisfaire l'objectif de doublement du nombre d'enquêteur spécialisé, la gendarmerie a conclu un partenariat avec l'université technologique de Troyes. Au plan local, les N-Tech initient à la spécialité des « correspondants » dans les brigades afin qu'ils puissent conduire les enquêtes de base.

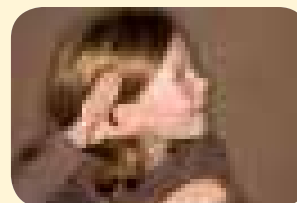


SPIE Communications Les entreprises et la cybercriminalité



Acteur majeur en matière de services « informatique, réseaux & télécoms » en France, SPIE Communica-

tions se positionne au cœur de la convergence voix-données et comme l'une des premières Sociétés de Services en Informatique au travers de son activité d'infogérance autour des Postes de travail et des Serveurs. Le chiffre d'affaires 2007 de SPIE Communications est de 285 M€. SPIE Communications focalise sa croissance sur le « service de proximité », en privilégiant, sur le terrain, réactivité, fiabilité technique et satisfaction maximale de l'utilisateur final. Aujourd'hui, SPIE Communications compte 66 700 clients en France et emploie plus de 2000 personnes réparties sur 6 directions régionales.



SPIE Communications a développé une réelle expertise dans le domaine de la sécurité et exerce aujourd'hui ses

compétences dans tous les domaines informatiques : contenu, communication, accès, sécurité des postes de travail, gestion des identités, Network Access Center (NAC), ... et propose une offre de service étendue allant du conseil à l'infogérance en passant par l'intégration, l'hébergement et les services managés

Cette expertise se traduit par un programme rigoureux de formation et plus de 50 certifications réparties sur l'ensemble du territoire prévues en 2009.

Afin de répondre aux fortes contraintes juridiques auxquelles sont soumis nos clients, SPIE Communications a développé une spécialité dans les domaines de la gestion de logs et du NAC sur lesquelles nous avons effectué de très belles réalisations et investissons massivement. Notre service de veille permet également d'anticiper les changements technologiques et d'avoir une approche pragmatique sur des sujets comme le DLP ou les problèmes de sécurité liés à la voix sur IP.



Présent sur les principaux événements autour de la sécurité, SPIE Communications, au travers de sa direction régionale Nord Est, a choisi le salon de la Cybercriminalité pour venir à la rencontre des utilisateurs et intervenir sur différents sujets dont le nomadisme.

Sur le stand, des démonstrations interactives seront organisées autour de :

- La gestion de logs,
- La sécurisation des réseaux Wi-Fi,
- La sécurisation du poste de travail,

La direction régionale Nord Est a en effet décidé de faire de la sécurité des systèmes d'information un de ses axes majeurs de développement en 2009 en créant un pôle sécurité et en consolidant son offre de conseil. Nous réalisons notamment des prestations de prédiagnostic de sécurité, d'aide à l'élaboration de politique de sécurité, d'audits de vulnérabilité, mais également de la conduite du changement, des études d'opportunité, de faisabilité ou d'homogénéisation du système d'information.



Thales

Cybersécurité : Protection des systèmes d'information et résilience des organisations

L'exposition des applications critiques aux cyberagressions s'est accrue dans des proportions exponentielles avec l'ouverture des systèmes d'information et le développement des menaces polymorphes. Au-delà de l'indispensable rappel aux bonnes pratiques, il nous faut imaginer de nouveaux modèles de systèmes d'information intrinsèquement sécurisés et forger de nouveaux concepts d'organisations résilientes.

En ouvrant leurs systèmes d'information au grand public, fournisseurs et partenaires dans un environnement de nomadisme et de mutualisation des données, les organisations ont franchi un point de rupture entre leurs dispositifs traditionnels de protection et les risques encourus.

Il est urgent d'appliquer toutes les règles déjà définies et de les appliquer sans faille. L'écart entre les pratiques d'une part et les standards et référentiels d'autre part constitue à lui seul un gisement de sécurisation qui est à la fois important et facile d'accès. Les actions d'audit, de sensibilisation et de formation sont, dans ce contexte, de nature à faire baisser rapidement le niveau de risque.

Cependant il serait faux de penser que les actions offensives sont toujours effectuées par des individus à l'extérieur des organisations. Bien au contraire, les études montrent que la majorité des dommages sont déclenchés au sein même des entreprises ou des administrations.

Et tandis que s'accroît l'exposition des réseaux aux menaces d'intrusion, les risques encourus s'étendent à l'ensemble des fonctions qui, de plus en plus, s'y concentrent. Très économique, la téléphonie sur IP mutualise les réseaux entre l'informatique et les télécommunications, exposant ces deux fonctions vitales au déni simultané des services vocaux et des services de données.

Les nouveaux concepts de sécurisation des systèmes d'informations devront donc s'élaborer à deux niveaux, celui de la réduction des risques et celui de la résilience face aux chocs extrêmes.

Il est clair que les nouveaux défis de la sécurité sont des défis de créativité. Ici comme ailleurs l'innovation viendra des rapprochements, entre le civil et le militaire d'une part, entre le public et le privé d'autre part. On ne saurait trop encourager le partage des

approches méthodologiques (EBIOS, Critères communs, ...) ainsi que des outils et produits, mais aussi le renforcement mutuel des capacités d'analyse de flux.

