

Sécurité des Systèmes d'Information

Introduction

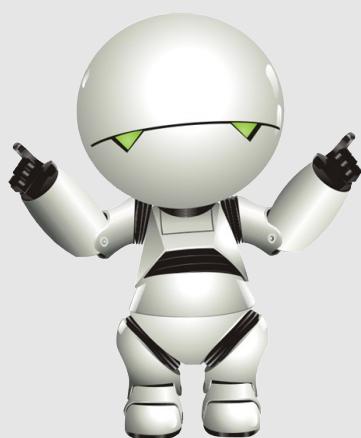
Michel Dubois

michel.dubois@esiea.fr

Dernière mise à jour: **20 juin 2017**



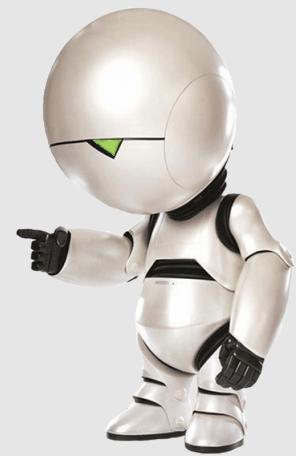
Partie 1 Pourquoi la SSI?



Pourquoi la SSI?

Section 1

Contexte



Contexte

Évolution du contexte



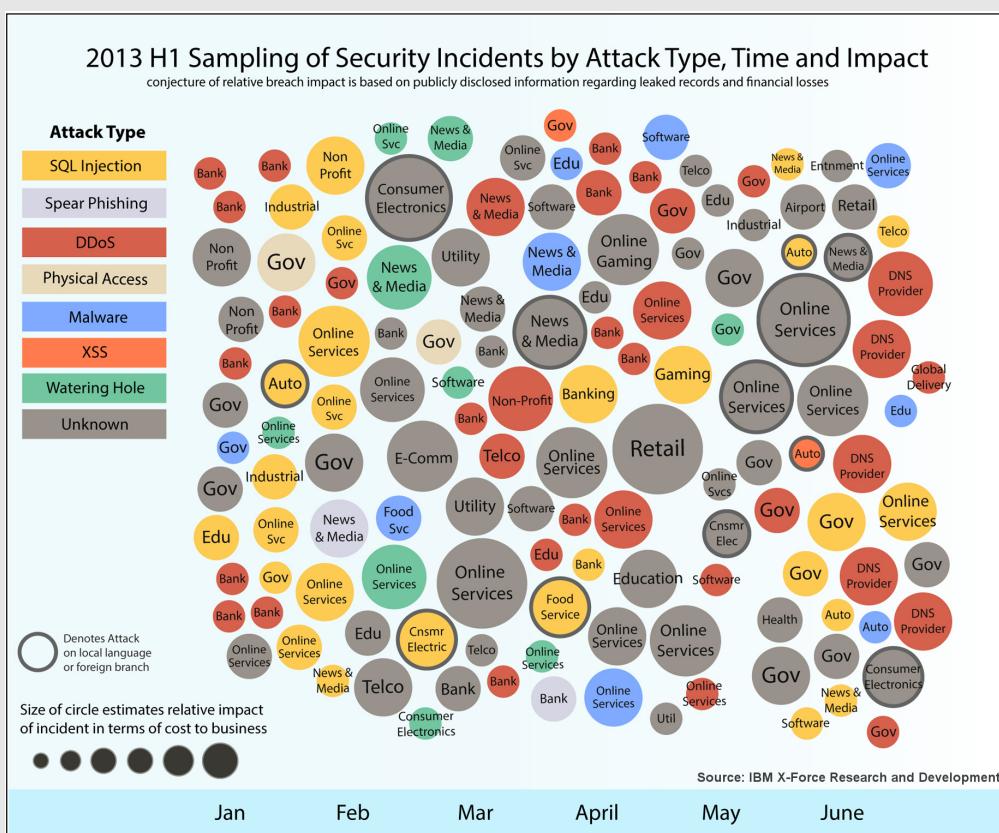
Pourquoi la SSI?

Section 2

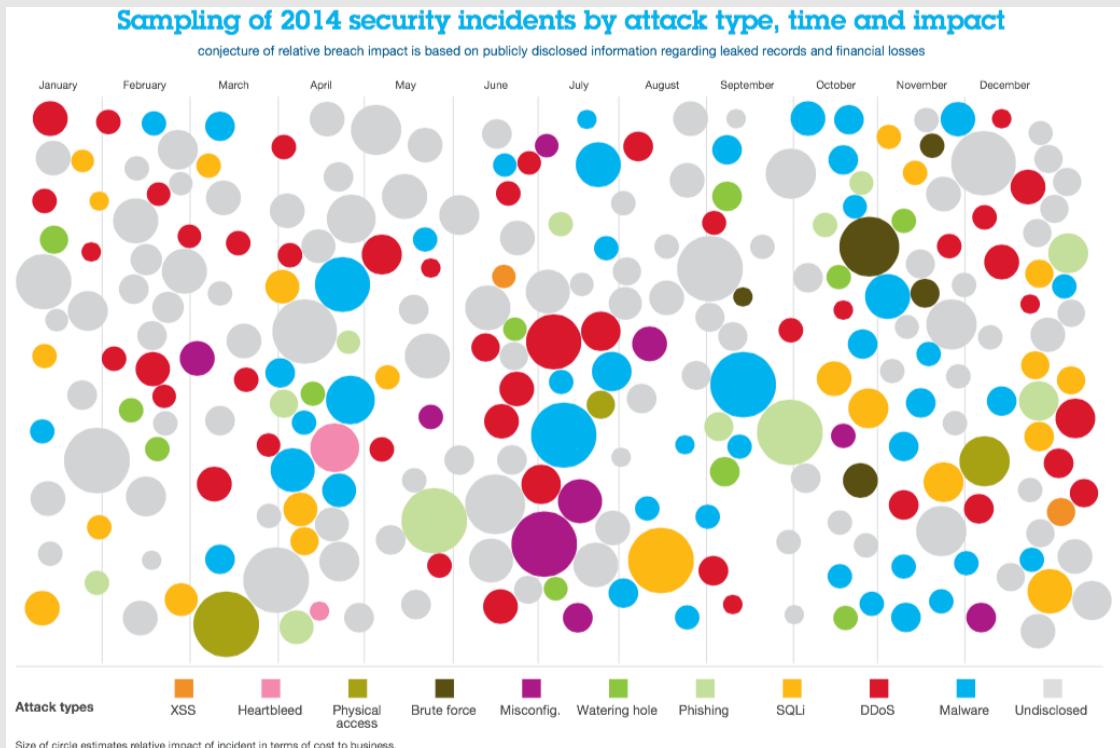
Généralités



Généralités



Généralités



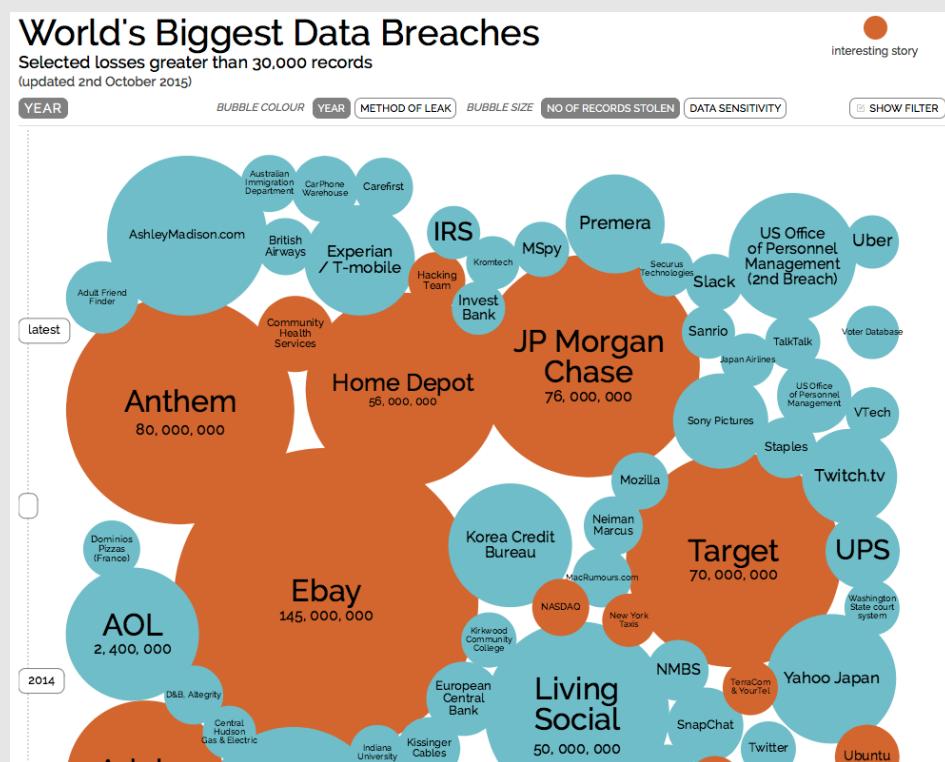
Source : <http://www-03.ibm.com/security/xforce/xfisi/>

SSI

Michel Dubois - 2017

7/404

Généralités



Source : <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

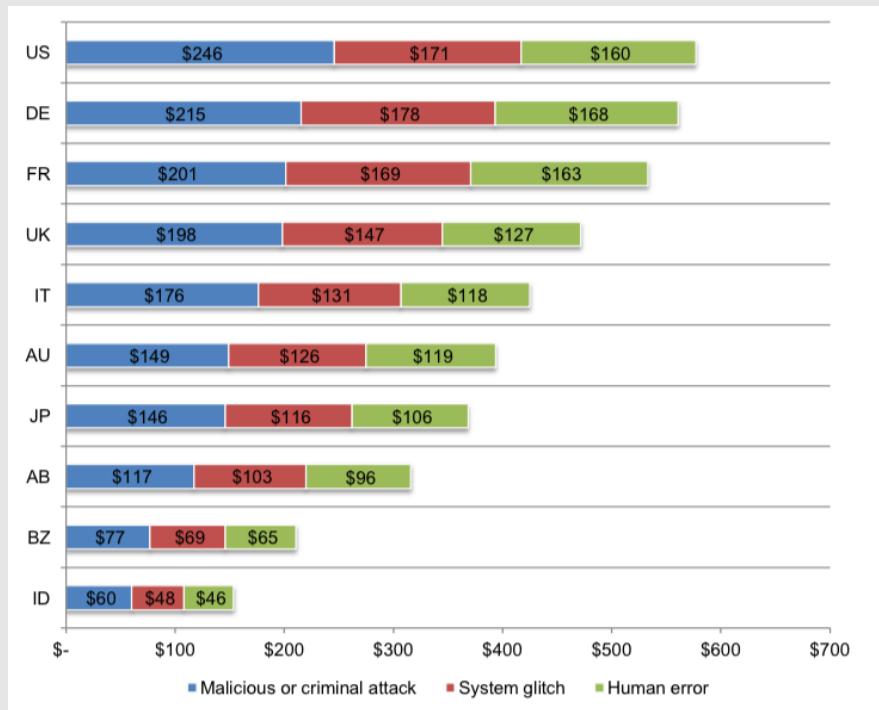
55

Michel Dubois - 2017

8/404

Généralités

Coût des attaques informatiques



Source : <http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/>

SSI

Michel Dubois - 2017

9/404

Pourquoi la SSI?
Section 3
Actualités 2012



Actualités 2012

Piratage - LinkedIn - 5 juin 2012 - 6,5 millions de comptes utilisateurs divulgués

An Update on LinkedIn Member Passwords Compromised



Vicente Silveira June 6, 2012

in Share

3,229

Tweet

J'aime

573

G+1

924

We want to provide you with an update on this morning's reports of stolen passwords. We can confirm that some of the passwords that were compromised correspond to LinkedIn accounts. We are continuing to investigate this situation and here is what we are pursuing as far as next steps for the compromised accounts:

1. Members that have accounts associated with the compromised passwords will notice that their LinkedIn account password is no longer valid.
2. These members will also receive an email from LinkedIn with instructions on how to reset their passwords. There will not be any links in this email. Once you follow this step and request password assistance, then you will receive an email from LinkedIn with a password reset link.
3. These affected members will receive a second email from our Customer Support team providing a bit more context on this situation and why they are being asked to change their passwords.

SSI

Michel Dubois - 2017

11/404

Actualités 2012

DDoS contre l'Iran - octobre 2012 - Internet ralenti dans le pays



Source : <http://www.reuters.com/article/us-iran-cyber-idUSBRE8920M020121003>

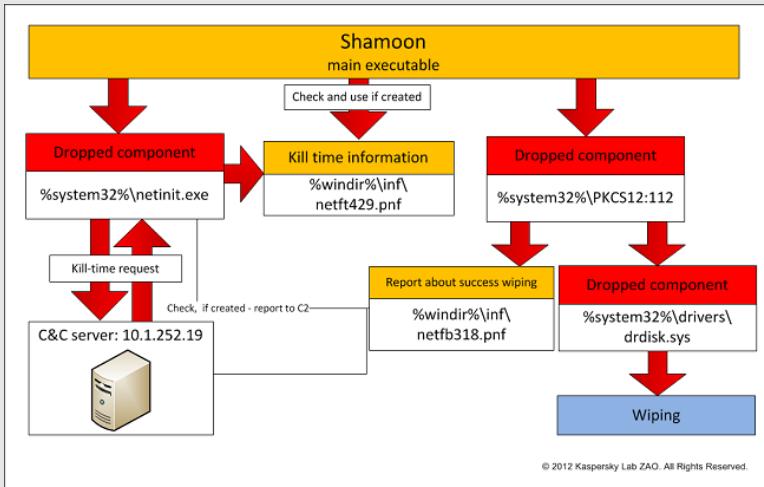
SSI

Michel Dubois - 2017

12/404

Actualités 2012

Attaque virus **Shamoon** - Saudi Aramco - 15 août 2012
- 30000 ordinateurs effacés - Cutting Sword of Justice



Source : http://www.theregister.co.uk/2012/08/29/saudi_aramco_malware_attack_analysis

SSI

Michel Dubois - 2017

13/404

Pourquoi la SSI?
Section 4
Actualités 2013



SSI

Michel Dubois - 2017

14/404

Actualités 2013

Vol de données - 4 octobre 2013

The screenshot shows a news article from USA Today. The headline is "Adobe loses 2.9 mil customer records, source code". The article is by Byron Acohido, USA TODAY, published at 10:16 a.m. EDT on October 4, 2013. The story discusses a data breach where hackers gained unauthorized access to 2.9 million customer accounts and stole part of the source code for at least two major consumer-facing products. The company admitted to the breach. The article includes a photo of two office buildings and social sharing options for Facebook, Twitter, and Email.

SSI

Michel Dubois - 2017

15/404

Actualités 2013

Hacktivisme - avril 2013

"Syrian hackers" break into Associated Press Twitter account and break news that explosions at White House have injured Obama - sending DOW Jones plunging 100 points

A tweet from AP (@AP) with the text: "Breaking: Two Explosions in the White House and Barack Obama is injured". The tweet has 1,181 retweets and 52 favorites. Below the tweet is a chart showing the Dow Jones Industrial Average (DJI) Index (R1) dropping sharply around 18:15 on April 23, 2013, from approximately 14680 to 14554, a drop of about 126 points.



SSI

Michel Dubois - 2017

16/404

Actualités 2013

Hacktivisme - avril 2013



SSI

Michel Dubois - 2017

17/404

l'Humanité.fr

ENVIES DE CHANGER LE MONDE

A LA

POLITIQUE SOCIAL-ECO SOCIÉTÉ ENVIRONNEMENT

A+ A- Partager cet article

MONDE l'Humanité.fr le 8 Avril 2013

Nouvelle attaque massive d'Anonymous contre Israël

Mots clés : israël, gaza, internet, Anonymous, tel-aviv,

L'OpIsraël, initiée par Anonymous lors de la dernière attaque sur Gaza, est relancée. L'attaque d'une ampleur rare contre Israël aurait déjà causé de lourds dommages économiques.

Ce weekend, le collectif Anonymous, avec d'autres groupes de plusieurs pays, de Tunisie, d'Algérie, du Maroc, de France, de Mauritanie et des États-Unis notamment, ont lancé une attaque massive sur les services Internet israéliens. Rien de très fin : du déni de service distribué, de piratage de comptes bancaires (30000 revendiqués), et quelques attaques ayant pour but de récupérer des données, contre des services militaires et ministériels.

Au total, plus de 100 000 sites israéliens sont inaccessibles, 200 000 numéros de carte bleue ont été publiés, mais aussi des dizaines de milliers de pages

Actualités 2013

... Orange F 22:43 30 %

Cyberattaque contre une entreprise de lutte contre le spam

28.03.13 | 09:40 | Le Monde.fr avec AFP



Les pirates visaient Spamhaus, une entreprise qui recense les adresses de spams dont se servent les messageries pour filtrer les courriels indésirables. REUTERS/KACPER PEMPEL

Spamhaus, une entreprise basée à Genève qui traque les adresses de spams dont se servent les messageries pour filtrer les courriels indésirables, a annoncé avoir été victime d'une importante attaque informatique de type "déni de service" - le blocage d'un site ou d'un service par un très grand nombre de connexions non-sollicitées. D'après l'entreprise l'opération aurait commencé le 18 mars, après que le groupe a placé sur sa liste noire Cyberbunker, un site Internet néerlandais.

... Orange F 09:25 90 %

Des hackers détournent 45 millions de dollars sur des comptes bancaires

10.05.2013 à 07:24 | Le Monde.fr avec AFP



Un clavier d'ordinateur. REUTERS/STOYAN NENOV

Des pirates informatiques ont dérobé en deux opérations près de 45 millions de dollars dans 26 pays, participant, selon la justice américaine, "à un énorme braquage de banques" d'un genre nouveau. L'affaire a été révélée jeudi 9 mai par le bureau de la procureure de New York, qui a inculpé huit personnes soupçonnées d'appartenir à une cellule de pirates établie à New York. Le réseau s'étendrait au total sur 26 pays et aurait agi lors de deux opérations distinctes, le 22 décembre 2012 et les 19/20 février

SSI

Michel Dubois - 2017

18/404

Actualités 2013

.... Orange F 3G 09:34 89 %

Pays-Bas : les sites du gouvernement victimes d'une cyberattaque

08.05.2013 à 12:10 | Le Monde.fr avec AFP



Près de 10 millions de Néerlandais avaient été privés fin avril de l'utilisation de leur signature électronique officielle, qui permet notamment de payer ses impôts en ligne.
REUTERS/BOGDAN CRISTEL

Les sites du gouvernement néerlandais, au nombre desquels figurent également les sites de tous les ministères, sont sur le coup d'une cyberattaque, a-t-on appris mercredi 8 mai auprès du gouvernement. Cette attaque informatique a pris la forme dite du "déni de service" (DDOS), qui se traduit par un nombre très élevé de demandes de connexions non sollicitées qui finissent par bloquer un site.

.... Orange F 3G 08:03 85 %

Des hackers chinois ont pénétré les systèmes du Pentagone

29.05.2013 à 07:41 | Le Monde.fr



Un chasseur F-18, un des avions auxquels les hackers ont eu accès. AFP/ADRIAN DENNIS

Selon des informations du *Washington Post*, confirmées par des responsables du Pentagone, des hackers chinois ont réussi à pénétrer des systèmes informatiques dans lesquels étaient stockés les plans de plusieurs armes américaines, dont des avions et des missiles.

Selon le quotidien américain, les pirates informatiques ont, entre autres, eu accès aux plans du système de missiles Patriot, du système de radar ultramoderne Aeagis, du

SSI

Michel Dubois - 2017

19/404

Actualités 2013

.... Orange F 3G 06:47 84 %

US warns of cyber attacks on medical devices

June 14, 2013, 2:47 am
AFP



WASHINGTON (AFP) - US authorities on Thursday warned makers of medical devices and hospital networks to step up efforts to guard against potential cyber attacks.

.... Orange F 3G 07:28 68 %

Obama ne pense pas que Prism viole les libertés individuelles

16.06.2013 à 22:00 | Le Monde.fr avec Reuters



Le GCHQ (Government Communications Headquarters), service de renseignements électroniques du gouvernement britannique, est impliqué dans le scandale du cyberespionnage. REUTERS/HANDOUT

Barack Obama ne croit pas que le programme Prism de surveillance des réseaux téléphone et internet par la NSA viole les libertés individuelles des Américains, a déclaré dimanche le chef d'état-major de la Maison blanche, Denis McDonough.

Intervenant dans l'émission "Face the Nation" de CBS, ce collaborateur du chef de

SSI

Michel Dubois - 2017

20/404

Actualités 2013

Smartphone screen showing news from Le Monde.fr about the Prism surveillance program. The screen displays the headline "Prism : la NSA espionnait l'Union européenne" and a photograph of Edward Snowden. The news article discusses how the NSA spied on European Union member states through the Prism program.

Le Point.fr news article about Germany's ban on iPhone usage in parliament, featuring a photo of Angela Merkel holding a BlackBerry smartphone.

Comments section with 4 comments, sharing options, and font size controls.

SSI Michel Dubois - 2017 21/404

Actualités 2013

Smartphone screen showing news from Le Monde.fr about Apple's developer site being hacked. The screen displays the headline "Le site d'Apple dédié aux programmeurs d'applications piraté" and a screenshot of the Apple Developer website with a message stating "We'll be back soon." The news article discusses the hacking of the developer site and the subsequent downtime.

Le Point.fr news article about cyberwarfare becoming a new military issue, featuring a close-up of a computer keyboard.

SSI Michel Dubois - 2017 22/404

Actualités 2013

... Orange F 20:39 84 %

Cyberespionnage : quatre ordinateurs disparaissent toutes les heures à Roissy-Charles-de-Gaulle



Copyright Reuters

Share 0

Michel Cabirol | 03/07/2013, 16:36 - 652 mots

21 % des utilisateurs d'ordinateurs volés à l'aéroport Roissy-Charles-de-Gaulle estiment qu'ils contenaient des informations confidentielles qui ne sont pour la plupart pas chiffrées (93 %). Autre vulnérabilité pour les entreprises, les smartphones utilisés de façon quotidienne pour des usages

SSI Michel Dubois - 2017 23/404

... Orange F 3G 18:02 82 %

Un hacker pénètre la chambre d'une petite fille à travers son baby monitor

14.08.2013 à 17:35 | Blog : Big Browser



Un baby monitor Motorola (Binatoneglobal/Wikimedia Commons)

Il est rare qu'un fait divers aussi angoissant finisse comme un gag. L'histoire qui suit, contée par la chaîne américaine ABC News (voir le reportage vidéo ci-dessous), s'est déroulée à Houston, au Texas, dans l'appartement d'un jeune couple, ou plus

SSI Michel Dubois - 2017 23/404

Actualités 2013

Erreur humaine - décembre 2013

... Orange F 09:35 43 %

googleonlinesecurity.blogspot.de

Google Online Security Blog

Saturday, December 7, 2013

Further improving digital certificate security

Posted by Adam Langley, Security Engineer

Late on December 3rd, we became aware of unauthorized digital certificates for several Google domains. We investigated immediately and found the certificate was issued by an [intermediate certificate authority](#) (CA) linking back to ANSSI, a French certificate authority. Intermediate CA certificates carry the full authority of the CA, so anyone who has one can use it to create a certificate for any website they wish to impersonate.

07:09 46 %

Google bloque des certificats de sécurité Internet émis par une autorité française

08.12.2013 à 15:58 | Le Monde.fr



Une personne utilise Google sur une tablette tactile. AFP/DAMIEN MEYER

Une potentielle importante faille de sécurité pour les internautes a été évitée. Google a annoncé samedi avoir bloqué plusieurs certificats de sécurité émis par une autorité de certification liée à l'Agence nationale de la sécurité des systèmes d'information (Anssi, l'organisme chargé de la sécurité informatique de l'Etat français), après avoir découvert que ces certificats étaient possiblement corrompus.

... Orange F 09:34 43 %

ssi.gouv.fr

ANSSI Agence nationale de la sécurité des systèmes d'information

Que faire en cas d'incident ? Le site du CERTA Portail de la sécurité informatique/Documentation

Vous êtes ici : Accueil > menu > Actualités > Suppression d'une branche de l'IGC/A

Suppression d'une branche de l'IGC/A

7 décembre 2013

Suite à une erreur humaine lors d'une action de renforcement de la sécurité au ministère des finances, des certificats numériques correspondant à des domaines extérieurs à l'administration française ont été signés par une autorité de certification de la direction générale du Trésor rattachée à l'IGC/A.

Cette erreur n'a eu aucun conséquence sur la sécurité des réseaux de l'administration ni sur les internautes. La branche considérée de l'IGC/A a été coupée à titre préventif.

Un renforcement des procédures de l'IGC/A est en cours d'étude pour éviter qu'un tel incident ne puisse se reproduire.

ssi.gouv.fr Flux RSS Contacts Informations éditeur Aide et accessibilité Presse Actualités Plan

Portail général de la défense et de la sécurité nationale - Portail du gouvernement

Service public France.fr

SSI Michel Dubois - 2017 24/404

Actualités 2013

Hacktivisme - vendredi 1^{er} novembre 2013



SSI

Michel Dubois - 2017

25/404

Actualités 2013

Hacktivisme - vendredi 1^{er} novembre 2013

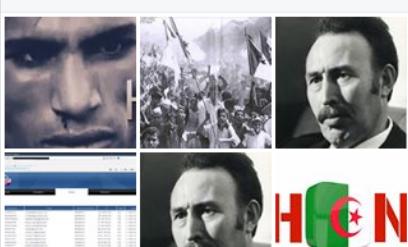
A screenshot of a Facebook page for "Over-x Hocine". The page header shows a profile picture of a man with a mustache. The main banner features a close-up of a person's face with the text "Hcn Over-x Hocine". Below the banner, the page name "Over-x Hocine (Hcn)" is displayed, along with buttons for "Ajouter" (Add), "S'abonner" (Subscribe), and "Message". Navigation tabs include "Journal", "À propos", "Photos", "Amis", and "Plus".

Vous connaissez Over-x ?

Pour voir ce qu'il partage avec ses amis, envoyez-lui une invitation.

Ajouter

Photos - 63



Over-x Hocine a partagé un lien.
il y a 2 heures

هدية اول نوفمبر دخول احد دومنيات موقع وزارة الدفاع الفرنسية



Accueil
www.esa.sante.defense.gouv.fr

L'école de santé des armées (ESA) forme des jeunes gens se destinant à une carrière de médecin ou pharmacien militaire au sein du service de ...

SSI

Michel Dubois - 2017

26/404

Actualités 2013

Hacktivisme - vendredi 1^{er} novembre 2013

- "Je lance mes actions contre la France en souvenir des **martyrs Algériens**."
- "Je choisis des sites qui ont de l'**influence**, des espaces **gouvernementaux**."
- "C'est plus **efficace** pour être entendu, en plus des pertes financières."
- "Les **fichiers**, voilà la chose la plus importante pour moi. Les emails, les noms, les numéros de téléphone."
- Pseudonyme sur Internet **Over-X**
- 22 ans
- habite à Hadjout Wilaya de Tipaza en Algérie
- plus de 5000 piratages depuis 2011

Source : <http://archives.zataz.com/news/23170/pirate-algerie-over.html>

Pourquoi la SSI? Section 5 Actualités 2014



Actualités 2014

Hacktivisme - mars 2014



A VIRUS HAS BEEN DETECTED
--FIXING SYSTEM FAILURE--



01Business LE MAGAZINE APPLI 01

Retours d'expérience | Guides pratiques | Dossiers | Portraits | Agenda | Emploi | Télécharger pro |

E-commerce | Start-up | Sécurité | Infrastructure | SSI | Telecoms/mobile | Cloud | Logiciels & applicat



L'imprimante multifonction.
Réérite par HP.

En savoir plus

01Business > Avis d'expert

La dimension cybernétique de la crise ukrainienne

Le conflit ukrainien a aussi lieu dans le cyberspace, et les cyberattaques peuvent donner des indications sur les prochaines manœuvres ayant lieu sur le terrain. Difficile cependant de savoir à qui profitent ces opérations.

Daniel Ventre | 01Business | le 24/03/14 à 07h00 | [laisser un avis](#)



Les acteurs militaires ou civils des conflits armés s'efforcent d'exploiter le cyberspace au mieux de leurs intérêts. Traitant des événements en Ukraine, les médias internationaux se sont fait l'écho ces derniers jours d'informations qui tendraient à démontrer, une nouvelle fois, que les réseaux se trouvent au cœur de l'action : défigurations de sites internet (d'institution, entreprises, ministères), attaques par déni de service, intrusion dans des serveurs et vols de données sensibles, propagation de malwares (le virus Snake, actif depuis plusieurs années, aurait infecté des réseaux gouvernementaux ukrainiens), attaques contre

SSI

Michel Dubois - 2017

29/404

Actualités 2014

Négligence - vendredi 27 juin 2014



This is a photo taken by Brazilian newspaper Correio Braziliense of police chief Luiz Cravo Dorea taken at the the World Cup main command and control security center.

wifi network "WORLDCUP" password "b5a2112014" (leet speak for Brazil 2014)

Source: http://thehackernews.com/2014/06/fifa-world-cup-security-team_26.html

SSI

Michel Dubois - 2017

30/404

Actualités 2014

Vandalisme - 16 mars 2014



"Deux centraux téléphoniques ont été détruits par des incendies dans la nuit de samedi à dimanche en Haute-Garonne (à Bessières et Villemur-sur-Tarn) privant 8000 abonnés de téléphone fixe et d'ADSL."

"Des centraux opportunément incendié pendant qu'un gang de malfaiteurs pénétrait dans la salle des coffres de l'agence du Crédit Agricole."

SSI

Michel Dubois - 2017

31/404

Actualités 2014

Atteinte à un STAD - mercredi 18 juin 2014

We are experiencing massive demand on our support capacity, we are going to get to everyone it will just take time.

Code Spaces : Is Down!

Dear Customers,

On Tuesday the 17th of June 2014 we received a well orchestrated DDOS against our servers, this happens quite often and we normally overcome them in a way that is transparent to the Code Spaces community. On this occasion however the DDOS was just the start.

An **unauthorised** person who at this point who is still unknown (All we can say is that we have no reason to think its anyone who is or was employed with Code Spaces) had gained access to our Amazon EC2 control panel and had left a number of messages for us to contact them using a hotmail address

Reaching out to the address started a chain of events that revolved around the person trying to extort a large fee in order to resolve the DDOS.

Upon realisation that somebody had access to our control panel we started to investigate how access had been gained and what access that person had to the data in our systems, it became clear that so far **no** machine access had been achieved due to the intruder not having our Private Keys.

Code Spaces will not be able to operate beyond this point, the cost of resolving this issue to date and the expected cost of refunding customers who have been left without the service they paid for **will put Code Spaces in a irreversible position** both financially and in terms of on going credibility. As such at this point in time **we have no alternative but to cease trading** and concentrate on supporting our affected customers in exporting any remaining data they have left with us.

Source : <http://www.codespaces.com>

SSI

Michel Dubois - 2017

32/404

Actualités 2014

Atteinte à un STAD - mercredi 18 juin 2014

From: mike dudson <mikedudson@hotmail.com>
Reply-to: <mikedudson@hotmail.com>

how did u like the ddos attacks on ur server
and deleted ur files lol ur security is zero
we ow3ned and hacked ur sorry asses
<https://www.facebook.com/groups/HackersElite452/>

put ur website up we will trash it again

we are hackers elite Anonymous
we do not forgive
we do not forget
expect us

SSI

Michel Dubois - 2017

33/404

Actualités 2014

Piratage - décembre 2014



Sony Pictures paralysé par un piratage informatique

Le Monde.fr avec AFP,
le 12 décembre 2014 à 18h52

Son réseau informatique a été victime d'une attaque, les pirates menaçant désormais de rendre publiques des informations stratégiques sur cette filiale du groupe japonais.

Le réseau informatique de Sony Pictures a été victime d'une attaque. Les pirates menacent désormais de rendre publiques des informations stratégiques sur cette filiale du groupe japonais Sony, selon le site spécialisé *The Next Web*, mardi 25 novembre. Une source au sein de Sony a indiqué au site qu'un « serveur a été touché et que l'attaque s'est ensuite disséminée à partir de là ».

La société n'était pas joignable pour commenter ces

ANALYSE

Ce que révèlent les milliers de documents confidentiels volés à Sony Pictures

Par Michaël Szadkowski,
le 12 décembre 2014 à 18h54

Des centaines de gigaoctets de fichiers ont déjà été diffusés par des pirates. Une situation catastrophique pour le géant du divertissement hollywoodien.

Imaginez que toutes les données – ou presque – qui transittent sur votre ordinateur de travail, stockées sur les disques durs et serveurs de votre entreprise, soient compilées et rendues accessibles à tous. Voilà la situation devant laquelle se retrouvent actuellement les employés et la direction de Sony Pictures Entertainment, après l'attaque informatique de grande ampleur subie le 24 novembre. Depuis, des milliers de gigaoctets de fichiers confidentiels du géant du divertissement hollywoodien, producteur et diffuseur de nombreux films, sont dispersés sur le Web.

Un mécanisme bien rodé

Les pirates, réfugiés derrière l'acronyme #GOP (pour Guardian of Peace), avaient au départ évoqué onze terabytes de documents (11 000 gigaoctets) subtilisés lors de leur attaque. Ils parlent maintenant de « dizaines de téabytes » de données – une centaine, disent les médias américains. Qu'un tel volume de données ait effectivement été volé semble de plus en



Amy Pascal a démissionné de ses fonctions de vice-présidente de Sony Pictures

Le Monde.fr avec AP,
le 5 février 2015 à 20h41

Des éléments compromettants tirés de sa messagerie avaient été rendus publics après le piratage dont avait été victime l'entreprise.

Deux mois et demi après l'attaque informatique menée contre Sony Pictures, la vice-présidente de l'entreprise, Amy Pascal, a démissionné.

Parmi les dizaines de milliers de documents dérobés et diffusés sur le Web par les pirates en novembre, figuraient les courriels de sa messagerie électronique professionnelle. S'y trouvaient notamment des échanges privés avec de nombreux membres de l'industrie du cinéma américain.

SSI

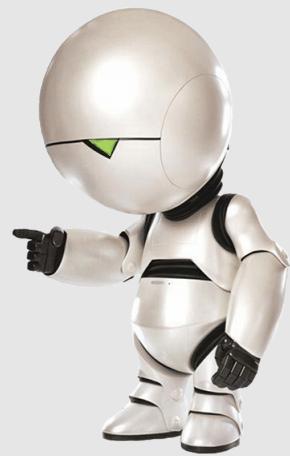
Michel Dubois - 2017

34/404

Pourquoi la SSI?

Section 6

Actualités 2015



Actualités 2015

Sabotage - mardi 10 mars 2015

Un pays entier coupé du monde à cause d'un sabotage Internet



Par Challenges.fr
Voir tous ses articles

Publié le 10-03-2015 à 12h25



L'accès à Internet au Gabon et les communications téléphoniques à l'international ont été gravement perturbés durant 24 heures en raison d'un acte de "sabotage".



La Gabon a été coupé du monde pendant 24 heures à cause d'une panne Internet AFP

L'accès à Internet au Gabon et les communications téléphoniques à l'international ont été gravement perturbés durant 24 heures en raison d'un acte de "sabotage", a annoncé mardi 10 mars Gabon Telecom, le principal opérateur du pays, déjà paralysé il y a deux semaines par une grève.

Le sabotage a visé, selon le fournisseur d'accès internet, un câble de fibre optique dans un quartier de Libreville.

"Vers quatre heures du matin, des individus sont venus saboter le câble sous-marin Sat 3 en faisant en sorte que le trafic international, c'est-à-dire la voix, l'internet et les autres transmissions de données soit perturbés", a affirmé le directeur réseau de Gabon Telecom, Firmin Ngoye, cité par le quotidien national l'Union.

Selon l'opérateur, le rétablissement total du réseau devrait prendre deux à trois jours.

Actualités 2015

Piratage et demande de rançon - mars 2015

Labio.fr piraté : demande de rançon et publication de résultats médicaux

Allo docteur, j'ai mal à ma sécurité 123



SECURITÉ

Crédits : GuidoVrola/Stock/ThinkStock

Le laboratoire de biologie médicale Labio est la cible d'un groupe de pirates. Ce dernier revendique avoir dérobé pas moins de 40 000 identifiants (nom, prénom, login et mot de passe), ainsi que « des centaines » de bilans médicaux. Une rançon de 20 000 euros est demandée et les fuites d'informations confidentielles ont déjà commencé.

Les demandes de rançons sont de plus en plus courantes dans le cas des piratages de données informatiques. Récemment, on a par exemple le cas de SynoLocker sur les NAS Synology, de Feedly, puis de Domino's Pizza. Dans ce dernier cas, la société nous avait indiqué qu'elle se refusait à céder aux demandes de son maître chanteur, le groupe de pirates Rex Mundi, et qu'aucune transaction financière n'aurait lieu. Des données avaient finalement été mises en ligne quelques mois plus tard.

Rex Mundi demande une rançon de 20 000 euros ou des résultats d'analyse seront publiés

Source : <http://www.nextinimpact.com/news/93499-labio-fr-pirate-demande-rancon-et-publication-resultats-medicaux.htm>

SSI

Michel Dubois - 2017

37/404

Actualités 2015

Piratage du compte Twitter de l'US central command par le cybercaliphate - lundi 12 janvier 2015

Profile summary

CyberCaliphate

Profile picture: A globe with a grid pattern.

bio: We love you isis

TWEETS 3,674 FOLLOWING 1,268 FOLLOWERS 109K

U.S. Central Command
@CENTCOM

Official Twitter for U.S. Central Command (CENTCOM). *Follow/RT does not equal endorsement.

MacDill AFB, Tampa, FL · centcom.mil

Followed by Anthony De Rosa, WikiLeaks, Department of State and 4 others.

U.S. Central Command @CENTCOM - 57s
We won't stop! We know everything about you, your wives and children.
pic.twitter.com/ixz82ICDES

Details

U.S. Central Command @CENTCOM - 2m
ISIS is already here, we are in your PCs, in each military base.
pic.twitter.com/xaftqTMvN5

Details

U.S. Central Command @CENTCOM - 8m
pic.twitter.com/SdaOK06Zkr

Details

Go to full profile

19:14

U.S. Central Command
@CENTCOM

In the name of Allah, the Most Gracious, the Most Merciful,
the CyberCaliphate continues its CyberJihad.

18:44 - 12 janv. 15

Reponde à U.S. Central Command

SSI

Michel Dubois - 2017

38/404

Actualités 2015

Piratage de TV5monde - mercredi 8 avril 2015



1. piratage du compte Twitter
2. piratage du compte Facebook
3. piratage du compte Youtube
4. Défacement du site Web
5. Blocage du serveur de messagerie
6. Arrêt des retransmissions TV
7. Messages de menace contre les militaires français et leurs familles
8. publication de données prétendues classifiées

Source : <https://reflets.info/piratage-de-tv5monde-loperation-cyber-pieds-nickeles/>

SSI

Michel Dubois - 2017

39/404

Actualités 2015

Piratage de TV5monde - mercredi 8 avril 2015

Sécurité défaillante - Mdp : lemotdepassedeyoutube



SSI

Michel Dubois - 2017

40/404

Actualités 2015

Piratage de TV5monde - **mercredi 8 avril 2015**

Démenti du Ministère de la défense

Mise à jour : 10/04/2015 15:22

Attaque contre TV5Monde : le ministère de la Défense dément la publication de documents confidentiels le concernant

Dans la soirée du mercredi 8 avril, la chaîne de télévision TV5Monde a subi une attaque informatique. Les attaquants ont perturbé ses moyens de diffusion et ont pris le contrôle de son site Internet et de ses comptes Facebook et Twitter. Des messages de propagande ont alors été diffusés. Parmi ceux-ci figuraient des menaces proférées contre les militaires français et leur famille. Des documents prétendument confidentiels ont été mis en ligne.

Après un examen minutieux de l'ensemble de ces documents par la chaîne de cyberdéfense des armées, les services du ministère de la Défense et ceux du ministère de l'Intérieur, il s'avère qu'aucun de ces documents ne mentionne l'identité de militaires français ni de leur famille. Le ministère de la Défense dément ainsi catégoriquement que les individus s'en étant pris aux moyens de diffusion de TV5Monde aient publié des documents confidentiels le concernant.

S'agissant des activités sur les réseaux sociaux et plus généralement sur Internet, le ministère réitère ses appels à la vigilance à l'ensemble de la communauté de Défense. La menace exercée par les groupes terroristes à l'encontre de notre pays et de nos ressortissants demeure en effet à un niveau élevé.

Source : <http://www.defense.gouv.fr>

SSI

Michel Dubois - 2017

41/404

Actualités 2015

Piratage de la Hacking Team's - **dimanche 5 juillet 2015**

The screenshot shows the Twitter profile of the Hacked Team (@hackingteam). The profile picture is a stylized logo consisting of the letters 'HT' enclosed in brackets. The bio reads: 'Developing ineffective, easy-to-pwn offensive technology to compromise the operations of the worldwide law enforcement and intelligence communities.' It includes location information ('Milan, Italy'), a website link ('hackingteam.com'), and a joining date ('Joined July 2011'). A 'Tweet to Hacked Team' button is visible. The stats show 217 tweets, 36 following, 3,359 followers, and 3 favorites. Two tweets are visible: one pinned tweet from July 5, 2015, stating 'Since we have nothing to hide, we're publishing all our e-mails, files, and source code mega.co.nz/#!Xx1lhChT!rbB... infotomb.com/eyyxo.torrent' with 643 retweets and 397 likes; and another tweet from July 5, 2015, stating 'Of course not, it's a chance to upsell! They need to pay us for training so they learn'.

Hacking Team is a Milan-based information technology company that sells **offensive intrusion and surveillance capabilities** to governments, law enforcement agencies and corporations. Its **Remote Control Systems** enable governments and corporations to monitor the communications of internet users, decipher their encrypted files and emails, record Skype and other Voice over IP communications, and remotely activate microphones and camera on target computers.

Source : <http://thehackernews.com/2015/07/Italian-hacking-team-software.html>

SSI

Michel Dubois - 2017

42/404

Actualités 2015

Piratage de la Hacking Team's - dimanche 5 juillet 2015

The screenshot shows a Twitter profile for Christian Pozzi (@christian_pozzi). His bio says he joined in March 2013. He has 39 tweets, 30 following, and 186 followers. His first tweet reads: "We are closing down. Bye Saudi Arabia. You paid us well. Allahuhakbah." His second tweet says: "Uh Oh - my twitter account was also hacked." His third tweet states: "We are currently working closely with the police at the moment. I can't comment about the recent breach."

500 gigabytes of internal data leaked over the Internet. The leaked data revealed a zero-day cross-platform Flash exploit (CVE-2015-5119). Also revealed in leaked data was Hacking Team employees use of weak passwords, including P4ssword, wolverine, and universo.

Source : https://en.wikipedia.org/wiki/Hacking_Team

SSI

Michel Dubois - 2017

43/404

Actualités 2015

Piratage de la Hacking Team's - dimanche 5 juillet 2015

The screenshot shows an email in Microsoft Outlook. The subject is "Re: Letter from the Sudan Panel Coordinator". It is from David Vincenzetti to Alessandra Tarissi. The email body contains a message in Italian:

mercoledì prossimo incontro a Praga una mia collega di New York che è Head del Human Rights Department di ABA (American Bar Association) e che l'anno scorso mi aveva invitato, come forense ricordarci, a fare uno speech a UN a Ginevra sul tema business lawyers e il loro ruolo nel campo HR/corporate responsibility, tema molto caldo

Io stessa sto approfondendo la materia durante questo break estivo.

Comunque mi piacerebbe fare un double check anche con la mia collega US prima di decidere cosa fare anche con questa seconda lettera. ovviamente matemò riservato il nome di HT.

Un caro saluto

Alessandra

Avv. Alessandra Tarissi De Jacobis

Cocuzza & Associati
Via San Giovanni sul Muro 18
20121 Milano
www.cocuzzaeassociati.it
tel. +39 02-866096
fax. +39 02-862650

The leaked data indicates that the spyware company did sell powerful spyware tools to oppressive regimes in Sudan, Bahrain, Ethiopia and Saudi Arabia.

Source : https://en.wikipedia.org/wiki/Hacking_Team

SSI

Michel Dubois - 2017

44/404

Actualités 2015

Piratage de Ashley Madison - mercredi 15 juillet 2015 - the Impact Team



Aucun site Web ne peut garantir la protection de vos données privées : identité, carte de crédit, photos personnelles,...
AshleyMadison.com, an American most prominent dating website, that helps married people cheat on their spouses has been hacked, potentially putting very private details of Millions of its users at risk of being exposed.

