Encadrement des usages illicites

Nous partons des deux règles fondamentales suivantes :

Un abonné à Internet doit veiller à ce que sa connexion ne soit pas utilisée à des fins illicites
art. L.335-12 et L.336-3 du CPI,

Le chef d'entreprise est responsable vis-à-vis de ses préposés (salariés)
art. 1384-5 du Code Civil,

« Le chef d'entreprise, le maire d'une commune, le DSI ou le RSSI se trouvent confrontés à un arsenal de menaces venant de l'ensemble des usages illicites réalisés sur le système informatique à l'origine des malveillance, dont son principal risque est qu'il en sera pleinement responsable ».

A QUELLES MENACES LE RESPONSABLE DOIT-IL FAIRE FACE ?

Comme il vous l'a été présenté dans notre rubrique« Mises en conformité avec la CNIL», collecter, stocker, traiter… ne serait-ce qu'une seule donnée personnelle, permettant d'identifier une personne physique vous oblige à déclarer, demander un avis ou l'autorisation de la CNIL avant tout usage.

Usage àtitre personnel des outils numériques de l'entreprise

Depuis la mise en place de la loi Hadopi en 2006, les abonnés

à Internet étant surveillés par des outils automatisés à leur domicile minimisent les risques en réalisant leurs téléchargements illégaux sur leur lieu de travail.
Ainsi ce n'est plus la responsabilité individuelle des utilisateurs qui sera recherchée, mais la responsabilité pénale du chef d'entreprise, de l'élu en charge d'une mairie, du DSI ou du RSSI.

Consultation de sites malveillants

Les sites malveillants, qui sont consultés sans surveillance ou sans encadrement à titre personnel peuvent contaminer le poste de l'utilisateur, le système informatique de l'entreprise et les futurs correspondants contactés par e-mail à partir du système informatique contaminé.

Consultation de sites illégaux

Inutile de se protéger derrière le fait qu'on ne savait pas que le site était illégal (c'est comme posséder des contrefaçons), consulter de tels sites, souvent sous surveillance, rendent pénalement responsable pour complicité l'utilisateur. c'est la responsabilité du titulaire de l'abonnement à Internet (à partir de l'adresse IP) qui sera d'abord recherchée.

Téléchargement illégal de musiques ou de films

Tout comme la consultation de sites illégaux, c'est à nouveau le titulaire de l'abonnement à Internet (à partir de l'adresse IP) qui sera d'abord responsable.

Salarié mal intentionné

Selon une étude de Symantec sur les «Indicateurs de risques comportementaux des employés mal intentionnés en entreprise »,

30% des violations de données seraient le fait d’employés mal intentionnés.

Virus, SpyWares et AutresWares, Ordinateur hacké

Les PC zombis sont des ordinateurs connectés à internet qui sont infectés par des malwares. Ces derniers sont contrôlés par des pirates, en général, afin de :

- Envoyer des mails de spams qui pourront être utilisés pour effectuer des attaques de phising.
- Effectuer des attaques de type DDOS
- Scanner des réseaux via des PC du botnet afin de découvrir des vulnérabilités et effectuer des attaques.
- Propager de nouvelles infections.
- La machine étant à la merci des pirates, il est aussi possible de :
- Récupérer des mots de passe Paypal, jeux en ligne pour les revendre, éventuellement des comptes de forums, sites WEB ou autres si les sites peuvent intéresser le pirate,
- Installer des adwares qui vont ouvrir des popups de publicité afin de rémunérer les pirates via votre PC.
- Installer d’autres malwares (pour les faire rentrer dans un autre botnet) ou mettre à jour les infections pour échapper à la détection des antivirus.

QUELS RISQUES ET QUELLES PEINES ?

Loi Informatique et Libertés (LIL) n°78-17 du 6 janvier 1978 modifiée le 6 août 2004

La CNIL, autorité administrative indépendante française, est chargée de veiller à ce que l’informatique soit au service du citoyen et qu’elle ne porte atteinte ni à l’identité humaine, ni aux droits de l’homme, ni à la vie privée, ni aux libertés

individuelles ou publiques. Elle exerce ses missions conformément à la loi n°78-17 du 6 janvier 1978 modifiée le 6 août 2004.

Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.
La loi pour la confiance dans l'économie numérique n° 2004-575 du 21 juin 2004 (LCEN)

La LCEN est une loi française sur le droit de l'Internet, transposant la directive européenne 2000/31/CE du 8 juin 2000 sur le commerce électronique et certaines dispositions de la directive du 12 juillet 2002 sur la protection de la vie privée dans le secteur des communications électroniques. La transposition de la directive 2000/31 aurait dû être effective le 17 janvier 2002 mais ne l'aura été que le 21 juin 2004.

USAGES ENCADRES PAR CETTE LOI :

Publicité par voie électronique

Est interdite la prospection directe au moyen d'un automate d'appel, d'un télécopieur ou d'un courrier électronique utilisant, sous quelque forme que ce soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen.

Responsabilité des hébergeurs

Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas

voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible.

Cette loi pourra rendre également pénalement responsable les propriétaires d'ordinateurs de salariés mal intentionnés mais aussi d'ordinateurs hackés, agissant (envoyant des spams, propageant des virus) ou stockant des données à leur insu (documents, vidéo, musiques, photo illégales).
La loi relative au droit d'auteur et aux droits voisins dans la société de l'information
du 3 août 2006 (DADVSI)

La loi DADVSI est une loi française issue de la transposition en droit français de la directive européenne 2001/29/CE sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.