A la transversalité institutionnelle doit correspondre une transversalité dans les organisations. La sécurité est aujourd'hui une contrainte dispersée dans de multiples fonctions. Très rares sont les organisations qui en individualisent la responsabilité globale. Celle-ci devrait être assumée par un directeur de la sécurité, rattaché à la direction générale comme toute fonction vitale ou stratégique et interlocuteur des pouvoirs publics.

Enfin, le moment est venu d'élargir le concept de résilience. Bien au-delà de la seule capacité des systèmes à fonctionner en cas de panne, il faut l'étendre à l'organisation elle-même pour la rendre capable de « manager la surprise ». Il conviendra donc de rapprocher deux fonctions trop souvent distantes, celle qui s'engage sur la continuité d'activité et celle qui anticipe la gestion des crises.

Reste à positionner sur le marché de la sécurité des systèmes critiques, des prestataires capables de mobiliser en leur sein des équipes pluridisciplinaires de consultants, d'architectes systèmes et d'ingénieurs pour proposer une approche à la fois technique et organisationnelle et fédérer le meilleur des quatre mondes, civil et militaire, public et privé.

Thales a pris l'initiative dans ce domaine en créant ISS, Information System Security qui réunit l'ensemble des compétences du Groupe en matière de sécurité.

Dans cette organisation, Thales concentre toute l'expertise sécurité, à la fois sur le conseil (Connaissance des normes et standards, audits, test de pénétration, ...), les technologies (cryptage, télécommunications sécurisées, signature électronique, ...) et les services.

Le Groupe consolide une approche de bout en bout de la sécurité qui couvre l'ensemble d'une chaîne « Secured by Thales » :

- analyse du contexte : identification des menaces, contraintes et règles applicables
- analyse des risques : risques acceptables, niveau de sécurité à atteindre
- conception sécurité : design sécurité et recommandations
- développement ou acquisition des technologies de sécurité
- tests et audits de sécurité interne : test d'intrusion, résistance aux attaques
- évaluation du niveau de sécurité, en regards des normes du secteur : banque, défense...
- audit et certification : vérification des modifications demandées.

Bien qu'il soit souhaitable d'envisager la sécurité de manière globale dès le lancement d'un projet, la sécurisation peut être mise en œuvre sur des projets déjà existants et sur des points précis de la chaîne Secured by Thales.

Gérard PESCH

Directeur Security Consulting & Evaluation
THALES ISS

« Microsoft a pris depuis longtemps des engagements forts »

Notre monde numérique avance à pas de géant :

interconnecté, foisonnant, mobile, coopératif, à l'image d'un internet qui évolue sans cesse. Chaque jour, les technologies ouvrent des horizons nouveaux et le champ des possibles. Dans leur sillage, les interrogations sont nombreuses. Comment préserver la vie privée et garantir la sécurité des données ? Comment s'assurer que des technologies différentes dialoguent simplement dans un univers technologique si divers ? Comment faire d'internet un espace de confiance pour les enfants et les adolescents ?

Sur nombre de ces sujets, nous sommes parmi ceux qui pensent qu'une régulation est nécessaire. Mais parce que notre société numérique évolue à très grande vitesse, il est du devoir des acteurs économiques de prendre leurs responsabilités.

Sur chacun de ces enjeux : protection de la vie privée, sécurité des données, ouverture et interopérabilité, protection de l'enfance en ligne, Microsoft a pris depuis longtemps des engagements forts. Certains ont créé la surprise par leur ampleur et nombre d'entre eux ont été salués par la presse. D'autres sont encore méconnus. En tout état de cause, nous ne les considérons pas comme un aboutissement mais comme des étapes.

Car dans cet univers en constante évolution, tous les acteurs doivent, sans relâche et sans faux semblants, assumer leurs devoirs. Pour notre part, nous nous y engageons jour après jour avec tous ceux qui sont concernés : citoyens, pouvoirs publics, partenaires, associations professionnelles...

Pour plus d'informations, consultez nos sites :

<http://www.microsoft.com/France/apropos> et <http://www.microsoft.com/france/securete>

Microsoft

Profil Technology

"Le risque numérique vient aussi de l'intérieur"

Les entreprises sont généralement bien sensibilisées aux risques venant de l'extérieur (virus, malware etc.) et sont équipées en conséquence. Trop peu intègrent par contre la dimension interne du risque numérique et ses conséquences en termes de productivité, d'investissements superflus voire même légales.

Les risques pour les entreprises et les chefs d'entreprise sont pourtant nombreux et ont des **conséquences financières directes** ; qu'il s'agisse de perte de productivité, de surcharge de bande passante, du stockage de contenus illégaux sur les ordinateurs de l'entreprise ou d'interventions illégales sur des forums via le réseau de l'entreprise. Ces risques peuvent s'avérer très pénalisants et nécessitent une protection adaptée généralement pas ou peu gérée par les logiciels de sécurité classiques (anti-virus, anti-malware, etc.).

Quatre risques principaux peuvent être ainsi identifiés : la diffusion d'informations confidentielles, la surcharge de la bande passante, la perte de productivité et les contenus ou interventions illégaux.

