



CyberEdu

La sécurité par l'enseignement supérieur des NTIC

Sensibilisation et initiation à la cybersécurité

Module 1 : notions de base

05/11/2015

Ce document pédagogique a été rédigé par un consortium regroupant des enseignants-chercheurs et des professionnels du secteur de la cybersécurité.



Il est mis à disposition par l'ANSSI sous licence Creative Commons Attribution 3.0 France.



CyberEdu

La sécurité par l'enseignement supérieur des NTIC

Plan du module

- 1. Les enjeux de la sécurité des S.I.**
- 2. Les besoins de sécurité**
- 3. Notions de vulnérabilité, menace, attaque**
- 4. Panorama de quelques menaces**
- 5. Le droit des T.I.C. et l'organisation de la sécurité en France**



CyberEdu

La sécurité par l'enseignement supérieur des NTIC

1. Les enjeux de la sécurité des S.I.

- a) Préambule
- b) Les enjeux
- c) Pourquoi les pirates s'intéressent aux S.I. ?
- d) La nouvelle économie de la cybercriminalité
- e) Les impacts sur la vie privée
- f) Les infrastructures critiques
- g) Quelques exemples d'attaques

1. Les enjeux de la sécurité des S.I.

a. Préambule

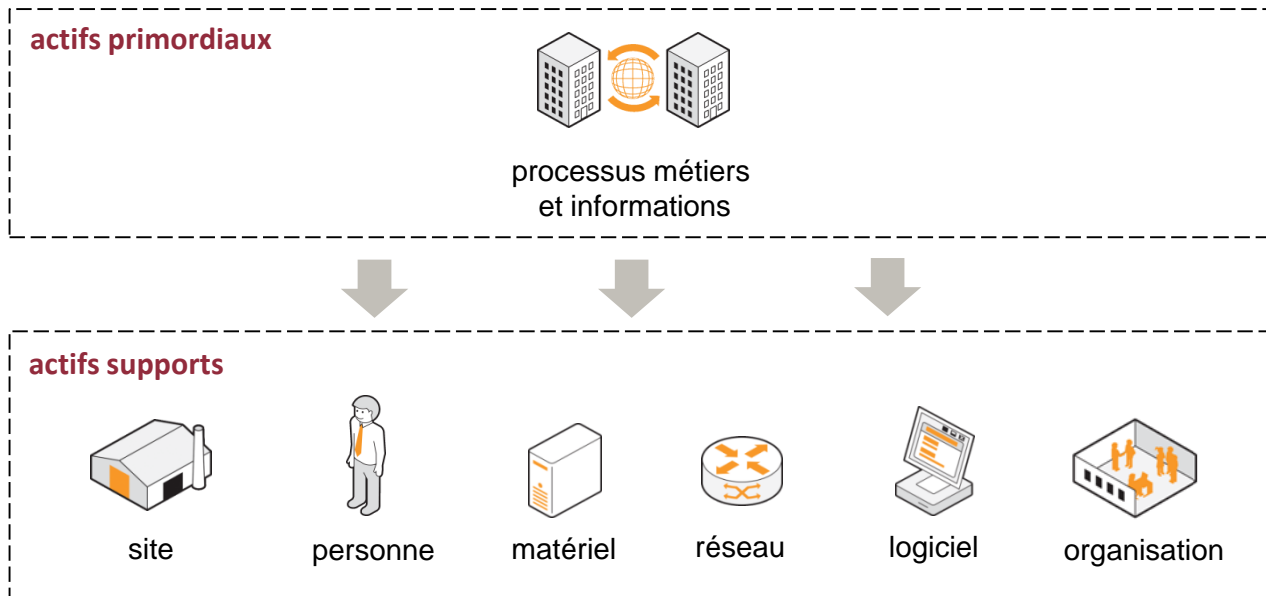
- Système d'Information (S.I.)
 - Ensemble des ressources destinées à **collecter, classifier, stocker, gérer, diffuser les informations** au sein d'une organisation
 - Mot clé : information, c'est le « nerf de la guerre » pour toutes les entreprises, administrations, organisations, etc.

Le S.I. doit permettre et faciliter la mission de l'organisation

1. Les enjeux de la sécurité des S.I.

a. Préambule

- Le système d'information d'une organisation contient un ensemble d'actifs :



Organisation
Internationale de
Normalisation

ISO/IEC 27005:2008

**La sécurité du S.I. consiste donc à assurer
la sécurité de l'ensemble de ces biens**

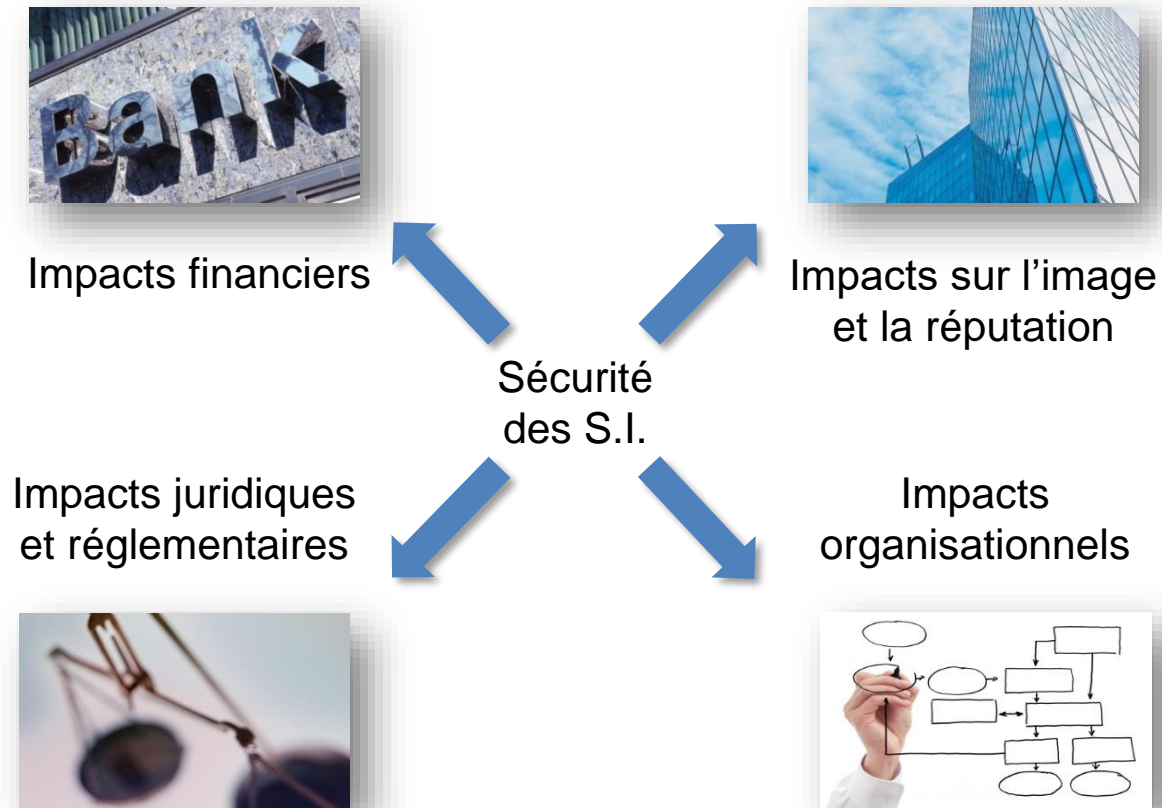
1. Les enjeux de la sécurité des S.I.

b. Les enjeux

- La sécurité a pour objectif de **réduire les risques** pesant sur le système d'information, pour **limiter leurs impacts** sur le fonctionnement et les activités métiers des organisations...
- La gestion de la sécurité au sein d'un système d'information n'a pas pour objectif de faire de l'obstruction. Au contraire :
 - Elle **contribue à la qualité de service que les utilisateurs** sont en droit d'attendre
 - Elle **garantit au personnel le niveau de protection** qu'ils sont en droit d'attendre

1. Les enjeux de la sécurité des S.I.

b. Les enjeux



1. Les enjeux de la sécurité des S.I.

c. Pourquoi les pirates s'intéressent-ils aux S.I. des organisations ou au PC d'individus ?

- Les motivations évoluent
 - Années 80 et 90 : beaucoup de bidouilleurs enthousiastes
 - De nos jours : majoritairement des actions organisées et réfléchies
- Cyber délinquance
 - Les individus attirés par l'appât du gain
 - Les « hacktivistes »
 - Motivation politique, religieuse, etc.
 - Les concurrents directs de l'organisation visée
 - Les fonctionnaires au service d'un état
 - Les mercenaires agissant pour le compte de commanditaires
 - ...

1. Les enjeux de la sécurité des S.I.

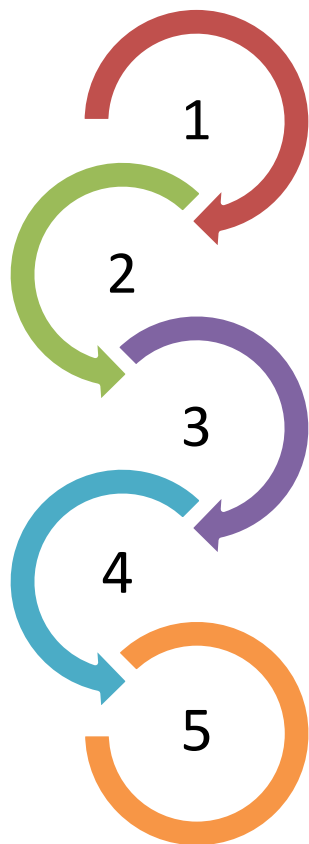
c. Pourquoi les pirates s'intéressent-ils aux S.I. des organisations ou au PC d'individus ?

- **Gains financiers** (accès à de l'information, puis monétisation et revente)
 - Utilisateurs, emails
 - Organisation interne de l'entreprise
 - Fichiers clients
 - Mots de passe, N° de comptes bancaire, cartes bancaires
- **Utilisation de ressources** (puis revente ou mise à disposition en tant que « service »)
 - Bande passante & espace de stockage (hébergement de musique, films et autres contenus)
 - Zombies (botnets)
- **Chantage**
 - Déni de service
 - Modifications des données
- **Espionnage**
 - Industriel / concurrentiel
 - Étatique
- ...

1. Les enjeux de la sécurité des S.I.

d. La nouvelle économie de la cybercriminalité

- Une majorité des actes de délinquance réalisés sur Internet sont commis par des groupes criminels organisés, professionnels et impliquant de nombreux acteurs



des groupes spécialisés dans le **développement de programmes malveillants** et virus informatiques

des groupes en charge de l'**exploitation et de la commercialisation** de services permettant de réaliser des attaques informatiques

un ou plusieurs **hébergeurs** qui stockent les contenus malveillants, soit des hébergeurs malhonnêtes soit des hébergeurs victimes eux-mêmes d'une attaque et dont les serveurs sont contrôlés par des pirates

des groupes en charge de la **vente des données volées**, et principalement des données de carte bancaire

des **intermédiaires financiers** pour collecter l'argent qui s'appuient généralement sur des réseaux de **mules**

1. Les enjeux de la sécurité des S.I.

d. La nouvelle économie de la cybercriminalité

- Quelques chiffres pour illustrer le marché de la cybercriminalité...

de **2 à 10 \$**

le prix moyen de commercialisation des **numéros de cartes bancaires** en fonction du pays et des plafonds

5 \$

le tarif moyen de location pour 1 heure d'un **botnet**, système permettant de saturer un site internet

2.399 \$

le prix de commercialisation du **malware** « Citadel » permettant d'intercepter des numéros de carte bancaire (+ un abonnement mensuel de 125 \$)

1. Les enjeux de la sécurité des S.I.

e. Les impacts de la cybercriminalité sur la vie privée (quelques exemples)

- **Impact sur l'image / le caractère / la vie privée**

- Diffamation de caractère
- Divulgence d'informations personnelles
- Harcèlement / cyber-bullying

- **Usurpation d'identité**

- « Vol » et réutilisation de logins/mots de passe pour effectuer des actions au nom de la victime

- **Perte définitive de données**

- malware récents (rançongiciel) : données chiffrées contre rançon
- connexion frauduleuse à un compte « cloud » et suppression malveillante de l'ensemble des données

- **Impacts financiers**

- N° carte bancaire usurpé et réutilisé pour des achats en ligne
- Chantage (divulgence de photos ou d'informations compromettantes si non paiement d'une rançon)



Ces impacts – non exhaustifs – ne signifient pas qu'il ne faut pas utiliser Internet, loin de là !

Il faut au contraire apprendre à anticiper ces risques et à faire preuve de discernement lors de l'usage d'Internet/smartphones...

