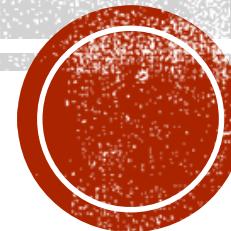


Sécurité Informatique

Architecture Intranet / Internet



Mouhcine Bouayad

Octobre 2019

2

SENSIBILISATION ET INITIATION À LA CYBERSÉCURITÉ

Module 1 : notions de base

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**

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

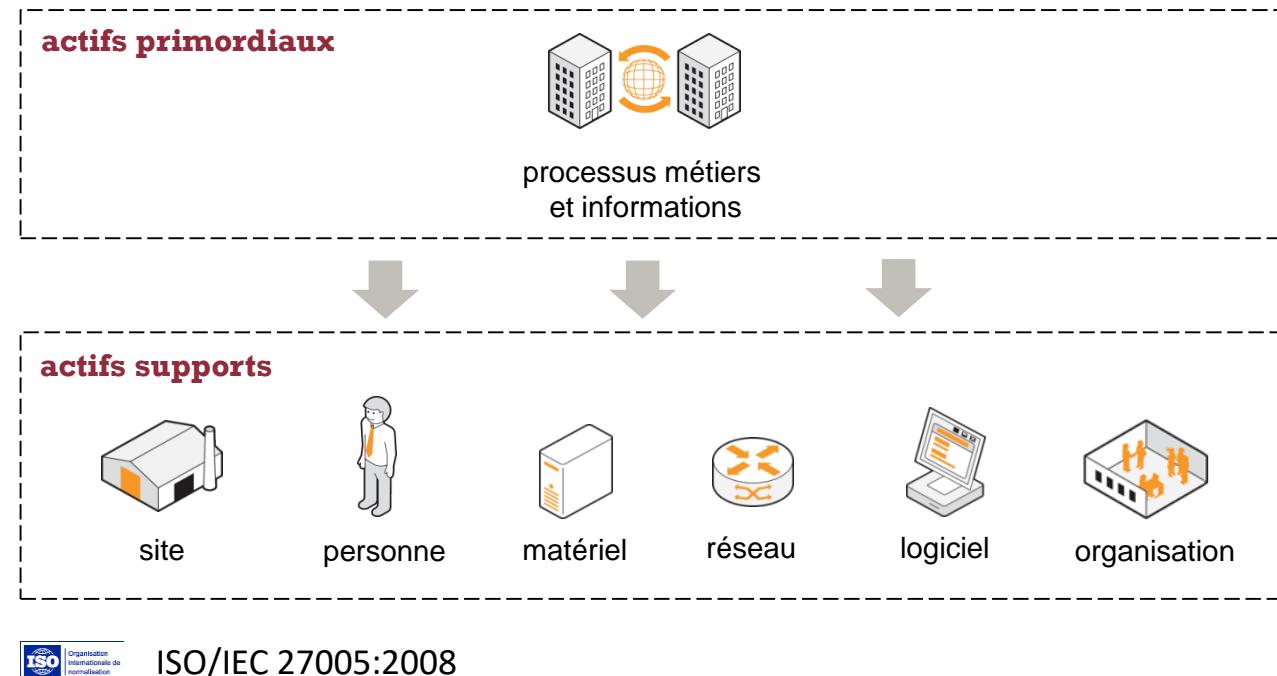
Qu'est-ce qu'un Système d'Information (S.I.) ?

- Ensemble des ressources destinées à **collecter, classifier, stocker, gérer, diffuser les informations** au sein d'une organisation
- Mot clé : **informations**, 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 :



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 SI.

actifs primordiaux



processus métiers
et informations



UN PROCESSUS MÉTIER

L'exemple ci-dessous correspond à un processus de gestion de prise de commande jusqu'à la livraison finale.



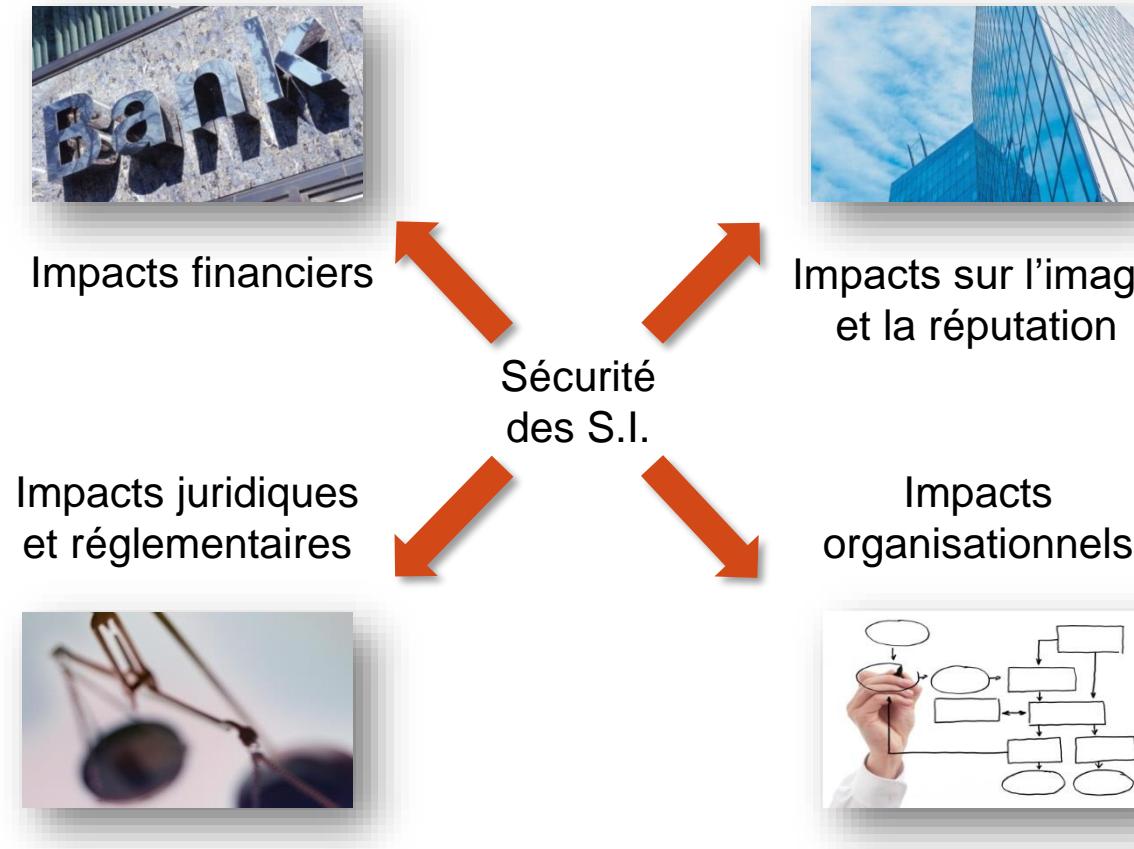
1. LES ENJEUX DE LA SÉCURITÉ DES S.I.

▪ 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)

■ Espionnage

- Industriel / concurrentiel
- Étatique

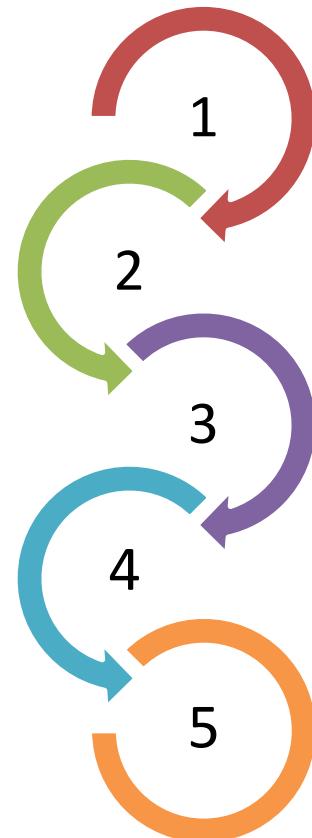
Chantage

- Déni de service
- Modifications des données

1. LES ENJEUX DE LA SÉCURITÉ DES SI.

▪ 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 SI.

▪ d. La nouvelle économie de la cybercriminalité

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

de **2 à 10 \$**

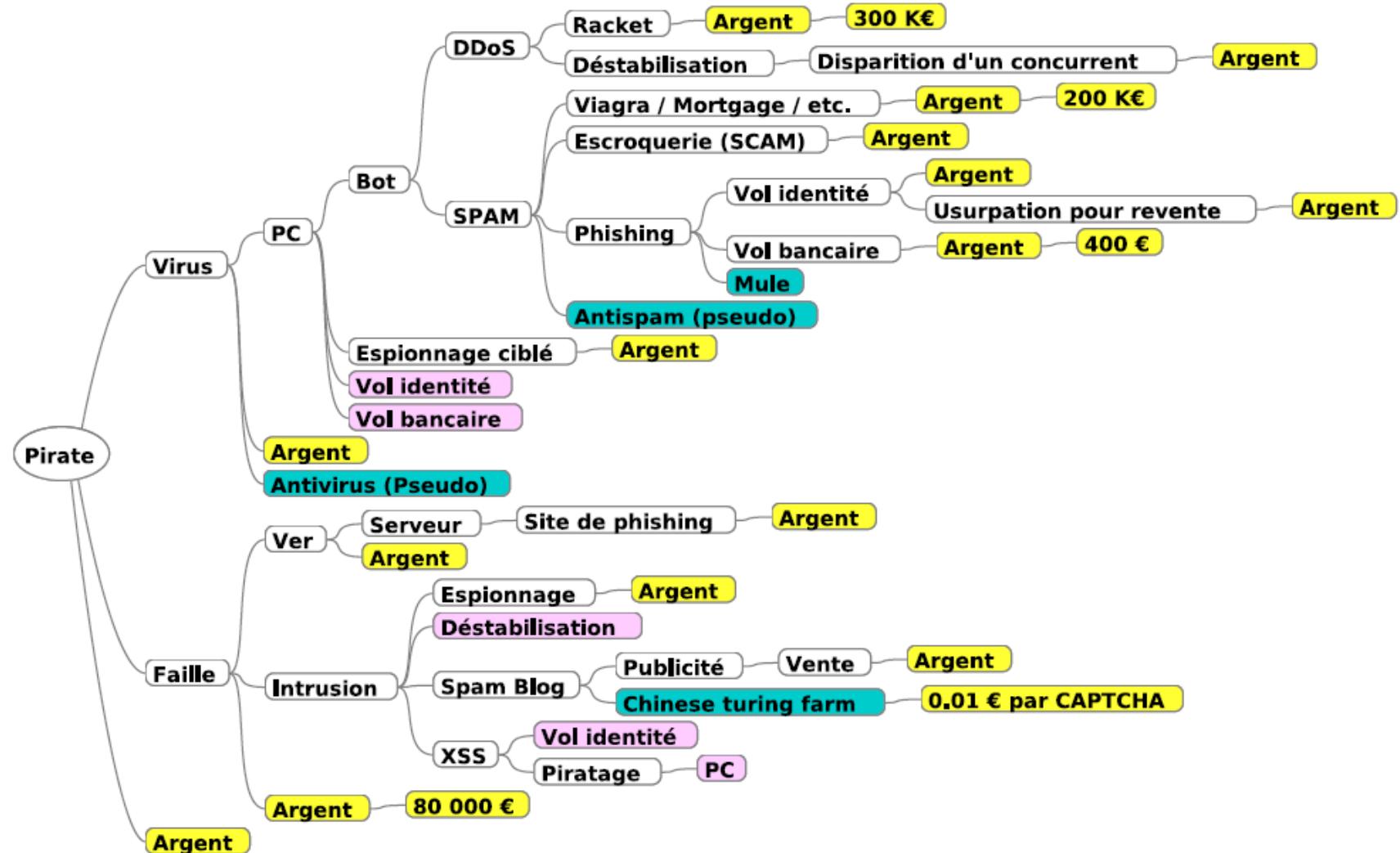
le prix moyen de commercialisation des **numéros de cartes bancaires** en fonction du pays et des plafonds

5 \$

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

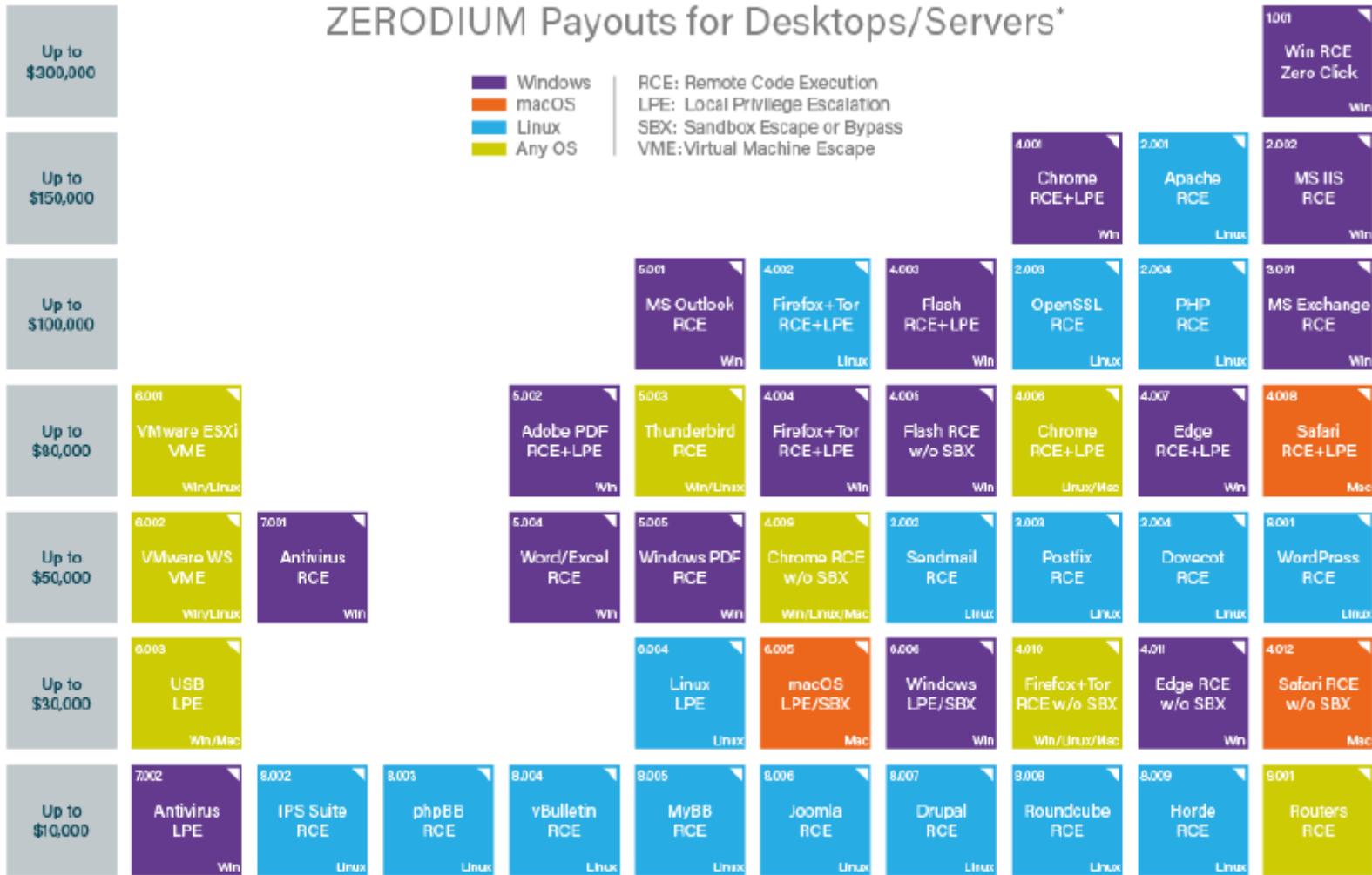
2.399 \$

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



- Faille inconnue(0 day)
 - Faille iOS 10 payée 1,5 million de \$ par Zérorium
- Phreaking téléphonique : 2 000 - 70 000 \$ par attaque réussie
- 30% des américains ont acheté après un spam
- ROI de "indian herbal" 0,1 cents pour 65 €
- 3,5 \$ pour une DoS de 1 heure et de 30 Gbit/s
- Vol d'identité
 - Perte estimée pour le vol d'une identité : 400 €(bénéfice pour le pirate : entre 50 et 100 €))
 - en 2007, l'estimation des pertes dues à la cybercriminalité était de plus de 1 milliard par an.
- Depuis 2007 C.A. cybercriminalité >C.A. drogue. 2018 : 600 milliards \$
- Pourquoi les sites porno et les sites proxy sont gratuits ?