La diffusion d'informations confidentielles

est souvent effectuée de bonne foi.

Elle peut notamment porter :

- sur l'envoi des coordonnées directes du dirigeant, provoquant ainsi de nombreux contacts téléphoniques à but commercial ;
- sur la diffusion par erreur de documents comptables (factures, bilans, etc.) ou commerciaux non-définitifs (tarifs, fiches produits, etc.) et pouvant se retrouver entre les mains de partenaires ou concurrents ;
- sur l'achat avec la carte bancaire de l'entreprise sans intention de nuire mais sans validation préalable, un problème devenu récurrent dans certaines entreprises ;
- etc.

La surcharge de la bande passante due à la consultation de vidéos en ligne (DailyMotion, YouTube, etc.), les téléchargements abusifs (P2P notamment), les jeux en réseau... impactent directement les ressources informatiques de l'entreprise et participent fortement à l'inflation des besoins d'investissements matériels dans ce domaine.

La perte de productivité liée à la consultation de sites extra-professionnels (voyages, bourse, réseaux sociaux, messageries instantanées, sites de recherche d'emploi, etc.) se voit peu en termes d'utilisation de la bande passante, mais un grand nombre d'heures de travail sont ainsi perdues chaque année. Ainsi, on estime que chaque employé peut perdre jusqu'à une journée de travail par semaine en activités extra-professionnelles sur Internet !

La détention ou la diffusion de contenus illégaux en passant par le réseau de l'entreprise peut également poser un problème de responsabilité légale au chef d'entreprise.

Afin d'établir un bon niveau de protection et améliorer les ratios coûts/rentabilité des ressources informatiques mises à la disposition de ses employés, le chef d'entreprise peut limiter ces 4 risques en mettant en place des solutions techniques adaptées. Celles-ci doivent permettre de filtrer les sites Internet accédés par les employés selon leurs besoins professionnels, d'interdire l'envoi de certaines informations et documents par email par certains groupes ou personnes, voire de limiter les contacts emails autorisés, d'interdire certaines applications ou types (vidéos ou exécutable par exemple), de disposer de rapports sur l'utilisation faite des outils informatiques à disposition des employés (attention, la déclaration à la CNIL est obligatoire dans le cas d'un stockage de données nominatives ou pour pouvoir être utilisé comme preuve juridique, l'employé doit également être prévenu de la mise en place d'un tel système) afin de pouvoir les consulter en cas d'activités illégales et de pouvoir adapter la solution aux utilisations particulières au sein de chaque entreprise.

Si des solutions existent, elles sont souvent mal adaptées aux problématiques des PME : produits souvent lourds à administrer ou appliances nécessitant une installation. Une solution logicielle au déploiement simplifié semble être la mieux adaptée à ces problématiques, car elle a l'avantage de la souplesse pour sa mise en œuvre au cœur de réseaux déjà existants, et permet une gestion directe depuis le poste du chef d'entreprise par exemple, sans forcément devoir passer par un administrateur réseau.

Pour plus d'informations sur les solutions proposées par Profil Technology à destination des entreprises, connectez-vous sur :

www.ProfilTechnology.com

PROFIL
TECHNOLOGY



Véritable **observatoire des pratiques et des risques liés à la sécurité de l'information**, le CLUSIF, Club de la sécurité de l'information français, agit pour sensibiliser tous les acteurs économiques et dans l'intérêt général des utilisateurs des systèmes d'information.

Ce Club professionnel est un lieu d'échanges où secteurs public et privé, monde de l'Education (2ème et 3ème cycles universitaires, Grandes Ecoles) et des fédérations professionnelles se rencontrent et mettent en commun leurs réflexions. Le CLUSIF intervient pour l'intérêt de tous dans des contextes très ouverts incluant la sécurité des réseaux, la lutte antivirus, les plans de continuité d'activité, la sécurité physique des centres informatiques, la malveillance téléphonique, le management des risques, le droit, la défense de l'information, la cybercriminalité...

Le mode de production repose d'une part sur l'organisation de conférences thématiques ouvertes au public et d'autre part, la constitution de Groupes de Travail dont l'objectif est la rédaction d'un document ou d'une prise de position publique.

De nombreux travaux sont issus réalisés, tous **gratuits et disponibles en téléchargement** et certains traduits en anglais : panoramas de la cybercriminalité, études sur les menaces informatiques et les pratiques de sécurité en France, synthèses, ouvrages de référence.

Le CLUSIF est aussi l'auteur de la méthode d'analyse de risques MEHARI™ qui permet de concilier les objectifs stratégiques des directions générales et les nouveaux modes de fonctionnement de l'entreprise avec un management des risques incluant l'analyse des vulnérabilités. C'est un excellent outil de contrôle et de gestion, à court, moyen ou long terme de la sécurité de l'Information de toute structure. La flexibilité de MEHARI™ permet de qualifier le respect de normes telles que ISO 2700x, ou de lois, telle que la Loi de Sécurité Financière. MEHARI™ constitue aussi un outil efficace pour traiter les risques opérationnels liés au traitement de l'information, tels que ceux décrits par la réglementation Bâle II pour les professions bancaires. MEHARI™ est totalement gratuit, à télécharger sur le site web de l'association.