1. Les enjeux de la sécurité des S.I.

e. Les impacts de la cybercriminalité sur les infrastructures critiques

- Infrastructures critiques = un ensemble d'organisations parmi les secteurs d'activité suivants, et que l'État français considère comme étant tellement critiques pour la nation que des mesures de sécurité particulières doivent s'appliquer
 - Secteurs étatiques : civil, justice, militaire...
 - Secteurs de la protection des citoyens : santé, gestion de l'eau, alimentation
 - Secteurs de la vie économique et sociale : énergie, communication, électronique, audiovisuel, information, transports, finances, industrie.
- Ces organisations sont classées comme **Opérateur d'Importance Vitale (OIV)**. La liste exacte est classifiée (donc non disponible au public).

1. Les enjeux de la sécurité des S.I.

g. Quelques exemples d'attaques



Actualités > Société

Une panne réseau a cloué au sol les avions d'American Airlines

Près de 670 vols ont été annulés hier, en raison d'un problème d'accès au système de réservation. La compagnie s'est appuyée sur les réseaux sociaux pour informer ses clients.



Gilbert Kallenborn, avec AFP | 01net | le 17/04/13 à 11h23 | laisser un avis

Tweet +1 5

Panne informatique à l'hôpital de

En l'espace de deux jours, mercredi et jeudi, l'accueil aux urgences de a été très perturbé. Il a fallu diriger les patients vers d'autres hôpitaux.

Publié le 10.01.2009

Copé, Hortefeux, Dassault... leurs messageries Orange piratées

par Emilien Ercolani, le 07 mai 2013 15:04 ★★★★★

Les messageries des téléphones portables de plusieurs personnalités politiques (JF Copé, B Hortefeux) ou industrielles (la famille Dassault) ont été piratées plusieurs semaines durant. Des plaintes ont été déposées, alors qu'Orange a lancé une enquête interne.

Publié le 13 avril 2014 à 12h24 | Mis à jour le 13 avril 2014 à 12h24

Le centre allemand de recherche spatiale cible d'une cyberattaque

Agence France-Presse

Le centre allemand de recherche aéronautique et spatiale (DLR) a été la cible il y a quelques mois d'une cyberattaque présumée par un service de renseignements étranger, affirme le magazine Der Spiegel dimanche.

Des machines à sous vidées à cause d'une faille informatique

Le Monde.fr | 15.04.2014 à 09h09 • Mis à jour le 15.04.2014 à 10h46

Abonnez-vous à partir de 1 € Réagir Classer Partager



Ukraine : le mystérieux virus Snake infecte les ordinateurs du gouvernement

Publié le 08.03.2014, 16h50 | Mise à jour : 17h23

Recommander 52 personnes le recommandent. Inscription pour ce que vos amis recommandent. 64 +1 Share



Illustration. Un mystérieux virus a été réactivé ces derniers jours et vise les ordinateurs ukrainiens. | L.P. / Olivier Arandjel

1. Les enjeux de la sécurité des S.I.

g. Quelques exemples d'attaques



Bug informatique à La Poste : "Tout est rentré dans l'ordre"



par Caroline Piquet
le 30 juillet 2013 à 15h50 , mis à jour le 30 juillet 2013 à 18h59.

A la suite d'une panne informatique, les opérations de prélèvements et de virements bancaires accusent un retard de 24 heures. Ce mardi, les clients ne pouvaient accéder à leurs soldes sur Internet et il leur était impossible de retirer de l'argent aux distributeurs automatiques.

Hacker un pacemaker, c'est possible et c'est dangereux

10:12 - vendredi 19 octobre 2012 - Par Johann Mise - Source : France Info



Une panne informatique paralyse Wall Street pendant 3 heures

Edité par MYTF1News avec AFP
le 23 août 2013 à 06h50 , mis à jour le 23 août 2013 à 07h02.

Help! My fridge is full of spam and so is my router, set-top box and console
Security company says it discovered spam and phishing campaign run over Christmas, which involved internet fridge

Charles Arthur
Follow @charlesarthur Follow @guardiantech
theguardian.com, Tuesday 21 January 2014 11.40 GMT
Jump to comments (19)



Un avion espion « plante » le système informatique d'un aéroport

Par Pierre Dandumont 5 MAI 2014 12:30 - Source: NBC News | 0 COMMENTAIRE

Gibraltar: un incendie interrompt des services de paris en ligne

AFP, 20/04 23:31 CET



1. Les enjeux de la sécurité des S.I.

Sony Pictures Entertainment



« Si vous n'obéissez pas, nous publierons au monde les informations suivantes ». Ce message était affiché sur plusieurs ordinateurs de Sony Pictures Entertainment le 24 nov 2014

- GOP pour Guardian of Peace
- Des données internes ont été publiées contenant :
 - les numéros de sécurité sociale et les numérisations de passeport appartenant aux acteurs et directeurs.
 - des mots de passe internes
 - des scripts non publiés
 - des plans marketing
 - des données légales et financières
 - et 4 films entiers inédits
- La probabilité de vol d'identité est très forte désormais pour les personnes dont les informations ont été publiées.
- Les studios concurrents de Sony, ont une visibilité sur les plans stratégiques de Sony.

**La source de l'attaque reste à déterminer.
La Corée du Nord est soupçonnée d'être à l'origine de l'attaque.**

1. Les enjeux de la sécurité des S.I.

Vols de données en 2014

- L'année 2014 a été l'année de tous les records en matière de fuite de données.
- Infographie réalisée par www.silicon.fr



1. Les enjeux de la sécurité des S.I.

Quelques exemples d'attaques ciblant l'enseignement



Forum Général
Forum ForEva
Contacts

Espace étudiants

Ce Forum est un espace ouvert de communication entre étudiants, tuteurs, moniteurs et enseignants pour discuter des cours, des exercices, des travaux pratiques.

> **Poster un nouveau message** <

Liste des messages postés

pages 1 2 3 4 5 6 7 8 9 10

HACKED BY SWAN HACKED BY SWAN
HACKED BY SWAN HACKED BY SWAN
HACKED BY SWAN HACKED BY SWAN

Défacement de site

Vol de données personnelles

TheWMURChannel.com

Dartmouth Computer Hackers

POSTED: 4:07 PM EDT August 1, 2004

HANOVER, NH -- Hackers hit the computer system at Dartmouth College last week and got access to sensitive information about thousands of employees and students.

Larry Levine, Dartmouth's chief information officer, said he did not know for sure what the hackers' purpose was. He said one of the compromised computer servers contained information on college employees, retired employees and their families. Other servers involved contained research data and staff and student immunization information.

1. Les enjeux de la sécurité des S.I.

Quelques exemples d'attaques ciblant l'enseignement

Click2Houston.com

Police: Student Installs Device On Teacher's Computer To Sell Tests

Warnings Sent To Other School Districts

POSTED: 5:23 pm CST February 1, 2005
UPDATED: 5:39 pm CST February 1, 2005

HOUSTON -- A high school student is facing criminal charges for allegedly hooking a device up to a teacher's computer to steal test information to sell to other students, Local 2 reported Tuesday.

The student attended **Clements High School**, 4200 Elkins Dr., in the **Fort Bend Independent School District**.

Officials said the 16-year-old boy hooked up a keystroke decoder to a teacher's computer and downloaded exams in November.

"Sometime in mid-December, we got a tip that this student was selling test exams that had apparently come from a teacher's computer, so that's when the investigation began," said Mary Ann Simpson, with the Fort Bend School District.

The student confessed when he was confronted, officials said.

**Vol de données
professionnelles**

Video




[See How Keystroke Decoder Works](#)

Note des lecteurs: **5.0/5**

Rebond pour fraude externe

Exclusif : Tentative de fraude bancaire via le site de l'Union françaises des Professeurs de Physique et de Chimie.

Un pirate informatique, spécialisé dans la fraude bancaire et l'**hameçonnage**  a décidé de s'attaquer aux clients de la banque en ligne EGG. Pour ce faire, l'escroc a été installer son piège directement dans le site de l'Union des Professeurs de Physique et de Chimie (udppc.asso.fr). A première vue, eux aussi auront droit à des devoirs de vacances pour bien protéger leur site Internet. (iago)

1. Les enjeux de la sécurité des S.I.

Quelques exemples d'attaques, ce qui pourrait arriver

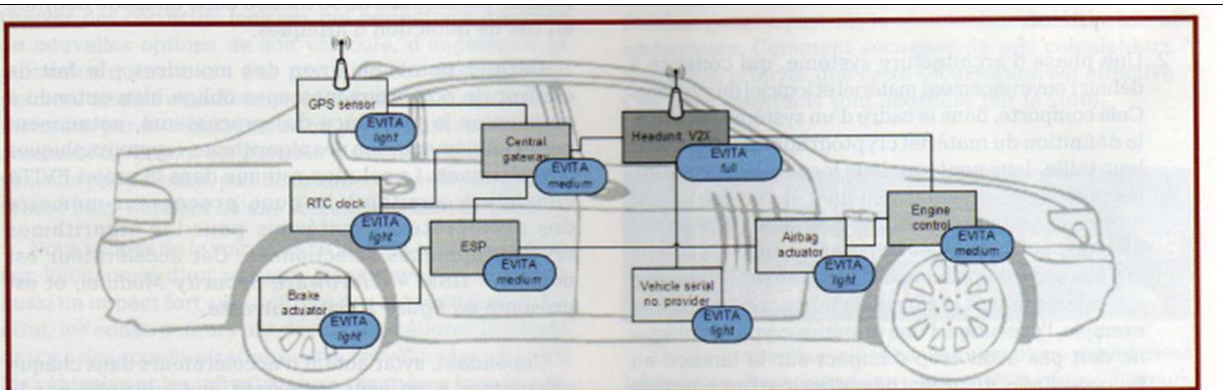
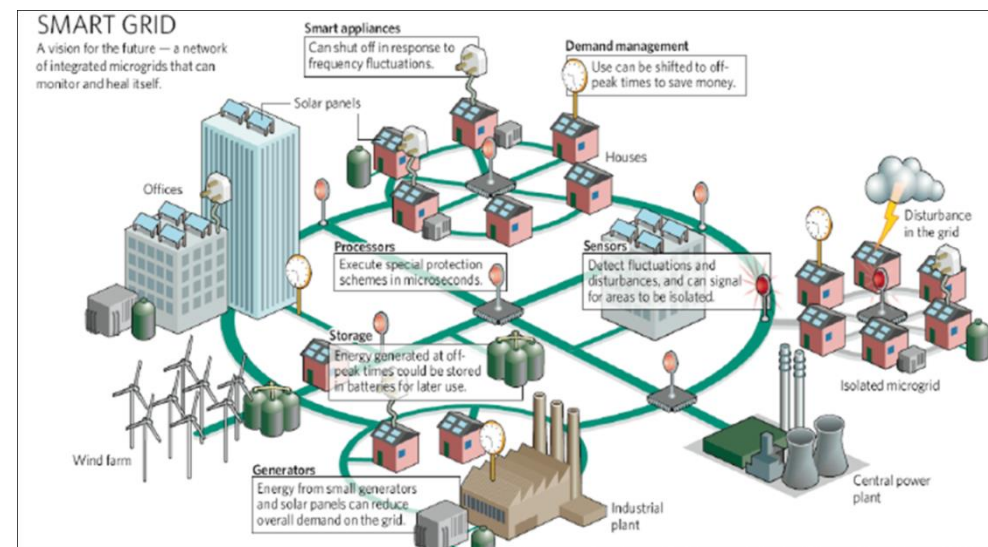


Figure 2 : Les modules de sécurité HSM sont ajoutés à tout ordinateur embarqué. Selon la nature du calculateur, une version simplifiée du HSM peut être implantée afin de réduire le coût de l'architecture.

Cyberattaques sur la voiture connectée envisagées à l'horizon 2020
Exemple : Prise de contrôle du système de frein

Déploiement des smart grid prévu à l'horizon 2030
Exemple : Blackout sur une grille.



2. Les besoins de sécurité

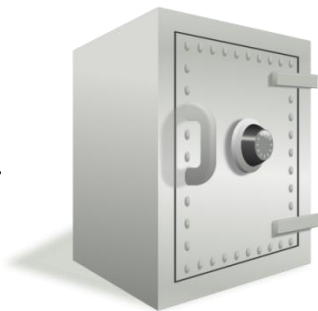
- a) Introduction aux critères DIC
- b) Besoin de sécurité : « Preuve »
- c) Différences entre sureté et sécurité
- d) Exemple d'évaluation DICP
- e) Mécanisme de sécurité pour atteindre les besoins DICP

2. Les besoins de sécurité

a. Introduction aux critères DIC

- Comment définir le niveau de sécurité d'un bien du S.I. ? Comment évaluer si ce bien est correctement sécurisé ?
- 3 critères sont retenus pour répondre à cette problématique, connus sous le nom de D.I.C.

