metis
UMR 7619

Sécurité des Systèmes d'Information : un art martial ?

Jean-Marie Mouchel
DU (délégation de la DSI et du RSSI)

Philippe Marty
CSSI (& ICS)

Christophe Bonnet
ASR, ASSI

Bénédicte Sabatier
chargée de mission au service informatique

SI : systèmes d'information
(services informatiques ***& autres !!!***)

DSI : direction des SI
(1 CNRS + 1 UPMC)

RSSI : responsable de la sécurité des SI
(1 CNRS + 1 UPMC)

CSSI : chargé de la SSI
(1/labo)

ASSI : adjoint à la SSI
(si possible/nécessaire)

ASR : administrateur systèmes & réseaux
(donc purement informatique)

PSSI : politique de SSI
(1 Etat > 1 CNRS + 1 UPMC > 1/labo)

Expériences préliminaires …

- Qui a vu la faille dans mon email d'annonce du séminaire ?
  - Savoir lire un email … Savoir lire une page web …
- Qui a repéré les notifications de MàJ Win10 ? Où ?
  - Attention en février …
- Combien de sources bluetooth ouvertes dans la salle ?
  - Savoir configurer son matériel …
- Combien de sources wifi ?
  - Cf. aussi dans les transports en commun … dans une rue …

Conclusion en guise d'introduction !

- La plus grosse faille de sécurité est …
  … l'utilisateur/e !!!
  => 99% des incidents ont pour origine un mauvais comportement
- Comparaison :
  informatique (vulnérabilité) / automobile (freins par exemple)
  => l'utilisateur :
  - malchanceux ou inattentif (verglas)
  - malformé (utilisation, entretien, réparation)
  - malveillant (sabotage)
- Nécessité d'intégrer formation à la sécurité dans les cursus !

Historiques & Raccourcis grossiers …

- Problème : les moyens informatiques se développent plus vite que les formations !

– 1980 µ-informatique autodidacte		plantages ?
1985 « clubs »		« piratages » (copies)
1990 web académique (1.0 - waap)	*(internet <> www !)*	malwares
1995 web grand public (1.5 ?)		spams, hoax …
2000 informatique « multimédia »	*(www <> adsl/box !)*	darknet, deepweb …
2005 web collaboratif (2.0 - saas)	Services Informatiques	hackers
2010 web social & économique (2.5 ?)	PSSI Etat (hadopi …)	cybercrime
2015 big data & clouds (2.75 ?)	PSSI Organisme	cyberguerre
2020 objets connectés	PSSI Labos	cybersingularité
& web sémantique (3.0 – haas)		& horizon tech. ?

- Dans les années 2000, on a commencé à percevoir la nécessité de formation DE MASSE à l'informatique technique & scientifique (=> filières SI, e-commerce, bio-info, etc.)
- Depuis 2010, on perçoit enfin la nécessité de formation DE MASSE à la sécurité informatique, mais c'est comme la formation au secourisme (WW2 > PC) ou à l'écologie (GP > COP21)
  => l'équivalent informatique de la COP21 s'appelle la PSSI !

Sociologie

- Le 100% sécurisé n'existe pas
  => limitation et gestion du risque (et des responsabilités)
  => SE CONNAITRE SOI-MEME, SES OUTILS, SON ENVIRONNEMENT !
- 5 niveaux de comportements :
  - Naïveté (google est mon ami !)
  - Laxisme (je n'ai rien à cacher ! se noyer dans la masse ?)
  - « médian »
  - Tour d'ivoire (centralisation = source unique / pratique … mais facile de tout perdre d'un coup !)
  - Paranoïa (je n'ai pas facebook, d'ailleurs je vais jamais sur internet, d'ailleurs j'ai même pas d'ordi …)
- 3 niveaux d'exposition :
  - intelligence économique (domaine publique) <=> ingénierie sociale (big data) <=> espionnage (illégal)
  - les configurations par défaut sont souvent au profit du constructeur / opérateur, pas de l'utilisateur !
- 4 leviers de corruption :
  - MICE : money, ideology, coercion (sex, drugs, games …), ego