En raison de la diversité de ses membres et de la variété des sujets traités en réunions ou en conférences, le CLUSIF est sollicité pour répondre à des consultations gouvernementales. Il participe ainsi à des travaux à caractère national ou international. L'association est également interviewée par des médias de la presse écrite, de la radio ou de la télévision pour fournir un décryptage des événements lorsque les journalistes veulent comprendre ou remettre en perspective un incident informatique qui défraie la chronique.

L'action d'intérêt général s'est aussi renforcée ces dernières années par la mise en place de portails : cybervictime, mastères SSI, CLUSIR et CLUSI notamment. Le portail cybervictime, réalisé en collaboration officielle avec les services d'Etat met à disposition un point de contact avec les services de Gendarmerie et de Police pour les Internautes ou les entreprises victimes d'une malveillance informatique. Le portail SSI, plus récent, a pour objet d'orienter les étudiants vers des mastères universitaires pour des études spécialisées en sécurité des systèmes d'information. Il sera prochainement complété par une rubrique d'offres et demandes de stages étudiants. Enfin, les portails CLUSIR (huit régions) et CLUSI (cinq pays) informent d'activités en région ou à l'étranger par des associations consœurs : prise de contact, documentations produites et l'annonce d'événements locaux.

www.clusif.asso.fr



La CNIL, un conseil en amont pour les entreprises innovantes

Afin de comprendre et d'accompagner le développement technologique et pour qu'il respecte au mieux les principes de protection des données, la CNIL entretient de nombreux contacts avec les entreprises du secteur privé qui conçoivent des nouvelles technologies et les conseille. De nombreuses actions ont été menées en 2008 : auditions en séance plénière d'industriels comme Orange, Auchan, Carrefour, Leroy-Merlin, HP et Métrobus ; visites d'entreprises, de centres de recherche ou de « showrooms » comme au CEA-Minatec de Grenoble, aux laboratoires de recherche d'HP à Bristol ou à l'Echangeur à Paris, ont été organisées avec des membres de la Commission. Au quotidien, le lancement de nouvelles offres est l'occasion pour des sociétés comme Microsoft, Google, Hitachi ou des compagnies d'assurance de venir présenter leurs produits à la CNIL. Lors de ces réunions, la CNIL est amenée à recommander des mesures techniques permettant une meilleure protection des données personnelles, dès la conception du système. Ces échanges permettent ainsi à la CNIL d'anticiper au mieux l'avènement des nouvelles technologies et de jouer un rôle essentiel en accompagnant ces entreprises afin que leurs innovations intègrent la protection des données. L'intérêt des entreprises est évident car elles gagnent ainsi la confiance de leurs utilisateurs.

La CNIL, un régulateur de la surveillance des salariés par les employeurs

Les dispositifs de contrôle des salariés liés aux nouvelles technologies se multiplient : vidéosurveillance, cybersurveillance, applications biométriques, géolocalisation. Ces applications enregistrent de nombreuses informations à caractère personnel sur les salariés. La loi Informatique et Libertés fixe un cadre à la collecte et au traitement de ces données afin de les protéger, dans la mesure où leur divulgation ou leur mauvaise utilisation est susceptible de porter atteinte aux droits et libertés des personnes, ou à leur vie privée. Le respect, par les entreprises et les administrations, des règles de protection des données est un facteur de transparence et de confiance à l'égard des salariés. C'est aussi un gage de sécurité juridique pour les employeurs qui sont responsables de ces traitements informatiques et de la sécurité des données qu'ils contiennent. Ils peuvent ainsi voir leur responsabilité, notamment pénale, engagée en cas de non-respect des dispositions de la loi. C'est pourquoi la CNIL est chargée de veiller au respect de ces principes et souhaite informer les salariés des droits dont ils disposent, ainsi que les employeurs, en les conseillant sur les mesures à adopter pour se conformer à la loi. Un guide a pour vocation de leur donner les clés pour bien utiliser ces outils et les fichiers mis en œuvre en matière de gestion des ressources humaines. C'est aussi le but du « correspondant informatique et libertés », interlocuteur privilégié de la CNIL dont la désignation permet, au-delà de l'exonération de déclaration, d'intégrer pleinement la problématique de la protection des données personnelles et de se prémunir contre de nombreux risques vis-à-vis de l'application de la loi.



INHESJ

L'INHESJ (Institut National des Hautes Etudes de la Sécurité et de la Justice), créé par le décret n°2009-1321 du 28 octobre 2009, est un établissement public national à caractère administratif placé sous la tutelle du Premier Ministre. Il est issu de la fusion de l'Institut National des Hautes Etudes de Sécurité (INHES) et de l'Institut d'Etudes et de Recherche pour la Sécurité des Entreprises (IERSE), préconisée par le rapport confié en août 2007 à Alain Bauer par le Président de la République sur la recherche et la formation dans le domaine des questions de sécurité et stratégiques.

L'INHESJ intervient dans les domaines de la formation, des études, de la recherche, de la veille et de l'analyse stratégique en matière de sécurité intérieure, sanitaire, environnementale et économique ainsi que dans ceux intéressant la justice et les questions juridiques.