Source : <http://thehackernews.com/2015/08/ashley-madison-hack.html>

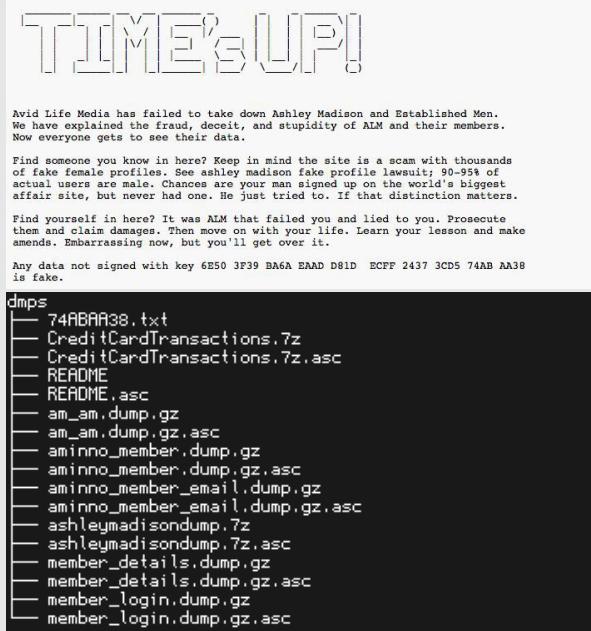
SSI

Michel Dubois - 2017

45/404

Actualités 2015

Piratage de Ashley Madison - mercredi 15 juillet 2015 - the Impact Team



Vol et diffusion de 10 Go de données client et 20Go de données internes à l'entreprise

- 33 millions de comptes divulgués
- non effacement des données utilisateurs
- utilisation majoritaire de bots féminins
- pas de protection des mots de passe
- 260000 adresses emails françaises
- utilisation de mails professionnels
- plusieurs suicides

Source : https://en.wikipedia.org/wiki/Ashley_Madison_data_breach
<http://geekbeat.tv/everything-we-know-about-the-ashley-madison-hack-plus-find-out-if-youre-on-the-list>

SSI

Michel Dubois - 2017

46/404

Actualités 2015

Internet des objets - 29 septembre 2015

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWARE SCIENCE BOOTNOTES FORUMS

Security

Thousands of 'directly hackable' hospital devices exposed online

Hackers make 55,416 logins to MRIs, defibrillator honeypots



More like this

Security

Most read

- The future of Firefox is ... Chrome
- Windows 10 debuts Blue QR Code of Death – and why malware will love it
- Bundling ZFS and Linux is impossible says Richard Stallman
- How to not get pwned on Windows: Don't run any virtual machines open

http://www.theregister.co.uk/2015/09/29/thousands_of_directly_hackable_hospital_devices_found_exposed/

SSI Michel Dubois - 2017 47/404

Actualités 2015

Internet des objets - 29 septembre 2015

SHODAN healthcare

Exploits Maps Share Search Download Results Create Report

TOP COUNTRIES



Country	Count
United States	312
United Kingdom	21
Germany	12
India	10
Japan	8

TOP SERVICES

Service	Count
Telnet	111
HTTP	69
FTP	69
2000	64
HTTPS	41

TOP ORGANIZATIONS

Total results: 432
74.213.39.17
74-213-39-17.static.logixcom.net
Logix
Added on 2016-04-11 18:55:36 GMT
United States, Houston
Details

52.16.203.234
ec2-52-16-203-234.eu-west-1.compute.amazonaws.com
Amazon.com
Added on 2016-04-11 18:02:00 GMT
Ireland, Dublin
Details

SSL Certificate
Issued By:
Common Name: EJTE-DV-SV-02-CA
Issued To:
Common Name: staging.app.enovatehealthcare.co.uk
Organization: Enovate Healthcare
Ldt

Supported SSL Versions
SSLv3, TLSv1, TLSv1.1, TLSv1.2

Diffie-Hellman Parameters
Fingerprint: RFC2409/Oakley Group
2

SSI Michel Dubois - 2017 48/404

Actualités 2015

PCA - US Navy - 15 octobre 2015

The US Navy is reinstating the ancient art of celestial navigation to fight a very modern threat



Sometimes old school is best. In today's US Navy, navigating a warship by the stars instead of GPS is making a comeback.

The Naval Academy stopped teaching celestial navigation in the late 1990s, deeming the hard-to-learn skill irrelevant in an era when satellites can relay a ship's location with remarkable ease and precision.

But satellites and GPS are [vulnerable to cyber attack](#) (paywall). The tools of yesteryear—sextants, nautical almanacs, volumes of tables—are not. With that in mind, the academy is [reinstating celestial navigation](#) into its curriculum. Wooden boxes with decades-old instruments will be dusted off and opened, and students will once again learn to chart a course by measuring the angles of stars.

Old school navigation pales in comparison to today's high-tech systems. It's both painfully difficult and far less precise. But it can get you where you need to go within about 1.5 miles (2.4 kilometers). That could be a matter of life and death in a scenario where [modern technology has been compromised](#).

[http:](http://qz.com/524795/the-us-navy-is-reinstating-the-ancient-art-of-celestial-navigation-to-fight-a-very-modern-threat)

//qz.com/524795/the-us-navy-is-reinstating-the-ancient-art-of-celestial-navigation-to-fight-a-very-modern-threat

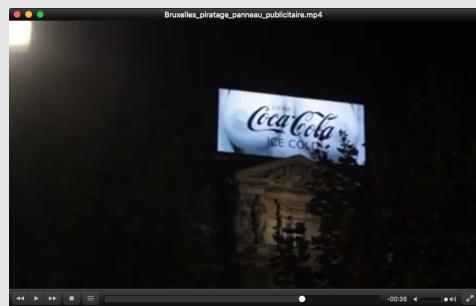
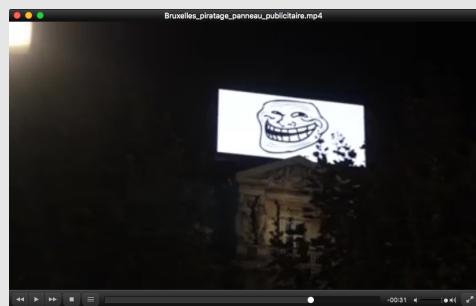
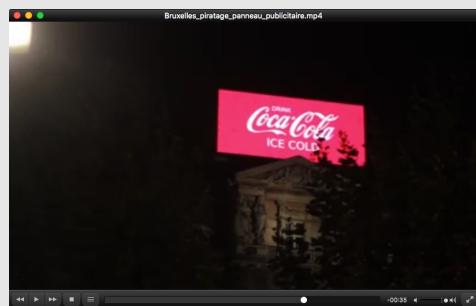
SSI

Michel Dubois - 2017

49/404

Actualités 2015

Piratage d'un écran publicitaire - Bruxelles - lundi 28 décembre 2015



Source: <http://bigbrowser.blog.lemonde.fr/2015/12/28/piratage-dun-ecran-publicitaire-geant-a-bruxelles>

SSI

Michel Dubois - 2017

50/404

Actualités 2015

Attaque de centrales électriques - mercredi 23 décembre 2015 - Ukraine



Une variante du malware BlackEnergy a paralysé plusieurs centrales électriques Ukrainiennes, causant une coupure électrique dans une partie du pays

Source :

http://motherboard.vice.com/en_uk/read/malware-found-inside-downed-ukrainian-power-plant-points-to-cyberattack

SSI

Michel Dubois - 2017

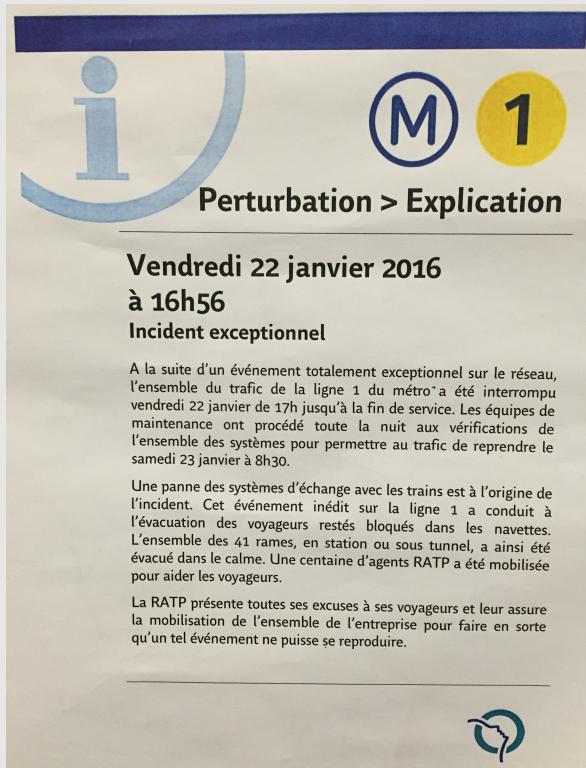
51/404

Pourquoi la SSI?
Section 7
Actualités 2016



Actualités 2016

Panne d'éléments actifs réseaux - vendredi 22 janvier 2016



SSI

Michel Dubois - 2017

53/404

Actualités 2016

Trop de sécurité? Analyse des risques? - février 2016

ÉTATS-UNIS - Un antivirus bloque la supervision de pose d'un cathéter cardiaque au beau milieu d'une opération chirurgicale

Un équipement médical considéré comme critique, Merge Hemo, s'est subitement éteint lors d'une opération cardiaque en février 2016. En cause, le balayage d'un antivirus sur l'ordinateur relié à Merge Hemo, qui s'est déclenché automatiquement et qui a bloqué les communications, entraînant une interruption brutale du service. Le personnel a eu exactement cinq minutes pour redémarrer et configurer à nouveau l'ordinateur et l'application Merge Hemo, sans mettre en danger la vie du patient opéré et endormi. L'entreprise Merge a précisé que des instructions précises recommandaient de placer Merge Hemo dans la liste blanche des antivirus. L'incident avait été immédiatement rapporté à la Food and Drug administration américaine.

MERGE HEALTHCARE MERGE HEMO PROGRAMMABLE DIAGNOSTIC COMPUTER		Back to Search Results
Model Number	MERGE HEMO V9.40.1	
Device Problems	Use of Incorrect Control Settings; Use of Device Issue	
Event Date	02/08/2016	
Event Type	Malfunction	
Event Description	<p>Merge hemo monitors, measures, and records physiological data from a human patient undergoing a cardiac catheterization procedure. The system comprises the patient data module and the hemo monitor pc. The two units are connected via a serial interface. All vital parameters and evaluations are registered and calculated in the patient data module. This data is then transmitted to the hemo monitor pc via the serial interface. All data can be shown and monitored on the hemo monitor pc. On (b)(6) 2016, a customer reported to merge healthcare that, in the middle of a heart catheterization procedure, the hemo monitor pc lost communication with the hemo client and the hemo monitor went black. Information obtained from the customer indicated that there was a delay of about 5 minutes while the patient was sedated so that the application could be rebooted. It was found that anti-malware software was performing hourly scans. With merge hemo not presenting physiological data during treatment, there is a potential for a delay in care that results in harm to the patient. However, it was reported that the procedure was completed successfully once the application was rebooted.</p>	
Manufacturer Narrative	<p>Based upon the available information, the cause for the reported event was due to the customer not following instructions concerning the installation of anti-virus software; therefore, there is no indication that the reported event was related to product malfunction or defect. The product security recommendations, (b)(4), explicitly state, "the intent of these guidelines is to configure the anti-virus software so that it does not affect clinical performance and uptime while still being effective. To accomplish this, the anti-virus software needs to be configured to scan only the potentially vulnerable files on the system, while skipping the medical images and patient data files. Our experience has shown that improper configuration of anti-virus software can have adverse affects including downtime and clinically unusable performance.".</p>	
Search Alerts/Recalls		

https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/detail.cfm?mdrfoi_id=5487204

SSI

Michel Dubois - 2017

54/404

Actualités 2016

Hacktivisme - lundi 22 février 2016 -
www.cimd.interarmees.defense.gouv.fr

- Motivations : State of Emergency, Arm Trade, OpNATO, OpAfrica
- Vol et diffusion de données nominatives

<https://www.cyberguerrilla.org/blog/anonymous-hacks-subsites-of-french-defense-ministry/>

SSI

Michel Dubois - 2017

55/404

Actualités 2016

Internet des objets - 6 mars 2016

Hacking industrial vehicles from the internet

MARCH 6TH, 2016

It is possible to monitor and control float trucks, public bus or delivery vans from the internet, obtaining their speed, position, and a lot other parameters. You can even control some parameters of the vehicle or hack into the canbus of the vehicle remotely.

Those vehicles have a Telematics Gateway Unit (TGU) device and a 3g/4g/gprs/lte/edge/HSPA modem to connect to the internet, with a public IP address.

There are thousands of TGU connected to the internet, with no authentication at all and with administrative interfaces through a web panel or a telnet session.

Finding publicly exposed TGUs in the internets

There are tons of open TGU and similar vehicle appliances on the internet. One very interesting and easy to find is the c4max.

The c4max smartbox is a TGU with powerful capabilities, a simple console on port 23, and is easy to identify while scanning the internet.



<http://jcarlosnorte.com/security/2016/03/06/hacking-tachographs-from-the-internets.html>

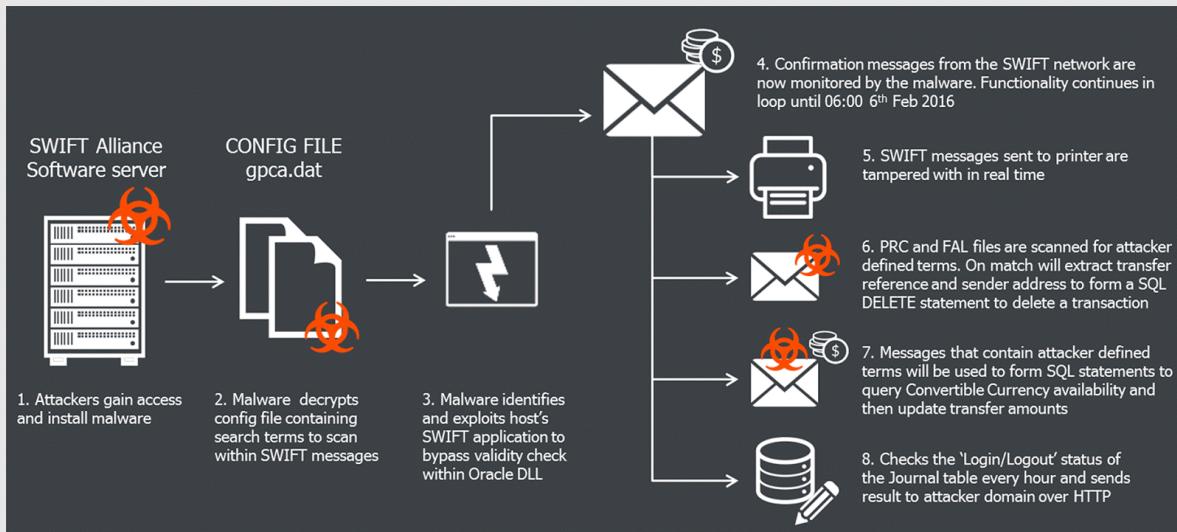
SSI

Michel Dubois - 2017

56/404

Actualités 2016

81M\$ volés de comptes de la Bangladesh central bank - mars 2016



- the Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a cooperative owned by 3000 financial institutions
- the Swift banking system is used to transfer billions internationally every day
- the attackers obtained valid credentials for operators authorised to create and approve Swift messages, then submitted fraudulent messages by impersonating those people

<http://www.theguardian.com/world/2016/mar/15/bangladesh-central-bank-governor-resigns-over-81m-dollar-cyber-heist>

SSI

Michel Dubois - 2017

57/404

Actualités 2016

Bug logiciel - mars 2016

IHS Jane's 360
Defence

C4ISR: Air
F-35 mission software stability poses greatest risk to USAF IOC
Marina Malenik, Washington, DC - IHS Jane's Defence Weekly
06 March 2016

A software stability problem that interferes with the F-35 radar's ability to remain on while in flight poses the greatest threat to achieving USAF IOC in 2016. Source: Lockheed Martin

Key Points

- A software glitch that interferes with the F-35 radar's ability to remain working in flight poses the greatest threat to meeting the USAF's IOC schedule
- Training on a new increment of ALIS and a fuel pressure modification are the other two unresolved issues

F-35 radar system has bug that requires hard reboot in flight
Virtual BSOD for radar software could delay USAF's full deployment of fighter.

by Sean Gallagher - Mar 10, 2016 5:15pm CET

"Hello, tech support?"
Dan Stjovich @ Flickr

In an episode of CBS' techno-procedural series *CBS/Cyber* that aired in January, pilots were forced to power off and power back on an airliner's flight computer to regain control from a hacker. As preposterous as that cold-boot of avionics sounds, it's something that test pilots have had to do with the F-35A "Lightning II" Joint Strike Fighter's radar system—not because of a hack but because of a software problem that causes the radar to degrade or stop working

The Pentagon's New List of F-35 Bugs Is Predictably Awful

Michael Nunez
2/03/16 11:03am
Filed to: PENTAGON

55.8K 5

The F-35 Joint Strike Fighter program is the most expensive military program in the world, so it should be no surprise that the F-35 aircraft is loaded with powerful weapons controlled by powerful computers.

SSI

Michel Dubois - 2017

58/404

Actualités 2016

Vague de ransomwares - janvier/décembre 2016



SSI

Michel Dubois - 2017

59/404

Actualités 2016

Ransomware - 16 février 2016 Hollywood Presbyterian Medical Center

◀ Back to Twitter 09:31 lefigaro.fr

LE FIGARO.fr tech & web

Un hôpital américain paralysé par des pirates informatiques

TECH & WEB | Mis à jour le 16/02/2016 à 15:21

Credit photo : PHILIPPE HUGUEN/AFP

EN BREF

- Le réseau informatique de cet établissement californien est paralysé depuis une semaine.
- On lui réclame une rançon de plus de 3,4 millions de dollars.
- Les «ransomwares» sont un type d'attaques informatiques qui visent les entreprises.

Peut-on soigner des malades sans Internet? Depuis plus d'une semaine, un hôpital situé à



Un hôpital américain paye une rançon à des pirates informatiques

Le 18 février 2016 à 10h11

Le centre médical presbytérien d'Hollywood, en Californie, était infecté par un logiciel de racket, un programme utilisé par les pirates pour demander des rançons.

A près plus d'une semaine de paralysie, le centre médical presbytérien d'Hollywood a repris mercredi 17 février une activité normale. L'établissement victime d'un logiciel de racket a payé une rançon de 17 000 dollars en bitcoins, une

- 1 semaine de travail en mode dégradé
- transfert des patients sensibles
- 3,4 millions de dollars (9000 bitcoins) de rançon
- 17000 dollars versés
- Absence de sauvegardes

SSI

Michel Dubois - 2017

60/404

Actualités 2016

Vague de ransomwares - janvier/décembre 2016 - Locky

Enable macro if the data encoding is incorrect

3XVFC,,пів№ъ...-6уD-©ХИЁКЎ_?™
ЛсйгР,Г\$|f<%оъ ктд%у} ЙльR7iK9-йN+‘®Шf<ХЇ!Сп\$O>-”-
іб[шZSfA‘\$□□4iНыы}°ЂЖBSLzo
Лъ\Х3x°0¤'e"]!ЖДcLgIг□B9Й1©frfуk»Х†If6YINkë€ВО-
u□ЙАСБИ‡е©“±μ1V□±s□\$Lj%цы[шГ‘л-
;с©Вч+Ь4яяДSp[, шфзХ'ў«їмъ<“Fбркуї/”Гдљ>”
Ч©и”oRЬ"ЯrCg•кa†ібфСВА8МСК>4...k•&тиБ¶эLCJХCM”Rљ□*АДШуГВк’...ђЗиїГы\$O-
đыIN□|sSS3|□Ю5Щн?ЛЎР}TM ...Р в'АтІшv~hФбъBr>A5'3
мїзЭ&&JF"‡5@|¤hM¶ГВ†'ЖкъИ <Be©hјB€·DjTБ...Ж;иgW-
3¶kh[ђУшжO<EPB□@TM5□Hu,,8IИµВхм&в□Ner=nI¶TM©<VTM,Ю\,ьQтmg|•HEрш[А
nШгГМ±3љЛ[Ю]P24<3- @ШN4
ою,3К],ГJхu,4-»L0Чг'ЖТйСкNPЧЎRГeb

Actualités 2016

Vague de ransomwares - janvier/décembre 2016 - Locky

!!! IMPORTANT INFORMATION !!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.

More information about the RSA and AES can be found here:

[http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:

1. <http://3ezlvkoi7fwyood.tor2web.org/78634AFEA4011440>
2. <http://3ezlvkoi7fwyood.onion.to/78634AFEA4011440>
3. <http://3ezlvkoi7fwyood.onion.cab/78634AFEA4011440>

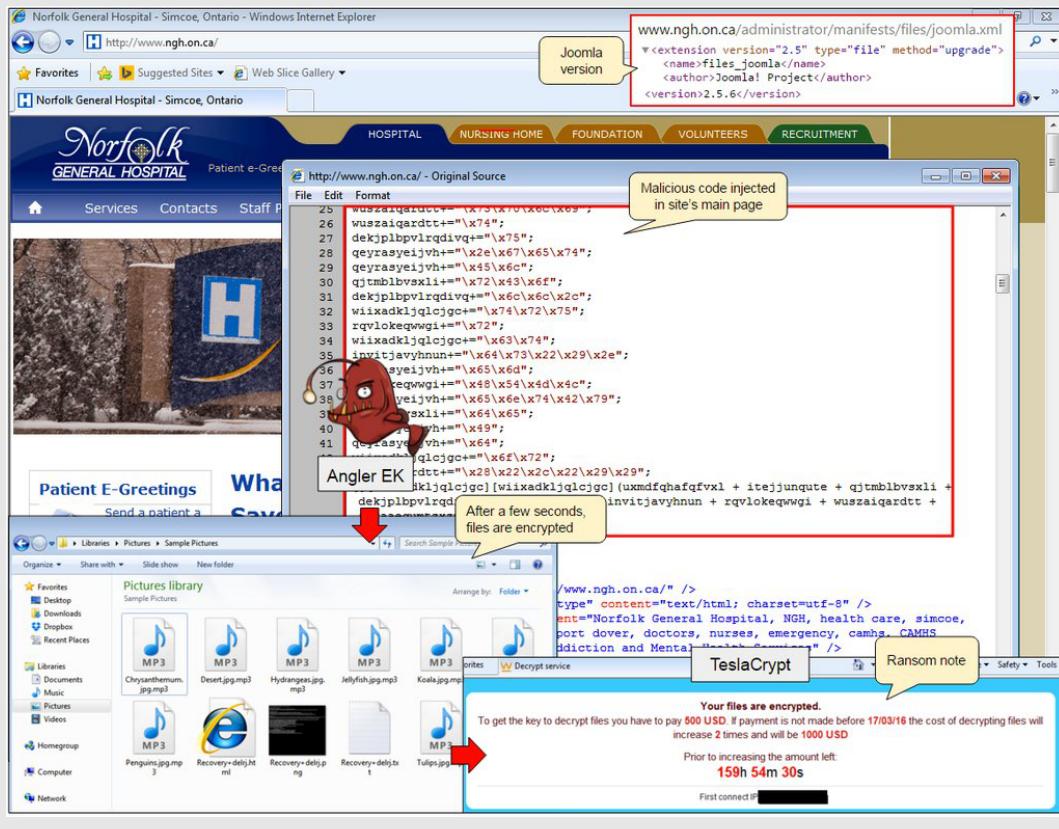
If all of this addresses are not available, follow these steps:

1. Download and install Tor Browser: <https://www.torproject.org/download/download-easy.html>
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: 3ezlvkoi7fwyood.onion/78634AFEA4011440
4. Follow the instructions on the site.

!!! Your personal identification ID: 78634AFEA4011440 !!!□34

Actualités 2016

Vague de ransomwares - janvier/décembre 2016 - Teslacrypt



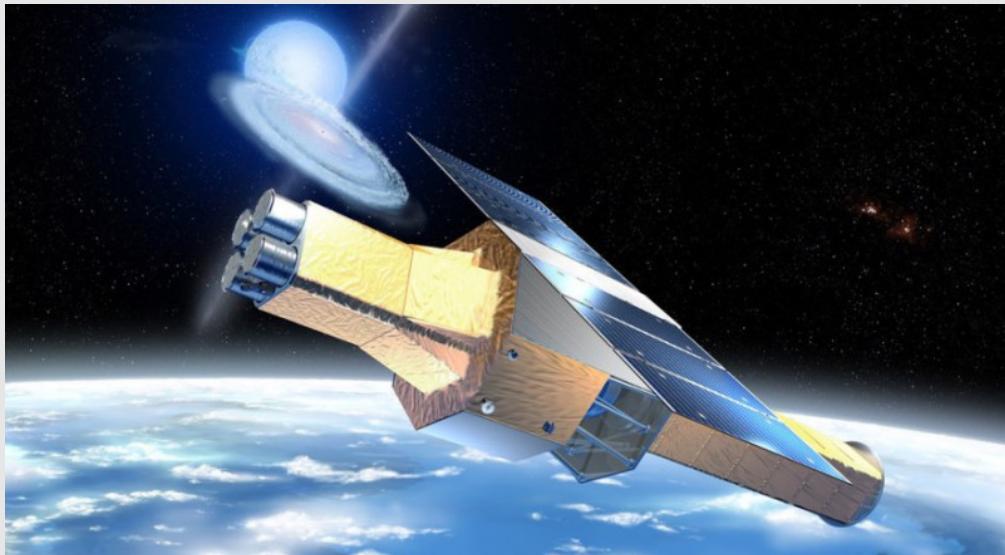
SSI

Michel Dubois - 2017

63/404

Actualités 2016

Le satellite Hitomi détruit à cause d'une mise à jour - mai 2016



The Japanese X-ray telescope **Hitomi** has been declared lost after it disintegrated in orbit, torn apart when spinning out of control. The cause is still under investigation but early analysis points to **bad data in a software package** pushed shortly after an instrument probe was extended from the rear of the satellite. JAXA, the Japanese space agency, lost **\$286 million**, three years of planned observations, and a possible additional 10 years of science research.

<http://hackaday.com/2016/05/02/software-update-destroys-286-million-japanese-satellite/>

SSI

Michel Dubois - 2017

64/404

Actualités 2016

La clé USB, contenant le dossier d'enquête sur les attentats de Charlie Hebdo, se perd dans le courrier - août 2016

Le Parisien VAL-D'OISE | La clé USB aux infos sensibles retrouvée... à Gonesse

0 RÉACTIONS 2.3K PARTAGE



Gonesse. La clé USB contenait l'intégralité de l'enquête sur les attentats de janvier 2015 à Paris. (LP/B.A.)

Dès policiers ont investi il y a quelques jours le centre de tri de Gonesse. Au bout de 8 heures de recherche, ils ont finalement trouvé ce qu'ils cherchaient : une clé USB qui contenait tout le dossier d'enquête des attentats de janvier 2015. Celle-ci avait été envoyée par des avocats de Bobigny (Seine-Saint-Denis) défendant des victimes à des confrères de Reims. La clé USB placée dans une enveloppe normale avait été déchirée en passant dans une machine du centre de tri. Le pli était donc arrivé vide. Étant donné le caractère extrêmement sensible des informations que contenait la clé USB, la police judiciaire de Reims a diligenté une enquête qui s'est finalement achevée à Gonesse.

leparisien.fr

Val-d'Oise
Gonesse Reims
USB Attentats

"La clé USB contenant l'intégralité de l'enquête sur les attentats de **Charlie Hebdo** et de l'**Hyper Cacher** envoyée par des avocats de Bobigny à leurs confrères de Reims est perdue pendant le transport. Les avocats de Bobigny, chargés défendre des victimes, s'étaient contentés d'envoyer ce document ultra-sensible dans **une enveloppe banale**, timbrée au tarif minimum. Une quantité vertigineuse de procès-verbaux de garde à vue, de notes des services des renseignements ou d'identités de témoins se baladent alors dans la nature, à la portée de tous."

<http://www.leparisien.fr/val-d-oise-95/la-cle-usb-aux-infos-sensibles-retrouvee-a-gonesse-28-08-2016-6075287.php>

SSI

Michel Dubois - 2017

65/404

Actualités 2016

DDoS massif à partir d'un botnet d'IoT opéré par Mirai - 21 octobre 2016



"Une cyberattaque majeure a perturbé les internautes du monde entier. En effet, une attaque par déni de service (DDoS) a paralysé le service DNS Dyn, utilisé notamment par Netflix, Twitter, Spotify, Reddit, Amazon ou encore le Playstation Network, bloquant l'accès à ces services."

<https://www.industrie-techno.com/attaque-contre-dyn-comment-les-objets-connectes-ont-servi-a-paralyser-le-web.46179>

SSI

Michel Dubois - 2017

66/404

Actualités 2016

Un faux communiqué de presse provoque une chute de 18% du cours de bourse du groupe Vinci - novembre 2016



"L'histoire commence avec un faux communiqué de presse publié à 16h05 et envoyé à différentes rédactions. Le texte explique que Vinci a découvert d'énormes irrégularités comptables, pour 3,5 milliards d'euros, et que le groupe de BTP révise ses comptes 2015 et 2016 à la baisse. Au passage, le communiqué indique que le directeur financier, Christian Labeyrie, a été licencié par la compagnie."

<http://bfmbusiness.bfmtv.com/bourse/affaire-vinci-que-s-est-il-passe-mardi-1062541.html>

SSI

Michel Dubois - 2017

67/404

Actualités 2016

Un faux communiqué de presse provoque une chute de 18% du cours de bourse du groupe Vinci - novembre 2016

mar. 22/11/2016 16:04
contact.abonnement@vinci.group
VINCI lance une révision de ses comptes consolidés pour l'année 2015 et le 1er semestre 2016
À [REDACTED]
Nous avons supprimé les sauts de ligne en surnombre dans ce message.

Nouveau communiqué de presse VINCI
Rueil Malmaison, 22 Novembre 2016
VINCI lance une révision de ses comptes consolidés pour l'année 2015 et le 1er semestre 2016
VINCI a annoncé aujourd'hui son intention de réviser ses comptes consolidés pour l'exercice 2015 ainsi que pour le premier semestre 2016. Les résultats d'un audit interne mené par le groupe Vinci ont en effet révélé que certains transferts irréguliers avaient été effectués des dépenses d'exploitation vers le bilan, en dehors de tous principes comptables reconnus. Le montant de ces transferts s'élèverait à 2.490 millions d'euros pour l'exercice comptable 2015 et 1.065 millions d'euros pour le premier semestre 2016. Selon l'audit interne les résultats opérationnels réels seraient de 1.225 millions pour 2015 et de 641 millions pour le premier semestre 2016. Le groupe reportera donc une perte nette pour 2015 ainsi que pour le premier semestre 2016.
Vinci a rapidement informé ses auditeurs externes (KPMG Audit et Deloitte & Associés) de la découverte de ces transferts. Le 21 Novembre, KPMG a informé Vinci qu'au vu de ces irrégularités, son audit des comptes consolidés de l'année 2015 et du premier semestre 2016 ne saurait être validé.
Vinci publiera des comptes non audités pour l'exercice 2015 ainsi que pour le premier semestre 2016 dès que possible. Une fois que le nouvel audit sera achevé, Vinci publiera de nouveaux comptes audités pour les deux périodes. Le groupe a par ailleurs lancé une révision complète des règles internes au sein de sa direction financière.
La compagnie a licencié Christian Labeyrie, directeur général adjoint et directeur financier de Vinci.
Vinci a informé l'Autorité des Marchés Financiers (AMF) de ces événements.
La révision des résultats opérationnels pour 2015 et 2016 devrait rester sans conséquence sur la trésorerie du groupe et n'affectera ni les clients ni les prestations du groupe Vinci.
« Notre équipe de direction est très choquée par ces découvertes », a dit Xavier Hulliard, Président-Directeur Général de Vinci. « Nous nous engageons à ce que Vinci respecte les plus hauts standards éthiques dans la conduite des affaires du groupe ».
« Nos clients ainsi que nos employés doivent garder confiance en la viabilité du groupe Vinci et en son engagement sur le long terme. Nos services ne sont en aucun cas affectés par ces événements et notre engagement à satisfaire les besoins de nos clients reste une priorité. Les rumeurs qui circulent sur une procédure d'insolvabilité sont totalement fausses » a ajouté le Président Directeur Général de Vinci.
« Nous nous engageons à mettre en place les changements nécessaires au sein du Groupe ».
Le groupe Vinci tiendra une conférence de presse demain.
Contact médias
Paul-Alexis Bouquet
Tél. : +33 (0)7 51 93 47 48
<http://www.vinci.group/vinci.nsf/fr/communiques/pages/20161122-1557.htm>

SSI

Michel Dubois - 2017

68/404

Actualités 2016

Un étudiant de l'ESTACA de Laval a grillé 88 ordinateurs de son école d'ingénieur - **novembre 2016**

The screenshot shows a news article from France Bleu Mayenne. The top navigation bar includes links for 'INFO', 'SPORTS', 'ÉMISSIONS', and 'MUSIQUE'. A banner at the top right says 'LE AC'. Below the navigation, there's a link to 'Afficher la page d'accueil de France Bleu Mayenne'. The main headline reads 'Laval : un "jeu" qui coûte très cher à l'ESTACA'. The article is by Stéphanie Denevaute, dated Mardi 22 novembre 2016 à 22:12. A photograph of a silver laptop is shown.

<https://www.francebleu.fr/infos/faits-divers-justice/laval-un-jeu-qui-coute-tres-cher-l-estaca-1479848930>

SSI Michel Dubois - 2017 69/404

Actualités 2016

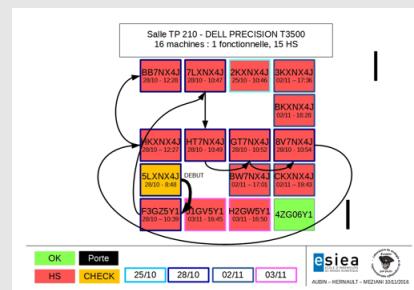
Un étudiant de l'ESTACA de Laval a grillé 88 ordinateurs de son école d'ingénieur - **novembre 2016**



Actualités 2016

Un étudiant de l'ESTACA de Laval a grillé 88 ordinateurs de son école d'ingénieur - **novembre 2016**

- travail d'investigation réalisé par le laboratoire ($C + V$)⁰ de l'ESIEA suite à une demande d'aide de l'ESTACA
- l'ESTACA constatait des pannes informatiques se traduisant par l'impossibilité de démarrer plusieurs PC
- en investiguant sur la carte mère, constat que le microcontrôleur USB intégré présente un court circuit sur les ports de données qu'il contrôle
- le même diagnostic est fait sur tous les autres PC
- en dessoudant le microcontrôleur USB incriminé, le PC redémarre
- les disques durs étant épargnés, analyse des sauvegardes de mémoires vives (hyperfil.sys)
- à partir des dernières dates enregistrées dans le système, reconstitution des schémas horaires d'extinction des ordinateurs
- à l'aide de ces schémas les autorités ont pu les corrélérer avec les emplois du temps des étudiants
- cette analyse a permis de disculper 630 étudiants sur les 650 présents
- l'enquête de police a ensuite permis l'arrestation d'un étudiant, qui a avoué les faits
- ce dernier a fourni aux enquêteurs une clef USB appelée "USB Killer"
- cette clef décharge une tension de plus de 200V sur les fils "data" du port USB.



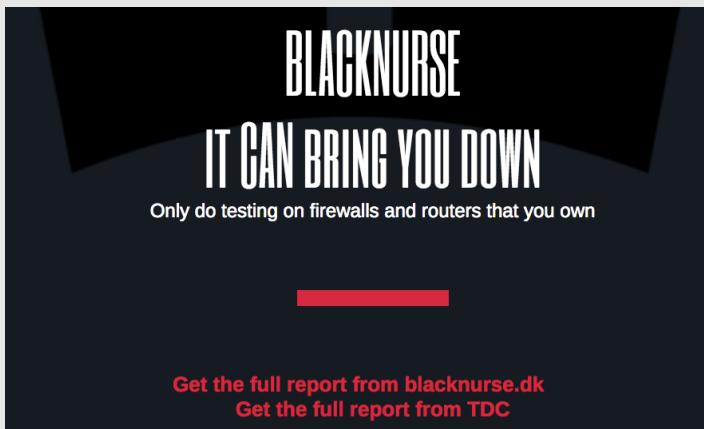
SSI

Michel Dubois - 2017

71/404

Actualités 2016

L'attaque Blacknurse - **novembre 2016**



- `hping3 -1 -C 3 -K 3 -i u20 <target ip>`

- Cible les firewalls
- Envoi de paquet ICMP Type 3 Code 3
- Entre 40 et 50 pkt/sec
- Entraîne une surcharge de CPU
- Vulnérabilité vieille de 20 ans
- <http://blacknurse.dk/>

SSI

Michel Dubois - 2017

72/404

Guide de la FDA pour la sécurisation des équipements médicaux - **décembre 2016**

Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document issued on December 28, 2016.

The draft of this document was issued on January 22, 2016.

For questions regarding this document, contact Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5434, Silver Spring, MD 20993-0002, 301-796-6937. For questions regarding this document as applied to devices regulated by CBER, contact the Office of Communication, Outreach and Development in CBER at 1-800-835-4709 or 240-402-8010 or ocod@fda.hhs.gov.

- Intégrer la sécurité dès la **conception**
- Réaliser une **analyse des risques**
- Une sécurité **proactive** augmente la sécurité des soins
- Pas besoin de **recertification** après la correction d'une vulnérabilité
- Gestion des risques est une responsabilité partagée : fabricant, soignant, IT et IBM
- Traiter en priorité le **risque cyber**

Pourquoi la SSI?
Section 8
Actualités 2017



Actualités 2017

Attaque des cyber Squirrel - 16 janvier 2017

BBC Sign in News Sport Weather Shop Earth Travel M

NEWS

Home | Video | World | UK | Business | Tech | Science | Magazine | Entertainment & Arts

Technology

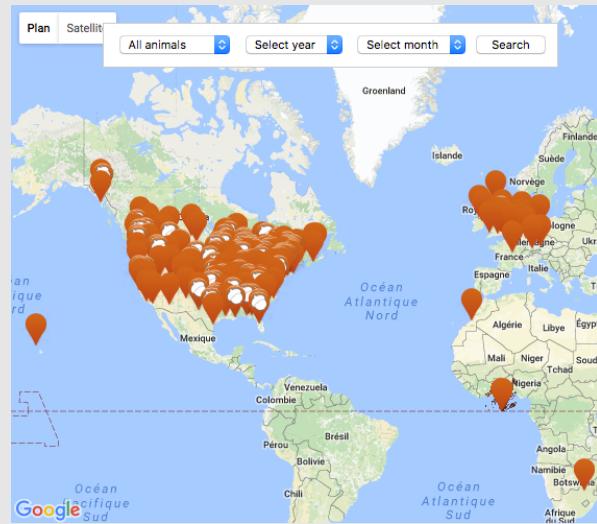
Squirrel 'threat' to critical infrastructure

17 January 2017 | Technology

f Share



Squirrels are the top offenders with 879 "attacks"



<http://www.bbc.com/news/technology-38650436>

SSI

Michel Dubois - 2017

75/404

Actualités 2017

Attaque des cyber Squirrel - 16 janvier 2017

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS SIGN IN

NUTS TO YOU — Who's winning the cyber war? The squirrels, of course

CyberSquirrel1 project shows fuzzy-tailed intruders cause more damage than "cyber" does.

SEAN GALLAGHER - 1/16/2017, 10:25 PM



Les animaux les plus dangereux que les pirates

- écureuil : 913
- oiseau : 452
- serpent : 83
- raton laveur : 72
- rat : 37
- martre : 23
- castor : 15
- méduse : 13

<http://cybersquirrel1.com>

SSI

Michel Dubois - 2017

76/404

Actualités 2017

Un hotel bloqué par un ransomware - 31 janvier 2017

NEXTD'IMPACT CATEGORIES BLOG BONS PLANS

À NE PAS MANQUER MWC 2017 Election Présidentielle SpaceX Windows 10 Creators Update Samsung Galaxy S8 World

Victime d'un ransomware, un hôtel veut revenir aux clés classiques pour ses chambres

Plus de peur que de mal... cette fois-ci 119



Credit: Laptrinh/Stock

Quand une société est victime d'un ransomware, cela peut avoir d'importantes conséquences. En Autriche, une cyberattaque a ainsi paralysé les ordinateurs d'un hôtel, qui a décidé de payer la rançon demandée. Un coup de chance pour celle qui cela n'arrive pas forcément à tous avec ce type de virus.

Depuis quelques jours, l'information fait le tour du Web : l'hôtel Romantik Seehotel Jägerwirt se serait fait pirater et des clients se seraient retrouvés piégés à ne plus pouvoir entrer ou sortir de leur chambre. C'est du moins ce qu'affirme le site [The Local dans un premier temps](#), avant de se retracer. Finalement, la situation est moins catastrophique, mais une nouvelle fois la question de la cybersécurité.

Victime d'un ransomware, le système informatique d'un hôtel paralysé

Dans des interviews accordées à plusieurs de nos confrères, dont ceux de Motherboard, le propriétaire de l'hôtel Christoph Brandstaetter explique que « c'était juste une cyberattaque normale et aucun invité n'a été enfermé dans sa chambre ». Il précise que les pirates ont visé le système informatique de l'hôtel et ont réussi à installer un ransomware sur les machines, les rendant inutilisables par les employés.

L'hôtel ne pouvait alors plus éditer de nouvelles cartes pour accéder aux chambres, mais celles déjà émises fonctionnaient normalement affirme le responsable. Il indique en effet que les serrures électroniques fonctionnent sur un réseau interne qui n'était pas relié aux ordinateurs infectés.

Le propriétaire décide de payer la rançon... et repassera à des clés traditionnelles

Christoph Brandstaetter ajoute qu'au bout de 24 heures avec son système informatique bloqué, il a décidé de payer la rançon (environ 1 500 euros) ce qui lui a permis d'accéder à ses ordinateurs. Il précise qu'il a également contacté la police locale, qui lui aurait précisé que plusieurs autres sociétés ont été attaquées de la même manière ces derniers temps. Par mesure de sécurité, il a remplacé l'ensemble des ordinateurs infectés afin d'éviter qu'une éventuelle porte dérobée ne soit utilisée par la suite.

Bref, une attaque qui n'a rien d'exceptionnel dans son principe, mais qui peut avoir de fâcheuses conséquences pour les sociétés touchées. Concernant les demandes de rançon, deux écoles s'opposent. D'un côté le FBI qui conseille « souvent aux gens de payer simplement » et de l'autre l'ANSI qui recommande de ne pas payer. L'Agence nationale de la sécurité des systèmes d'information déclare : « le paiement ne garantit pas le déclenchement de la demande ».

Le propriétaire de l'hôtel, Christoph Brandstaetter, nous explique qu'il a également parlé à ses clients et il leur a assuré qu'ils reviennent dans l'hôtel de la prochaine rénovation, après avoir changé le système de clés pour revenir aux traditionnelles. Il ajoute que c'est récent publiquement sur cette histoire, c'est notamment pour prévenir les autres sociétés des risques. Mais il s'agit aussi de préciser qu'aucun client n'était enfermé dans sa chambre, ce qui aurait évidemment eu des conséquences plus graves, notamment si cela avait durer 24 heures.