■ Prix des failles

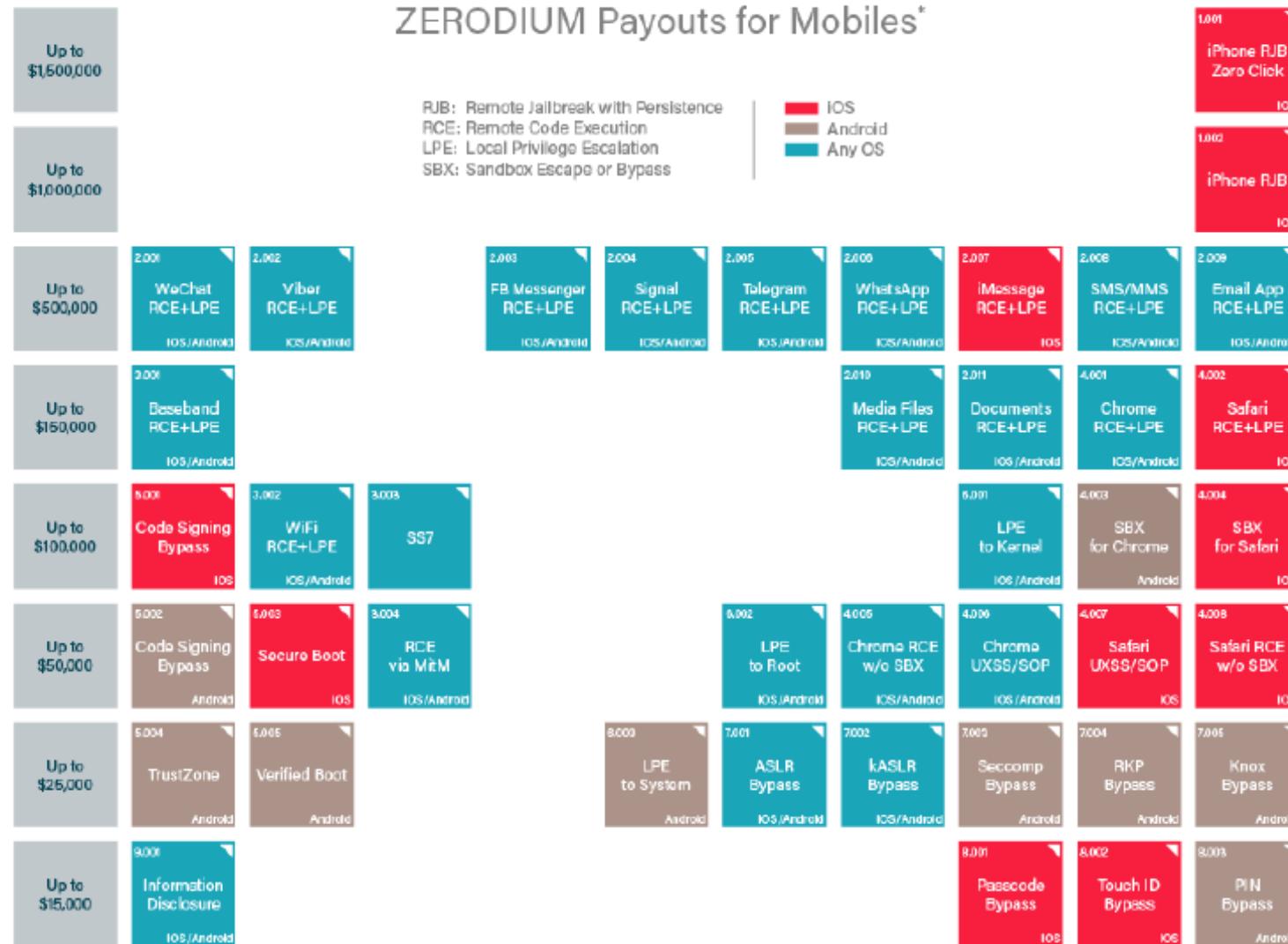


* All payouts are subject to change or cancellation without notice, at the discretion of ZERODIUM. All trademarks are the property of their respective owners.

2017/08 © zerodium.com

<https://zerodium.com/program.html>

■ Prix des failles mobiles



2017/08 © zerodium.com

<https://zerodium.com/program.html>

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
- Divulgation 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 (divulgation 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 SI.

▪ g. Quelques exemples d'attaques



Derniers articles | Archives | Recherche

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.



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](#) 5

Panne informatique à l'hôpital de

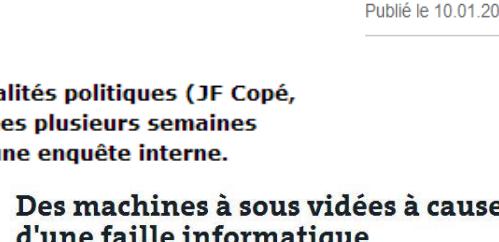
En l'espace de deux jours, mercredi et jeudi, l'accueil aux urgences de a été très perturbé. Il a fallu diriger les patients vers d'autres hôpitaux.

Publié le 10.01.2009

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. Incription pour [Twitter](#) 84 [g+1](#) [Share](#) [Email](#)



1. LES ENJEUX DE LA SÉCURITÉ DES SI.

▪ 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



Zoom

Une panne informatique paralyse Wall Street pendant 3 heures

Édité 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 \(19\)](#)



Gibraltar: un incendie interrompt des services de paris en ligne

AFP, 20/04 23:31 CET

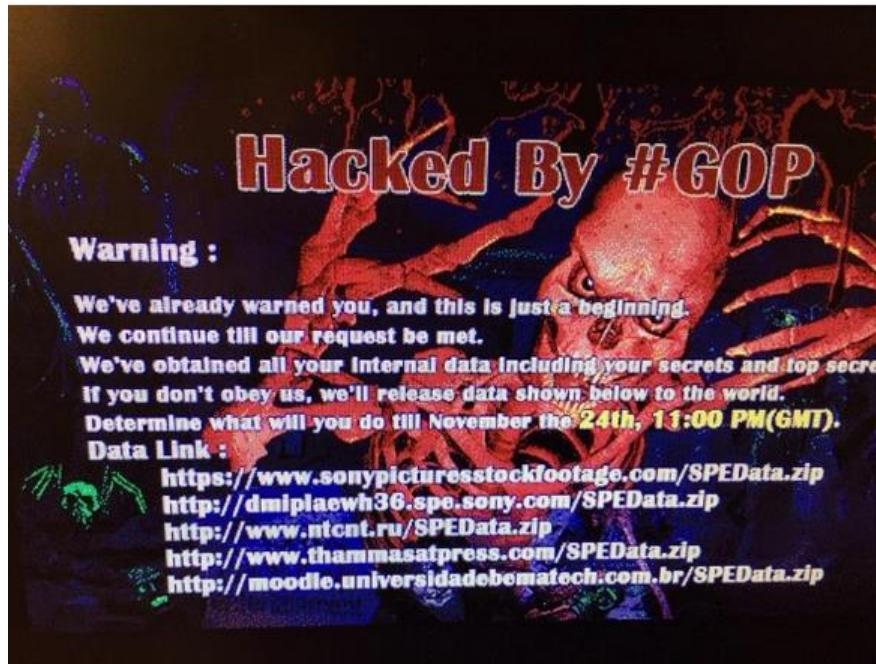


Un avion espion « plante » le système informatique d'un aéroport

Par Pierre Dandumont 5 MAI 2014 12:30 - Source: NBC News | [0 COMMENTAIRE](#)

1. LES ENJEUX DE LA SÉCURITÉ DES SI.

■ 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.

<http://www.tomsguide.com/us/biggest-data-breaches,news-19083.html>

1. LES ENJEUX DE LA SÉCURITÉ DES SI.

- 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 SI.

- 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

Vol de données personnelles

Défactement de site

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 SI.

- 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.

Video



 See How Keystroke Decoder Works

Vol de données professionnelles

Rebond pour fraude externe

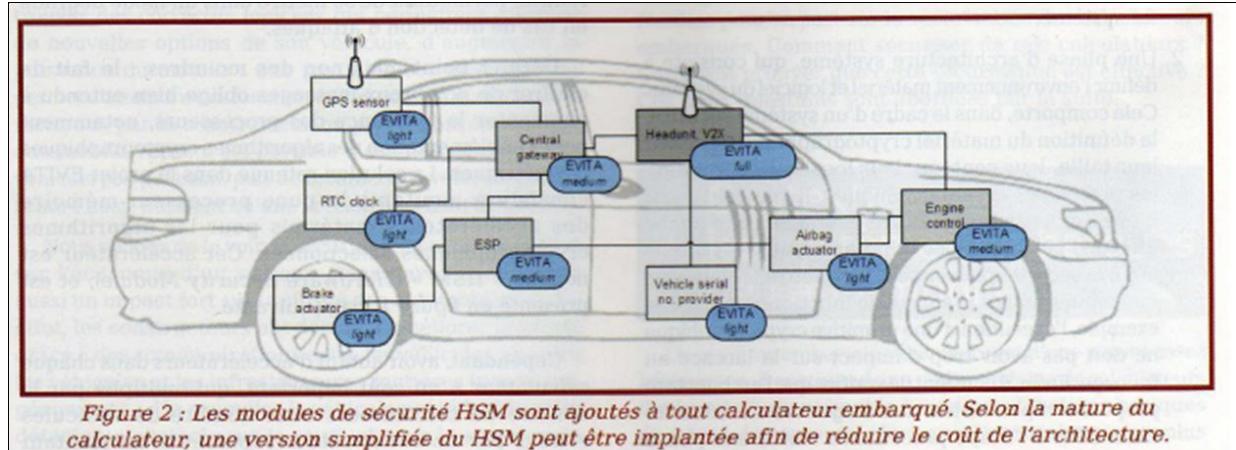
Note des lecteurs: **5.0/5**

Exclusif : Tentative de fraude bancaire via le site de l'Union française 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)

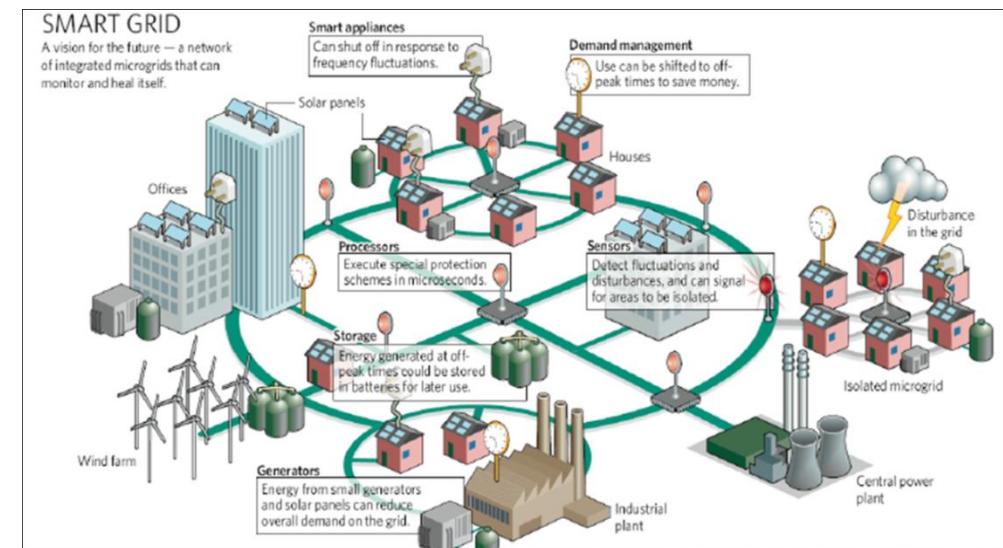
1. LES ENJEUX DE LA SÉCURITÉ DES SI.

- Quelques exemples d'attaques, ce qui pourrait arriver



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

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



Et si on ne sait pas faire ☺ ????

DDOS SERVICE

DDOSERVICE.COM PROTECT

Login Chat

1. Login the chat as a guest.
2. Tell us your target.
3. We will test attack your target for 10 mins.
4. We will set the price.
5. After you decide to deal with us, you will choose your payment method and pay us.
6. After we receive payment we will start DDoS.