Bien à protéger



Disponibilité

Propriété d'**accessibilité au moment voulu** des biens par les personnes autorisées (i.e. le bien doit être disponible durant les plages d'utilisation prévues)

Intégrité

Propriété d'**exactitude et de complétude** des biens et informations (i.e. une modification illégitime d'un bien doit pouvoir être détectée et corrigée)

Confidentialité

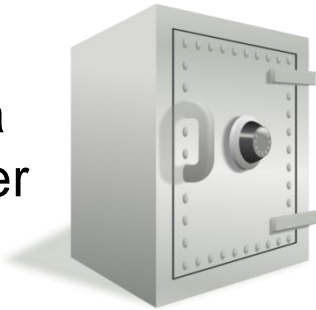
Propriété des biens de **n'être accessibles qu'aux personnes autorisées**

2. Les besoins de sécurité

b. Besoin de sécurité : « Preuve »

- Comment définir le niveau de sécurité d'un bien du S.I. ? Comment évaluer si ce bien est correctement sécurisé ?
- 1 critère complémentaire est souvent associé au D.I.C.

Bien à
protéger



Preuve

Propriété d'un bien permettant de retrouver, avec une **confiance suffisante**, les circonstances dans lesquelles ce bien évolue. Cette propriété englobe
Notamment :

La **traçabilité** des actions menées

L'**authentification** des utilisateurs

L'**imputabilité** du responsable de l'action effectuée

2. Les besoins de sécurité

c. Différences entre sûreté et sécurité

« Sûreté » et « Sécurité » ont des significations différentes en fonction du contexte. L'interprétation de ces expressions peuvent varier en fonction de la sensibilité de chacun.

Sûreté

Protection contre les dysfonctionnements et accidents involontaires

Exemple de risque : saturation d'un point d'accès, panne d'un disque, erreur d'exécution, etc.

Quantifiable statistiquement (ex. : la durée de vie moyenne d'un disque est de X milliers d'heures)

Parades : sauvegarde, dimensionnement, redondance des équipements...

Sécurité

Protection contre les actions malveillantes volontaires

Exemple de risque : blocage d'un service, modification d'informations, vol d'information

Non quantifiable statistiquement, mais il est possible d'évaluer en amont le niveau du risque et les impacts

Parades : contrôle d'accès, veille sécurité, correctifs, configuration renforcée, filtrage...*

* Certaines de ces parades seront présentées dans ce cours

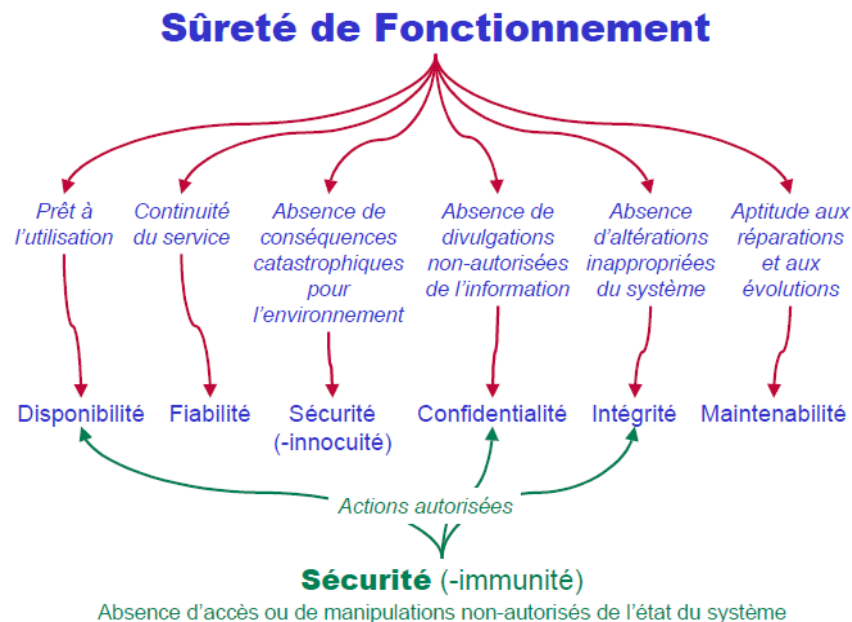
2. Les besoins de sécurité

c. Différences entre sûreté et sécurité

Sûreté : ensemble de mécanismes mis en place pour assurer la continuité de fonctionnement du système dans les conditions requises.

Sécurité : ensemble de mécanismes destinés à protéger l'information des utilisateurs ou processus n'ayant pas l'autorisation de la manipuler et d'assurer les accès autorisés.

Le périmètre de chacune des 2 notions n'est pas si clairement délimité dans la réalité : dans le cas de la voiture connectée on cherchera la sécurité et la sûreté.



On constate sur le schéma que la notion de sécurité diffère selon le contexte :

- sécurité ► innocuité
- sécurité ► immunité

2. Les besoins de sécurité

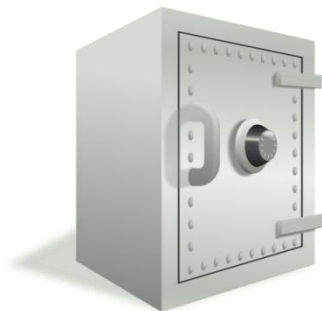
d. Exemple d'évaluation DICP

Ainsi, pour évaluer si un bien est correctement sécurisé, il faut auditer son niveau de Disponibilité, Intégrité, Confidentialité et de Preuve. L'évaluation de ces critères sur une échelle permet de déterminer si ce bien est correctement sécurisé.

L'expression du besoin attendu peut-être d'origine :

- **Interne** : inhérente au métier de l'entreprise
- ou **externe** : issue des contraintes légales qui pèsent sur les biens de l'entreprise.

Exemple des résultats d'un audit sur un bien sur une échelle (Faible, Moyen, Fort, Très fort) :



| | |
|-----------------------------------|-----------|
| Niveau de Disponibilité du bien | Très fort |
| Niveau d'Intégrité du bien | Moyen |
| Niveau de Confidentialité du bien | Très fort |
| Niveau de Preuve du bien | Faible |



Le bien bénéficie d'un niveau de sécurité adéquat

2. Les besoins de sécurité

d. Exemple d'évaluation DICP

- Tous les biens d'un S.I. n'ont pas nécessairement besoin d'atteindre les mêmes niveaux de DICP.
- Exemple avec un site institutionnel simple (statique) d'une entreprise qui souhaite promouvoir ses services sur internet :

Disponibilité = **Très fort** ✓

Un haut niveau de disponibilité du site web est nécessaire, sans quoi l'entreprise ne peut atteindre son objectif de faire connaître ses services au public

Intégrité = **Très fort** ✓

Un haut niveau d'intégrité des informations présentées est nécessaire. En effet, l'entreprise ne souhaiterait pas qu'un concurrent modifie frauduleusement le contenu du site web pour y insérer des informations erronées (ce qui serait dommageable)



Serveur
web

Confidentialité = **Faible** ✓

Un faible niveau de confidentialité suffit. En effet, les informations contenues dans ce site web sont publiques par nature!

Preuve = **Faible** ✓

Un faible niveau de preuve suffit. En effet, ce site web ne permet aucune interaction avec les utilisateurs, il fournit simplement des informations fixes.

2. Les besoins de sécurité

e. Mécanismes de sécurité pour atteindre les besoins DICP

Un Système d'Information a besoin de mécanismes de sécurité qui ont pour objectif d'assurer de garantir les propriétés DICP sur les biens de ce S.I. Voici quelques exemples de mécanismes de sécurité participant à cette garantie :

| | | D | I | C | P |
|--|--|---|---|---|---|
| Anti-virus | Mécanisme technique permettant de détecter toute attaque virale qui a déjà été identifiée par la communauté sécurité | ✓ | ✓ | ✓ | |
| Cryptographie | Mécanisme permettant d'implémenter du chiffrement et des signatures électroniques | | ✓ | ✓ | ✓ |
| Pare-feu | Équipement permettant d'isoler des zones réseaux entre-elles et de n'autoriser le passage que de certains flux seulement | ✓ | | ✓ | |
| Contrôles d'accès logiques | Mécanismes permettant de restreindre l'accès en lecture/écriture/suppression aux ressources aux seules personnes dûment habilitées | | ✓ | ✓ | ✓ |
| Sécurité physique des équipements et locaux | Mécanismes de protection destinés à protéger l'intégrité physique du matériel et des bâtiments/bureaux. | ✓ | ✓ | ✓ | |

2. Les besoins de sécurité

e. Mécanismes de sécurité pour atteindre les besoins DICP

| | | D | I | C | P |
|--|--|---|---|---|---|
| Capacité d'audit | Mécanismes organisationnels destinés à s'assurer de l'efficacité et de la pertinence des mesures mises en œuvre. Participe à l'amélioration continue de la sécurité du S.I. | ✓ | ✓ | ✓ | ✓ |
| Clauses contractuelles avec les partenaires | Mécanismes organisationnels destinés à s'assurer que les partenaires et prestataires mettent en œuvre les mesures nécessaires pour ne pas impacter la sécurité des S.I. de leurs clients | ✓ | ✓ | ✓ | ✓ |
| Formation et sensibilisation | Mécanismes organisationnels dont l'objectif est d'expliquer aux utilisateurs, administrateurs, techniciens, PDG, clients, grand public, etc. en quoi leurs actions affectent la sécurité des S.I. Diffusion des bonnes pratiques de sécurité. Le cours actuel en est une illustration ! | ✓ | ✓ | ✓ | ✓ |

Certains de ces mécanismes seront présentés dans le cadre cette sensibilisation à la cybersécurité



CyberEdu

La sécurité par l'enseignement supérieur des NTIC

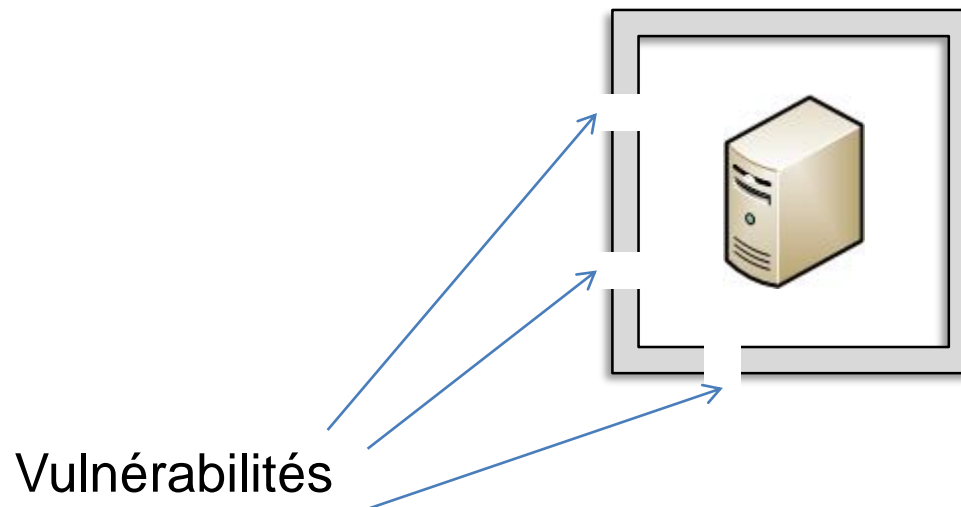
3. Notions de vulnérabilité, menace, attaque

- a) Notion de « Vulnérabilité »
- b) Notion de « Menace »
- c) Notion d'« Attaque »
- d) Exemple de vulnérabilité lors de la conception d'une application
- e) Illustration d'un usage normal de l'application vulnérable
- f) Illustration de l'exploitation de la vulnérabilité présente dans l'application

3. Notions de vulnérabilité, menace, attaque

a. Notion de « Vulnérabilité »

