Cybersurveillance: quelle sécurité Internet en interne et en externe pour l'entreprise?

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

INTRODUCTION

- La sécurité informatique: quelques chiffres
- Internet a crée 700.000 emplois sur les 15 dernières années
- Parallèlement les cyber-attaques se sont multipliées, 5.000 sociétés sont attaquées chaque année en France.
- Les attaques contre les banques ont augmenté de 17% en 2010.
- En Hongrie, les pirates(ou hackers) se réunissent à Budapest pour parler de « *Hacktivity* »

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU-2012

La cubersurveillance en interne

- Définir le niveau de confidentialité que l'on veut dans l'entreprise

DEFINITIONS:

- Qu'est-ce qui est confidentiel, secret ou stratégique?
- Confidentiel: les données à caractère personnel, ex: les données sur les employés (nom et prénoms, santé, religion, etc..)

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

- Secret: cf le secret des affaires, article…. Code pénal ensemble des informations sensibles de l'entreprise: données sur fichiers clients, méthodes marketing, données sur le CA, sur les salaires etc…
- Le chef d'entreprise doit définir avec son département des réseaux et de la sécurité informatique quelles sont les données relevant du secret des affaires.

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

- Données stratégiques: données d'entreprises de secteurs sensibles comme le nucléaire, la défense nationale; les projets à court et moyen terme, les implantations nouvelles, les innovations, les brevets, les équipes etc..

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

I- La cybersurveillance en interne

A- Les obligations des employés

- Principe de loyauté: l'employeur est en droit d'attendre de l'employé qu'il exécute son contrat de travail de façon loyale. La protection de la vie privée ne crée pas une bulle d'immunité autour de l'employé.

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

Employé: que puis-je faire?

- Jouer en ligne au bureau ? NON illégal en entraine licenciement pour faute grave si jeu sur temps de travail et ordinateur de l'entreprise (cass. Soc, 14 mars 2000);
- Consulter des sites pornographiques: NON si consultation sur temps de travail et ordinateur de l'entreprise, entraine licenciement pour faute grave

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

- Dénigrer mon employeur par mail sur ordinateur de l'entreprise : NON, licenciement pour faute grave;

- Dénigrer mon supérieur hiérarchique: OUI si mail personnel sur ordinateur personnel adressé à un collègue sur boîte personnelle, Cass. Soc. 26 janv 2012

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

- Participer à un forum de discussion: non si usage de la messagerie professionnelle pour dénigrer son employeur
- Tenir un blog en ligne: oui si blog personnel en dehors des heures de travail sans dénigrement de l'employeur

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

Enquête: Blog et employés?

- Si les médias sociaux font désormais partie de la statégie des entreprises, 29% de celles-ci n'hésitent pas à bloquer leur accès au travail, et 27% à en monitorer l'usage. Tel est le constat que révèle la récente enquête « Réseaux sociaux sur le lieu du travail » (pdf) publiée par Proskauer, un groupe international d'avocats, qui a interrogé les dirigeants de 120 multinationales.

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

- **3/4 des entreprises utilisent les médias sociaux à des fins professionnelles**

- **76% des multinationales** interrogées affirment **les utiliser pour leur activité**,

- **Accès limité pour les employés**
- La majorité des entreprises interrogées ont tendance à restreindre, voire fermer l'accès aux médias sociaux :
  > **25% des entreprises** n'autorisent **aucun accès aux médias sociaux** pour des raisons non professionnelles
  > **26,7% autorisent seulement certains** de leurs employés
  Une pratique répandue dans de nombreux groupes, dont Porsche, Volkswagen ou Commerzbank, essentiellement pour des raisons de sécurité et de productivité.

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

Problèmes liés aux réseaux sociaux

- **43,6%** des entreprises interrogées, soit **presque 1 entreprise sur 2**, déclarent que **leur activité a dû faire face des mauvais usages des médias sociaux**. Et **31,3%**, soit près d'un 1/3, déclarent avoir déjà **pris des mesures disciplinaires à l'encontre d'un employé**, suite à des dérapages sur les médias sociaux.

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

- **29,3% des entreprises bloquent systématiquement tout accès aux médias sociaux** depuis les postes de travail, et que **27,4% déclarent en contrôler l'accès**.

- **Et en France**, avant de contrôler les contributions de ses employés sur les médias sociaux, une entreprise doit en informer les employés concernés sous peine de nullité, ainsi que la CNIL, afin de pouvoir enregistrer et archiver les contributions.

