



POUR DES COMPÉTENCES TOUJOURS À LA POINTE

Télécom Evolution

Mastère Spécialisé

Big Data Gestion et analyse des données massives Programme - MS Big Data :

Période 3 : Sécurité informatique

Session 1 : Introduction Sécurité Informatique (SSI)



Quelques proverbes et citations

« Face au monde qui change, il vaut mieux penser le changement que changer de pansement » *Pierre DAC*

« L'habituel défaut de l'homme est de ne pas prévoir l'orage par beau temps » *Nicolas Machiavel*

« C'est au pied du mur qu'on voit le mieux le mur » *Lao-Tseu ou Confucius*

« Les tuiles qui protègent de la pluie ont toutes été posées par beau temps » *Proverbe chinois*

« Qui n'a rien ne risque rien. Qui ne risque rien n'a rien » *Proverbe Français*

Ces 25 dernières années jusqu'à ce jour

Naissances d'Industries

- ❑ PC, Architecture Client-Serveur, Lan, Wan, Man
- ❑ Sécurité, Internet, e-Commerce, Mobilité, Cloud, IOT,
- ❑ Transformation Numérique



Internet World Stats

Usage and Population Statistics

WORLD INTERNET USAGE AND POPULATION STATISTICS JUNE 30, 2016 - Update

| World Regions | Population (2016 Est.) | Population % of World | Internet Users 30 June 2016 | Penetration (% Population) | Growth 2000-2016 | Users % of Table |
|----------------------------------|------------------------|-----------------------|-----------------------------|----------------------------|------------------|------------------|
| Africa | 1,185,529,578 | 16.2 % | 339,283,342 | 28.6 % | 7,415.6% | 9.4 % |
| Asia | 4,052,652,889 | 55.2 % | 1,792,163,654 | 44.2 % | 1,467.9% | 49.6 % |
| Europe | 832,073,224 | 11.3 % | 614,979,903 | 73.9 % | 485.2% | 17.0 % |
| Latin America / Caribbean | 626,054,392 | 8.5 % | 384,751,302 | 61.5 % | 2,029.4% | 10.7 % |
| Middle East | 246,700,900 | 3.4 % | 132,589,765 | 53.7 % | 3,936.5% | 3.7 % |
| North America | 359,492,293 | 4.9 % | 320,067,193 | 89.0 % | 196.1% | 8.9 % |
| Oceania / Australia | 37,590,704 | 0.5 % | 27,540,654 | 73.3 % | 261.4% | 0.8 % |
| WORLD TOTAL | 7,340,093,980 | 100.0 % | 3,611,375,813 | 49.2 % | 900.4% | 100.0 % |

Aujourd'hui en France

Internet Stats and Facebook Usage in Europe November 2015 Statistics

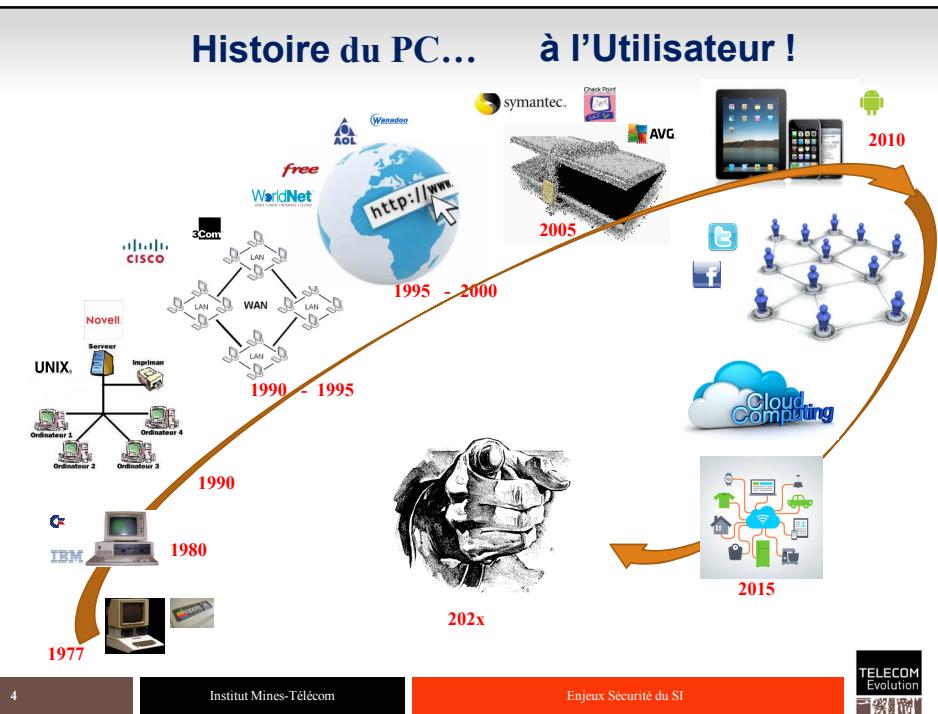
| EUROPE | Population (2015 Est.) | Internet Users, 30-Nov-2015 | Penetration (% Population) | Users % in Europe | Facebook 15-Nov-2015 |
|---------------|------------------------|-----------------------------|----------------------------|-------------------|----------------------|
| France | 66,132,169 | 55,429,382 | 83.8 % | 9.2 % | 32,000,000 |

TELECOM Evolution

3

Institut Mines-Télécom

2015



4

Institut Mines-Télécom

Enjeux Sécurité du SI

TELECOM Evolution

1 seconde sur Internet !

 = 54 000 recherches (90 milliards / mois)

 = 52 083 likes / 3 472 uploads photo (1,09 milliard pers. / jour)

 = 124 900 vidéos vues

 = 6 000 tweets

 = 1 099 photos / vidéos (95 millions/ jour)

 = 81 millions users (environ 1450h00 séries & films /sec)

Rappel :

1991 = 1 seul site Web + poignée users

2016 = + 1 milliard de sites Web

5

Institut Mines-Télécom



Les 25 prochaines années

2017-20XX : Industrie du « Tout-Cyber » :



- Cyber-économie, Cyber-commerce, Cyber-consommation
- Cyber-menaces, Cyber-criminalité, Cyber-guerre,
- Cyber-incidents, Cyber-sécurité, Cyber-conférence,
- Cyber-défense, Cyber-attaque, Cyber-conflits,
- Cyber-collaboration, Cyber-démocratie,



Le Tout Cyber : la norme pour le futur

Aujourd’hui, il n’y a aucune crise dans le monde de quelle nature que ce soit qui ne présente pas une cyber-dimension, ou un cyber-aspect !



6

Institut Mines-Télécom



Les pires scénarios : et si demain



Exploitation de faille de sécurité dans un barrage pour l'ouverture de vannes ?



Contrôle à distance de transformateurs de centrale nucléaire ?



7

Institut Mines-Télécom



Les pires scénarios : et si demain



Pour un état, perte du contrôle du trafic aérien au profit d'un autre ?