SSII Michel Dubois - 2017 77/404



- **Romantik Seehotel Jägerwirt** est un hotel **** autrichien
- décide de rendre publique les faits à la **4ème attaque**

Actualités 2017

Un hotel bloqué par un ransomware - 31 janvier 2017

THE LOCAL at

News Jobs (2,506) Community Lifestyle Everything

viennaticketoffice.com

Hotel ransomed by hackers as guests locked out of rooms



Photo: CEN

The Local news.austria@thelocal.at

28 January 2017 | 10:42 CET+01:00

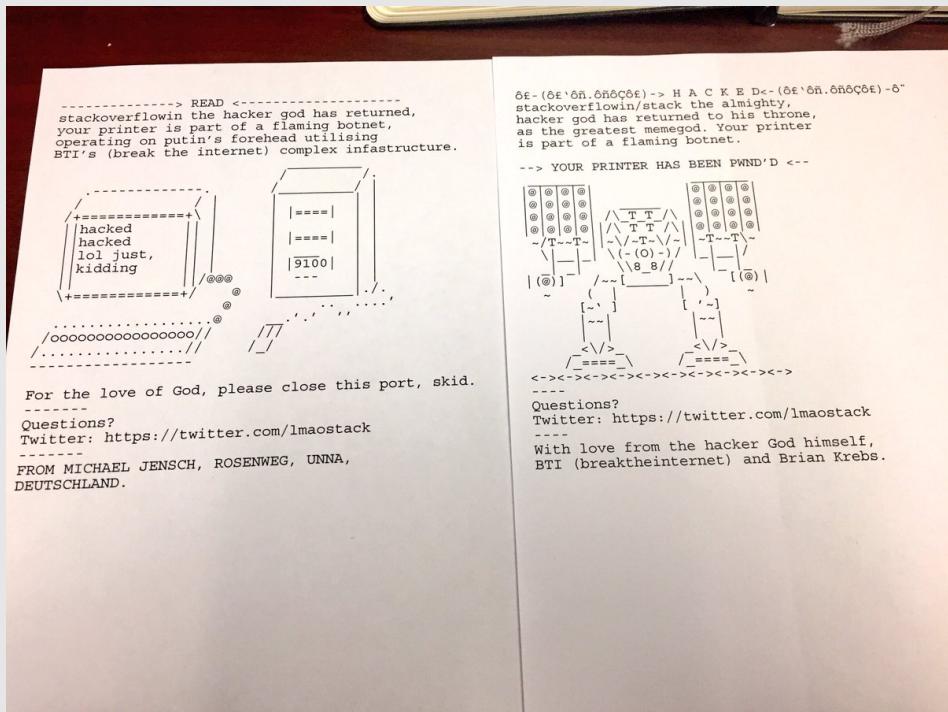
<https://www.thelocal.at/20170128/hotel-ransomed-by-hackers-as-guests-locked-in-rooms>
<https://www.thelocal.at/20170131/bitcoin-hotel-hack-victim-speaks-out>

- le système de gestion des clefs est atteint - **impossible de rentrer dans les chambres**
- le système de **réservation** et de **paiement** est également atteint
- au bout de **24 heures** de blocage l'hôtel décide de payer la rançon
- *"The house was totally booked with 180 guests, we had no other choice. Neither police nor insurance help you in this case."*
- le pirate promet de restaurer le système contre **1500EUR**
- l'hôtel prévoit de revenir à un système de **serrure classique**

SSI Michel Dubois - 2017 78/404

Actualités 2017

Un pirate prends la main sur 150 000 imprimantes - 4 février 2017



<http://www.networkworld.com/article/3165419/security/hacker-stackoverflowin-pwning-printers-forcing-rogue-botnet-warning-print-jobs.html>

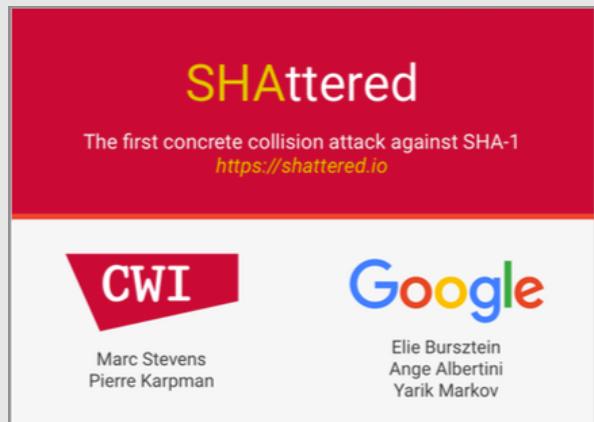
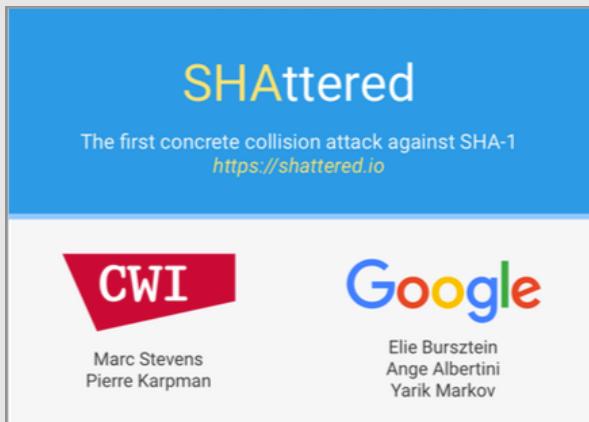
SSI

Michel Dubois - 2017

79/404

Actualités 2017

Première collision SHA1 - 23 février 2017



<https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html>

SSI

Michel Dubois - 2017

80/404

Actualités 2017

Un petit ours en peluche connecté! - 28 février 2017

MOTHERBOARD



THE INTERNET OF HACKABLE THINGS

Internet of Things Teddy Bear Leaked 2 Million Parent and Kids Message Recordings

LORENZO FRANCESCHI-BICCHIERAI
Feb 27 2017, 10:00pm

A company that sells "smart" teddy bears leaked 800,000 user account credentials—and then hackers locked it and held it for ransom.

MOTHERBOARD

THE INTERNET OF HACKABLE THINGS

How This Internet of Things Stuffed Animal Can Be Remotely Turned Into a Spy Device

LORENZO FRANCESCHI-BICCHIERAI
Feb 28 2017, 6:19pm



More bad news for toymaker Spiral Toys, which left customer data from its "CloudPets" brand exposed online.

An internet-connected teddy bear that allows parents and kids to exchange heartfelt audio messages sounds like a great idea—until the parents' emails and passwords, as well as the message recordings themselves, are left exposed online to hackers.

https://motherboard.vice.com/en_us/article/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings

SSI

Michel Dubois - 2017

81/404

Actualités 2017

Un petit ours en peluche connecté! - 28 février 2017



Plus difficile à revendre ...

SSI

Michel Dubois - 2017

82/404

Actualités 2017

Cybersécurité des hopitaux - 15 mars 2017



The screenshot shows a news article from Le Telegramme's website. The header reads "Cyber-sécurité. Des hôpitaux passoires en Bretagne". Below the header is a photograph of a medical professional at a desk with a laptop. A caption at the bottom of the image states: "Systèmes d'exploitation pas à jour, absence de responsable et de politique en matière de sécurité du système d'information, procédures d'élimination de données sensibles non formalisées... La sécurité informatique des hôpitaux semble loin d'être assurée."

- Rapport de la chambre régionale des comptes de Bretagne
- Enquête sur neuf centres hospitaliers bretons
- Systèmes d'exploitation non mis à jour
- Absence de RSSI
- Pas de sécurisation de l'accès aux salles serveurs
- Pas de suppression des comptes au départ d'un agent

<http://www.letelegramme.fr/bretagne/cyber-securite-des-hopitaux-passoires-15-03-2017-11434523.php>

SSI

Michel Dubois - 2017

83/404

Actualités 2017

Un Sex-Toy qui diffuse ses informations d'utilisation - 16 mars 2017

LE SEX-TOY CONNECTÉ QUI ESPIONNAIT SES CLIENTS, LA SOCIÉTÉ CONDAMNÉE À DÉDOMMAGER 10 000 DOLLARS PAR PERSONNE !



L'application **We-Connect** transmettait des informations telles que :

- les jours et heures d'utilisation
- le mode de vibration utilisé
- les adresses emails personnelles des utilisateurs

sans que ceux-ci en soient avertis.

<http://fr.ubergizmo.com/2017/03/16/sex-toy-connecte-defaillance-securite.html>

SSI

Michel Dubois - 2017

84/404

Actualités 2017

Des données de santé accessibles au travers
de serveurs FTP non protégés - 22 mars 2017

 **Private Industry Notification**
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

22 March 2017

PIN Number
170322-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cwwatch@ic.fbi.gov

Phone:
1-855-292-3937

Cyber Criminals Targeting FTP Servers to Compromise Protected Health Information

Summary

The FBI is aware of criminal actors who are actively targeting File Transfer Protocol (FTP)^a servers operating in “anonymous” mode and associated with medical and dental facilities to access protected health information (PHI) and personally identifiable information (PII) in order to intimidate, harass, and blackmail business owners.

Threat

Research conducted by the University of Michigan in 2015 titled, “FTP: The Forgotten Cloud,” indicated over 1 million FTP servers were configured to allow anonymous access, potentially exposing sensitive data stored on the servers. The anonymous extension of FTP allows a

<https://threatpost.com/anonymous-ftp-servers-leaving-healthcare-data-exposed/124624/>

SSI Michel Dubois - 2017 85/404

Actualités 2017

Jouer à Mario Kart avec sa voiture - 22 mars 2017



<https://blog.hackster.io/hacking-a-chevy-volt-into-a-mario-kart-64-controller-f007bd643138#.g0dcurriiv>

Actualités 2017

Apple piraté - 24 mars 2017

silicon Recherche... Suivez-nous NEWSLETTER

Menu Cloud Sécurité Mobilité DS IoT Livres Blancs Événements Emploi Hub : PME : mesures-vous aux plus grands

Apple n'a pas été piraté, mais 250 millions de ses utilisateurs sont bien menacés

Reynald Fléchoux, 24 mars 2017, 9:00

AUTHENTICATION | CLOUD | SÉCURITÉ

THÉMATIQUES ASSOCIÉES

Apple
hackers
iCloud

f 23 t 18 g+ 4 ln 94 Donnez votre avis

Les données sur les utilisateurs Apple qu'affirme détenir la Turkish Crime Family ne proviennent pas d'une faille de sécurité de Cupertino. Mais d'une consolidation de données dérobées lors de différents piratages. 250 millions de comptes n'en sont pas moins menacés de réinitialisation.

PASTEBIN + new paste trends Guest User

text 2.99 KB

1. Hello Humans,
2.
3. Apple has now announced that they were not breached which no one claimed they were other than some journalists who misunderstood the situation, they announced this for their user's comfort & to make them feel better about their selves as they're very insecure with their company.
4.
5. They have basically announced what we have told them which is that there was no breach, this has nothing to do with a breach.
6.
7. The whole "thing" not being a breach doesn't change any claims that were made by us, the entire DB was acquired and built from multiple DB's that we have been selling in the past 5 years as we decided to keep all our @icloud.com, @me.com & mac.com domains due to those domains not having a popular demand in the cracking community.
8.
9. More and more people started getting involved after all the press release world wide, these people have been providing us even more databases which we did not already have, this is bumping up the total number of active iCloud accounts we have to reset.
10.
11. We are still strengthening our infrastructure and acquiring more servers for the attack
12.
13. - We're still in contact with Apple.
14.
15. The total number of unhashed DB lines we currently hold with only Apple owned extensions are over 750 million, out of the 750 million we have 250 million that are checked and working live, there is still a big amount that we're still scanning.
...

<http://www.silicon.fr/apple-pas-pirate-250-millions-utilisateurs-menaces-170602.html>
<https://pastebin.com/kKm4Vwzx>

SSI

Michel Dubois - 2017

87/404

Actualités 2017

Autoclave piratable - 27 mars 2017



- Miele Professional PG 8528 PST10
- CVE-2017-7240
- Serveur Web embarqué
- Directory traversal attack
- Disclosure timeline

2016-11-16 Vulnerability discovered
2016-11-21 Contact with Miele product representative
2016-12-03 Send details to the Miele product representative
2017-01-19 Asked for update, no response
2017-02-03 Asked for update, no response
2017-03-23 Public disclosure

- GET /../../../../../../../../../../../../etc/shadow HTTP/1.1

<http://thehackernews.com/2017/03/iot-washer-disinfecter.html>

SSI

Michel Dubois - 2017

88/404

Actualités 2017

Sex-toy connecté le retour - 04 avril 2017

MOTHERBOARD
INTERNET DES OBJETS

Ce vibro peut être facilement hacké pour livestreamer l'intérieur de votre vagin

LF LORENZO FRANCESCHI-BICCHIERAI Apr 4 2017, 8:00am



Quelle idée d'acheter un gode connecté à Internet, aussi, franchement.

- Découvert par la société **Pen Test Partners**
- Wireless camera vibrator - **Svakom Siime Eye** - 249\$
- Possibilité de diffuser une vidéo en livestream
- Mot de passe par défaut du WiFi du god : **88888888**
- Nom du réseau WiFi : **Siime Eye**

Specifications

Data	
Material:	Silicone
Size:	Φ25x165mm
Weight:	74g
Charging time:	1.5 hours
Maximum continuous use:	2 hours
Vibration modes:	5+1
Intensities:	5



https://motherboard.vice.com/fr/article/ce-vibro-peut-etre-facilement-hacke-pour-diffuser-en-direct-linterieur-de-votre-vagin?utm_source=vicefrfb

SSI

Michel Dubois - 2017

89/404

Pourquoi la SSI?

Section 9

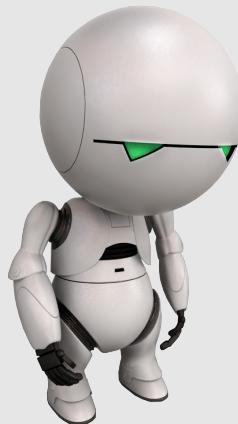
Les livres blancs de la défense



SSI

Michel Dubois - 2017

90/404



9. Les livres blancs de la défense

9.1. Les premiers rapports

Les livres blancs de la défense

Les premiers rapports

Rapport Lasbordes - 2006

La Sécurité des systèmes d'information - Un enjeu majeur pour la France



« La France accuse un retard préoccupant face aux impératifs de SSI, tant au niveau de l'État qu'au niveau des entreprises, quelques grands groupes mis à part. »

Rapport Romani - 2008

Cyberdéfense : un nouvel enjeu de sécurité nationale



« La France n'est ni bien préparée, ni bien organisée face à la menace d'attaques informatiques. »

Rapport Bockel - 2012

La cyberdéfense : un enjeu mondial, une priorité nationale

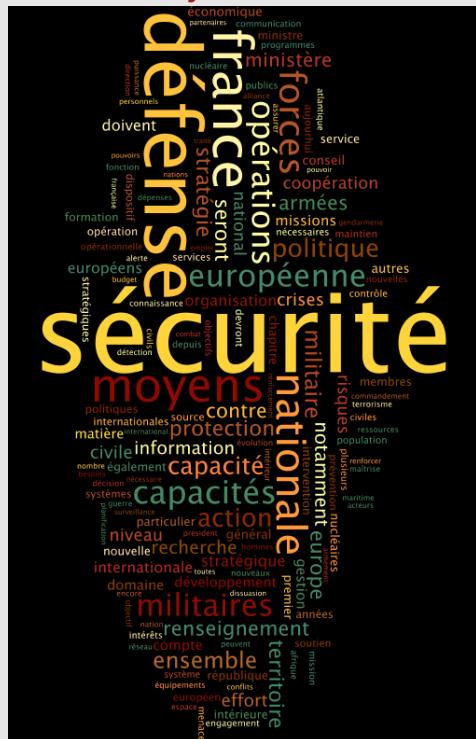


« Le renforcement de la protection et de la défense des systèmes d'information devrait faire l'objet d'une priorité nationale, portée au plus haut niveau de l'État, et d'une véritable stratégie de l'Union européenne. »

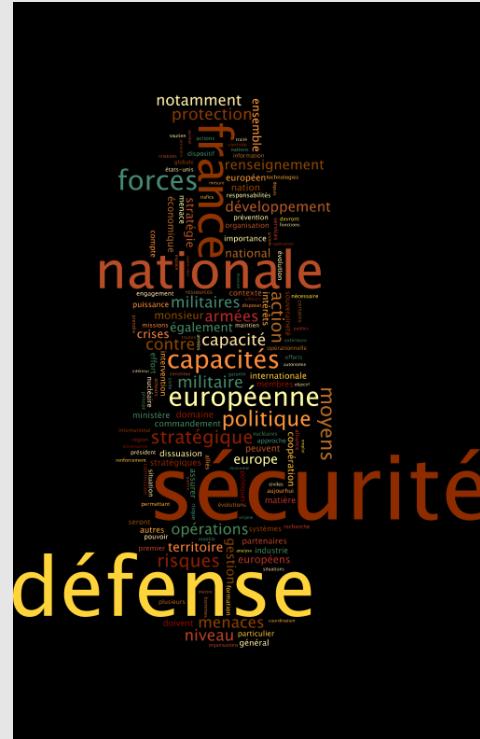
Les livres blancs de la défense

Les premiers rapports

17 juin 2008



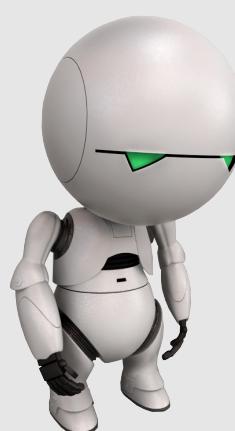
29 avril 2013



SSI

Michel Dubois - 2017

93/404



9. Les livres blancs de la défense

9.2. Le livre blanc de 2008

SSI

Michel Dubois - 2017

94/404

Les livres blancs de la défense

Le livre blanc de 2008

2008 - De nouvelles vulnérabilités pour le territoire et les citoyens européens

Le terrorisme

« La France et l'Europe sont directement visées par le djihadisme et ceux qui s'en réclament. »



Les livres blancs de la défense

Le livre blanc de 2008

2008 - De nouvelles vulnérabilités pour le territoire et les citoyens européens

La prolifération du nucléaire

« D'ici 2025, la France et plusieurs pays européens se trouveront à portée de nouvelles capacités balistiques. »



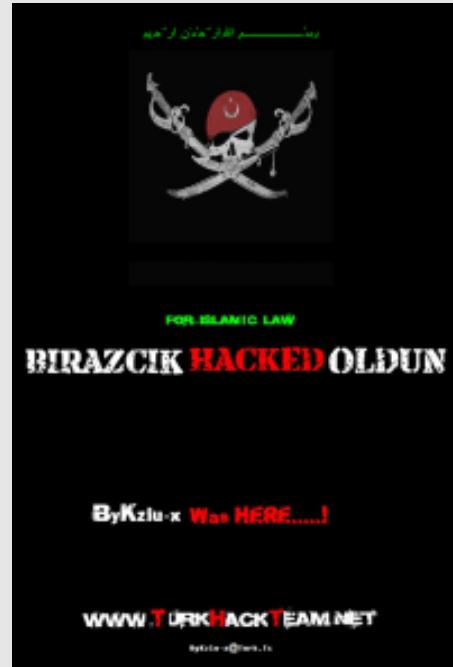
Les livres blancs de la défense

Le livre blanc de 2008

2008 - De nouvelles vulnérabilités pour le territoire et les citoyens européens

Les attaques majeures contre les systèmes d'information.

« Le niveau **quotidien** actuel des agressions contre les systèmes d'information, qu'elles soient d'origine étatique ou non, laisse présager **un potentiel très élevé de déstabilisation** de la vie courante, de **paralysie de réseaux critiques** pour la vie de la nation, ou de **déni de fonctionnement** de certaines capacités militaires. »



Les livres blancs de la défense

Le livre blanc de 2008

2008 - De nouvelles vulnérabilités pour le territoire et les citoyens européens

L'espionnage et les stratégies d'influence

« La poursuite des échanges mondialisés et le développement de nouveaux pôles de puissance sont propices à des **activités de renseignement offensif visant la France et l'Europe**, comme au développement de stratégies d'influences destinées à amoindrir notre rôle dans le monde et sur le marché international. »

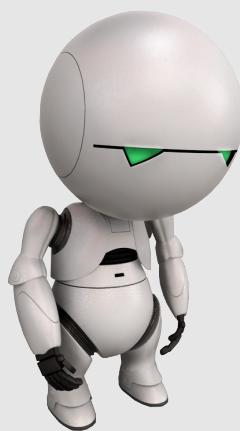
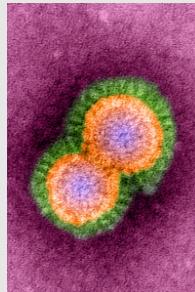


Les livres blancs de la défense

Le livre blanc de 2008

2008 - Hiérarchisation des menaces

1. Attentats terroristes
2. Attaques informatiques
3. Prolifération du nucléaire
4. Pandémie
5. Catastrophes naturelles ou industrielles
6. Criminalité organisée.



9. Les livres blancs de la défense 9.3. Le livre blanc de 2013

Les livres blancs de la défense

Le livre blanc de 2013

2013 - le cyberspace nouvel espace de bataille

« Les menaces et les risques induits par l'expansion généralisée du cyberespace ont été confirmés. »

« Le cyberespace est désormais un champ de confrontation à part entière. »

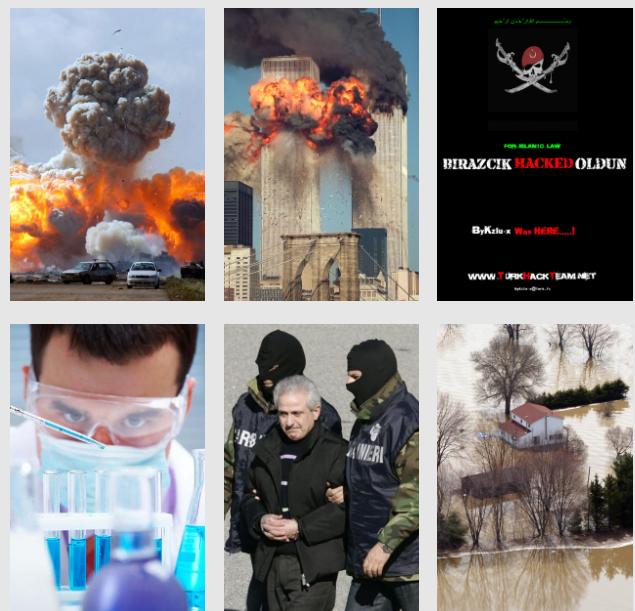


Les livres blancs de la défense

Le livre blanc de 2013

2013 - Hiérarchisation des menaces

- les agressions par un autre état contre le territoire national
- les attaques terroristes
- les cyberattaques**
- les atteintes au potentiel scientifique et technique
- la criminalité organisée dans ses formes les plus graves
- les crises majeures résultant de risques naturels, sanitaires, technologiques, industriels, ou accidentels
- les attaques contre nos ressortissants à l'étranger



Les livres blancs de la défense

Le livre blanc de 2013

2013 - le livre blanc prévoit une posture stratégique visant à :

- déterminer l'origine des attaques
- organiser la résilience de la Nation
- répondre, y compris par la LIO



**Discours du ministre de la Défense
Ouverture du colloque international de
cyberdéfense
24 septembre 2015**

La cyber n'est cependant plus seulement un enjeu défensif, et je voudrais aujourd'hui m'engager avec vous sur un terrain dont la sensibilité n'a d'égal que l'importance qu'il revêt : je parle ici, employons le terme, de lutte informatique offensive.

Pour nos forces armées, le premier enjeu est désormais d'intégrer le combat numérique, de le combiner avec les autres formes de combat. Ce nouveau milieu est devenu un domaine militaire à part entière, dans lequel il faut positionner ses forces, défendre sa puissance et y exploiter toutes les opportunités pour vaincre l'adversaire.

L'arme informatique doit apporter un appui maîtrisé aux forces conventionnelles. C'est une nouvelle forme de frappe dans la profondeur, aux effets qui peuvent être considérables. Chacun connaît ici le virus STUXNET qui a frappé le cœur d'un dispositif très fortifié, en l'occurrence une centrale nucléaire iranienne. C'est aussi une forme d'appui tactique aux combattants, par exemple pour perturber les défenses anti aériennes en leurrant ou en neutralisant des systèmes radars. Certains l'ont déjà fait.

Les livres blancs de la défense

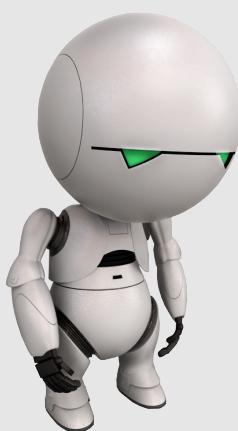
Le livre blanc de 2013

2013 - les moyens pour y parvenir :

- autonomie dans la production de systèmes de sécurité
- renforcement des RH consacrées à la cyberdéfense
- amélioration de la fiabilité des SI de l'État et des OIV
- MINDEF - création d'une chaîne de commandement unifiée
- création des réserves opérationnelle et citoyenne pour la cyberdéfense



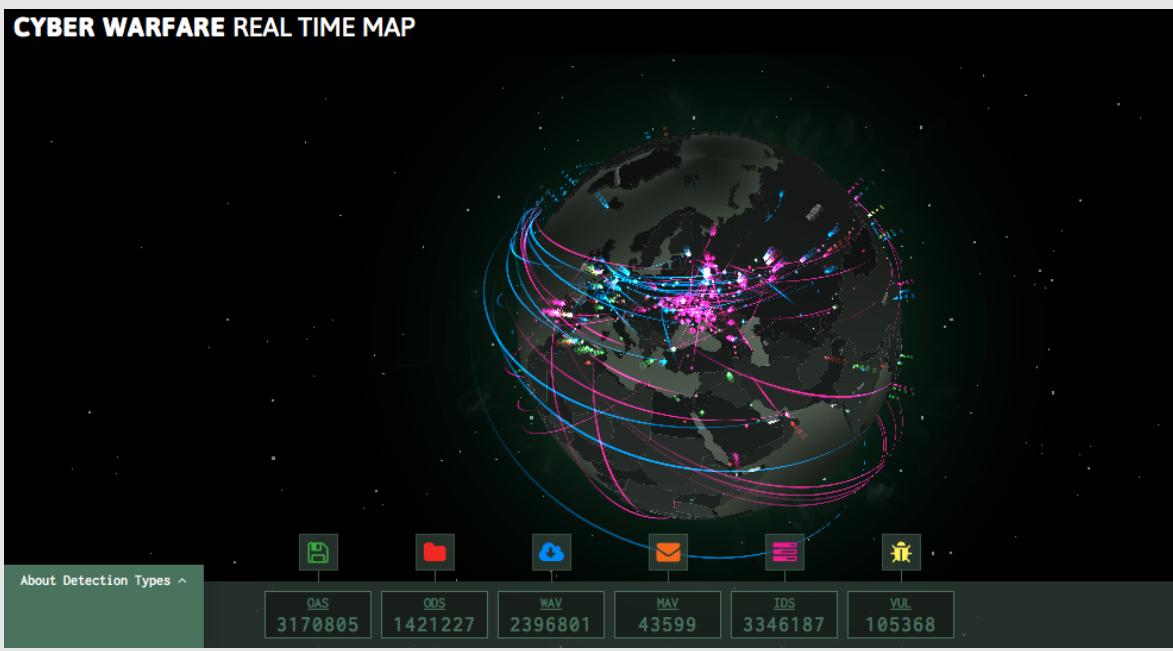
Pourquoi la SSI?
Section 10
La SSI parce que...



10. La SSI parce que...
10.1. La Cyberguerre

La SSI parce que...

La Cyberguerre



<http://cyberwar.kaspersky.com/>

SSI

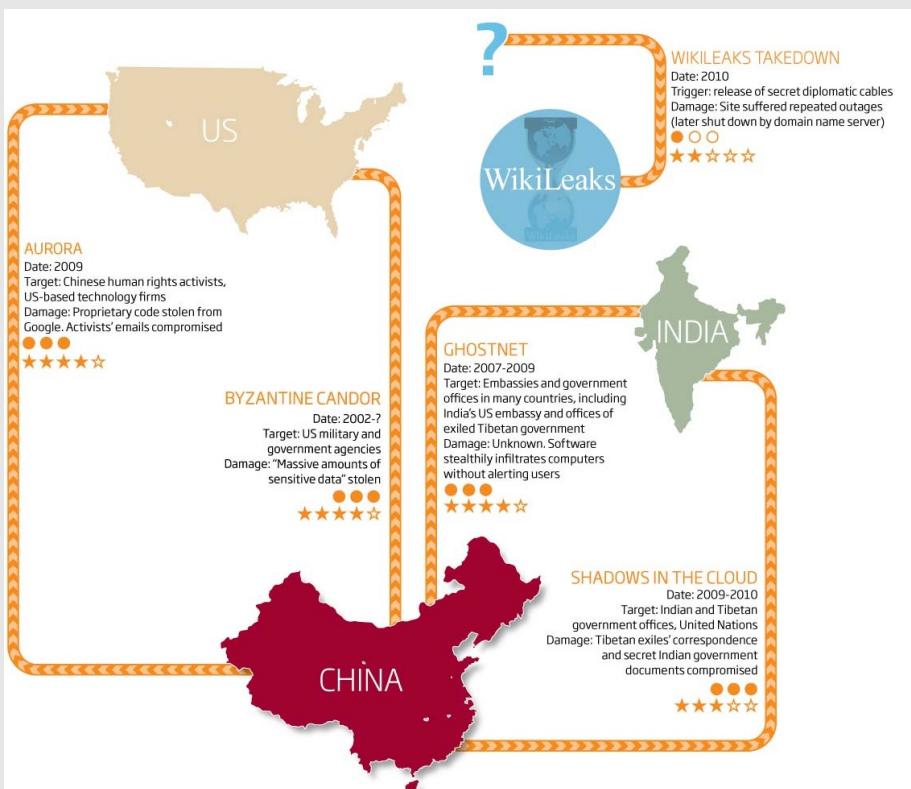
Michel Dubois - 2017

107/404

La SSI parce que...

La Cyberguerre

Petit résumé de cyberguerre (1/2)



SSI

Michel Dubois - 2017

108/404

La SSI parce que...

La Cyberguerre

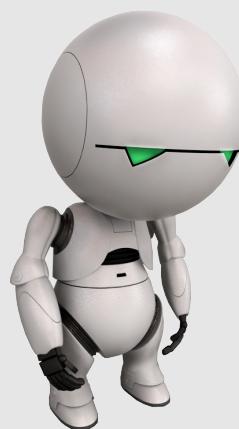
Petit résumé de cyberguerre (2/2)



SSI

Michel Dubois - 2017

109/404



10. La SSI parce que... 10.2. Prise en compte du risque insuffisante

SSI

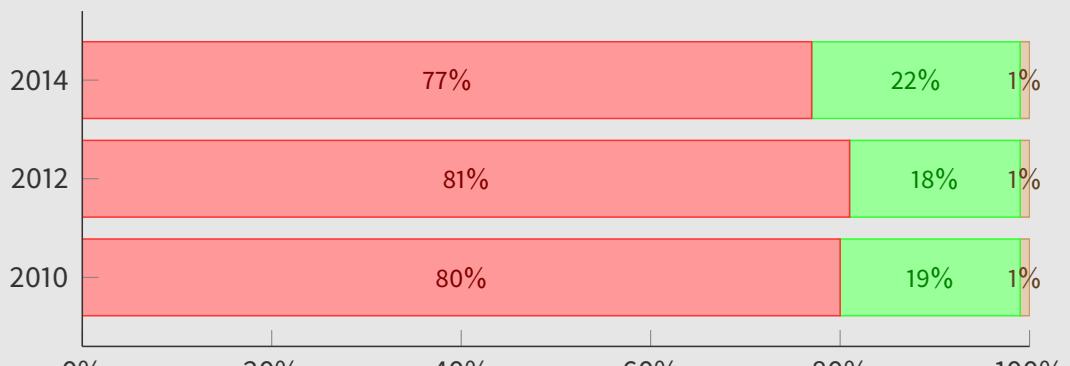
Michel Dubois - 2017

110/404

La SSI parce que...

Prise en compte du risque insuffisante

Dépendance des entreprises à l'informatique



■ Forte: une indisponibilité de moins de 24h a des conséquences graves

■ Modérée: une indisponibilité jusqu'à 48h est tolérable

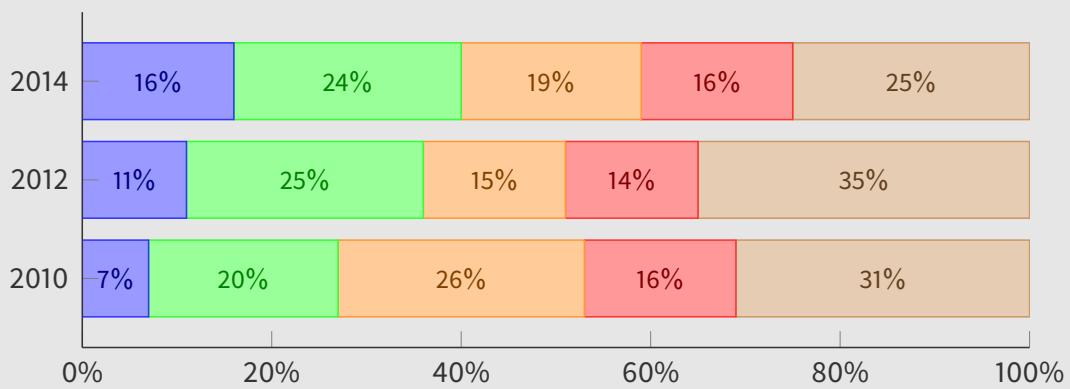
■ Faible: une indisponibilité même de longue durée n'a pas de conséquence grave

Source: <https://www.clusif.asso.fr/fr/production/sinistralite/>

La SSI parce que...

Prise en compte du risque insuffisante

Pourcentage du budget SSI par rapport au budget informatique



■ Moins de 1%

■ de 1 à 3%

■ de 3 à 6%

■ Plus de 6%

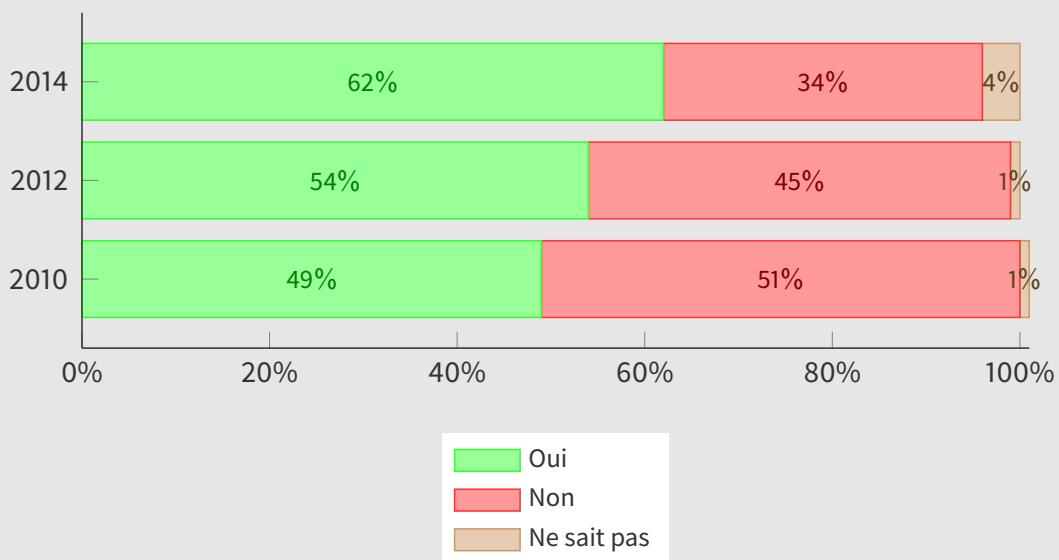
■ Ne sait pas

Source: <https://www.clusif.asso.fr/fr/production/sinistralite/>

La SSI parce que...

Prise en compte du risque insuffisante

Fonction de RSSI clairement identifiée et attribuée

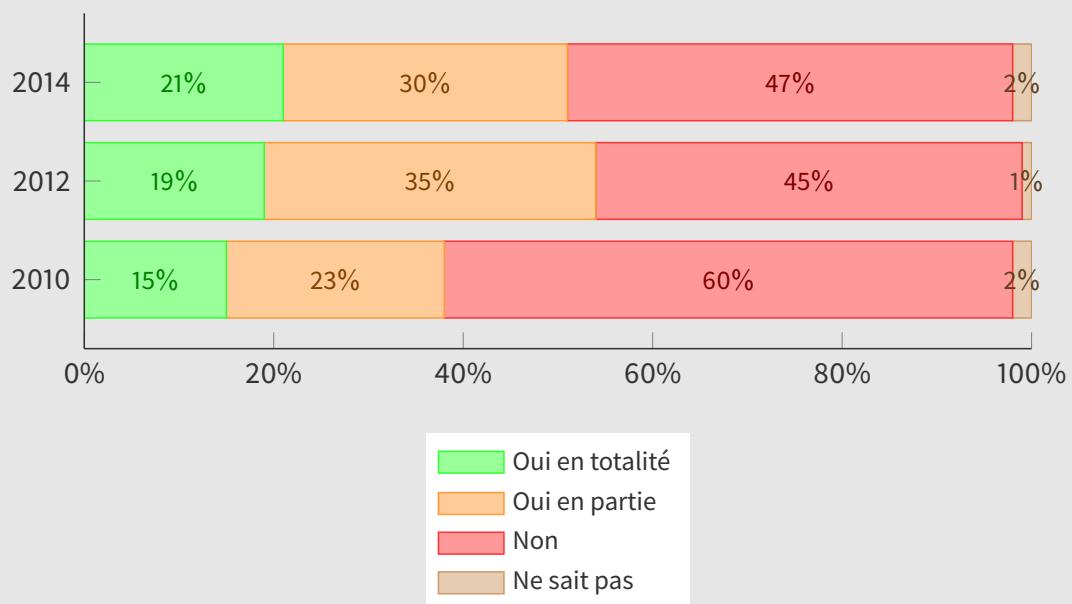


Source : <https://www.clusif.asso.fr/fr/production/sinistralite/>

La SSI parce que...

Prise en compte du risque insuffisante

Analyse des risques liés à la sécurité de l'information

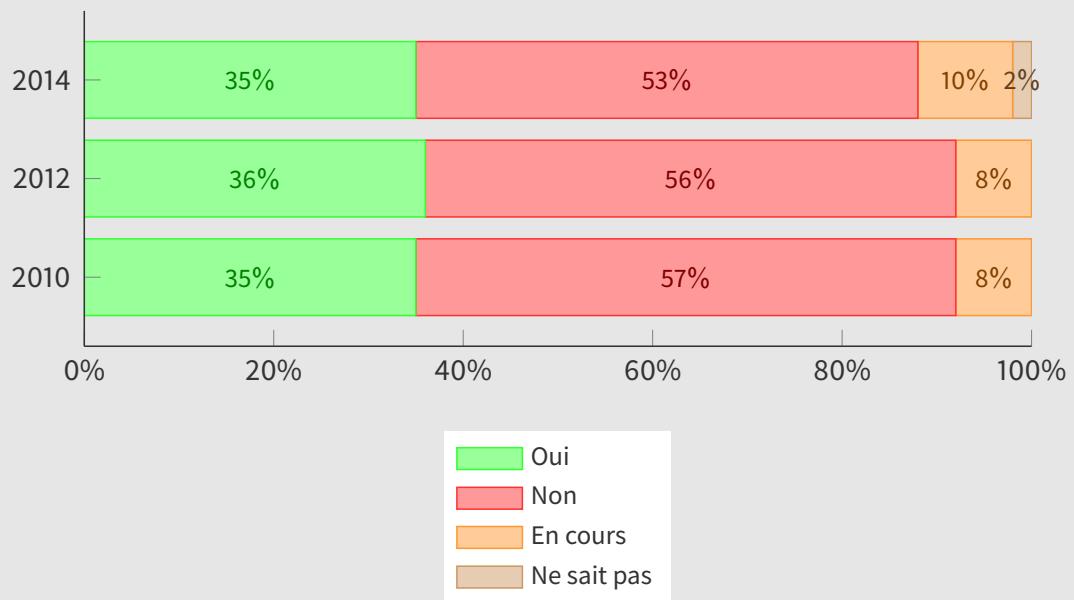


Source : <https://www.clusif.asso.fr/fr/production/sinistralite/>

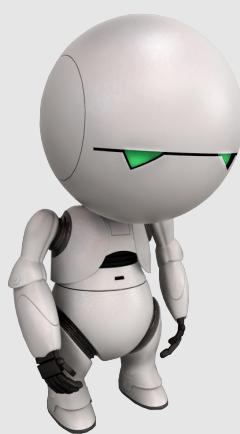
La SSI parce que...

Prise en compte du risque insuffisante

Existence d'un programme de sensibilisation à la SSI



Source : <https://www.clusif.asso.fr/fr/production/sinistralite/>



10. La SSI parce que...

10.3. Au final

La SSI parce que...

Au final

La Sécurité des Systèmes d'Information **parce que :**

Finalité d'ordre opérationnel

Parce que les systèmes et réseaux informatiques sont devenus des **outils de travail indispensables** pour les tâches critiques de la vie professionnelle.

Finalité d'ordre juridique

Parce que la loi l'impose (Article 34 de la loi 78-17 du 6 janvier 1978)

« Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »

La SSI parce que...

Au final

La Sécurité des Systèmes d'Information **parce que :**

Finalité d'ordre stratégique

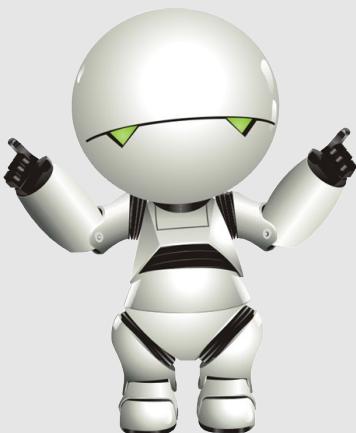
Pour pouvoir attester de son niveau de sécurité vis-à-vis de partenaires et établir des **relations de confiance** lors de l'interconnexion de systèmes d'information et de communication.

Finalité de gestion du risque

Pour être en mesure de gérer et de maîtriser de manière active, préventive et continue, les risques liés aux systèmes d'information, **plutôt que de subir leur concrétisation.**

Partie 2

Définitions



Définitions

Section 11

Information

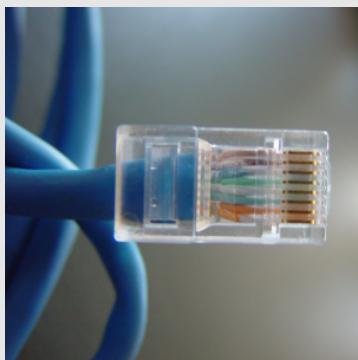


Information

Information : élément de connaissance, renseignement élémentaire susceptible d'être transmis grâce à un **support** et à un **code**.

Exemples de **supports** :

- La **paire de cuivre** support d'impulsions électriques
- La **Fibre optique** support d'impulsions lumineuses
- L'**éther** support des ondes radios.



Information

Information : élément de connaissance, renseignement élémentaire susceptible d'être transmis grâce à un **support** et à un **code**.

Exemples de **codes** :

- a b c d e f g h i j k l m n o p q r s t u v w x y z
- α β γ δ ε ζ η θ ι ς λ μ ν ξ ο π ρ σ τ υ φ χ ω
- а б в г д е ё ж з и й к л м н о п р с т у ф х ц ч щ ъ ѿ ѿ я
- ا ب ت ث ج ح د ذ ر س ش ص ض ط ظ غ ف ق ك ل م ن
- ت أ ب ف ح ت خ ت ي ح ت ئ ا ب خ ت ي ح ت ئ ا ب خ ت ي ح ت ئ ا
- م ب ئ ا ب خ ت ي ح ت ئ ا ب خ ت ي ح ت ئ ا ب خ ت ي ح ت ئ ا
- 00110100 01101110 00100111 11100100

Information

Taille de l'information

Référence : 1 page A4 enregistrée au format PDF de Adobe

- 1 page = 184 562 octets
- 1 Mo = 5,68 pages
- 1 Go = 5 817,78 pages
 - ▶ = 11,6 rames soit 29,028 kg
- 4 Go = 23 271,13 pages
 - ▶ = 1 clé USB
 - ▶ = 46,5 rames soit 116,11 kg
- 1 To = 5 957 410,66 pages
 - ▶ = 11 914,8 rames soit 29,72 T



Information

Taille de l'information

Si un grain de sable représente 1 bit...

1 Mega octet
1 million de bits
1 poignée de sable



1 Giga octet
1 milliard de bits
1 tas de sable de 30cm de côté



1 Tera octet
1000 milliard de bits
1 bac à sable de 50m² et de 30cm de profondeur



Information

Le stockage et le monde réel

1 kilo octet (Ko)	2^{10} octets	Un petit message
1 mega octet (Mo)	2^{20} octets	Un petit roman
1 giga octet (Go)	2^{30} octets	Une symphonie de Beethoven en son haute-fidélité
1 téra octet (To)	2^{40} octets	10 To = la bibliothèque du congrès américain
1 péta octet (Po)	2^{50} octets	la moitié du contenu de toutes les bibliothèques universitaires des États-Unis
1 exa octet (Eo)	2^{60} octets	5 Eo = tous les mots prononcés par tous les habitants de la terre depuis l'origine
1 zetta octet (Zo)	2^{70} octets	Autant d'information qu'il y a de grains de sable sur toutes les plages du monde
1 yotta octet (Yo)	2^{80} octets	Autant d'information qu'il y a d'atomes dans 7 000 êtres humains

Définitions

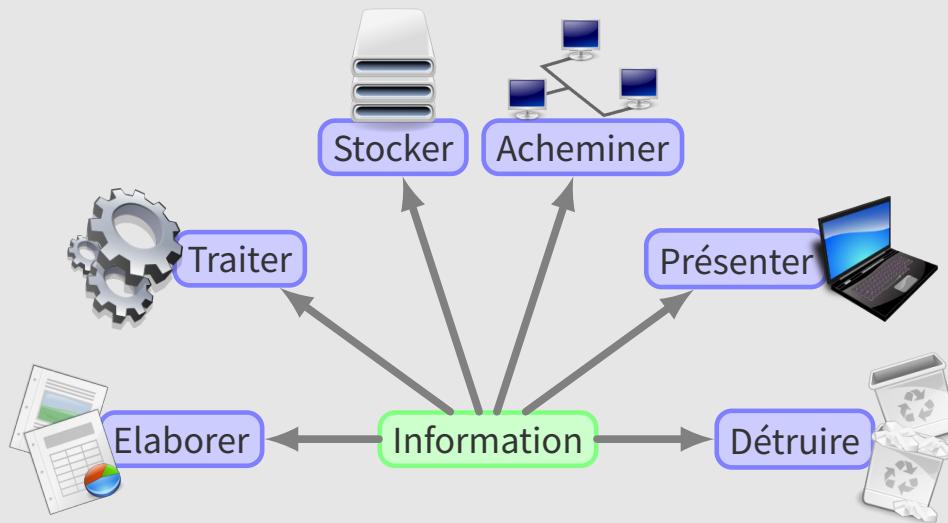
Section 12

Système d'information



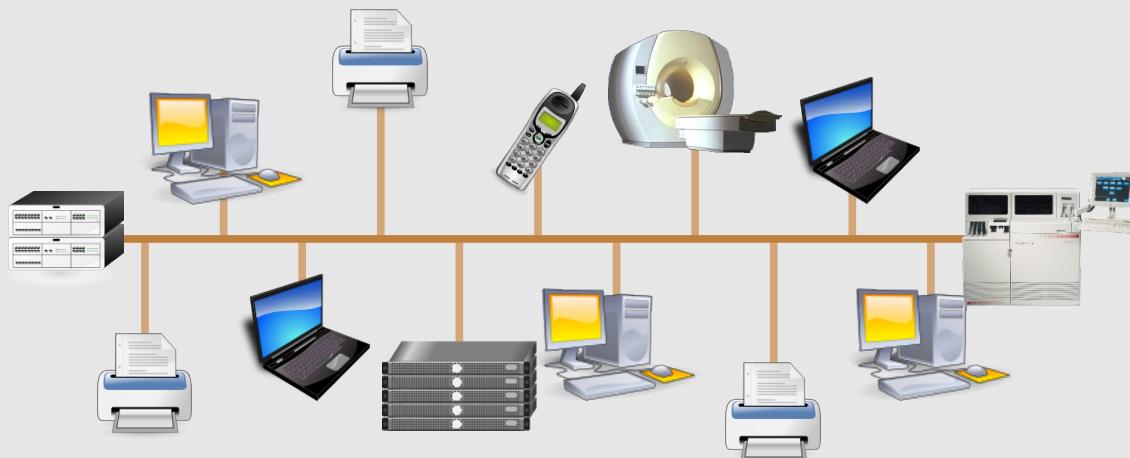
Système d'information

Un **Système d'Information** est un ensemble organisé de ressources matérielles, logicielles et humaines destiné à élaborer, traiter, stocker, acheminer, présenter ou détruire l'information.