Introduction en guise de conclusion …

- JCVanDamme avait raison ! SOYEZ « AWARE » !
  - avoir les bonnes pratiques et savoir pourquoi !
  - ne pas laisser la technologie évoluer plus vite que les usages,
    ne pas laisser les constructeurs imposer les configurations par défaut
    (lieux de stockage, paramètres, rapports « d'erreurs », mises à jour …)
  - PB : la perception dépend de l'observateur : un aware (aux yeux d'un autre aware) sera perçu comme parano par un naïf ; ou comme naïf par un parano ;-)
- ARTS MARTIAUX : pas de formule magique ou unique … entraînement permanent !
  - SE PREPARER AU PIRE :
    - identifier le risque : classification des informations
    - le minimiser (prévention) : compartimentage des informations, choix & bon usage des outils
      (ex : hardware opensource : « Purism » Librem …)
    - vivre avec (curation) : sauvegardes des données, redondances matérielles, assurances …
  - ESPERER LE MEILLEUR :
    - ne pas voir le diable partout ! rester « open » (-source ;-)

Authentification

- Mots de passe (& codes pins & patterns)
  - mnémotechnique & robustesse
  - compartimentage
  - les murs n'ont pas que des oreilles …
  - la « mémoire » des écrans tactiles …
  - les « coffres-forts » à mots de passe
- Clefs SSH/SSL
  - avec ou sans passphrase ?
- Certificats TLS
  - https://igc.services.cnrs.fr/ & https://services.renater.fr/tcs/
- Tokens
- Biométrie : ATTENTION ! On ne peut pas « révoquer » ses empreintes biométriques !
- Single Sign On …

Un mot de passe n'est utile que s'il est requis !

=> login au boot
=> screenlock
=> screensaver
=> veille
=> hibernation
=> autologout

Menaces : Origines

- Windows / Linux / MacOS :
  les réalités d'hier et celles d'aujourd'hui ?
  (vive le crossplatform …)
- Pages web : java-scripts, plugins, spoofing
- Emails : phishing, liens, java-scripts, images « remote »
- Fichiers :
  - exécutables vérolés (downloads sur sites officieux)
  - pdf et office : scripts !
- Clefs usb : auto-exécutées

Menaces : Types & Méthodes

- Malware (maliciel)
  - Virus, Ver, Cheval de Troie
  - Adware (publiciel)
  - Spyware (espiongiciel)
  - Ransomware (rançongiciel)
  - Scareware (terroriciel)
- Botnet
  - (distributed) denial of service
  - squat d'espace de stockage
  - diffusion illicite de fichiers ou emails
- Nuisance
  - défiguration, propagande
  - effacement
- Vol, Espionnage

- Dissimulation dans un logiciel banal ou dans un email
- Hacking
  - X Site Scripting
  - Vulnérabilités / « exploit »
  - Portes dérobées
  - Force brute
- Phishing
- Spoofing
- Man in the Middle

Remèdes ?

- Antivirus …
  - bien choisir et paramétrer !
- Parefeu …
  - ou juste fermer les services !
- Cloisonnement !
  - NAT, VLAN, VM
- « Awareness » !
  - choix des outils
  - comportement (configuration, utilisation, mises à jour)
  - coder proprement
- Chiffrement (cryptage)
  - couche réseau (SSL, TLS, PGP)
  - couche logicielle (IPSec, Tokens)
  - couche données (TrueCrypt)
  - couche matérielle (disks et clés auto-chiffrants)
- Pourquoi se protéger ?
  - données sensibles ?
  - perte de temps ?

Que faire en cas de piratage constaté ?

- Ne pas paniquer, ni culpabiliser, ni avoir honte
  - même si victime d'un levier « MICE »
- Circonscrire
  - débrancher le réseau
- NE PAS ETEINDRE
  - préserver les traces
- Alerter immédiatement
  - rester factuel (pas d'interprêtation ni des intentions des attaquants ni des réactions des défenseurs)
- Attendre autorisation avant de réparer / réinstaller …

That's all, folks !

- Au moins pour cette fois …
- Rendez vous la prochaine fois pour « Computer Wars, Episode II »