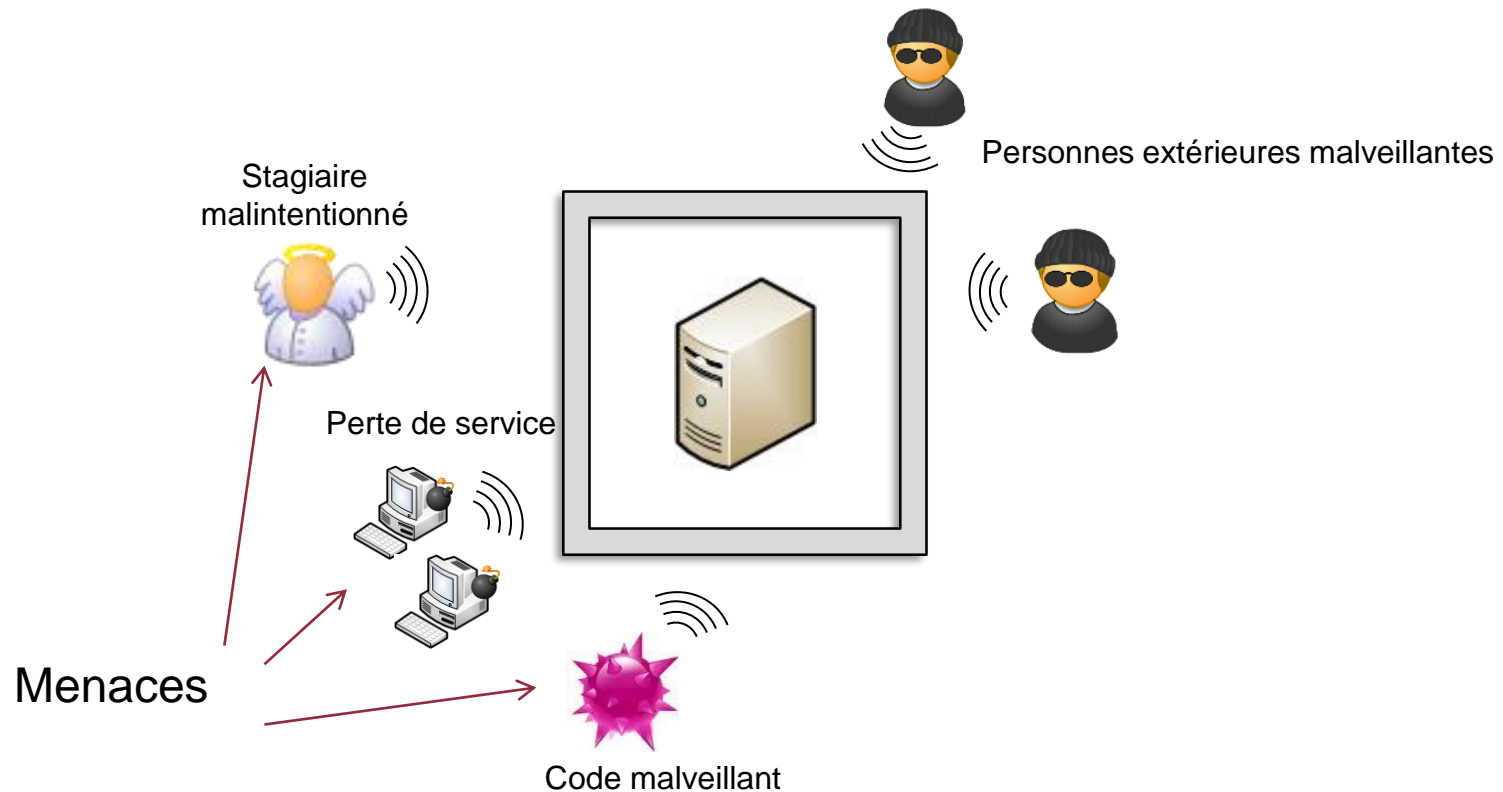
- **Vulnérabilité**
- **Faiblesse au niveau d'un bien** (au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation du bien).



3. Notions de vulnérabilité, menace, attaque

b. Notion de « Menace »

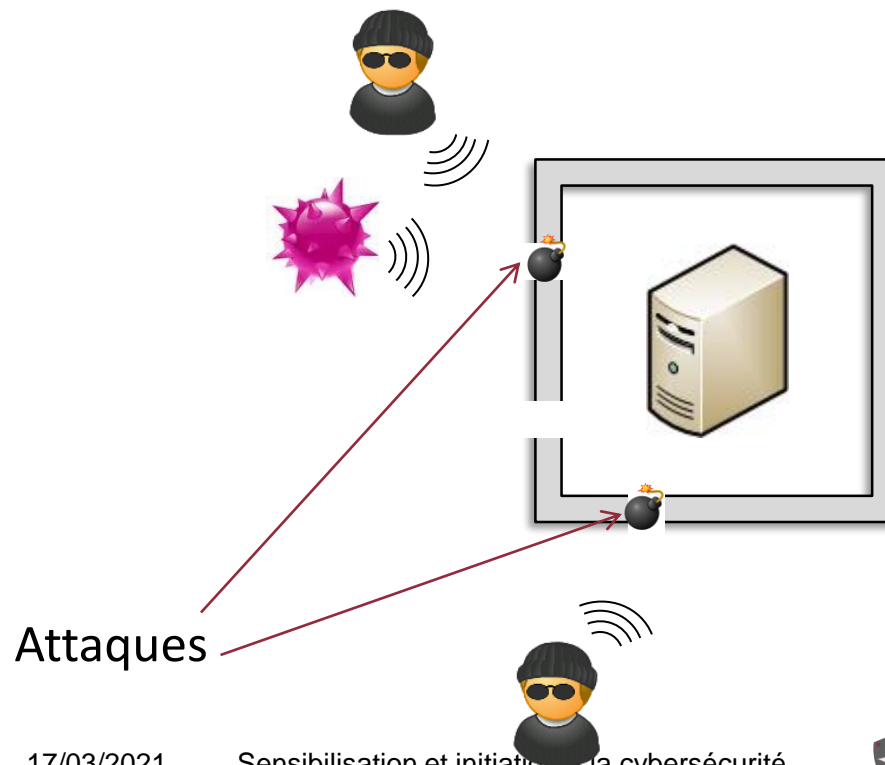
- **Menace**
- **Cause potentielle d'un incident**, qui pourrait entraîner des dommages sur un bien si cette menace se concrétisait.



3. Notions de vulnérabilité, menace, attaque

c. Notion d'« Attaque »

- **Attaque**
- **Action malveillante** destinée à porter atteinte à la sécurité d'un bien. Une attaque représente la **concrétisation d'une menace**, et nécessite l'**exploitation d'une vulnérabilité**.



3. Notions de vulnérabilité, menace, attaque

c. Notion d'« Attaque »

- **Attaque**
- Une attaque ne peut donc avoir lieu (et réussir) que si le bien est affecté par une vulnérabilité.



Ainsi, tout le travail des experts sécurité consiste à s'assurer que le S.I. ne possède aucune vulnérabilité.

Dans la réalité, l'objectif est en fait d'être en mesure de maîtriser ces vulnérabilités plutôt que de viser un objectif 0 inatteignable.

3. Notions de vulnérabilité, menace, attaque

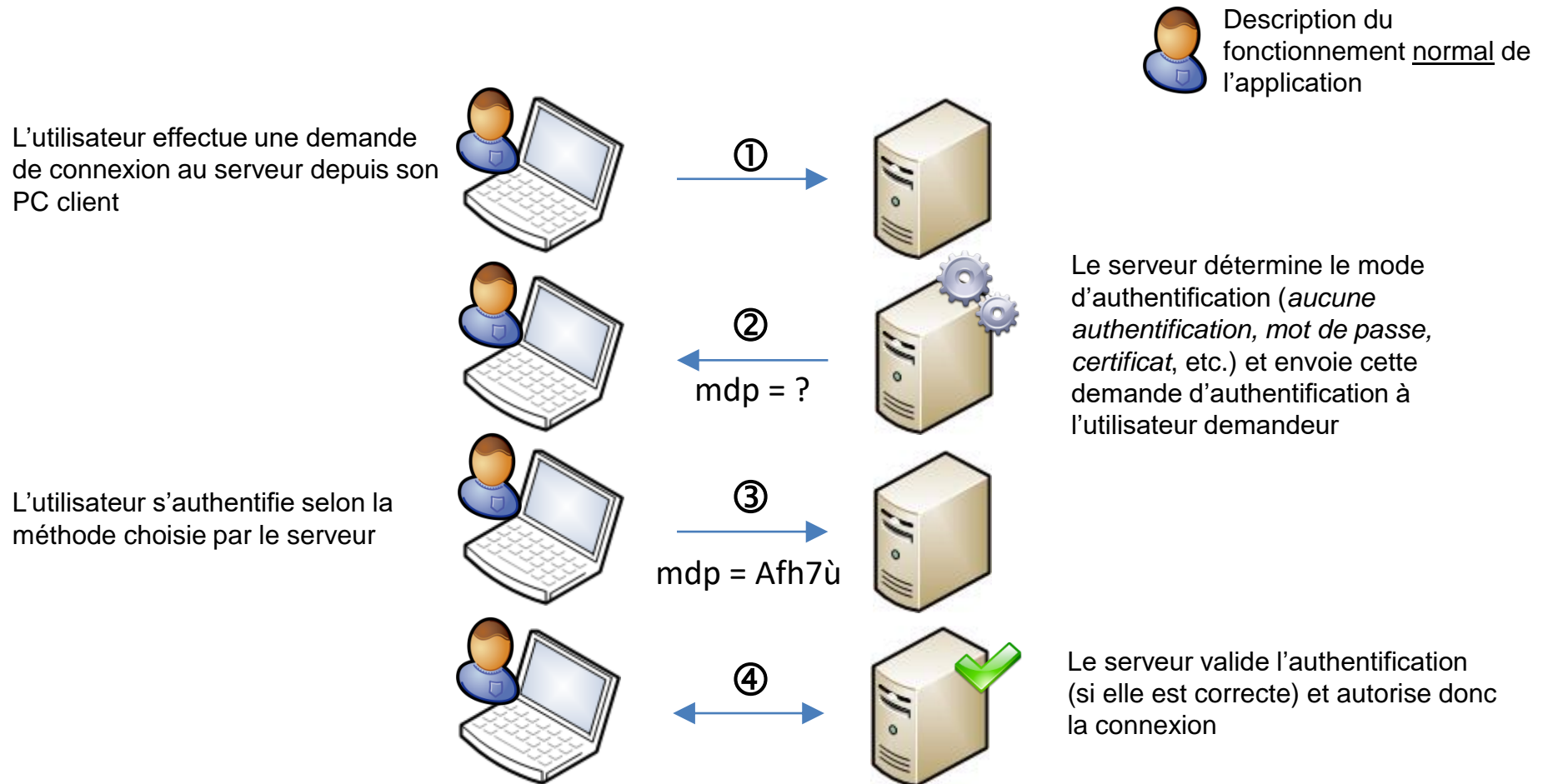
d. Exemple de vulnérabilité : Contournement de l'authentification dans l'application VNC

L'application VNC permet à un utilisateur de prendre en main sur une machine distance, après qu'il se soit authentifié.

- La vulnérabilité décrite dans les planches suivantes est corrigée depuis de nombreuses années. Elle est symptomatique d'une **vulnérabilité dans la conception d'une application** ;
- L'application permet en temps normal à un utilisateur de se connecter à distance sur une machine pour y effectuer un « partage de bureau » (i.e. pour travailler à distance sur cette machine) ;
- En 2006, il est découvert que cette application – utilisée partout dans le monde depuis de très nombreuses années – présente une vulnérabilité critique : il est possible de se connecter à distance sur cette application **sans avoir besoin de s'authentifier** (i.e. tout utilisateur sur internet peut se connecter à distance sur les systèmes en question) ;
- Le diaporama suivant illustre la **vulnérabilité technique** sous-jacente à ce comportement.

3. Notions de vulnérabilité, menace, attaque

e. Illustration d'un usage normal de l'application vulnérable



3. Notions de vulnérabilité, menace, attaque

f. Illustration de l'exploitation de la vulnérabilité présente dans l'application

L'attaquant effectue une demande de connexion au serveur depuis son PC client



①



Description du fonctionnement modifié par un attaquant

L'attaquant choisit de s'authentifier avec le mécanisme de son choix, et non pas avec le mécanisme choisi par le serveur. Ici il choisit la méthode « pas d'authentification »



②

mdp = ?