Déviation d'un bateau pour le lancer sur un port ! Exemple : Méthanier (345m Long - 54m large; + grand que Charles De Gaulle- 266000 m3 GNL (= consommation ville de Lyon / un an)



Cyber-attaque sur un sous-marin dans un port avec un réacteur allumé !



8

Institut Mines-Télécom



Profils Cyber attaquants

Cyber violents visent les personnes, les internautes
(menaces, insultes, diffamations, harcèlements)



Cyber escrocs appât du gain
(relèvent d'une délinquance à grande échelle organisée)



Cyber espions s'approprier données sensibles
(stratégiques/économiques)



Cyber mercenaires : proposent services sur Darknet
(perpétrer attaques pour états, individus ou organisations)



Cyber terroristes : idéologies extrémistes
(utilisent Internet comme tribune / moyen de radicalisation)

9

Institut Mines-Télécom



Motivations

Finalités : gain, blocage, destruction, notoriété, intérêt personnel, chantage mais aussi fraude, vol de données, intelligence économique ou même cyber-guerre (cyberattaques d'Etat)

Autres motivations :

- ▶ raisons politiques
- ▶ raisons morales (Ashley Madison, ...)
- ▶ réputation (Sony,...)
- ▶ parfois simplement par « jeu » !



Ransomware : attaque sans cible précise. Concentre les attaques sur les points d'accès, le chantage et l'extorsion (nouveaux moyens pour les criminels de gagner leur vie de manière « online »)

10

Institut Mines-Télécom



La menace Cryptolocker LOCKY

Source Kaspersky

Innombrables ravages



Impacts retentissants : paralysie de l'activité, perte financière, voir fermeture définitive d'organisation.



15000 € = rançon moyenne exigée par les ravisseurs



+ 60 variantes de ce ransomware.



72 heures = délai moyen avant suppression des données

5 antivirus / 57 éditeurs ont détecté Locky (lors de la propagation initiale soit - 10 %)

11

Institut Mines-Télécom



Contexte

- 1 nouveau malware par ½ seconde
- 30 000 nouvelles adresses URL infectieuses par jour
 - 80% sites légitimes compromis
- 1 million d'ordinateurs portables perdus ou volés chaque année
- 1 employé sur 3 est prêt à donner son mot de passe à un inconnu
- 600 000 comptes Facebook compromis chaque jour



Sources : Ponemon Institute, Verizon, Facebook

12

Institut Mines-Télécom

Enjeux Sécurité du SI



Contexte

The screenshot shows the 01net homepage with a search bar and a navigation menu. Below the menu, a news article is displayed with the title "eBay : 145 millions de comptes clients compromis (MAJ)". The article discusses a cyberattack that compromised 145 million eBay accounts. The footer of the page includes links for Institut Mines-Télécom and TELECOM Evolution.

Contexte

The screenshot shows a Facebook message thread between Nathalie and Christophe D'Arcy. They discuss Nathalie's phone being hacked and her need for help. A separate message from Tim is shown, reporting that his account was cloned. A blue box contains a link to ContactPrive.com with instructions for reporting hacked accounts. The footer of the page includes links for Institut Mines-Télécom and TELECOM Evolution.

Contexte

Urgent décès

1 message

tania <tania@yahoo.fr>
Répondre à : tania <tania@yahoo.fr>

15 mai 2014 12:38

Bonjour ,Comment vas tu ? bien je l'espère moi pas du tout c'est le cœur lourd, plein de larmes et de tristesse que je t'annonce le décès de stefane et Karina suite a un très grave accident de route a Bamako (Mali) entre un poids-lourd et deux voiture j'ai des blessures a la mâchoire et dans le dos ,nous sommes allés pour un projet,je suis traumatisé et encore sous le choc je suis en larme je n'arrête pas de pleurer .je voudrais mourir... pour ne plus avoir a souffrir de cette terrible tragédie je suis a Bamako et je dois faire le rapatriement de leurs dépouilles , mais a vrai dire malheureusement je me retrouve avec une petite somme pour régler les frais de transport et d'autre frais qui sont,

L'autorisation de transport international des dépouilles ,
Frais de rapatriement des dépouilles
Certificat médical de décès
Les cercueils,les soins de conservation

J'aimerais avoir ton aide, une aide financière pour régler certains frais car je suis désespéré je te supplie de me répondre afin de pouvoir te remettre mes coordonnées pour me faire parvenir un mandat postal a mon nom je compte énormément sur toi c'est une urgence.

PS: Je suis injoignable contacte moi par mail au plus vite.

Tania

15

Institut Mines-Télécom

Enjeux Sécurité du SI



Contexte

► Les plus grandes menaces actuelles

- **Faux antivirus** et fausses applications d'améliorations de performances (nettoyage de registry, CPU boost).
- **Black Hat SEO** : Empoisonnements des moteurs de recherche
- **Réseaux sociaux et profilage social** (géo localisation, vol d'informations)
- **Attaques Autorités de Certifications, Registraires**
- **Mobiles / Consumérisation (BYOD)**
- **Hacktivisme / Attaques ciblées**
- **Sites Web infectés**
- **Cloud Computing**

M Technologies

TECHNOLOGIES Jeux vidéo Hits Playtime Libertés numériques Téléphonie mobile Droit d'auteur

Un Français arrêté pour le piratage de 17 000 smartphones

Le Monde.fr | 19.10.2012 à 16h50 • Mis à jour le 19.10.2012 à 17h42

16

Institut Mines-Télécom

Enjeux Sécurité du SI



Agenda

1. Contexte
- 2. Les Entreprises et les Systèmes d'Information**

3. Nouveaux Enjeux, Nouvelles Menaces , Nouveaux Usages
4. Principales Menaces
5. Les Grands Principes de la Sécurité Informatique
6. Responsable Sécurité du Système d'Information
7. Le Cloud Computing
8. Conclusion

17

Institut Mines-Télécom

Enjeux Sécurité du SI



Les Entreprises et les Systèmes d'Information

- Entreprises / Organisations / Etablissements Publics
- Le SI fait partie du patrimoine de l'entreprise
 - Savoir faire
 - Patrimoine immatériel / informationnel
- Budget :
 - Industrie 2 à 5% du CA
 - Etablissement financier : 15 à 20% du CA (SI = usine)
- Complexité et variété des métiers et des technologies
 - Réseaux
 - Systèmes, OS
 - Mobiles
 - Applications (ERP, CRM)
 - Téléphonie
 - Collaboratif
 - Développement
 - Projet, management

*Sans informatique,
l'entreprise cesse de
fonctionner !*

18

Institut Mines-Télécom

Enjeux Sécurité du SI



Les Entreprises et les Systèmes d'Information

- Patrick Pailloux, ex directeur général de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) :

« En matière de sécurité informatique, la priorité c'est l'hygiène. Il y a un certain nombre de vérifications et de mesures à prendre »

- L'ANSSI a publié un guide précis en 13 étapes et 40 règles concrètes et pratiques pour assainir le système d'information

« Ces règles doivent être toutes appliquées systématiquement, partout. Les appliquer garantira à vos systèmes d'information une meilleure résilience face aux cyberattaques »

« Avec ce document, plus personne n'a désormais d'excuse pour ne pas appliquer ces mesures. Ceux qui n'auront pas appliqué ces mesures ne pourront s'en prendre qu'à eux-mêmes. »

Assises de la Sécurité – Oct. 2012

19

Institut Mines-Télécom

Enjeux Sécurité du SI



Les Entreprises et les Systèmes d'Information

- Enjeux Concurrentiel
 - Image de l'entreprise
 - Nombreuses attaques récentes
 - Cybersquatting
 - Gestion de crise
- Intelligence économique / Espionnage industriel
- SI vulnérable
 - Eclatement de l'entreprise (mobilité, tierces parties, cloud,...)
 - Naïveté, curiosité des employés (clefs USB abandonnées, www)
 - Grande distribution des technologies : Consumérisation (BYOD)



Site de Malaysia Airlines piraté le 26 janv. 2015

Seules 14 % des entreprises considèrent les cyber-menaces comme faisant partie de leurs 3 principaux risques!