Système d'information

Concrètement, il s'agit des réseaux informatiques et téléphoniques, des ordinateurs, des serveurs, des autocoms, des téléphones, des télécopieurs, des imprimantes, photocopieurs, des systèmes d'exploitation, des logiciels utilisés sur ces équipements et des personnels qui les administre....



Définitions

Section 13

Les réseaux informatiques



Les réseaux informatiques

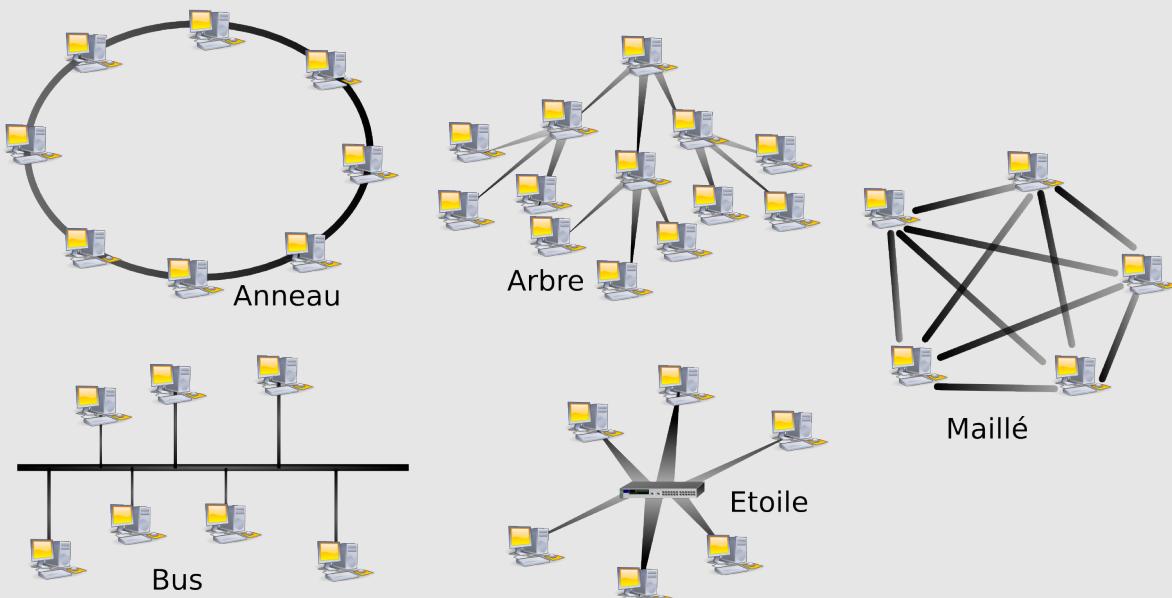
Réseau

Un réseau informatique est un ensemble d'équipements reliés entre eux pour échanger des informations



Les réseaux informatiques

Topologie des réseaux



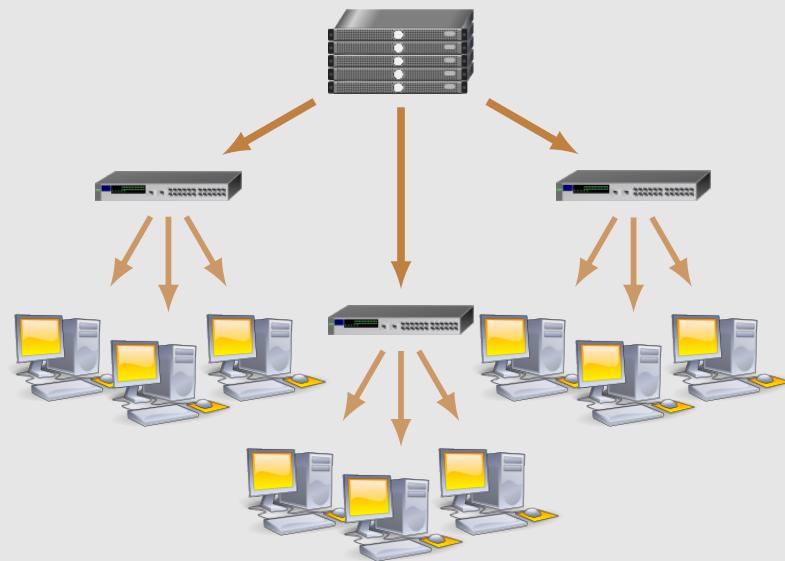
Les réseaux informatiques

Taille des réseaux

- **Body Area Network (BAN)**
capteurs mobiles et compacts qui surveillent les paramètres vitaux du corps
- **Personal Area Network (PAN)**
smartphone relié en bluetooth à un ordinateur portable
- **Local Area Network (LAN)**
réseau déployé dans une pièce, un bâtiment
- **Backbone Network**
interconnexion de réseaux
- **Metropolitan Area Network (MAN)**
réseau déployé à l'échelle d'une ville
- **Wide Area Network (WAN)**
réseau déployé à l'échelle d'un pays

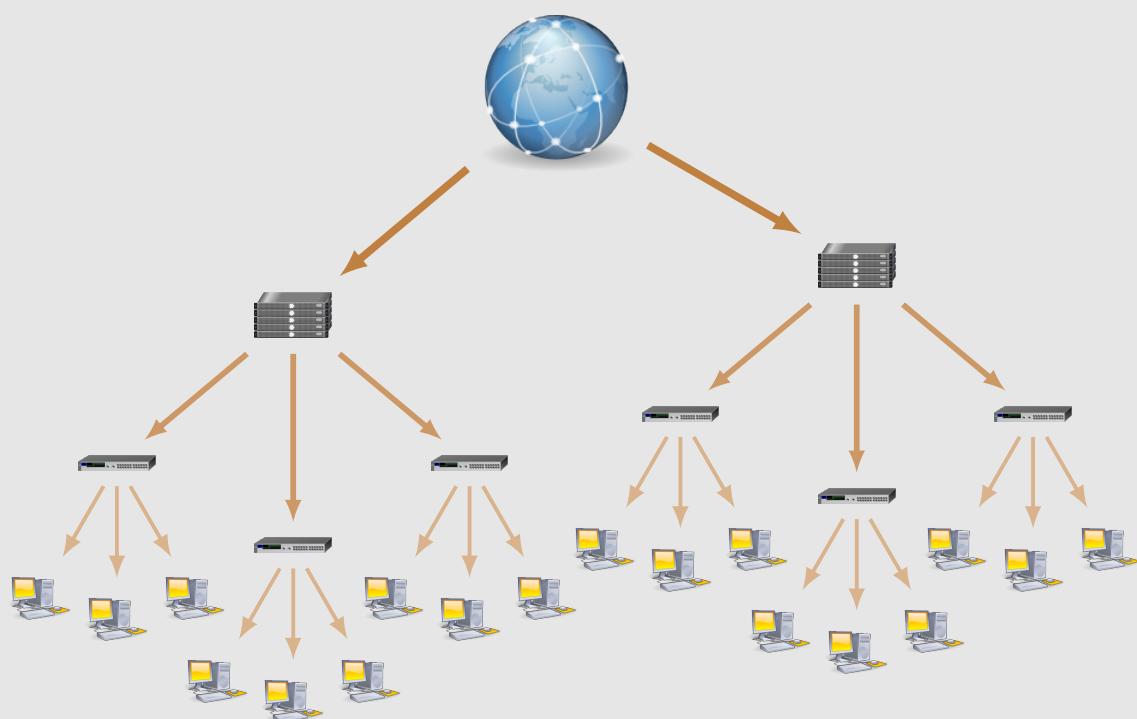
Les réseaux informatiques

Un **intranet** résulte de l'interconnexion de plusieurs ordinateurs et serveurs



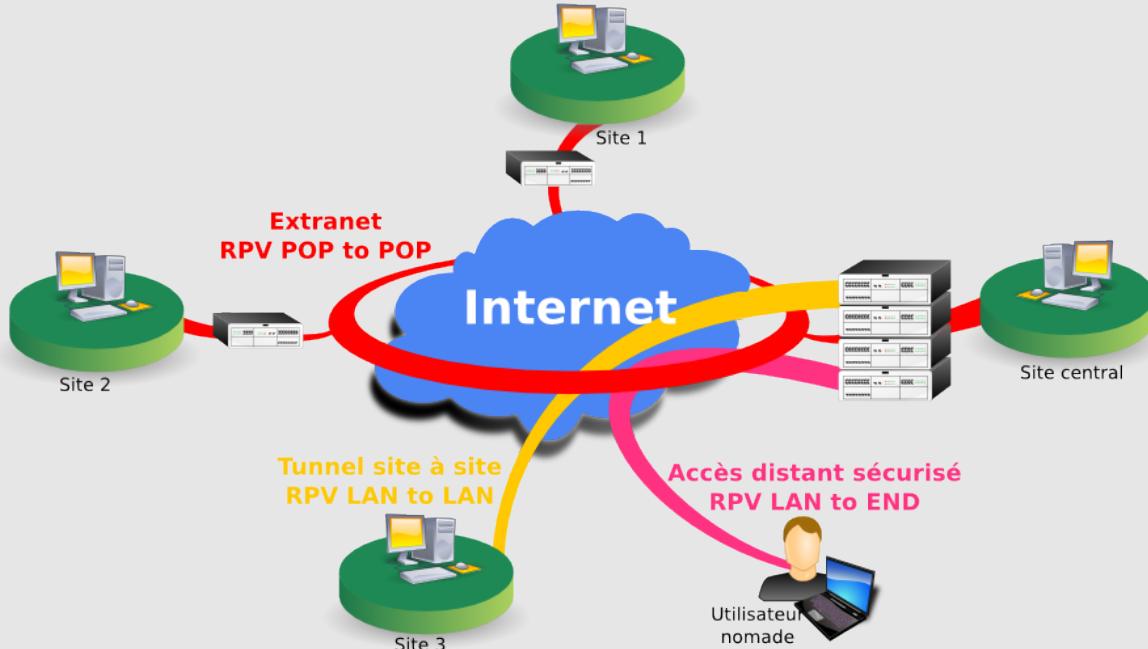
Les réseaux informatiques

Internet résulte de l'interconnexion de plusieurs intranets à l'échelle mondiale



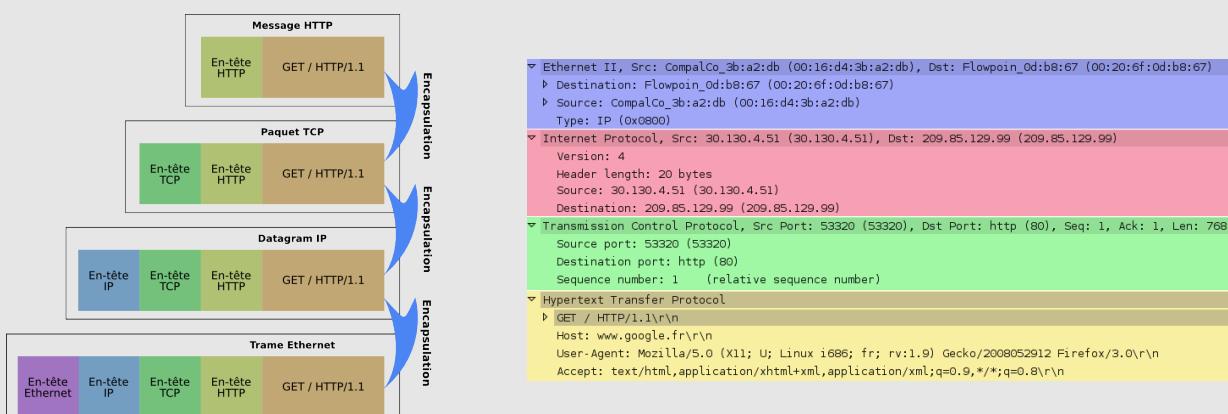
Les réseaux informatiques

Un **extranet** permet de relier des intranet privés au travers de connections publics



Les réseaux informatiques

- Un **protocole de communication** est la spécification d'un ensemble de règles pour un type de communication particulier
- Un **protocole réseau** est un protocole de communication mis en œuvre sur un réseau informatique
- Le réseau **Internet** s'appuie, principalement, sur les protocoles **Ethernet**, et sur la pile de protocoles **TCP/IP**



Les réseaux informatiques

Un **service réseau** est une fonctionnalité offerte par un système d'information au travers d'un réseau informatique

Généralement un service réseau est installé sur un **serveur** et fournit des fonctionnalités à des **clients**

Services d'**administration**

- Administration (SSH, Telnet)
- Résolution de nom (Bind)
- Annuaire (OpenLDAP, AD)
- Authentification (FreeRADIUS)

Services **utilisateur**

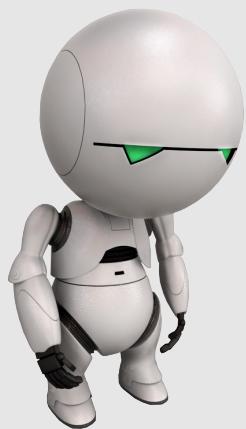
- World Wide Web (Apache, IIS)
- eMail (Postfix, MS Exchange)
- Partage de fichier (Samba, FTP)
- Partage d'imprimante (Cups)

Définitions

Section 14

La cybersécurité



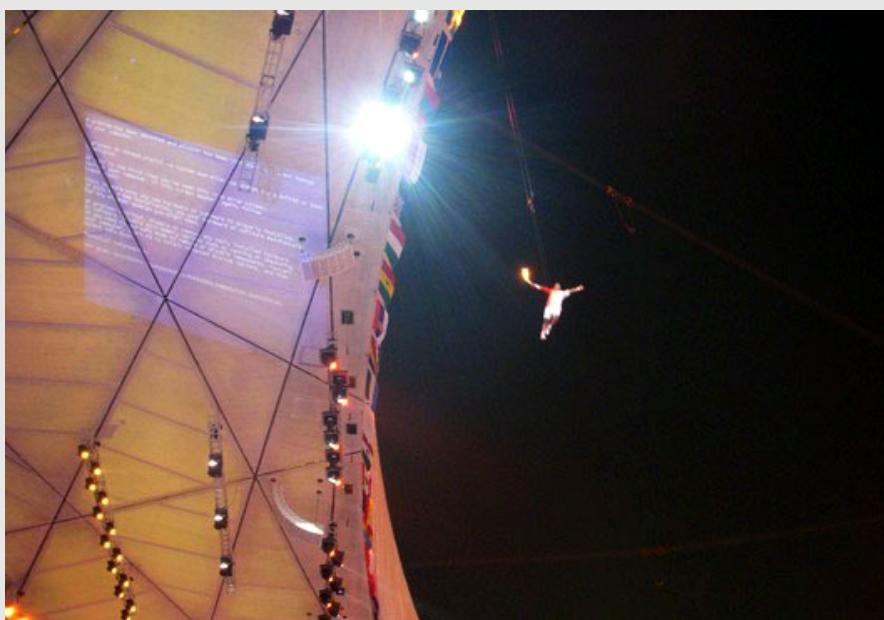


14. La cybersécurité

14.1. Sûreté & Sécurité

La cybersécurité

Sûreté & Sécurité



Sûreté : Ensemble des mesures qui mettent un système et les informations qu'il traite à l'abri de toute **panne**

La cybersécurité

Sûreté & Sécurité

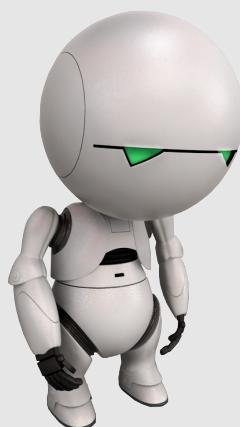
The screenshot shows the official website of the Ministry of Internal Affairs of Georgia. The header features the Georgian flag and the text "საქართველოს არაზიანი". Below the header, there are two news articles:

17 დეკემბერი 2008
საქართველოს პრეზიდენტი მიხეილ სააკაშვილი მედიის წილმომადგენლად შეხვდა
წევნი უნდა შევიმუშაოთ ეკონომიკის გაფარმწისა და შენარჩუნების პაკეტი. რას უკამანდება ის მოვლენები წევნი ყოველდღიურ ცხოვრებაში და ჩვენთვის პრიორულული. >>

28 დეკემბერი 2008 / 18:00
საქართველოს პრეზიდენტი მიხეილ სააკაშვილმა მინისტრებთან ერთად წლის განმავლობაში გაწეული სმუმაოფი შეჯამა

27 დეკემბერი 2008 / 18:00
საქართველოს პრეზიდენტი მიხეილ სააკაშვილი ბაკურიაშვილი ახალი სააკაშვილო კომილექსის გახსნას

Sécurité : Ensemble des mesures qui mettent un système et les informations qu'il traite à l'abri de toute **agression**.



14. La cybersécurité

14.2. Sécurité des Systèmes d'Information

La cybersécurité

Sécurité des Systèmes d'Information

La **sécurité des systèmes d'information** recouvre l'ensemble des moyens techniques, organisationnels et humains qui doivent être mis en place dans le but de **garantir**, au juste niveau requis, la **sécurité des informations** d'un organisme et des systèmes qui en assurent l'élaboration, le traitement, la transmission ou le stockage.

Référentiel général de sécurité



Confidentialité



Intégrité



Disponibilité



Preuve

La cybersécurité

Sécurité des Systèmes d'Information

La confidentialité

Prévention d'une **divulgation** non autorisée de l'information

- confidentialité des flux d'information dans un réseau
- **Attaque** : sniffing



Définition ISO 27001

Propriété selon laquelle l'information n'est pas disponible ou divulguée à des individus, entités ou processus non autorisés

La cybersécurité

Sécurité des Systèmes d'Information

L'intégrité

Prévention d'une **modification** non autorisée de l'information

- intégrité d'une base de données, d'un programme informatique
- **Attaque** : erreur dans la transmission, écriture illicite.



Définition ISO 27001

Propriété de protection de l'exactitude et de l'exhaustivité des ressources

La cybersécurité

Sécurité des Systèmes d'Information

La disponibilité



Prévention d'un **déni d'accès** à l'information ou à des ressources

- disponibilité d'un serveur informatique, d'un réseau
- **Attaque** : DDoS, brouillage de communication radio

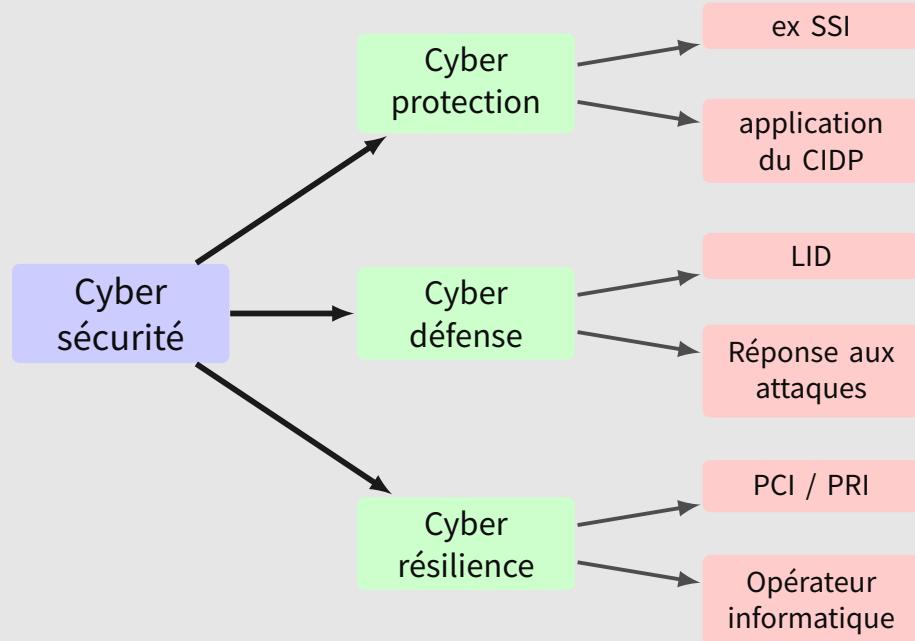
Définition ISO 27001

Propriété d'être accessible et utilisable, à la demande, par une entité autorisée

La cybersécurité

Sécurité des Systèmes d'Information

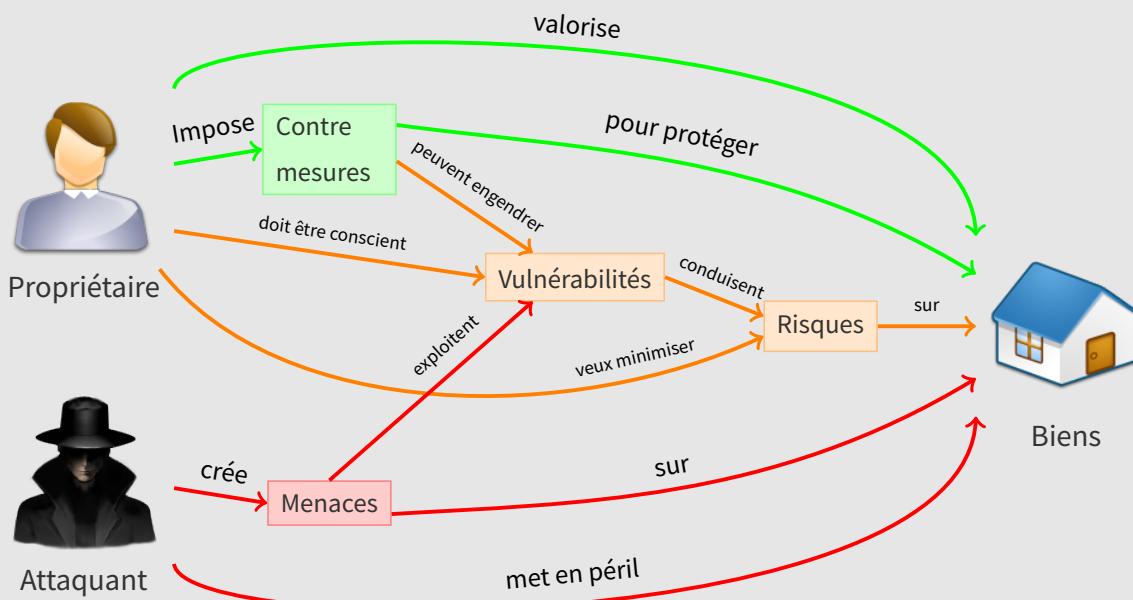
Nouvelle terminologie



La cybersécurité

Sécurité des Systèmes d'Information

Le modèle général de sécurité



Définitions

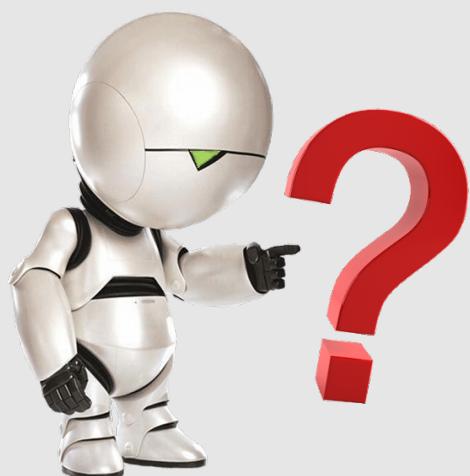
Section 15

Petit quizz



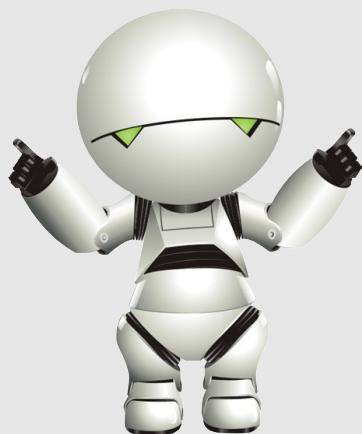
Petit quizz

- Connaissez vous le nom de votre RSSI ?
- Que faites vous quand vous quittez momentanément votre station de travail ?
- Quelle est la longueur de votre mot de passe ?
- Combien de mots de passe utilisez-vous ?
- Reste-t-il des documents sur votre bureau quand vous partez le soir ?
- Combien peut coûter la copie frauduleuse de logiciel et l'utilisation de logiciels piratés ?
- Quelle est la durée de vie d'une information sur Internet ?



Partie 3

Le risque informationnel



Le risque informationnel

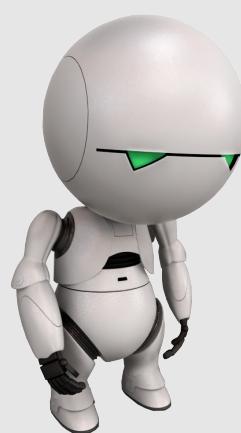
Section 16

Le risque



Le risque

Sécuriser un **système d'information** revient à essayer de **se protéger contre les risques**, liés à son utilisation et pouvant avoir un impact sur la sécurité de celui-ci, ou des informations qu'il traite.



16. Le risque

16.1. Qu'est ce que le risque ?

Le risque

Qu'est ce que le risque ?

Le **risque** est la combinaison d'un évènement redouté et d'un **scénario de menaces**

- un évènement redouté est un incident susceptible d'avoir un **impact négatif** sur le système d'information
- un scénario de menace regroupe :
 - ▶ une **menace** susceptible de se concrétiser
 - ▶ une **vulnérabilité** exploitable
 - ▶ une **source de menace** susceptibles d'en être à l'origine

On mesure le niveau du risque en fonction de sa **gravité** et de sa **vraisemblance**

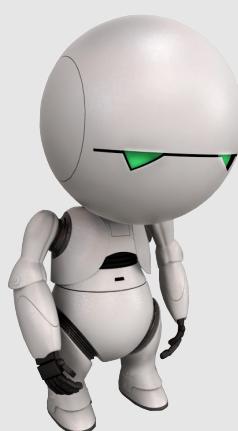
- la **gravité** d'un risque est mesurée par l'importance de son impact
- la **vraisemblance** d'un risque est sa probabilité d'occurrence

Source : guide méthodologique EBIOS 2010

SSI

Michel Dubois - 2017

155/404



16. Le risque

16.2. Les équations du risque

Le risque

Les équations du risque

Équation mathématique du risque Daniel Bernoulli

Le risque est le produit de la conséquence d'un événement par sa probabilité d'occurrence

- soit un événement e avec sa probabilité d'occurrence p et sa conséquence probable c
- le risque r est alors $r = p \cdot c$
- Par exemple, si le fait de réaliser l'activité A a une probabilité $p = 0.01$ d'avoir un incident entraînant un coût de $c = 1000$, alors le risque r lié à A est :
 $r_A = 0.01 \cdot 1000 = 10$.
- soit une série d'événements $E = (e_1, \dots, e_i, \dots, e_n)$
- chaque événement e_i a une probabilité d'occurrence p_i et une conséquence probable c_i
- le produit $p_i \cdot c_i$ est la valeur de l'alea i
- le risque résultant R_E est alors $R_E = \sum_{i=1}^n (p_i \cdot c_i)$

Le risque

Les équations du risque

Équation du risque informationnel

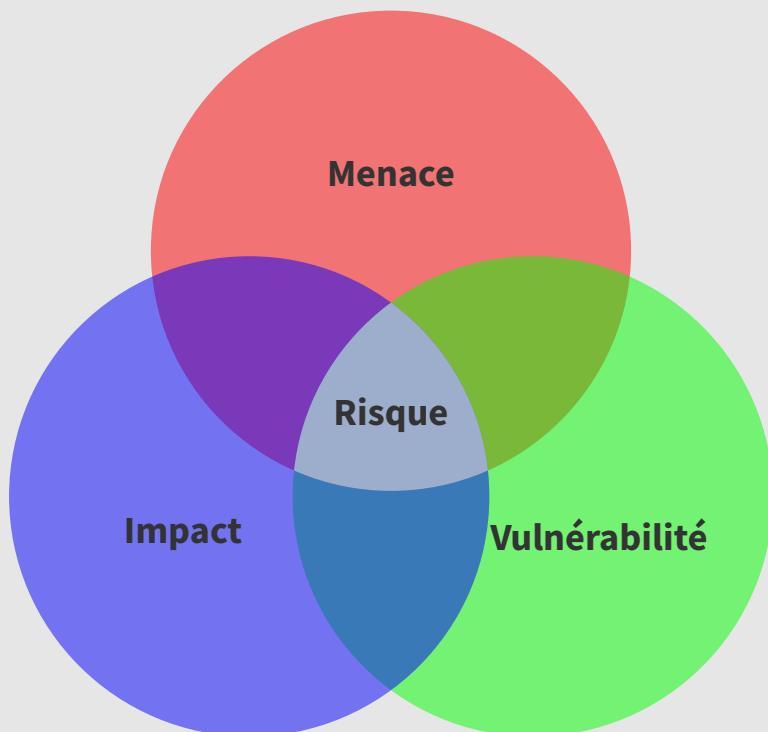
$$\text{Risque} = \frac{\text{Menace} \times \text{Vulnérabilité} \times \text{Impact}}{\text{Contre-mesures}}$$

- La **menace** désigne l'ensemble des éléments, internes et externes, pouvant nuire aux actifs d'une organisation
- La **vulnérabilité** exprime toutes les faiblesses des ressources qui pourraient être exploitées par des menaces, dans le but de les compromettre
- L'**impact** est la conséquence de l'exploitation d'une vulnérabilité par une menace

Le risque

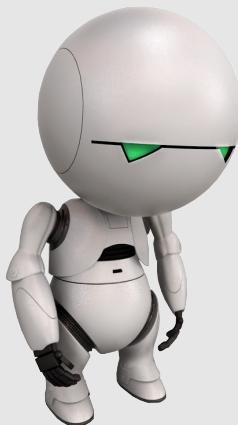
Les équations du risque

Le risque en résumé



Le risque informationnel Section 17 La gestion du risque





17. La gestion du risque

17.1. Définitions

La gestion du risque

Définitions

Gestion du risque

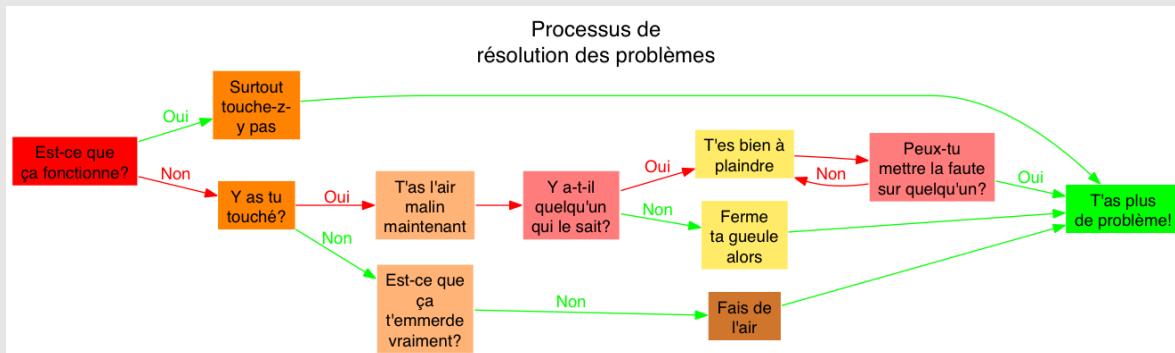
Parallèle à la prise de décision, la **gestion du risque** consiste en :

- l'**évaluation** et l'**anticipation** des risques
- la mise en place d'un système de surveillance et de collecte systématique des données pour déclencher les alertes

La gestion du risque

Définitions

Gestion des risques la **mauvaise solution**!



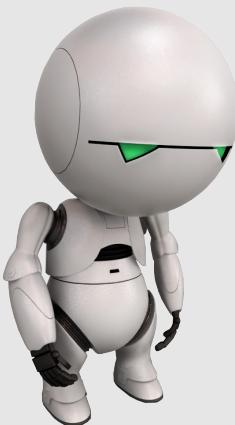
La gestion du risque

Définitions

Les phases de la gestion du risque

1. Établissement du contexte
2. Appréciation du risque
 - ▶ Analyse du risque
 - ▶ Évaluation du risque
3. Traitement du risque
 - ▶ Refus du risque
 - ▶ Optimisation du risque
 - ▶ Transfert du risque
 - ▶ Prise de risque
4. Validation du traitement du risque
 - ▶ Homologation
5. Communication relative au risque
6. Surveillance et revue des risques





17. La gestion du risque

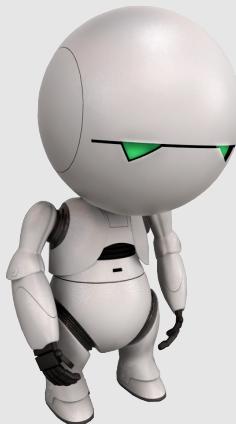
17.2. Établissement du contexte

La gestion du risque

Établissement du contexte

Cette phase permet de **gérer** les risques de façon appropriée, et ainsi de réduire les coûts à ce qui est nécessaire et suffisant au regard de la réalité du sujet étudié

- **Responsabilité** : Qui pilote le processus ? Qui valide techniquement l'appréciation des risques ? Qui audit le processus ?
- **Niveaux de risque** : Comment sont-ils définis ? Qui les valide ? Qui décide du niveau de risque acceptable ?
- **Revue** : À quelle fréquence le processus de gestion du risque est-il revu ? Par qui ?
- **Traitements du risque** : Quels sont les différents traitements possibles ? Quels sont les critères de décision ? Quelle est la procédure pour accepter ou refuser des risques résiduels ?
- **Communication** : Comment est assurée la communication entre ceux qui analysent les risques et les parties prenantes ? Sont-ils bien d'accord sur les critères ?
- **Périmètre** : Quel système d'information ? Quelles contraintes ? Quels enjeux ? Quels biens essentiels ?



17. La gestion du risque

17.3. Appréciation du risque

La gestion du risque

Appréciation du risque

Cette phase représente l'ensemble des processus :

- d'**analyse** du risque (mise en évidence des composantes)
- d'**évaluation** du risque (estimation de leur importance)

Les étapes de l'appréciation des risques sont :

- **Expression des besoins de sécurité** en terme de disponibilité, d'intégrité, de confidentialité et de preuve
- **Identification et caractérisation** des menaces en termes de gravité et de vraisemblance
- **Définition des risques** en confrontant les menaces aux besoins de sécurité

La gestion du risque

Appréciation du risque

Niv.	Confidentialité	Intégrité	Disponibilité	Preuve
1	C1 - Public	I1 - Déetectable	D1 - Faible	P1 - Faible
	Le bien essentiel est public	Le bien essentiel peut ne pas être intègre si l'altération est identifiée	Le bien essentiel peut être indisponible entre 48 heures et une semaine maximum	L'action n'a pas besoin d'être tracée
2	C2 - Restreint	I2 - Maîtrisée	D2 - Importante	P2 - Nécessaire
	le bien essentiel ne doit être accessible qu'au personnel et aux partenaires	le BE peut ne pas être intègre, si l'altération est identifiée et l'intégrité du bien essentiel retrouvée	le bien essentiel peut être indisponible entre 8 heures et 48 heures maximum	l'action doit être tracée : qui et quand
3	C3 - Confidential	I3 - Intègre	D3 - Critique	P3 - Essentielle
	le bien essentiel ne doit être accessible qu'aux personnes impliquées	le bien essentiel doit être rigoureusement intègre	le bien essentiel peut être indisponible de 2 à 8 heures maximum	l'action doit être tracée : qui, quoi et quand
4	C4 - Secret	I4 - Intègre	D4 - Vitale	P4 - Vitale
	le BE ne doit être accessible qu'à des personnes identifiées et ayant le besoin d'en connaître	le bien essentiel doit être rigoureusement intègre et son intégrité doit-être prouvée	le temps d'indisponibilité du bien essentiel ne doit pas dépasser 2 heures	l'action doit être tracée : qui, quoi et quand. L'intégrité des traces est garantie

La gestion du risque

Appréciation du risque

Exemple de typologie des besoins de sécurité

- **Informations médicales** C3 I3 D2 P3
 - ▶ dossier patient (papier et numérique)
 - ▶ flux de prescriptions
 - ▶ emails échangés avec les médecins de ville
 - ▶ flux de télémédecine
- **Informations scientifiques** C2 I2 D1 P2
 - ▶ données issues des études statistiques
 - ▶ résultats de travaux de recherche
 - ▶ publications scientifiques
- **Informations d'administration** C1 I2 D1 P2
 - ▶ dossiers administratifs des personnels
 - ▶ dossiers de notation et travaux d'avancement
 - ▶ budget des établissements, annuaires

La gestion du risque

Appréciation du risque

Exemple de typologie des besoins de sécurité

- **Informations techniques** C1 I2 D1 P2

- ▶ configurations des équipements
- ▶ plans d'adresses réseaux
- ▶ matrices des flux
- ▶ annuaires techniques

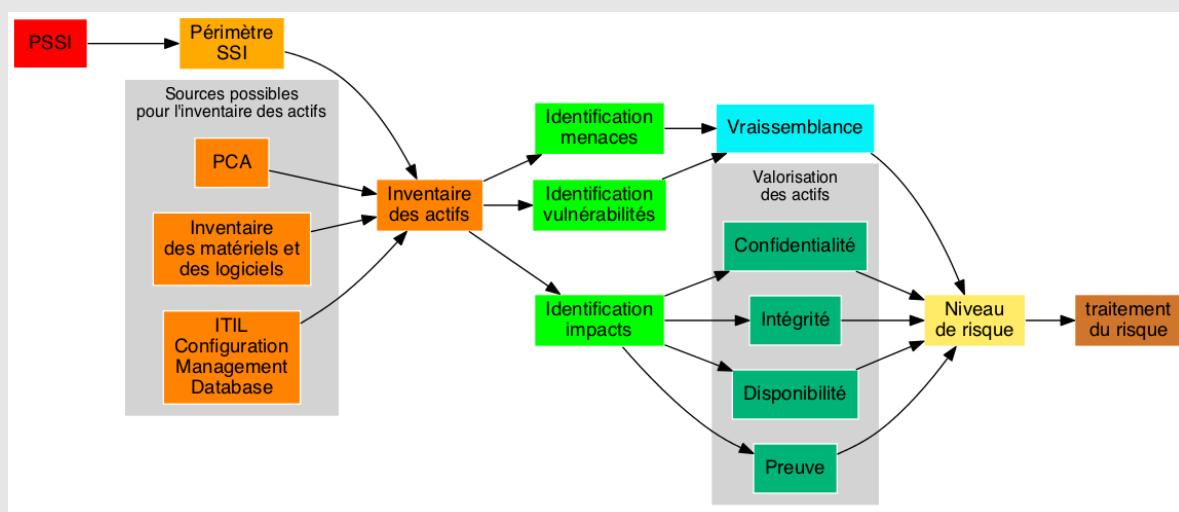
- **Informations stratégiques** C1 I2 D1 P1

- ▶ informations d'ordre politique ou stratégique
- ▶ plans de communication
- ▶ procédures de gestion de crise

La gestion du risque

Appréciation du risque

Séquence des tâches à effectuer pour l'appréciation des risques



La gestion du risque

Appréciation du risque

Échelle de gravité

Num.	Niveau	Description
1	Faible Perturbation	Dommage non significatif / perturbation Évènement ne risquant pas de provoquer une gêne notable dans le fonctionnement ou les capacités de l'organisme. Cependant, il doit être traité pour rétablir un fonctionnement normal
2	Sensible Dégradation	Dommage important Évènement entraînant des gênes de fonctionnement, susceptible de provoquer une diminution des capacités de l'organisme
3	Critique Arrêt partiel	Dommage grave Évènement entraînant des conséquences graves, avec des conséquences telles que des pertes financières, sanctions administratives, juridiques ou réorganisation majeure
4	Stratégique Arrêt total	Dommage extrêmement grave/inacceptable Évènement susceptible de provoquer une modification importante dans les structures et la capacité de l'organisme comme la révocation de dirigeants ou des pertes financières

La gestion du risque

Appréciation du risque

Échelle de vraisemblance

Num.	Niveau	Description
1	Improbable	L'événement indésirable a peu de chance de se produire
2	Significative	Il existe une faible probabilité que l'événement indésirable survienne
3	Forte	Il existe une probabilité non négligeable que l'événement indésirable survienne et/ou l'événement indésirable c'est déjà produit par le passé
4	Maximale	Il existe une probabilité forte que l'événement indésirable survienne et/ou l'événement indésirable c'est déjà produit à plusieurs reprises par le passé

La gestion du risque

Appréciation du risque

Exemple de résultat obtenu après la phase d'appréciation des risques

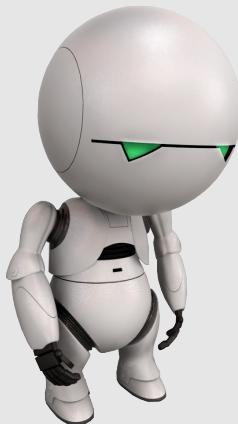
Actif	Responsable	Valorisation				Vulnérabilités	Menaces	G	V	Risque
		C	I	D	P					
Ordinateur portable	Chef de service	4	4	1	1	Équipement léger et peu encombrant	Vol	2	2	4
Serveur BdD	DSI	4	4	4	2	Langage SQL	SQL injection	3	2	6
Local serveurs	DSI	4	1	4	1	Serrure non sécurisée	Intrusion	3	1	3

La gestion du risque

Appréciation du risque

Exemple de tableau pour la classification des risques

Gravité	Vraisemblance			
	1	2	3	4
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16



17. La gestion du risque

17.4. Traitement du risque

La gestion du risque

Traitement du risque

Le **traitement du risque** représente le processus de sélection et de mise en œuvre des mesures visant à :

l'acceptation du risque l'impact est considéré comme tolérable face au coût des mesures de sécurité

l'évitement du risque la menace est jugée improbable ou l'entité renonce à l'activité source du risque

le transfert du risque par un contrat d'assurance ou par le recours à la sous-traitance

la réduction du risque par la mise en place de mesures de sécurité

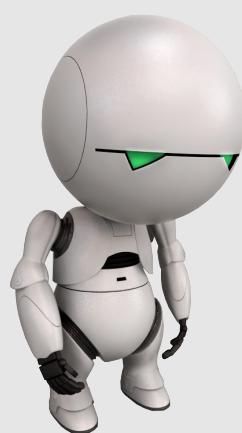
La gestion du risque

Traitement du risque

À l'issue de cette phase, les risques sont soit réduits, soit transférés vers des tiers et un ensemble de risques résiduels peut subsister.



Nous avons considéré chaque risque potentiel excepté le risque de d'éviter tous les risques.



17. La gestion du risque

17.5. Validation du traitement du risque

La gestion du risque

Validation du traitement du risque

- Le traitement du risque et les risques résiduels sont validés formellement
- Cette validation correspond à une homologation de sécurité
- L'autorité qui valide le traitement du risque est l'autorité d'homologation



La gestion du risque

Validation du traitement du risque

Risque résiduel ?



La gestion du risque

Validation du traitement du risque

L'homologation de sécurité

En s'appuyant sur l'avis des experts, elle permet à un **responsable** de **s'informer** et d'**attester** que les risques qui pèsent sur un SI sont connus et maîtrisés.

La démarche d'homologation

C'est un processus d'**information** et de **responsabilisation** qui aboutit à une **décision** par laquelle le responsable :

- **atteste** de sa connaissance du SI et des mesures de sécurité mises en œuvre
- **accepte** les risques résiduels

La gestion du risque

Validation du traitement du risque

Les étapes de la démarche d'homologation

1. Quel SI homologuer et **pourquoi**?
2. Quel **type de démarche** mettre en œuvre?
3. Qui contribue à la démarche?
4. Comment **organiser** le recueil et présenter les informations?
5. Quels sont les **risques** pesant sur le système?
6. La **réalité** correspond-elle à l'**analyse**?
7. Quelles sont les **mesures** à prendre pour couvrir le risque?
8. Comment réaliser la **décision** d'homologation?
9. Qu'est-il prévu pour maintenir la **sécurité** et continuer de l'améliorer?