* Ddos level : prolexic/nexusguard servers !
* 攻击范围: 黄色网, 赌钱网, 私服, 骗子网, 国外网.

contact us: ddosservice@ymail.com
call us : +60177174768
sms : +60177174768

www.ddosservice.com

没有帖子。

[主页](#)

订阅：[帖子 \(Atom\)](#)

source <http://www.ddosservice.com>

Statistiques à l'université de Toulouse

Ces chiffres sont des moyennes en 2017

- 200 tests par seconde (17 000 000 par jour)
- 1200 scans par jour (>3 ports ou 10 machines)
- 16 à 2000 machines à chaque fois
- 5 à 10 campagnes de phishing par jour.

2. LES BESOINS DE SÉCURITÉ

- a) Introduction aux critères DIC
- b) Besoin de sécurité : « Preuve »
- c) Différences entre sûreté 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

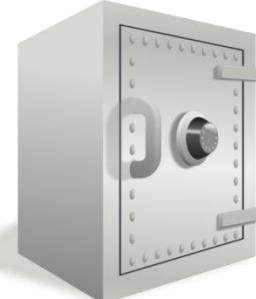
Propriété des biens de **n'être accessibles**
qu'aux personnes autorisées

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 sureté 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

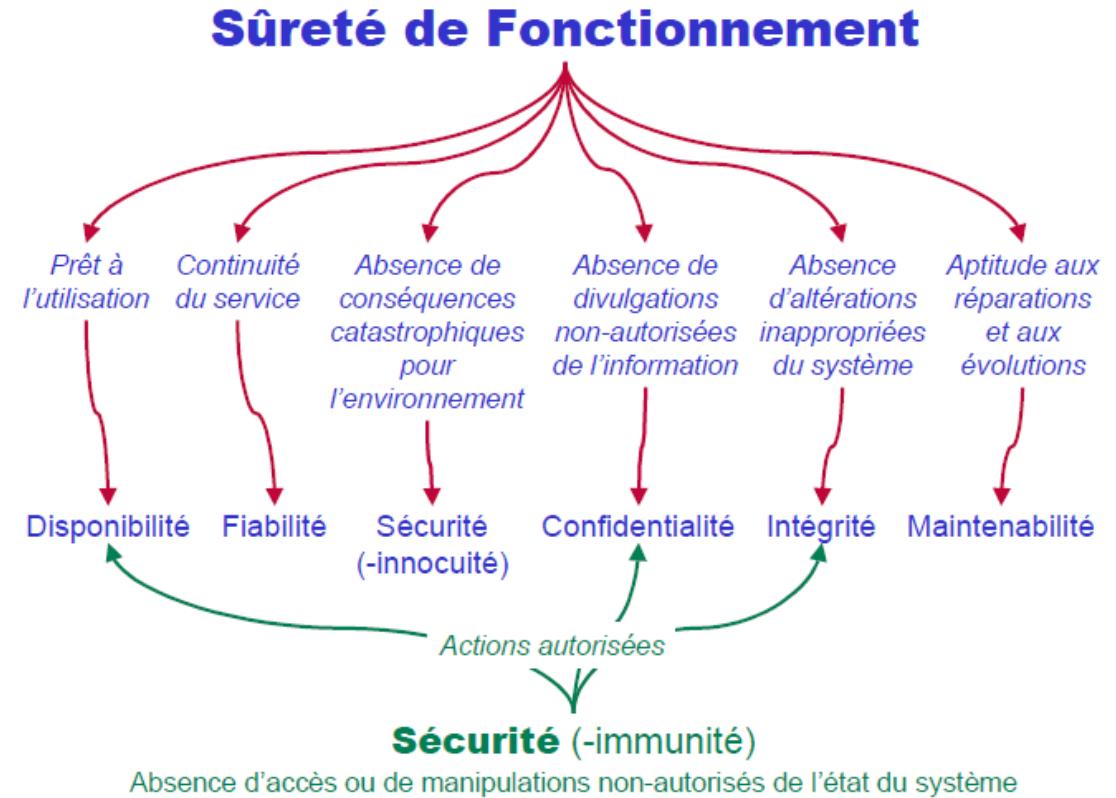
2. LES BESOINS DE SÉCURITÉ

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

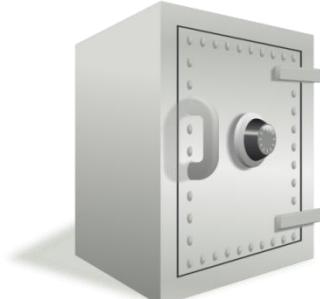
▪ d. Exemple d'évaluation DICP

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)



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	✓	✓	✓	
Cryptographie		✓	✓	✓
Pare-feu	✓		✓	
Contrôles d'accès logiques	✓	✓	✓	
Sécurité physique des équipements et locaux	✓	✓	✓	

2. LES BESOINS DE SÉCURITÉ

■ e. Mécanismes de sécurité pour atteindre les besoins DICP

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.

D I C P

✓ ✓ ✓ ✓

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

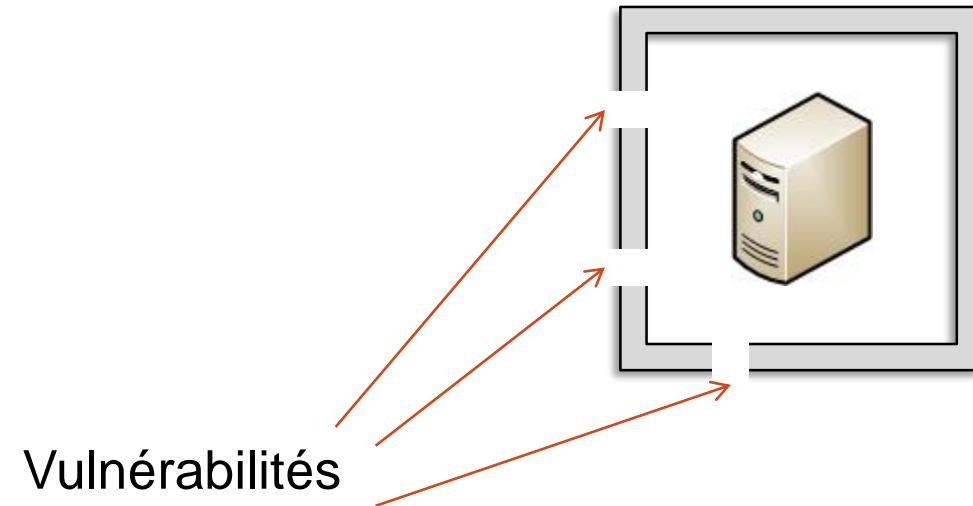
3. NOTIONS DE VULNÉRABILITÉ, MENACE, ATTAQUE

- 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).

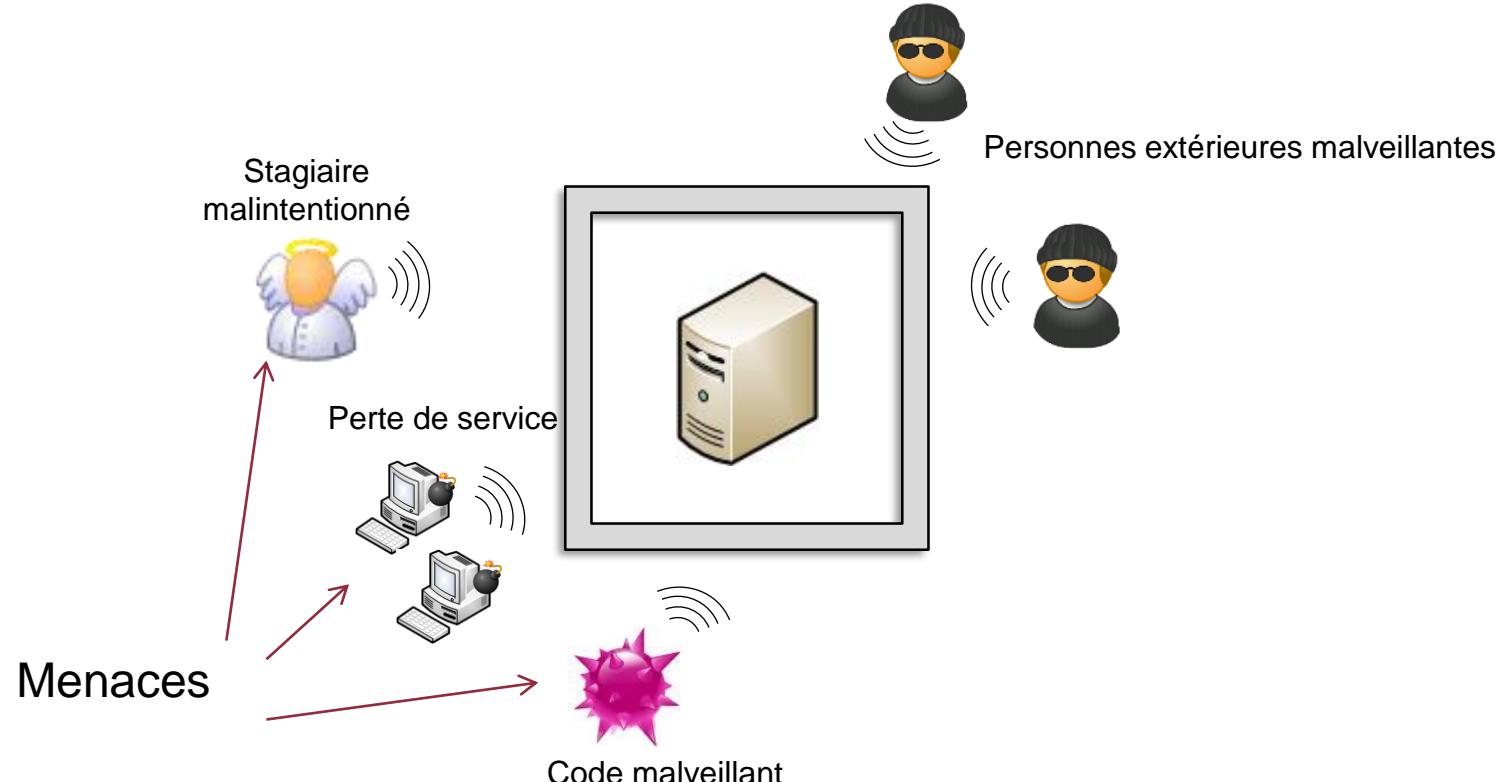


3. NOTIONS DE VULNÉRABILITÉ, MENACE, ATTAQUE

▪ b. Notion de « Menace »

▪ Menace

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

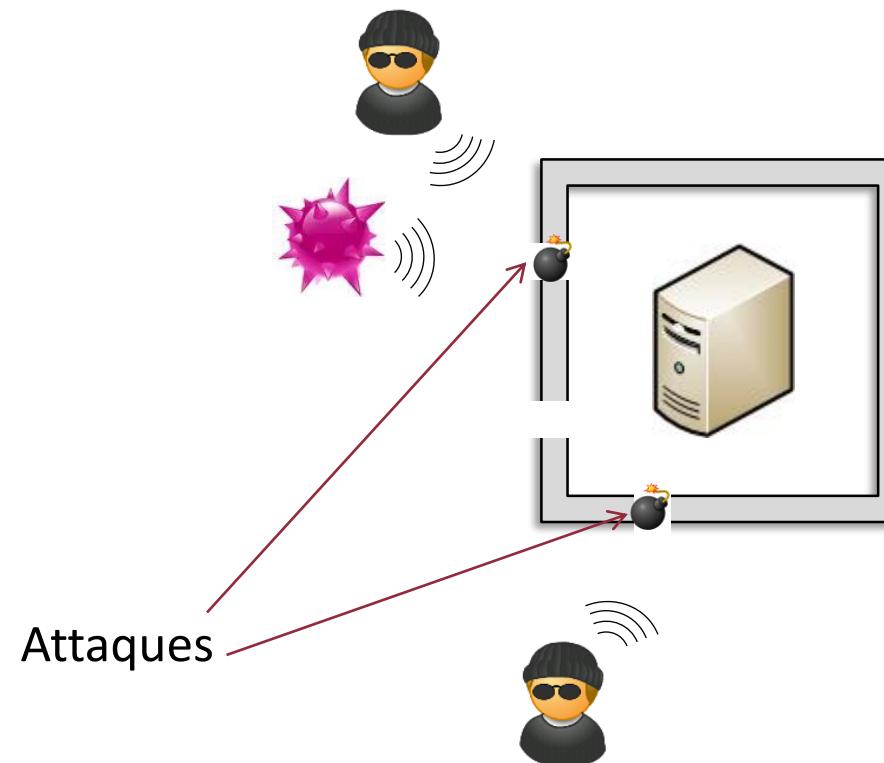


3. NOTIONS DE VULNÉRABILITÉ, MENACE, ATTAQUE

■ c. Notion d'« Attaque »

▪ **Attaque**

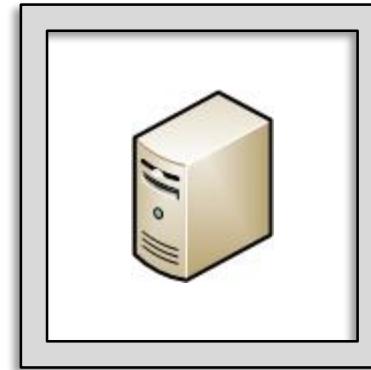
- **Action malveillante** destinée à porter atteinte à la sécurité d'un bien. Une attaque représente la **concrétisation d'une menace**, et nécessite **l'exploitation d'une vulnérabilité**.