Le serveur détermine le mode d'authentification (*aucune authentification, mot de passe, certificat, etc.*) et envoie cette demande d'authentification à l'utilisateur demandeur



③

authent = NON



④



Le serveur valide l'authentification (car elle est valide i.e. aucune authentification est une méthode valide) et autorise donc la connexion

Référence : CVE-2006-2369

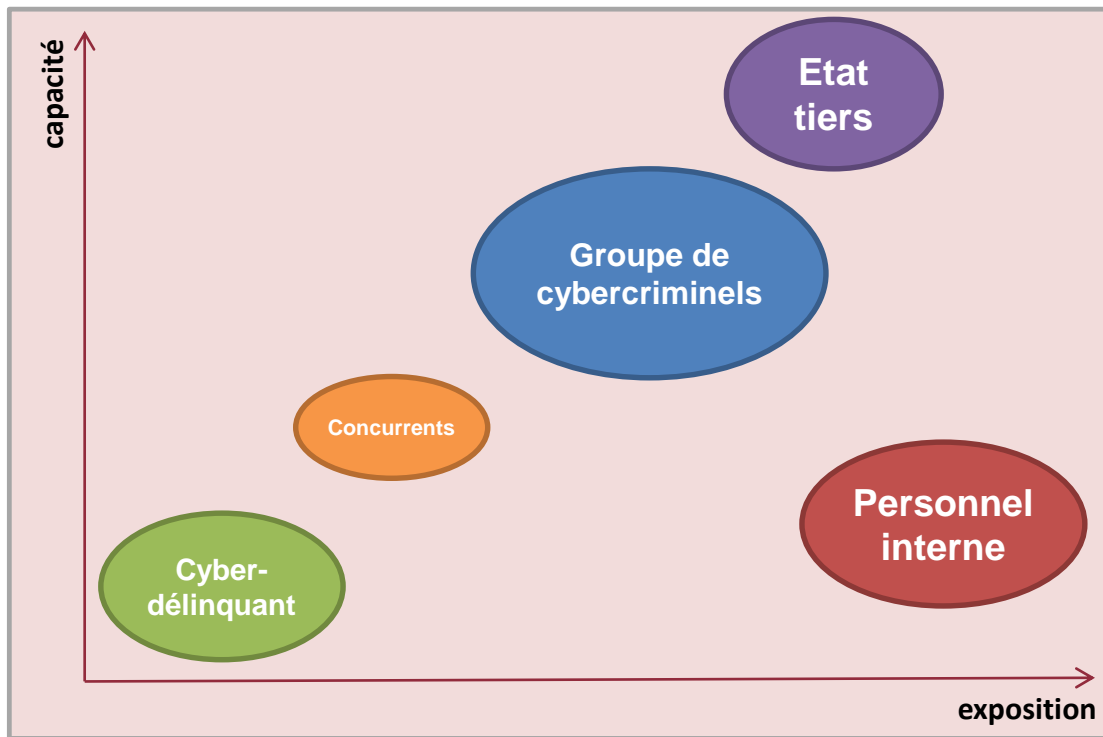
La vulnérabilité se situe ici : le serveur ne vérifie pas que le type d'authentification retourné par le client correspond à celui demandé. A la place, il vérifie simplement que l'authentification est correcte (et « authent = NON » est effectivement une authentification qui est toujours correcte)

4. Panorama de quelques menaces

- a) Les sources potentielles de menaces
- b) Panorama de quelques menaces
- c) Hameçonnage & ingénierie sociale
- d) Déroulement d'une attaque avancée
- e) Violation d'accès non-autorisé
- f) Fraude interne
- g) Virus informatique
- h) Déni de service Distribué (DDoS)
- i) Illustration d'un réseau de botnets

4. Panorama de quelques menaces

a. Sources potentielles de menaces



Exemple d'une cartographie des principales sources de menaces qui pèsent sur un S.I.

Capacité

degré d'expertise et ressources de la source de menaces

Exposition

opportunités et intérêts de la source de menaces

Attention : cette cartographie doit être individualisée à chaque organisation car toutes les organisations ne font pas face aux mêmes menaces.

Exemple : le S.I. d'une administration d'état ne fait pas face aux mêmes menaces que le S.I. d'un e-commerce ou d'une université

4. Panorama de quelques menaces

b. Panorama de quelques menaces

**Hameçonnage &
ingénierie sociale**

Fraude interne

**Violation d'accès
non autorisé**

Virus informatique

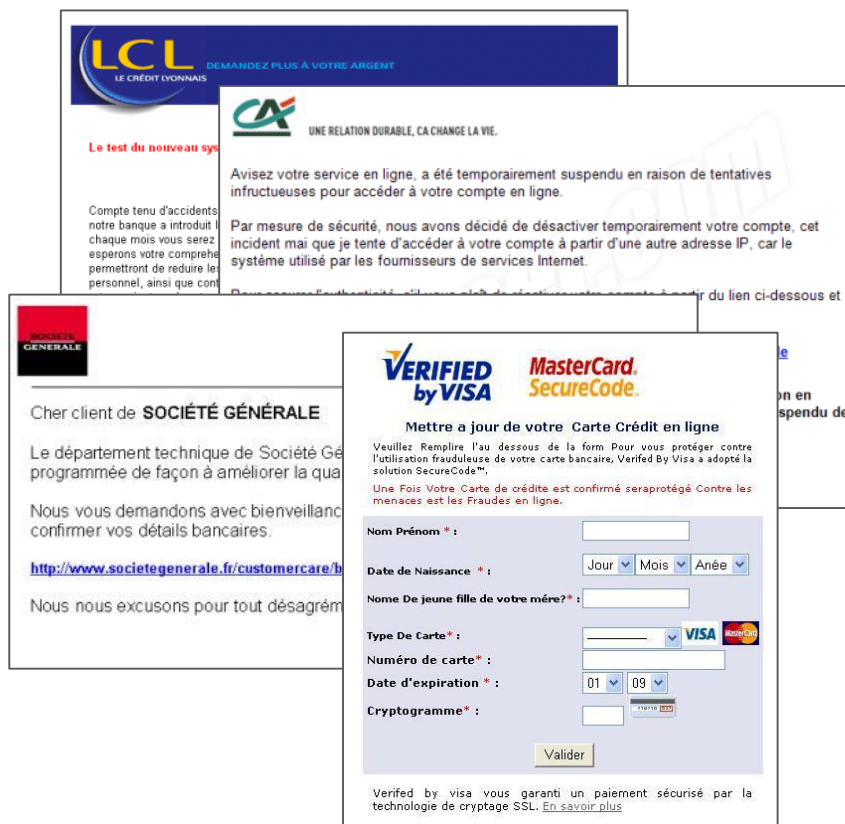
**Déni de service
distribué**

4. Panorama de quelques menaces

c. Hameçonnage & ingénierie sociale

L'hameçonnage (anglais : « **phishing** ») constitue une « attaque de masse » qui vise à abuser de la « naïveté » des clients ou des employés pour récupérer leurs identifiants de banque en ligne ou leurs numéros de carte bancaire...

- 1 Réception d'un mail utilisant le logo et les couleurs de l'entreprise
- 2 Demande pour effectuer une opération comme la mise-à-jour des données personnelles ou la confirmation du mot de passe
- 3 Connexion à un faux-site identique à celui de l'entreprise et contrôlé par l'attaquant
- 4 Récupération par l'attaquant des identifiants/mots de passe (ou tout autre donnée sensible) saisie par le client sur le faux site



4. Panorama de quelques menaces

c. Hameçonnage & ingénierie sociale

L'« **ingénierie sociale** » constitue une « attaque ciblée » qui vise à abuser de la « naïveté » des employés de l'entreprise :

- pour dérober directement des informations confidentielle, ou
- pour introduire des logiciels malveillants dans le système d'information de la banque



par téléphone



par réseaux
sociaux



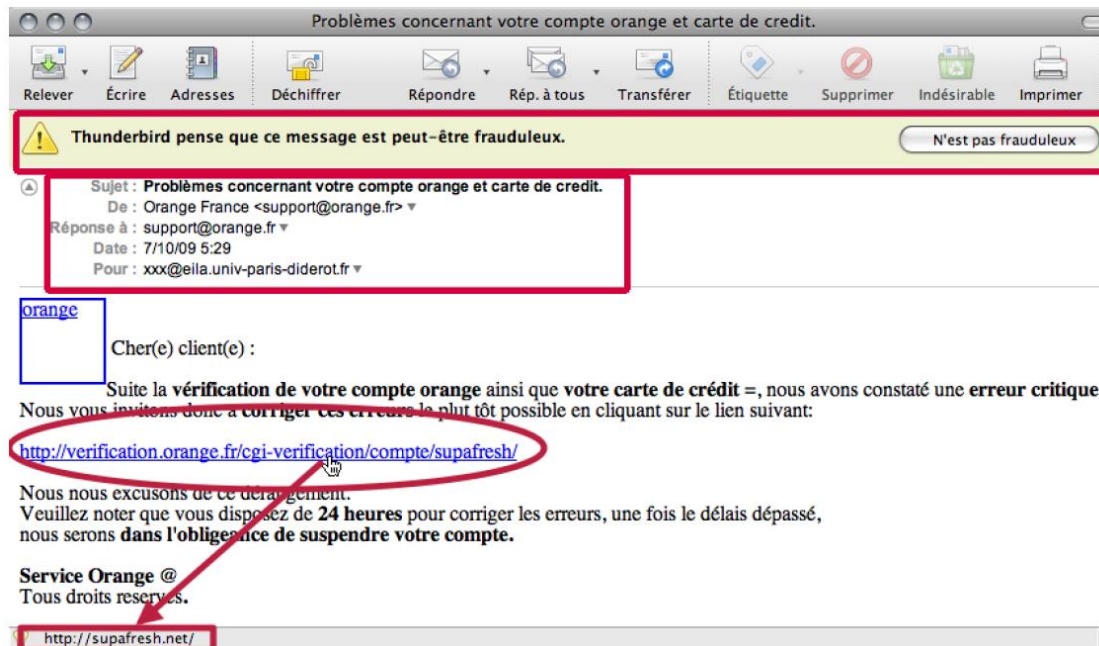
par e-mail

les scénarios d'ingénierie sociale sont illimités, avec pour seules limites l'imagination des attaquants et la naïveté des victimes...

4. Panorama de quelques menaces

c. Hameçonnage & ingénierie sociale

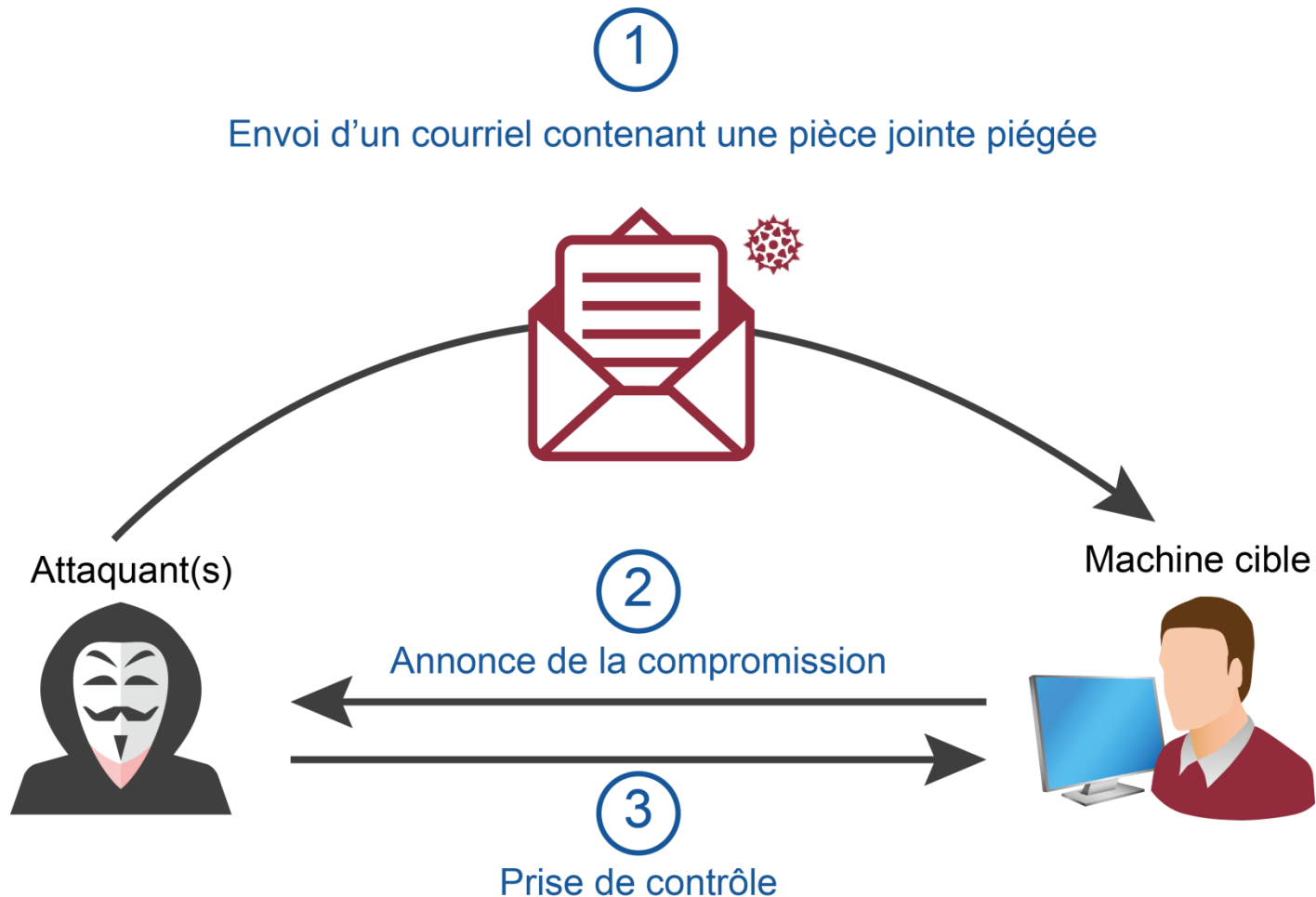
Exemple de *phishing* ciblant les employés d'un grand groupe français...



