ECOLE NATIONALE SUPÉRIEURE D'INFORMATIQUE

Introduction à la sécurité informatique

Mohamed ANANE

Objectifs du cours

Chapitre 1

- Contribuer à une meilleure compréhension des risques de sécurité liés à l'usage de l'outil informatique.

- Sensibiliser aux bonnes pratiques peux coûteuses et faciles à mettre en œuvre permettant de limiter une grande partie des risques liés à l'usage de l'informatique.

Mieux vaut prévenir que guérir

Objectifs du cours

Chapitre 2

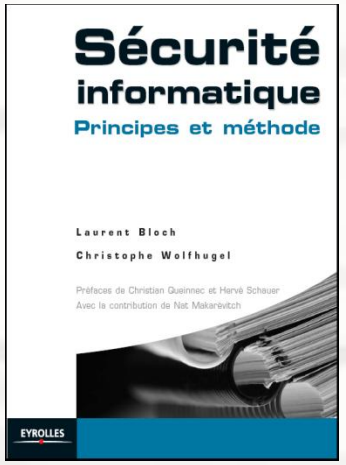
- Comprendre le rôle de la cryptographie dans la protection de l'information.
- Découvrez le fonctionnement des primitives cryptographique.
- Apprendre à les utiliser correctement et à raisonner sur la sécurité (garantir un ou plusieurs services de la sécurité).

Livres recommandés

- Laurent Bloch, Christophe Wolfhugel

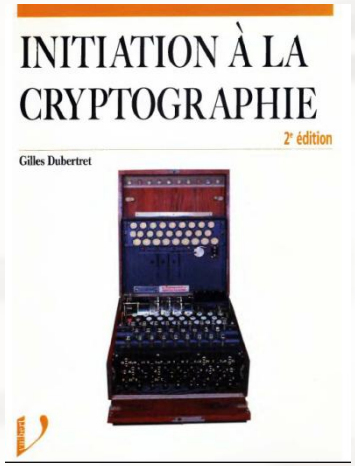
  Sécurité Informatique

  Principes et méthodes.



- Gilles Dubertret

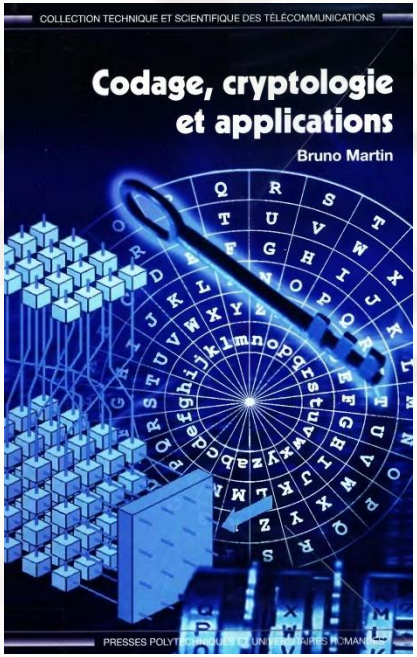
  Initiation à la Cryptographie



Livres recommandés

- Bruno Martin

Codage, cryptographie et applications



Citations

- *« Le moyen d'être sauf, c'est de ne pas se croire en sécurité »*

Thomas Fuller
Physicien anglais

Plan du cours

Concepts de base

- **L'enjeux de la sécurité (Pourquoi sécuriser ?)**
- **Définir ce que la sécurité dans le contexte des S.I.**
- **Menaces**
  - **Relevant des Pbs non spécifiques à l'informatique**
  - **Relevant de l'informatique (Détournement de l'information, Espionnage, logiciels malveillants).**
  - **Contres mesures pour lutter contre ces malveillances.**
- **Les différents niveaux de sécurité (***Sécurité de communication et d'opérations* **).**
- **Politique de sécurité (***Définition, Etapes d'établissement d'une politique de sécurité,* **EBIOS, MEHRI, ISO17799).**
- **Les services de la sécurité (***Confidentialité, Authentification, Identification, Intégrité, non-répudiation***).**

Introduction à la cryptographie

- **Historique de la cryptographie avant l'ère de la technologie.**
- **Cryptographie moderne (Principes de Kerckhoffs, Codage de l'information)**
- **Principe du chiffrement symétrique**
  - **Protocole de chiffrement AES**
    - **Calcul dans le corps de Galois GF(2^8)**
    - **Force d'un mot de passe.**
- **Principe du chiffrement asymétrique**
  - **Protocole de chiffrement RSA**
    - **Calcul modulaire**
    - **Exponentiation modulaire**
  - **Protocole de chiffrement ECC**
- **Chiffrement hybride**
- **Protocoles d'échange de clés (Diffie-Hellman, El Gamal)**
  - **Génération des clés du RSA (Publique et privé)**
- **Utilisation de ces protocoles de chiffrement pour garantir les services de la sécurité (*Confidentialité, Authentification, Identification, Intégrité, non-répudiation*).**
- **Les fonctions de Hachage (MD5, SHA2)**
- **Notion sur les certificats et autorité de certification.**

Evaluation

- **Un control Intermédiaire CI (sur 10points)**
- **Une ou deux interrogations surprises IN (durant le cours) (sur 5points)**
- **Un control Finale CF (sur 20 points)**
- **Un Bonus (7points)**

Moyenne = (2*(CI+IN) + 2*CF + Bonus)/4

Chapitre I
Concepts de base

Pourquoi sécuriser

- L'informatique est devenue un outil incontournable dans l'entreprise
  - ➡ La Gestion, l'Organisation, la Production et la Communication.

- Le réseau de l'entreprise qui met en œuvre des données sensibles.
  - ➡ les stocker, les partager en interne,
  - ➡ les communiquer au-delà des murs (à d'autres entreprises ou personnes).

Pourquoi sécuriser

- Cette ouverture vers l'extérieur conditionne des gains de productivité et de compétitivité.
  - ➡ Impossible de renoncer aux bénéfices de l'informatisation (Isoler le réseau, retirer les données confidentielles).

- Les données sensibles du SI de l'entreprise sont donc exposées aux actes de malveillance.
  - ➡ Vole, sabotage etc.

Pourquoi sécuriser

- **Une protection juridique faible**
  - ➡ Les malfaiteurs sont difficilement identifiables (agissent à distance, à travers des relais).
  - ➡ Les attaques sont souvent transfrontalières. Juridictions différentes ⇒ l'impunité reste de fait.

- **Des obligations légales à respecter.**
  - ➡ Obligation de protéger les données nominatives (clients, patients, salariés, etc.)
  - ➡ Obligation dans le cadre d'accords de partenariat (**B**usiness to **B**, secret Défense, etc.)

Pourquoi sécuriser

- **La délinquance informatique : une réalité**
  - ➡ Les pirates informatiques sont des malfaiteurs (professionnels)
  - ➡ Les statistiques Europol (Agence Européenne de Police) révèlent:
    (60% des équipes effectuant des attaques lourdes sont financées par le crime organisé.
    80% des attaques sont à but financier)

Pourquoi sécuriser

- **La gravité des impacts**
  - La survie de l'entreprise: (étude du Gardner Group) 95% des PME (piratées sévèrement) ont stoppé leurs activités dans l'année qui suivait
  - Paralyse: (destruction des données, de la capacité de production; dégradation de l'image de l'entreprise
  - Vole : détournement de fonds, chantage.

Le monde de la cyber-criminalité est en constante évolution, mais les entreprises restent la cible numéro un.

Premières notions de sécurité

Définition

La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles.

→ Sécurité = " Safety" السلامة

Protection des systèmes informatiques contre les accidents dus à l'environnement, les défauts du système.

Domaine d'élection: *les systèmes* informatiques contrôlant des procédés temps réels et mettant en danger des vies humaines (transports, énergie.)

Premières notions de sécurité

Sécurité = "Security" الأمن

Protection des systèmes informatiques contre des actions malveillantes intentionnelles.