3. NOTIONS DE VULNÉRABILITÉ, MENACE, ATTAQUE

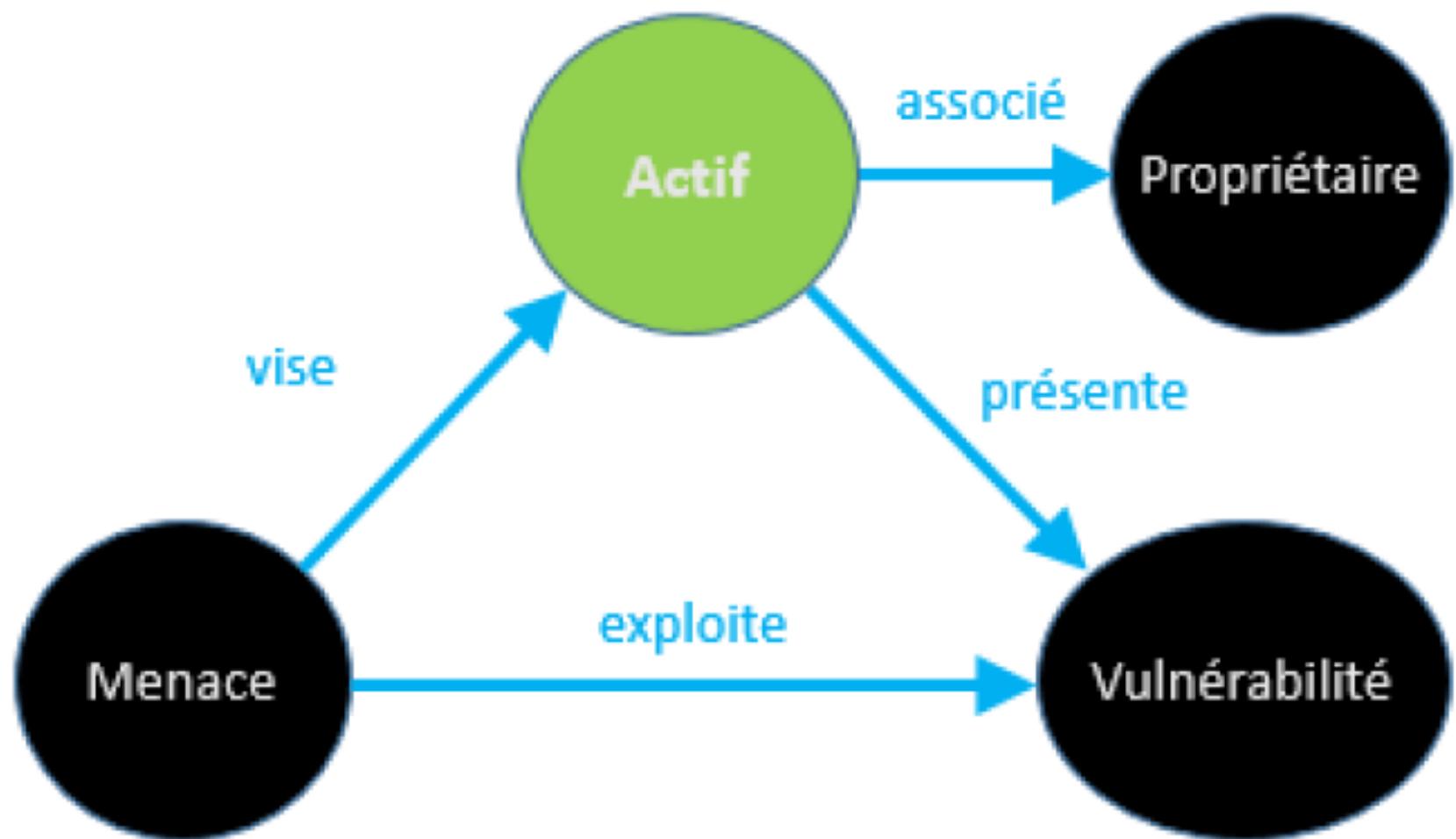
■ c. Notion d'« Attaque »

- **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

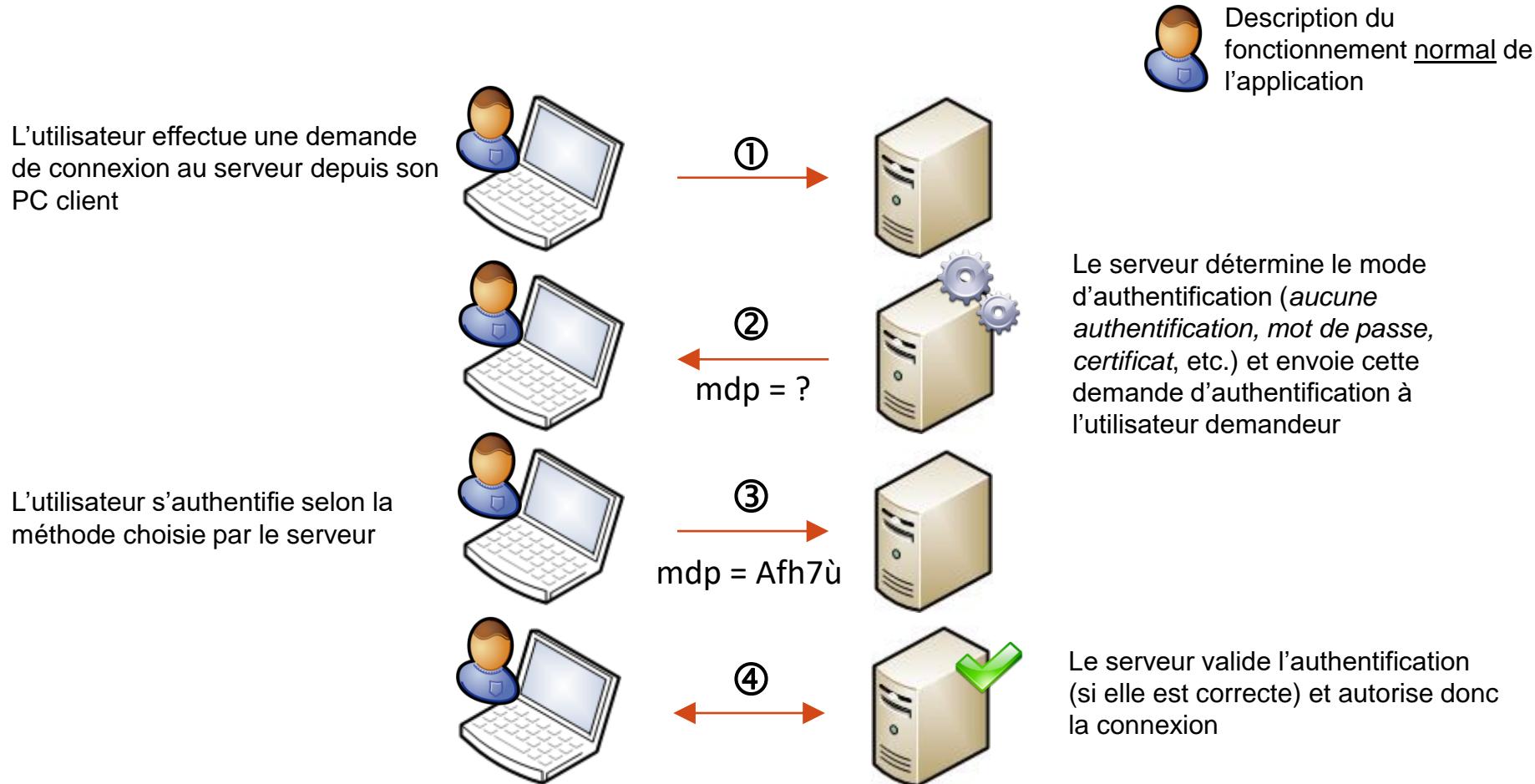
- d. Exemple de vulnérabilité : Contournement de l'authentification dans l'application VNC

L'application VNC permet à un utilisateur de prendre en main sur une machine distante, 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

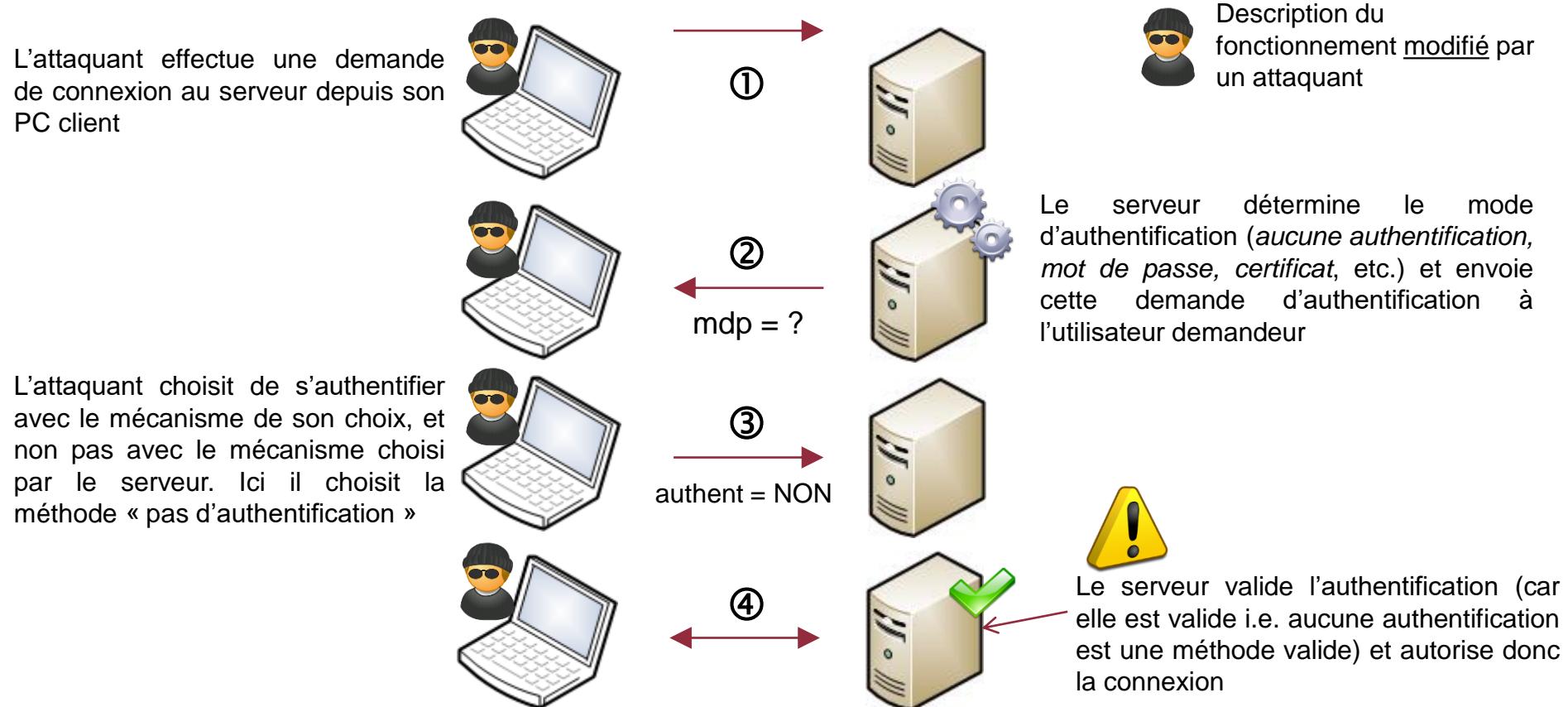
■ e. Illustration d'un usage normal de l'application vulnérable



Référence : CVE-2006-2369

3. NOTIONS DE VULNÉRABILITÉ, MENACE, ATTAQUE

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



Référence : CVE-2006-2369

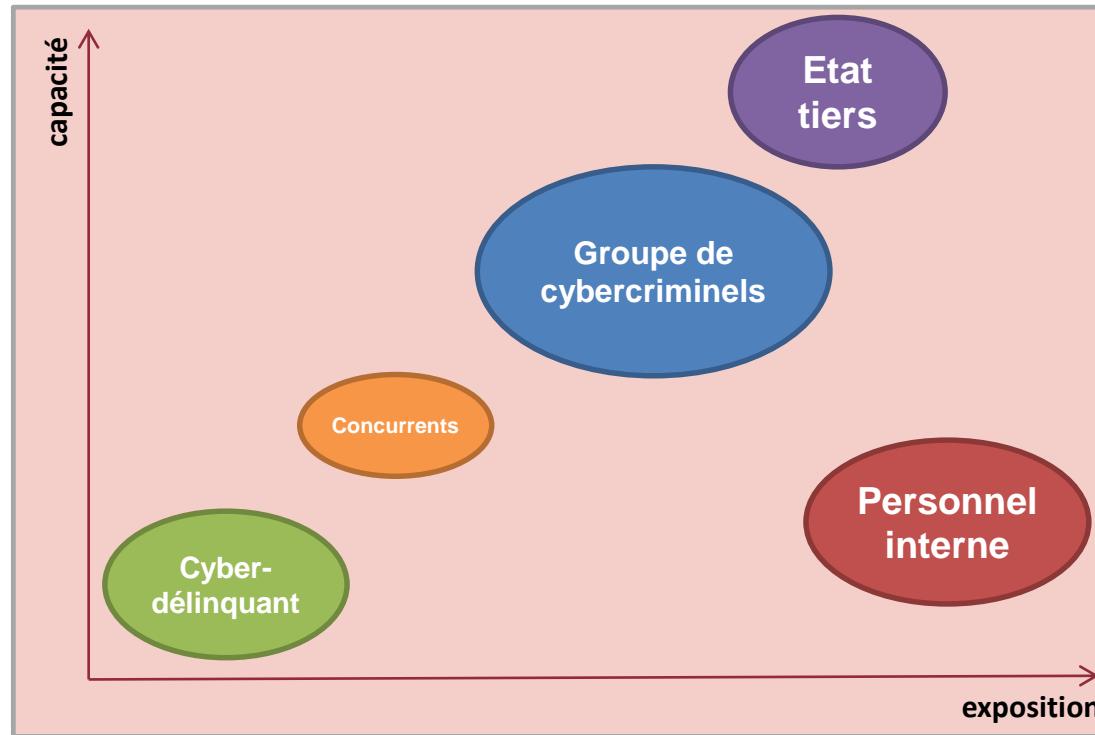
La vulnérabilité se situe ici : le serveur ne vérifie pas que le type d'authentification retourné par le client correspond à celui demandé. A la place, il vérifie simplement que l'authentification est correcte (et « authent = NON » est effectivement une authentification qui est toujours correcte)

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.

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

The image contains three screenshots of phishing emails:

- Screenshot 1 (Top):** A fake LCL (Le Crédit Lyonnais) email. The subject is "Le test du nouveau système". It claims the account has been suspended due to failed login attempts and asks the user to click a link to reactivate it.
- Screenshot 2 (Bottom Left):** A fake Société Générale email. The subject is "Mettre à jour de votre Carte Crédit en ligne". It asks the user to update their card information via a "Verified by Visa" form.
- Screenshot 3 (Bottom Right):** Another fake Société Générale "Mettre à jour de votre Carte Crédit en ligne" page. This one specifically targets MasterCard users with "MasterCard SecureCode". It includes fields for Name, Date of Birth, Mother's Maiden Name, Card Type, Card Number, Expiry Date, and CVV.