Il a vocation à réunir des responsables de haut niveau, magistrats et cadres appartenant à la fonction publique civile et militaire ainsi qu'aux différents secteurs d'activité de la Nation, des États membres

de l'Union européenne ou d'autres États, en vue d'approfondir en commun leur connaissance des questions de sécurité.

Il s'attache également à promouvoir et à diffuser toutes connaissances utiles dans les domaines relevant de sa mission.

Au sein de l'Institut, le Département Sécurité Économique forme des directeurs et responsables de la sécurité/sûreté, de l'intelligence économique et du management de crises, et conduit une politique dynamique de recherche sur les thèmes liés à la sécurité/sûreté des entreprises et à l'intelligence économique.

Lieu d'échanges entre les administrations et les entreprises, ce département participe au débat et à l'approfondissement des savoirs sur la sécurité économique. C'est à ce titre qu'il s'intéresse tout particulièrement aux problématiques liées à la cybercriminalité.

Ce département dirige également une collection spécialisée permettant de nourrir la réflexion collective sur ces problématiques.

www.inhesj.fr



ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée par le décret n° 2009-834 du 7 juillet 2009 (Journal officiel du 8 juillet 2009).

Le Livre blanc sur la défense et la sécurité nationale, publié le 17 juin 2008, a mis en exergue l'importance de la cyber-menace. Il a retenu le risque d'une attaque informatique contre les infrastructures nationales comme l'une des menaces majeures des quinze prochaines années. Le développement de la société de l'information, l'utilisation croissante des réseaux dans les processus vitaux de l'État et de la société font de la prévention et de la réaction aux attaques informatiques une priorité majeure de nos dispositifs de sécurité nationale.

Le Livre blanc sur la défense et la sécurité nationale a souligné la nécessité de doter notre pays d'une capacité de défense informatique capable de détecter et de contrer les attaques les plus

subtiles comme les plus massives. Face à ce risque, il a identifié une série de mesures, dont la création d'une capacité de détection précoce des attaques informatiques, le recours accru à des produits et à des réseaux de haut niveau et la mise en place d'un réservoir de compétences au profit des administrations et des opérateurs d'infrastructures vitales. Ces missions sont confiées à la nouvelle Agence nationale de la sécurité des systèmes d'information (ANSSI), qui reprend également les missions de l'ancienne direction centrale de la sécurité des systèmes d'information (DCSSI). Cette agence est rattachée au Secrétaire général de la défense et de la sécurité nationale.

La création d'une Agence de la sécurité des systèmes d'information permet à la France de se doter d'une véritable capacité de défense de ses systèmes d'information. Elle sera l'instrument de la mise en œuvre d'une véritable politique de défense contre les attaques informatiques.

www.ssi.gouv.fr



1 - Déceler-Etudier-Former : une voie nouvelle pour la recherche stratégique. Rapprocher les institutions publiques chargées de penser la sécurité globale. Rapport remis le 20 mars 2008 au Président de la République et au Premier ministre. Supplément au n°4 des Cahiers de la sécurité, avril-juin 2008.

LEGALEDHEC

LegalEdhec est le Centre de Recherche de l'EDHEC dédié à la performance juridique. L'objectif principal de LegalEdhec est de réfléchir sur les modes de recours au droit par l'entreprise en vue de soutenir ou de créer des avantages concurrentiels. En d'autres termes, cela revient à déterminer la place que le droit devrait occuper dans la stratégie d'entreprise. L'une des idées-clef est que les entreprises doivent raisonner en terme de gestion juridique des risques, tout autant qu'en terme de gestion des risques juridiques. A cet effet, divers travaux sont menés par les membres de LegalEdhec, certains en partenariat avec des institutions extérieures. Ainsi, un ambitieux projet est actuellement développé avec l'Association Française des Juristes d'Entreprise (AFJE), sur le thème de la culture juridique d'entreprise.

LegalEdhec s'applique également à observer la performance juridique dans des domaines particuliers qui sont le droit de la concurrence, le droit de la propriété intellectuelle, la com-

pliance réglementaire, et l'économie numérique. Le choix de ces champs est certes lié aux expertises des membres du Pôle mais, de manière plus objective, ils correspondent également aux domaines de risque les plus fréquemment cités par les entreprises. Notre ambition est de réussir à faire reconnaître le caractère stratégique du recours au droit dans l'entreprise, à élaborer des critères de mesure de la performance juridique, et, le cas échéant, de proposer des évolutions législatives ou réglementaires lorsqu'il apparaît que la performance juridique passe actuellement par la transgression de la loi. Les travaux de LegalEdhec donnent lieu à de nombreuses publications et participations à des conférences, tant au niveau national qu'international.

Pour plus d'informations :

<http://www.performancejuridique.com>



L'I.R.E.E.N.A.T.