Source : Kaspersky

20

Institut Mines-Télécom

Enjeux Sécurité du SI



Agenda

1. Contexte
2. Les Entreprises et les Systèmes d'Information
- 3. Nouveaux Enjeux, Nouvelles Menaces , Nouveaux Usages**
4. Principales Menaces
5. Les Grands Principes de la Sécurité Informatique
6. Responsable Sécurité du Système d'Information
7. Le Cloud Computing
8. Conclusion

21

Institut Mines-Télécom

Enjeux Sécurité du SI



Nouveaux Enjeux, Nouvelles Menaces

- Pendant longtemps, piratage = gloire ou déni de service,
- Aujourd'hui : vol, exploitation des ressources (botnet)
- Economie parallèle Cybermafia, cybercriminels extrêmement compétents.
 - Utilisateur + ordinateur = Cible / Produit !
 - Bases de données de coordonnées bancaires
 - Botnet pour attaques ou diffusion de spam
 - Zero day threat / Menace jour 0
- Criminalité, terrorisme, guerre : « cyber » !
- Cyberdéfense
 - Attaque informatique = déclaration de guerre
- Attaques autorités de certifications (DigiNotar)
- APT : Advanced Persistent Threats (Stuxnet)
 - Attaque des systèmes industriels souvent moins bien protégés

Estonie 2007. Plus grande attaque en DDS. Paralysie de l'ensemble du pays => Emeutes, pillages, plusieurs M\$ de perte

22

Institut Mines-Télécom

Enjeux Sécurité du SI



Cyberguerre ?

Piratage de Sony : le vol des films n'était qu'un début

Le Monde.fr | 03.12.2014
Les hackers, qui ont vraisemblablement diffusé des films Sony pas encore sortis en salle, ont également publié de nombreuses données confidentielles de Sony Pictures Entertainment.

L'Interview qui tue : les spectateurs américains menacés !

Le retrait du film de Sony scandalise Hollywood

Par LEXPRESS.fr, publié le 18/12/2014

Le studio Sony Pictures a renoncé à sortir son film *The Interview* après le piratage et les menaces dont il est l'objet. Une décision qui indigne et inquiète les personnalités du milieu.

La Corée du Nord suspectée !

LE FIGARO.fr

La cyberguerre fait rage dans la péninsule coréenne

Publié le 23/12/2014 à 17:48

Pyongyang a été privé d'Internet, tandis que Séoul subissait une attaque informatique sur une centrale nucléaire.

Michael Moore | 14:14 - 17 déc. 2014

Dear Sony Hackers: now that you run Hollywood, I'd also like less romantic comedies, fewer Michael Bay movies and no more Transformers.



"L'interview qui tue": pour Hollywood, les hackers ont gagné" BFM TV

La cyberguerre perdue par les US ?

Le Point.fr

Mises à jour le 14 juillet à 11h52

Piratage de Sony : vers une cyberguerre mondiale ?

La Maison-Blanche examine les options "appropriées" pour répliquer aux attaques et aux menaces visant le studio, contraint d'annuler la sortie d'un film.



23

Institut Mines-Télécom

Enjeux Sécurité du SI

Cyberguerre !



12/01/2015



«Op Charlie Hebdo»: La contre-attaque d'Anonymous atteint ses premières cibles



CHARLIE HEBDO

Bretagne Toutes les régions

Publié le 06/10/2014 | 18:41

La cyber-défense, 4 ème armée de Jean-Yves Le Drian

Des centaines de sites français piratés.

Des mairies, conseils généraux, établissements scolaires, universités, églises ou entreprises ont été visés par ces cyberattaques.

Le Figaro.fr | 12/01/2015

Le Monde.fr | 20/01/2015

Proche-Orient Le commandement de l'armée américaine au Moyen-Orient visé par une cyberattaque

Le Monde.fr avec AFP | 12.01.2015

Un groupe se réclamant de l'Etat islamique (EI) a piraté, lundi 12 janvier, le compte Twitter du commandement de l'armée américaine au Moyen-Orient et en Asie centrale.

24

Institut Mines-Télécom

Enjeux Sécurité du SI



Cyberguerre !!

M Amériques

Le Monde.fr avec AFP | 31.12.2016

Aux Etats-Unis, un programme malveillant détecté dans un ordinateur portable lié à un fournisseur d'électricité

L'ordinateur dans lequel a été repéré ce code, qui serait lié à une opération de piratage informatique russe, n'était pas connecté au réseau électrique, affirme la compagnie du Vermont.

l'express

Par LEXPRESS.fr avec AFP - publié le 08/01/2017

24 000 cyberattaques déjouées en France en 2016, selon Jean-Yves Le Drian

Harcèlement, espionnage, tentatives de perturbation de systèmes de drones... selon le ministre de la Défense, les tentatives de déstabilisation informatiques contre la France ne cessent d'augmenter.

LE HUFFINGTON POST

INTERNATIONAL | 30/12/2016

"Grizzly Steppe", l'opération de piratage russe pointée du doigt par le FBI

Les pirates ont notamment envoyé des courriels trompeurs à des membres du parti démocrate, les convaincant d'installer un logiciel malfaisant ou de communiquer leurs identifiants.

25

Institut Mines-Télécom

Enjeux Sécurité du SI



Nouveaux Usages

- Smartphones connectés à Internet > Ordinateurs
 - Smartphones beaucoup moins bien sécurisés
 - iPhone ® sécurisé de base, mais vulnérable une fois cracké
- Réseaux sociaux
- Cloud
- Il y a 15 ans, notion de réseau inconnue du grand public, aujourd'hui avec Internet, tout le monde le comprend, mais n'est pas compétent pour autant.
- Démocratisation d'internet et de l'informatique.
 - 3 milliards de personnes connectées,
 - 3 milliards de cibles pour les cyber cambrioleurs,
 - 3 milliards de pirates...
- Sites web illégitimes propagateurs de virus
- Sites web légitimes infectés



A new power is born ...



26

Institut Mines-Télécom

Enjeux Sécurité du SI



Tous pirates ?