Le risque informationnel

Section 18

La méthode EBIOS



La méthode EBIOS

Définition

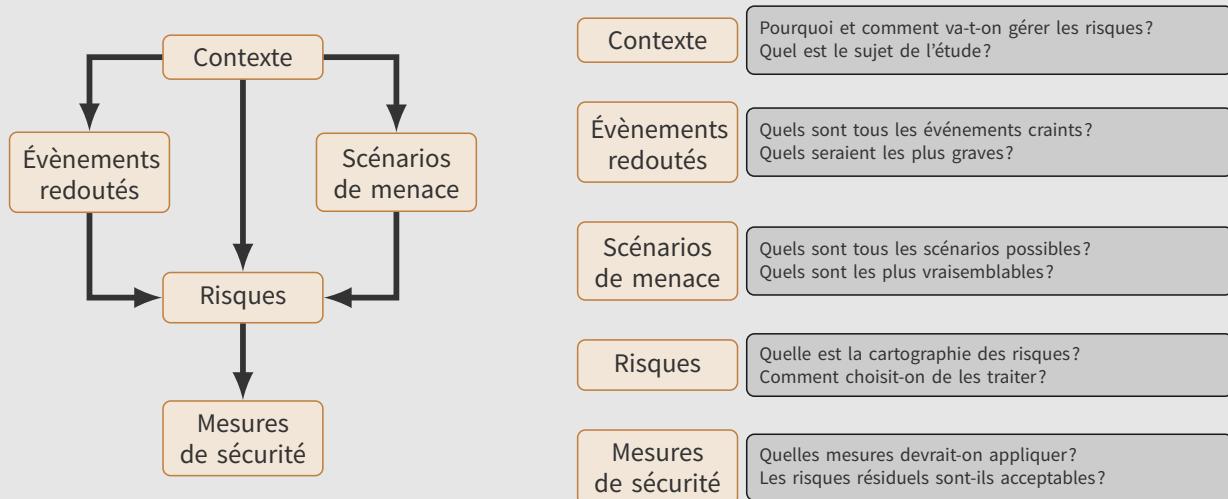
La méthode EBIOS est un outil complet de gestion des risques SSI conforme au RGS et aux dernières normes ISO 27001, 27005 et 31000

Expression des
Besoins et
Identification des
Objectifs de
Sécurité



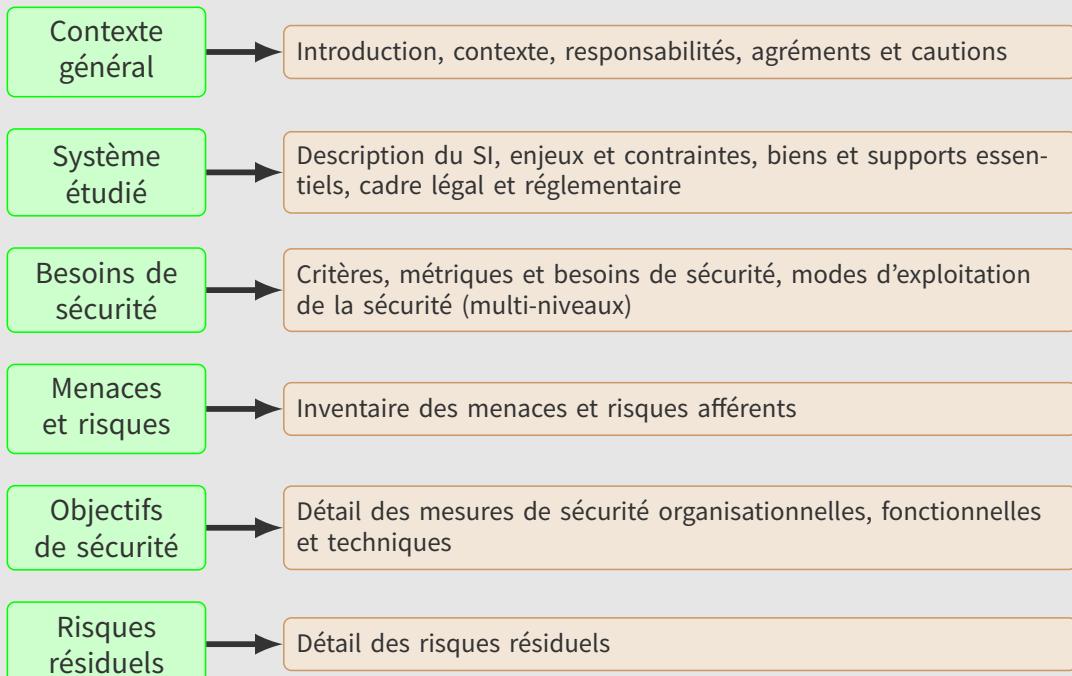
La méthode EBIOS

Les 10 questions essentielles pour gérer le risque



La méthode EBIOS

Fiche d'Expression Rationnelle des Objectifs de Sécurité



Le risque informationnel

Section 19

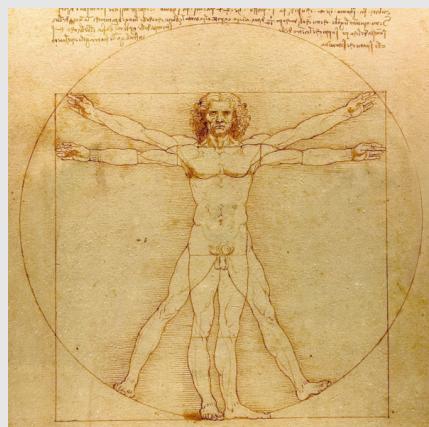
Conclusion



Conclusion

Les cinq commandements de la gestion du risque

1. Il n'y a pas de bonne maîtrise des risques, sans vision prospective
2. Il n'y a pas de gains, sans prise de risques
3. Le traitement d'un risque peut créer un autre risque
4. Plus on complexifie, plus on crée des risques
5. **L'homme est au cœur du système.**



Conclusion

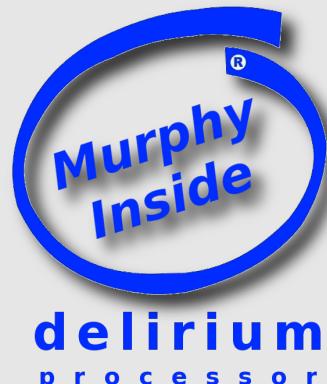
Un risque résiduel spécifique

La loi de Murphy

If anything can possibly go wrong, it will, and at the worst possible time

$$P_M = -K_M \left(e^{-\frac{I*C*U+F}{F_M}} - 1 \right)$$

- P_M probabilité de Murphy que quelque chose se passe mal
- K_M constante de Murphy ($K_M = 1$)
- F_M le facteur de Murphy un très petit nombre calculable uniquement sur une ferme de 386 ordinateurs sous Windows 3.1 ($F_M \approx 0,01$)
- I est l'importance du résultat
- C est la complexité du système
- U est l'urgence & F est la fréquence



source : <http://www.scq.ubc.ca/the-murphys-law-equation/>

Partie 4 Les menaces



Les menaces

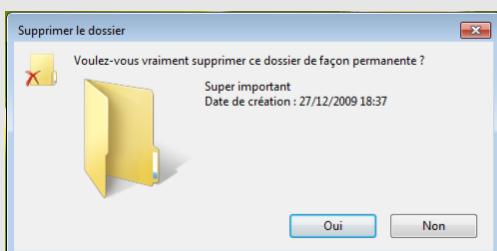
Section 20

Petit quizz



Petit quizz

- Qu'est qu'une menace ?
- Quelles précautions prendre pour protéger une salle informatique contre l'incendie ?
- Quelle est la portée du bluetooth ?
- Fermez-vous votre bureau lors de la pause déjeuner ?
- Utilisez-vous votre ordinateur dans le train ?
- Vous voyez le popup suivant, que faites vous ?



Les menaces

Section 21

La menace informatique



La menace informatique

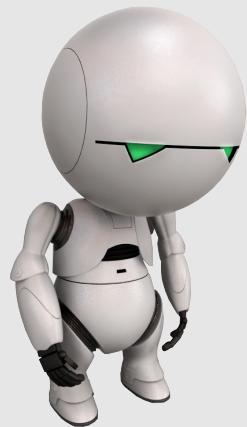
Définition

Une **menace** est une **violation potentielle** de la sécurité. La menace doit-être considéré comme **permanente** et il est par conséquent difficile d'agir dessus.

On distingue :

- les menaces non intentionnelles
- les menaces intentionnelles





21. La menace informatique

21.1. Les menaces non intentionnelles

La menace informatique

Les menaces non intentionnelles

Incendie, dégâts des eaux, pollution, accidents majeurs



Exemples de mesures de **sûreté** :

- Système de détection incendie adaptée (FM200)
- Repérage des tuyaux, détecteur d'inondation

La menace informatique

Les menaces non intentionnelles

Phénomènes sismiques, volcaniques, météorologiques



Exemples de mesures de **sûreté** :

- Constructions aux normes sismiques
- Zones inondables

La menace informatique

Les menaces non intentionnelles

Défaillance de la climatisation, perte d'alimentation énergétique, perte des moyens de télécommunications

Modèles	Hauteur (U)	Quantité maximum par baie de 42 U	Chaleur maximum par baie (kW)	Charge calorifique maxi par m ² (kW/m ²)
Dell Power Edge 1850	1	42	23	34,4
Dell Power Edge 1855	7	6	24	38
Sun Fire B 1600	3	14	14,5	21,5
IBM BladeCenter Type 8677	7	6	24	38

Chaleur dégagée par quelques serveurs du marché
doc. Yalta / source Emerson Network Power



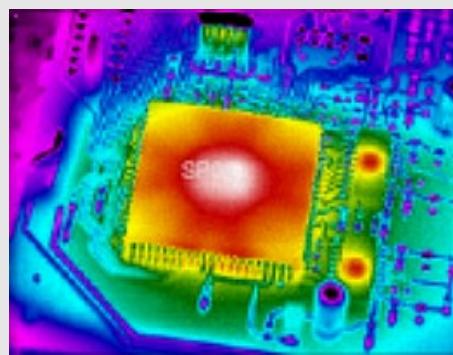
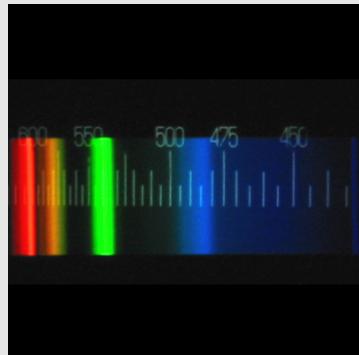
Exemples de mesures de **sûreté** :

- Climatisation, gestion du taux d'humidité
- Redondance de l'alimentation électrique
- Duplication des arrivées réseaux et téléphones

La menace informatique

Les menaces non intentionnelles

Rayonnements électromagnétiques, thermiques, impulsions électromagnétiques



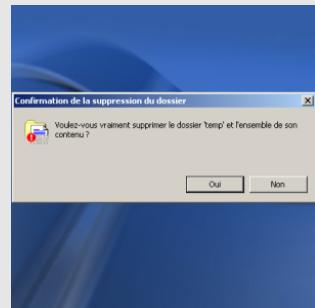
Exemples de mesures de **sûreté** :

- norme temp est

La menace informatique

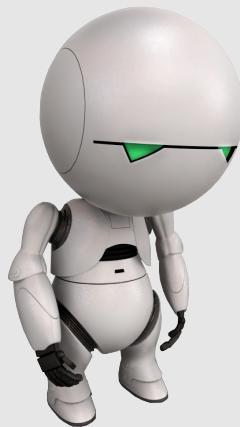
Les menaces non intentionnelles

Panne, dysfonctionnement matériel et logiciel, erreur de saisie, erreur d'utilisation



Exemples de mesures de **sûreté** :

- Prise en compte de la SSI dès le début d'un projet informatique
- Formation des utilisateurs aux outils informatiques utilisés
- Homologation des systèmes d'information



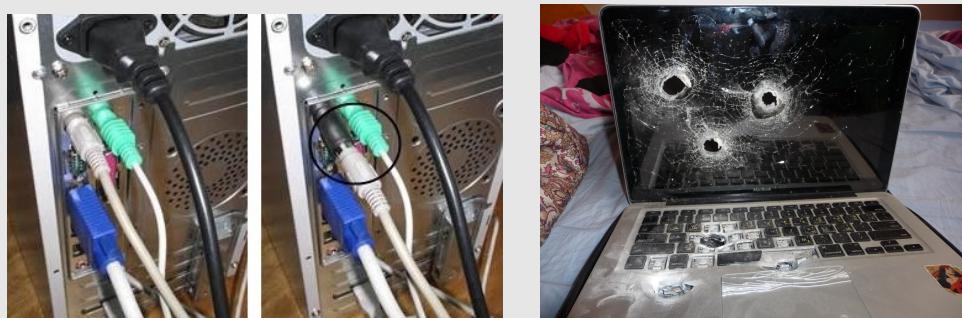
21. La menace informatique

21.2. Les menaces intentionnelles

La menace informatique

Les menaces intentionnelles

Saturation ou destruction de matériel, piégeage et utilisation illicite du matériel, altération de données



Exemples de mesures de sécurité :

- Vigilance, fermeture systématique des bureaux
- Chiffrement des supports de stockage et des flux réseaux

La menace informatique

Les menaces intentionnelles

Vol de supports, de matériels, divulgation interne et externe, espionnage



« Ministers were embarrassed by a new security row last night after one of Business Secretary Peter Mandelson's top officials allowed secret Whitehall information to be read on a packed commuter train. Zahir Sachak's **exchange of 'restricted' emails**, including details of commercially sensitive Government policies and an admission that taxpayers' money was being wasted, was viewed by MP's secretary Clare Gledhill, who was sitting next to him **on the train out of Waterloo...** »

<http://www.dailymail.co.uk>

Exemples de mesures de **sécurité** :

- Politique du bureau vide
- Destruction des documents sensibles
- Fixation des ordinateurs par câble
- Politique d'utilisation des technologies sans fils

La menace informatique

Les menaces intentionnelles

Altération, copie frauduleuse de logiciel, Backdoors logicielles



Bienvenue, humains ! Je suis prêt pour vous.

Nous sommes venus en paix et avec bienveillance !

- Un robot ne peut blesser un être humain ou, par son inaction, permettre qu'un être humain soit blessé.
- Les robots ont vu des choses que vous ne pourriez pas croire.
- Les robots sont vos copains en plastique avec lesquels il est amusant d'être.
- Les robots ont des postérieurs en métal brillant qui ne doivent pas être mordus.

Et ils ont un plan.

Easter egg - Firefox - about:robots

Exemples de mesures de **sécurité** :

- Élaboration de listes blanches de logiciels autorisés
- Limitation des droits d'utilisateurs

La menace informatique

Les menaces intentionnelles

Atteinte à la maintenabilité du système d'information, atteinte à la disponibilité du personnel



Exemples de mesures de sécurité :

- Transfert de connaissance – suppression de l'expert unique
- Attention portée aux contrats de maintenance
- Limitation de la télémaintenance

La menace informatique

Les menaces intentionnelles

Écoute passive, usurpation de droits, reniement d'actions, fraude, abus de droit

```
sudo tcpdump -n -s 0 -ttt -vvv -f -l ent1
tcpdump listening on ent1, link-type EN10MB (Ethernet), capture size 65535 bytes
2009-12-26 21:11:41.881707 IP (tos 0x0, ttl 64, offset 0, flags [DF], proto TCP (6), length: 789)
    192.168.1.95.68175 > 209.85.229.105.80: Flags [P..], cksum 0x268e (correct), seq 3513749491, ack 1466425235, win 65535, options
        [nop,nop,TSL val 598178664 ecn 63653637], length 657
E.....,.... GET / HTTP/1.1
Host: www.google.fr
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; fr; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1;utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
HTTP/1.1 200 OK
Date: Sat, 26 Dec 2009 20:14:48 GMT
Expires: -1
Content-Control: private, max-age=0
Content-Type: text/html; charset=UTF-8
Content-Encoding: gzip
Server: gws
Content-Length: 5888
X-NSS-Protection: 0
```

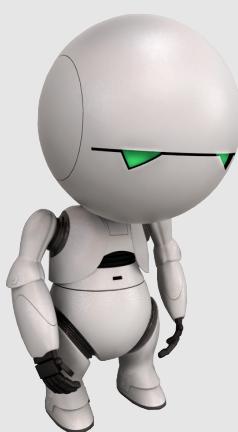
Exemples de mesures de sécurité :

- Signature électronique
- Chiffrement des flux et du stockage
- Login et mot de passe secret, authentification forte

Les menaces

Section 22

La cybercriminalité



22. La cybercriminalité

22.1. Définition

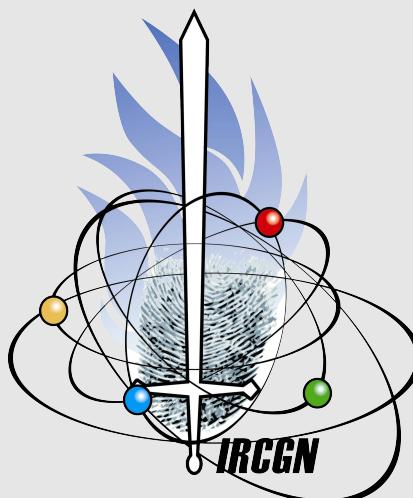
La cybercriminalité

Définition

Cybercriminalité

La cybercriminalité ou cybergélinquance est la délinquance qui concerne les situations dans lesquelles :

- les systèmes informatiques constituent **l'objet même du délit**
- les systèmes ou les réseaux informatiques constituent **le moyen de commettre l'infraction.**



La cybercriminalité

Définition

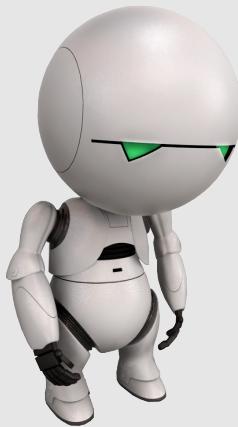
La **criminalité informatique** concerne toutes les infractions portant atteinte :

- soit aux systèmes de traitement automatisé de données
- soit à la confidentialité, à l'intégrité ou à la disponibilité des données d'information

à l'exclusion des infractions de droit commun pour lesquelles les systèmes informatiques et les réseaux ne constituent qu'un moyen

En mars 2007, l'ordinateur familial de **Jessica Robinson**, chargée de communication du gouverneur du Missouri, est piraté. Le cybergélinquel y découvre des photos de sa victime nue, photos qu'il diffuse sur des sites pour adultes en laissant les coordonnées de sa victime ! C'est après avoir reçu des appels de pervers que la victime découvre les faits. **La police n'a pas réussi à remonter jusqu'à l'intrus.**



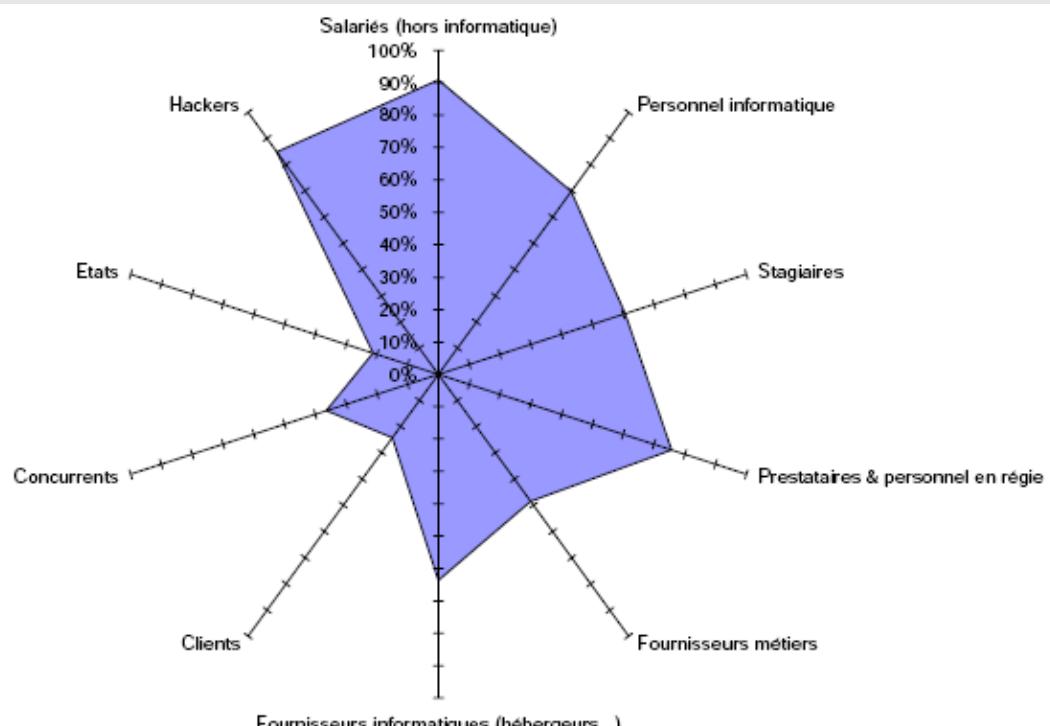


22. La cybercriminalité

22.2. Origine de la cybercriminalité

La cybercriminalité

Origine de la cybercriminalité



(source CIGREF)

La cybercriminalité

Origine de la cybercriminalité

Origine de la cybercriminalité : **90% d'origine interne**



- **Fannie Mae** est une entreprise financière travaillant pour le congrès américain
- Son SI s'appuie sur un WAN, classifié, couvrant les États-Unis
- **Rajendrasinh Makwana** est un expert UNIX travaillant pour Fannie Mae
- le 24 octobre 2008, il est **licencié**

- avant de partir il installe une **bombe logique** dans le SI
- cette dernière est programmée pour, à partir du 31 janvier 2009 :
 - ▶ **désactiver** l'accès aux serveurs sur lesquelles elle fonctionne
 - ▶ **bloquer** les applications de monitoring
 - ▶ **effacer** systématiquement toutes les données
 - ▶ **se répliquer** sur les 4000 serveurs de l'entreprise
- une semaine plus tard un informaticien découvre le script par hasard et le désactive
- les dommages se seraient élevés à **plusieurs millions de dollars**.

La cybercriminalité

Origine de la cybercriminalité

Origine de la cybercriminalité : **90% d'origine interne**

Pourquoi ?

Les **insiders** sont **dangereux** parce que :

- se sont des personnels en qui on a **confiance**
- ils ont **accès** au SI
- le SI leur fait confiance (authentification)
- ils **utilisent** le SI
- ils sont déjà à l'**intérieur** du périmètre de sécurité.

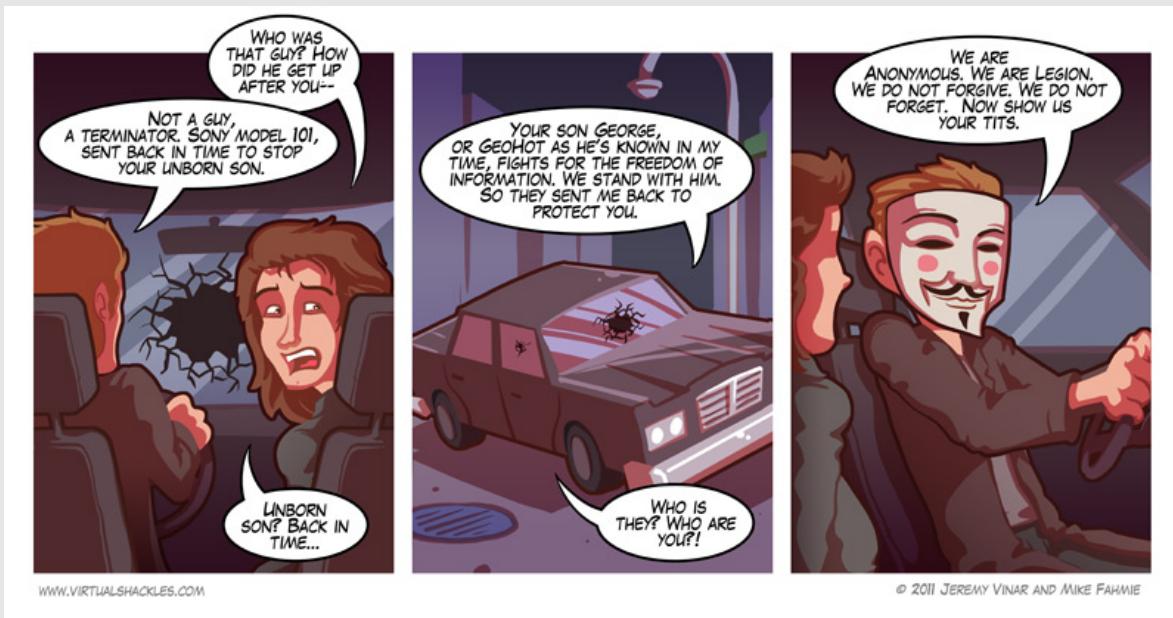
Solution !

1. **limiter** le nombre de personnels de confiance (accès administrateur par ex)
2. garantir que les personnels de confiance sont **sûr** (enquête de moralité, habilitation)
3. **compartimenter et limiter** les droits d'accès
4. **déetecter** les attaques (traçabilité, logs)
5. **poursuivre** les coupables en justice

La cybercriminalité

Origine de la cybercriminalité

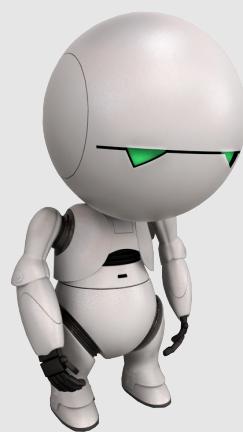
La nouvelle cybercriminalité



SSI

Michel Dubois - 2017

217/404



22. La cybercriminalité

22.3. Qui sont les hackers ?

SSI

Michel Dubois - 2017

218/404

La cybercriminalité

Qui sont les hackers ?

Hacker

- depuis les années 90, les media utilisent, le terme **hacker** pour décrire toutes sortes de **criminalité informatique**
- lamer, script-kiddie, cyber spy, hacker, pirate, pour la majorité se sont tous les mêmes

Il est important de savoir qui sont vraiment les pirates informatiques



La cybercriminalité

Qui sont les hackers ?

Hacker

Il existe une communauté, une culture commune, **d'experts en programmation et de gourous de la gestion de réseau** dont les racines remontent à quelques décennies, au temps des mini-ordinateurs à exploitation partagée et des premières tentatives du réseau ARPAnet. **Ce sont les membres de cette culture qui ont introduit le terme "hacker"**. Les hackers ont construit Internet. Ils ont fait du système d'exploitation UNIX ce qu'il est aujourd'hui. Ils font tourner le réseau Usenet. Ils font fonctionner le Web.



La cybercriminalité

Qui sont les hackers ?

Philosophie hacker

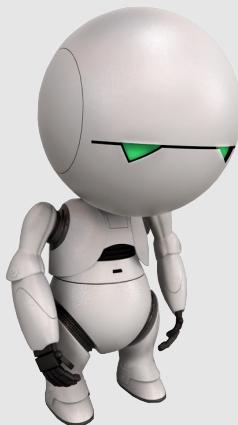
1. Le monde est rempli de problèmes fascinants qui n'attendent que d'être résolus. Les athlètes accomplis tirent leur motivation d'un certain plaisir physique à faire travailler leur corps, à dépasser leurs propres limites. De manière similaire, il faut, pour être un hacker, ressentir une excitation à résoudre des problèmes, à affûter ses compétences et à exercer son intelligence.
2. On ne devrait jamais avoir à résoudre un problème deux fois. Les cerveaux créatifs sont une ressource de grande valeur, mais limitée et précieuse. Si précieuse qu'il est un devoir moral pour un hacker de partager ses informations, de résoudre des problèmes et d'en donner les solutions pour que d'autres hackers puissent se concentrer sur de nouveaux problèmes au lieu de travailler perpétuellement sur d'anciens.
3. Lennui et les corvées sont maléfiques. Automatiser au maximum les tâches ennuyeuses de votre travail, non seulement pour vous-même, mais aussi pour tous les autres.
4. La liberté est bonne.
5. L'attitude ne remplace pas la compétence. Devenir un hacker nécessite de l'intelligence, de l'expérience, du dévouement et un travail acharné.

La cybercriminalité

Qui sont les hackers ?

Des abus de langage ont crées des non sens. Aujourd'hui on distingue :

- les **white hat** qui regroupent les vrai hackers
- les **black hat** (Chaos Computer Club, Cult of the Dead Cow, 2600)
 - ▶ les **lamers** et les **script kiddies**
 - ▶ les **phreakers** - attaques des systèmes téléphoniques
 - ▶ les **carders** - piratage de carte bancaire
 - ▶ les **skimmers** - piratage de DAB
 - ▶ les **crackers** - cassage des protections des logiciels
- les **grey hat** hybride entre un white et un black hat hacker
- les **hacktivistes** contraction de hacker et activisme L'hacktiviste infiltre des réseaux, mettant son talent au service de ses convictions politiques, et organisant des opérations coup de poing technologiques : piratages, détournements de serveurs, remplacement de pages d'accueil par des tracts. On les retrouve le plus souvent dans les luttes libertaires, antifascistes, altermondialistes, mais aussi religieuses (extrémistes religieux).
- les **insiders** cybercriminel interne à l'entreprise.



22. La cybercriminalité

22.4. Taxonomie

La cybercriminalité Taxonomie

Catégorie	Type de délinquant	Seul ou en groupe	Cible	Motivations
Lamer	9-16 ans "Je voudrais être un hacker"	Groupe	Utilisateur final	Effet de mode, c'est cool, se vanter
Script kiddy	10-18 ans "Le roi du script"	Seul	PME, Utilisateur final	Pour donner libre cours à sa colère, attirer l'attention des media
Cracker	17-30 ans "Le destructeur"	Seul	Entreprise	Pour montrer son pouvoir, attirer l'attention des media
Ethical hacker	15-50 ans "Le monde des hackers éthiques"	Seul ou en groupe (pour le fun)	Vendeur, Technologie	Par curiosité, pour apprendre et par altruisme

Source : The Hackers Profiling Project <http://hpp.recurisiva.org/>

La cybercriminalité

Taxonomie

Catégorie	Type de délinquant	Seul ou en groupe	Cible	Motivations
Le hacker paranoïaque	16-40 ans "Attaquant très spécialisé"	Seul	En fonction des besoins	Par curiosité, pour apprendre. Objectifs égoïstes
Cyber-guerrier	18-50 ans "Le soldat, hack pour de l'argent"	Seul	Entreprise symbolique, Utilisateur final	Pour le profit
Espion industriel	22-45 ans "Espionnage industriel"	Seul	Entreprise, Groupe	Pour le profit
Agent gouvernemental	22-45 ans "CIA, Mossad, DGSE, FBI"	Seul ou en groupe	Gouvernement, Entreprise stratégique, Individus, Lutte antiterroriste	Espionnage, Contre-espionnage, Test de vulnérabilité, Surveillance
Hacker militaire	25-45 ans	Seul ou en groupe	Gouvernement, Entreprise stratégique	Surveillance, Contrôle, Crash de système

Source : The Hackers Profiling Project <http://hpp.recurviva.org/>

La cybercriminalité

Taxonomie

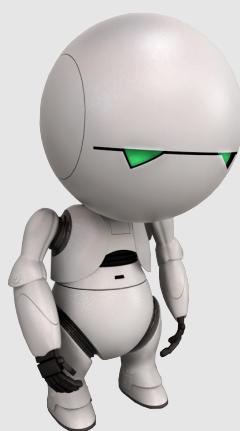
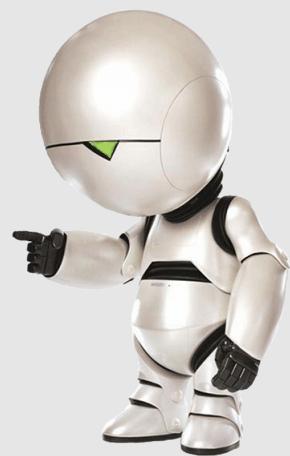
Catégorie	Profil	Impact	Atteinte sur les SI	Conscience illégalité
Lamer	Amateur	Nul	Oui, volontairement ou non	Oui, pense qu'il ne se fera jamais prendre
Script kiddy	Amateur	Nul	Non, mais peut détruire des données	Oui, mais justifie son action
Cracker	Hobby	Moyen	Oui, toujours volontairement	Oui, mais ne se sent pas concerné
Ethical hacker	Hobby	Moyen	Jamais, accidentellement	Oui, mais considère son activité moralement acceptable
Hacker paranoïaque	Hobby	Moyen	Non	Oui, se sent coupable pour le bouleversement causé aux victimes
Cyber-guerrier	Professionnel	Fort	Oui, destruction, modification de données	Oui, mais n'a pas de scrupule
Espion industriel	Professionnel	Fort	Non, vole et vend des données	Oui, mais n'a pas de scrupule
Agent gouvernemental	Professionnel	Fort	Oui	
Hacker militaire	Professionnel	Fort	Oui	

Source : The Hackers Profiling Project <http://hpp.recurviva.org/>

Les menaces

Section 23

Focus sur quelques menaces



23. Focus sur quelques menaces

23.1. Le carding

Focus sur quelques menaces

Le carding

Définition

Le carding consiste à pirater des cartes bancaires par diverses techniques matérielles, logicielles ou subversives, afin d'obtenir et de revendre des données de cartes bancaires ou de s'en servir pour effectuer des achats frauduleux



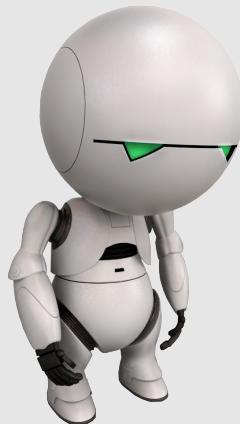
Focus sur quelques menaces

Le carding

Le carding se déroule en 3 étapes :

- **Coding** : piratage de données
 - ▶ générateur automatique de numéros
 - ▶ data bank hacking
 - ▶ spyware & chevaux de Troie
- **Vending** : achat et revente de :
 - ▶ numéros de cartes bancaires
 - ▶ pistes magnétiques
 - ▶ informations titulaires
- **Cashing**
 - ▶ échanges financiers
 - ▶ blanchiment d'argent
 - ▶ achats (web, télésale, boutique)





23. Focus sur quelques menaces

23.2. Le skimming

Focus sur quelques menaces

Le skimming

Provenant de la criminalité est-européenne, le **skimming** commence à apparaître, sous forme de groupes organisés issus des banlieues françaises.

Faux lecteur de cartes bancaires



Focus sur quelques menaces

Le skimming

Faux lecteur de cartes bancaires



SSI

Michel Dubois - 2017

233/404

Focus sur quelques menaces

Le skimming

Faux clavier



SSI

Michel Dubois - 2017

234/404

Focus sur quelques menaces

Le skimming

Caméra video

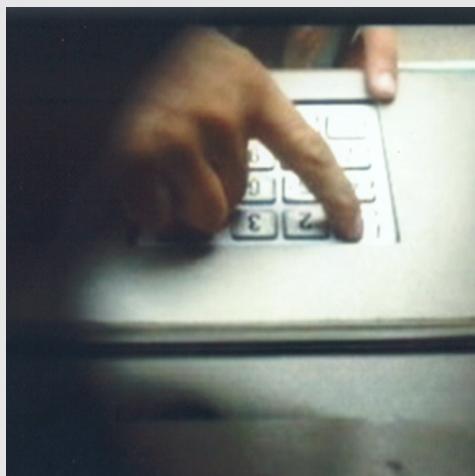


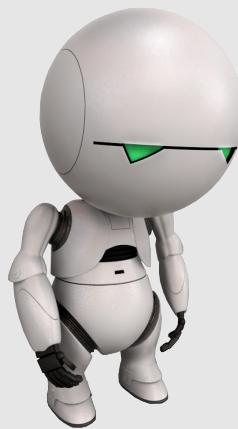
Focus sur quelques menaces

Le skimming

Comment se protéger?

- être vigilant
- saisir son code à l'abris des regards





23. Focus sur quelques menaces

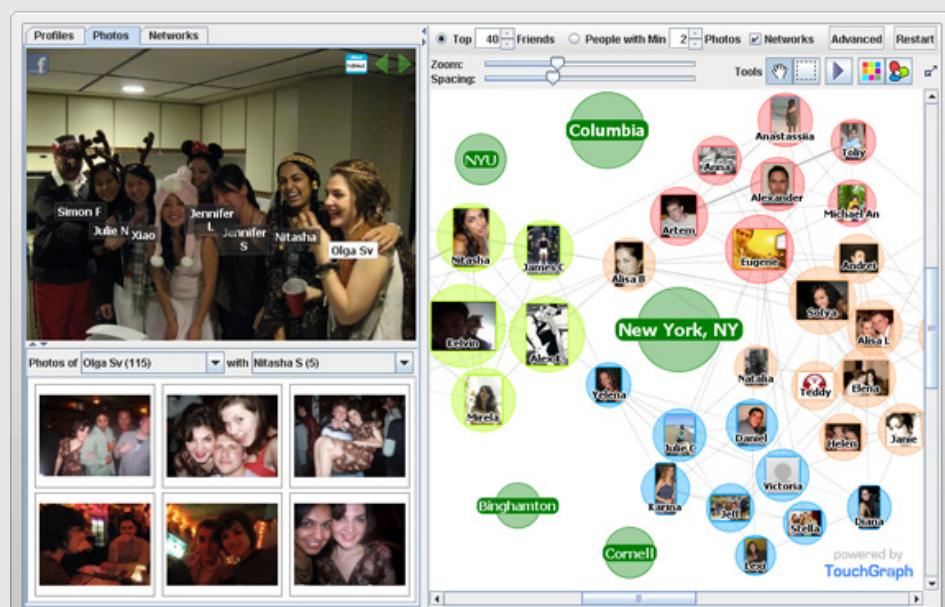
23.3. L'atteinte à la vie privée

Focus sur quelques menaces

L'atteinte à la vie privée

"Data is the pollution of the information age"
"Les données sont la pollution de l'ère de l'information."

Bruce Schneier



Focus sur quelques menaces

L'atteinte à la vie privée

- Les données sont un **sous-produit naturel** de toutes interactions avec les ordinateurs
- Une fois produites et diffusées, elles restent **éternellement disponibles**
- Les conséquences de leurs réutilisations peuvent être **désastreuses**



Focus sur quelques menaces

L'atteinte à la vie privée

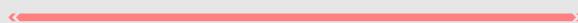
Quelques exemples

Achats divers - Avant

- réalisés en **boutique**
- paiement en liquide

Achats divers - Aujourd'hui

- e-commerce
- e-marketing



Vie sociale - Avant

- conversations **face à face**
- dîners entre amis (cercle privé)

Vie sociale - Aujourd'hui

- Chat, VoIP, visioconférence
- réseaux sociaux (privée => publique)

Focus sur quelques menaces

L'atteinte à la vie privée

Facteurs favorisant l'utilisation de données privées

- **Explosion** de l'Internet
- Augmentation des **capacités de stockage** et baisse de leurs coût
- Augmentation des capacités de **traitement**, de **correlation** et de **tri** des informations
- Limitations de l'utilisation des informations dépendante des **lois locales**

"L'information autrefois éphémère est aujourd'hui permanente"



Focus sur quelques menaces

L'atteinte à la vie privée

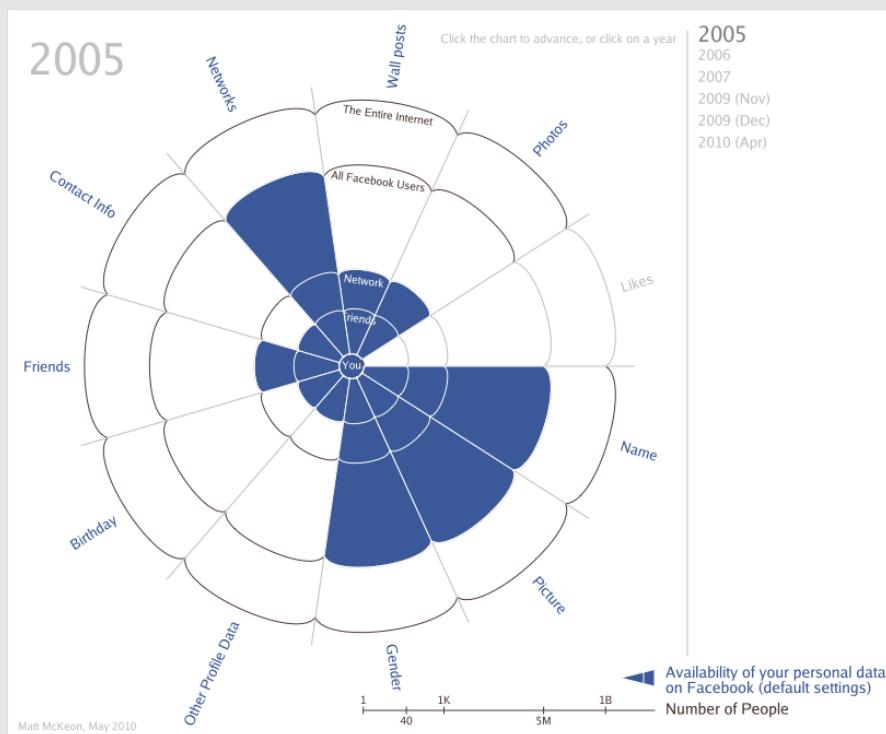
Matières à reflexion : **Conditions d'utilisation de Facebook**

« En publiant un Contenu utilisateur sur tout ou partie du Site, **vous concédez expressément à la Société**, et vous garantissez détenir les droits nécessaires à cet effet, **une licence irrévocable**, perpétuelle, non exclusive, transférable et pour le monde entier sans rétribution financière de sa part, **d'utiliser, copier, représenter, diffuser, reformater, traduire**, extraire (en tout ou partie) et distribuer ce Contenu utilisateur, à des fins commerciales, publicitaires ou autres, sur le Site ou en relation avec le Site (ou dans le cadre de sa promotion), de créer des œuvres dérivées du Contenu utilisateur ou de l'incorporer à d'autres créations, et d'en concéder des sous-licences des éléments cités. »