(Institut de Recherche sur l'Evolution de l'Environnement Normatif des Activités Transnationales), e.a. N° 3612 de l'Université de Lille 2, dirigé par le Professeur Jean-Jacques Lavenue, est spécialisé dans l'étude de la dimension publique de la mise en oeuvre de la réforme de l'Etat et des nouvelles technologies (e-administration, sécurité juridique et sécurité informatique, protection libertés). Cette équipe de recherche composée de juristes de droit public et de droit privé, d'informaticiens, et de politologues travaille actuellement dans le cadre de projets ANR à des recherches relative à la prise en compte de la dimension juridique de la mise en oeuvre des technologies de surveillance complexe (video, audio, interconnexion de fichiers),

notamment pour la protection de libertés et des données personnelles :

- Projet CanADA (Comportements anormaux: Analyse, Détection, Alerte);
- Projet Scarface (Caractérisation Sémantique de Visages pour la Recherche dans des Archives Video);
- Projet Smartvision (Système multi senseur de détection d'objets cachés pour une meilleure gestion du flux passager) de contrôles par par systèmes multi-senseurs (scanners corporels dans les aéroports) et les problèmes de protection des libertés.

La société OSIA est une société spécialisée en sécurité des SI, depuis sa création en 1991 à Strasbourg. Elle intervient dans l'analyse et l'audit de la sécurité, pour des expertises technologiques, et la conception de politiques de sécurité et de plans de continuité de divers secteurs stratégiques : télécommunications, finances, aéronautique, énergie, recherche, santé, etc., et enfin en matière d'intelligence économique.

Elle est dirigée depuis 1991 par Daniel Guinier, Dr. ès Sciences, consultant principal, certifié CISSP, ISSMP, ISSAP en sécurité des SI et MBCI en gestion de continuité, membre senior IEEE et ACM, et du New York Academy of Sciences. Il est expert OSEO/ANVAR depuis 1989, et expert judiciaire depuis 1991, avec de nombreuses expertises traitant pour la lutte contre la cybercriminalité. Il est lieutenant-colonel de réserve citoyenne de la Gendarmerie Nationale. Il a contribué à plusieurs normes internationales en sécurité : IEEE, NIST, et de façon significative à la protection du patrimoine informationnel,

la biométrie, la signature et l'identité électroniques, l'inforensique et l'archivage légal. Il a été ingénieur de recherche, au CNRS de 1967 à 1990, et entre temps, professeur à la US Naval Postgraduate School, puis PDG de la société OSIA dès 1991. Il est régulièrement conférencier en Europe et en Amérique du Nord, et enseigne en 3ème cycle aux universités de Compiègne (UTC-IMI) et de Strasbourg (IECS/IAE), et au CESSI (SCSSI/DCSSI) de 1992 à 1994. Enfin, il est l'auteur de plus de 200 publications et de deux livres : «Sécurité et qualité des SI» (Masson, 1991), «Catastrophe et management» (Masson, 1995), «Le courrier électronique et l'archivage légal» (IBM). Il est aussi coauteur de deux autres livres : «Les SI - Art et pratiques» - Sécurité et cybercriminalité (Eyrolles, 2002) et «Les tableaux de bord pour diriger en contexte incertain» - La sécurité des tableaux de bord (Eyrolles, 2004), et de «l'encyclopédie de l'informatique et des systèmes d'information» - La politique de sécurité (Vuibert, 2006).

Contact :
Mèl guinier@acm.org ;
Tél. 03 88 76 12 81.



Le Laboratoire de recherche en Ingénierie Pédagogique intègre aussi la dimension « Sciences de l'Information et de la Communication » et des travaux y sont menés autour de la place de l'individu dans la Société de l'Information, de la cyber-citoyenneté, de l'Intelligence économique et des outils de veille compétitifs qu'il convient dès aujourd'hui d'intégrer dans nos enseignements pour former les futurs travailleurs du savoir.

C'est à ce titre que ce laboratoire est aujourd'hui présent sur le terrain par ses écrits, ses enseignements, ses recherches et ses nombreuses conférences et interventions en France et à l'étranger.

Le laboratoire assure également en tant que cellule de veille l'animation de bulletins hebdomadaires d'informations sur ces problématiques à destination de publics professionnels. Le blog <http://cybercriminalite.wordpress.com/> animé par Jean-Paul Pinte, Docteur en Information Scientifique et Technique, enseignant-chercheur au sein du laboratoire et expert en veille et intelligence compétitive en est un exemple.

<http://www.univ-catholille.fr/>



L'Université Catholique de Lille rassemble, dans une dimension de visibilité, de mutualisation, de transversalité, d'interdisciplinarité et de synergie, 6 Facultés, 20 Grandes Écoles, Écoles et Instituts, 33 équipes de recherche, un groupe hospitalier de 700 lits, un institut de rééducation psychothérapeutique.

Ces établissements partagent avec leurs 20.307 étudiants en 2008-2009 une même philosophie éducative conjuguant excellence et humanisme, performance et solidarité. Ils inscrivent leurs actions au service de l'homme, de la société et du monde pour contribuer aux évolutions économiques et sociales.

Dans cet ensemble universitaire se côtoient aussi des équipes de recherche autour d'un conseil de recherche couvrant aujourd'hui 8 thématiques de recherche :

- la théologie,
- les lettres
- et sciences humaines,
- la médecine,
- les sciences,
- l'éthique,
- le droit,
- l'économie,
- l'ingénierie
- pédagogie.