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

Attention: l'employeur peut être responsable du fait de son employé (article 1384 du code civil)

- Ex: blog personnel de l'employé crée avec l'ordinateur et les moyens de l'entreprise pour dénigrer entreprise tierce= responsabilité de l'employeur.

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

Importance de bien définir les règles de l'usage d'internet en interne

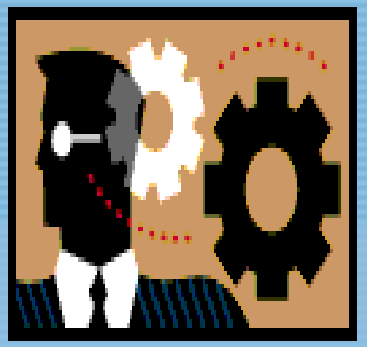
- 1) définir le caractère des données
- 2) le niveau de contrôle
- 3) le responsable du contrôle
- 4) qui peut faire quoi?
- 5) les sanctions en cas d'irrespect

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

B- Les obligations des employeurs

1- Préalable pour l'entreprise: établir une charte de confidentialité

- Cela vise les entreprises mais aussi les universités et les centres de recherche.
- Chaque employé doit signer personnellement cette charte pour qu'elle lui soit opposable.



Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

- Faire signer cette charte dès l'entrée en fonction de l'employé.
- Par sa signature, chaque employé reconnaît avoir été informé des obligations mises à sa charge, des contrôles du respect de la confidentialité auxquels il pourrait se voir exposé, ainsi que des sanctions disciplinaires auxquelles il s'expose en cas de non respect des règles posées par la Charte.

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

Selon l'article 122-39 du code du Travail, cette charte peut être assimilée à un règlement intérieur.

Pour qu'elle soit dotée de la même valeur juridique qu'un règlement intérieur, la charte doit remplir certaines conditions, à savoir :

i) obtenir l'avis du Comité d'entreprise, ou à défaut, l'avis des délégués du personnel ;

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

ii) assurer la publicité de la Charte par voie d'affichage ;

iii) déposer un exemplaire au secrétariat greffe au Conseil des Prud'hommes ;

iv) communiquer la Charte à l'inspecteur du travail.

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

2-Obligations de l'employeur: transparence et proportionnalité

- Obligation d'information des employés préalable à la mise en place d'un système de collecte de données à caractère personnel (art. L. 1221-9 du code du travail) ainsi que le CE.
- Si irrespect de l'obligation de transparence: responsabilité de l'employeur pour manquement.

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

- Surveillance possible de l'employé sur son lieu de travail et son temps de travail mais par des procédés légaux (en droit civil).
  - Ex: enregistrement des conversations est légal si information préalable de l'employé.

Obligation de proportionnalité: mesures restrictives de liberté que si elles sont justifiées par la nature de la tâche à accomplir et proportionné au but recherché.

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

Employeur: que puis-je faire?

- Téléphone: conserver les numéros de tel des employés pendant 6 mois (délibération CNIL 2004);
- Appels personnels des employés: remboursement exigible
- Secret des correspondances: inviolabilité des correspondances privées: l'employeur ne peut ni consulter, ni intercepter, ni diffuser les messages personnels de son employé.

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

- Contrôle biométrique: possible si autorisation de la CNIL sous certaines conditions (information préalable, impératif de sécurité, proportionné au but recherché, non divulgation des données à caractère personnel).
- Géolocalisation: oui si information préalable et si légitime selon l'activité de l'entreprise (délibération CNIL 2006-066/067)

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

- **II- La Cybersurveillance en externe pour l'entreprise**
- Nous évoquerons deux cas: le cas d'attaque extérieure: intrusion dans le système informatique et le vol de données.

- A- Attaque extérieure sur l'entreprise

Le rapport du CLUSIF en 2005 fait état de quatre grandes catégories d'infractions:

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

- L'économie souterraine avec prise de contrôle à distance;
- Les chevaux de Troie et les rootkits (programme invisible à la sécurité);
- Les vols et pertes de données;
- Le harcèlement.
- Atteinte à l'intégrité du système informatique (Système de Traitement Automatisé des Données): entraver ou fausser le fonctionnement du STAD est puni de 5 ans de prison et de 75.000 euros d'amende (art. 323-2 du code pénal.

