

# Sécurité et modernité : un défi pour l'entreprise ?

Forum annuel Cert-IST 2011

Compte-rendu

Saâd Kadhi <[saad.kadhi@hapsis.fr](mailto:saad.kadhi@hapsis.fr)>

- Association loi 1901
- Industrie, services et tertiaire
- Services de prévention des risques et d'assistance au traitement d'incidents
- 9 présentations
- Avocats, magistrats, spécialistes sécurité


Excellente  
ouverture de  
session

# Introduction « Sécurité et Modernité »

Antoine GARAPON, magistrat

- Intervention à la demande du Cert-IST
- Suite à la parution d'un article dans la revue ESPRIT
- *L'imaginaire pirate de la mondialisation, 06/09*
- Peu de connaissances en informatique

- La révolution numérique a introduit un nouveau rapport à l'espace
- Rétraction
- Parallèle avec la révolution maritime
- La justice est liée à la terre
- Impunité dans l'espace maritime
- Manque de traces, pas d'appropriation



Lieu de prise

- Métaphore maritime reprise par LulzSec
- En sécurité, on continue de penser en termes terrestres, en champs de bataille
- On assiste à 2 mouvements
- « Déterritorialisation »
- « Déterrestrisation »

- On accepte la circulation des biens, des flux
- Passage du moule au modulable
- L'important consiste à repérer le mouvement
- La sécurité passe par la prévision



Traces



Profilage


- Il faut commencer par exclure deux extrêmes
- Idéalisme libertaire des hackers
- Le contrôle sur un mode terrestre (étatique)
- Antinomie entre domination par une entité et Internet

- Il faut s'orienter vers la transaction, le compromis
- Ex. le Social Networking Privacy Act en discussion entre le gouv. US et FaceBook
- Il y a un marché des données personnelles
- Mais pas de marché de protection de ces données !



Auto-  
régulation

- Toutefois, assiste-t-on à une reterritorialisation ?
- Attaques = acte de cyberguerre (gouv. US)
- Régulation inter-étatique avec la collaboration des entreprises ?
- Peu probable, les russes et les chinois ne jouent pas le jeu




Un bon  
retour d'exp.

# Réguler le virtuel : expérience du jeu en ligne

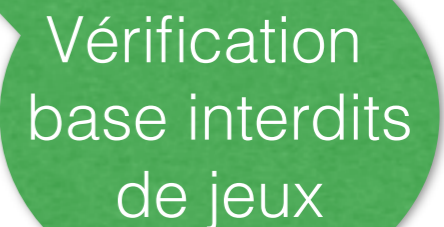
Stéphane VAUGELADE, Française des jeux

- Un peu d'histoire
- 1996 : 1ers sites Web de paris en ligne
- 1998 : 1ers sites Web de poker
- ... 2009 : ARJEL prévue
- 12 mai 2010 : création de l'ARJEL (loi 2010-476)
- 5 juin 2010 : 1ers agréments d'opérateurs

- Missions ARJEL
- Délivrer des agréments
- S'assurer de la sécurité et de la sincérité des opérateurs
- Protéger les populations « vulnérables »




Pas de  
scoring des  
joueurs



Vérification  
base interdits  
de jeux

- Le cahier des charges comprend 11 points
- Point 1 à 9 : fonctionnel
- Point 10 et 11 : S.I. (8 pages / 17)
- Candidat doit implémenter le frontal, communiquer le code source à l'ARJEL, le faire auditer et détailler son S.I.

- Le dossier soumis par la Française des jeux comprend plusieurs milliers de pages
- Dossier des exigences techniques décrit de façon précise l'archi. du frontal (annexe de 89 pages)
- Le frontal doit archiver les données en temps réel sur un site en France métro et mis à dispo. de l'ARJEL



Copie ou  
accès distant

- Le coffre-fort de journalisation doit être certifié par l'ANSSI
- Examen de dossier avant agrément
- Transparence très élevée
- Haute traçabilité à disposition de l'autorité sur son territoire

- Si données dans le Cloud, il faut obligatoirement garder les traces
- Pas d'approche par les risques
- ARJEL dicte ce qu'il faut faire

Bonne  
présentation  
d'Interpol

# Retours d'expérience d'Interpol sur l'évolution des attaques « high-tech »


Vincent DANJEAN, Interpol

Évolution  
un peu  
confuse

- 188 pays membres
- 1 bureau national par pays, fonctionnaires de police
- 1 secrétariat général de 600 personnes
- 62 M€ de budget annuel
- 80 nationalités différentes
- Pas de souveraineté



Une  
semaine de  
budget FBI



Aux  
locaux de  
travailler

- Historiquement, beaucoup d'attaques
- Protections en place permettant de se concentrer sur les attaques « importantes »
- Principalement, abus aux signes distinctifs d'Interpol
- 100 formulaires de fraude / semaine env.