L'ARIST Nord Pas de Calais, service de la Chambre Régionale de Commerce et d'Industrie (CRCI), accompagne les entreprises en matière d'intelligence économique, en leur proposant différents modes d'intervention selon leur besoin :

- Sécurité des systèmes d'information (pré-diagnostic SSI),



Le Service de coordination à l'intelligence économique

Le dispositif d'intelligence économique commun au ministère de l'Économie, de l'Industrie et de l'Emploi et au ministère du Budget, des Comptes Publics et de la Fonction Publique est placé sous l'autorité de Cyril Bouyeure, Coordonnateur ministériel à l'intelligence économique (CMIE). Rattaché au Secrétaire général des ministères, le CMIE anime l'action des différentes directions afin de mutualiser les compétences en matière d'intelligence économique.

Le CMIE dirige le Service de coordination à l'intelligence économique (SCIE) qui comprend un échelon central et un réseau de 23 Chargés de mission régionaux à l'intelligence économique (CRIE). Les missions du SCIE procèdent de 3 priorités :

- Sensibiliser et former les chefs d'entreprises à la démarche d'intelligence économique

Les actions de sensibilisation (réalisations et diffusions de supports d'information, formations, colloques...) couvrent les volets défensif (sécurité des systèmes d'information, protection de la propriété intellectuelle...) et offensif (démarches d'acquisition de l'information, utilisation d'outils numériques...). Ces actions ciblent en priorité les PME, moins sensibilisées et disponibles à ces enjeux. Les pôles de compétitivité, sources de développement technologique, sont par ailleurs accompa-

- Protection du savoir-faire (pré-diagnostic propriété industrielle et accompagnement à la mise en œuvre des outils de propriété industrielle),
- Suivi des évolutions et sécurisation des projets (prestations de veille)
- Prospective et développement de l'entreprise (méthode Casciopée)
- Recherche de partenaires (dans le cadre du Réseau Entreprise Europe notamment)

L'activité de l'ARIST s'inscrit dans le cadre du réseau des Chambres de Commerce et d'Industrie, certaines actions étant menées avec le soutien de l'État, de la Région et de l'Europe.

Contact : aristnpsc@aristnpsc.org
Tel. 03 20 63 68 00

gnés pour mieux connaître leur environnement concurrentiel international et se protéger contre toute intrusion extérieure non sollicitée. Une action est en cours sur la sécurisation de leurs plateformes électroniques d'échanges.

- Assurer la protection d'actifs stratégiques pour l'économie nationale

Au titre de la défense de ses intérêts économiques essentiels, l'État se doit d'assurer la protection et la défense du patrimoine technologique industriel national. Le réseau des CRIE participe aux actions de défense des entreprises sensibles dont les activités sont considérées comme stratégiques. De manière générale, le SCIE a une expertise sur les risques de dépendance dans le domaine des technologies de l'information et des nouveaux services numériques.

- Constituer une capacité de veille stratégique

Le SCIE mène une veille stratégique destinée à éclairer les menaces et opportunités, pour l'économie française, résultant des évolutions prévisibles de l'environnement concurrentiel. Les domaines d'investigation sont diversifiés : évolutions des politiques publiques et des stratégies des grands groupes internationaux, fonctionnement de certains marchés, veille technologique, suivi des pays émergents...



Service de coordination à l'intelligence économique

Caprioli & Associés

Fondé en 1995 par **Eric A. Caprioli**, avocat à la Cour de Paris, spécialiste en droit de la propriété intellectuelle et des TIC, Docteur en droit, le **Cabinet Caprioli & Associés** dispose d'une expertise juridique confirmée ainsi que de connaissances techniques poussées en matière de technologies de l'information et de la communication (TIC).

Basé à Paris et à Nice, le Cabinet Caprioli & Associés regroupe une équipe composée d'une dizaine de personnes ayant une formation juridique intégrant le droit des nouvelles technologies. En outre, qu'il s'agisse des responsables du pôle Sécurité et dématérialisation, du Pôle Vie privée et Données personnelles, du Pôle Informatique et Propriété intellectuelle et du pôle Droit public, chacun de ses membres enseigne depuis plusieurs années, et ce, notamment sur les aspects juridiques des TIC. Enfin, exerçant depuis sa création dans la sécurité de l'information et des questions connexes, le Cabinet Caprioli & Associés jouit d'une expérience reconnue dans ces domaines.

Le Cabinet intervient à titre principal dans des domaines d'activités couverts par une équipe d'avocats et de juristes hautement qualifiés, créatifs et spécialisés, soucieux de fournir des prestations de qualité, en consulting et accompagnement de projets liés notamment à la dématérialisation des échanges et au développement des TIC, en conseil juridique (par exemple, contrats, politiques, chartes informatiques, ...) et dans le domaine du contentieux et de l'arbitrage.

Les membres du Cabinet ont également développé une activité rédactionnelle florissante, auteurs appréciés d'articles et d'ouvrages techniques publiés et de documents en ligne sur le site du cabinet (www.caprioli-avocats.com). Afin d'honorer les demandes des organismes publics et des entreprises, ils participent à des conférences nationales et internationales, des colloques universitaires et organisent des sessions de formation juridique particulièrement adaptées aux attentes des professionnels.