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 confidentielles, ou
- pour introduire des logiciels malveillants dans le système d'information de la banque



par téléphone



par réseaux sociaux



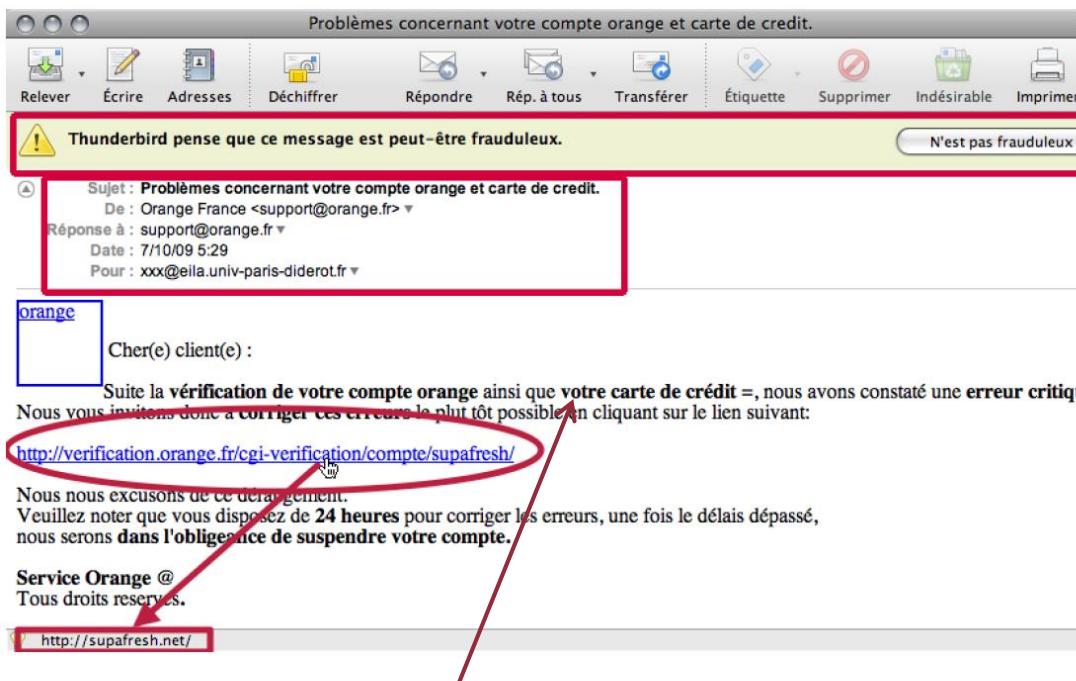
par e-mail

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

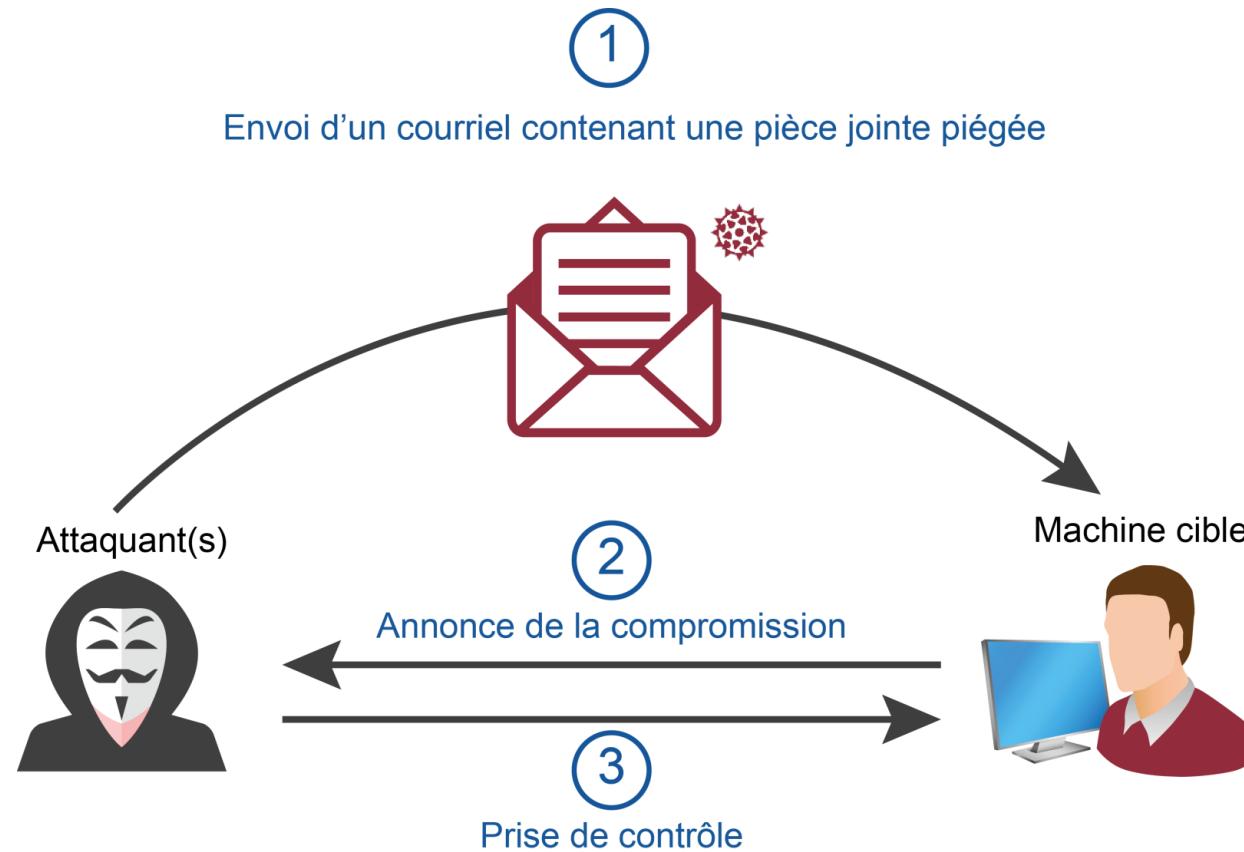
Exemple de *phishing* ciblant les employés d'un grand groupe français...



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

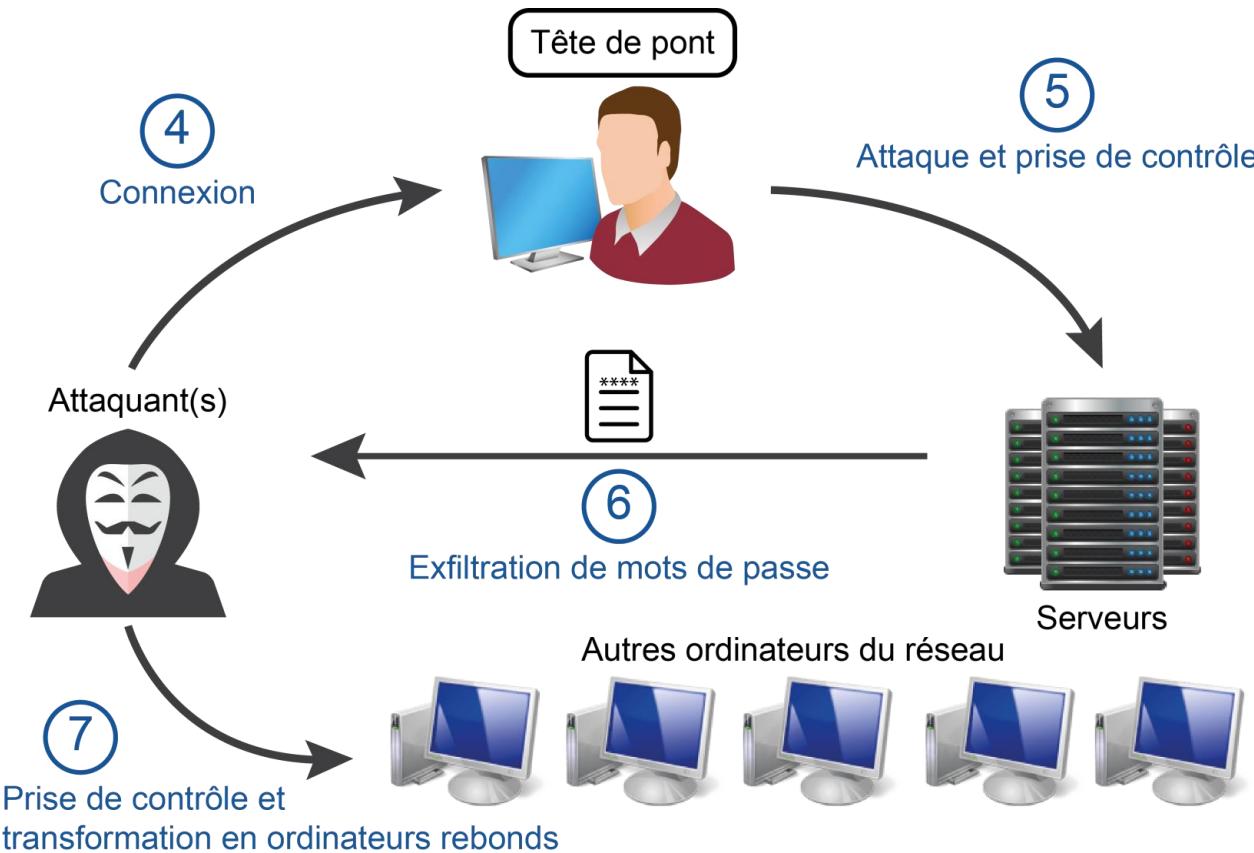
4. PANORAMA DE QUELQUES MENACES

▪ d. Déroulement d'une attaque avancée



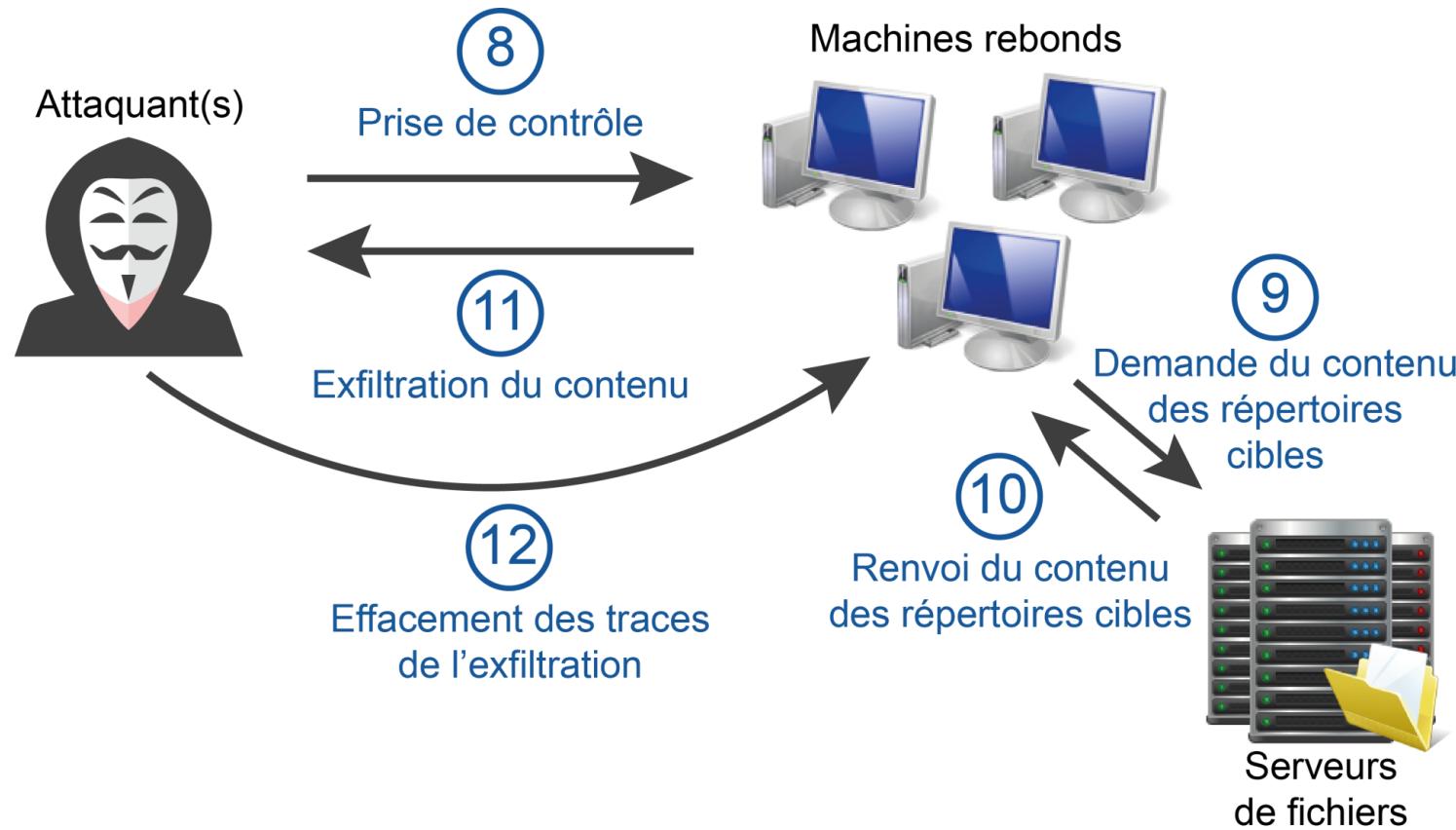
4. PANORAMA DE QUELQUES MENACES

▪ d. Déroulement d'une attaque avancée



4. PANORAMA DE QUELQUES MENACES

▪ d. Déroulement d'une attaque avancée



4. PANORAMA DE QUELQUES MENACES

▪ d. Déroulement 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 Kardashian, 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 falsifie 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

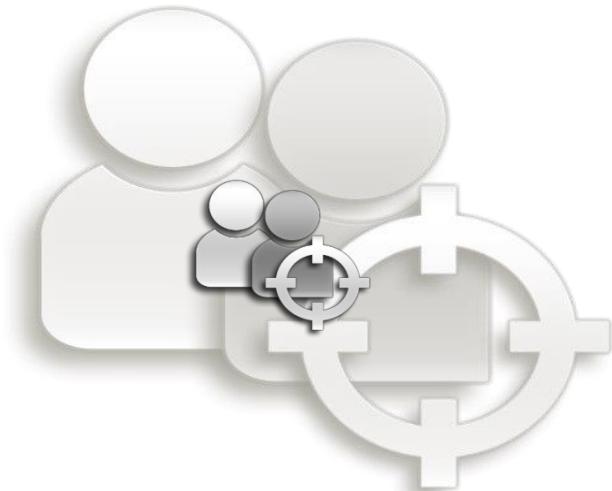
Active Directory : est un système d'annuaire sous Windows répertoriant les ressources du réseau notamment les sites, les machines, les utilisateurs.