Domaine d'élection: *les systèmes* informatiques réalisant des traitements sensibles ou comprenant des données sensibles.

La sécurité des systèmes d'information (SSI) est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire et mis en place pour conserver, rétablir, et garantir la sécurité du systèmes d'information.

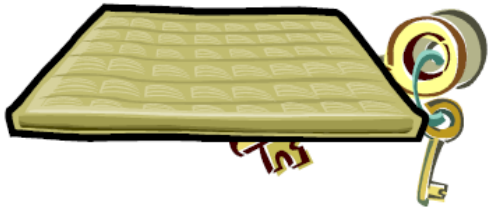
Premières notions de sécurité

- Le système d'information (S.I) est pour beaucoup d'entreprises un élément absolument vital.
  - ➡ tout ce qui le menace est potentiellement mortel.

- Les menaces, risques contre les S.I :
  - ➡ Atteinte à la disponibilité des systèmes et des données
  - ➡ Destruction de données
  - ➡ Corruption ou falsification de données
  - ➡ Vol ou espionnage de données
  - ➡ Usage illicite d'un système ou d'un réseau
  - ➡ Usage d'un système compromis pour attaquer d'autres cibles.

Premières notions de sécurité

- Exemple d'un risque: Le cambrioleur



Vulnérabilité:
Clés sous le tapis.

Menace:
Cambrioleur essaie d'entrer.

Impact: Cambrioleur casse l'armoire, vole de l'argent, crée des ennuis.

Risque = Vulnérabilité • Menace • Impact

Risque = probabilité d'occurrence ×préjudice

Premières notions de sécurité

- Exemple d'un risque résiduel : Le pickpocket

Réduction de risque :
Prendre les clés avec soi.

Risque résiduel : Un pickpocket vole les clés.

→ La sécurité à 100% n'existe pas.

Les menaces

- Deux grandes catégories de menaces

  1 Ceux qui concernent la sécurité de l'ordinateur proprement dit, de son système d'exploitation et des données qu'il abrite.

  2 Ceux qui découlent directement de l'utilisation des réseaux et d'internet.

Les menaces

- Première catégorie de menaces (qui existe depuis la naissance de l'informatique)
  - Menaces relevant de problèmes non spécifique à l'informatique. (Incendie, inondation …)
    - Vol et sabotage de matériels

      (vol et destruction du matériel, destruction du support de stockage)
    - Autres risques.

      (Départ du personnels stratégiques, Grèves …)
  - Les pannes et les erreurs non intentionnés.
    - Pannes/dysfonctionnement (matériel ou logiciel)
    - Erreurs d'exploitation.(oubli de sauvegarde écrasement de fichiers).
    - Erreur de manipulation des informations (Erreur de saisie, de transmission ou d'utilisation.

Les menaces

- Deuxième catégorie de menaces (qui concerne ce cours)

  - Les menaces intentionnelles. (L'ensemble des actions malveillantes)
    (Qui devrait être l'objet principal des mesures de protections)

    - Menaces passives (Détournement des données)
      (Espionnage industriel et commercial,
      Violation déontologique,
      Copie de logiciel…)

Les menaces

- Deuxième catégorie de menaces (qui concerne ce cours)

  - Les menaces intentionnelles. (L'ensemble des actions malveillantes)

    - Menaces actives.
      - Modification de l'information (Fraude financière informatique, sabotage …
      - Modification des logiciels Malware: bombe logique, virus, cheval de Troie, ver…

Les menaces

- Pourcentages des différentes menaces
  - Action malveillantes 61% (en croissance)
  - Risques accidentels 24%
  - Pannes et erreurs 12%
  - Autres 3%

Explication de l'importance des actions malveillantes.

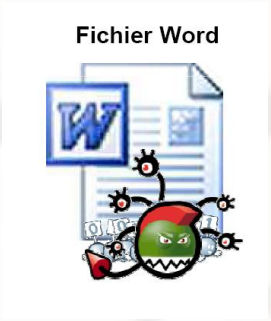
- Développement de l'informatique
- Complexité croissante donc plus de vulnérabilité.
- L'ambiance de non sensibilisation au problèmes de la sécurité.

Types de logiciels malveillants

Virus

Un virus est un logiciel qui s'attache à tout type de document électronique «hôtes», et dont le but est d'infecter ceux-ci et de se propager sur d'autres documents et d'autres ordinateurs.

Un virus a besoin d'une intervention humaine pour se propager.



Types de logiciels malveillants

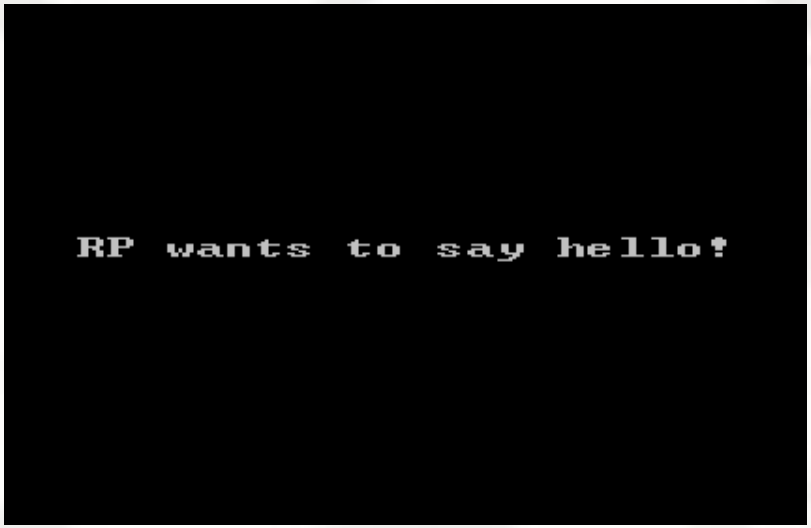
- Analogie avec le virus biologique puisqu'il présente des similitudes dans sa manière de se propager en utilisant les facultés de reproduction de la cellule hôte

- Sur le net: (appliquettes Java ou procédures JavaScript) des programmes qui s'exécuter sur votre PC en se chargeant à distance depuis le serveur Web visité.

Types de logiciels malveillants

- Exemples concrets de Virus:

Boot Sector: Rhubarb



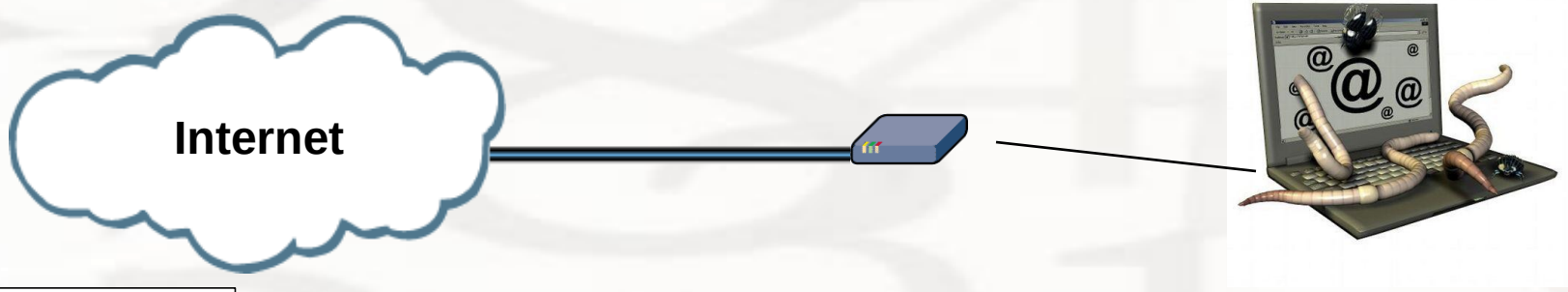
Types de logiciels malveillants

Vers « *Worm* »

Un **ver informatique** se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet en s'envoyant à travers le réseau

(e-mail, Bluetooth, chat..) (apparue en 2003)

Le ver n'a pas besoin de l'interaction humaine pour pouvoir se proliférer.



