CONFERENCE

La révélation des failles de sécurité, risques et enjeux

Franck EBEL & Jérôme Hennecart
CDAISI & ACISSI

Raphaël RAULT
Avocat – BRM Avocats - Lille

Tests d'intrusion : jusqu'où peut-on aller ?

I. Quelles sont les techniques d'intrusion existantes ?

Quels sont les risques encourus par les sociétés de sécurité informatique dans le cadre des tests d'intrusion ?

1) Faux point d'accès = accès au réseau WIFI d'un tiers

- **Côté « pirate » : Accès et maintien frauduleux dans un système d'information => article 323-1 du Code Pénal (2 ans prison et 30.000€ amende)**

- **Côté abonné : Manquement aux obligations de surveillance et de sécurité de son système d'information :**

  - en cas de contrefaçon => article L.336-3 du CPI (contravention de 1.500 € assortie d'une peine complémentaire de suspension de l'accès internet pour une durée maximale d'un an)

  - en cas de traitement illicite de données à caractère personnel => article 226-17 du Code pénal (5 ans prison et 300.000€ amende)

2) Le détournement de connexion sécurisée = atteinte à l'intégrité des données

- **Article 323-3 du Code Pénal :**

« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75.000 euros d'amende »

3) Le vol de données par aspiration via une clef USB = accès et maintien frauduleux dans un système d'information

- **Article 323-1 alinéa 1 CP : « *Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende* » (idem pour la tentative)**

- **Article 323-1 alinéa 2 CP : « *Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende* »**

4) Le vol de données par aspiration d'une clef USB = sanction du créateur du programme malveillant :

- **Article 323-3-1 du Code Pénal (LCEN 21 juin 2004) :**

« Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée » **(de 2 à 5 ans prison et de 30.000 à 75.000€ amende)**

5) Le forçage de la connexion par mot de passe = double sanction :

- **Côté « pirate » : Atteinte à l'intégrité du système**

  - **323-2 du Code Pénal : « *Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende* »**

- **Côté utilisateur du système d'information :**

  - **si la personne est salariée, elle peut être passible d'une sanction disciplinaire si cela est prévu dans la charte informatique et que cette charte est annexée au règlement intérieur de l'entreprise**

6) Les mails avec usurpation d'identité

- **Article 2 du projet LOPPSI II (du 270509 et AN 160210) :**

Nouvel article 222-16-1 du Code pénal :

« Le fait de faire usage, sur un réseau de communications électroniques, de l'identité d'un tiers ou de données de toute nature permettant de l'identifier, en vue de troubler la tranquillité de cette personne ou d'autrui, est puni d'un an d'emprisonnement et de 15.000 € d'amende.

Est puni de la même peine le fait de faire usage, sur un réseau de communications électroniques, de l'identité d'un tiers ou de données de toute nature permettant de l'identifier, en vue de porter atteinte à son honneur ou à sa considération. »

7) Les keylogers

- Sanction du créateur du programme malveillant => article 323-3-1 du Code Pénal (de 2 à 5 ans prison et de 30.000 à 75.000€ amende)

- Complicité d'atteinte à l'intégrité des données => article 323-3 du Code pénal (5 ans prison et 75.000 euros amende)

II. Comment se prémunir contre les failles de sécurité ?

1) Obligation de notification des failles de sécurité

- Proposition de loi « visant à mieux garantir le droit à la vie privée à l'heure du numérique » adoptée par le Sénat le 23 mars 2010

- Article 7 : précise l'obligation de sécurisation des données incombant au responsable du traitement (article 34 LIL) et crée une obligation de notification à la CNIL des failles de sécurité

Contenu minimum de la notification faite à l'abonné ou au particulier :

- la nature de la violation de données à caractère personnel

- les points de contact auprès desquels des informations supplémentaires peuvent être obtenues

- recommande des mesures à prendre pour atténuer les conséquences négatives possibles de la violation de données à caractère personnel.

Contenu minimum de la notification faite à la CNIL :

- les conséquences de la violation de données à caractère personnel

- les mesures proposées ou prises par le FAI pour y remédier.

Les FAI doivent également tenir à jour un inventaire des violations de données à caractère personnel à la disposition de la CNIL.