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) constituent 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

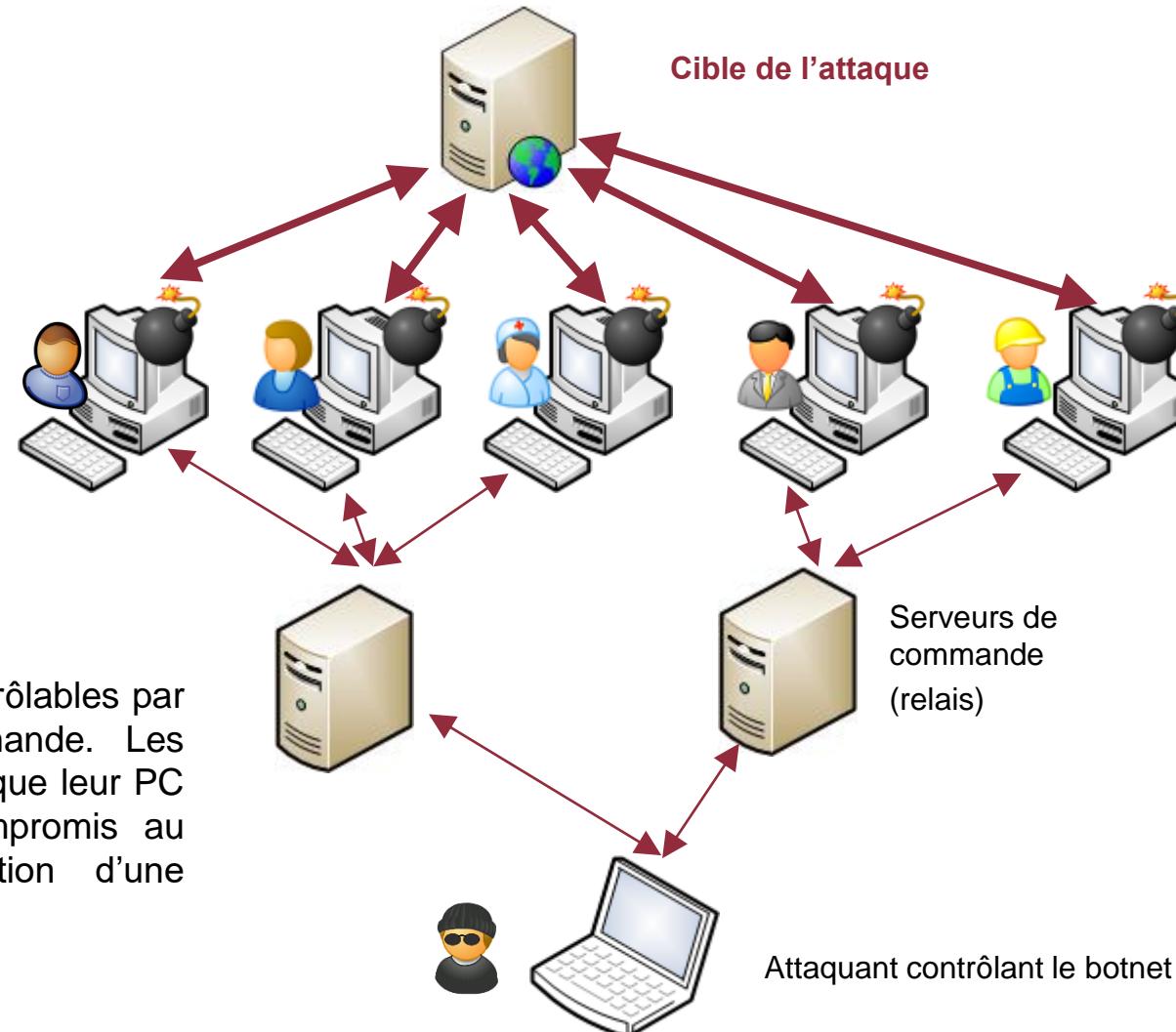
The collage consists of three news articles from different sources:

- 'Historic' DDoS Attacks Against Major U.S. Banks Continue** (Source: TechCrunch, September 27, 2012)
Summary: GoDaddy stopped by massive DDoS attack. Millions of sites may be affected – *not* by Anonymous, it appears.
- Global internet slows after 'biggest attack in history'** (Source: BBC News, December 8, 2010)
Summary: PNC Bank appears, as promised, to be the latest victim of the attack. Chase & Co. and Bank of America are on a list of banks taken of responsibilities for the attacks as retaliation for the portrayal movie trailers uploaded to YouTube.
- Update: MasterCard, Visa others hit by DDoS attacks over WikiLeaks** (Source: Computerworld, December 8, 2010)
Summary: Computerworld - The main Web site of MasterCard was knocked offline today in a large distributed denial of service (DDoS) attack apparently launched in retaliation for the credit card company's decision this week to cut off services to WikiLeaks.

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)

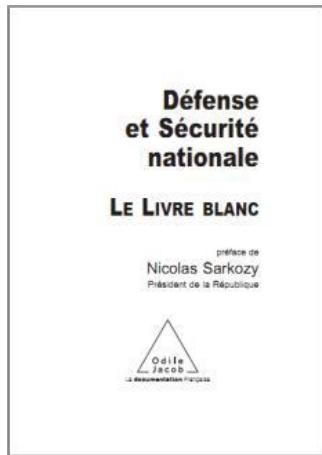
5. LE DROIT DES T.I.C. ET L'ORGANISATION DE LA CYBERSÉCURITÉ EN FRANCE

- 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 CYBERSECURITÉ EN FRANCE

▪ a. L'organisation de la sécurité en France

Cyberdéfense : un véritable enjeu de sécurité nationale

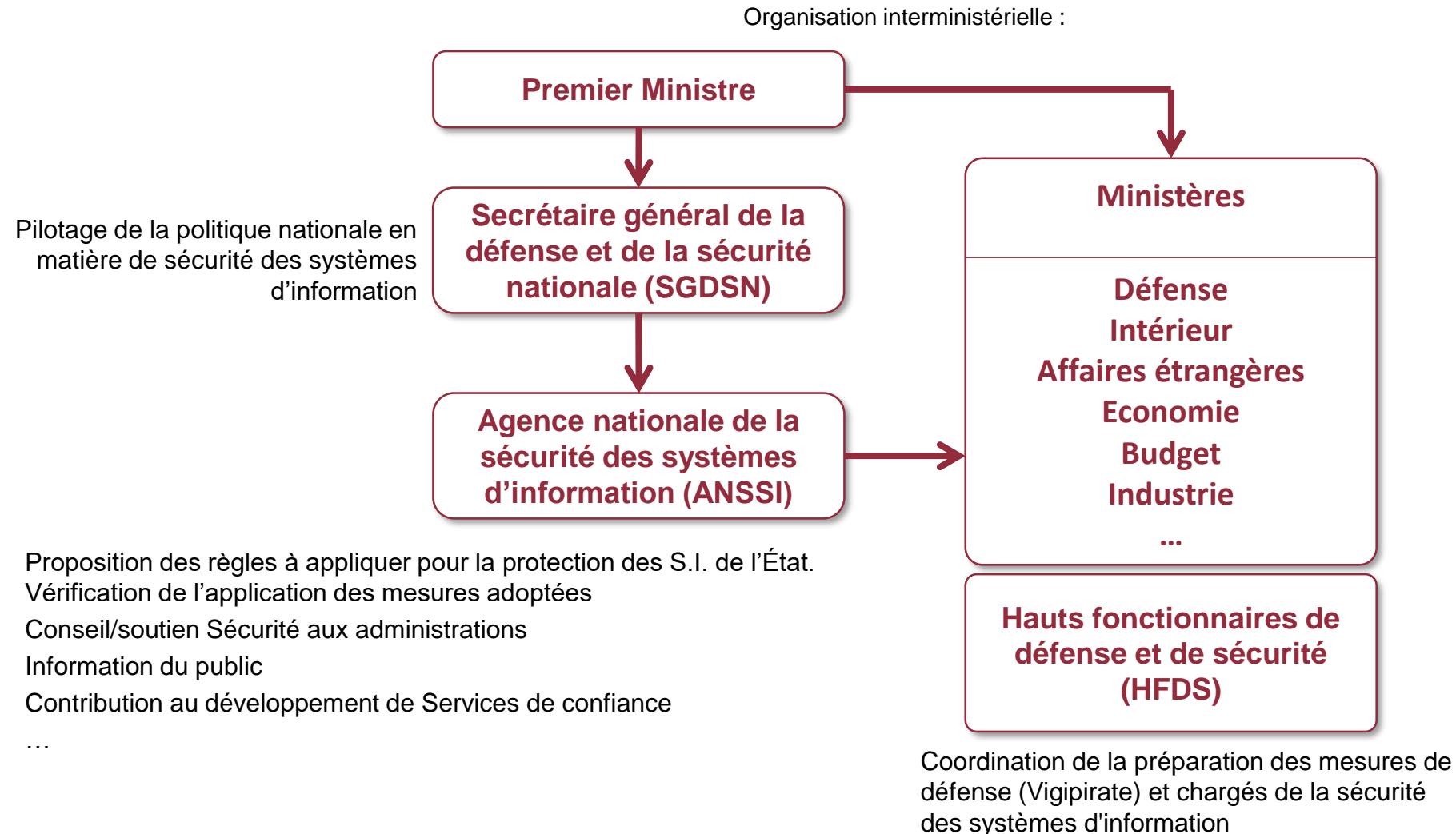


« **Les cyberattaques**, parce qu'elles n'ont pas, jusqu'à présent, causé la mort d'hommes, n'ont pas dans l'opinion l'impact d'actes terroristes. Cependant, dès aujourd'hui, et plus encore à l'horizon du Livre blanc, elles constituent une menace majeure, à forte probabilité et à fort impact potentiel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

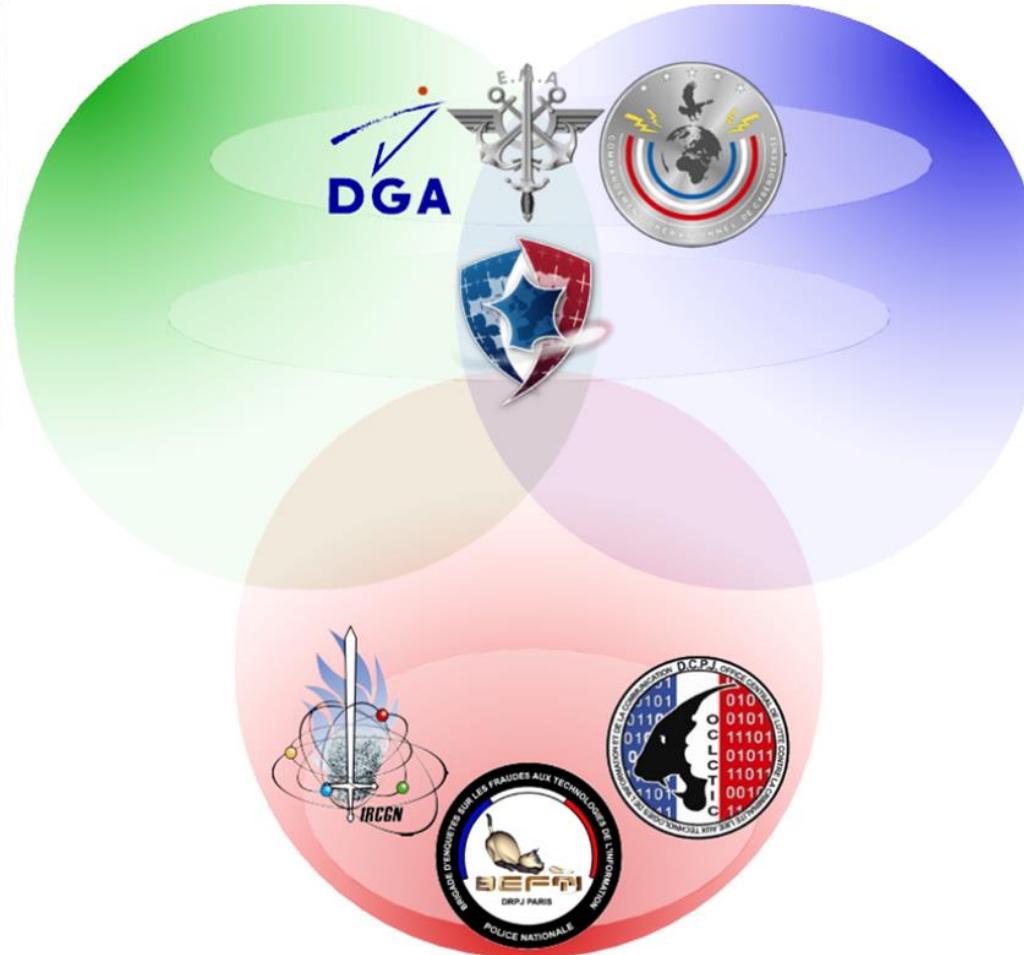
▪ a. L'organisation de la sécurité en France



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



- Préfecture de Police (BEFTI)
- Direction Général de l'Armement (DGA)
- Etat-Major des Armées (EMA)
- Gendarmerie Nationale (IRCGN)
- Police Nationale (OCLCTIC)
- Officier Général "Cyber"

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

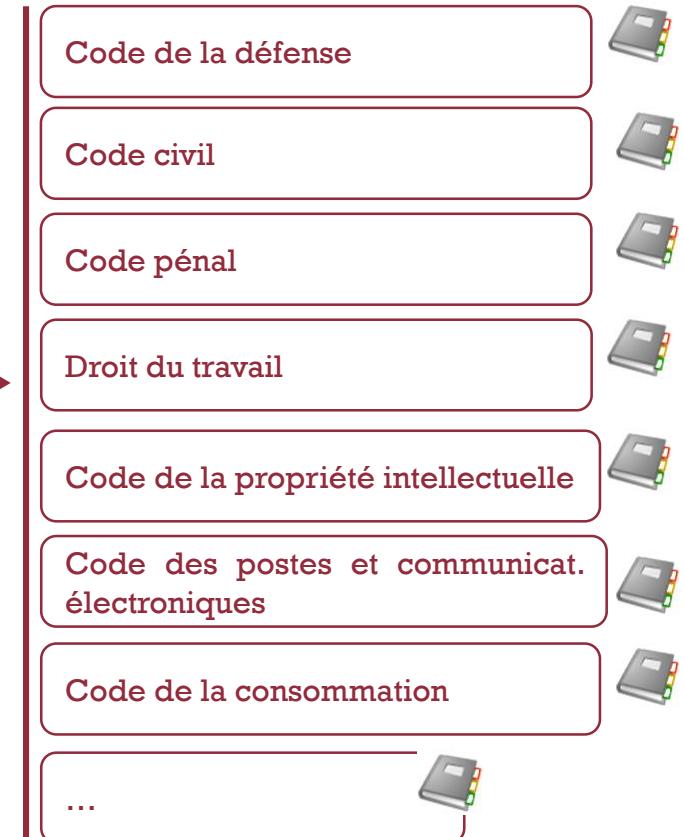
Cybercriminalité

... 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 contreviolents 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

SENSIBILISATION ET INITIATION À LA CYBERSÉCURITÉ

- Module 2 : règles d'hygiène informatique

PLAN DU MODULE

- 1. Connaitre le Système d'Information**
- 2. Maitriser le réseau**
- 3. Sécuriser les terminaux**
- 4. Gérer les utilisateurs**
- 5. Sécuriser physiquement**
- 6. Contrôler la sécurité du S.I.**

1. CONNAÎTRE LE SYSTÈME D'INFORMATION

- a) Identifier les composants du S.I.
- b) Inventorier les biens
- c) Types de réseau
- d) Interconnexion

1. CONNAÎTRE LE SYSTÈME D'INFORMATION

a. Identifier les composants du S.I.