Types de logiciels malveillants

L'objectif d'un ver n'est pas seulement de se reproduire :

- Espionner l'ordinateur où il se trouve ;
- Offrir une porte dérobée à des pirates informatiques ;
- Détruire des données sur l'ordinateur où il se trouve ou y faire d'autres dégâts ;
- Envoyer de multiples requêtes vers un serveur Internet dans le but de le saturer (déni de service).

L'activité d'un ver a souvent des effets secondaires :

- le ralentissement de la machine infectée ;
- le ralentissement du réseau de la machine infectée ;
- le plantage de services ou du système d'exploitation de la machine infectée.

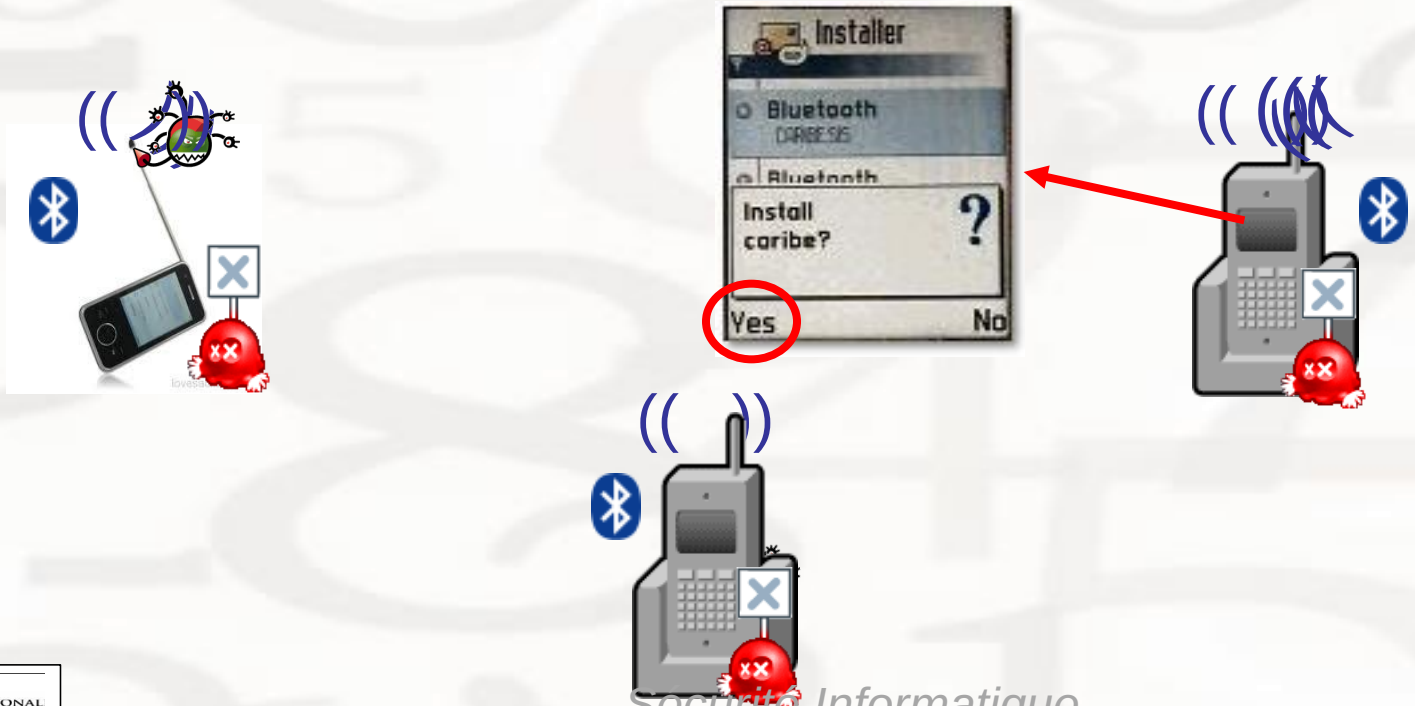
Types de logiciels malveillants

- StuxNet 2010 est un ver informatique spécifique au système Microsoft Windows.
- Attaquer les systèmes SCADA: qui sont des systèmes de télégestion à grande échelle permettant de traiter en temps réel un grand nombre de télémesures et de contrôler à distance des installations techniques
- Le ver a affecté 45 000 systèmes informatiques, dont 30 000 situés en Iran. (lancé contre le nucléaire iranien).
- Symantec (2011) publie une analyse:
  - Conception sophistiquée
    5 à 10 personnes pendant 6 mois
  - Conçu par le gouvernement américain ou israélien ?

Types de logiciels malveillants

Vers GSM

Un **ver** GSM se reproduit en s'envoyant à un autre téléphone mobile par moyen Bluetooth ou MMS.



Types de logiciels malveillants

SPAM **pourriel** (poubelle courriel) **polluriel** (pollution et courriel)

Le spam est du courrier électronique non sollicité envoyé a un très grand nombre de personnes sans leur accord préalable. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires. 95 % des messages échangés

Spiced Ham
jambon épicé

Types de logiciels malveillants

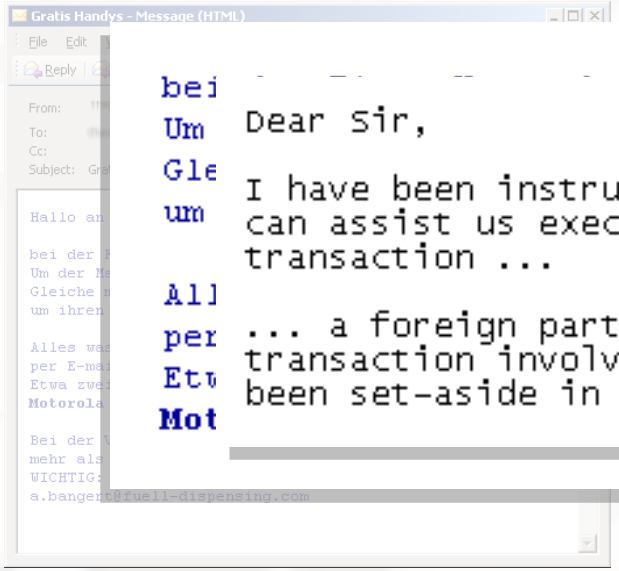
Contenu et objectifs du spam: la publicité.

- Les médicaments (des hormones anti vieillissement ou la perte de poids etc).
- le crédit financier, les casinos en ligne, les montres de contrefaçon, les diplômes falsifiés et les logiciels craqués.

Types de logiciels malveillants

SCAM
Le **spam** à but d'escroquerie

Gratis Handy (HOAX)



Nigeria 419 (Email/Fax&Fraude)

Types de logiciels malveillants

Cheval de Troie (Virus réticulaire) *(Trojan horse)*

Programme bénin (jeux, documents…) cachant un autre programme.
Lorsque le programme est exécuté, le programme caché s'exécute aussi et pourrait ouvrir une « porte cachée ».