Procédure d'alerte en cas de violation d'un traitement de données personnelles :

1. Information du CIL par le RT

2. En absence de CIL : information de la CNIL par le RT

3. Mesures nécessaires pour rétablir la protection (RT + CIL)

4. Information de la CNIL par le CIL

5. Si dommages sur les DP : information des personnes par le RT

2) Se prémunir des risques internes : la charte d'utilisation de l'outil informatique

- 72 % des entreprises considèrent que le comportement de leurs salariés sur les réseaux sociaux peuvent mettre en danger la sécurité de leur activité (réseau social considéré comme le plus dangereux = FACEBOOK pour 61 % des entreprises) => rapport « Security Threat Report : 2010 » publié par SOPHOS

- Besoin de sensibilisation des salariés sur les risques liés à la sécurité informatique

- Article 1384 al. 5 Code civil : responsabilité de l'employeur du fait des agissements de ses salariés

- **Transparence :**

  - **information préalable des salariés**

  - **consultation du Comité d'entreprise ou des Représentants du personnel**

  - **déclaration CNIL**

- **Proportionnalité :**

  - **Les moyens de contrôle de l'activité des salariés par l'employeur sont possibles (cybersurveillance) mais il existe des limites : ces moyens doivent être justifiés par la nature de la tâche à accomplir et proportionnés au but recherché (article L1121-1 Code travail) => arrêt « Nikon » du 2 octobre 2001**

- **Principales clauses de la Charte informatique :**

  - **Grands principes d'utilisation du système d'information (traçabilité, imputabilité, opposabilité et conformité)**

  - **Utilisations professionnelle et personnelle de la messagerie électronique, d'internet et des accès à distance (correspondances privées, analyse des connexions)**

  - **Respect des droits des tiers par les salariés (contrefaçon, diffamation, traitements de données personnelles, piratage, informations confidentielles,…)**

  - **Expression des syndicats et des IRP (intranet, internet,…)**

  - **Dispositifs de sécurité (responsabilité des mots de passe et ID, formations)**

  - **Rôle du Correspondant Informatique & Libertés (alerte, registre, formations)**

3) Se prémunir des risques externes : Contractualiser les tests d'intrusion pour les sociétés de sécurité informatique

- **73 % des entreprises victimes de cyberattaques en 2009 (pertes moyennes = 2,4 millions d'euros) => rapport « 2010 State of Entreprise Security » publié par SYMANTEC)**

- **Pour caractériser les infractions de la loi GODFRAIN, il faut une intention frauduleuse, ce qui n'est pas le cas lorsque le client a autorisé / habilité le prestataire de sécurité informatique à effectuer des tests d'intrusion contre son système d'information**

- Clauses principales :

- **Exonération de responsabilité du prestataire vis-à-vis du client pour : les infractions loi GODFRAIN et LCEN, correspondances privées, contrefaçon,...**

- **Autorisations des partenaires du client : hébergeur, prestataires tiers (sécurité, maintenance, SAAS, ASP,...)**

- **Périmètre (quel SI et quels types d'attaques) et durée des tests d'intrusion**

- **Traitements de données personnelles**

- **Confidentialité**

- **Transparence avec le client sur les contenus illicites découverts lors des investigations**

III. Quels sont les risques encourus par les sociétés de sécurité informatique dans le cadre de la révélation des failles de sécurité? (CCass, 27/10/09)

Cour de cassation, 27 octobre 2009 (art 323-3-1 CP) :

FAITS :

Le gérant d'une société spécialisée dans le conseil en sécurité informatique avait diffusé sur son portail internet des scripts permettant d'exploiter des failles de sécurité informatiques de Windows, directement visibles sur son site accessible à tous

PREMIERE INSTANCE => relaxe car aucune intention délictueuse et motif légitime :

- Il n'incitait pas au piratage

- Son unique souci était d'informer des menaces existantes les utilisateurs de Windows

Cour de cassation, 27 octobre 2009 (art 323-3-1 CP) :

APPEL => rejette le motif légitime et le condamne à une amende de 1.000€ :

- Système d'alerte mis en place par Microsoft et non utilisé par le gérant

- Intention délictueuse et mauvaise foi car il tirait des revenus publicitaires de la fréquentation de son site et il avait connaissance des risques de ces informations

CASSATION => confirme l'arrêt d'appel :

La constatation de la violation, sans motif légitime et en connaissance de cause, de l'une des interdictions prévues par l'article 323-3-1 du Code Pénal implique de la part de son auteur l'intention coupable exigée pour retenir la responsabilité pénale.