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

Ingénierie sociale : aspects juridiques et mise en oeuvre

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

Plan

- Aspects juridiques
- Mise en œuvre d'une attaque

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

Usurpation d'identité

- Quelques exemples
  - Usurpation de l'identité d'un membre important de l'organisme
    - Contact avec des subalternes
  - Mise en œuvre de scénarios de chantages
    - Usurpation de l'identité d'un membre de l'organisme cible
    - Traces d'utilisation de services ou de produits moralement et/ou légalement répréhensibles
    - Chantage de la cible

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 »

Escroquerie

- Quelques exemples
  - L'attaquant se fait passer pour le responsable financier d'un grand groupe et demande au service comptabilité de faire un virement sur un compte à l'étranger
  - Usurpation de l'identité d'un utilisateur d'un site de vente en ligne (Amazon) et appel au service client pour demander le remplacement d'un produit défectueux
  - Des attaquants se font passer pour des membres des forces de l'ordre et appellent le central afin d'obtenir des informations sur les casiers judiciaires de rappeurs Français connus

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

Mise en œuvre d'une attaque

- L'ingénierie sociale comme
  - Une finalité
  - Un moyen
- Méthodologies existantes
- Le *Phishing*
- Les preuves
- Mise en situation

L'ingénierie sociale comme une finalité

- L'attaquant atteint son but au travers de l'Ingénierie Social
  - Son but ?
    - Récupérer des informations sensibles (Informations métiers, informations financières, projets en cours, etc...)
    - Faire réaliser directement des actions par les cibles
      - Passer un virement sur un compte à l'étranger
      - Envoyer un objet sans l'avoir payé (Ex. Attaque chez Amazon)
      - Toute autre action ayant un impact direct pour la cible

L'ingénierie sociale comme un moyen

- Le complément de tout « bon » attaquant
  - Plusieurs techniques
    - *Phishing*
      - Récupération de mots de passe
      - Envoie de pièces jointes piégées (logiciels malfaisants)
        - Intrusion directe au sein du SI
    - Téléphone
    - Physique (intrusion, séduction, manipulation...)

  - Informations utiles pour la suite de l'attaque *technique*
    - Mots de passe
    - Architecture réseau
    - Mesures de sécurité (versions des applications, anti-virus, etc...)
    - Informations personnelles et sur l'organisation

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

Le *Phishing*

- Attaque très répandue
  - Récupération d'informations liées au site usurpé
- Commence toujours de la même manière
  - Envoi d'un mail aux cibles
- Construit sur un scénario dépendant du contexte de l'attaque
  - Actualité
  - Métier de l'organisme
- Un facteur déclenchant le clic
  - Gain financier
  - Meilleur emploi

Les preuves

- Le Phishing
  - Le mail envoyé aux cibles
    - Informations sur l'adresse IP source du mail
    - Pièces jointes envoyées par l'attaquant
  - Nom de domaine utilisé
    - A-t-il été acheté par une personne physique ?

Les preuves

- Le contact direct ou par téléphone
  - Numéro de téléphone utilisé
  - En cas d'intrusion physique
    - Caméra de vidéo surveillance
    - Logs d'accès des mesures de sécurité physique
      - Lecteur de badge
      - Lecteur de carte

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

Questions