Conséquences de cette attaque

- contrôle du PC de l'extérieur
- perte de données
- divulgation de données privées (chat, e-mails …)
- espionnage: microphone, webcam
- attaques à partir du PC « infecté » (Zombi)

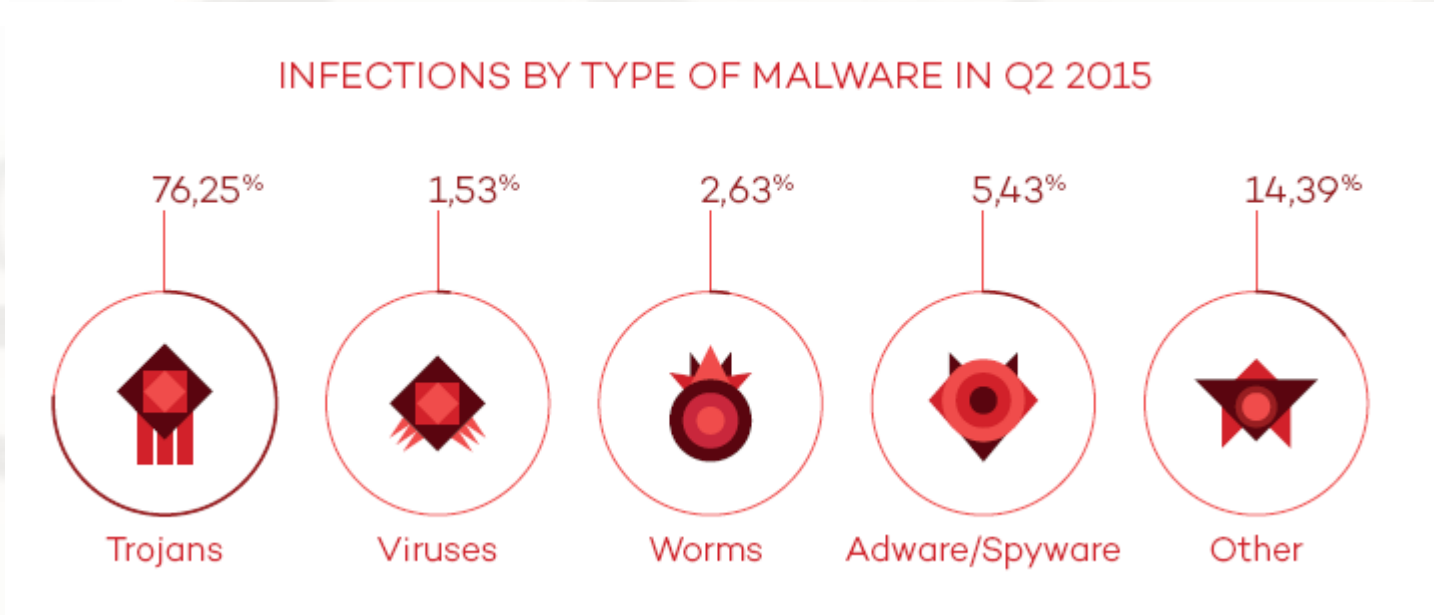
Types de logiciels malveillants

Ransomware ou **Rançongiciel**,
est un logiciel malveillant qui prend en otage des données personnelles. Pour ce faire, un rançongiciel chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer. ...

[1]Avec plus de 25 millions de nouveaux échantillons de malwares mis en circulation au cours des trois derniers mois, soit une moyenne de 285.000 nouveaux fichiers malveillants chaque jour.

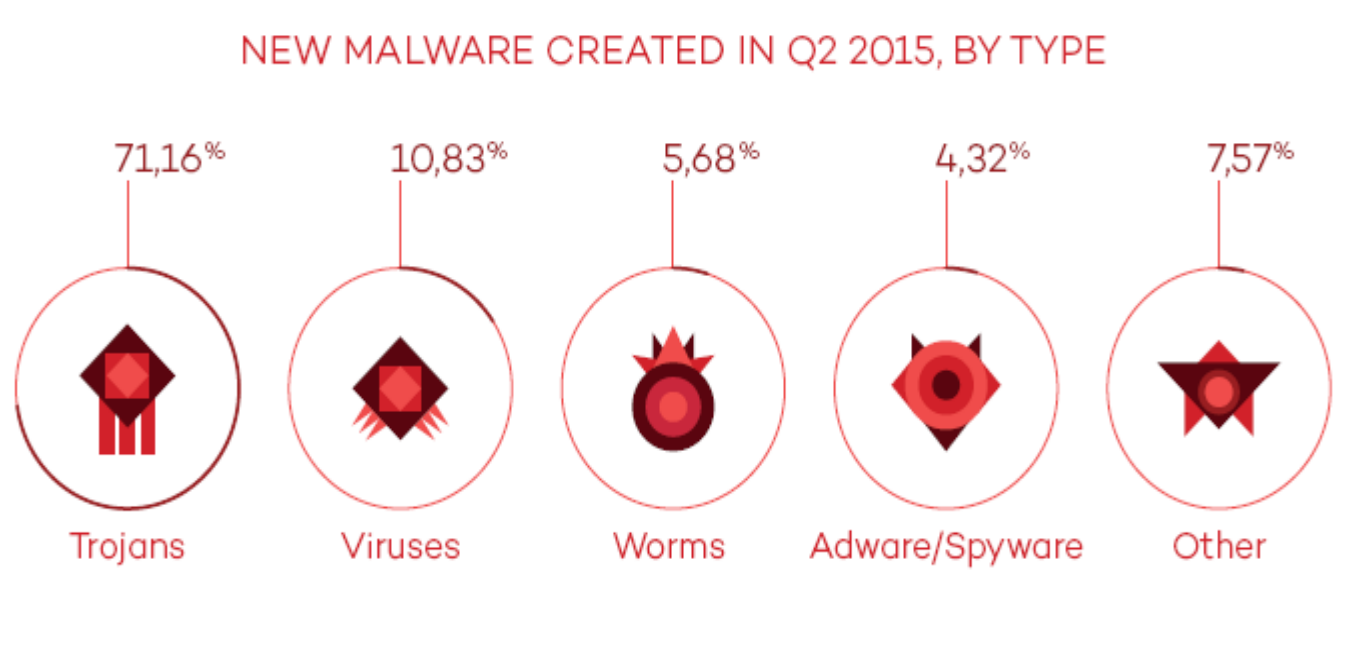
[1]PandaLabs-Annual Report 2017

Infection par types de logiciels malveillants



PandaLabs-Report_Q2-2015

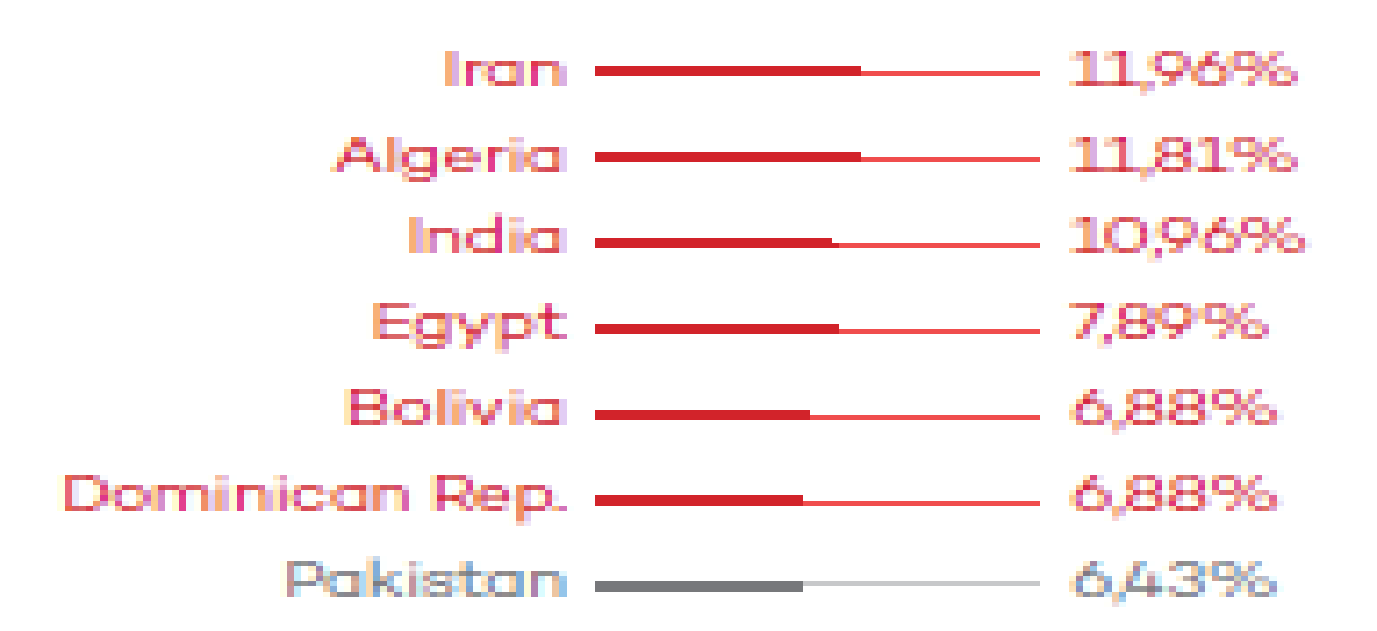
Nouveaux logiciels malveillants par types