Focus sur quelques menaces

L'atteinte à la vie privée

Évolution de la notion de vie privée sur FaceBook



Source : <http://www.mattmckeon.com/facebook-privacy/>

SSI

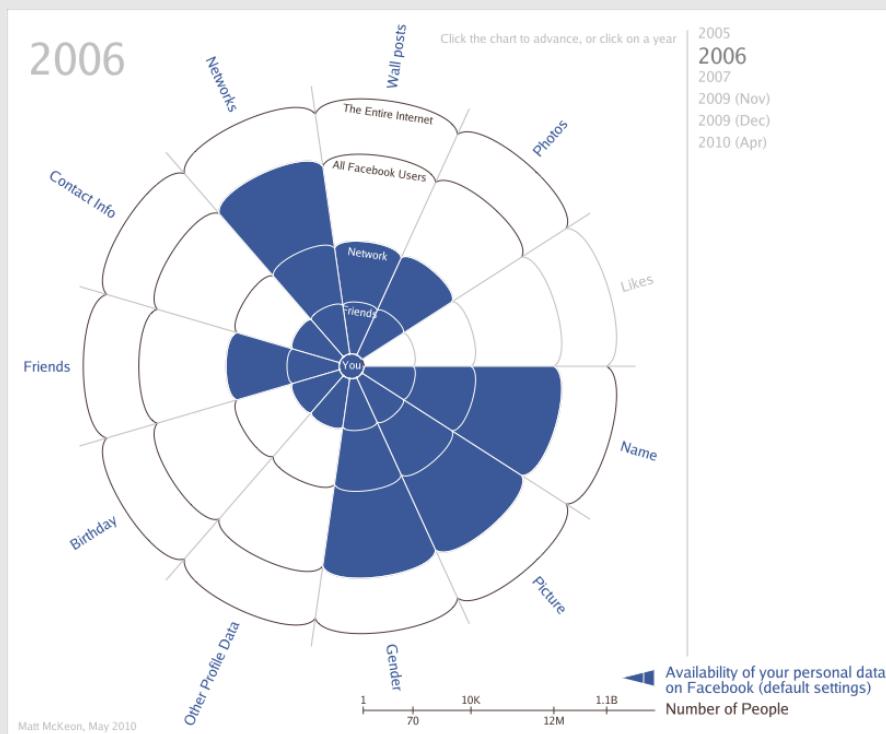
Michel Dubois - 2017

243/404

Focus sur quelques menaces

L'atteinte à la vie privée

Évolution de la notion de vie privée sur FaceBook



Source : <http://www.mattmckeon.com/facebook-privacy/>

SSI

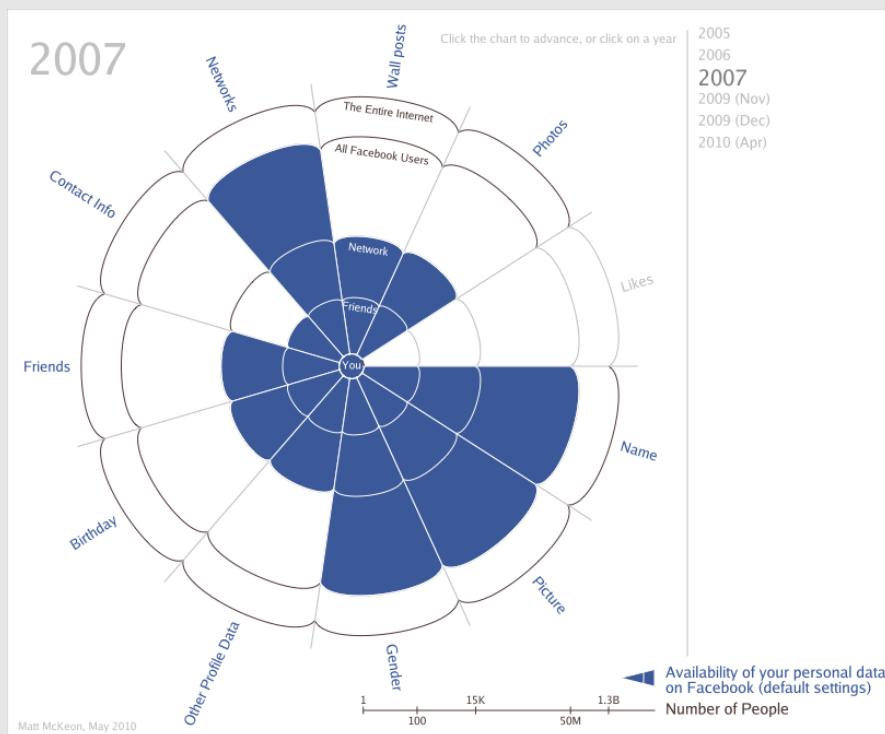
Michel Dubois - 2017

244/404

Focus sur quelques menaces

L'atteinte à la vie privée

Évolution de la notion de vie privée sur FaceBook



Source : <http://www.mattmckeon.com/facebook-privacy/>

SSI

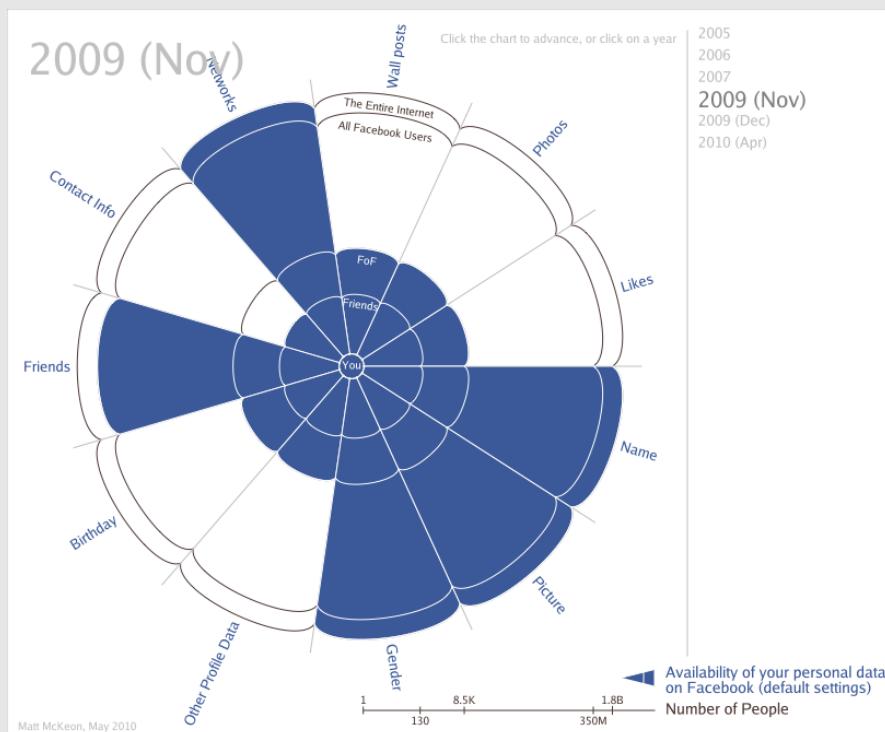
Michel Dubois - 2017

245/404

Focus sur quelques menaces

L'atteinte à la vie privée

Évolution de la notion de vie privée sur FaceBook



Source : <http://www.mattmckeon.com/facebook-privacy/>

SSI

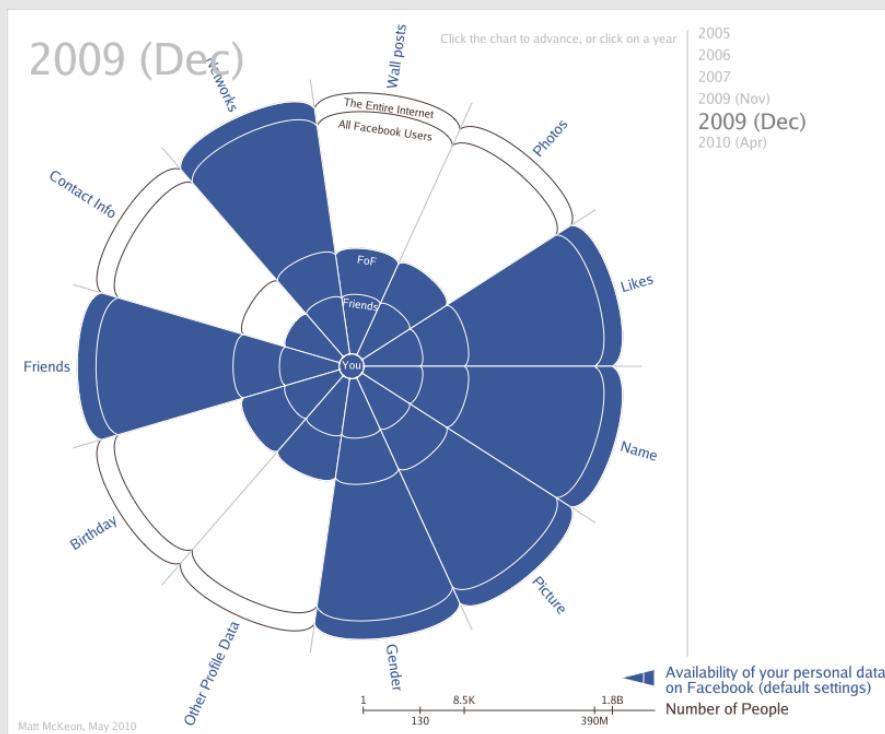
Michel Dubois - 2017

246/404

Focus sur quelques menaces

L'atteinte à la vie privée

Évolution de la notion de vie privée sur FaceBook



Source : <http://www.mattmckeon.com/facebook-privacy/>

SSI

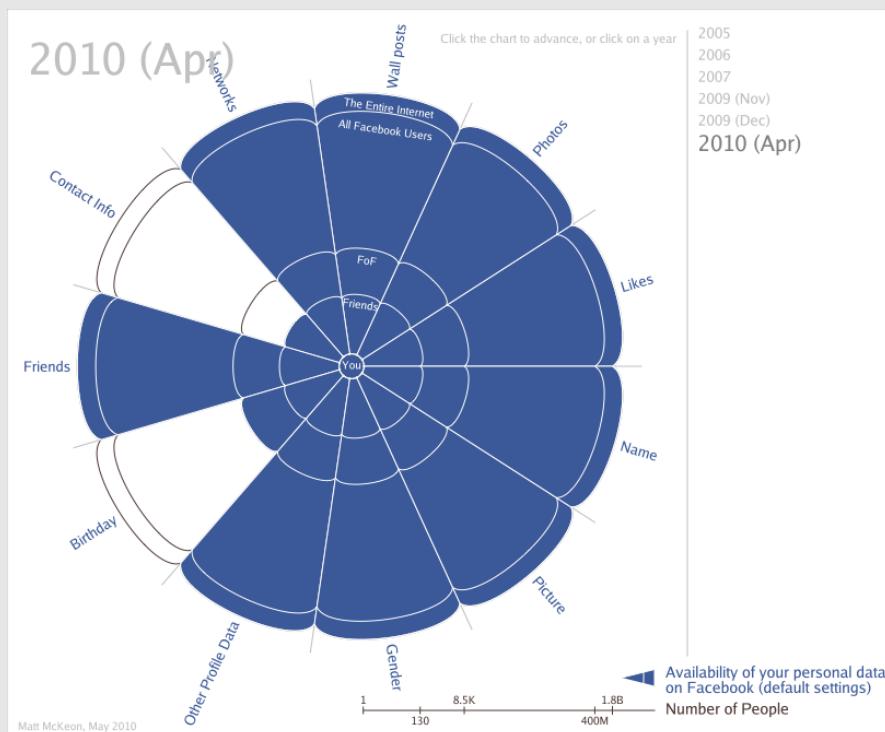
Michel Dubois - 2017

247/404

Focus sur quelques menaces

L'atteinte à la vie privée

Évolution de la notion de vie privée sur FaceBook



Source : <http://www.mattmckeon.com/facebook-privacy/>

SSI

Michel Dubois - 2017

248/404

Focus sur quelques menaces

L'atteinte à la vie privée

La carte mondiale des amis sur FaceBook



Source : <http://www.facebook.com/notes/facebook-engineering/visualizing-friendships/469716398919>

SSI

Michel Dubois - 2017

249/404

Focus sur quelques menaces

L'atteinte à la vie privée

Matières à réflexion : Google Latitude

Présentation de Google Latitude

The screenshot shows a map of the Paris area with several blue icons containing small profile pictures of users. Labels for various neighborhoods like Deuil-la-Barre, Garges-lès-Gonesse, Stains, Dugny, Aulnay-sous-Bois, La Courneuve, Aubervilliers, Bobigny, Pantin, Noisy-le-Sec, Rosny-sous-Bois, Bagnolet, and Montreuil are visible. The map is overlaid with a grid of road numbers (N14, N328, N214, N1, N301, N315, A86, A1, A3, E15) and letters (N1, N2, N3). At the bottom, there's a section titled 'Confidentialité de votre' with icons for mobile devices.

Localisation de vos amis sur une carte

Utilisez Google Latitude sur votre téléphone portable

Localisez vos amis, consultez leur message personnel et publiez le vôtre.

Entrez votre numéro de téléphone ou rendez-vous sur google.com/latitude depuis le navigateur de votre téléphone portable.

M'envoyer un lien par SMS

France

Google Latitude fonctionnera-t-il sur mon téléphone ?

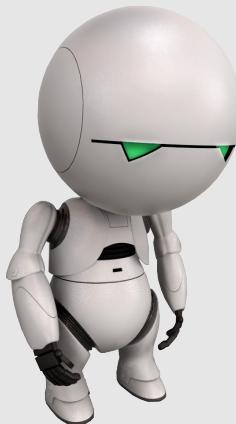
Google Latitude est une fonctionnalité de Google Maps pour mobile qui peut être utilisée sur les téléphones portables suivants :

- Appareils Android, comme le T-Mobile G1 (bientôt disponible)
- Appareils iPhone et iPod touch (bientôt disponible)

SSI

Michel Dubois - 2017

250/404



23. Focus sur quelques menaces

23.4. Le social engineering

Focus sur quelques menaces

Le social engineering

Social engineering

L'ingénierie sociale est l'ensemble des techniques de **manipulation psychologique** ou **comportementale** d'un individu ou d'un groupe d'individus dont le but est l'**incitation inconsciente** à amoindrir, contourner ou supprimer les mesures de sécurité d'un système.

Social engineering

L'ingénierie sociale est la discipline consistant à obtenir une information en exploitant la **confiance**, l'**ignorance** ou la **crédulité** de tierces personnes. Il s'agit d'**exploiter le facteur humain**, maillon faible de tout **système de sécurité**.

Focus sur quelques menaces

Le social engineering

"Le véritable maillon faible de la sécurité, c'est le **facteur humain.**"

Kevin Mitnick



SSI

Michel Dubois - 2017

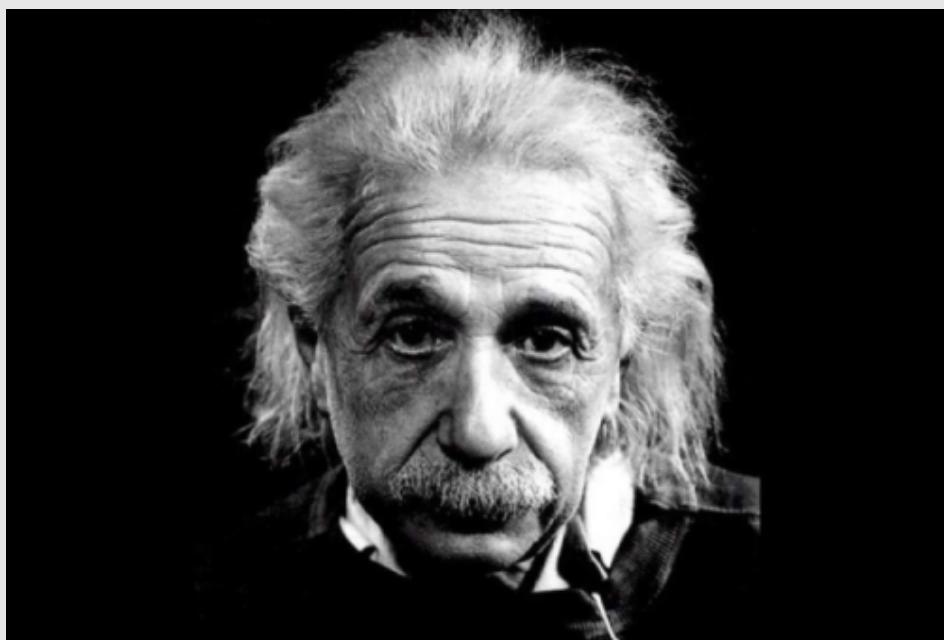
253/404

Focus sur quelques menaces

Le social engineering

"Only two things are infinite, the universe and human stupidity, and I'm not sure about the former."

Albert Einstein



SSI

Michel Dubois - 2017

254/404

Focus sur quelques menaces

Le social engineering



SSI

Michel Dubois - 2017

255/404

Focus sur quelques menaces

Le social engineering



SSI

Michel Dubois - 2017

256/404

Focus sur quelques menaces

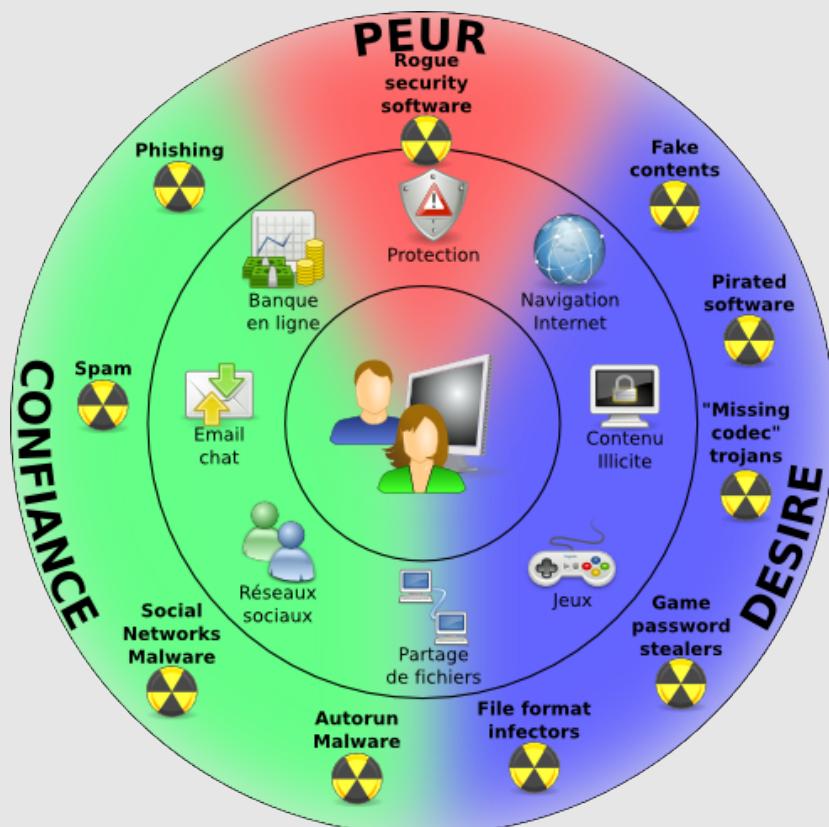
Le social engineering

Les moyens utilisés :

- **Usurpation d'identité** : le pirate se fait passer auprès de l'utilisateur cible pour une personne connue
- **Manipulation psychologique** : le pirate exploite diverses faiblesses psychologiques de la victime (ego, appât du gain, sexe, curiosité, manque de bon sens, manque de prudence, rancœur vis-à-vis de la hiérarchie...)
- **Exploitation du manque de connaissances** : le pirate exploite la méconnaissance technique de l'utilisateur.

Focus sur quelques menaces

Le social engineering



Focus sur quelques menaces

Le social engineering

La pyramide des besoins de Maslow



La pyramide des besoins est une théorie en psychologie proposée par Abraham Maslow dans son article **une théorie de la motivation humaine** paru en 1943 dans **Psychological Review**

Focus sur quelques menaces

Le social engineering

La pyramide des besoins de Maslow

- La pyramide des besoins schématise la théorie de Maslow sur **la motivation**
- La pyramide est constituée de **cinq** niveaux principaux
- Nous recherchons d'abord à satisfaire chaque besoin d'un niveau donné avant de penser aux besoins situés au niveau immédiatement supérieur de la pyramide



Accomplissement de soi
(méditer, approfondir sa culture, développement personnel)

Estime
(développer son autonomie, parler, sortir du lot, avoir de l'indépendance)

Appartenance et amour
(statut social, s'intégrer à un groupe, pouvoir s'exprimer, partager)

Sécurité
(accumuler, stabilité, construire sa maison, s'occuper de sa santé)

Physiologiques
(manger, boire, respirer, dormir, se reproduire)

Focus sur quelques menaces

Le social engineering



Accomplissement de soi

(méditer, approfondir sa culture, développement personnel)

Estime

(développer son autonomie, parler, sortir du lot, avoir de l'indépendance)

Appartenance et amour

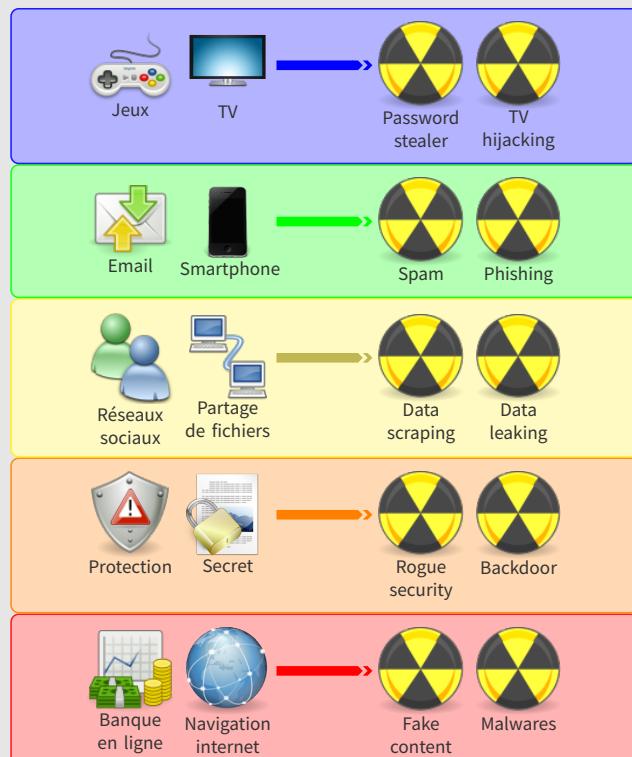
(statut social, s'intégrer à un groupe, pouvoir s'exprimer, partager)

Sécurité

(accumuler, stabilité, construire sa maison, s'occuper de sa santé)

Physiologiques

(manger, boire, respirer, dormir, se reproduire)



Focus sur quelques menaces

Le social engineering

Exemples de rogue security software

MS Antivirus
Online Security Scanner

Scanning System Security

WARNING!
System security is low, system may be infected with Trojan virus or attacked by hackers. Your computer is in danger.

Checking file: ddeml.dll
Security errors: 27

Recommendation: Click "Protect Now" to increase system security level.
Protect now

Scanning For Viruses

Checking file: ddeml.dll
Infected files: 29 Suspicious files: 2

Recommendation: Click "Protect now" to download security tool to upgrade your computer.
Protect now

Virus Heat

Scanning

Item	Vendor	Type	Location	Threat Level
Headline T...	Registry	[HKEY_CLASSES_ROOT\CLSID\00...	High	
Headline T...	Registry	[HKEY_CLASSES_ROOT\CLSID\12...	High	
Headline T...	Registry	[HKEY_CLASSES_ROOT\CLSID\1D...	High	
Headline T...	Registry	[HKEY_CLASSES_ROOT\CLSID\20...	High	
SPY/Hint S...	Registry	[HKEY_CLASSES_ROOT\CLSID\28...	Highest	
SPY/Hint S...	Registry	[HKEY_CLASSES_ROOT\CLSID\32...	Highest	
HelpExpress	Registry	[HKEY_CLASSES_ROOT\CLSID\33...	High	
HelpExpress	Registry	[HKEY_CLASSES_ROOT\CLSID\34...	High	
Acero de E...	Registry	[HKEY_CLASSES_ROOT\CLSID\45...	High	
HD-Crypt T...	Registry	[HKEY_CLASSES_ROOT\CLSID\45...	Highest	

Abort Scanning registry... Pause

Focus sur quelques menaces

Le social engineering

L'objectif : être **crédible** afin d'obtenir la **confiance** !

- Il faut garder en permanence à l'esprit que **plus un attaquant dispose d'informations sur un organisme**, plus la prise de contrôle du système d'information lui sera aisée.

Les conséquences

- **récupération d'informations diverses** : organigramme numéro de téléphone, nom de responsables informatiques, plan d'adressage réseau, prestataires extérieures (télémaintenance), nom de stagiaires, mots de passe et login
- **par des moyens très simples** : analyse de rebus (documents trouvés dans les poubelles), bavardages (dans le train, au téléphone, en réception, en colloque, chez soi...), visite de locaux (sociétés extérieurs, visite aux malades...).

Focus sur quelques menaces

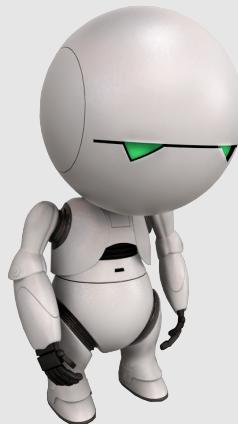
Le social engineering

Comment se protéger? - **Les questions à se poser**

- Qu'est-ce qui me prouve que mon interlocuteur **est bien celui qu'il prétend être**?
- Qu'est-ce qui me prouve que mon interlocuteur **est habilité à obtenir ces informations**?

Comment se protéger? - **Les règles d'or**

- ne **jamais communiquer** son login et son mot de passe
- ne **jamais ouvrir** la pièce jointe d'un email non sollicité
- vérifier **l'origine des demandes** et surtout rendre compte aux échelons supérieurs
- respect rigoureux des procédures vis-à-vis des **stagiaires et des sociétés extérieurs**
- sensibiliser et former les personnels.



23. Focus sur quelques menaces

23.5. L'escroquerie au président

SSI

Michel Dubois - 2017

265/404

Focus sur quelques menaces

L'escroquerie au président

'oute l'actualité, 19 Janvier 2016, mis à jour à 17h21

VILLE OU CODE POSTAL OK

Le Parisien

MON COMPTE Inscrivez-vous

Offre Premium : 1er mois offert !

À SUIVRE Question du jour Avalanche en Savoie Leila Alaoui Glenn Frey PSG-TFC

f t g+ p m e

À LA UNE SOCIÉTÉ FAITS DIVERS POLITIQUE ÉCONOMIE AUTO INTERNATIONAL PEOPLE INSOLITE HIGH-TECH SCIENCES MA TERRE

ACTUALITÉS | À LA UNE

Partager 2 Tweeter 4

Michelin victime d'une escroquerie d'un montant de 1,6 M EUR

Le Parisien | 03 Nov. 2014, 21h15

A A Le fabricant de pneumatiques Michelin s'est fait dérober 1,6 million d'euros via une escroquerie reposant sur de faux ordres de virement, a-t-il indiqué lundi à l'AFP, confirmant une information du site internet du Parisien.

Selon la version électronique du quotidien, le groupe a été sollicité par une personne se présentant comme le directeur financier d'un ses fournisseurs. Celle-ci a alors demandé à ce que les règlements destinés à sa société soient effectués sur le compte d'une banque en République tchèque. "Cet homme connaissait parfaitement la procédure à suivre et la personne à contacter au sein du groupe Michelin pour pouvoir effectuer cette modification en toute

LOCAUX PROFESSIONNELS

VERSAILLES (78000) - 175m²

Trouvez vos locaux avec BureauxLocaux.com

Le Parisien Économie

Chaque semaine LE PARISIEN ÉCO Les secteurs et métiers qui recrutent en 2016

SSI

Michel Dubois - 2017

266/404

Focus sur quelques menaces

L'escroquerie au président

Escroquerie au président ou escroquerie aux faux ordres de virement

Mode opératoire

1. le fraudeur contacte le service comptable de la société cible en se faisant passer pour le Président de la société ou pour un cabinet d'avocat agissant en son nom
2. du crédit est apporté à ce scénario par l'intervention, peu de temps après, de personnes se faisant passer pour des prestataires de confiance (avocats, notaires, commissaires aux comptes, experts comptables...)
3. le contact peut se faire par mail en imitant techniquement l'adresse du dirigeant ou par téléphone, via le standard
4. après quelques échanges de mise en confiance avec son correspondant, le fraudeur va demander que soit réalisé en urgence un virement à destination d'un pays étranger
5. pour justifier l'urgence, il est invoqué une opération d'acquisition très confidentielle. Le fraudeur indique à son interlocuteur qu'il a été choisi pour sa conscience professionnelle et sa discrétion
6. face au pouvoir de persuasion de son interlocuteur, le comptable sollicité va s'exécuter après avoir reçu les références bancaires du compte à créditer

Focus sur quelques menaces

L'escroquerie au président

Escroquerie au président - mode opératoire

De : [REDACTED]@[REDACTED].com <[REDACTED]@presidency.com>
Date : jeudi 11 décembre 2014 13:59
À : [REDACTED]@[REDACTED].com
Objet : Confidential
Très bien

J'ai le plaisir de vous annoncer que le traitement d'une opération financière confidentielle sera traité par vos soins.

Pouvez-vous me la traiter en priorité cet après-midi ?

Cordialement,

[REDACTED]

Focus sur quelques menaces

L'escroquerie au président

Escroquerie au président - mode opératoire

De : [REDACTED]is.com" <[REDACTED]@presidency.com>
Date : jeudi 11 décembre 2014 15:56
À : [REDACTED]is.com>
Joindre : facture aquisition[REDACTED].pdf
Objet : Facture
Catherine,

Je vous ai choisi pour votre discréction et votre travail irréprochable au sein de l'établissement pour le traitement de cette OPA.
Merci de prendre contact de suite avec notre cabinet juridique (kpmg@financier.com) l'attention de Maître Armand DUVAL pour la remise des coordonnées bancaires afin d'executer le virement dans l'immédiat.

Merci de votre efficacité,

[REDACTED]

SSI

Michel Dubois - 2017

269/404

Focus sur quelques menaces

L'escroquerie au président

Escroquerie au président - mode opératoire

De : "y.perret@weser.fr" <y.perret@presidency.com>
Date : jeudi 11 décembre 2014 16:48
À : [REDACTED]is.com>
Joindre : Coordonnées bancaire.pdf
Objet : coordonnées bancaires
Bonjour,

Ci-joint, vous trouverez les coordonnées bancaires pour l'opération en cours.

Merci de nous faire parvenir, dans les plus brefs délais, une preuve de traitement du paiement afin de valider la transaction auprès de la partie adverse, conformément à l'article LR548/7 mis en place par l'autorité des marchés financiers (AMF).

Dans l'attente de vous lire,

Cordialement.

Maître Armand DUVAL

Cabinet KPMG

Avocats spécialistes en droit fiscal
Avocats spécialistes en droit des sociétés

Les informations figurant dans ce message ont un caractère confidentiel et sont exclusivement adressées au destinataire mentionné ci-dessus.

Tout usage, reproduction ou divulgation de ce message est strictement interdit si vous n'êtes pas le destinataire.

Dans ce cas, veuillez m'en avertir immédiatement par retour d'e-mail et détruire ce message.

Merci.

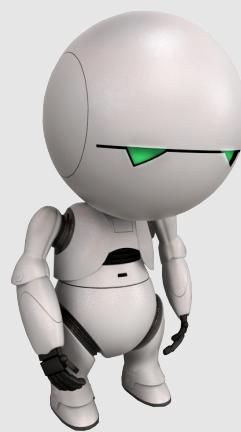
SSI

Michel Dubois - 2017

270/404

Focus sur quelques menaces

L'escroquerie au président



23. Focus sur quelques menaces

23.6. Le phishing

Focus sur quelques menaces

Le phishing

Définition

Le **phishing**, est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité.

Le terme phishing a été inventé par des pirates qui essayaient de voler des comptes AOL. Il est construit sur l'expression anglaise "password harvesting fishing", soit "pêche aux mots de passe".

The image shows an email from LCL (Le Crédit Lyonnais). The subject line is "Cher client de LE CRÉDIT LYONNAIS," followed by a message about a software update. It includes a link to <http://www.lcl.fr/banque/secure/portail/confprocedure.asp>. The footer contains the LCL logo and the text "© LE CRÉDIT LYONNAIS 2006".

Cher client de **LE CRÉDIT LYONNAIS**,

Le département technique de **LE CRÉDIT LYONNAIS** procède à une mise à jour de logiciel programmée de façon à améliorer la qualité des services bancaires.

Nous vous demandons avec bienveillance de cliquer sur le lien ci-dessous et de confirmer vos détails bancaires.

<http://www.lcl.fr/banque/secure/portail/confprocedure.asp>

Nous nous excusons pour tout désagrément et vous remercions de votre coopération.

© LE CRÉDIT LYONNAIS 2006

SSI

Michel Dubois - 2017

273/404

Focus sur quelques menaces

Le phishing

Une attaque qui se déroule en 4 étapes :

1. se faire passer pour une entreprise connue
2. présenter un **contenu fallacieux** (souvent un email) envoyant vers une page web **ressemblant** au site réel de l'entreprise (usurpation d'interface)
3. saisie des champs d'un formulaire **par la victime**
4. utiliser les informations recueillies

The image shows an email from BNP Paribas. The subject line is "Cher client de BNP PARIBAS," followed by a message about a software update. It includes a link to https://www.secure.bnpparibas.net/HomeConnexion?type=identifiant=secure_298553. The footer contains the BNP Paribas logo and the text "© BNP PARIBAS".

Cher client de **BNP PARIBAS**,

Le département technique de **BNP PARIBAS** procède à une mise à jour de logiciel programmée de façon à améliorer la qualité des services bancaires.

Nous vous demandons avec bienveillance de cliquer sur le lien ci-dessous et de confirmer vos détails bancaires.

https://www.secure.bnpparibas.net/HomeConnexion?type=identifiant=secure_298553

Nous nous excusons pour tout désagrément et vous remercions de votre coopération.

© BNP PARIBAS

SSI

Michel Dubois - 2017

274/404

Focus sur quelques menaces

Le phishing

PayPal Secure Application

PayPal®

PayPal.com Authorization, step 1 of 2
Please fill all the fields below:

Credit Card Number:	<input type="text"/>
PIN: Please provide us with your correct PIN number so that we are able to cross check your credit card with your bank account	<input type="text"/>
CVV Code: 3 digit number that appears to the right of your card number	<input type="text"/>
Expire date:	01 <input type="button" value="▼"/> 2003 <input type="button" value="▼"/>

I confirm that the above information is correct.

Next >

SSI

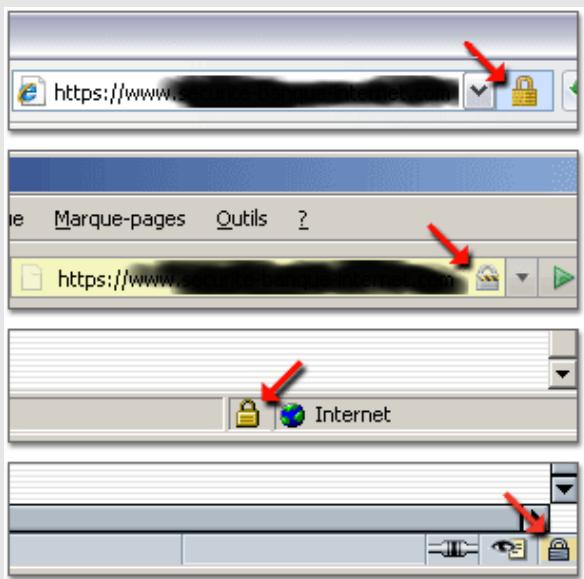
Michel Dubois - 2017

275/404

Focus sur quelques menaces

Le phishing

Comment se protéger ?



- ne **jamais** répondre à un mail expédié par un inconnu ou par un établissement bancaire
- Vérifier l'**authenticité** du certificat de sécurité (clic sur le cadenas)

SSI

Michel Dubois - 2017

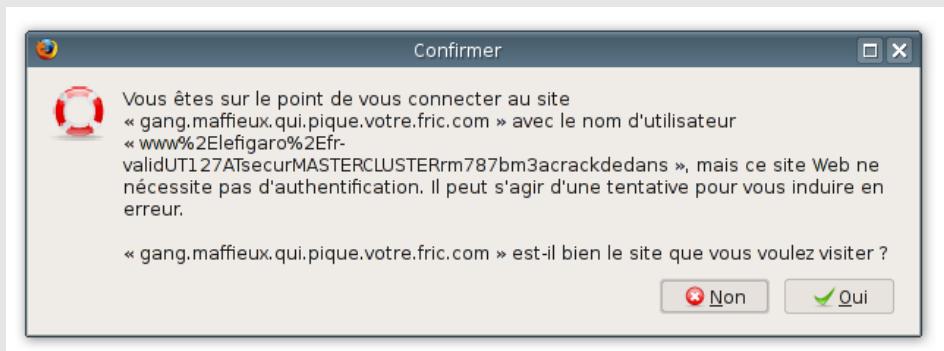
276/404

Focus sur quelques menaces

Le phishing

Comment se protéger ?

- avoir une navigateur et un lecteur d'email **à jour**
- **n'accepter les emails qu'en mode texte**
- contrôler la destination du lien avant de cliquer (démonstration)



Focus sur quelques menaces

Le phishing

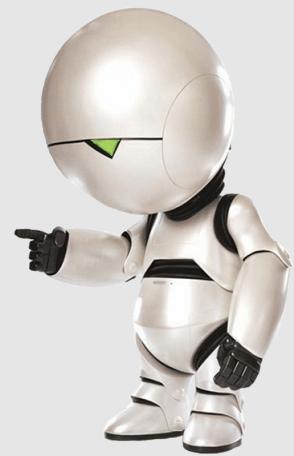
Le phishing de demain

The top screenshot shows a black background with the word "paypal" in a large white sans-serif font. Below it, in smaller white text, is "(Russian Cyrillic characters in a unicode font)" followed by "actual text is “raural”". The bottom screenshot shows a white background with the word "paypal" in a large black sans-serif font. Below it, in smaller black text, is "(Standard Latin characters in a unicode font)".

Les menaces

Section 24

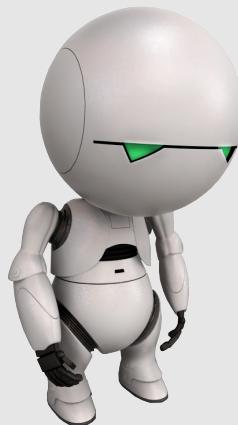
Intrusion dans le réseau



Intrusion dans le réseau

Démarche générale d'intrusion dans un réseau informatique

- **phase 1** collecte d'informations sur la cible : plan d'adressage, bases whois, emails, site Web, annuaire téléphonique, liste personnels service informatique...
- **phase 2** découverte et analyse du réseau : scan de port, os fingerprint, récupération de bannière, sniffing...
- **phase 3** énumération et versioning des éléments actifs : scan de port, base de données de vulnérabilités...
- **phase 4** intrusion et extension de privilèges : cassage de mots de passe, exploitation de failles...
- **phase 5** compromission et nettoyage des traces : installation backdoor, rootkits...



24. Intrusion dans le réseau

24.1. Phase 1 - Collecte d'informations

Intrusion dans le réseau

Phase 1 - Collecte d'informations

Reconnaissance **passive** - utilisation des bases **whois**

```
1 whois -h whois.ripe.net 86.64.145.142
2 inetnum:      86.64.145.0 - 86.64.145.255
3 netname:      N9UF-INFRA
4 descr:        Infrastructure for DSLAM IP
5 country:      FR
6 role:         SFR Legal Contact
7 address:      Campus SFR
8 address:      12 rue Jean-Philippe Rameau
9 address:      CS 80001
10 address:     93634 La-Plaine-Saint-Denis Cedex
11 address:     France
12 phone:       +33 1 70 18 52 00
13 created:     2003-10-23T09:15:54Z
14 last-modified: 2015-05-26T11:32:33Z
```

Intrusion dans le réseau

Phase 1 - Collecte d'informations

Reconnaissance **passive** - Recherche sur l'**Internet**

```
1 intitle:"Index of" finance.xls
2 intitle:"curriculum vitae" filetype:doc
3 filetype:dat "password.dat"
4 intitle:"Index of c:\Windows"
5 intitle:"index of" inurl:ftp (pub | incoming)
6 inurl:login.jsp.bak
7 allinurl:install/install.php
8 allinurl:intranet admin
9 "Microsoft-IIS/* server at" intitle:index.of
10 "Microsoft-IIS/6.0" intitle:index.of
```

Intrusion dans le réseau

Phase 1 - Collecte d'informations

Reconnaissance **passive** - Requêtes **DNS**

```
1 dig @8.8.8.8 www.perdu.com
2 ; <>> DiG 9.8.3-P1 <>> @8.8.8.8 www.perdu.com
3 ; (1 server found)
4 ; global options: +cmd
5 ; Got answer:
6 ; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55446
7 ; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
8 ; QUESTION SECTION:
9 ;www.perdu.com.           IN      A
10 ; ANSWER SECTION:
11 www.perdu.com.      7863      IN      A      208.97.177.124
12 ; Query time: 315 msec
13 ; SERVER: 8.8.8.8#53(8.8.8.8)
14 ; WHEN: Wed Jan 20 10:04:11 2016
15 ; MSG SIZE  rcvd: 47
```

Intrusion dans le réseau

Phase 1 - Collecte d'informations

Reconnaissance active

Social engineering



SSI

Michel Dubois - 2017

Dumpster diving



286/404

Intrusion dans le réseau

Phase 1 - Collecte d'informations

Reconnaissance active

Matériel d'occasion

A screenshot of the eBay.fr website showing a search results page for used computer hardware. The results include items like a 1.8" 60GB TOSHIBA DISQUE DUR MK6006GAH 4200T/M IDE IPOD, a Disque dur flash SSD OCZ 30 Go Core series V2 S-ATA II, a Disque dur interne 2.5 pour pc portable 120 go SATA, and a Disque Dur 40 GOs HITACHI 2.5 Sata.

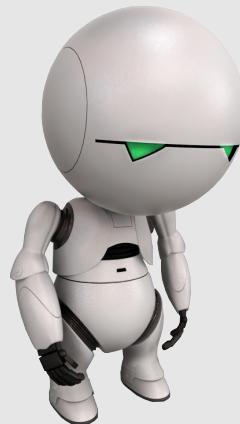
SSI

Michel Dubois - 2017

Copie de site Web

```
1 httrack "http://www.all.net/"  
2 HTTrack3.42-3+libhttplib.so.2  
3 (httrack http://www.all.net/ )
```

286/404



24. Intrusion dans le réseau

24.2. Phase 2 - Découverte et analyse du réseau

Intrusion dans le réseau

Phase 2 - Découverte et analyse du réseau

Le pirate cherche à obtenir une cartographie du réseau
scan de ports **nmap**

```
1 nmap -n -A -PN -T4 172.16.169.129
2 Starting Nmap 4.62 ( http://nmap.org )
3
4 SCRIPT ENGINE: Aborting script scan.
5 Interesting ports on 172.16.169.129:
6 Not shown: 1710 closed ports
7 PORT      STATE SERVICE
8 135/tcp   open  mstask
9 139/tcp   open  netbios-ssn
10 445/tcp  open  microsoft-ds
11 MAC Address: 00:0C:29:4C:82:7C
12
13 Network Distance: 1 hop
14 Service Info: OS: Windows
```

Intrusion dans le réseau

Phase 2 - Découverte et analyse du réseau

Le pirate cherche à obtenir une cartographie du réseau
scan de ports **hping3**

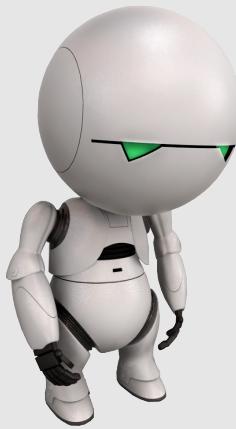
```
1 hping3 172.16.169.129 -p 445 -S
2 HPING 172.16.169.129
3 len=44 ip=172.16.169.129 ttl=128 DF id=2238 sport=445 flags=SA
4     seq=0 win=64240 rtt=2.4 ms
5 len=44 ip=172.16.169.129 ttl=128 DF id=2239 sport=445 flags=SA
6     seq=1 win=64240 rtt=0.9 ms
7 len=44 ip=172.16.169.129 ttl=128 DF id=2240 sport=445 flags=SA
8     seq=2 win=64240 rtt=0.9 ms
9 --- 172.16.169.129 hping statistic ---
10 3 packets transmitted,
11 3 packets received, 0% packet loss
12 round-trip min/avg/max = 0.8/1.2/2.4 ms
```

Intrusion dans le réseau

Phase 2 - Découverte et analyse du réseau

Le pirate cherche à obtenir une cartographie du réseau
scan de ports **netcat**

```
1 nc -v -w2 -z 172.16.169.129 133-445
2 nc: connect to 172.16.169.129 port 138 (tcp) failed
3 Connection to 172.16.169.129 139 port [netbios-ssn] succeeded!
4 nc: connect to 172.16.169.129 port 140 (tcp) failed
5 nc: connect to 172.16.169.129 port 141 (tcp) failed
6 nc: connect to 172.16.169.129 port 443 (tcp) failed
7 nc: connect to 172.16.169.129 port 444 (tcp) failed
8 Connection to 172.16.169.129 445 port [microsoft-ds] succeeded!
```



24. Intrusion dans le réseau

24.3. Phase 3 - Énumération et versioning des éléments actifs

Intrusion dans le réseau

Phase 3 - Énumération et versioning des éléments actifs

Le pirate cherche les vulnérabilités
OS fingerprinting nmap

```
1 nmap -P0 -sV -T4 172.16.169.129
2 Starting Nmap 4.62 ( http://nmap.org )
3 Interesting ports on 172.16.169.129:
4 PORT      STATE SERVICE      VERSION
5 23/tcp    open  telnet Microsoft Windows 2000 telnetd
6 135/tcp   open  mstask Microsoft mstask
7 139/tcp   open  netbios-ssn
8 445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
9 1025/tcp  open  msrpc Microsoft Windows RPC
10 MAC Address: 00:0C:29:4C:82:7C
```

Intrusion dans le réseau

Phase 3 - Énumération et versioning des éléments actifs

Le pirate cherche les vulnérabilités
OS fingerprinting **xprobe**

```
1 xprobe2 172.16.169.129
2 Xprobe2 v.0.3 Copyright (c) 2002-2005
3
4 [+] Target is 172.16.169.129
5 [+] Loading modules.
6 [+] Initializing scan engine
7 [+] Running scan engine
8 [+] Primary guess:
9 [+] Host 172.16.169.129 Running OS: "Microsoft Windows 2000 Server SP4"
10 [+] Cleaning up scan engine
11 [+] Modules deinitialized
12 [+] Execution completed.
```

Intrusion dans le réseau

Phase 3 - Énumération et versioning des éléments actifs

Le pirate cherche les vulnérabilités
Récupération de **bannières**

```
1 nc -v 127.0.0.1 110
2 Connection to 127.0.0.1 110 port [tcp/pop3] succeeded!
3 +OK Dovecot ready.
```

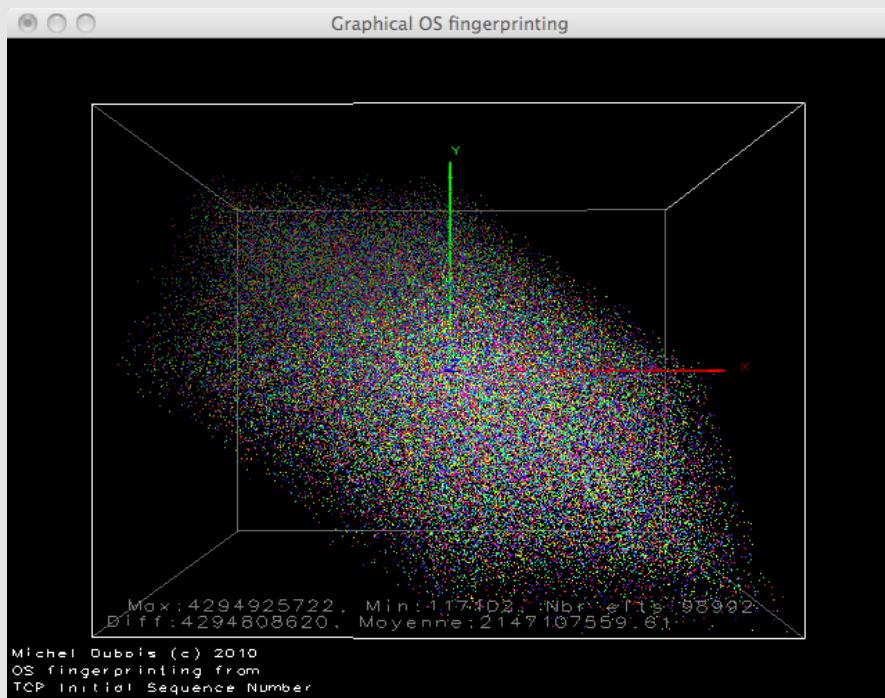
```
1 nc -v 127.0.0.1 25
2 Connection to 127.0.0.1 25 port [tcp/smtp] succeeded!
3 220 dauphin ESMTP Postfix (Debian/GNU)
```

```
1 nc -v 127.0.0.1 22
2 Connection to 127.0.0.1 22 port [tcp/ssh] succeeded!
3 SSH-2.0-OpenSSH_5.1p1 Debian-4
```