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

- Formes de l'entrave: destruction de fichiers, de programmes, de sauvegarde, saturation (flaming) provoquant des ralentissements ou des paralysies du STAD.
- Exemples :
- EDF/ Greenpeace: piratage informatique sur les données de Greenpeace France pour surveiller les ordinateurs face à la protection de l'EPR;

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

- condamnation d'EDF à 1.5 million d'euros pour recel et complicité d'accès et maintien frauduleux dans un STAD (tribunal correctionnel Nanterre 10 novembre 2011)
- Le pirate de Deezer: juste après sa création en 2007, ses bases de données ont été piratées par un pirate qui les a diffusées sur le site firstfm.eu. Il a été condamné à 1.000€ d'amende pour accès frauduleux dans le STAD. Amende légère car faible impact sur deezer. TGI Paris, 17/12/2010.

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU-2012

- Saturation: 3Wimédia c/ Netpass. Net: le gérant d'une société concurrente Elypsal menaçait la société 3wimédia de saturation par courriers électroniques s'il ne fermait pas ou ne cédait pas sa société. Le pirate a bombardé la société 3wimédia entrainant la paralysie momentanée du STAD. Il a été condamné 5.000€ d'amende, 9600€ pour la mobilisation des RH et 3.000€ d'atteinte à l'image (TGI Paris, 19 mai 2006, 12ème ch.)

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

- **B- Vol de données**
- La fuite intentionnelle de données se caractérise par le recel d'information et constitue un délit pénal.
- Le recel est puni à l'article 321-1 du code pénal de 5 ans d'emprisonnement et de 375.000€ d'amende. L'intrusion informatique est punie à l'article 321-1 du code pénal de 2 ans de prison et de 30.000€ d'amende. Si l'intrusion vise la suppression ou la modification de données contenues dans le système, la sanction est portée à 3 ans de prison et 45.000€ d'amende.

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

- Le recel d'information est difficilement chiffrable pour les entreprises. Mais à l'heure du numérique et de l'internationalisation des ressources humaines, l'environnement numérique facilite ce type de recel.
- Les récentes affaires Michelin et Renault prouvent que l'information est un bien immatériel qui s'ignore et que les dispositions actuelles ne suffisent plus à l'heure du numérique et des échanges à l'international dans un système concurrentiel accru.

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

- http://www.legalis.net/spip.php?article3241
- Projet de loi: le député Carayon a dévoilé le 12 janvier 2011 un projet de loi visant à renforcer la protection du secret des affaires.
- jwplayer}http://www.portail-ie.fr/videos/bc_secrets_affaires_110404.mp4&jwversion=5_html5&img=http://www.portail-ie.fr/images/videos/bc_secrets_affaires_110404.jpg
- Une nouvelle catégorie d'information va apparaître, l'information économique protégée accompagnée de mesures juridiques appropriées pour préserver les intérêts économiques des entreprises.

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

An Eye on the Usa

- Le ***Cohen Act*** (1996)vise à protéger le secret des affaires, défini très largement comme une information privilégiée et instaure un délit de « vol de secret des affaires » puni de 10 ans de prison et 5 millions d'amende de dollars en cas de violation.
- Objectif: protéger les entreprises contre l'espionnage économique mais met les entreprises et leurs droits de propriété intellectuelle dont le savoir-faire au cœur des préoccupations économiques.

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

Privacy Act 2005

- Le *Privacy Act* of 2005 définit de façon large les données à caractère personnel, et inclus notamment les e-mails, photographies et numéro de téléphone.

- Cette loi prévoit aussi le nom de la personne ou entité qui rassemble ces données, et d'informer de l'utilisation qui en sera faite, le type d'informations personnelles et la description des destinataires possibles.

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

Que doit faire l'entreprise?

- Le Privacy Act oblige les entreprises à mettre en place des systèmes de sécurité pour lutter contre la fuite d'informations. Les entreprises ont aussi l'obligation d'informer leurs clients lorsqu'elles sont victimes de telles fuites ou attaques.
- Exemple, l'Université de Los Angeles a été victime d'un vol d'information sur 800.000 noms.

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012

Conclusion

- Définir dès le départ les données confidentielles, le secret des affaires et les données stratégiques;
- Mettre en place un système de surveillance validé par la CNIL;
- Stocker sur des ordinateurs séparés les données relevant du secret des affaires de l'entreprise.

Cabinet LANDREAU, tous droits réservés à © Cabinet LANDREAU -2012