PandaLabs-Report_Q2-2015

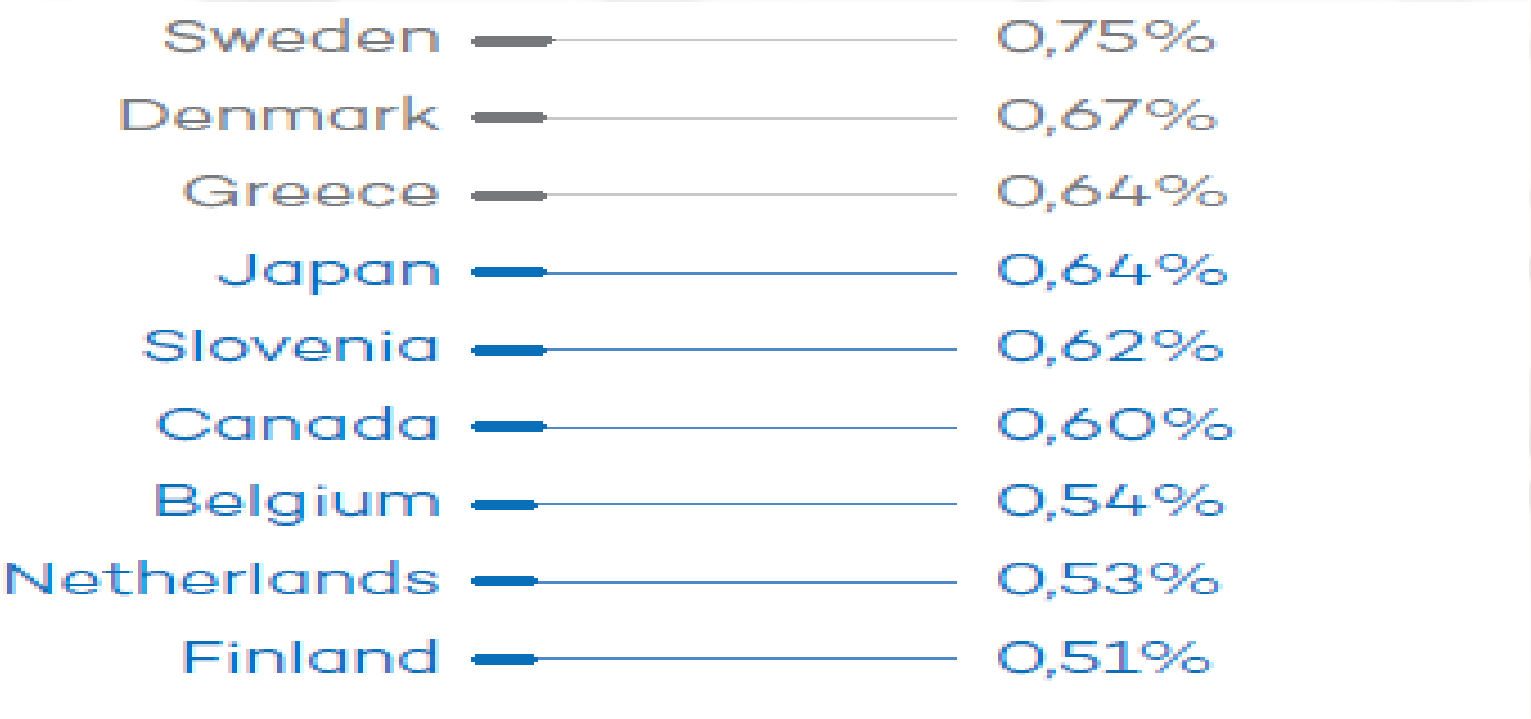
Pays les plus infectés par des virus

The percentage of machines attacked by country



PandaLabs Annual Report 2017

Pays les moins infectés par des virus



PandaLabs Annual Report 2017

Les 10 échantillons de malware les plus consultés

POS.	SEEN	TYPE	NAME
1	15/8/17	Trj/HackCCleaner.A	HackCCleaner
2	5/1/17	Trj/CerberCrypto.A	Cerber
3	15/5/17	Trj/RansomCrypt.I	WannaCry
4	15/8/17	Trj/HackCCleaner.A	HackCCleaner
5	17/5/17	Trj/Agent.SM	Downloader
6	24/2/17	Trj/Genetic.gen	Bot
7	15/5/17	Trj/RansomCrypt.I	WannaCry
8	12/5/17	Trj/RansomCrypt.K	WannaCry
9	15/5/17	Trj/Agent.PS	Downloader
10	12/5/17	Trj/RansomCrypt.K	WannaCry

backdoored version of CCleaner

Downloaders (Trojans that are used as an intermediary for installing all types of malware)

PandaLabs Annual Report 2017

Comment fonctionnent les malwares

- Différents moyens pour s'infiltrer et causer des dommages à votre système grâce aux logiciels malveillants.

1. Ingénierie sociale

L'ingénierie sociale est une technique utilisée par les cybercriminels pour inciter les gens à partager des informations confidentiels. l'accès à leurs appareils. (phishing)

- *92 % des logiciels malveillants sont transmis par e-mail ?*

Comment fonctionnent les malwares

2. Logiciels *bundled (Groupé)*

- lorsque vous téléchargez un logiciel gratuit livré avec des applications tierces supplémentaires dans lesquelles l'une d'entre elles pourrait contenir un logiciel malveillant.

Comment fonctionnent les malwares

3. Partage de fichiers en peer-to-peer

- Les protocoles de partage P2P (torrents) font partie des principales méthodes utilisées par les cybercriminels pour distribuer des logiciels malveillants. Permet de diffuser des codes malveillants par le biais de fichiers partagés via P2P.