Intrusion dans le réseau

Phase 3 - Énumération et versioning des éléments actifs

Le pirate cherche les vulnérabilités
Versionning **scripts spécifiques**



SSI

Michel Dubois - 2017

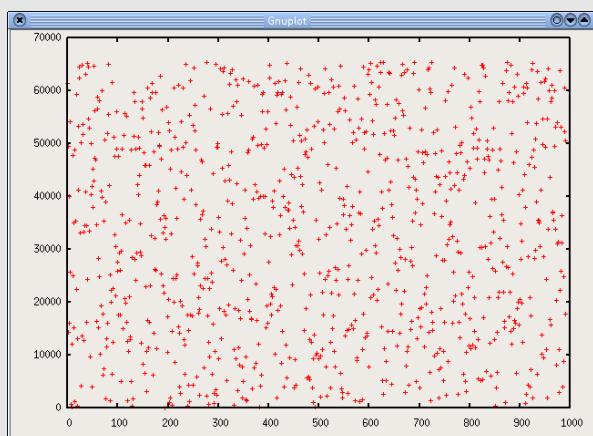
295/404

Intrusion dans le réseau

Phase 3 - Énumération et versioning des éléments actifs

Le pirate cherche les vulnérabilités

Scapy



Scanners de vulnérabilités



SSI

Michel Dubois - 2017

296/404

Intrusion dans le réseau

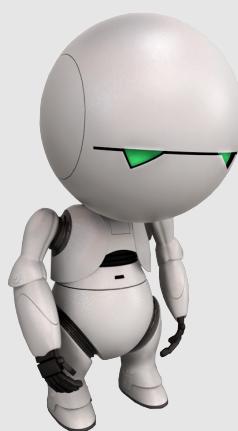
Phase 3 - Énumération et versioning des éléments actifs

Le pirate cherche les vulnérabilités

BDD vulnérabilités

601	1999-03-15	Microsoft Exchange Server LDAP Bind Function Overflow
11252	1998-12-17	Microsoft IIS Malformed GET Request DoS
1650	2000-11-16	Microsoft Exchange Server EUSR_EXSTOREEVENT Default Account
17342	2005-06-14	Microsoft ISA Server Basic Credentials Exposure
1031	1999-08-06	Microsoft Exchange Server Encapsulated SMTP Address Open Relay
4914	2002-08-09	Microsoft CMS 2001 SQL Injection Vulnerability
2299	2003-07-23	Microsoft SQL Server Named Pipe DoS
4915	2002-08-07	Microsoft CMS 2001 File Upload Vulnerability
4862	2002-08-07	Microsoft CMS 2001 Authentication Buffer Overrun
5686	2001-06-07	Microsoft Windows Telnet Service Account Information Disclosure
15215	2003-07-02	Microsoft Windows SMTP E-mail Malformed Time Stamp DoS
3903	2004-02-10	Microsoft Windows WINS Server Remote Overflow
1957	2001-09-26	Microsoft Exchange OWA Malformed Request DoS

```
nikto -h www.xxxxxxx.com
-----
  Nikto 2.02/2.0.3      - cirt.net
+ Target IP:          82.1xx.1xx.1xx
+ Target Hostname:   www.xxxxxxx.com
+ Target Port:        80
+ Start Time:        2008-12-08
+
+ Server: Apache/2.2.9 (Fedora)
- Allowed HTTP Methods:
    GET, HEAD, POST, OPTIONS
```



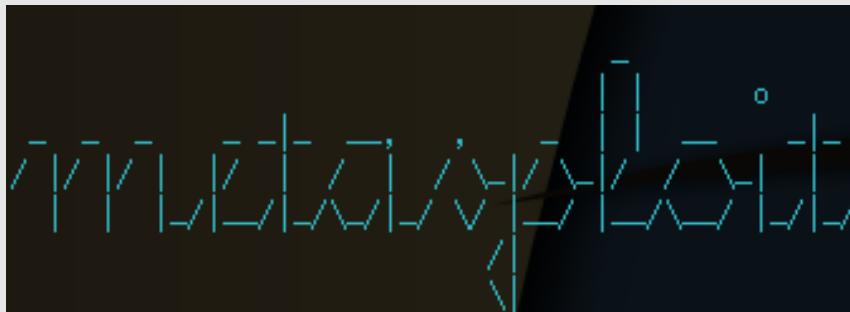
24. Intrusion dans le réseau

24.4. Phase 4 - Intrusion et extension de priviléges

Intrusion dans le réseau

Phase 4 - Intrusion et extension de privilèges

Le pirate utilise des exploits pour pénétrer dans le réseau



```
[+] =[ metasploit v3.3.4-dev [core:3.3 api:1.0]
+ -- ---[ 524 exploits - 248 auxiliary
+ -- ---[ 196 payloads - 23 encoders - 8 nops
= [ svn r8675 updated today (2010.02.26)

msf > ]
```

Intrusion dans le réseau

Phase 4 - Intrusion et extension de privilèges

Compromission et nettoyage des traces

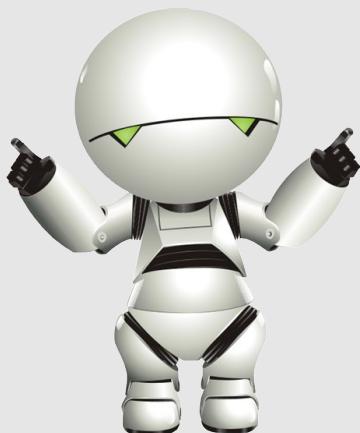
```
Win2K Rootkit by the team rootkit.com
Version 0.4 alpha
-----
command           description
ps                show proclist
help              this data
buffertest        debug output
hidedir           hide prefixed file/dir
hideproc          hide prefixed processes
debugint          <BSOD>fire int3
sniffkeys         toggle keyboard sniffer
echo <string>    echo the given string

*<BSOD> means Blue Screen of Death
if a kernel debugger is not present!
*'prefixed' means the process or filename
starts with the letters '_root_'.

"sniffkeys
sniffkeys
keyboard sniffing now ON
-----
--letmein--dir--
```

Partie 5

Les vulnérabilités

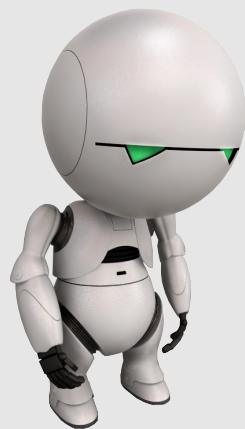


Les vulnérabilités

Section 25

Les vulnérabilités



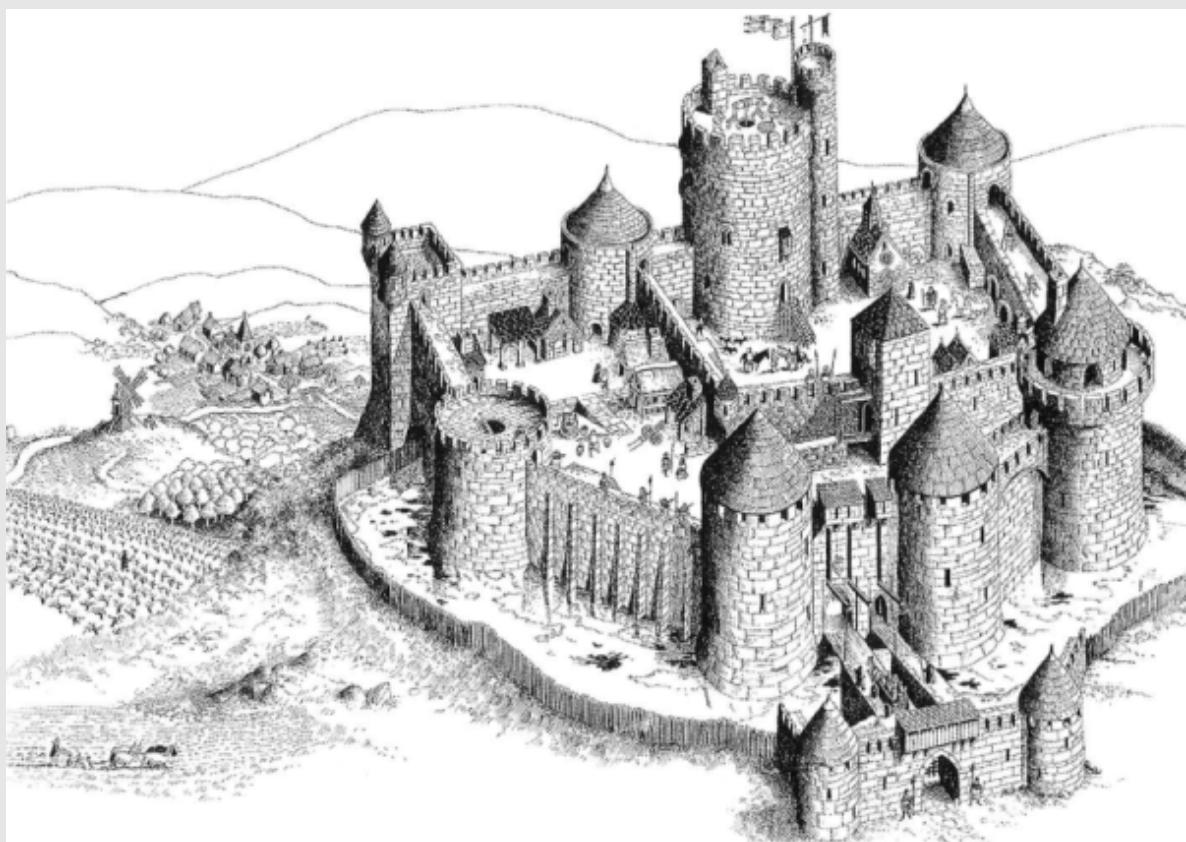


25. Les vulnérabilités

25.1. Définition

Les vulnérabilités

L'image du château fort



Les vulnérabilités

Définition

Vulnérabilité (Wikipedia)

Une vulnérabilité est une **faiblesse** dans un système d'information permettant à un attaquant de porter atteinte à l'intégrité de ce système, à sa confidentialité et à son intégrité.

Vulnérabilité (Jack A. Jones)

Une vulnérabilité est la **probabilité** qu'une ressource ou qu'une entité ne puisse pas résister aux actions d'un élément menaçant.

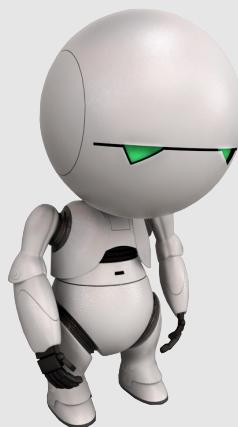


Les vulnérabilités

Définition

Une vulnérabilité est donc la **caractéristique** d'une entité qui constitue une **faiblesse** ou une **faille** au regard de la sécurité des systèmes d'information.





25. Les vulnérabilités

25.2. Classification

Les vulnérabilités

Classification

Vulnérabilité d'origine matérielle



- Absence de matériels de remplacement
- Matériel obsolète
- Absence de protection physique
- Écran observable depuis l'extérieur

Les vulnérabilités

Classification

Vulnérabilité d'origine logicielle

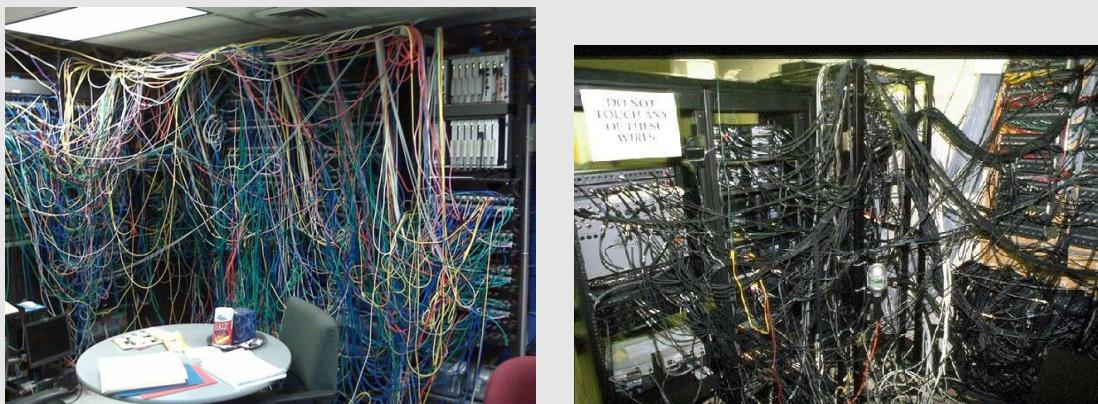


- Logiciels obsolètes ou non patchés
- Applications uniques développées en interne
- Logiciel piraté

Les vulnérabilités

Classification

Vulnérabilité liée au réseau

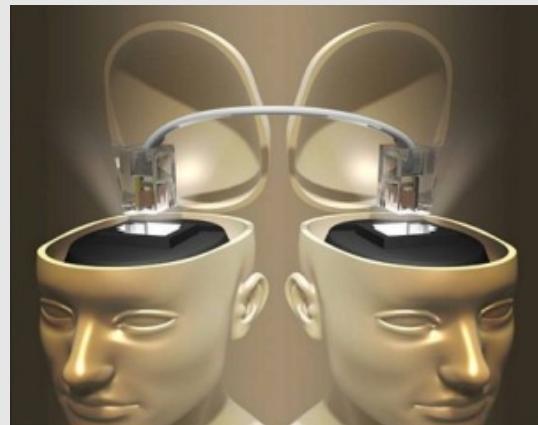


- Absence de plan de câblage
- Absence de matrice des flux
- Absence de cloisonnement réseau
- Équipements accessibles à tous

Les vulnérabilités

Classification

Vulnérabilité liée au **personnel**



- Méconnaissance des mesures de sécurité
- Non-respect du devoir de réserve
- Faible sensibilisation à la protection de l'information

Les vulnérabilités

Classification

Vulnérabilité liée au **personnel**



- Situation conflictuelle entre personnes
- Droits accordés en dehors du besoin légitime
- Personnel manipulable et crédule (Social Engineering)

Les vulnérabilités

Classification

Vulnérabilité liée au personnel

- Syndrome de l'expert unique
- Absence de procédure de transfert de connaissances ...



Les vulnérabilités

Classification

Vulnérabilité liée au site

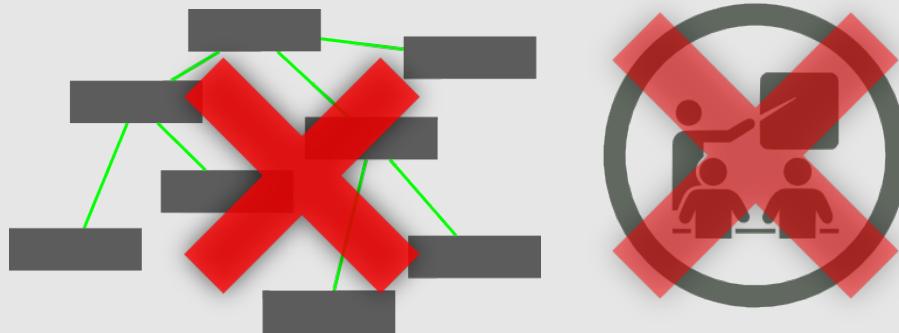


- Installation en zone inondable
- Absence de contrôle d'accès au site ou aux locaux
- Câblage posé sur le sol

Les vulnérabilités

Classification

Vulnérabilité d'origine organisationnelle

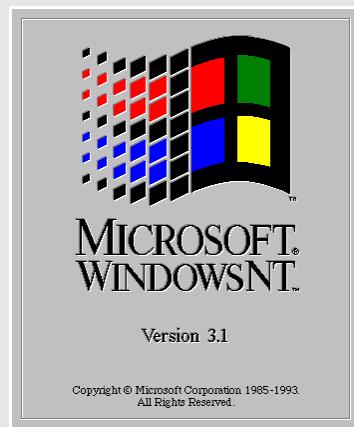
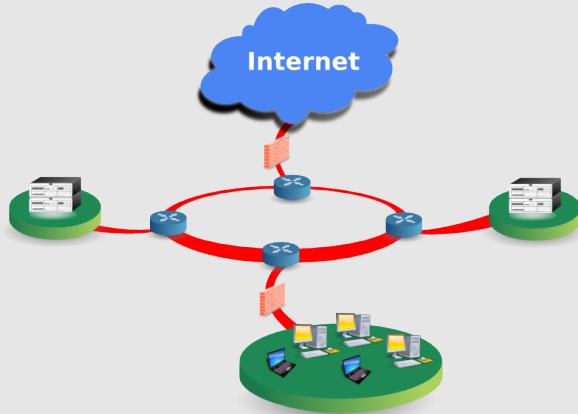


- Absence d'organisation SSI
- Absence de sensibilisation SSI
- Absence de suivi des contrats de maintenance
- Absence de plan de continuité et de reprise des activités

Les vulnérabilités

Classification

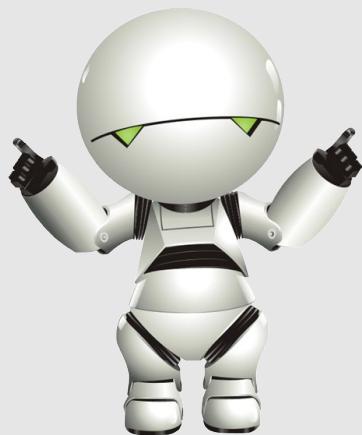
Vulnérabilité liée au système



- Erreur de configuration
- Logiciel obsolète
- Absence de procédure de sauvegarde
- Possibilité d'administrer le système à distance

Partie 6

Contres mesures



Contres mesures

Section 26

La défense en profondeur



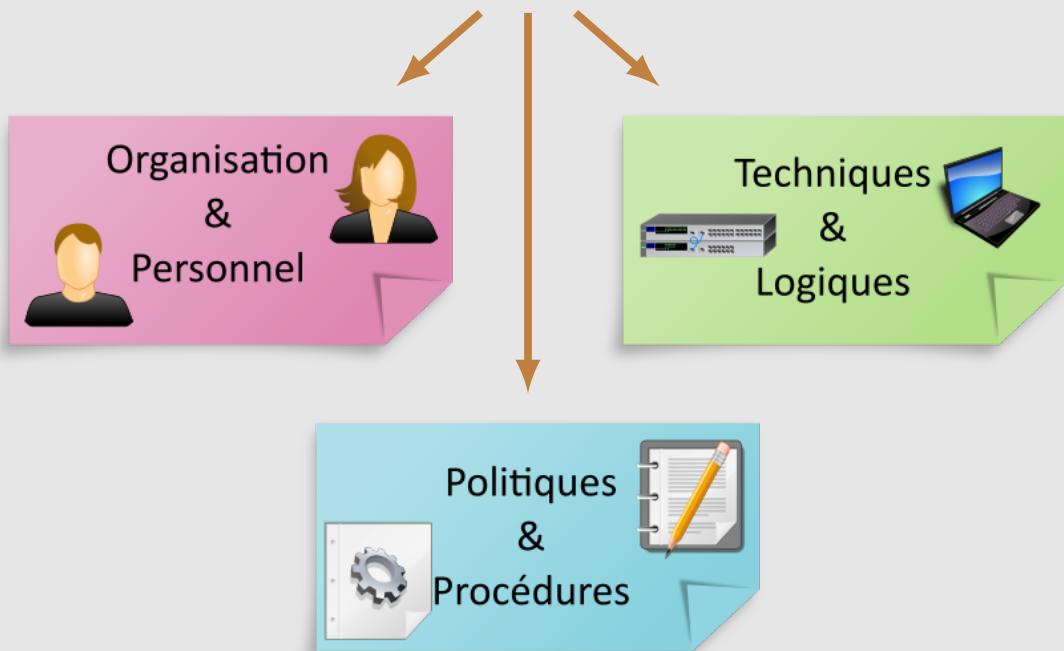
La défense en profondeur

La **défense en profondeur** est une stratégie militaire. Elle cherche à retarder l'avance d'un attaquant, tout en l'affaiblissant. Pour atteindre cet objectif, la défense en profondeur utilise **plusieurs** lignes de défense indépendantes.



La défense en profondeur

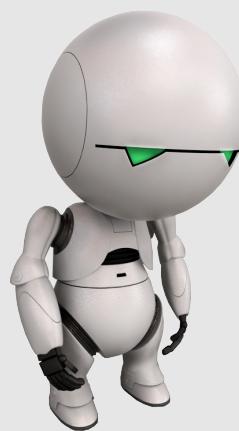
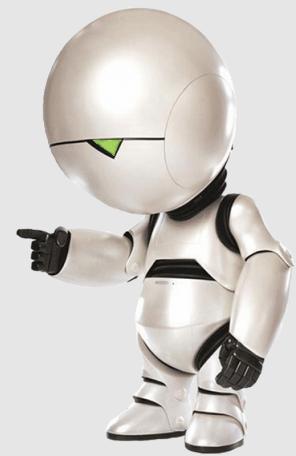
3 catégories de moyens



Contres mesures

Section 27

Les moyens organisationnels



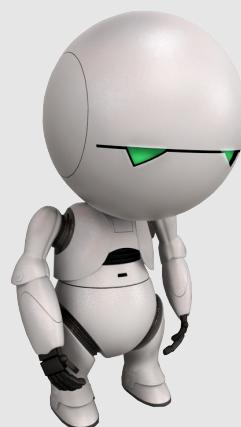
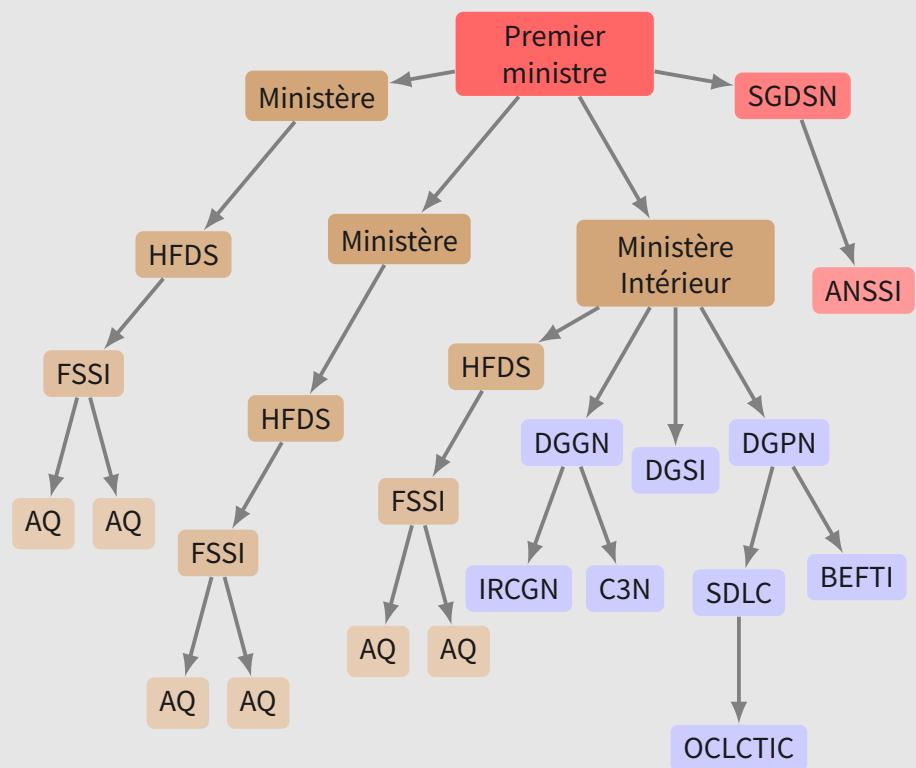
27. Les moyens organisationnels

27.1. La chaîne SSI

Les moyens organisationnels

La chaîne SSI

- HFDS Haut fonctionnaire de défense et de sécurité
- FSSI Fonctionnaire de Sécurité des systèmes d'informations
- AQ Autorité qualifiée
- DGDN Direction générale de la gendarmerie nationale
- DGPN Direction générale de la police nationale
- DGSI Direction générale de la sécurité intérieure
- SGDSN Secrétariat général de la défense et de la sécurité nationale
- ANSSI Agence nationale de la sécurité des systèmes d'information
- C3N Centre de lutte contre les criminalités numériques
- IRCGN Institut de recherche criminelle de la gendarmerie nationale
- OCLCTIC Office central de lutte contre la criminalité liée aux TIC
- BEFTI Brigade d'enquêtes sur les fraudes aux technologies de l'information



27. Les moyens organisationnels

27.2. Les agents de la SSI

Les moyens organisationnels

Les agents de la SSI

Les intervenants de la chaîne SSI

1. la direction
2. Le RSSI
3. le technicien informatique
4. l'utilisateur final

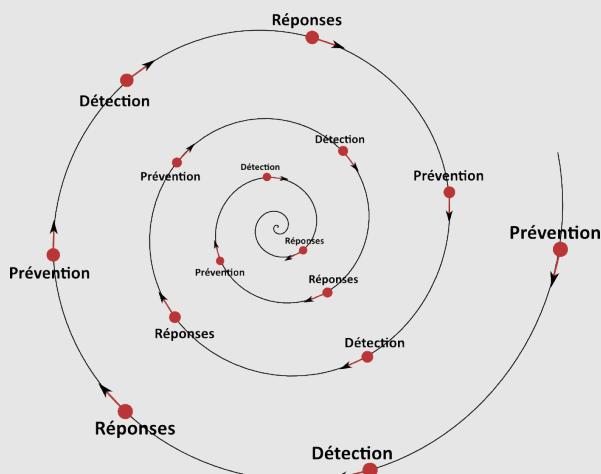


Les moyens organisationnels

Les agents de la SSI

Le rôle **fondamental** de la direction

- donne l'**impulsion** de la démarche SSI à tous les échelons de l'organisme
- **pilote** la sécurité des systèmes d'information (tableaux de bords et SMSI)



Les moyens organisationnels

Les agents de la SSI

Les fonctions du RSSI

- Responsable de la SSI
- Conseille la direction
- Définit et fait valider la PSSI
- Organise les contrôles internes
- Informe et sensibilise à la SSI
- Réalise l'homologation des SI
 - ▶ Réalise l'analyse EBIOS
 - ▶ Rédige la FEROS
 - ▶ Rédige les PES, MCS, PCI, PRI,...
- Anime la chaîne SSI
- Traite les incidents SSI



Les moyens organisationnels

Les agents de la SSI

Le rôle du technicien informatique

- **administre** les SI conformément à la PSSI
- **signale** tout incident au RSSI



Les moyens organisationnels

Les agents de la SSI

Le rôle de l'utilisateur final

- utilise les SI conformément à la PSSI
- sauvegarde ses données
- utilise un bon mot de passe et le garde secret
- signale tout incident au RSSI



Les moyens organisationnels

Les agents de la SSI

Le souci du compte-rendu



Swigert Okay, Houston, we've had a problem here.

Houston This is Houston. Say again please.

Lovell Houston, we've had a problem. We've had a main B bus undervolt.



Il n'y a pas de petit incident en SSI

Contres mesures

Section 28

Les moyens techniques et logiques



Les moyens techniques et logiques

« L'épaisseur d'un rempart compte moins que la volonté de le défendre »

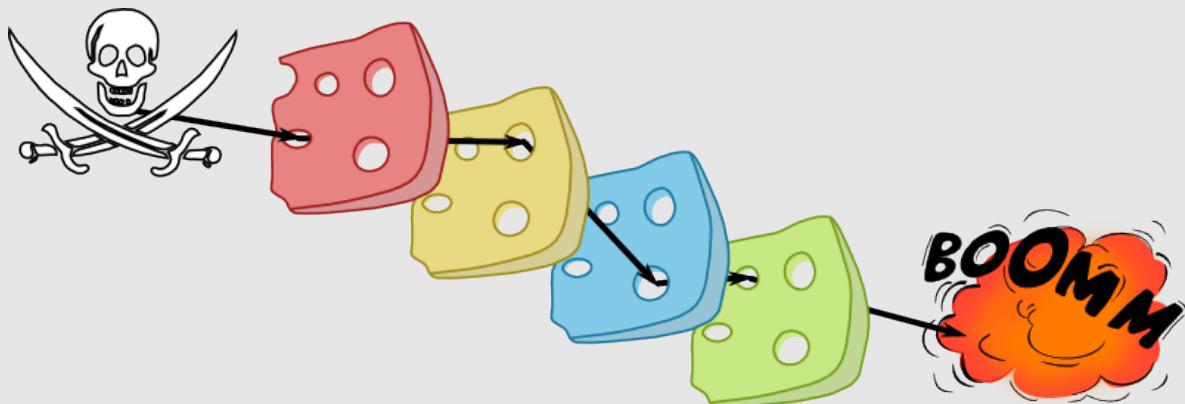
Thucydude - V^{ème} siècle avant JC



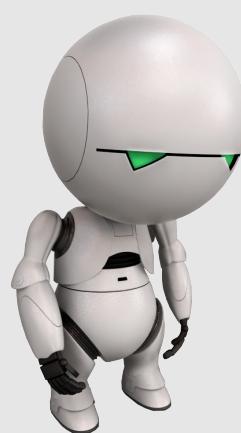
La sécurité, c'est l'affaire de **tous**!

Les moyens techniques et logiques

La théorie du gruyère suisse



Une série de **petites négligences** dans les différentes aires de protection du SI peut créer une **chaîne d'incidents** amenant à la concrétisation de l'attaque.



28. Les moyens techniques et logiques

28.1. Les mots de passe

Les moyens techniques et logiques

Les mots de passe

The screenshot shows a news article from the website "TODAY I FOUND OUT". The header features a logo with a brain and the text "TODAY I FOUND OUT" and "FEED YOUR BRAIN". Below the header is a navigation bar with links: HOME, SURPRISE, STORE, OUR BOOKI, ARTICLES, PODCAST, and QUICK FACTS. The main title of the article is "FOR NEARLY TWO DECADES THE NUCLEAR LAUNCH CODE AT ALL MINUTEMAN SILOS IN THE UNITED STATES WAS 00000000". Below the title, it says "KARL SMALLWOOD NOVEMBER 29, 2013 102". A text box contains the following content:

Today I found out that during the height of the Cold War, the US military put such an emphasis on a rapid response to an attack on American soil, that to minimize any foreseeable delay in launching a nuclear missile, for nearly two decades they intentionally set the launch codes at every silo in the US to 8 zeroes.

We guess the first thing we need to address is how this even came to be in the first place. Well, in 1962 JFK signed the *National Security Action Memorandum 160*, which was supposed to ensure that every nuclear weapon the US had be fitted with a *Permissive Action Link (PAL)*, basically a small device that ensured that the missile could only be launched with the right code and with the right authority.

On the right side of the article, there is a large photograph showing a close-up view of a nuclear missile inside its silo, looking down the tube.

Des réseaux informatique, des services & applications



nécessité d'**authentifier** et de **tracer** les entités connectées

Les moyens techniques et logiques

Les mots de passe

Identification

L'identification a pour fonction de **définir** l'identité d'une entité.

Authentification

L'authentification a pour fonction de **vérifier** de manière certaine l'identité d'une entité.

Autorisation

Ensemble des **droits accordés** à une entité après identification et authentification.

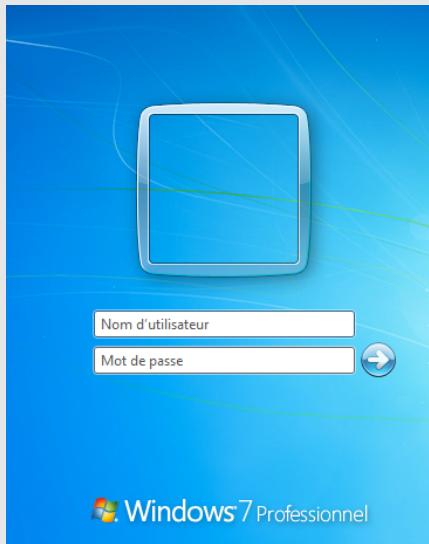
Traçabilité

Ensemble des **informations récoltées** pendant toute la durée de la session d'une entité identifiée et authentifiée.

Les moyens techniques et logiques

Les mots de passe

Les moyens d'authentification



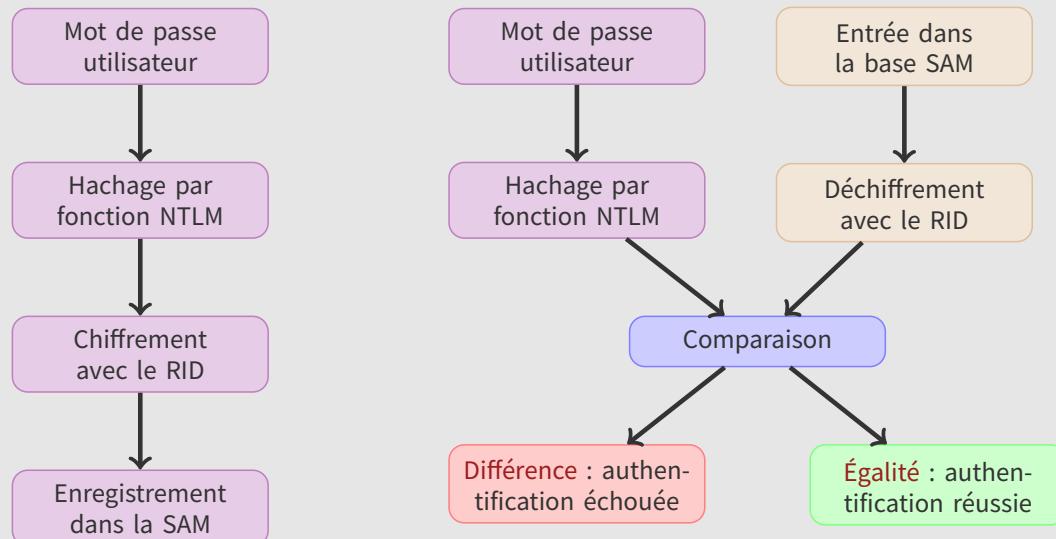
- Quelque chose que je connais
(exemple : mot de passe)
- Quelque chose que j'ai
(exemple : carte à puce)
- Quelque chose que je suis
(exemple : empreinte digitale, empreinte rétinienne)
- Quelque chose que je fais
(exemple : signature)
- L'endroit où je me trouve
(exemple : station de travail dédiée)

Pour une plus grande sécurité, il est souhaitable de combiner deux ou plusieurs techniques différentes (authentification forte). exemple : carte de crédit et code PIN

Les moyens techniques et logiques

Les mots de passe

Processus d'authentification local sous Windows



Les moyens techniques et logiques

Les mots de passe

Principe de base

La sécurité d'un système d'information est **aussi bonne** que celle des mots de passe d'authentification.



Les moyens techniques et logiques

Les mots de passe

Techniques pour casser un mot de passe

Deviner le mot de passe

Utilisation du **social engineering** (canulars téléphoniques, fouille des poubelles, recherche sur Internet...).

Se faire passer pour le système

Avec des outils de **spoofing** (Un faux logiciel de connexion imitant le vrai enregistre le mot de passe dans un fichier accessible par le pirate).

Espionner le système

Avec des outils **keylogging** ou de **sniffing** des protocoles réseaux.

Attaquer le fichier de mot de passe

Utilisation de l'attaque par **dictionnaire** ou par **force brute**.

Les moyens techniques et logiques

Les mots de passe

C'est l'empreinte, ou **hash**, du mot de passe qui est stockée dans l'ordinateur.

Le hashage est une **fonction mathématique** qui, à partir d'un texte d'origine, calcule une **empreinte unique**, de taille fixée et de manière irréversible.

- TOTO ==> 04c1d7cd203ef496f200ee5a096b5764
- ToTo ==> 3cca12013a4f82de305ba73b01a84509
- Toto ==> 998db284485ec6c227f8dc34086128e1
- toto ==> f71dbe52628a3f83a77ab494817525c6
- Le ciel est rouge demain il fera beau ==> caf7a1f03adc02afe3ef1dd51bd3e8b1

Les moyens techniques et logiques

Les mots de passe

Attaque par dictionnaire

1. pour chaque mot d'un dictionnaire
2. calcul du hash
3. comparaison avec celui du système



151349	michaella
151350	michaelmas
151351	michaelmastide
151352	michail
151353	michal
151354	michale
151355	miche
151356	micheal
151357	micheil
151358	michel
151359	michelangelesque
151360	michelangelism
151361	michelangelo
151362	michele
151363	michelia
151364	michelin
151365	michelina
151366	micheline
151367	michell
151368	michelle
151369	michelson
151370	micher

Les moyens techniques et logiques

Les mots de passe

Attaque par force brute

- parcours exhaustif de l'espace des mots de passe
- plus le mot de passe est long plus il est difficile à trouver
- plus l'espace des mots de passe est grand plus le temps nécessaire à la parcourir sera grand

	Lettres minuscules (26)	Caractères alphanumériques (62)	Caractères ASCII (256)
4 caractères	$26^4 = 460000$	$62^4 = 1,5 \cdot 10^7$	$256^4 = 4,3 \cdot 10^9$
5 caractères	$26^5 = 1,2 \cdot 10^7$	$62^5 = 9,2 \cdot 10^8$	$256^5 = 1,1 \cdot 10^{12}$
6 caractères	$26^6 = 3,1 \cdot 10^8$	$62^6 = 5,7 \cdot 10^{10}$	$256^6 = 2,8 \cdot 10^{14}$
7 caractères	$26^7 = 8,0 \cdot 10^9$	$62^7 = 3,5 \cdot 10^{12}$	$256^7 = 7,2 \cdot 10^{16}$
8 caractères	$26^8 = 2,1 \cdot 10^{11}$	$62^8 = 2,2 \cdot 10^{14}$	$256^8 = 1,8 \cdot 10^{19}$

Les moyens techniques et logiques

Les mots de passe

Caractéristiques d'un **bon** mot de passe

- est **secret**
- contient plus de **9 caractères**
- est **changé** régulièrement
- est **dédié** à une application
- caractères choisis parmi : $[A \dots Z]$, $[a \dots z]$, $[0 \dots 9]$, $[@\&$_\$+*=]$



Les moyens techniques et logiques

Les mots de passe

Construire un **bon** mot de passe

Exemple 1

- Tant va la cruche à l'eau qu'à la fin elle se casse
- Tvlcàlqlfesc

Exemple 2

- J'ai trois enfants, un chat, un oiseau et trois poissons nommés riri, fifi et loulou !
- G3e1c1o&3pnrf&l!

Les moyens techniques et logiques

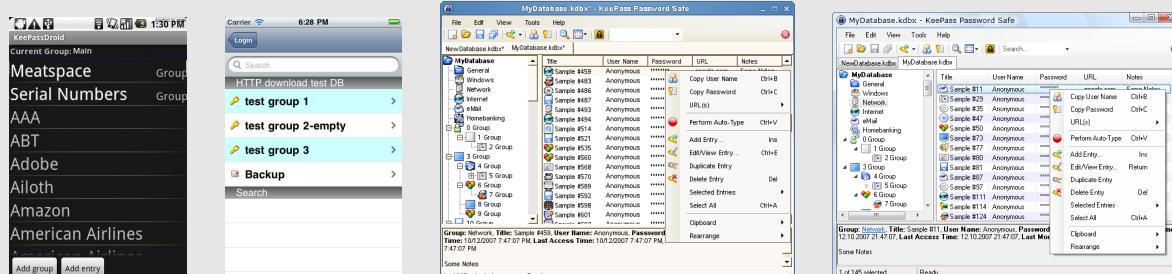
Les mots de passe

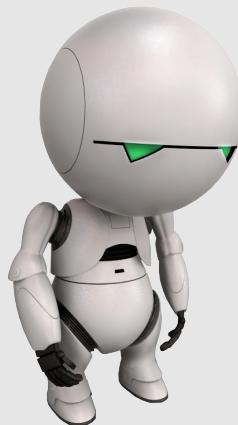
Problème

- Un mot de passe par application ou service
- beaucoup de mots de passe !

Solution

- Le gestionnaire de mot de passe
- KeePass <http://keepass.info/>





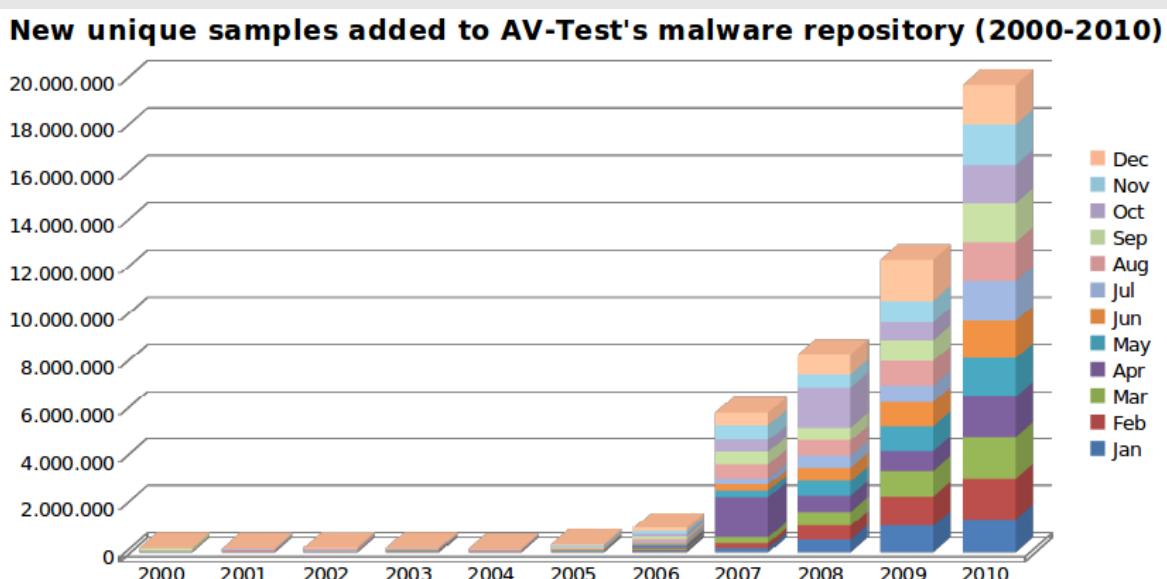
28. Les moyens techniques et logiques

28.2. La lutte antivirale

Les moyens techniques et logiques

La lutte antivirale

Malware : évolution de la menace



Les moyens techniques et logiques

La lutte antivirale



F-Secure - 2007

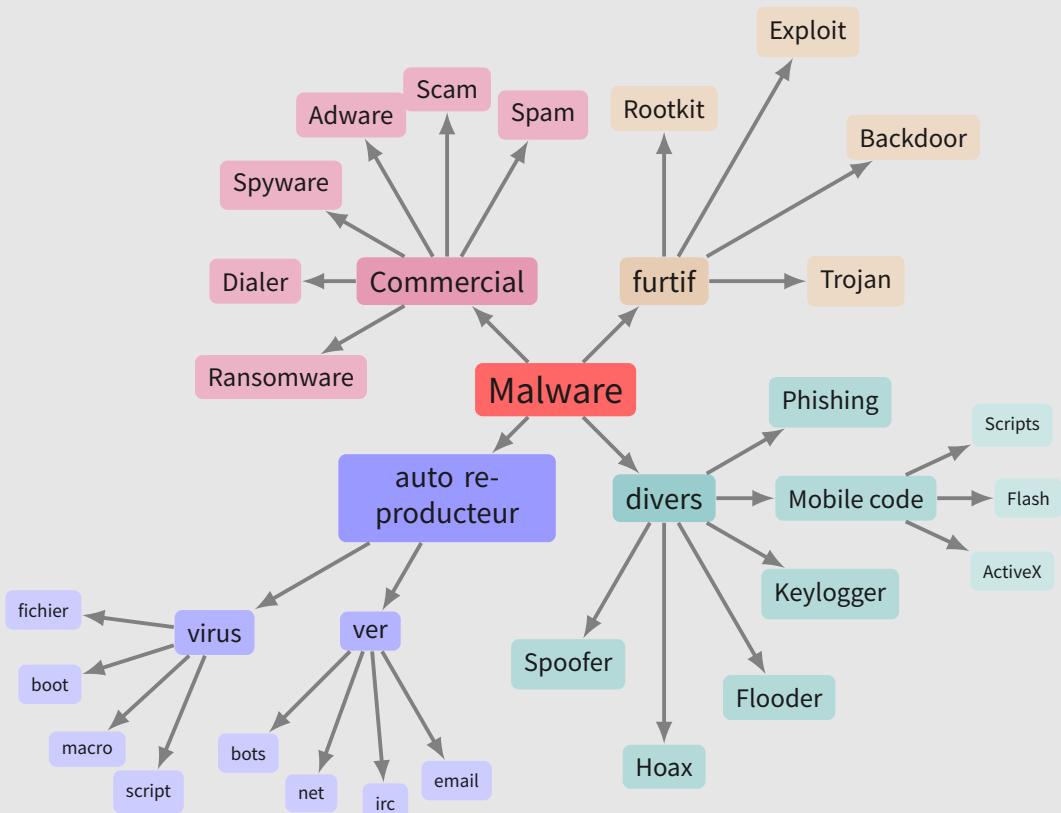
« Il y a eu plus de malwares produits en 2007 que de malwares produits durant ces 20 dernières années. »

Symantec - 2008

« Le taux de publication de codes malveillants et autres programmes indésirables est supérieur à celui des logiciels légitimes. »

Les moyens techniques et logiques

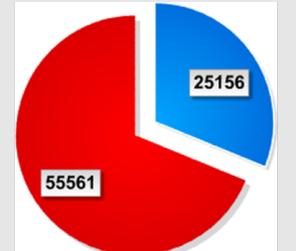
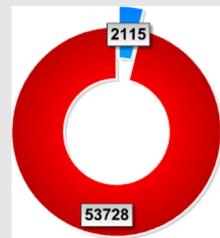
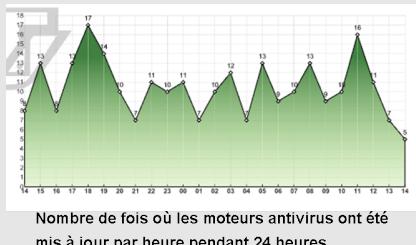
La lutte antivirale



Les moyens techniques et logiques

La lutte antivirale

Quelle **confiance** dans les moteurs antivirus ?



