HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

JSSI 2013

Ingénierie sociale : aspects juridiques et pratiques

Quentin Gaumer
<Quentin.Gaumer@hsc.fr>
Frédéric Connes
<Frederic.Connes@hsc.fr>

Plan

- Aspects juridiques
- Aspects pratiques

Aspects juridiques

- Usurpation d'identité
- Vol d'information
- Escroquerie

- Collecte déloyale de données personnelles

Usurpation d'identité

- Loi du 14 mars 2011
- Code pénal, art. 226-4-1
  - Le fait d'**usurper** l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa **tranquillité** ou celle d'autrui, ou de porter atteinte à son **honneur** ou à sa **considération**, est puni d'un an d'emprisonnement et de 15 000 euros d'amende
  - Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne
- Consentement => pas d'infraction
- Sinon : risque à l'égard de la personne dont l'identité est usurpée (pas à l'égard de la personne « ciblée » par l'ingénierie sociale)

Vol d'information

- Code pénal, art. 311-1
  - Le vol est la soustraction frauduleuse de la chose d'autrui
- Pendant longtemps
  - Copie de données sans soustraction de support => pas de vol
- Tribunal correctionnel de Clermont-Ferrand, 26 septembre 2011
  - Condamnation pour vol sans soustraction de support
  - Poids de la décision ?
- Si reconnaissance du vol d'information
  - Applicable à l'ingénierie sociale
  - Pas de fraude si l'audité a consenti à la soustraction des données

Escroquerie

- Code pénal, art. 313-1
  - L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de **tromper** une personne physique ou morale et de la déterminer ainsi, à son **préjudice** ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un **bien quelconque**, à fournir un service ou à consentir un acte opérant obligation ou décharge
  - L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende

- Notion de « bien quelconque »
- Préjudice ?

Collecte déloyale

- Loi du 6 janvier 1978, art. 6, 1°
  - Les données sont collectées et traitées de manière loyale et licite
- Code pénal, art. 226-18
  - Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende
- Données permettant d'identifier des personnes physiques
- Déloyal = à l'insu des personnes concernées
- Or, par hypothèse, les personnes ne peuvent pas être informées

Aspects pratiques

- L'ingénierie sociale comme
  - Une finalité
  - Un moyen
- Evolution du contexte
- Méthodologies existantes
- Construire un scénario de *phishing*
- Mise en situation
  - Scénarios par téléphone
- La sensibilisation : Un résultat mitigé

L'ingénierie sociale comme une finalité

- Finalités possibles
  - Mesurer le niveau de sensibilisation des utilisateurs
    - Par exemple
      - Quelles informations considèrent-ils comme confidentielles ?
      - Signalements
  - Mesurer le niveau d'exposition à la fuite d'information
    - Facteurs
      - Nombre d'utilisateurs faillibles
      - Criticité de l'information obtenue

- Les définir précisément avec le commanditaire
  - Le respect du périmètre est fondamental juridiquement

L'ingénierie sociale comme un moyen

- Audit « Red Team »
  - Définition
  - Un moyen parmi d'autres, mais très efficace
    - Phishing
    - Téléphone
    - Physique (intrusion, séduction...)
  - Permet de récupérer des informations capitales pour l'audit
    - Mots de passe
    - Architecture réseau
    - Mesures de sécurité (versions des applications...)
    - Informations personnelles et sur l'organisation

Evolution du contexte

- Externalisation de plus en plus fréquente
  - Pour le SI (exemple : *cloud computing*)
  - Pour le personnel (typiquement : *Help Desk*)
    - Service orienté client
      - Facteur de confiance différent
    - Anonymat
    - Mutualisation de la prestation
- Temps de crise
- Ne pas négliger la sécurité « humaine »

Méthodologies existantes

- Théorie
  - Effet de gel
  - Théorie de l'engagement
  - Dissonance cognitive
  - *Quiproquo*
  - Talonnage
  - Etc.

- Pratique
  - Exploiter la crédulité des cibles
  - Gagner la confiance de la cible
    - Tendance naturelle à faire confiance

Construire un scénario de *phishing*

- Différence avec le phishing classique
  - Récupération d'informations sur l'organisme client, et non sur le site usurpé
- Plusieurs niveaux possibles
  - Facilement détectable
  - Détectable après une sensibilisation
  - Très difficilement détectable
    - Connaissances techniques requises

- Niveaux intéressants pour la corrélation des résultats

Construire un scénario de *phishing*

- Prendre en compte le contexte
  - Actualité (vacances, Noël, soldes, événements...)
  - Métier de l'organisme
  - Profil des cibles (âge, responsabilités...)
  - Marché de l'emploi dans le secteur
- Identifier le facteur déclenchant le clic
  - Gain financier
  - Meilleur emploi
  - Bonne action
  - Immédiateté
- Rédiger un courrier électronique crédible
  - En fonction du niveau sélectionné

Construire un scénario de *phishing*

- Construire le site web
  - Nom de domaine (attractivité, propriétaire)
  - Hébergement (local, dédié, en France, à l'étranger...)
  - En SSL ? (confidentialité des données récupérées)
  - Charte graphique
  - Logo de la cible
  - Attention aux messages d'erreur
  - Récupération des informations collectées

- Envoi des courriers électroniques
  - Forme du message (expéditeur, destinataire, objet...)
- Durée de la mise en ligne du site
  - A définir avec le commanditaire / en fonction du taux de clics

Attaque par téléphone

Cas n°1 : Le stagiaire

Attaque par téléphone

Cas n°2 : Le Help Desk

Attaque par téléphone

Cas n°3 : L'anti-spam

La sensibilisation : un résultat mitigé

- Permet de réduire le risque de fuite d'informations
  - Identifier les informations confidentielles de l'entreprise
- Doit être ciblée en fonction du profil des employés
- N'est pas persistante
  - Doit être périodique
- Doit être accompagnée de mesures de sécurité techniques
  - Proxy avec avertissement que l'on sort du SI
  - Identification de l'appelant
    - Pas d'appels anonymes en interne
  - Filtrage des appels (« stop secret »)
- Mais n'est jamais parfaite

Questions