Ce lien pointe en fait vers un site frauduleux, et non pas vers un serveur légitime de l'entreprise

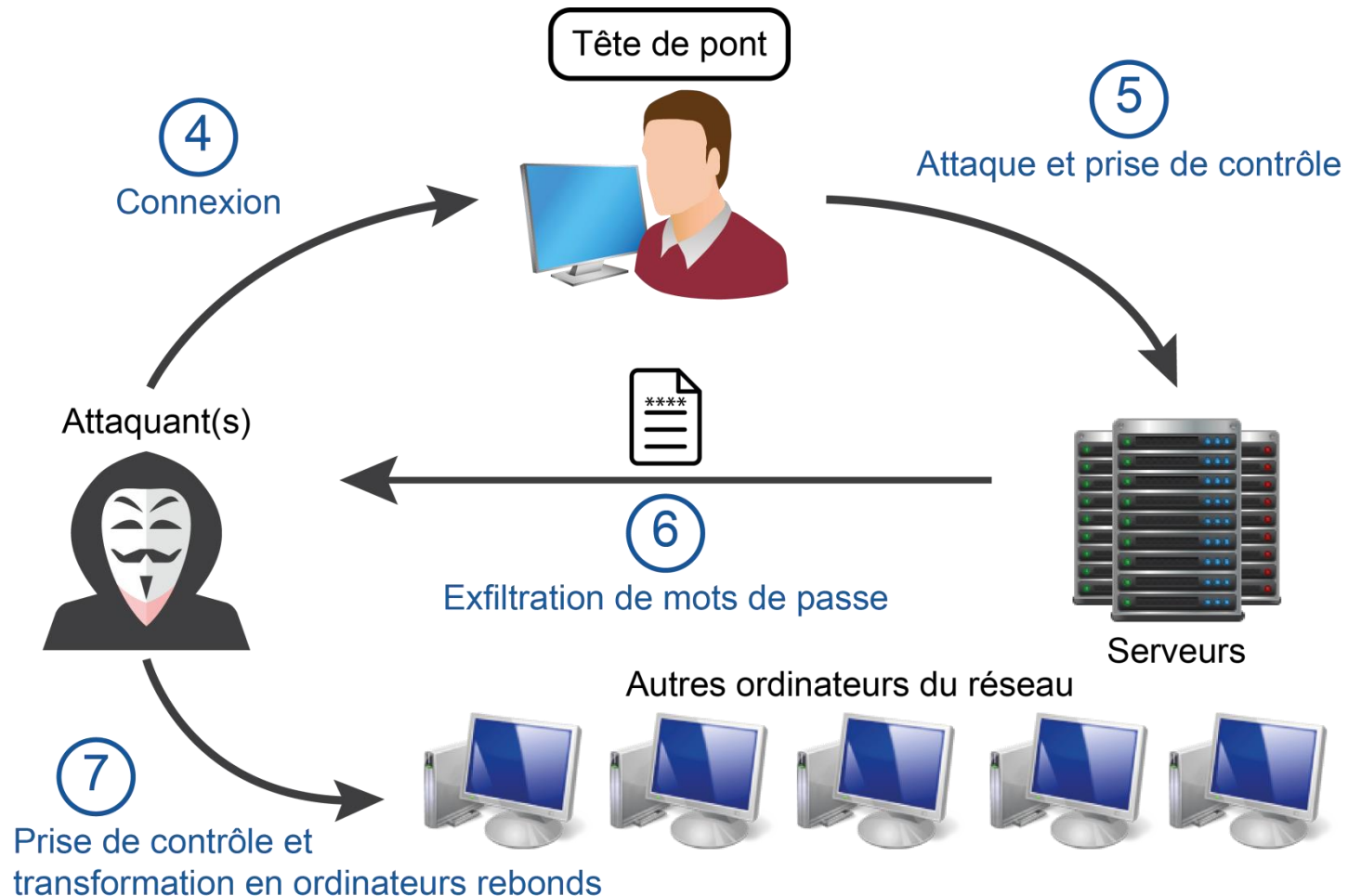
4. Panorama de quelques menaces

d. Déroulement d'une attaque avancée



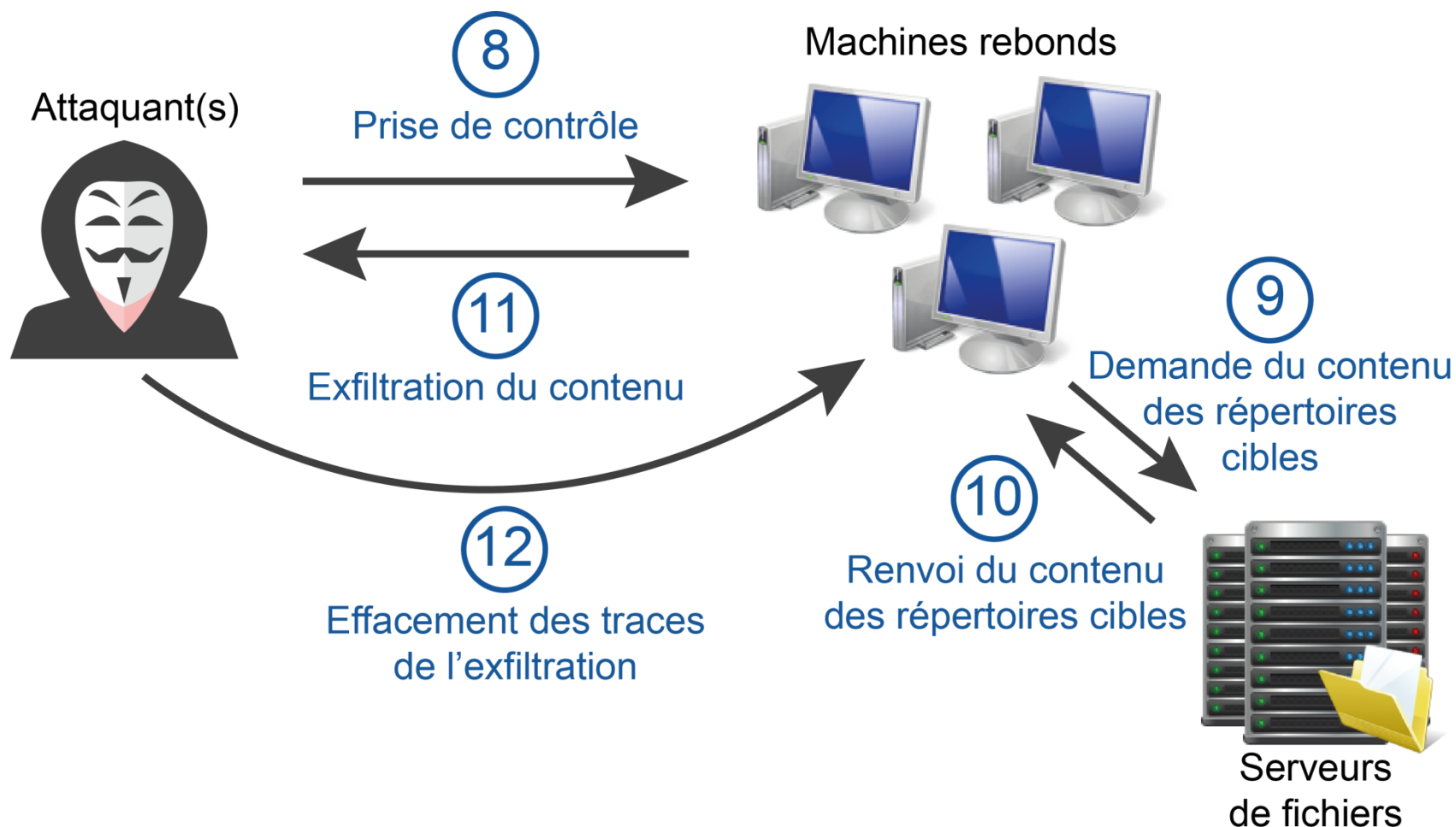
4. Panorama de quelques menaces

d. Dérroulement d'une attaque avancée



4. Panorama de quelques menaces

d. Déroulement d'une attaque avancée



4. Panorama de quelques menaces

d. Déroutement d'une attaque avancée (Exemple)



Des photos intimes d'acteurs, chanteurs, présentateurs célèbres stockées sur iCloud d'Apple ont été diffusées en ligne.

Les célébrités incluaient Jennifer Lawrence, Kate Upton, Rihanna, Kim Kadarshian, Selena Gomez entre autres.

- Apple indique que :
 - Ses services iCloud ou FindMyPhone n'ont pas été compromis
 - les comptes iCloud des stars concernées ont été compromis par des attaques ciblées de :
 - compte utilisateur
 - mot de passe
 - questions de sécurité
- Le nombre de tentatives de mots de passe avant verrouillage du compte était trop élevé.
 - permettant des attaques par « brute force »
- Il semblerait que l'attaque soit de type « social engineering ».
 - permettant de répondre aux questions de sécurité.

4. Panorama de quelques menaces

e. Fraude interne

La **fraude interne** est un « sujet tabou » pour les entreprises, mais un véritable sujet d'importance !

Catégories de fraudeurs

- Fraudeur occasionnel
- Fraudeur récurrent (petites sommes de manière régulière)
- Personne qui se fait embaucher pour effectuer une fraude
- Fraude en groupe

Vulnérabilités

- Faiblesse des procédures de contrôle interne et de surveillance des opérations
- Gestion permissive des habilitations informatiques
- Absence de séparation des tâches et de rotation

Typologies des fraudes

- Le détournement des avoirs de la clientèle
- Le détournement des avoirs de l'entreprise
- La création de fausses opérations
- La personne qui fausse ses objectifs pour augmenter sa rémunération

4. Panorama de quelques menaces

f. Violation d'accès non autorisé : mots de passe faibles

Des mots de passe simples ou faibles (notamment sans caractères spéciaux comme « ! » ou « _ » et des chiffres) permettent – entre autre – à des attaquants de mener les actions suivantes :

- Utiliser des **scripts automatiques** pour tester un login **avec tous les mots de passe couramment utilisés** (issus d'un dictionnaire) ;
- Utiliser des **outils pour tenter de « casser » le mot de passe**. Ces outils sont très efficaces dans le cadre de mots de passe simples, et sont beaucoup moins efficaces dans le cas de mots de passe longs et complexes.



Réflexion sur l'utilisation des mots de passe : les mots de passe constituent une faiblesse significative pour la cybersécurité. En effet, **les êtres humains n'ont pas la capacité de mémoriser de nombreux mots de passe**, complexes, différents pour chaque application, etc.

Pour cette raison, **d'autres moyens d'authentification émergent**, de façon à libérer les individus des problématiques des mots de passe. Quelques exemples : la biométrie, les *tokens* USB, les matrices papier, la vérification via un code SMS, les « one time password », etc.

4. Panorama de quelques menaces

f. Violation d'accès non autorisé : intrusion

Les intrusions informatiques constituent des « attaques ciblées » qui exploitent une ou des vulnérabilité(s) technique(s) pour dérober des informations confidentielles (ex. : mots de passe, carte bancaire...) ou prendre le contrôle des serveurs ou postes de travail

Depuis le réseau Internet sur les ressources exposées : sites institutionnels, services de e-commerce, services d'accès distant, service de messagerie, etc.

Depuis le réseau interne sur l'Active Directory ou les applications sensibles internes

Quelques chiffres issus de tests d'intrusion menés sur de nombreux S.I. :

80% des domaines Active Directory sont compromis en 2 heures

75% des domaines Active Directory contiennent au moins 1 compte privilégié avec un mot de passe trivial

50% des entreprises sont affectées par un défaut de cloisonnement de ses réseaux

80% des tests d'intrusion ne sont pas détectés par les équipes IT

Sources : tests d'intrusion Orange Consulting 2012-2013

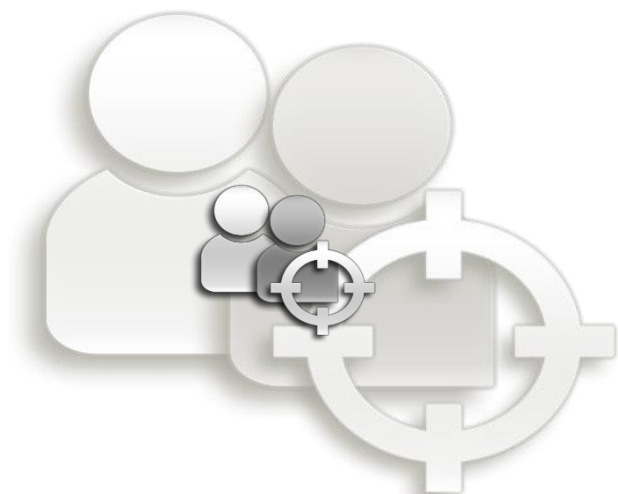
Active Directory : est un système d'annuaire sous Windows répertoriant les ressources du réseau notamment les sites, les machines, les utilisateurs.

4. Panorama de quelques menaces

g. Virus informatique

Les **virus informatiques** constituent des « attaques massives » qui tendent...

- à devenir de plus en plus ciblés sur un **secteur d'activité** (télécommunication, banque, défense, énergie, etc.)
- à devenir de plus en plus **sophistiqués** et **furtifs**



Quelques virus récents et médiatiques : Citadel, Flame, Stuxnet, Duqu, Conficker, Zeus, Shamoon (Aramco)...