- Arnaques
- Loterie
- Un site au look Interpol par pers. à arnaquer
- Depuis 2008, recrudescence
- Interpol est une cible connue et médiatisée

- En 2009, virus spécifiquement créé par Interpol
- 97 serveurs infectés en 2H
- Fin avril 2011, tentative de DDOS UDP
- 1,6 Gbps de flux

La réponse à incidents est primordiale

# Stratégie Nationale de Cyber défense

Patrick PAILLOUX, DG, ANSSI

Nb.  
important de  
messages

- Le DG de l'ANSSI passe les 3/4 de son temps sur des aspects opérationnels (réaction)
- De - en - de temps pour la prévention
- Il est primordial de se doter d'une capacité de réponse à incidents
- Temps de détection, temps de réaction

- 4 choses faites durant l'attaque de Bercy
- Se rendre compte de l'incident face à un signal faible
  - Mails infectés/piégés émanant de Bercy vers des prestataires
- Connaître l'étendue des dégâts
  - Bercy = 170k ordinateurs

- Nettoyage
  - 3 semaines de travail, bcp de préparation
  - A faire de façon discrète et sans utilisation du S.I.
- Renforcer la sécurité au niveau structurel
- L'ANSSI a mobilisé 30 pers. pendant 2 mois
  - Activité CERT

- L'attaque ne présente aucune sophistication technique
- Les attaquants disposaient de moyens très importants
- Ils étaient très organisés
- Recours systématique à l'anonymisation

- Il est nécessaire de se préparer à répondre à des incidents
- Ça arrive/arrivera à tout le monde
- Il faut détecter vite et ne pas hésiter à se faire aider
- Importance de l'organisation

- Le minimum est d'avoir des logs (traçabilité)
- Attaque Bercy = 4TB de fichiers texte à traiter au début de l'investigation
- Volonté de pénétrer des réseaux pour vol d'infos
- A des fins de déstabilisation

- SCADA est un gros sujet de travail en ce moment pour les interlocuteurs/opérateurs stratégiques
- Pub. d'une stratégie de cyberdéfense
  - Entité de cyberdéfense à venir (décret)

- ANSSI = 4 grands volets
- Renforcer la capacité d'intervention
- Augmenter le niveau de sécu. des dispositifs de l'état
  - Règles PSSI à minima pour tous les ministères
- Labeliser les produits
- Créer un réseau inter-ministériel piloté par un DSI central

- Nécessité de revoir l'éducation des ingénieurs et techniciens généralistes
- Ils doivent avoir des bases en SSI
- Relation avec les opérateurs d'infrastructures critiques
  - Temps réel, réseau d'alerte, déclaration d'incidents, audit
- Roadmap

- Cas des hôpitaux
- Mes données, ça intéresse qui ?
- Niveau de sécurité très faible
- Ne pas oublier la résilience des hôpitaux dans les discussions autour du dossier médical personnel et sa protection
- Que faire si plus d'IRM ou d'analyse de sans possible ?

- Question posée : cas des VIPs
- Pas de solution miracle
- Beaucoup de sensibilisation et de démonstration
- Ex. Siphonner le contenu d'un iPhone à distance

Bonne  
discussion

# Table ronde Réseaux Sociaux

Aucune  
solution  
miracle pour  
la SSI

Laurent DELHALLE, BEIC  
Jérôme BONDU, Inter-Ligere  
Arnaud RAYROLE, USEO  
Gérald SADDE, avocat  
Christophe BURCK, XTENSAW

- Enormément de pédagogie et de sensibilisation à faire
- Charte d'utilisation des réseaux sociaux nécessaire
  - Cf. Intel, IBM, Cisco
- FaceBook = 700M utilisateurs, 1/4 sur mobiles
- Commerce social à venir

Je reçois des offres sur mobile quand je passe devant un magasin

- Génération Y a acquis des réflexes « réseaux sociaux »
- Très difficile de se défaire de tels réflexes
- Les réseaux sociaux sont aussi une mine d'infos pour l'intelligence économique
- Google Alerts + éditeurs de solutions d'intelligence économique

- Attention à votre empreinte numérique
  - Les RH font souvent du screening sur les réseaux sociaux
  - Problème de collecte déloyale d'infos, interdite par la loi
- Le législateur n'arrive pas à suivre
  - Constat d'impuissance

- FaceBook est entrain de privatiser une bonne partie du Web
- Les réseaux sociaux sont du pain béni pour les enquêteurs
- Charte : comment suivre lorsque FB change la EULA et les paramètres avec des valeurs par défaut surprenantes très fréquemment ?