Au-delà de la connaissance des composants du S.I., l'inventaire permettra par la suite de mieux déterminer les menaces et les mesures de protection applicables.

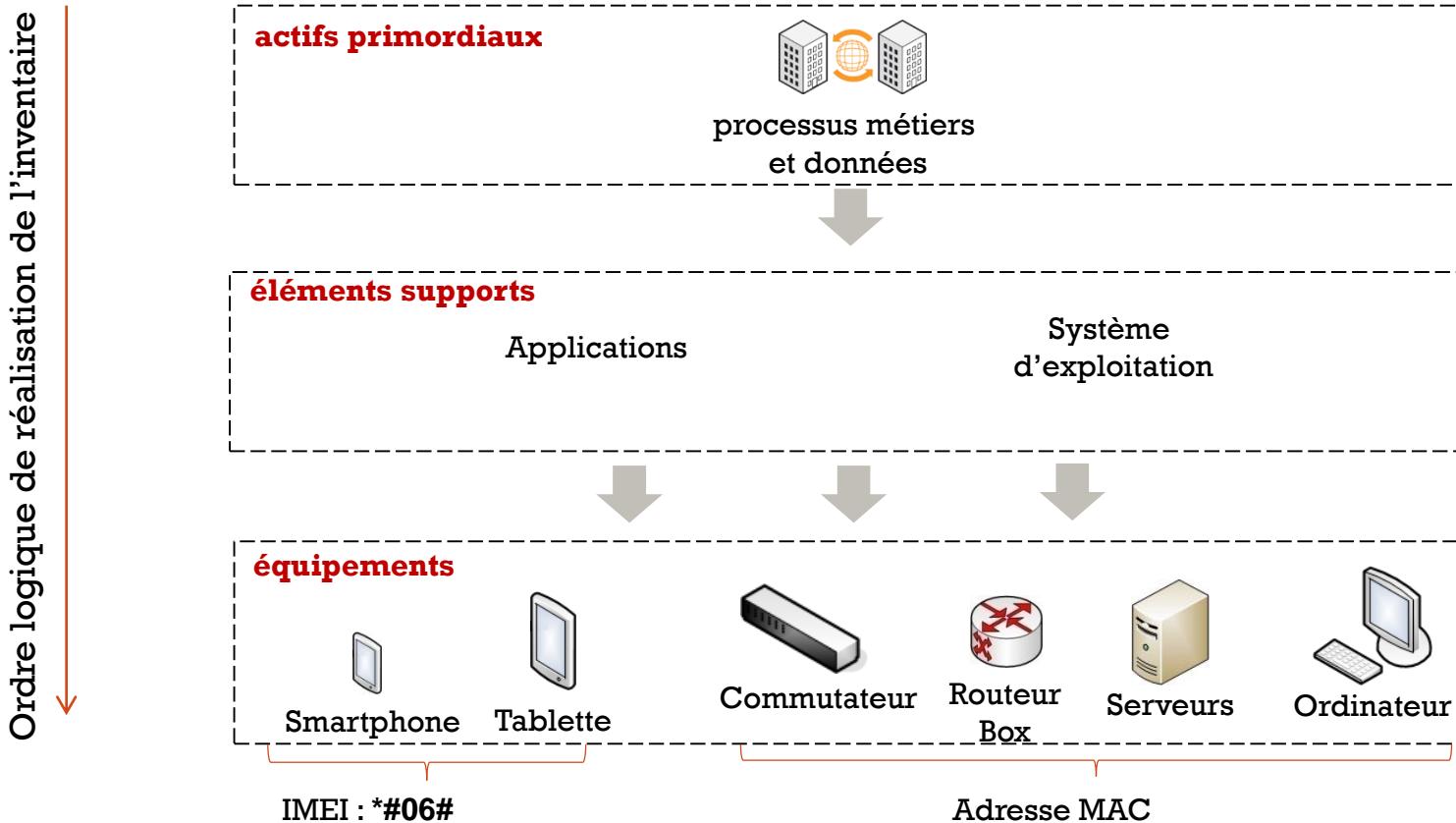
Tout projet sécurité doit donc forcément intégrer un **inventaire des biens**.

L'inventaire des biens doit suivre une **méthodologie logique** afin d'être exhaustif, en commençant par l'inventaire des métiers.

1. CONNAÎTRE LE SYSTÈME D'INFORMATION

a. Identifier les composants du S.I.

Différents éléments composent le SI



Comprendre son S.I. passe par l'identification de ses composants.

1. CONNAÎTRE LE SYSTÈME D'INFORMATION

b. Inventorier les biens

Identifier

- **Les données sensibles :**
 - mots de passe, cartes de crédit, documents personnels, etc.
 - plan marketing, fichier client, brevets, contrats, etc.
- **Les applications** avec leur version : Office 365, navigateur web, etc.
- **Les systèmes d'exploitation** : Android, iOS, Windows, Linux, MacOS, etc.
- **Equipements** : ordinateur, tablette, téléphone, serveur, box, routeur, etc.

Inventorier

- Outil d'identification des ordinateurs en réseau
 - Exemple : ServiceNow, HP OpenView ;
- Outil d'identification des logiciels installés sur un ordinateur/téléphone ainsi que des versions
 - Exemple : Everest.

1. CONNAÎTRE LE SYSTÈME D'INFORMATION

c. Types de réseau

- BAN (Body Area Network) : réseau composé de télé transmetteur utilisé dans le domaine de la santé ;
- PAN (Personal Area Network) : réseau centré autour d'une personne interconnectant ordinateur, téléphone, tablette, voiture... (moins de 10m) ;
- WPAN (Wireless PAN) : réseau PAN sans fil utilisant des technologies telles que : IrDA, ZigBee, Bluetooth, Wireless USB ;
- LAN (Local Area Network) : Réseau local interconnectant plusieurs périphériques et permettant l'échange d'informations entre plusieurs individus ;
- MAN (Metropolitan Area Network) : réseau plus large qu'un LAN et étendu par exemple sur une ville ;
- CAN (Campus Area Network) : réseau s'étendant sur plusieurs LAN, et de la taille d'une université ;
- WAN (Wide Area Network) : réseau d'une étendue nationale ou internationale. Exemple : Internet.

1. CONNAÎTRE LE SYSTÈME D'INFORMATION

d. Interconnexion

Connaitre et maîtriser les points d'interconnexion

- Accès Internet via :
 - Box Internet (ADSL, Fibre, ...) ;
 - téléphone/carte 3G/4G, etc.
- Interconnexion avec d'autres réseaux (universités, partenaires, prestataires, etc.)
 - Liaison dédiée : E1/T1 carrier, fibre noire ;
 - Réseau privé virtuel (VPN) sur un WAN appartenant à un opérateur ou sur Internet ;
 - Liaison satellite.

2. MAITRISER LE RÉSEAU

- a) Sécuriser le réseau interne
- b) BYOD (Bring Your Own Device)
- c) Contrôler les échanges internes
- d) Protéger le réseau interne d'Internet
- e) Accès distant
- f) Sécuriser l'administration
- g) Wifi

2. MAITRISER LE RÉSEAU

a. Sécuriser le réseau interne

Créer des zones dans le réseau interne

- Zones distinctes pour les serveurs, postes de travail, visiteurs ;
- Assurer la confiance par l'authentification mutuelle des composants :
 - chaque composant s'authentifie avant le début de l'échange ;
 - permet d'éviter l'usurpation d'identité.
- Assurer le cloisonnement au moyen de : VLAN, VRF, sous-réseaux et ne pas oublier d'implémenter un mécanisme de filtrage !

Restreindre les accès aux réseaux internes

- 802.1X permet de contrôler l'accès réseau et de s'assurer que l'autorisation n'est accordé qu'après authentification de l'utilisateur ;
- Recourir à l'authentification avant d'autoriser l'accès au réseau :
 - l'authentification peut se faire par l'usage d'un certificat ou d'une carte à puce ;
 - l'authentification est centralisée sur un serveur qui donne les accès en fonction de l'identité de l'utilisateur (Exemple : Serveur Radius).

2. MAITRISER LE RÉSEAU

b. *BYOD (Bring Your Own Device)*

- Le réseau permet de partager des informations, mais aussi de propager les infections de codes malveillants.
- Les terminaux personnels n'ont pas le même niveau de sécurité que les terminaux de l'entreprise / université :
 - Sur un terminal personnel, un utilisateur installe les logiciels de son choix, avec la configuration de son choix. L'antivirus n'est pas forcément à jour ;
 - Sur un terminal professionnel, les logiciels sont installés de manière centralisée, et les sources vérifiées.
- Les terminaux personnels sont connus pour être une source de fuite de données sensibles pour l'entreprise (de façon volontaire ou par erreur).

Le S.I. est un tout, un maillon faible peut affaiblir tout l'ensemble.

2. MAITRISER LE RÉSEAU

c. Contrôler les échanges internes

- **Filtrer les flux pouvant être échangés entre les zones :**
 - identifier les ports réseau utiles ;
 - identifier les protocoles réseau autorisés ;
 - disposer d'une matrice de flux indiquant les flux autorisés et interdits entre les zones.
- **Autoriser explicitement des adresses IP (machines) d'une zone à échanger avec les adresses IP (machines) d'une autre zone**
 - Utiliser une « liste blanche » d'adresse IP pour les échanges, et non pas une liste noire. Une liste noire ne peut en effet jamais être exhaustive, et est forcément d'un intérêt limité.

Appliquer le principe « *Tout ce qui n'est explicitement autorisé est interdit* » lors de la gestion des flux.

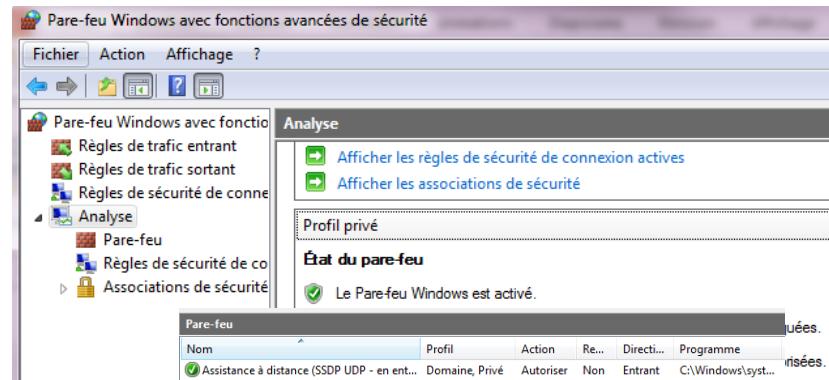
2. MAITRISER LE RÉSEAU

d. Protéger le réseau interne d'Internet

- Le réseau interne est à protéger et est considéré comme « **de confiance** » ;
- Les équipements interagissant avec Internet peuvent être
 - placés dans une zone spéciale appelée « **Zone Démilitarisée (DMZ)** » ;
 - avec un niveau de filtrage et de contrôle plus accru que le réseau interne.
 - protégés d'Internet par des « **pare-feux** » filtrant les échanges de flux
 - Équipement dédié protégeant le réseau ou logiciel « **pare-feu personnel** »

- sous Windows, utiliser le pare-feu par défaut ou un pare-feu tiers (exemple Zone Alarm) ;
- toujours contrôler les connexions entrantes ;
- autoriser les applications au travers du pare-feu, au cas par cas.

- protégés derrière des IDS et des IPS qui peuvent
 - détecter les tentatives d'intrusion ;
 - prévenir les attaques.



The screenshot shows the Windows Firewall with Advanced Security interface. The main window title is "Pare-feu Windows avec fonctions avancées de sécurité". The left pane displays a navigation tree with nodes like "Règles de trafic entrant", "Règles de trafic sortant", "Règles de sécurité de connexion", "Analyse", "Pare-feu", and "Associations de sécurité". The right pane has sections for "Analyse" (with buttons for "Afficher les règles de sécurité de connexion actives" and "Afficher les associations de sécurité") and "État du pare-feu" (with a message "Le Pare-feu Windows est activé"). Below these is a table titled "Pare-feu" showing a list of security rules:

Nom	Profil	Action	Re...	Directio...	Programme
Assistance à distance (SSDP UDP - en entrée)	Domaine, Privé	Autoriser	Non	Entrant	C:\Windows\system32\dhcpcsvc.dll
Assistance à distance (TCP-Entrée)	Domaine, Privé	Autoriser	Non	Entrant	C:\Windows\system32\dhcpcsvc.dll
Assistance à distance (TCP-Entrée)	Domaine, Privé	Bloquer	Non	Entrant	C:\Windows\system32\dhcpcsvc.dll
Assistance à distance (Trafic entrant TCP ...)	Domaine	Autoriser	Non	Entrant	C:\Windows\system32\dhcpcsvc.dll
Assistance à distance (Trafic entrant TCP ...)	Domaine	Bloquer	Non	Entrant	C:\Windows\system32\dhcpcsvc.dll
Assistance à distance (Trafic entrant TCP ...)	Domaine	Autoriser	Non	Entrant	C:\Windows\system32\dhcpcsvc.dll
Bureau à distance (TCP-Entrée)	Domaine, Privé	Autoriser	Non	Entrant	System

2. MAITRISER LE RÉSEAU

e. Accès distant

- Il est possible d'accéder à distance à un réseau pour faire :
 - du télétravail ;
 - de la téléassistance ;
 - de la téléadministration.
- Il est recommandé d'avoir des points d'entrée identifiés pour les accès distants :
 - Serveurs d'authentification : TACACS+, RADIUS ;
 - Concentrateurs VPN ;
 - Remote Access Server (RAS).

