La réalité du risque Cyber

Romain ELIOT

Adjoint au CISO Groupe
Crédit Agricole S.A.

romain.eliot@credit-agricole-sa.fr

Quelques faits

- **2015 - ANTHEM (assurances) : 80 millions de données personnelles**
  - Identité, adresses physiques et e-mail, niveau de revenu
- **2016 - Banque centrale du Bangladesh : 72 M€ dérobés**
  - via l'interface utilisateur SWIFT
- **2016 - Yahoo! : 500 millions de comptes piratés**
  - attaque réalisée en 2014 et rendue publique en 2016 lors du rachat de Yahoo! par Verizon
- **2017 -EQUIFAX : vol de données touchant 143 millions de personnes**
- **2017 - Maersk, Merck, Fedex, Saint Gobain : indisponibilité du SI pendant plus d'une semaine**
  - Contamination des PC et serveurs Windows par le virus NotPetya
  - Pertes et coût de reconstruction par entreprise : 250 M€
- **2018 - Atlanta : blocage partiel des SI de la ville, rançon demandée (50 000$)**
- **2019 - Altran : indisponibilité du SI pendant plus d'une semaine**

Le risque cyber

- **Motivation**
  - Financière (vol de données, vol d'argent, fraude, chantage)
  - Politico-stratégique (perturbation des services aux citoyens ou vitaux pour un Etat, intelligence économique)

- **Des attaquants motivés et dotés de moyens**
  - Groupes mafieux
  - Groupes étatiques spécialisés dans les attaques cyber : Unité 61398 (Chine), Tailored Access Operations (USA), Bureau 121 (Corée du Nord)…
  - « 4ème arme cyber » : en cas de conflit

- **Des vulnérabilités et défaillances**

Quelques techniques d'attaque

- **Attaques frontales sur des services exposés**
  - Déni de service
  - Défiguration
- **Les attaques ciblées sur les personnes**
  - Phishing
  - Spear phishing
- **Les attaques non ciblées ou indirectes**
  - Virus, Cheval de Troie
  - Point d'eau

L'attaquant profite d'une connexion d'un poste de travail à Internet pour franchir la protection périmétrique de l'entreprise

Un scénario redouté / les réponses

- **Le scénario redouté : attaque de type Advanced Persistent Threat (APT)**
  - La réduction des risques passe par la combinaison de plusieurs lignes de défense complémentaires
- **Protéger**
  - Concevoir des systèmes sécurisés et maintenus, veille permanente et mise à jour des systèmes
- **Détecter**
  - SOC, CERT
- **Réagir**
  - Une gestion de crise cyber efficace
- **Reconstruire**
  - Les données, le SI

Vers la cyber-résilience

- **Typologie des impacts : la cyber-menace est-elle surévaluée ?**
  - Beaucoup d'attaques sans impact
    - Les petites attaques ont peu de conséquences en raison du niveau de protection en place (et qui a un coût certain)
  - Quelques sinistres majeurs (100 à 1000 M€)
    - Le temps de retour des sinistres majeurs est élevé : conséquence bénéfique du niveau de protection en place (et non d'une rareté des attaques).
  - De rares sinistres létaux (plutôt sur des TPE/PME)
    - La cyber-résilience n'est plus une option : savoir reconstruire son SI et redémarrer quoi qu'il arrive. Cela suppose des moyens spécifiques et des changements profonds dans la gestion des SI d'entreprise.