M Société

SOCIÉTÉ

Police et justice Éducation Enquête Santé Centenaire 14-18 Religions Banlieue

Le logiciel espion Blackshades au cœur d'une grande enquête internationale

LE MONDE | 23.05.2014 à 19h45 • Mis à jour le 25.05.2014 à 13h55 |

Les enquêteurs le décrivent comme un « couteau suisse » de la cybercriminalité. Un logiciel espion pour pirate amateur, facile d'utilisation et accessible à tous.

M Blogs

10 juin 2014

INTRUSION 2.0 – Avec Shodan, contrôlez des webcams et imprimez chez les autres.

27

Institut Mines-Télécom

Enjeux Sécurité du SI



Information = Valeur Marchande

I GIVE PRIVATE INFORMATION ON CORPORATIONS TO YOU FOR FREE, AND I'M THE VILLAIN

Julian Assange

I GIVE YOUR PRIVATE INFORMATION TO CORPORATIONS FOR MONEY. AND I'M MAN OF THE YEAR

Mark Zuckerberg

28

Institut Mines-Télécom

Enjeux Sécurité du SI



Information = Valeur Stratégique

the guardian

NSA collecting phone records of millions of Verizon customers daily

Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama

Glenn Greenwald
The Guardian, Thursday 6 June 2013



M Amériques

INTERNATIONAL AMÉRIQUES Argentine Attentat de Boston Belize Bolivie Brésil

Edward Snowden

Verizon livre les relevés de ses abonnés aux renseignements américains

Le Monde.fr avec Reuters | 06.06.2013 à 06h08 • Mis à jour le 06.06.2013 à 12h00

29

Institut Mines-Télécom

Enjeux Sécurité du SI



Enjeux Economiques

Le marché de l'assurance contre les cyber risques va exploser ces prochaines années.

Global Security Mag, Jan 2016

M PIXELS

Le Monde.fr
23/09/2015

Le business des « zero day », ces failles inconnues des fabricants de logiciel.

Un million d'euros. C'est la somme qu'a promise, lundi 21 septembre, l'entreprise Zerodium à qui trouvera une faille informatique dans iOS 9, le nouveau logiciel qui équipe les iPhones.



Credence Research, Apr 2016

"In 2004, the global cybersecurity market was worth \$3.5 billion — and by 2017 it will be worth \$120 billion. "The cybersecurity market grew by roughly 35X over 13 years..."

We expect worldwide spending on cybersecurity products and services to eclipse \$1 trillion for the five-year period from 2017 to 2021"

Cybersecurity Ventures, Jun 2016

30

Institut Mines-Télécom

Enjeux Sécurité du SI



Enjeux Economiques

AP The Associated Press [Follow](#)

Breaking: Two Explosions in the White House and Barack Obama is injured

Reply Retweet Favorite More

662 RETWEETS 25 FAVORITES

10:07 AM - 23 Apr 13

CBS moneywatch Markets Investing Tech Leadership Small Business Saving Spending

DOW -11.31 14498.15 S&P 500 +0.08 1578.46 NASDAQ -5.56 3263.78 WILSHIRE -0.09

By ALAIN SHERTER / MONEYWATCH / April 23, 2013, 2:24 PM

Fake AP tweet sends stocks briefly plunging

Zoom: 1d 2d 1m 3m 6m YTD 1y 5y 10y All
Apr 23, 2013 - Apr 23, 2013 +128.98 (0.89%)

Tue Apr 23 11 am 12 pm 1 pm 2 pm 3 pm

TELECOM Evolution

Bug Bounty

LE FIGARO.fr tech & web Mis à jour le 04/05/2016

À 10 ans, il pirate Instagram et reçoit 10.000 dollars de récompense

Un jeune Finlandais a découvert une faille de sécurité permettant de supprimer les commentaires laissés sur les photos. Facebook, propriétaire d'Instagram, lui a offert 10.000 dollars.

Programme Bug Bounty

Un bug bounty est un programme proposé par de nombreux sites web et développeurs de logiciel qui permet à des personnes de recevoir reconnaissance et compensation après avoir reporté des bugs, surtout ceux concernant des exploits et des vulnérabilités. Ces programmes permettent aux développeurs de découvrir et de corriger des bugs avant que le grand public en soit informé, évitant ainsi des abus. Les bugs bounty ont été mis en place par Facebook, Yahoo!, Google, Reddit, et Square.

[Wikipedia](#)

32 Institut Mines-Télécom Enjeux Sécurité du SI TELECOM Evolution

Bug Bounty



LE MONDE | 20.06.2016

La défense américaine va étendre son programme incitant des hackeurs à chercher ses failles

1 410 participants, 138 failles repérées, plus de 70 000 dollars distribués : l'opération « Hack the Pentagon », annoncée en mars par le ministère américain de la défense, a porté ses fruits.



33

Institut Mines-Télécom

Enjeux Sécurité du SI



Agenda

1. Contexte
2. Les Entreprises et les Systèmes d'Information
3. Nouveaux Enjeux, Nouvelles Menaces , Nouveaux Usages
- 4. Principales Menaces**
5. Les Grands Principes de la Sécurité Informatique
6. Responsable Sécurité du Système d'Information
7. Le Cloud Computing
8. Conclusion

34

Institut Mines-Télécom

Enjeux Sécurité du SI



Principales Menaces

- **Spam (encore très répandu !) :**
courrier électronique non sollicité, généralement porteur de publicité ou de malware
- **Malwares :** logiciel malveillant qui peut espionner, détruire, saturer
 - ▶ **Virus :** programme malveillant se propageant en s'insérant dans des programmes légitimes
 - ▶ **Vers (Worm) :** virus se propageant par le réseau
 - ▶ **Cheval de Troie (Trojan) :** logiciel apparemment légitime qui effectue des actions à l'insu de l'utilisateur
 - ▶ **Porte dérobée (Backdoor) :** fonctionnalité qui ouvre un accès extérieur au système à l'insu de l'utilisateur
 - ▶ **Keylogger :** programme qui enregistre les touches tapées au clavier
- **Phone Scam :** Arnaque téléphonique (ex : Support MS)
- **Légende Urbaine / Canular (Hoax) :** rumeur destinée à être retransmise indéfiniment



Principales Menaces

- **Ingénierie sociale :** manipulation mentale visant à obtenir des informations confidentielles
- **Hameçonnage (Phishing) :** email orientant vers sites internet apparemment légitimes (collecte d'informations confidentielles).
- **Botnet :** ensemble d'ordinateurs légitimes piratés (bots) visant à lancer des campagnes de spams ou d'attaques.
- **Faux antivirus :** logiciel malveillant ayant l'apparence d'une solution de sécurité
- **Black Hat SEO :** manipulation des résultats des moteurs de recherche
- **0 day :** attaque sur vulnérabilité non encore connue
- **Clickjacking :** incitation à cliquer sur un lien qui déclenche un malware caché.
ex : Facebook likejacking



Ingénierie Sociale

The screenshot shows a web browser window for 'Banque Populaire Rives de Paris' at the URL www.rivesparis.banquepopulaire.fr/info-client.htm. The page features a logo for 'BANQUE POPULAIRE RIVES DE PARIS' and an 'ATTENTION' section. It contains a cartoon illustration of a burglar at a computer and text warning against fraudsters impersonating bank employees to request access codes for Cyberplus. A blue button labeled 'Poursuivre vers Cyberplus' is visible. To the right, a sidebar titled 'Les fiches de police de rappeurs divulguées' discusses the sharing of police files for rappers. The footer includes links for '37', 'Institut Mines-Télécom', 'Enjeux Sécurité du SI', and the 'TELECOM Evolution' logo.

