La révélation des failles de sécurité, risques et enjeux

Franck EBEL & Jérôme Hennecart
ACISSI & CDAISI

Raphaël RAULT
Avocat – BRM Avocats - Lille

I . Récupération d'information

Techniques et risques encourus

I . Récupération d'information

a) Faux point d'accès WIFI

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 entreprise : Manquement aux obligations de surveillance et de sécurité de son système d'information.

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

I . Récupération d'information

b) Le vol de données par aspiration via une clef USB

Côté pirate

Article 323-1 alinéa 1 CP : ***accès et / ou maintien frauduleux***

deux ans d'emprisonnement et 30000 euros d'amende

Article 323-1 alinéa 2 CP : ***suppression / modification de données***

trois ans d'emprisonnement et 45000 euros d'amende

Côté salarié

Sanctions disciplinaires si interdit dans la charte informatique

II . Usurpation de connexion

Côté pirate

Atteinte à l'intégrité du système article 323-2 du Code Pénal

Atteinte à l'intégrité des données article 323-3 du Code Pénal

cinq ans d'emprisonnement et 75000 euros d'amende

Côté salarié

Pas de sanction (session verrouillée)

Côté entreprise

Manquement à l'obligation de la sécurisation de son système d'information

III . Les mails avec usurpation d'identité

Côté pirate

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

Nouvel article 222-16-1 du Code pénal :

Un an d'emprisonnement et15.000 € d'amende

IV . Les keylogers

Côté créateur

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

V - Comment se prémunir contre les failles de sécurité ?

a) 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 :

- obligation de sécurisation des données incombant au responsable du traitement (article 34 LIL)

- obligation de notification à la CNIL des failles de sécurité

V - Comment se prémunir contre les failles de sécurité ?

b) Risques internes : la charte informatique

- Réseaux sociaux

- 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

V - Comment se prémunir contre les failles de sécurité ?

- **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)**

V - Comment se prémunir contre les failles de sécurité ?

c) Risques externes : tests d'intrusion

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

V - Comment se prémunir contre les failles de sécurité ?

- 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

VI - Illustration

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

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

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

CASSATION => confirme l'arrêt d'appel

Merci de votre attention

Questions ?