Très bonne  
présentation

# La sécurisation des mobiles pour l'entreprise

Jean-Marie MELE, France Télécom Orange

BYOD  
abordé

- Usage de + en + fréquent de terminaux personnels avec SIM pro
- BYOD (Bring Your Own Device)
- Évolution rapide
  - Substitution au PC
  - Arrivée du Cloud et du multi-devices
- Plus rapide que l'accompagnement par les équipes SSI

- Ex. de menaces
- Safari sans bac à sable et privilégié sur iPhone/iPad
- Contournement code verrouillage via DFU
- ZITMO (Zeus sur mobile)
- Android très ciblé

Windows  
Phone 7 très  
"sandboxé"

- En plus d'être ciblé, Android est un marché très fragmenté
- Un nouveau terminal tous les 2/3 mois
  - Pas de volonté de sortir les correctifs
- Android Market n'a pas de processus de validation
  - Suppr. des apps à postériori

- Avant, politique d'interdiction des terminaux personnels
- Auj., politique d'accompagnement
- Risques juridiques importants avec le BYOD
- Les données stockées sur un terminal perso restent la propriété du possesseur du terminal

- Quelques pistes de solution
- Déclinaison des règles d'usage des terminaux
- Sensibilisation, rédaction exigences SSI
- Mise en oeuvre de mesures org. et tech. avec les juristes

- Solutions de sécurité pour mobiles
- Marché embryonnaire
- MDM, Mobile Device Management
- Se préparer à composer avec un env. extrêmement dynamique
- Détection et contrôle

Orientée  
fournisseurs du  
Cloud

# Sécurisation des solutions de Cloud Computing

Arnaud FILLETTE, Alcatel-Lucent

Peu d'apports  
pour les  
"consommateurs" du  
Cloud

- Explication des différences entre SaaS, PaaS et IaaS
- Définition du Cloud (NIST)
- On-demand net access to a shared pool of configurable computing resources rapidly provisioned and released with minimal efforts
- Définition du public / private / hybrid / community Cloud

- Revue des services ou certifications sécurité du top 10 des fournisseurs selon [searchCloudComputing.com](http://searchCloudComputing.com)
- Amazon Web Services : ISO 27001, SAS Type II
- Verizon : idem
- ...

Très bonne  
présentation

# Cloud Computing : questions juridiques

Jean-Marie JOB, Avocat

Cloud : des  
précautions à prendre

- Ateliers ADIJ autour des aspects juridiques du Cloud
- Association pour le Développement de l'Informatique Juridique
- Groupe de travail de 20 à 30 participants par séance
- CNIL, avocats, DSI, etc.
- [cloudcomputingadij.eklablog.fr](http://cloudcomputingadij.eklablog.fr)

- Absence de régime réglementaire spécifique
- Le Cloud Computing s'inscrit néanmoins dans un cadre réglementaire complexe
  - Code de la consommation, loi Informatique et Libertés, réglementations sectorielles,...
- L'objet et périmètre du contrat doivent être clairement définis

- Données personnelles : qui est responsable du traitement ?
- La CNIL envisage une possibilité d'une dualité de responsables
- Client du Cloud et fournisseur
- Les fournisseurs essaient de repousser la responsabilité vers les clients

- Attention au transfert des données personnelles hors UE. Principe d'interdiction sauf
  - Safe Harbor (US)
  - Protection jugée adéquate dans le pays destination
  - Signature de clauses contractuelles type (commission euro)
  - Binding Corporate Rules (BCR) au sein d'un même groupe

Quid art. 69  
loi info et  
lib.?

- Travaux en cours CNIL avec homologues G29
- Présenter un cadre juridique harmonisé en matière de Cloud Computing
- Étendre les BCR + Safe Harbor aux sous-traitants
- Certains fournisseurs s'engagent à laisser les données en UE

- Multitude de scénarios de Cloud et de contrats possibles
- Pas de contrat type
- Plan d'assurance sécurité, SLA, audit client, certifications SAS 70, ISO 27001, polices d'assurances, garanties contractuelles...

- Ne pas sous-estimer l'investissement en ressources et en temps nécessaire pour définir le cahier des charges
- Points d'attention
- Taux de disponibilité, temps de réponse, localisation des données, préservation des données, réversibilité

- Prévoir le respect de la confidentialité par le prestataire et tous ses sous-traitants
- Délimiter précisément les dommages couverts, svt. directs et prévisibles
- Traiter la question des dommages indirects (image de marque, perte CA,...)
- Quid du risque pénal (piratage)

- Anticiper les scénarios catastrophe
- Est-ce que le prestataire s'engage à transférer les données chez un concurrent ?
- Le transfert des données concerne aussi l'accès depuis l'extérieur de l'UE
- Création d'un comité de surveillance pour observer les pratiques des fournisseurs : pas à l'ordre du jour

A priori  
intéressant...

# Les attaques APT

David TRESGOTS, Cert-IST

... Mais j'avais un train  
à prendre

- APT = Advanced Persistent Threat
- Les attaquants scénarisent. Ce n'est pas opportuniste
- Attaques généralement peu automatisées
- Attaquants motivés et avec des moyens financiers conséquents

- Les attaques APT sont dites à signaux faibles
- Impact majeur cependant
- Gérées comme un projet
- Le gain financier et/ou industriel n'est pas immédiat...

Et là, je suis  
obligé de  
partir...

# Hapsis



45 rue de la chaussée  
d'Antin  
75009 Paris  
FRANCE

Tél. : +33 (0)1 53 16 30 60 -  
Fax : +33 (0)1 53 16 30 62  
Email : [contact@hapsis.fr](mailto:contact@hapsis.fr)  
Web : <http://www.hapsis.fr/>