Phishing / Hameçonnage

The screenshot displays two examples of phishing. On the left, a Trusteer mobile app promotional email to a customer, highlighting its security features for banking and messaging. On the right, a Facebook phishing attempt where a user's account has been deactivated; it prompts the user to sign in and provides a link to reactivate the account. The footer links are identical to the previous slide.

Phishing / Hameçonnage

Objet : [Votre facture n° 5656983JK]

Pour l'e-mail de recevoir tous nos emails, merci d'ajouter espaceclient@orange.fr
Votre carnet d'adresses email.
Si vous n'arrivez pas à lire cet e-mail, [suivez ce lien](#)

Problème de facturation:

Cher client :
Ce mail vous est envoyé en dernier avis, après plusieurs tentatives infructueuses de vous joindre sur votre numéro personnel.
En effet le 29/09/2011 une **encre bleue** a été produite lors des prélevements de la manœuvre effectuée sur votre compte ce dernier était doublument débité de la somme de cinquante-neuf quatre-vingt 59,80 € (59,90 €)*
Pour une régularisation immédiate de votre situation, et le remboursement de la somme débitée vous devez remplir instantanément le formulaire ci-dessous.

Cliquez ici pour activer votre compte

Merci pour votre compréhension.
Toute demande de rétractation des informations demandées entraîne conséquemment le rejet automatique de votre demande et le non remboursement de la somme 59,80 €.
Notre service décline toute responsabilité juridique à défaut d'une réponse immédiate de votre part et aucune réclamation ne sera acceptée.

Service Clients Mobile Orange 33732
BORDEAUX Cedex 9

Fabrice André
Directeur Service Client
www.Orange.fr

France Télécom SA au capital de 10 595 434 424 € - RCS Paris 389 129 866
place d'Alfort 75605 Paris Cedex 15

Merci de nous répondre à ce courrier électronique. Pour nous contacter, cliquez [ici](#).
Nous nous rappelons que France Télécom / Orange ne nous demandera jamais vos coordonnées bancaires par email, et vous invitons à nous signaler tout message suspect à l'adresse suivante abuse@orange.fr.

Les informations que vous nous fournissez sont traitées par France Télécom dans le cadre de l'exécution de votre contrat. Conformément à la loi Informatique et Libertés du 6 janvier 1978, vous disposez d'un droit d'accès, de rectification et d'opposition aux données vous concernant en écrivant à Orange Service Clients, Gestion des données personnelles, 33-34 Bordeaux Cedex 9 (indiquez vos nom, prénom, adresse, numéro de téléphone et joignez un justificatif d'identité).

Images !

39 Ins... www.clickforeplay.com/systeme-login.php

TELECOM Evolution

Phishing / Hameçonnage

edf

Cher(e)Client(e) EDF,

Nous avons constaté un impayé sur votre dernière facture.
Afin de régulariser votre situation veuillez vous référer ci-dessous :

Résoudre le problème maintenant

Lors d'échec de régularisation de votre situation, nous serions contraints de procéder à la suspension de votre approvisionnement en électricité.

Cordialement ,

Where do we send your 5 payments?
1 message

Danica <admin@cjsender.com> 23 février 2016 à 19:43
Répondre à : Danica <admin@cjsender.com> <christophe.darcy@gmail.com>

You have several payments due and as of yet we have been unable to send them despite attempting to contact you.

Full details enclosed here

We have no indication on our records of any payments been sent to you therefore you should complete and update your details as soon as you can.

Update here

We will then forward the 5 payments

Thanks again,
Danica

TELECOM Evolution

40 Institut Mines-Télécom Enjeux Sécurité du SI

Phishing / Hameçonnage

Hello,

Today we have completed and processed the payment of the outstanding balance of US\$ 1.2 Million as per attached swift copy.

We expect that it will reflect in your bank within 2-3 working days.

Please acknowledge receipt of the attached swift copy.

Dawn Chen
Manager of Shanghai Office
Sibneft Oil and Gas Company..
Mobile: 18621951943
Tel: 021-50896325
Fax: 021-50898117
Add: R44-203, Songjiang Caohejin Hi-Tech Park,
No.258, Xinzhuang Road, Shanghai.



Que devons nous faire de votre colis ?

1 message

Colis ref : 24345463 <laure@jenreman.com>
Répondre à : laure@jenreman.com
À : "christophe.darcy@mail.com" <christophe.darcy@mail.com>

30 juillet 2016 à 08:46

Bonjour,
Je vous informe que vous avez un potentiel colis d'une valeur de **500€** en attente de validation.



41

Institut Mines-Télécom

Enjeux Sécurité du SI

TELECOM
Evolution

Principales Menaces

- Les malwares s'attaquent à ce qui est le plus utilisé ou le plus à la mode :
 - ▶ PDF Reader, FlashPlayer
 - ▶ Facebook, Twitter
 - ▶ iPhones, Android
 - ▶ Recherches les plus répandues
 - ▶ Cloud Computing
 - ▶ Java
 - ▶ Ou pas : espionnage industriel, cyberguerre
 - ▶ APT : Advanced Persistent Threats
 - ▶ Stuxnet
 - ▶ Systèmes de process industriel



42

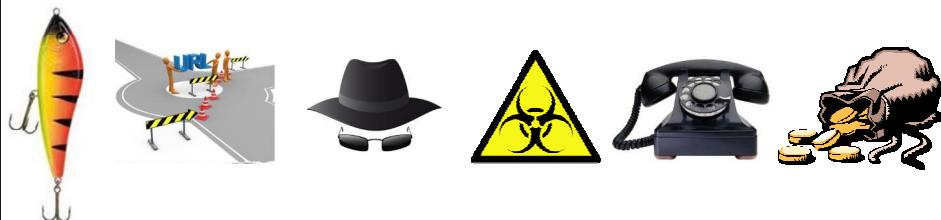
Institut Mines-Télécom

Enjeux Sécurité du SI

TELECOM
Evolution

Attaque Web en 6 Etapes

| 1. | 2. | 3. | 4. | 5. | 6. |
|--------|-------------------------------|--|-----------------------|---|----------------|
| Leurre | Redirection vers site infecté | Exploit Kit identifie les vulnérabilités de l'ordinateur | Installation du virus | Call Home Connexion avec les systèmes du pirate | Vol de données |



43

Institut Mines-Télécom

Enjeux Sécurité du SI



« Fraude au président »



Faux virements : l'enseigne Intermarché escroquée de 15 millions d'euros

Stéphane Sellami | 05 Mai 2015, 18h12 | MAJ : 05 Mai 2015, 19h29



Après avoir pris attaché avec un salarié du siège de cette enseigne, située dans le XVe arrondissement à Paris, les aigrefins sont parvenus à le convaincre d'opérer plusieurs virements vers des comptes bancaires, situés en Pologne.
LP

C'est une des dernières victimes connues de l'arnaque dite «au président», également baptisée escroquerie aux faux ordres de virement internationaux (FOVI)...