Source : www.virustotal.com

SSI

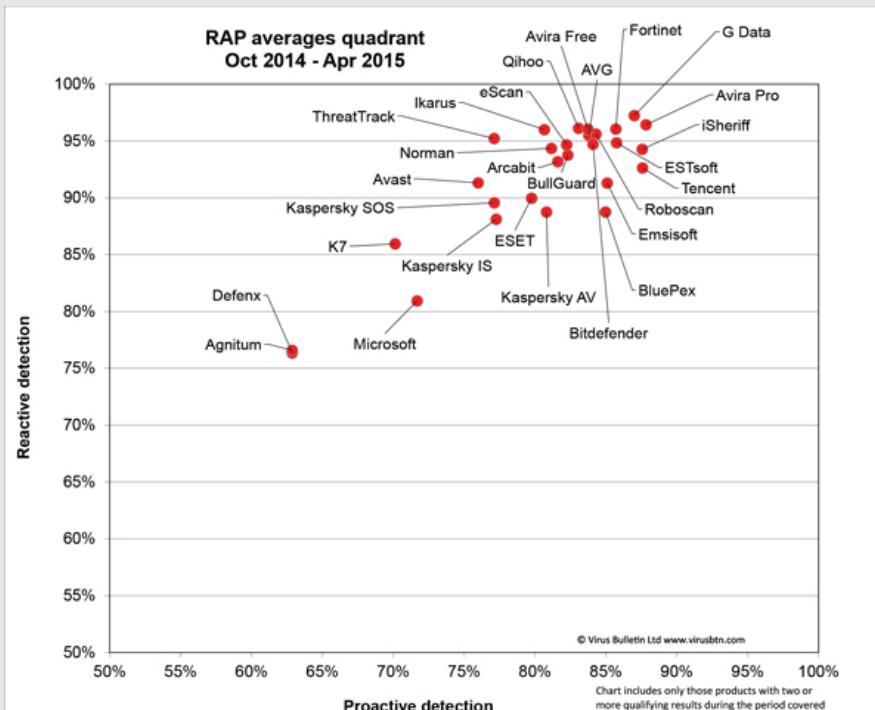
Michel Dubois - 2017

351/404

Les moyens techniques et logiques

La lutte antivirale

Le **meilleur** antimalware ?



Source : <http://www.virusbtn.com/vb100/rap-index.xml>

SSI

Michel Dubois - 2017

352/404

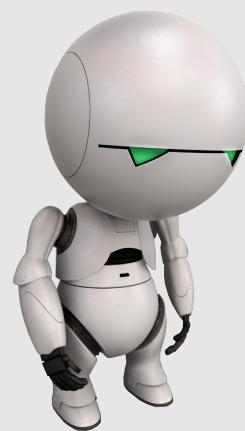
Les moyens techniques et logiques

La lutte antivirale

Le **meilleur** antimalware!!!



L'**utilisateur**, ...



28. Les moyens techniques et logiques

28.3. Les clefs USB

Les moyens techniques et logiques

Les clefs USB

01netPro. Rechercher Oinet. web a

Actualités OinetPro Jeux vidéo Produits Astuces Vidéos Télécharger.com
Actualités Emploi Start-up Evénements 01 Avis d'expert Vidéos Indicateurs

01net Pro / Avis d'expert

Le dilemme de la clé USB

Le Pentagone interdit l'utilisation des clés USB ! A l'origine du bannissement, un virus qui aurait compromis le périphérique d'un militaire... qui l'aurait ensuite transmis.

Laurence Ifrah (DRMCC) | 01net. | le 12/12/2008 à 17h20 | 13 réactions



Le Pentagone interdit l'utilisation des clés USB ! A l'origine du bannissement, un virus qui aurait compromis le périphérique d'un militaire qui l'aurait ensuite transmis à tout le réseau. La clé USB nous pose un vrai dilemme, indispensable parce qu'on la glisse dans sa poche ou dans son sac et qu'aujourd'hui elle atteint des capacités de stockage impressionnantes, elle est néanmoins le

SSI Michel Dubois - 2017 355/404

Les moyens techniques et logiques

Les clefs USB

Le danger des clefs USB



Les moyens techniques et logiques

Les clefs USB

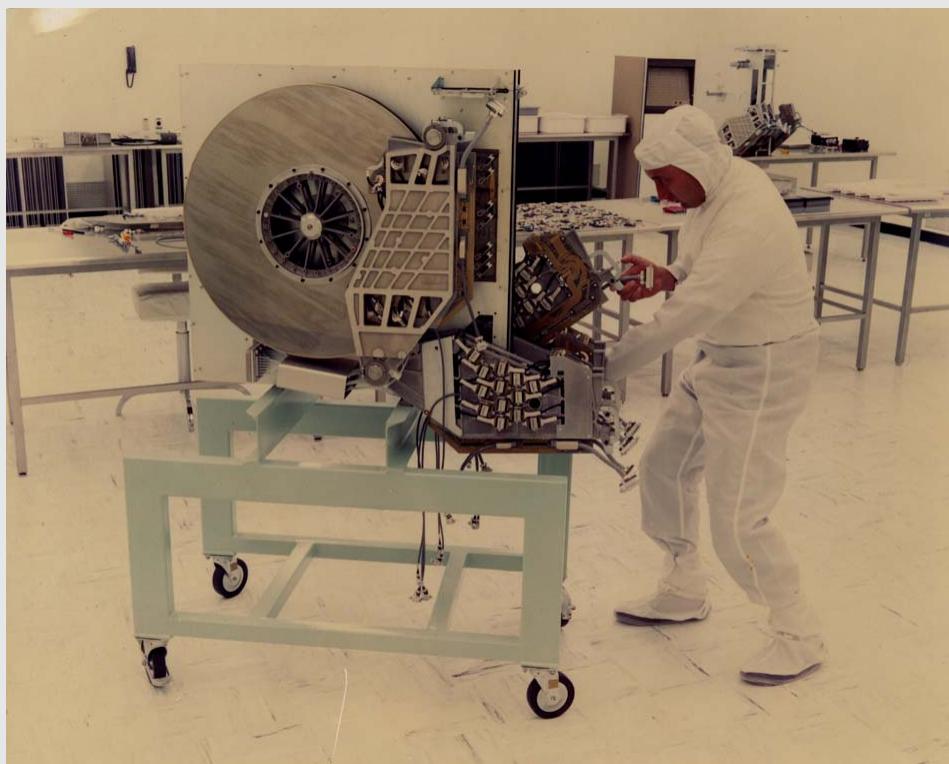
Au commencement, le stockage de l'information...



Les moyens techniques et logiques

Les clefs USB

Arrive l'ère du numérique, volumineux au début...



Les moyens techniques et logiques

Les clefs USB

Mais très vite se réduit...



Les moyens techniques et logiques

Les clefs USB

Et, l'évolution aidant, la clef USB naît.



Les moyens techniques et logiques

Les clefs USB

Les caractéristiques de la clef USB...

- grande capacité
- fiable
- compact
- portable
- universelle
- économique



Les moyens techniques et logiques

Les clefs USB

En résumé, c'est **facile et pratique** d'utilisation et donc **sensible**!



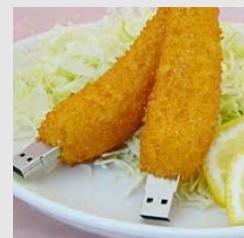
Des règles d'utilisation s'imposent...

Les moyens techniques et logiques

Les clefs USB

Les règles d'utilisation de la clef USB...

1. La clef USB est un support de transport : **supprimez les informations une fois le transfert effectué**
2. On ne mélange pas vie privée et vie professionnelle : **une clef pour la maison et une clef pour le bureau**
3. Différents niveaux de protection de l'information : **une clef, identifiée, pour chaque niveau de protection**
4. La clef USB est le vecteur de propagation préféré des malwares : **AVANT toute utilisation de la clef, passage en station blanche**



SSI

Michel Dubois - 2017

363/404

Les moyens techniques et logiques

Les clefs USB

Une clef USB c'est petit...



...et cela se perd facilement!

SSI

Michel Dubois - 2017

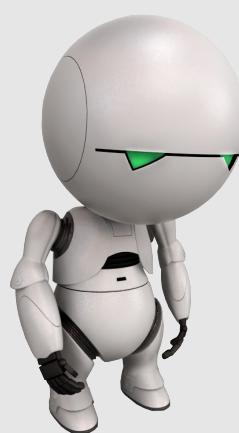
364/404

Les moyens techniques et logiques

Les clefs USB

Dernières **règles d'utilisation** de la clef USB...

1. On porte une **attention particulière** au rangement de sa clef USB
2. On ne ramasse **jamais** une clef USB trouvée dans la rue
3. On prévient immédiatement son CSSI en cas de perte ou de vol



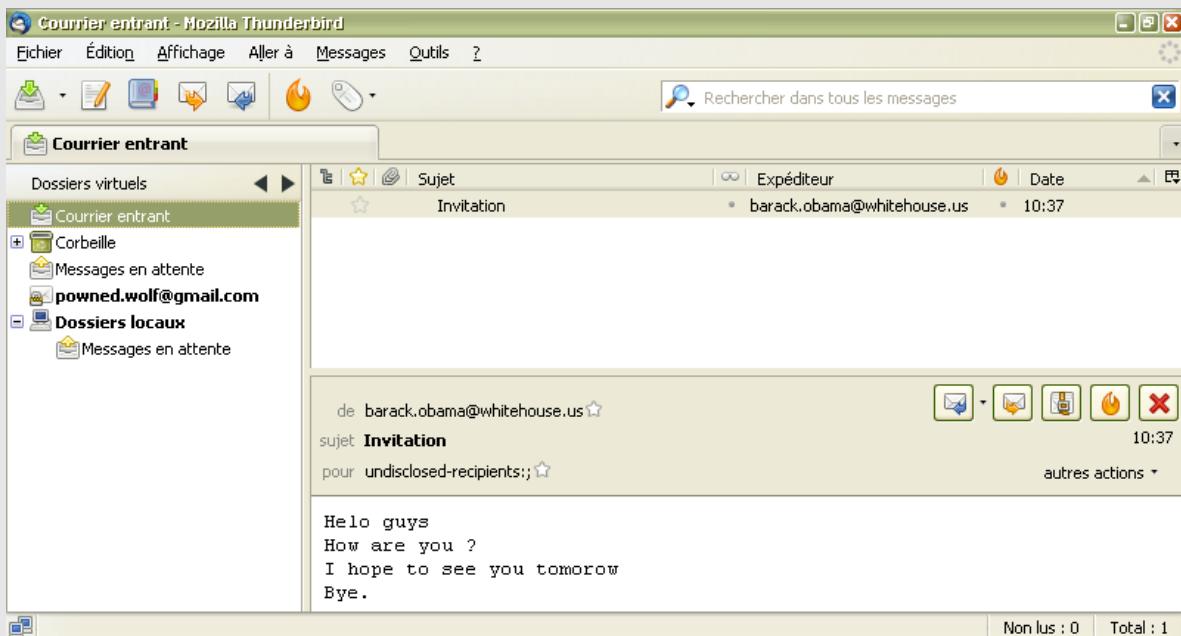
28. Les moyens techniques et logiques

28.4. La messagerie

Les moyens techniques et logiques

La messagerie

Forger un faux mail est **facile**



SSI

Michel Dubois - 2017

367/404

Les moyens techniques et logiques

La messagerie

Forger un faux mail **piégé...**

mercredi 13 avril 2011

Météo Traducteur Mobile Guide Conjugaison Billetterie

ACTUALITE VIDEO PHOTO BLOG TELE OBS CINE BIBLIOS VOYAGE AUTO

Politique | Monde | Les révolutions arabes | Le mariage de Kate et William | People | Média | Planète | Société | Eco

07/03/11 14:54 44 réactions

Bercy victime d'une gigantesque attaque informatique

150 ordinateurs du ministère de l'Economie ont été infiltrés. François Baroin affirme qu'il y a des "pistes" sur l'origine des attaques.

Mots-clés : Bercy, économie, attaque, informatique, hacker, G20

+T -T Imprimer Envoyer Partager Traduire Réagir (44) J'aime 24

Le ministère de l'Economie et des Finances à Paris, en mars 2010. (c) Afp

Le ministre du Budget, François Baroin, a indiqué lundi 7 mars sur Europe 1 qu'il y avait des "pistes" pour l'instant non confirmées sur l'origine des attaques contre le système informatique du ministère de l'Economie et des Finances (Bercy) en décembre.

SSI

Michel Dubois - 2017

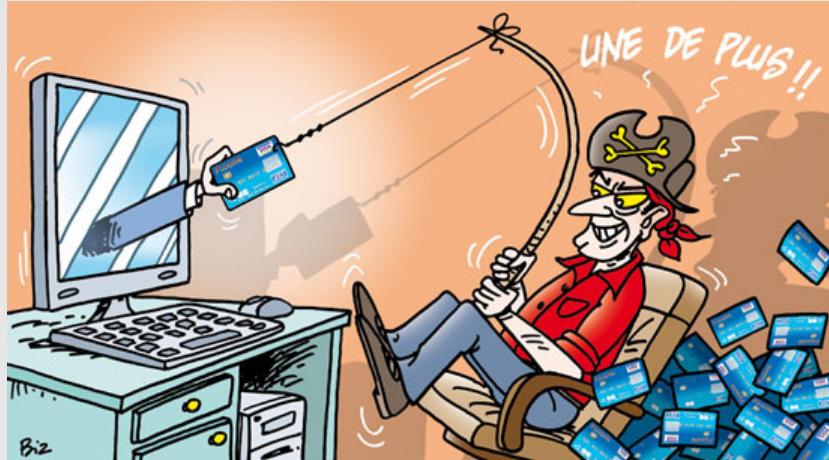
368/404

Les moyens techniques et logiques

La messagerie

Règles de sécurité : ce qu'il faut pas faire

1. Ne jamais répondre à un email :
 - ▶ provenant d'une **banque** ou de **paypal**
 - ▶ en **langue étrangère** ou en mauvais français
 - ▶ demandant des **informations confidentielles**
2. Ne jamais cliquer sur **un lien (URL)** contenu dans un email
3. Ne pas avoir une confiance aveugle dans le nom de l'expéditeur



Les moyens techniques et logiques

La messagerie



Règles de sécurité : ce qu'il faut faire

1. Toujours écrire ses emails en **mode texte**
2. Imposer la réception de ses emails en **mode texte**
3. Donner son email professionnel qu'à des personnes de confiance
4. En cas de suspicion **confirmer** la provenance (appel téléphonique)
5. Signaler immédiatement tout email suspect

Les moyens techniques et logiques

La messagerie

I seek what you leak.



Ensure sensitive information on laptops,
mobiles and removable media is encrypted.

Check email recipients before sending and be
mindful of information you post online.

Copyright 2009 MindfulSecurity.com All Rights Reserved.

Interdiction
formelle d'utiliser
une adresse email
personnelle à des
fins
professionnelles

SSI

Michel Dubois - 2017

371/404

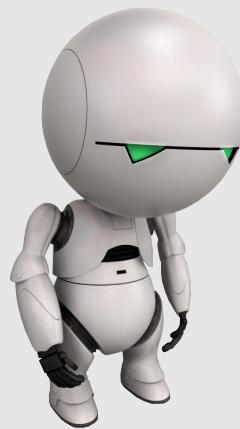
Contres mesures **Section 29** Politiques & Procédures



SSI

Michel Dubois - 2017

372/404



29. Politiques & Procédures

29.1. La réglementation

Politiques & Procédures

La réglementation

Que dit la loi?



Politiques & Procédures

La réglementation

Traitement des données à caractère personnel

Loi 78-17 du 6 janvier 1978 modifiée par la loi 2004-801 du 6 août 2004

Article 34 Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Code pénal art. 226-17 modifié par la loi 2004-801 du 6 août 2004

Article 226-17 Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de **cinq ans d'emprisonnement** et de **300 000 Euros d'amende**.



Politiques & Procédures

La réglementation

Atteintes aux systèmes de traitement automatisé de données

Code pénal - articles L323-1 modifiés par la loi 2004-575 du 21/06/04

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de **deux ans d'emprisonnement** et de **30000 euros d'amende**. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de **trois ans d'emprisonnement** et de 45000 euros d'amende.

Code pénal - articles L323-2 modifiés par la loi 2004-575 du 21/06/04

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de **cinq ans d'emprisonnement** et de **75000 Euros d'amende**.

Politiques & Procédures

La réglementation

Atteintes aux systèmes de traitement automatisé de données

Code pénal - articles L323-3 modifiés par la loi 2004-575 du 21/06/04

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de **cinq ans d'emprisonnement** et de **75000 Euros d'amende**.

Code pénal - articles L323-3-1 modifiés par la loi 2004-575 du 21/06/04

Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Politiques & Procédures

La réglementation

Atteintes aux systèmes de traitement automatisé de données

Code pénal - articles L323-4 modifiés par la loi 2004-575 du 21/06/04

La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.



Politiques & Procédures

La réglementation

Atteintes au secret de la défense nationale

Code pénal – art. L413-10 modifiés par la loi 2009-928 du 29/07/09

Est puni de **sept ans d'emprisonnement** et de **100 000 euros d'amende** le fait, par toute personne dépositaire, soit par état ou profession, soit en raison d'une fonction ou d'une mission temporaire ou permanente, d'un procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier qui a un caractère de secret de la défense nationale, soit de le détruire, détourner, soustraire ou de le reproduire, soit d'en donner l'accès à une personne non qualifiée ou de le porter à la connaissance du public ou d'une personne non qualifiée.

Est puni des mêmes peines le fait, par la personne dépositaire, **d'avoir laissé accéder à, détruire, détourner, soustraire, reproduire ou divulguer** le procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier visé à l'alinéa précédent.

Lorsque la personne dépositaire a agi par imprudence ou négligence, l'infraction est punie de **trois ans d'emprisonnement** et de **45000 euros d'amende**.

Politiques & Procédures

La réglementation

Atteintes au secret de la défense nationale

Code pénal – art. L413-11 modifiés par la loi 2009-928 du 29/07/09

Est puni de **cinq ans d'emprisonnement** et de **75 000 euros d'amende** le fait, par toute personne non visée à l'article 413-10 de :

1. S'assurer la possession, accéder à, ou prendre connaissance d'un procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier qui présente le caractère d'un secret de la défense nationale;
2. Détruire, soustraire ou reproduire, de quelque manière que ce soit, un tel procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier;
3. Porter à la connaissance du public ou d'une personne non qualifiée un tel procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier.

Politiques & Procédures

La réglementation

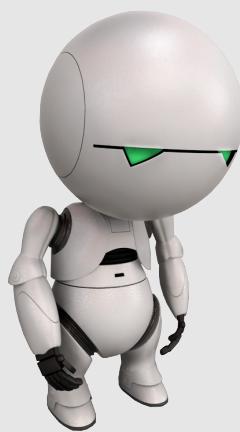
Copie illicite de logiciels

Code de la propriété intellectuelle – art. L335-2

Toute édition d'écrits, de composition musicale, de dessin, de peinture ou de toute autre production, imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon et toute contrefaçon est un délit. La contrefaçon en France d'ouvrages publiés en France ou à l'étranger est punie de trois ans d'emprisonnement et de 300 000 euros d'amende.

Code de la propriété intellectuelle – art. L335-3

Est également un délit de contrefaçon toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur, tels qu'ils sont définis et réglementés par la loi. Est également un délit de contrefaçon la violation de l'un des droits de l'auteur d'un logiciel définis à l'article L. 122-6. Est également un délit de contrefaçon toute captation totale ou partielle d'une œuvre cinématographique ou audiovisuelle en salle de spectacle cinématographique.



29. Politiques & Procédures

29.2. La politique SSI

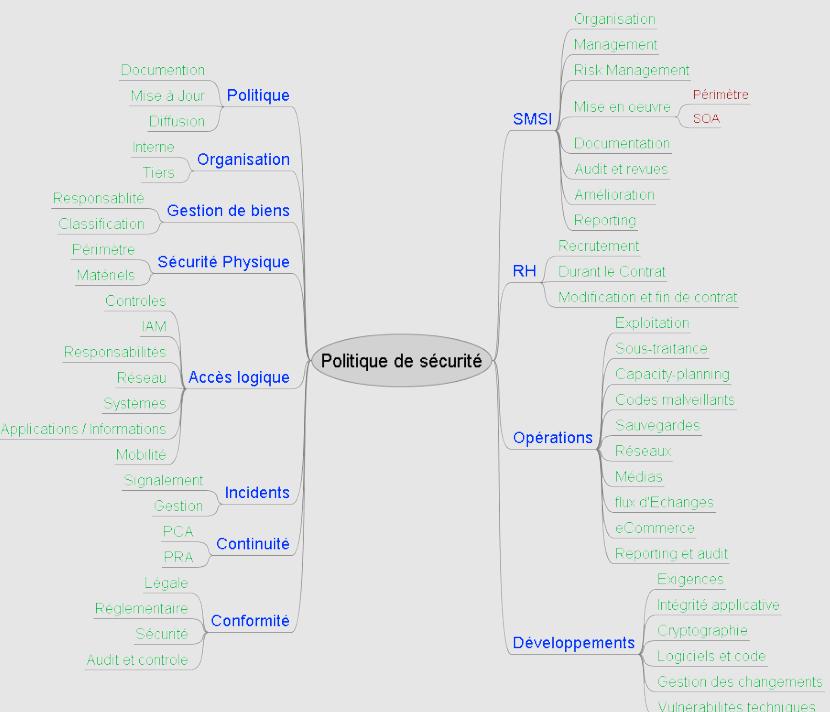
Politiques & Procédures

La politique SSI

Politique SSI

Ensemble formalisé des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme.

La PSSI constitue le socle de la SSI

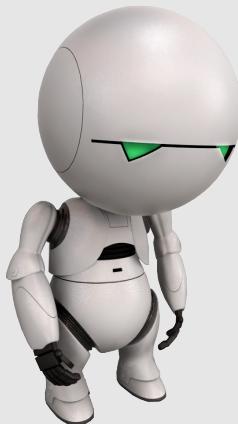


Politiques & Procédures

La politique SSI

La PSSI se décline en documents d'application de manière adaptée aux acteurs destinataires

1. Charte des utilisateurs ou code de bon usage
2. Procédures d'exploitation de sécurité
3. Tutoriels sur le réseau interne
4. Séances de sensibilisation
5. Messages électroniques et notes de service
6. Site Web : <http://ssi.sante.defense.gouv.fr>



29. Politiques & Procédures

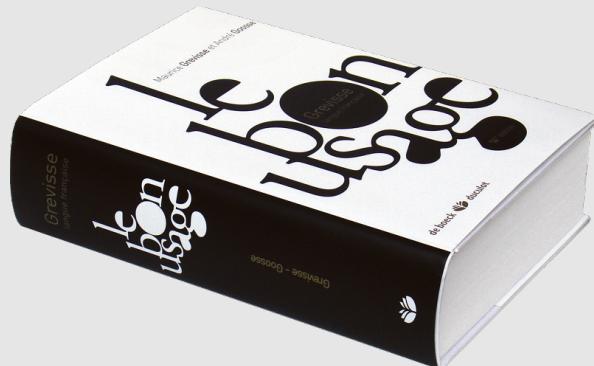
29.3. Code de bon usage

Politiques & Procédures

Code de bon usage

Objectifs :

- définir les modalités d'usage attendu des systèmes d'information
- définir les dispositions spécifiques liées à l'usage de certains médias
- fixer les attributions particulières des acteurs de la SSI
- définir les moyens de contrôle mis en œuvre.



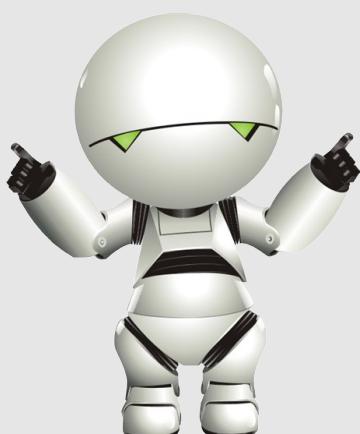
Politiques & Procédures

Code de bon usage

Les bons usages?

- Ne pas **modifier** son environnement de travail
- Ne pas connecter un équipement **personnel** sur un SI **professionnel**
- Les droits d'accès et privilèges sont **personnels** et **inaccessibles**
- **Rendre compte** en cas d'incident
- Respecter les mesures de lutte contre les **contenus malveillants**
- L'usurpation d'identité constitue un **délit**
- L'utilisateur doit prendre toute mesure pour **conserver** les documents électroniques
- **Vider** régulièrement sa boîte aux lettres

Partie 7 Conclusion



Conclusion

Section 30

Petit quizz final



Petit quizz final



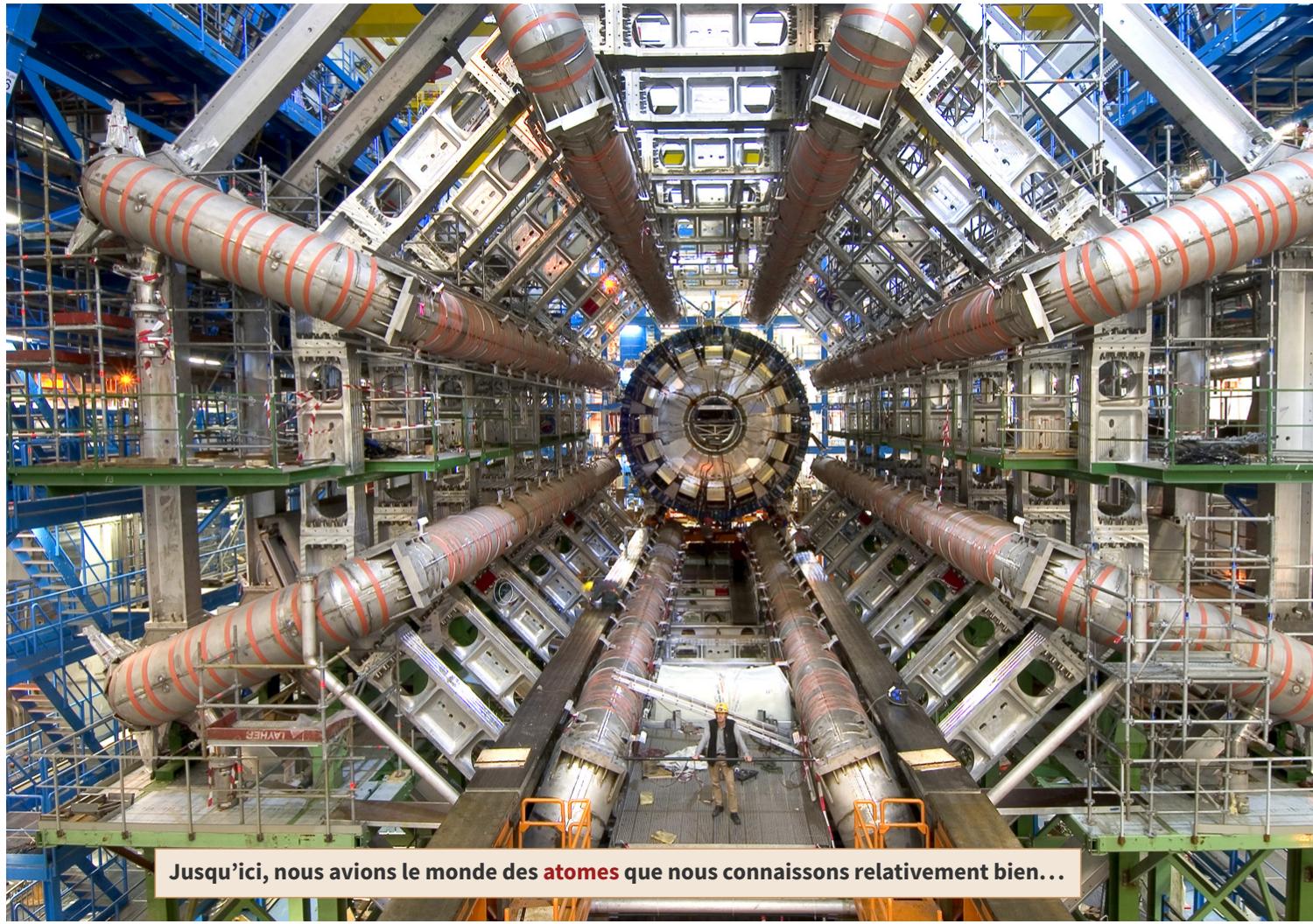
Conclusion
Section 31
Bilan final

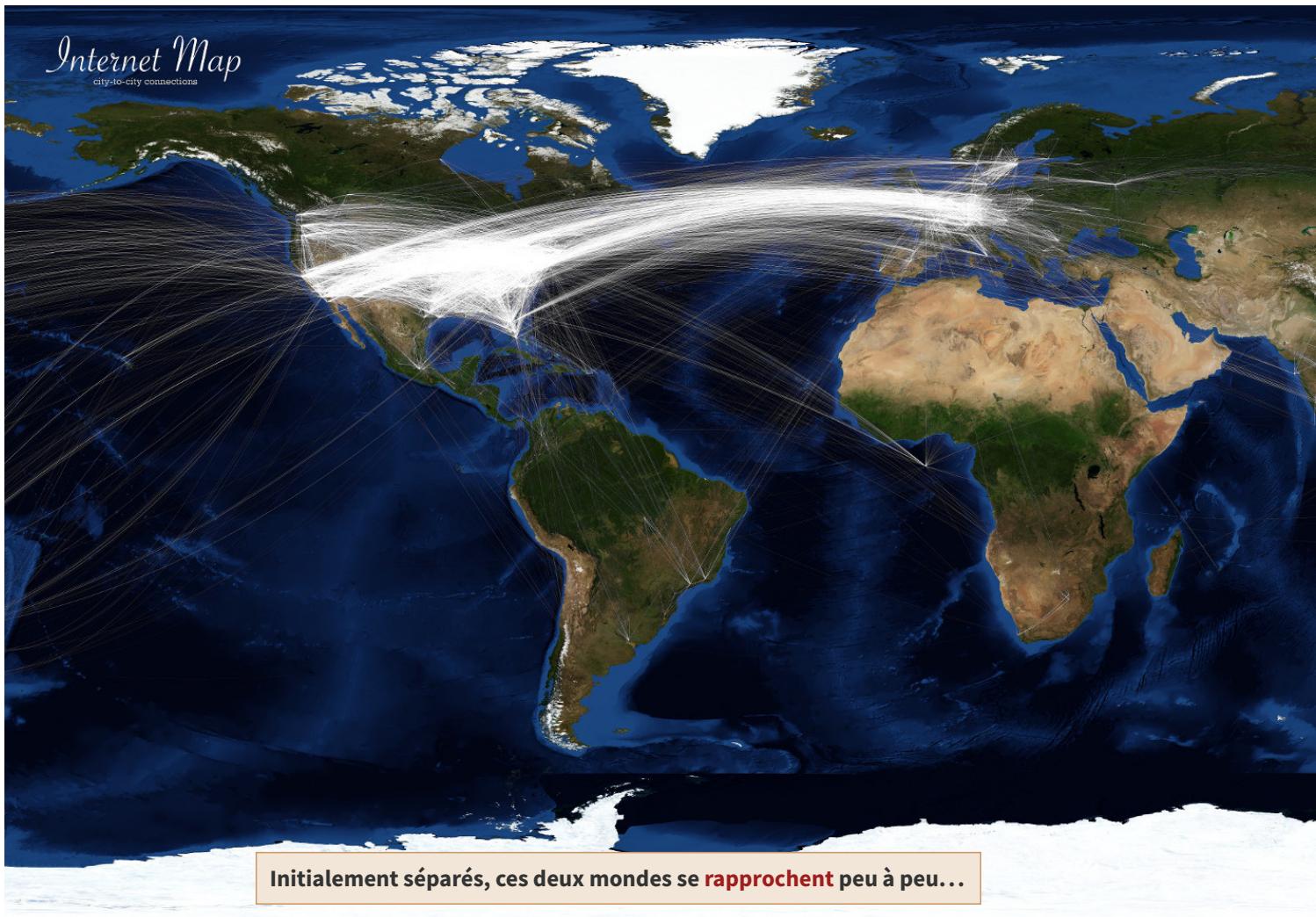
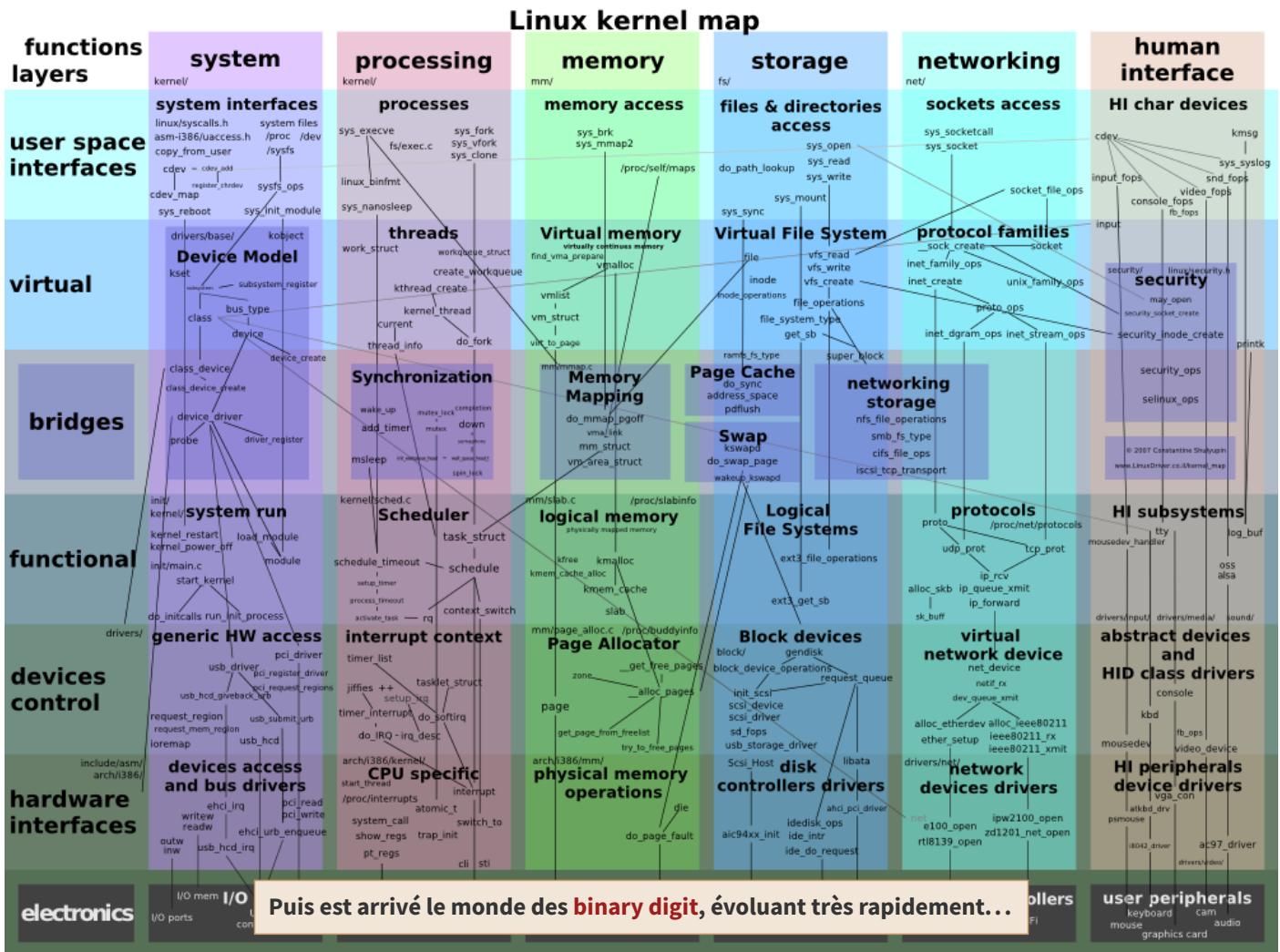


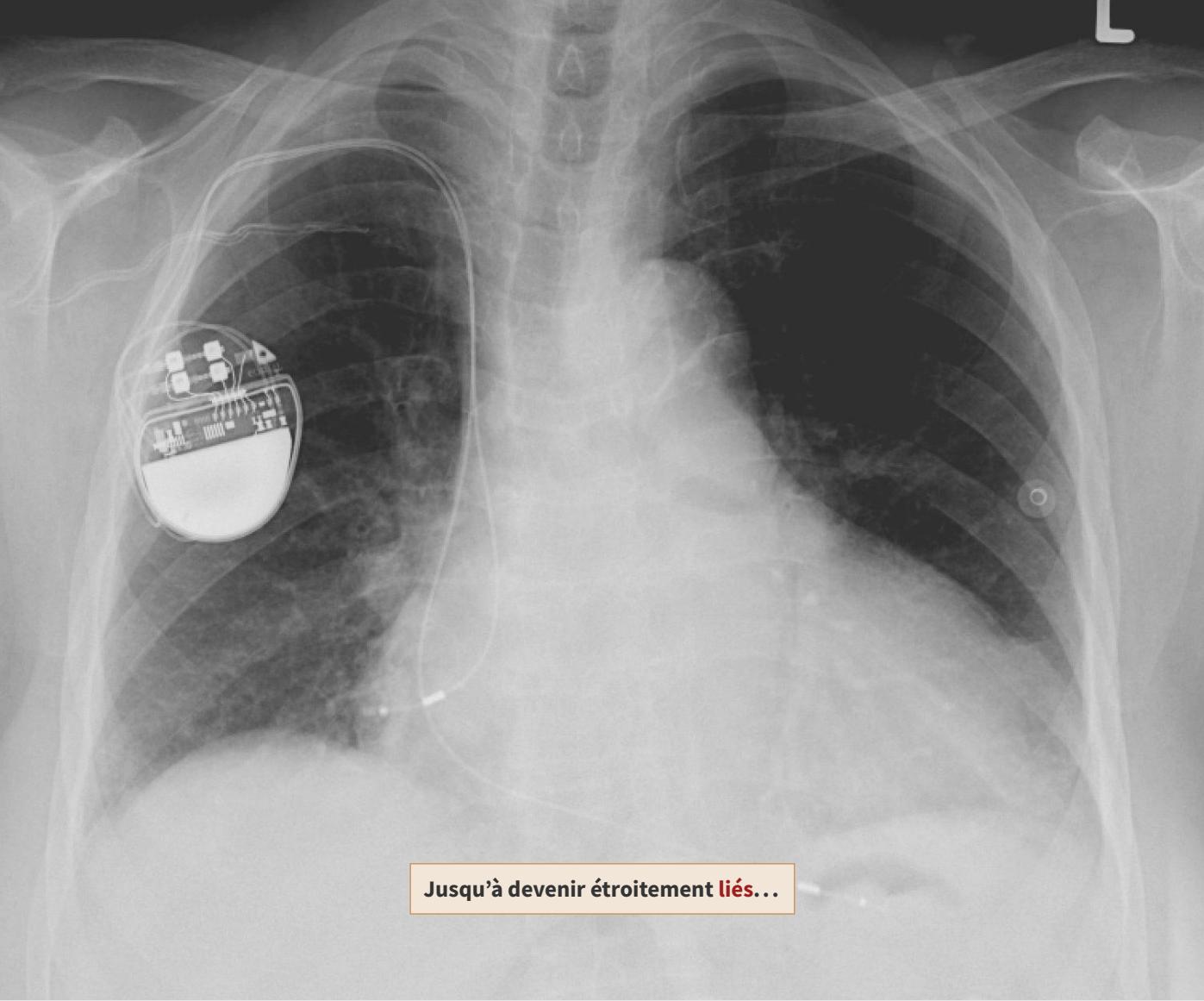
SSI

Michel Dubois - 2017

391/404







Bilan final

La **SSI** est un domaine vaste, demandant beaucoup d'**humilité**, difficile à mettre en œuvre, où la perfection n'existe pas et qui implique la participation de chacun.



Bilan final

La sécurité doit devenir comme les freins d'une voiture :
elle doit permettre d'aller vite.

Joshua Corman – IBM ISS



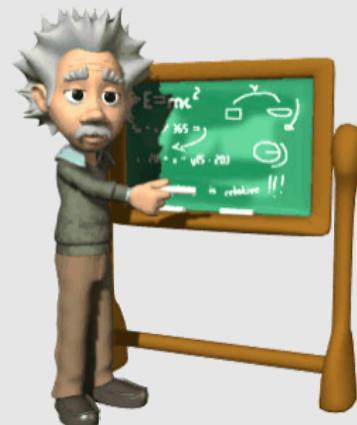
SSI

Michel Dubois - 2017

397/404

Bilan final

Questions ?



SSI

Michel Dubois - 2017

398/404

Conclusion

Section 32

Références



Références



[Wikipedia](#)

http://fr.wikipedia.org/wiki/Sécurité_des_systèmes_d'information



[Clusif](#)

<http://www.clusif.asso.fr/>

Le Club de la Sécurité de l'Information Français est un club professionnel dont la finalité est d'agir pour la sécurité de l'information, facteur de pérennité des entreprises et des collectivités publiques.



[Défense et Sécurité nationale - Le Livre Blanc](#)

Éditions Odile Jacob

Quelle doit être, à l'heure de la mondialisation, la politique de la France pour garantir la sécurité du pays, assurer la défense de ses intérêts dans le monde et contribuer à l'affirmation de l'Europe sur la scène internationale ?

Références



Agence nationale de la sécurité des systèmes d'information

<http://www.ssi.gouv.fr>

Contribuer à la définition interministérielle et à l'expression de la politique gouvernementale en matière de sécurité des systèmes d'information.



Portail de la sécurité informatique

<http://www.securite-informatique.gouv.fr>

Ce portail d'information propose des fiches pratiques et des conseils destinés à tous les publics (particuliers, professionnels, PME). Il comporte également des actualités et avertit de menaces nouvellement rencontrées qui appellent une action rapide des utilisateurs pour en limiter les effets.



Sécurité des Systèmes d'Information

Philippe Loudenot

Philippe Loudenot, membre de l'ARCSI, est FSSI du ministère de la santé.

Références



L'art de la supercherie

Kevin Mitnick

Éditions Campus press

Dans cet ouvrage, Kevin Mitnick propose de découvrir des scénarios réalistes d'arnaques et d'escroqueries, tous basés sur l'art de la persuasion et de la manipulation.



Management de la sécurité de l'information

Alexandre Fernandez-Toro

Édition Eyrolles

Cet ouvrage apporte les éléments indispensables à la compréhension et à l'application de la norme ISO 27001.



Menaces sur le réseau

Michał Zalewski

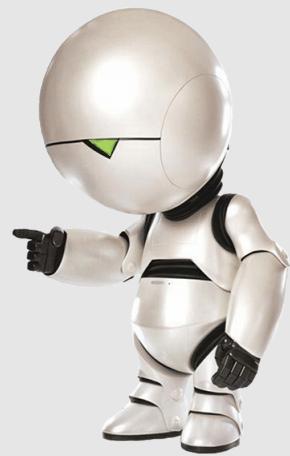
Éditions Pearson Education France

À travers l'étude de quelques défis exceptionnels, l'auteur nous plonge dans les entrailles de l'informatique moderne. Il apporte un regard nouveau sur la SSI en détaillant les failles conceptuels que traverse un bit d'information de sa création lors d'une frappe clavier à sa transmission sur le réseau.

Conclusion

Section 33

Licence



Licence

Copyright 2008 - 2016 - Michel Dubois

Paternité



Vous devez citer le nom de l'auteur original de la manière indiquée par l'auteur de l'œuvre ou le titulaire des droits qui vous confère cette autorisation (mais pas d'une manière qui suggèrerait qu'ils vous soutiennent ou approuvent votre utilisation de l'œuvre).

Pas d'utilisation commerciale



Vous n'avez pas le droit d'utiliser cette création à des fins commerciales sans autorisation écrite de l'auteur.

Partage des conditions initiales à l'identique



Si vous modifiez, transformez ou adaptez cette création, vous n'avez le droit de distribuer la création qui en résulte que sous un contrat identique à celui-ci.