Les principaux vecteurs d'infection...

- **Message** avec pièce-jointe
- Support amovible (**clé USB**...)
- **Site Web** malveillant ou piratés
- **Partages réseaux** ouverts, systèmes vulnérables...



... avec comme conséquences potentielles ...

- Installation d'un « **cheval de Troie** » pour accéder au poste de travail à distance
- **Récupération de données** ciblées : cartes bancaires, identifiants/mots de passe...
- **Surveillance à distance** des activités : capture des écrans, des échanges, du son ou de la vidéo !
- **Destruction des données** des postes de travail
- **Chiffrement des données** pour une demande de rançon
- ...

4. Panorama de quelques menaces

h. Déni de service distribué (DDoS)

La **déni de service distribué** (DDoS) constitue une « attaque ciblée » qui consiste à saturer un site Web de requêtes pour le mettre « hors-service » à l'aide de « **botnets** », réseaux d'ordinateurs infectés et contrôlés par les attaquants

... une menace majeure et en augmentation pour les sites Internet



34,5 heures

durée moyenne d'une attaque



48,25 Gbps

bande passante moyenne d'une attaque



75 % des attaques au niveau infrastructure

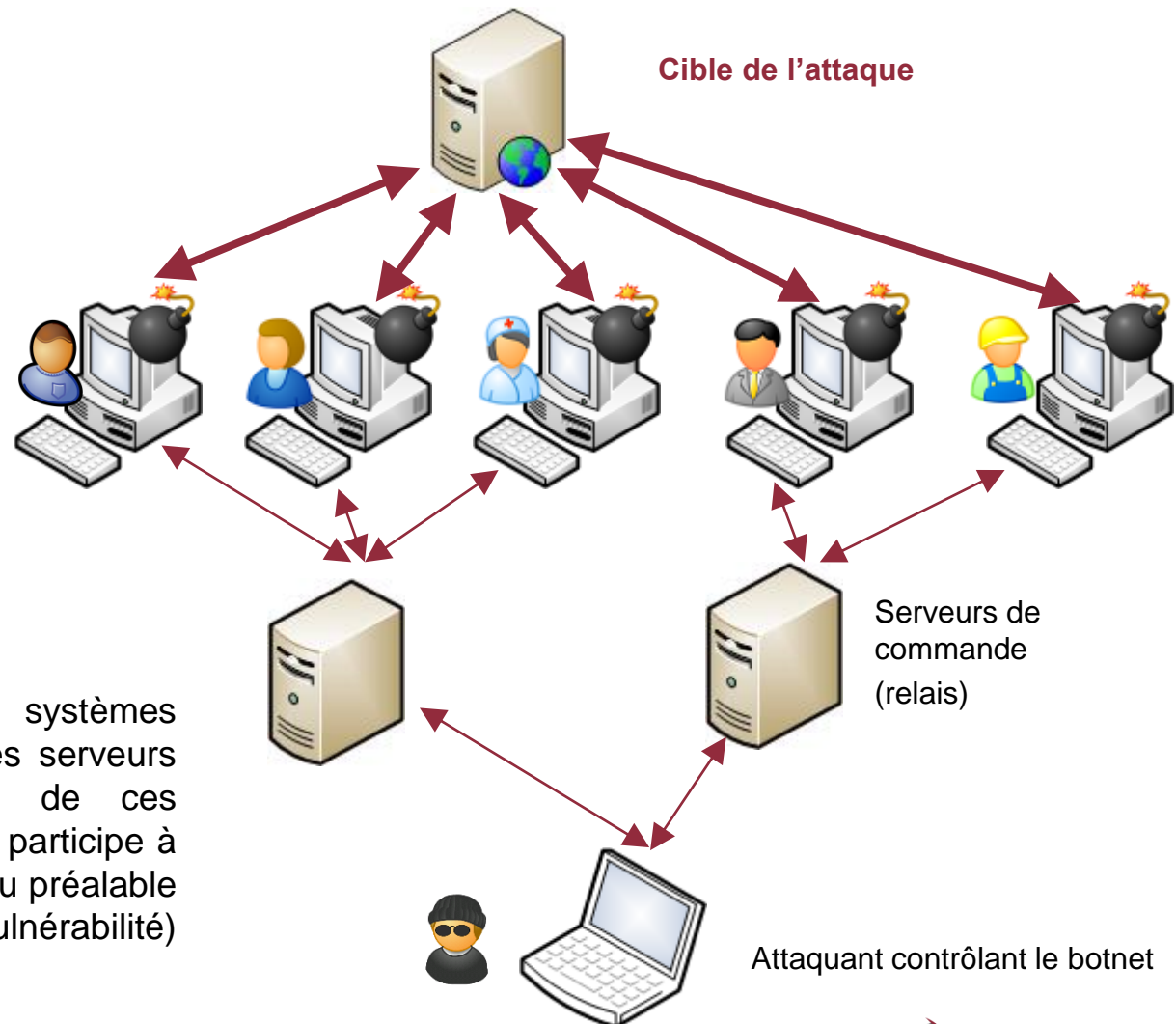
25% des attaques au niveau application



4. Panorama de quelques menaces

i. Illustration d'un réseau de botnets

Milliers ou millions d'ordinateurs infectés, prêts à attaquer une cible sur ordre de l'attaquant



Un **botnet** est un ensemble de systèmes contrôlables par un attaquant via des serveurs de commande. Les propriétaires de ces systèmes ne savent pas que leur PC participe à un botnet (leur PC a été compromis au préalable et à leur insu via l'exploitation d'une vulnérabilité)

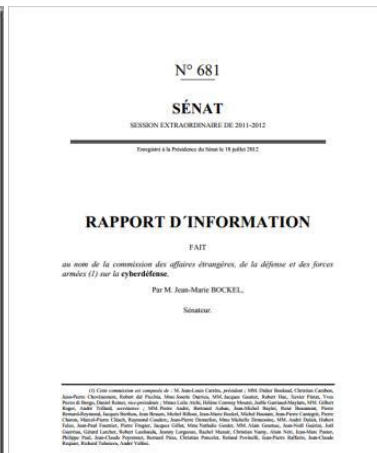
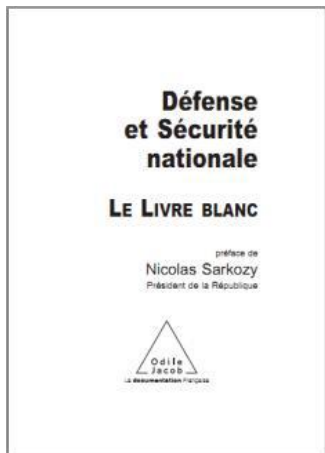
5. Le droit des T.I.C. et l'organisation de la cybersécurité en France

- a) L'organisation de la sécurité en France
- b) Le contexte juridique
- c) Le droits des T.I.C.
- d) La lutte contre la cybercriminalité en France
- e) Le rôle de la CNIL : La protection des données à caractère personnel

5. Le droit des T.I.C. et l'organisation de la cybersécurité en France

a. L'organisation de la sécurité en France

Cyberdéfense : un véritable enjeu de sécurité nationale



LIVRE BLANC

DÉFENSE ET SÉCURITÉ NATIONALE
2013



Cybersécurité*, l'urgence d'agir

« **Les cyberattaques**, parce qu'elles n'ont pas, jusqu'à présent, causé la mort d'hommes, n'ont pas dans l'opinion l'impact d'actes terroristes. Cependant, dès aujourd'hui, et plus encore à l'horizon du Livre blanc, elles constituent **une menace majeure, à forte probabilité et à fort impact potentiel** » (Chapitre 4, Les priorités stratégiques, livre blanc 2013)

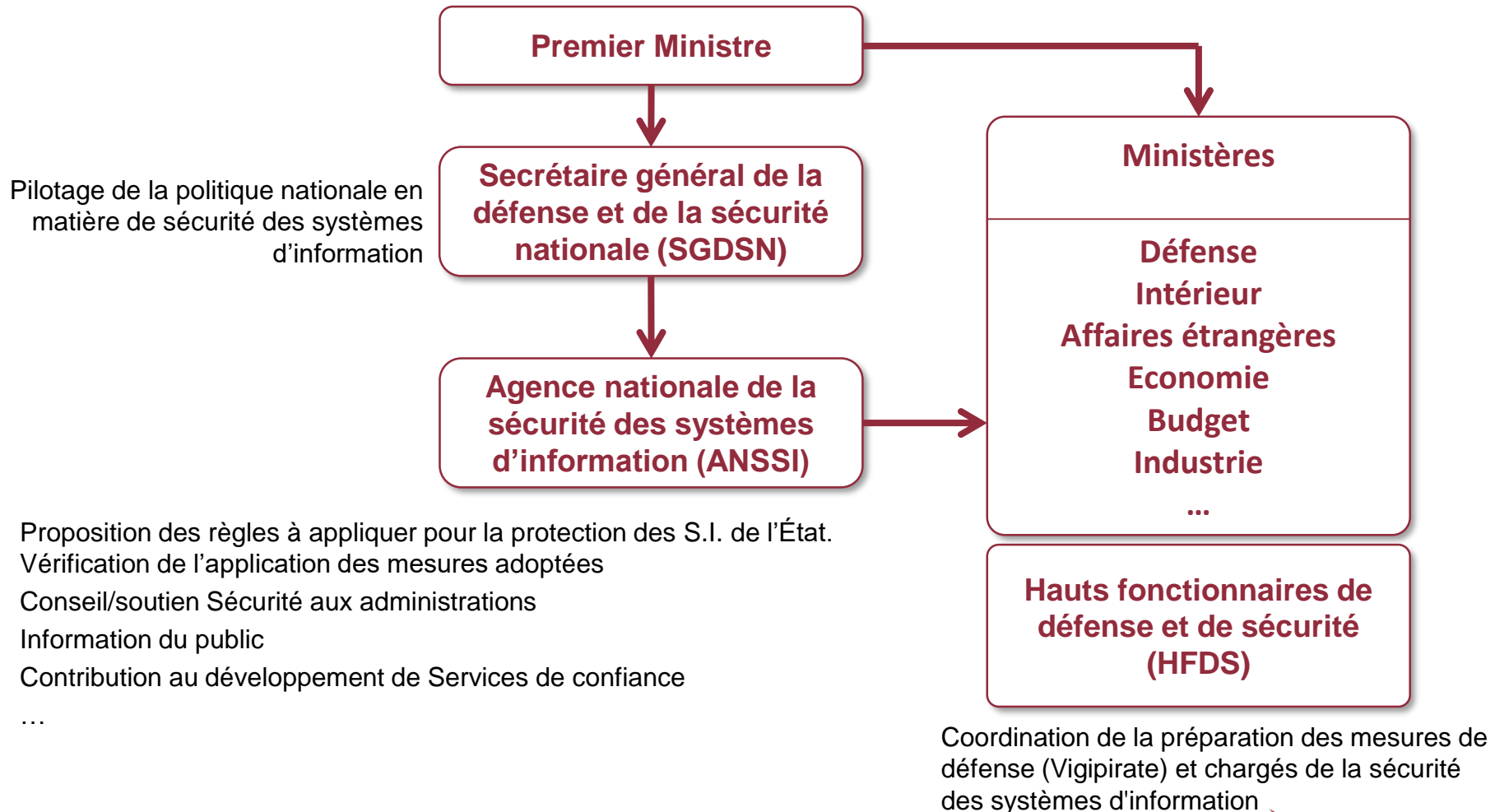
« Le développement de capacités de cyberdéfense militaire fera l'objet **d'un effort marqué** » (Chapitre 7, Les moyens de la stratégie, , livre blanc 2013)