L'enseigne de grande distribution Intermarché a été ciblée, à la fin du mois d'avril, par des escrocs se faisant passer pour le PDG de cette entreprise.

44

Institut Mines-Télécom

Enjeux Sécurité du SI



« Fraude au président »

La « fraude au président » et ses variantes

- La « fraude au président »
Elle repose sur une usurpation d'identité. Un escroc se fait passer pour un haut responsable d'une entreprise et ordonne à un collaborateur d'effectuer un virement frauduleux en prétextant l'urgence et la confidentialité.
- La fraude par « malware »
Un logiciel espion contenu dans un courriel envoyé par le fraudeur permet de récupérer les codes de la banque en ligne de l'entreprise.

- Le changement d'Iban
Le fraudeur se fait passer pour un des fournisseurs de l'entreprise et envoie un faux courrier pour signaler un changement de banque et de numéro de compte. Parfois, le faux fournisseur a appelé l'entreprise quelques jours auparavant pour signaler un changement de coordonnées téléphoniques. Ainsi, si l'entreprise cherche à contrôler les coordonnées bancaires de son fournisseur, elle tombe sur le fraudeur.

« La « Fraude au président » représentait début 2015 plus de 400 millions d'euros de dommages pour les entreprises qui en ont été victime. Les tentatives – et les réussites – sont désormais quotidiennes. Au départ, il s'agissait plutôt de sociétés du CAC 40, parce qu'elles sont plus faciles à cerner par les fraudeurs, mais aujourd'hui les PME et les TPE sont également touchées. »

W. Dubost, Fédération bancaire française. Août 2015

Agenda

1. Contexte
2. Les Entreprises et les Systèmes d'Information
3. Nouveaux Enjeux, Nouvelles Menaces , Nouveaux Usages
4. Principales Menaces
- 5. Les Grands Principes de la Sécurité Informatique**
6. Responsable Sécurité du Système d'Information
7. Le Cloud Computing
8. Conclusion

Les Grands Principes de la Sécurité

- Confidentialité
 - ▶ l'information ne doit être accessible qu'aux personnes autorisées à y accéder,
 - ▶ elle doit demeurer indéchiffrable pour les autres,
 - ▶ cela reste vrai pendant les transferts.

- Intégrité
 - ▶ les données sont bien celles qu'elles sont censées être,
 - ▶ Possibilité de déterminer si les données n'ont pas été modifiées (volontairement ou non) pendant un traitement ou un transfert.



47

Institut Mines-Télécom

Enjeux Sécurité du SI



Les Grands Principes de la Sécurité

- Disponibilité
 - ▶ Maintien du bon fonctionnement du système d'information pour garantir l'accès à un service ou à des ressources
 - ▶ Accès aux informations et aux ressources associées, par les utilisateurs autorisés, lorsqu'ils en ont besoin.

- Non répudiation (Traçabilité, Preuve)
 - ▶ Garantie qu'une transaction ne peut être reniée
 - ▶ Maintien d'un audit des accès, actions ou échanges réalisés, en vue de contrôles ou de recherches de preuves.



48

Institut Mines-Télécom

Enjeux Sécurité du SI



Agenda

1. Contexte
2. Les Entreprises et les Systèmes d'Information
3. Nouveaux Enjeux, Nouvelles Menaces , Nouveaux Usages
4. Principales Menaces
5. Les Grands Principes de la Sécurité Informatique
- 6. Responsable Sécurité du Système d'Information**
7. Le Cloud Computing
8. Conclusion

49

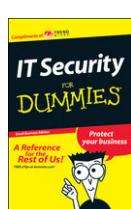
Institut Mines-Télécom

Enjeux Sécurité du SI



RSSI

- **Le Responsable de la Sécurité du Système d'Information**
 - ▶ Rôle de plus en plus important, complexe, et flou !
- **Garant des Technologies de Protection**
- **Gestion de la Sécurité Interne**
- **Plan de Continuité d'Activité**
- **Sécurité Physique**
- **Gouvernance**
- **Audits**



50

Institut Mines-Télécom

Enjeux Sécurité du SI



Technologies de Protection

- Protection des postes de travail et des serveurs
 - ▶ Antivirus
 - ▶ Firewall
 - ▶ Gestion des patchs de sécurité système et applicatif
 - ▶ Chiffrement
 - ▶ Auto run clefs USB et CD/DVD
- Protection des communications internes / externes
 - ▶ Access lists
 - ▶ Messagerie (spam, phishing, blacklists,...)
 - ▶ Messagerie instantanée
 - ▶ ToIP
 - ▶ Web (filtrage, blacklists,...)
 - ▶ Accès distants (VPN, portails,...)
 - ▶ WiFi

Risques associés
✓ Déni de service
✓ Perte de productivité
✓ Piratage
✓ Perte / vol d'information



Technologies de Protection

- Protection Périphérique
 - ▶ Firewall
 - ▶ Systèmes de détection et de prévention d'intrusion
- Protection des appareils mobile
 - ▶ Identification / Authentification
 - ▶ Chiffrement
 - ▶ Procédure en cas de perte ou de vol
- Détection et suivi des incidents de sécurité
 - ▶ Plate forme de supervision des incidents de sécurité
 - ▶ Workflow
 - ▶ Procédures d'escalade
 - ▶ Documentation



Sécurité Interne

- Gestion des identités et des droits d'accès
 - Gestion des identifiants et des mots de passe
 - Méta-annuaire
 - Account provisioning
 - Certification des habilitations
 - Signature unique (SSO)
 - Self service utilisateur
 - PKI
- Protection de l'information
 - Protection de la propriété intellectuelle
 - Protection des données individuelles et privées
 - Prévention de la fuite d'information (DLP)

Risques associés

- ✓ Non-conformité
- ✓ Poursuites pénales
- ✓ Perte / vol d'information

CONFIDENTIEL

53

Institut Mines-Télécom

Enjeux Sécurité du SI



Plan de Continuité d'Activité

- Evaluation des risques
- Définition de scénarios
- Rédaction de documentations
- Sélection des fournisseurs
- Formation des employés
- Tests réguliers
- Mises à jour des plans de continuité



Risques associés

- ✓ Déni d'image
- ✓ Non-conformité
- ✓ Perte de productivité
- ✓ Perte de marché



54

Institut Mines-Télécom

Enjeux Sécurité du SI



Sécurité Physique / Audit

- Sécurité physique
 - ▶ Accès
 - ▶ Protection incendie
 - ▶ Air conditionné
 - ▶ Onduleurs
 - ▶ Contrats de maintenance et d'entretien
- Audits
 - ▶ tests d'intrusion,
 - ▶ Application des standards techniques,
 - ▶ Application des politiques,
 - ▶ Conformité liée aux processus de l'entreprise,