Comment fonctionnent les malwares

4. Freeware

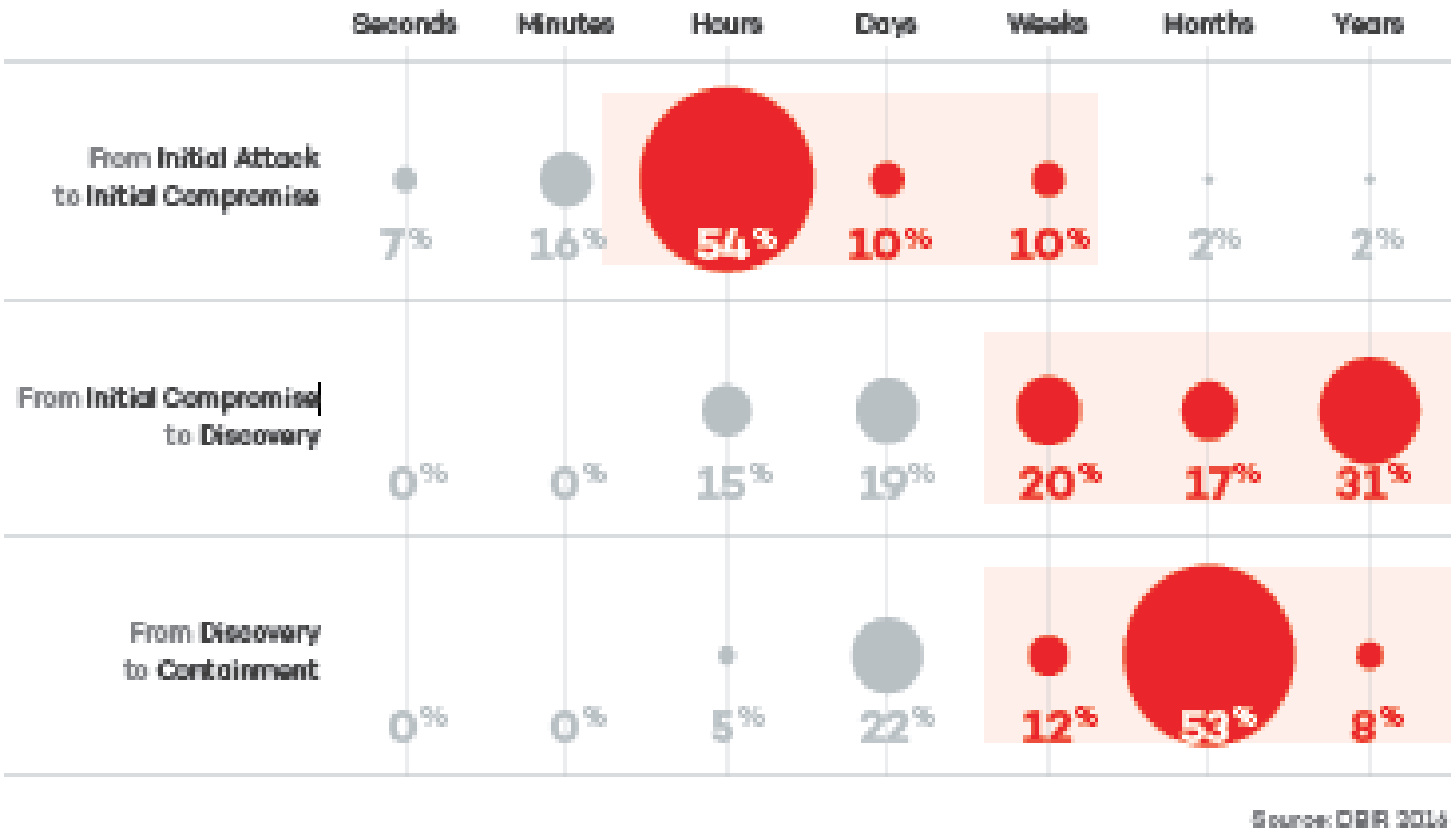
- **Les logiciels gratuits** téléchargés à partir de sources inconnues ou non fiables sont souvent infectés par des logiciels malveillants qui peuvent endommager votre système et compromettre vos données.

Comment fonctionnent les malwares

5. Homogénéité

- L’homogénéité peut être une cible facile pour les attaques de logiciels malveillants. Les malwares peuvent se propager rapidement à travers les systèmes connectés au même réseau et exécutant le même système d’exploitation. Si un appareil est infecté, il y a de fortes chances que l’ensemble du réseau soit compromis.

From penetrating defenses to concealing malware



PandaLabs Annual Report 2017

Lutte contre les malveillances informatiques

Comment se protéger?

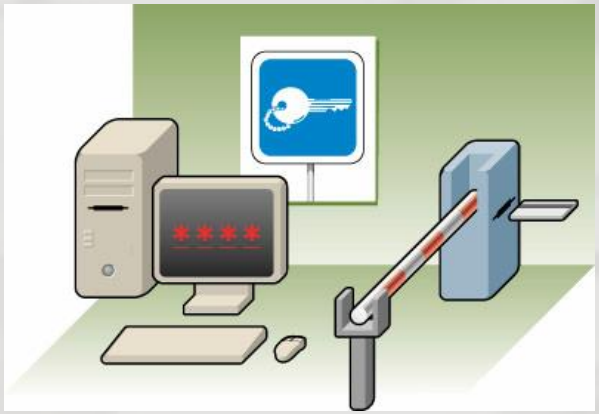
Contre-mesures techniques

A) Limitez vos droits

B) Auto-Update

C) Anti-virus

D) Personal firewall



Contre-mesures humaines

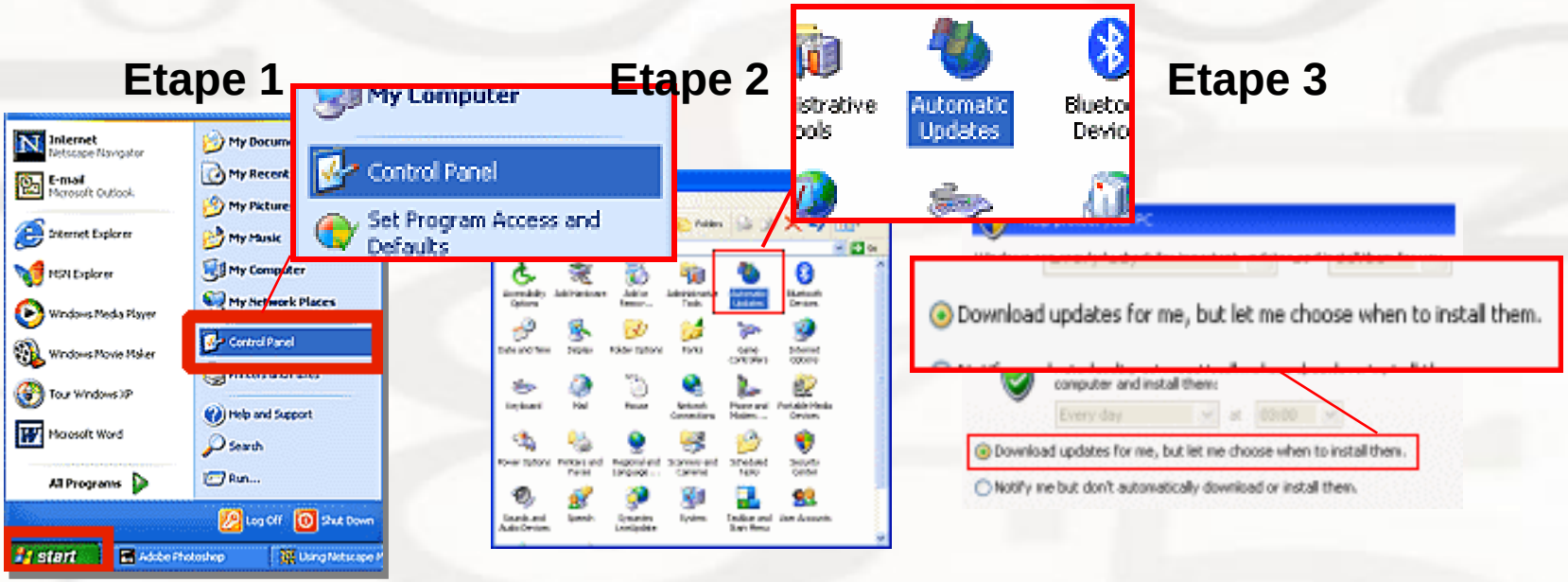
Attention aux messages d'avertissement

A) Limitez vos droits !