5. Le droit des T.I.C. et l'organisation de la cybersécurité en France

a. L'organisation de la sécurité en France

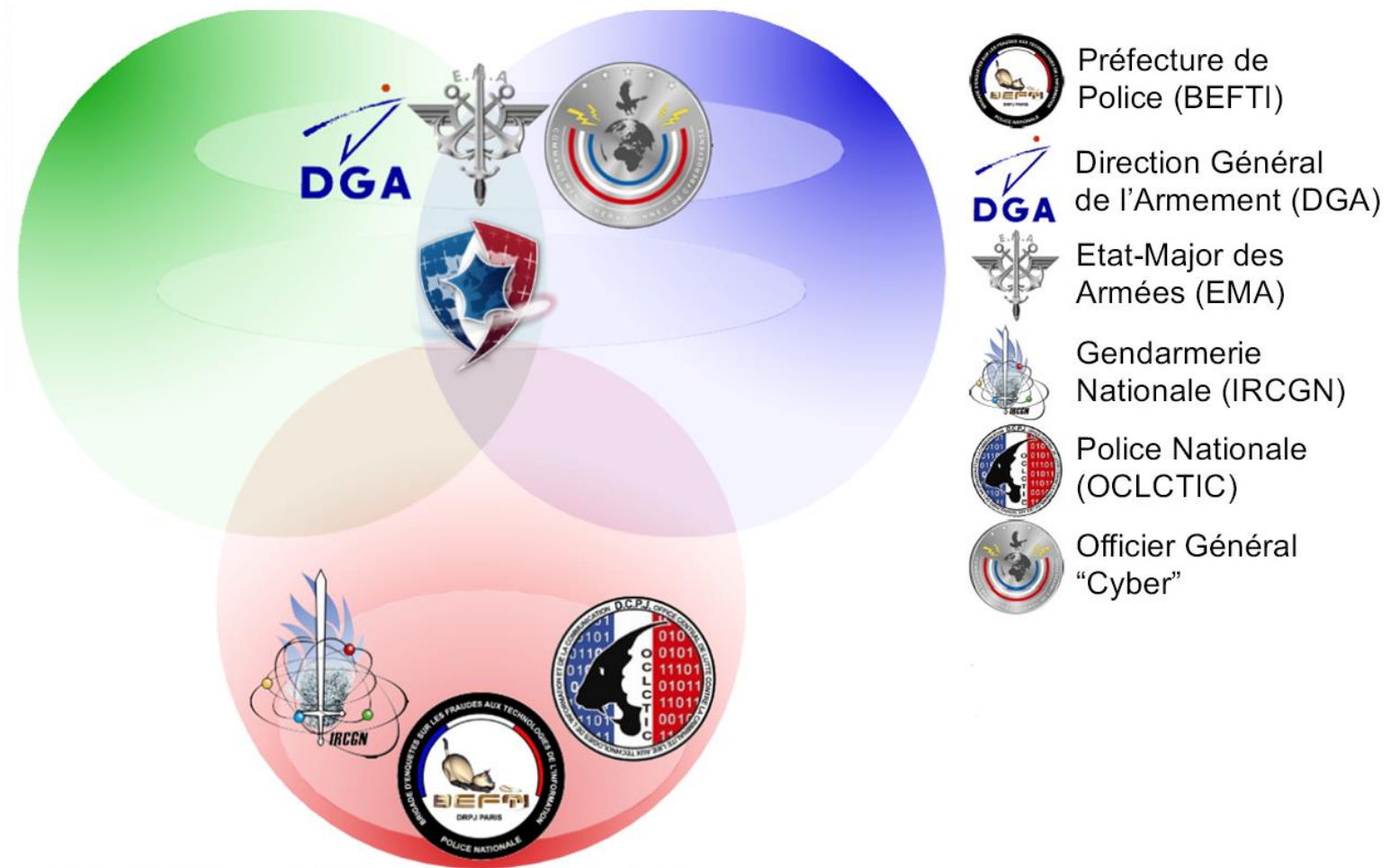
Organisation interministérielle :



5. Le droit des T.I.C. et l'organisation de la cybersécurité en France

a. L'organisation de la sécurité en France

Cybersécurité = SSI + cyberdéfense + cybercriminalité



5. Le droit des T.I.C. et l'organisation de la cybersécurité en France

b. Le contexte juridique

- Quels domaines doivent être couverts ?

Liberté d'expression

Protection du e-commerce

Propriété intellectuelle

Protection de la vie privée

Protection des entreprises

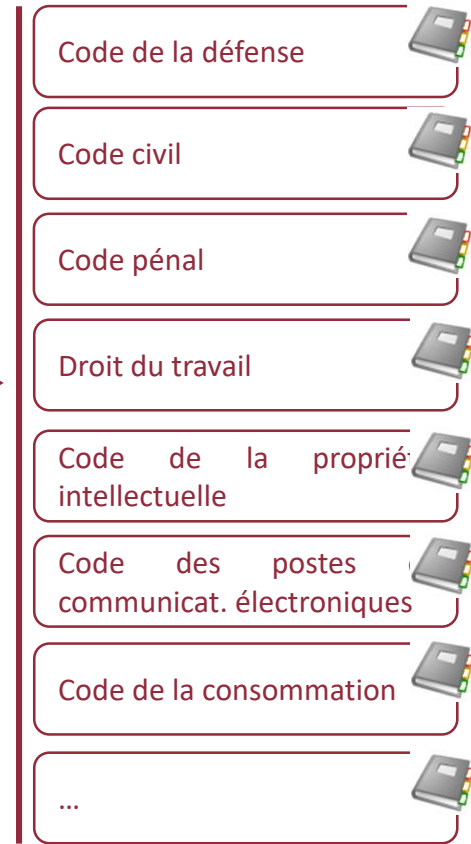
Cybercriminalité

... et bien d'autres...

5. Le droit des T.I.C. et l'organisation de la cybersécurité en France

c. Le droit des T.I.C.

- Un droit **non codifié** : des dizaines de codes en vigueur
- ... et difficile d'accès
 - Au carrefour des autres droits
 - En évolution constante et rapide
 - Issu de textes de toute nature /niveaux
 - Caractérisé par une forte construction jurisprudentielle*
- nécessitant un effort de veille juridique.



(*) La « jurisprudence » est formée de l'ensemble des décisions de justice , « à tous les étages » de l'ordre judiciaire, ce qui donne lieu parfois à des décisions contradictoires, à l'image de l'évolution de la société.

5. Le droit des T.I.C. et l'organisation de la cybersécurité en France

d. La lutte contre la cybercriminalité en France

Définition de la cybercriminalité :

Ensemble des actes contrevenants aux traités internationaux ou aux lois nationales utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible.

Définition de l'investigation numérique (*forensics*) :

Ensemble des protocoles et de mesures permettant de rechercher des éléments techniques sur un conteneur de données numériques en vue de répondre à un objectif technique en respectant une procédure de préservation du conteneur.

5. Le droit des T.I.C. et l'organisation de la cybersécurité en France

d. La lutte contre la cybercriminalité en France

La loi Godfrain du 5 janvier 1988 stipule que **l'accès ou le maintien frauduleux** dans tout ou partie d'un système de traitement automatisé de données – STAD (art. 323-1, al. 1 du CP), est puni de 2 ans d'emprisonnement et de 30.000 € d'amende au maximum.

- Élément matériel de l'infraction : la notion d'accès ou maintien
- La fraude ou l'élément moral : « être conscient d'être sans droit et en connaissance de cause »
- Éléments indifférents :
 - Accès « avec ou sans influence » (i.e. avec ou sans modification du système ou des données)
 - Motivation de l'auteur et origine de l'attaque (ex. Cass.soc. 1er octobre 2002)
 - La protection du système, condition de l'incrimination ? (affaire Tati/Kitetoa CA Paris, 30 octobre 2000 ; affaire Anses / Bluetouff TGI Créteil, 23 avril 2013)



Jurisprudence sur la définition des STAD : Le réseau France Télécom, le réseau bancaire, un disque dur, une radio, un téléphone, un site internet...



Tendance des tribunaux : une plus grande intransigeance à l'égard de certaines « victimes » d'accès frauduleux dont le système n'est pas protégé de manière appropriée

5. Le droit des T.I.C. et l'organisation de la cybersécurité en France

d. La lutte contre la cybercriminalité en France

- Le fait **d'entraver ou de fausser** le fonctionnement d'un tel système (art. 323-2 du CP) est puni d'un maximum de 5 ans d'emprisonnement et de 75.000 € d'amende
- **L'introduction, la suppression ou la modification frauduleuse de données** dans un système de traitement automatisé (art. 323-3 du CP) est puni d'un maximum de 5 ans d'emprisonnement et de 75.000 € d'amende
- L'article 323-3-1 (créé par la LCEN) incrimine le fait **d'importer, de détenir, d'offrir, de céder ou de mettre à disposition, sans motif légitime, un programme ou un moyen permettant de commettre les infractions** prévues aux articles 323-1 à 323-3. (mêmes sanctions)

- Art. 323-4 : l'association de malfaiteurs en informatique
- Art. 323-5 : les peines complémentaires
- Art. 323-6 : la responsabilité pénale des personnes morales
- Art. 323-7 : la répression de la tentative

5. Le droit des T.I.C. et l'organisation de la cybersécurité en France

e. Le rôle de la CNIL : La protection des données à caractère personnel



Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

- Quel est le champ d'application de la loi ?
 - Art. 2 « La présente loi s'applique aux **traitements automatisés** de données à caractère personnel, ainsi qu'aux **traitements non automatisés** de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles, lorsque leur **responsable** remplit les conditions prévues à l'article 5 (relevant du droit national). »
- Qu'est qu'une donnée à caractère personnel ?
 - « Constitue une donnée à caractère personnel **toute information** relative à une **personne physique** identifiée ou **qui peut être identifiée, directement ou indirectement**, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. »

5. Le droit des T.I.C. et l'organisation de la cybersécurité en France

e. Le rôle de la CNIL : La protection des données à caractère personnel



La loi protège les droits des personnes physiques identifiées ou identifiables par les données à caractère personnel

- Un traitement de données à caractère personnel doit être « *loyal et licite* »
 - Les données sont collectées pour des **finalités déterminées** explicites et légitimes
 - de manière **proportionnée** (adéquates, pertinentes et non excessives)
 - avec le **consentement de la personne concernée** (sauf exception)
 - **pendant une durée** n'excédant pas celle nécessaire à la réalisation des finalités !
- Les personnes physiques disposent de différents droits sur les données à caractère personnel qui font l'objet d'un traitement...
 - Un **droit d'information** préalable au consentement
 - Un **droit d'accès** aux données collectées
 - Un **droit de rectification**
 - Un **droit d'opposition pour raison légitime**

5. Le droit des T.I.C. et l'organisation de la cybersécurité en France

e. Le rôle de la CNIL : La protection des données à caractère personnel



Le responsable de traitement est la personne qui détermine les finalités et les moyens du traitement de données à caractère personnel

- **Obligations administratives** auprès de la CNIL
 - Le régime de la **déclaration préalable** (art. 22 à 24)
 - Le traitement peut faire l'objet d'une dispense de déclaration
 - Le traitement échappe à l'obligation de déclaration car le responsable du traitement a désigné un correspondant à la protection des données (CIL)
 - Dans tous les autres cas, le traitement doit effectivement faire l'objet d'une déclaration préalable
 - Le régime **d'autorisation préalable** (art. 25 à 27)
 - Régime applicable pour les « traitements sensibles » (listés à l'art. 25)
 - Examen de la demande par la CNIL sous deux mois (le silence vaut rejet).

5. Le droit des T.I.C. et l'organisation de la cybersécurité en France

e. Le rôle de la CNIL : La protection des données à caractère personnel

- Des **obligations de confidentialité et de sécurité** des traitements et de secret professionnel
 - De **mettre en œuvre les mesures techniques et organisationnelles appropriées**, au regard de la nature des données et des risques, pour **préserver la sécurité des données** et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès (art. 34)
 - Absence de prescriptions techniques précises
 - Recommandation de réaliser une analyse de risques préalable voire, pour les traitements les plus sensibles, une étude d'impact sur la vie privée (PIA)
 - Publication par la CNIL de « guides sécurité pour gérer les risques sur la vie privée » (méthodologie d'analyse de risques et catalogue de bonnes pratiques)
 - De veiller à ce que, le cas échéant, les **sous-traitants** apportent des garanties suffisantes au regard des mesures de sécurité techniques et d'organisation
 - Est considéré comme sous-traitant celui qui traite des données à caractère personnel pour le compte et sous la responsabilité du responsable du traitement (article 35)

5. Le droit des T.I.C. et l'organisation de la cybersécurité en France

e. Le rôle de la CNIL : La protection des données à caractère personnel



Les différents risques et sanctions en cas de manquements aux différentes obligations

- Des **sanctions pénales** (articles 226-16 et suivants du Code pénal) : Douze délits punis de 3 à 5 ans d'emprisonnement et jusqu'à 300.000 euros d'amende
 - Concernant les obligations de sécurité « 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 » (art. 226-17)
- Des **sanctions civiles** (articles 1382 et suivants du Code civil) : Dommages-intérêts en fonction du préjudice causé aux personnes concernées
- Des **sanctions administratives** associées aux pouvoirs conférés à la CNIL
 - Pouvoir d'injonction de cesser le traitement pour les fichiers soumis à déclaration ou de retrait de l'autorisation accordée
 - Pouvoir de sanction pécuniaire
 - Procédure d'urgence : pouvoir d'interruption de la mise en œuvre du traitement ou de verrouillage des données (3 mois)
 - Mesures de publicité des avertissements et, en cas de mauvaise foi, pour les autres sanctions



CyberEdu

La sécurité par l'enseignement supérieur des NTIC

Merci de votre attention

Ce document pédagogique a été rédigé par un consortium regroupant des enseignants-chercheurs et des professionnels du secteur de la cybersécurité.



Il est mis à disposition par l'ANSSI sous licence Creative Commons Attribution 3.0 France.