Le texte, publié au Journal officiel le 3 août 2006, prévoit des amendes d'un montant de 300 000 euros ainsi que 3 ans de prison pour toute personne éditant un logiciel manifestement destiné à la mise à disposition du public non autorisée d'œuvres ou d'objets protégés, et jusqu'à 6 mois de prison et 30 000 euros d'amende pour toute personne diffusant ou facilitant la diffusion d'un logiciel permettant de casser les mesures techniques de protection (DRM, pour Digital Rights Management) qui selon ses défenseurs visent à empêcher la contrefaçon.
Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet
n°2009-669 du 12 juin 2009 (HADOPI).

La loi Hadopi ou loi Création et Internet « loi favorisant la diffusion et la protection de la création sur internet1 », est

une loi française qui vise à principalement mettre un terme aux partages de fichiers en pair à pair lorsque ces partages se font en infraction avec les droits d'auteur.
Le 31 décembre 2009, la Loi Hadopi s'est vue complétée jour par la loi Hadopi 2 avec pour objectif de réintroduire le volet répressif de la première loi qui a été déclaré partiellement non conforme à la constitution par le Conseil Constitutionnel.

Le 13 mai 2013, Pierre Lescure, ancien patron de Canal+, remet un rapport à François Hollande, le « Rapport Lescure », dans lequel parmi les 80 recommandations formulées, on découvre la suppression de la Hadopi mais pas de la réponse graduée, la mise en place d'une nouvelle taxe sur les appareils connectés et l'augmentation de l'offre de vidéo à la demande.
La loi d'orientation et de programmation pour la performance de la sécurité intérieure
(LOPPSI) n° 2011-267 du 14 mars 2011 est une loi française qui concerne la gestion de la police et de la gendarmerie.
Elle couvre différents chapitres dont :

LUTTE CONTRE LA CYBERCRIMINALITÉ, INFORMATIQUE ET INTERNET

L'usurpation d'identité sur Internet sera un délit puni d'un an d'emprisonnement et 15 000 euros d'amende.

- Il sera possible d'imposer aux fournisseurs d'accès à Internet le blocage de sites Web publiant du contenu pédo-pornographique. Initialement, ce blocage pouvait être décrété par une autorité administrative, mais la commission des lois a imposé le passage par une décision de justice. Toutefois, en deuxième lecture, l'Assemblée nationale a de nouveau supprimé le contrôle du juge.
  Une liste noire des sites, non rendue publique, sera établie par l'administration, les FAI seront quant à eux tenus de bloquer l'accès à ces sites.

- Une obligation de filtrage des adresses IP désignées par arrêté du ministre de l'Intérieur
- La police, sur autorisation du juge des libertés, pourrait utiliser tout moyen (physiquement ou à distance) pour s'introduire dans des ordinateurs et en extraire des données dans diverses affaires, allant de crimes graves (pédophilie, meurtre, etc.) au trafic d'armes, de stupéfiants, au blanchiment d'argent, mais aussi au délit « d'aide à l'entrée, à la circulation et au séjour irrégulier d'un étranger en France commis en bande organisée », sans le consentement des propriétaires des ordinateurs.

QUELLES SONT LES SOLUTIONS A APPLIQUER POUR MINIMISER SA RESPONSABILITÉ ?

Mesure de l'existant
Généralement sous forme d'audit, cette étape permet de déterminer un état des lieux précis

- Traitements de données personnelles
- Présence de données illicites
- Relevés du trafic internet entrant et sortant
- Analyse des relevés

L'audit permet l'édition d'un rapport.
Son analyse et son interprétation permet d'identifier la présence ou non de données illicites à l'intérieur du système informatique et de lister des actions à mener.

Application de contre-mesures

La priorisation des actions amène tout naturellement le chef d'entreprise à agir face aux risques.
Il est rare que les données récoltées amènent jusqu'au

licenciement d’un salarié, mais la mise en place ou la mise à jour d’une Charte Informatique et la mise en place ou la mise à jour de moyens de blocage ou de filtrage permettent généralement de rendre quasiment sain un système informatique, réduisant par la même occasion les risques du chefs d’entreprise face aux risques venant de son système informatique.

Suivi

Les usages de l’informatique évoluent chaque année.
Chaque jour, des milliers de nouveaux sites voient le jour.
Chaque jour, Google identifie 9500 nouveaux sites internet infectés et 300.000 téléchargements risqués (Source : www.zdnet.fr).
Selon Sophos, en 2007 on dénombrait 29 700 nouveaux sites Web par jour et 80 % d’entre eux sont des sites Internet malicieux, copies de sites Internet de confiance.
En 2012, le nombre de plaintes en rapport avec les données personnelles a encore continué d’augmenter. D’après la CNIL, ces plaintes auraient augmenté de 5% en 2012. Du « droit d’oubli » au vol pur et simple de données privées, 6 017 plaintes ont été déposées l’année dernière. Cette hausse est une conséquence logique de la conjoncture actuelle, selon 01Net. Pour le site, l’explosion des télécommunications et du web ont fait que le vol de données est devenu « un sport national ».
Un suivi minutieux de l’évolution des usages de votre système informatique est un moyen supplémentaire pour garantir une réduction des risques du chef d’entreprise face à l’évolution des usages de l’informatique.