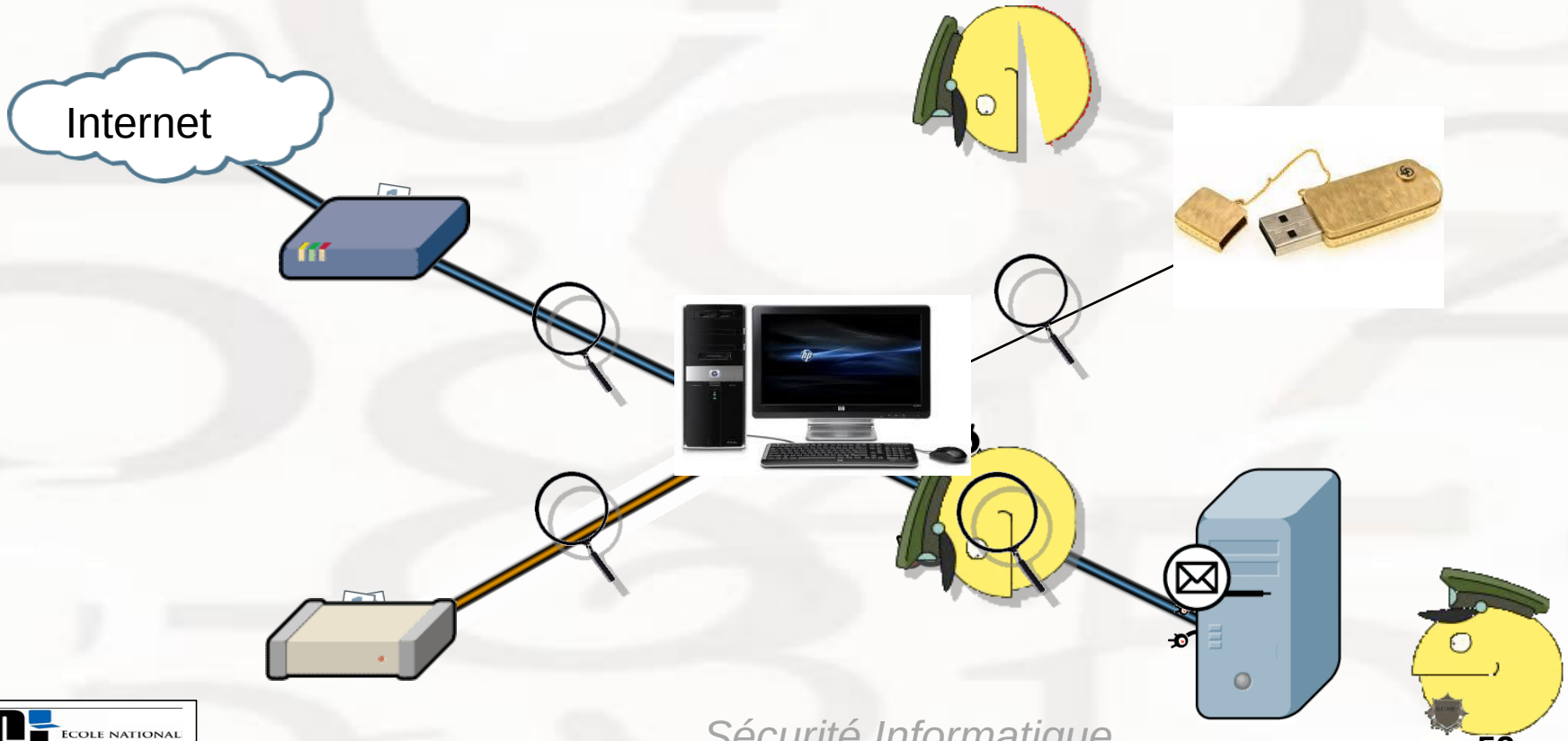
- GSM: Ne laissez pas Bluetooth allumé en permanence.
- PC: Coupez Internet si vous ne surfez pas.
- PC: Créez un utilisateur SURF avec des droits limités.

↳ Si vous êtes alors attaqué, le pirate ne peut causer que des dommages limités.

B) Activez la fonction « Automatic Updates »



C) Anti-virus



Lutte contre les malveillances informatiques

Contre-mesures techniques

D) Un *Personal firewall* Un pare feu (mur de feu)
est un logiciel qui forme une barrière impénétrable autours de l'ordinateur, il permet :

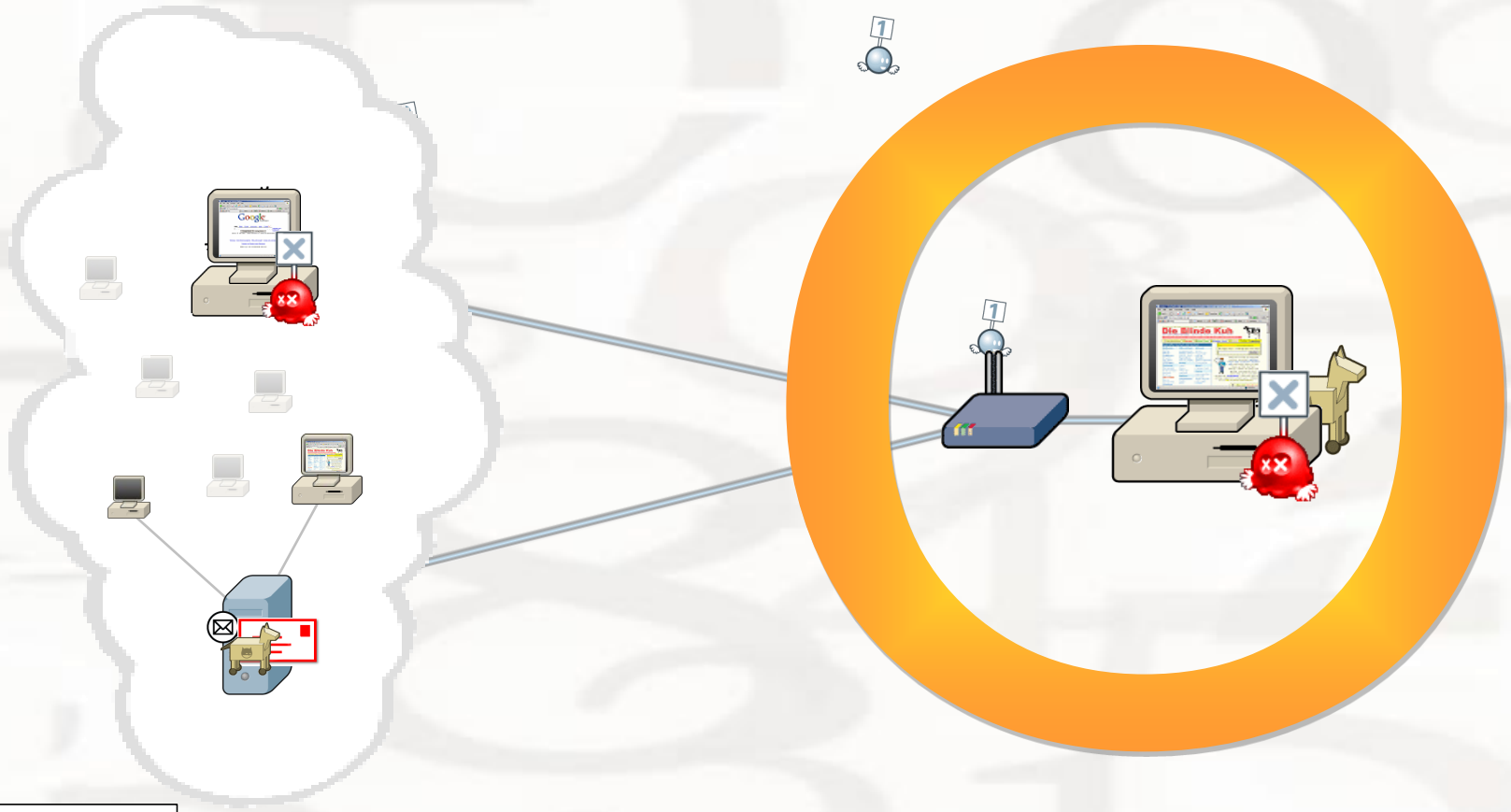
D'autoriser la connexion (*allow*) ;
De bloquer la connexion (*deny*) ;
De rejeter la demande de connexion sans avertir l'émetteur (*drop*).

1. Système proactif/réactif avec fonctions additionnelles.
2. Permets de contrôler les accès Internet de programmes spécifiques.
3. Fonctions additionnelles : Filtre de processus, Anti Spam etc.