55

Institut Mines-Télécom

Enjeux Sécurité du SI



Gouvernance

- Rédaction des politiques de sécurité (globale, spécifiques)
- Direction des projets exclusivement liés à la sécurité informatique
- Formation des équipes informatiques
- Formation et communication aux utilisateurs
- Sensibilisation des utilisateurs, tant dans l'usage professionnel que personnel.
 - ▶ Réticence naturelle
 - ▶ Bon usage
 - ▶ Diffusion des informations perso / pro sur les réseaux sociaux
- Pour tout ce qui a trait à l'informatique le RSSI est la liaison avec :
 - ▶ Le service de sécurité physique
 - ▶ Le service d'audit interne
 - ▶ Le service juridique
- Gestion du risque



56

Institut Mines-Télécom

Enjeux Sécurité du SI



Sensibilisation



Outil d'Audit

| A | B | C | D | E | F | G |
|------|--|-----------------------|----------|---|---|-------------|
| # | DESCRIPTION | REPONSE / COMMENTAIRE | RESULTAT | | | OBSERVATION |
| | | | 2 | 1 | 0 | |
| II.1 | Existence d'une politique de sécurité informatique interne | | | | | |
| II.2 | Existence d'une charte informatique faisant référence à cette politique de sécurité informatique | | | | | |
| II.3 | Existence de politiques de sécurité informatique spécifiques si nécessaires (mobiles, accès distant, WiFi,...) | | | | | |
| II.4 | Assurance que la politique de sécurité est communiquée à tous les niveaux de l'organisation | | | | | |
| II.5 | Promotion de la sécurité informatique, démonstrations de soutien et d'engagement par la direction générale vis-à-vis de la sécurité informatique : notes de services, objectifs généraux et individuels, ratification de la politique de sécurité par la direction, mentions dans réunions plénières,... | | | | | |
| II.6 | Signature par tout nouvel employé de la charte de sécurité informatique | | | | | |

Agenda

1. Contexte
2. Les Entreprises et les Systèmes d'Information
3. Nouveaux Enjeux, Nouvelles Menaces , Nouveaux Usages
4. Principales Menaces
5. Les Grands Principes de la Sécurité Informatique
6. Responsable Sécurité du Système d'Information
- 7. Le Cloud Computing**
8. Conclusion

59

Institut Mines-Télécom

Enjeux Sécurité du SI



Le Cloud Computing



« Le Cloud Computing est une offre de services qui propose des ressources informatiques matérielles ou logicielles « à la demande ». Que ce soit un espace de stockage, une plate-forme d'intégration, ou une solution logicielle complète, l'offre est disponible partout et à tout moment; elle est entièrement adaptée et calibrée en fonction des besoins utilisateurs.»

60

Institut Mines-Télécom

Enjeux Sécurité du SI



Cloud Computing

- Trois approches possibles :
 - ▶ privé interne : géré en interne par une entreprise,
 - ▶ privé externe : externalisé, mais dédié à une seule entreprise,
 - ▶ Public : géré par entreprises spécialisées qui louent leur services à de nombreuses entreprises.
- Particularité Importante du Cloud « Souverain » : 100% français
- Trois niveaux possibles :
 - ▶ SaaS (Software as a Service) : Logiciel en ligne
 - ▶ SalesForce.com (CRM), Google (Google Apps), Microsoft (Online Services)
 - ▶ PaaS (Platform as a Service) : Plate forme d'intégration / Middleware
 - ▶ Oracle
 - ▶ IaaS (Infrastructure as a Service) : Stockage
 - ▶ Amazon, DropBox

La Sécurité Exacerbée dans le Cloud

- Une des raisons du passage au Cloud est la baisse des coûts, or la sécurité est toujours le parent pauvre dans une baisse des coûts !!
- La virtualisation permet de créer une nouvelle instance très facilement et très rapidement. Or la rapidité vient souvent en opposition à la sécurité.



La Sécurité est la préoccupation majeure du passage au Cloud !

- Nécessité d'implémenter les outils et processus de façon encore plus rigoureuse
- Chiffrement (données stockées et en cours de transfert), IAM, DRM, double authentification, IDS/IPS, anti-malware

La Sécurité dans le Cloud

- **Exigences contractuelles et juridiques :**
 - ▶ Opérateurs implantés dans différents pays,
 - ▶ Exigences européennes non respectées,
- **Disponibilité :**
 - ▶ Défaillance de l'opérateur ou d'Internet
 - ▶ Taux de disponibilité contractuel et pénalités
 - ▶ Réplication
 - ▶ Résilience
 - ▶ Continuité
- **Traçabilité des accès et des changements**
- **Respect des réglementations et de l'état de l'art en matière de sécurité**
 - ▶ Audits par cabinets reconnus indépendants
- **Consommation énergétique**



63

Institut Mines-Télécom

Enjeux Sécurité du SI

TELECOM
Evolution

Les Fuites de Données dans le Cloud

- **Facteur humain**
 - ▶ Personnel du client : impunité, consumérisation, manque de confiance dans la solution.
 - ▶ Personnel de l'opérateur: couche supplémentaire de vulnérabilité
- **Passage par des réseaux non sécurisés ou non contrôlés**
- **Stockage dans pays non conformes aux exigences Européennes**
- **Législations locales (USA : droit d'audit)**
- **Etanchéité entre les clients ?**
- **Piratage de l'intérieur**
- **Garantie d'effacement des données ?**
- **Gestion des Changements (ex : DropBox)**



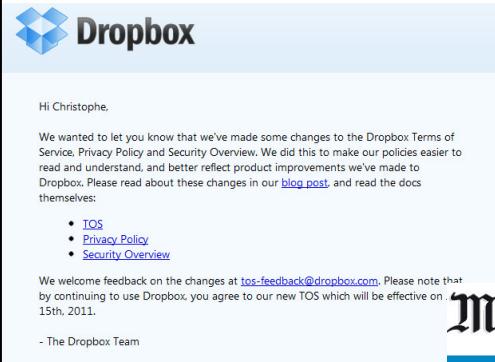
64

Institut Mines-Télécom

Enjeux Sécurité du SI

TELECOM
Evolution

Les Fuites de Données dans le Cloud



The screenshot shows an email from Dropbox. The subject line is "Dropbox - Les dernières modifications à nos termes d'utilisation". The body of the email starts with "Hi Christophe," and explains that they've made changes to their Terms of Service, Privacy Policy, and Security Overview. It encourages users to read these changes and the product improvements made to Dropbox. Links to the TOS, Privacy Policy, and Security Overview are provided. The message concludes with "We welcome feedback on the changes at tos-feedback@dropbox.com. Please note that by continuing to use Dropbox, you agree to our new TOS which will be effective on 15th, 2011." The message is signed off by "The Dropbox Team".