Blandine POIDEVIN

Avocat au Barreau de Lille
3 rue Bayard 59000 LILLE
10 rue Weber 75116 Paris
Tel : 00.333.20.21.97.18
Fax : 00.333.20.63.22.25
Mail : bpoidevin@jurisexpert.net

Tiers-aviseur au CMAP
(arbitrage des «.fr»)

Le Cabinet de Maître Blandine POIDEVIN est inscrit au Registre des Représentants d'Intérêts de la Commission Européenne. Blandine Poidevin est partenaire du cabinet Arden du barreau de Californie, USA et du cabinet Langlais du barreau de Montréal.

A l'issue d'une formation en droit des affaires, elle s'est orientée vers un diplôme de propriété industrielle et de nouvelles technologies dès 1996.

A ce jour, elle a développé un domaine de compétences particulier en matière de droit des technologies. Elle accompagne des entreprises innovantes et des collectivités, au niveau Régional, National et International.

A ce titre, elle participe à des négociations, notamment en matière de contrats informatiques, et à la mise en place d'un cadre juridique respectant les normes les plus pointues en matière de sécurité informatique.

Elle enseigne des matières telles que la négociation des contrats informatiques, le droit du commerce électronique, auprès de l'Université de Droit de LILLE II, l'Ecole des Mines de DOUAI, l'ESC LILLE et l'IAE.

Elle dirige chaque année les travaux universitaires de plusieurs étudiants des masters professionnels 2e année. Elle est fréquemment consultée lors de la rédaction de décrets ou de projets de loi relatifs à son domaine d'activité.

Elle collabore régulièrement avec des organismes de formation internationaux, tels que REED BUSINESS INFORMATION, ainsi qu'avec des revues scientifiques autorisées, telles que EXPERTISES DES SYSTEMES D'INFORMATION.



s@ntinel

NOS OBJECTIFS

Dans un contexte de mondialisation et de développement d'Internet, la dépendance des sociétés à l'égard des technologies de l'information et de la communication (TIC) présente des risques potentiels que savent exploiter des délinquants et des criminels avertis et de plus en plus souvent organisés.

A l'initiative de la région de gendarmerie Nord-Pas de Calais, le Forum international sur la cybercriminalité a permis de mesurer l'intérêt de près de 600 participants pour les technologies numériques qui transforment notre vie quotidienne en offrant un espace de liberté et d'échanges sans précédent. Le 20 mars 2008, la deuxième édition du FIC a accueilli plus de 800 participants.

Devant les attentes des chefs d'entreprises, il a été décidé de relayer l'action de la gendarmerie et de poursuivre leur accompagnement par la création d'un pôle professionnel de lutte contre la cybercriminalité : S@NTINEL.

- Un site web et un blog (en cours),
- Des visites d'entreprises,
- Des conférences et ateliers thématiques,
- Un forum international sur la cybercriminalité...

LES PUBLICS CONCERNÉS

- Dirigeants d'entreprises,
- Pôles de compétitivité,
- Réseau consulaire,
- Directeurs des systèmes d'information,
- Responsables sécurité des systèmes d'information,
- Responsables de collectivité,
- Organisations professionnelles,
- Associations,
- Université, instituts de formation,
- Praticiens de la justice,
- Fonctionnaires des services compétents pour lutter contre la criminalité numérique de la région Nord-Pas-de-Calais, des pays voisins intéressés.

Une synergie internationale, une ambition collective.

ACTIONS

- Développer votre image et votre notoriété en vous associant à une action d'exception,
- Partager votre expérience avec les acteurs des TIC européens,
- Valoriser vos savoir-faire et produits lors de rencontres thématiques, ateliers et visites d'entreprises,
- Établir des contacts privilégiés avec les dirigeants ou responsables informatiques des entreprises,
- Offrir à vos cadres et à vos clients une formation et une information régulières,
- Promouvoir l'interopérabilité des équipements et des services sur le plan régional, transfrontalier et européen,
- Sensibiliser, former aux enjeux de la cybercriminalité,
- Accompagner les dirigeants d'entreprises dans les mutations de leurs systèmes d'information,
- Promouvoir des solutions techniques et comportementales,
- Promouvoir et renforcer la mise en réseau, l'échange et la diffusion de bonnes pratiques présentant un intérêt commun,
- Encourager la recherche scientifique et technique,
- Favoriser un échange entre les mondes des entreprises, les organismes publics, les professions de justice, le milieu associatif, le milieu universitaire,
- Faire évoluer les politiques nationales et européennes dans ce domaine.

Le cyberpôle professionnel d'excellence de lutte contre la criminalité numérique
128 ter, Grand Rue
59100 ROUBAIX



© Région de Gendarmerie Nord - Pas de Calais
Dépôt légal en cours
Achevé d'imprimer le 30 mars 2010
Imprimerie La Monsoise

Numéro ISBN : 978-2-11-099343-4



31 MARS
1^{er} AVRIL
2010
**LILLE
GRAND PALAIS**

4^e FORUM INTERNATIONAL SUR LA **CYBERCRIMINALITE**

Ensemble pour un espace numérique plus sûr !

2000 PARTICIPANTS
50 PAYS
30 CONFÉRENCES
SCIENTIFIQUES



Retrouvez ce guide en version numérique
sur www.fic2010.fr

Numéro ISBN : 978-2-11-099343-4