Lutte contre les malveillances informatiques

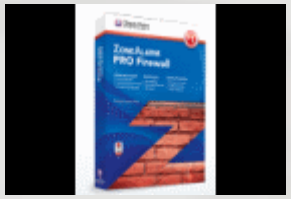
Contre-mesures techniques

- D) *Personal firewall* (le pare-feu)



Plusieurs firewall existent

1. Commerciaux.
Pratiquement tous les antivirus proposent un firewall dans le pack.



2. windows
3. Gratuit (http://www.01net.com)

Les différents niveaux de sécurité

- **Sécurité physique**

Relative à la protection des objets physiques, objets ou des zones contre tout accès non autorisé ou abus

- **Sécurité du personnel**

Relative à la protection physique des employés et à la protection du S.I. de l'entreprise contre ses employés

- **Sécurité du réseau**, pour protéger les composants du réseau, les connexions et le contenu

Les différents niveaux de sécurité

- **Sécurité de l'information**, pour protéger la **confidentialité**, **l'intégrité** et la **disponibilité** des informations actifs, que ce soit dans le stockage, le traitement ou la transmission. Il est réalisé via l'application des politiques, éducation, formation et sensibilisation, et technologie.
- **Sécurité des communications** Pour protéger les supports de communication, la technologie et le contenu
- **Sécurité des opérations**

Relative à la protection des échanges de données et des systèmes informatiques.

1.2. La politique de sécurité

1.2.1.Définition

Une **politique de sécurité informatique** est une **stratégie** visant à **maximiser** la sécurité informatique d'une entreprise. Elle est matérialisée dans un document qui reprend l'ensemble des enjeux, objectifs, analyses, actions et procédures faisant parti de cette stratégie.

- Deux philosophies pour la mise en place d'une politique :
  - Prohibitive : tout ce qui n'est pas explicitement autorisé est interdit.(institutions financières ou militaires)
  - Permissive : tout ce qui n'est pas explicitement interdit est autorisé. Ex. éducation familiale

1.2. La politique de sécurité

Nombreuses mesures possibles pour assurer la sécurité du système d'information de l'entreprise

- une bonne **maintenance du parc informatique**
- une **responsabilisation du personnel**
- la **formation du personnel** aux bonnes pratiques informatiques
- l'utilisation **d'outils** permettant d'être prêt face aux attaques informatiques (tels que **antivirus, antispam, pare-feux** etc.)
- le **contrôle des accès Internet** de l'entreprise
- le **contrôle des accès aux informations de l'entreprise**, et notamment aux **informations sensibles**
- l'hébergement des données dans des **environnements sécurisés et monitorés**
- la mise en place de **sauvegardes adaptées, sécurisées, redondées**

1.2 La politique de sécurité

1.2.2. Étapes types dans l'établissement d 'une politique de sécurité

- **Identification des vulnérabilités**
  - En mode fonctionnement normal :définir tous les points faibles
  - En cas d'apparition de défaillances (*le système est fragilisé donc vulnérable*) : c'est dans ces moments qu'une intrusion peut le plus facilement réussir
- ***Évaluation des probabilités associées à chacune des menaces***

1.2. La politique de sécurité

- 1.2.2. Étapes types dans l'établissement d 'une politique de sécurité
  - ***Évaluation du coût d'une intrusion réussie***
  - ***Choix des contre mesures***
  - ***Évaluation des coûts des contre mesures***
  - ***Décision***

1.2. La politique de sécurité

- La sécurisation des informations d'une organisation n'est pas seulement une question technique
  - Les activités techniques ne sont qu'un aspect d'une démarche qui se doit être globale.
  - Avant toute mise en place de procédures visant à améliorer la sécurité d'un organisme, il faut procéder à une analyse des risques et de rédiger une politique de sécurité.

1.3. MÉTHODE D'ANALYSE DES RISQUES

- Quelques méthodes :
  - EBIOS (Expressions des Besoins et Identification des Objectifs de Sécurité) http://www.ssi.gouv.fr/fr/conance/ebios.html
  - MEHARI (MEthode Harmonisée d'Analyse de Risques) http://www.clusif.asso.fr/fr/production/mehari
  - Critères Communs http://www.commoncriteriaportal.org
  - La norme ISO 17799 Présentation: http://www.clusif.asso.fr/fr/production/ouvrages/pdf/Presentation-ISO17799-2005.pdf

License Pro Introduction à la sécurité informatique

La politique de sécurité

- Composantes d'une politique de sécurité
  - Politique d'achat
  - Politique de confidentialité
  - Politique d'accès
  - Politique de responsabilité
  - Politique d'authentification
  - Politique d'audit et de reporting

Les services de la sécurité

- Authentification
- Identification
- Intégrité
- Non-répudiation
- Confidentialité

Authentification

- L'authentification est la procédure qui consiste, pour un système informatique, à vérifier l'identité d'une entité afin d'autoriser l'accès de cette entité à des ressources (systèmes, réseaux, applications...).
  - L'authentification permet donc de valider l'authenticité de l'entité en question.
  - Elle protège de l'usurpation d'identité

- Les entités à authentifier peuvent être :
  - une personne
  - un programme qui s'exécute (processus)
  - une machine dans un réseau (serveur ou routeur)

Authentification

- Dans le cas d'un utilisateur, l'authentification consiste, en général, à vérifier que celui-ci possède une preuve de son identité ou de son statut, sous l'une des formes (éventuellement combinées) suivantes :
  - Ce qu'il sait (mot de passe, code PIN).
  - Ce qu'il possède (carte à puce, certificat électronique).
  - Ce qu'il est (caractéristique physique, voir biométrie).
  - Ce qu'il sait faire (geste, signature).

- La phase de vérification fait intervenir un protocole d'authentification
  - **SSL/TLS** (Secure Socket Layer)/(Transport Layer Security): Crée un canal sécurisé entre deux machines: commerce électronique, etc (qui peut également fournir un service de confidentialité par chiffrement)
  - **Kerberos**, standard utilisé par Windows et Linux pour se connecter sur une machine

Authentification

- ❑ Une authentification simple est une procédure d'authentification qui requiert un seul élément ou «facteur» d'authentification valide pour permettre l'accès à une ressource.
  - ❖ Ex. login/password sur Linux
- ❑ Une authentification forte est une procédure d'authentification qui requiert au moins deux éléments ou «facteurs» d'authentification valides pour permettre l'accès à une ressource
  - ❖ Ex. carte bancaire (1.être en possession de la carte; 2.connaître le PIN)

Authentification

- Une authentification mutuelle impose une double authentification entre les deux entités

Identification

- L'authentification peut inclure une phase d'identification, au cours de laquelle l'entité indique son identité.
  Cependant, cela n'est pas obligatoire ; il est en effet possible d'avoir des entités munies de droits d'accès mais restant anonymes.

- L'identification permet donc de *connaitre l'identité d'une* entité alors que l'authentification permet de *vérifier cette* identité

Intégrité et Non-répudiation

- L'intégrité des données consiste à vérifier qu'elles n'ont pas été altérées accidentellement ou frauduleusement au cours de leur transmission ou de leur stockage.
  - Ce principe regroupe un ensemble de fonctionnalités mises en œuvre afin de s'assurer de leur intégrité, comme les fonctions de hachage

- Un mécanisme de non-répudation permet d'empêcher à une personne de nier le fait qu'elle a effectué une opération (exemple : envoi d'un message, passage d'une commande).
  - Pour assurer la non-répudiation d'un message, on peut, par exemple, utiliser la signature électronique.

Confidentialité

- La confidentialité est la propriété qui assure qu'une information ne peut être lue que par des entités habilitées (selon des contraintes précises)
  - Le chiffrement (cryptage) est le procédé grâce auquel on peut rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement.
  - On distingue deux familles de systèmes de chiffrement :
    - Chiffrement symétrique ou à clé privé.
    - Chiffrement asymétrique ou à clé publique (en réalité utilisant une paire de clés)

- CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS
www.clusif.asso.fr
- LA SÉCURITÉ DE L'INFORMATION POUR TOUS
WWW.CASES.LU