M Amériques

INTERNATIONAL AMÉRIQUES Argentine Attentat de Boston Belize Bolivie Brésil

Verizon livre les relevés de ses abonnés aux renseignements américains

Le Monde.fr avec Reuters | 06.06.2013 à 06h08 • Mis à jour le 06.06.2013 à 12h00

65 Institut Mines-Télécom Enjeux Sécurité du SI TELECOM Evolution

Et même des Pertes de Données

- Plan de continuité de l'opérateur: perte définitive des données en cas de sinistre majeur (ex: Amazon).
- Réversibilité : récupération des données ou transfert vers un autre opérateur.
- Effectuer ses propres sauvegardes
- L'opérateur Cloud devient une cible évidente pour un DOS majeur
- SPOH !
- Problème d'accès aux données (internet outage)



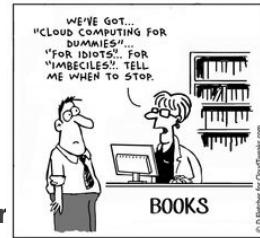
L'empilement des opérateurs démultiplie tous ces problèmes !

66 Institut Mines-Télécom Enjeux Sécurité du SI TELECOM Evolution

Et pourtant

Les entreprises continuent à utiliser le cloud, même si elles savent que ce n'est pas sûr !

- Le cloud paraît l'option disponible la plus sûre,
- Le cloud fournit un système de sauvegarde automatique,
- Les services cloud couvrent les coûts de maintenance,
- Le cloud c'est facile !
- Elles s'appuient sur le cloud sans même savoir que ce sont des services cloud,
- Elles n'ont pas conscience des alternatives.



Quelles Données dans le Cloud ?

« Le passage au Cloud nécessite une analyse très fine de l'ensemble des données de l'entreprise, et la définition d'une classification de ces données par sensibilité, risque de fuite, contraintes contractuelles et juridiques afin de déterminer la possibilité de les transférer ou de les gérer dans le Cloud, et chez quels types de fournisseurs. »

M Technologies

TECHNOLOGIES Jeux vidéo Hits Playtime Libertés numériques Téléphonie mobile Droit

"Pourquoi stocker toutes nos vies sur des serveurs aux Etats-Unis ?"

Le Monde.fr | 12.06.2013 à 19h24 • Mis à jour le 12.06.2013 à 23h48

C'est la première phase d'un projet DLP !

Agenda

1. Contexte
2. Les Entreprises et les Systèmes d'Information
3. Nouveaux Enjeux, Nouvelles Menaces , Nouveaux Usages
4. Principales Menaces
5. Les Grands Principes de la Sécurité Informatique
6. Responsable Sécurité du Système d'Information
7. Le Cloud Computing
- 8. Conclusion**

69

Institut Mines-Télécom

Enjeux Sécurité du SI



Menaces attendues

- De plus en plus d'utilisateurs connectés : Mobiles, applications cloud, menaces multi-plateformes (Windows 10), profilage social,
- Black Hat SEO sur événements à large diffusion (M. Schumacher, élections, événements sportifs, JO, Coupe du Monde, cinéma,...),
- NFC : Near Field Communication, paiement sans contact,
- Réseaux de process,
- Cyber-conflits : états, organisations, hacktivistes, ...
- Ransomware : déblocage d'un ordinateur contre rançon,
- Objets connectés,
- Big data,
- Pay By Phone.



70

Institut Mines-Télécom

Enjeux Sécurité du SI



Question à se poser



La 1^{ère} et véritable question à se poser
n'est pas tant :

« Puis-je être victime d'une APT ? »

mais plutôt

**« Quand vais-je l'être
ou
ne le suis-je pas déjà »**

71

Institut Mines-Télécom



Des moyens de protections



Maintenir à jour ses systèmes

- ▶ Systèmes et applications (Java, IE, PRA, etc.)
- ▶ Protection périphériques (Firewall, IDS, IPS, DLP, etc.)
- ▶ Solutions antivirales, antimalware, ..
- ▶ Pour mémoire :
 - ▶ L'attaque Aurora aurait pu être stoppée, ou ralentie si des utilisateurs n'utilisaient pas IE6.
 - ▶ Stuxnet exploitait de nombreuses vulnérabilités connues depuis très longtemps.



72

Institut Mines-Télécom



Des moyens de protections



Sensibiliser les utilisateurs

- A être vigilant



- A remonter toutes anomalies

- – Compte bloqué
- – Problème à l'ouverture d'un fichier (PDF ou autres)

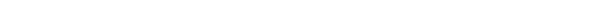
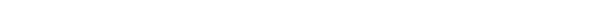
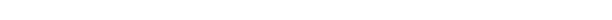
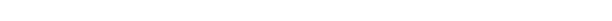
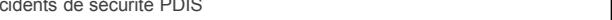


- Aux bonnes pratiques en matière d'hygiène de sécurité



73

Institut Mines-Télécom



Recommandations juridiques

- ▶ Déterminer comment protéger juridiquement un objet industriel connecté et ses composants
- ▶ Savoir quels choix opérer pour la mise sur le marché d'un objet industriel connecté
- ▶ Connaître les limites à l'exploitation des données
- ▶ Évaluer la responsabilité associée à l'utilisation d'un objet industriel connecté

75

Institut Mines-Télécom



Conclusion

- ▶ Les entreprises sont totalement dépendantes de leur SI
- ▶ Il n'y a plus de frontière entre informatique personnelle et professionnelle => perméabilité aux risques
- ▶ Les menaces sont toujours plus nombreuses, plus variées, plus sophistiquées et bénéficient de plus en plus de moyens
- ▶ Chaque nouveauté est une vulnérabilité
- ▶ Le RSSI a un rôle primordial, complexe, transversal, et de plus en plus flou
- ▶ L'externalisation des ressources ou des données n'entraîne pas une externalisation du risque
- ▶ La sensibilisation des utilisateurs est fondamentale : l'humain ne doit pas être considéré comme le maillon faible !



La garantie à 100% n'existe pas

La sécurité est l'affaire de tous !

76

Institut Mines-Télécom

Enjeux Sécurité du SI



Conclusion

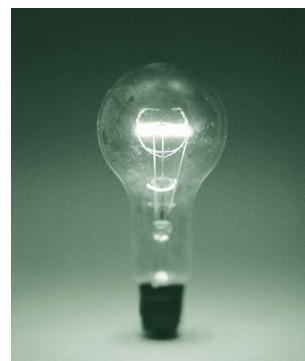
- ❖ Déterminer et maintenir une organisation relatives au processus de gestion du risque
- ❖ Identifier des responsabilités (RSSI, RPCA, DPO, CISO, CySE...)
- ❖ Disposer d'un PCA/PRA et le maintenir en condition opérationnelle
- ❖ Mettre en place une politique de gestion et de prévention de la fuite d'information
- ❖ Créer un centre de commandement des incidents cyber
- ❖ Implanter une cellule de GdC au sein de votre organisation
- ❖ Maintenir à jour tous vos systèmes de protection et vos machines dans votre entreprise
- ❖ ESF : Eduquer , Former , Sensibiliser
- ❖ Traiter les aspects juridiques
- ❖ Impliquer tous vos collaborateurs



TELECOM
Evolution

Q/R

Questions ?



TELECOM
Evolution



MANAGEMENT DE L'INFORMATION,
DU RISQUE ET DE LA
CONTINUITÉ D'ACTIVITÉ

79

Institut Mines-Télécom