2. MAITRISER LE RÉSEAU

e. Accès distant

- Utiliser des moyens sécurisés pour les accès distants :
 - **SSH** au lieu de telnet : pour l'établissement de connexion à distance sur un équipement ;
 - Secure remote desktop : pour la prise en main à distance d'un bureau ;
 - **SFTP** ou **SCP** : pour la copie distante ;
 - **HTTPS** : pour l'accès à une interface Web (Exemple : Teamviewer) ;
- Réseau Privé Virtuel (**VPN**) établit sur un réseau qu'on ne maîtrise pas, tel que Internet :
 - VPN IPSEC : permet l'authentification et le chiffrement. Il est utilisé pour protéger le trafic réseau ;
 - VPN SSL : protège essentiellement le trafic Web, et est facile à déployer.

2. MAITRISER LE RÉSEAU

f. Sécuriser l'administration

▪ Restreindre/Interdire les interfaces d'administration depuis Internet

- L'administration d'un composant ne doit pouvoir se faire que depuis le réseau interne (ouvrir un accès VPN en cas de nécessité d'accéder à distance) ;

▪ Restreindre les accès aux interfaces d'administration sur les sites Web :

- Pour des sites web développés avec des CMS (Content Management System) comme Joomla ou WordPress :
 - Le lien de la page d'administration peut être facilement trouvé (sauf à la modifier) ;
 - Des attaques en « brute force » peuvent être menées pour deviner le mot de passe administrateur ;
 - Modifier le compte « admin » par défaut.

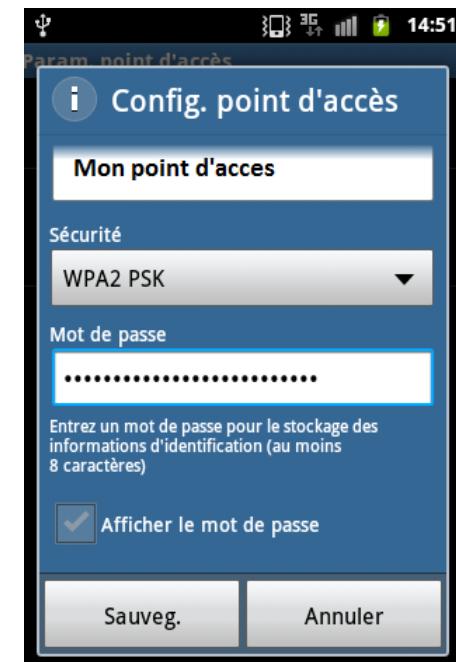
▪ Utiliser un réseau d'administration dédié :

- Ce réseau doit être séparé du réseau de production de manière à ce que seul les postes autorisés puissent s'y connecter ;
- Avoir une liste blanche des administrateurs autorisés à se connecter à ce réseau ;
- Authentifier mutuellement les postes des administrateurs et les équipements à administrer.

2. MAITRISER LE RÉSEAU

g. Wifi

- Pour sécuriser son réseau Wifi (fourni par sa box ou son téléphone), il faut :
 - Protéger la confidentialité des communications en effectuant un chiffrement à l'aide d'une clé :
 - La clé doit être composée de plusieurs caractères alphanumérique(au moins 15).
 - Choisir la technologie WPA2 (**Wi-Fi Protected Access 2**) ;
 - Choisir l'algorithme de chiffrement CCMP (**Counter Cipher Mode Protocol**) lorsque possible ;
 - Modifier le SSID (nom du réseau Wifi fourni) ;
 - Modifier les identifiants fournis par défaut pour accéder à l'interface d'administration :
 - en général, sur les box, saisir l'url « `http://192.168.1.1` » pour atteindre l'interface d'administration.
 - Ne pas divulguer protéger sa clé WIFI.



2. MAITRISER LE RÉSEAU

g. Wifi : WPS

- Ne pas utiliser le WPS (Wi-Fi Protected Setup), notamment fourni sur certaines box internet, car reconnu vulnérable à une attaque par force brute sur le code PIN. Sur les box internet, il est donc préférable de configurer la connexion Wi-Fi manuellement et choisir son propre mot de passe (robuste) ;
- ou cocher l'option qui permet de désactiver automatiquement le WPS au-delà de 5 tentatives de clé.

2. MAITRISER LE RÉSEAU

g. Wifi : Wifi privé vs Wifi public

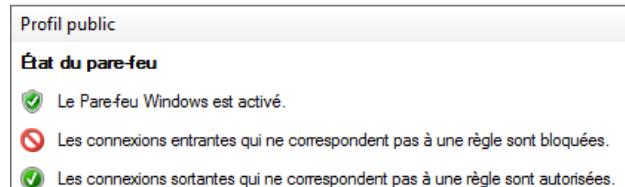
- Le Wifi privé peut être utilisé dans le réseau interne pour donner l'accès à des personnes de confiance. Dans un LAN, on peut utiliser le wifi comme moyen d'interconnexion. On parle alors de WLAN ;
 - Pour ces wifi en entreprise, mettre en place si possible une authentification par certificats, cela évite que tous les utilisateurs partagent le même mot de passe.
- Le Wifi public (hotspots) : est fourni aux personnes « de non confiance » ou au grand public, et est généralement fourni pour un accès Internet uniquement :
 - Hotspot Wifi : Wifi dans les aéroports, McDo, etc.
 - Être conscient que tous les utilisateurs connectés sur le même hotspot peuvent écouter toutes les conversations (sauf si la page WEB visitée est en HTTPS).

2. MAITRISER LE RÉSEAU

g. Wifi : Bonnes pratiques en cas d'usage du Wifi Public

- désactiver les options de partage :
 - arrêter la découverte réseau ;
 - arrêter le partage de fichier et d'imprimantes.

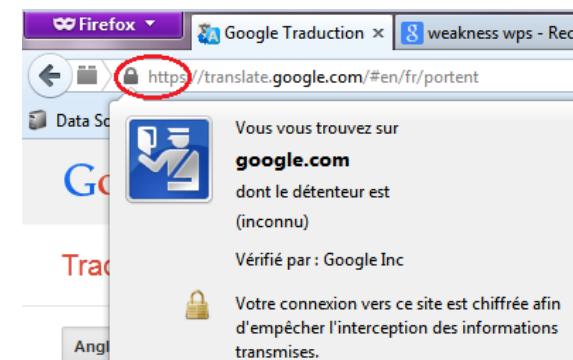
- Activer le pare-feu du poste
 - Sous Windows, un pare-feu existe par défaut :
 - Contrôler les connexions entrantes et lorsque possible, les connexions sortantes ;



- Activer la journalisation.
 - Éviter de se connecter sur des sites peu sécurisés (utilisant du HTTP) ;
 - Vérifier que les communications vers les sites Internet se font en HTTPS.

The screenshot shows the Windows Network and Sharing Center. Under 'Public' settings, it includes:

- Recherche du réseau**: A note about network discovery being activated, with radio buttons for 'Activer la découverte de réseau' (unchecked) and 'Désactiver la découverte de réseau' (checked).
- Partage de fichiers et d'imprimantes**: A note about file and printer sharing being activated, with radio buttons for 'Activer le partage de fichiers et d'imprimantes' (unchecked) and 'Désactiver le partage de fichiers et d'imprimantes' (checked).
- Partage de dossiers publics**: A note about public folder sharing being activated, with radio buttons for 'Activer le partage afin que toute personne avec un accès réseau puisse lire et écrire des fichiers dans les dossiers Public' (unchecked) and 'Désactiver le partage des dossiers Public (les personnes connectées à cet ordinateur peuvent continuer d'accéder à ces dossiers)' (checked).



Si cela est possible, utiliser un VPN sur un Wifi public.

3. SÉCURISER LES TERMINAUX

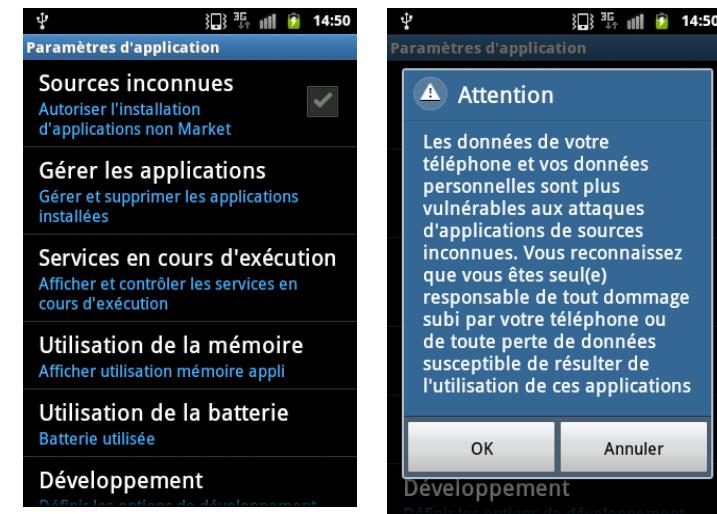
- a) Choisir les applications
- b) Mises à jour logicielles et systèmes
- c) Antivirus / Antimalware / Antispyware
- d) Symptômes de présence des codes malicieux
- e) Protéger les données
- f) Durcissement de configuration des équipements

3. SÉCURISER LES TERMINAUX

a. Choisir les applications

- Pourquoi faut-il être vigilant concernant les logiciels téléchargeables ?
 - On ne connaît pas forcément ni l'auteur, ni le site hébergeant ce logiciel ;
 - Certains escrocs sont spécialisés dans la fourniture de chevaux de Troie : un malware est fourni avec le logiciel, dont l'objectif peut être de récupérer login, mot de passe, numéro de carte bancaire.

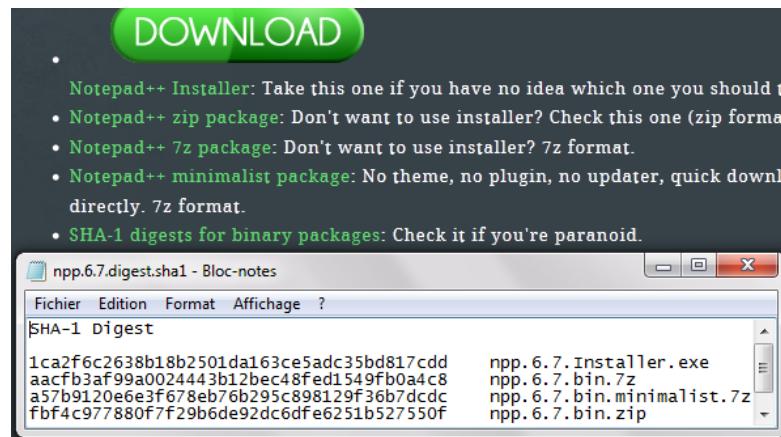
- Préférer des sources « sûres »
 - utiliser des sources « de confiance » pour télécharger les logiciels ;
 - Sous Android : interdire le téléchargement d'application depuis des sources inconnues.
 - utiliser les sites officiels (site de l'éditeur) pour les téléchargements.



3. SÉCURISER LES TERMINAUX

a. Choisir les applications

- Vérifier la signature d'un logiciel
 - recalculer la signature du fichier téléchargé avec la signature (checksum) indiquée sur le site, et comparer.



3. SÉCURISER LES TERMINAUX

a. Choisir les applications

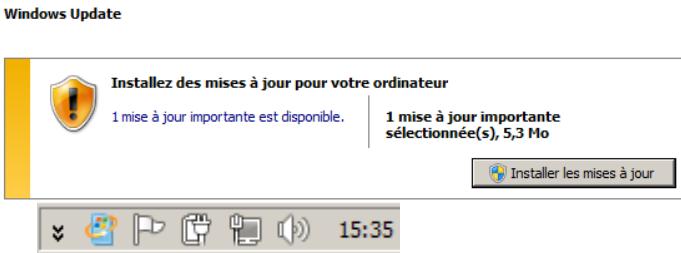
- « Crack » logiciels
 - les sites proposant les « cracks » ou clés gratuites pour les logiciels payants sont souvent truffés de logiciels malveillants ;
 - les versions « crackées » de logiciels contiennent souvent des logiciels malveillants.
- Les logiciels gratuits
 - SnapDo est un pirate de navigateur qui infiltre les navigateurs Internet (Internet Explorer, Google Chrome, et Mozilla Firefox) via des téléchargements de logiciels gratuits.



3. SÉCURISER LES TERMINAUX

b. Mises à jour logicielles et systèmes

- Rôle : apporter des corrections à un(e) logiciel/application afin de corriger un dysfonctionnement ou une vulnérabilité ;
- Les mises à jour s'appliquent :
 - aux applications, aux systèmes d'exploitation, etc.



- En entreprise, les mises à jour s'effectuent de manière centralisée
 - Téléchargement sur des serveurs dédiés exemple serveur WSUS pour Windows ;
 - Déploiement et observation sur des machines de test ;
 - Sauvegarde des machines de production ;
 - Déploiement sur les machines de production.

3. SÉCURISER LES TERMINAUX

b. Mises à jour logicielles et systèmes

- Les mises à jour ne concernent pas que le système d'exploitation : tous les logiciels peuvent présenter des failles et doivent être mis à jour régulièrement également ;
 - Flash, Shockwave, Javascript, les lecteurs PDF sont connus pour nécessiter des mises à jour régulières ;
 - La plupart des logiciels ont une option qui permet une « mise à jour automatique », il est recommandé de l'activer.
- Attention en entreprise, c'est à l'administrateur de planifier et valider les mises à jour (cela inclut notamment des tests préalables de non régression).

3. SÉCURISER LES TERMINAUX

c. *Antivirus / Antimalware / Antispyware*

- Ces logiciels peuvent être :
 - Gratuits :
 - installé par défaut lors de l'achat du terminal ou par l'éditeur du système d'exploitation (Microsoft Security Essential) ;
 - ou manuellement : Avast, Malwarebytes.
 - Payants : par exemple McAfee, Norton Antivirus.
- Ils nécessitent des mises à jour régulières du **moteur** et de la **base antivirale** pour détecter les nouveaux codes malveillants ;
- Lors de l'apparition d'un nouveau code malveillant, des éditeurs de solutions antivirales effectuent des analyses afin de :
 - déterminer la « **signature** » de ce code malveillant pour l'identifier de manière unique ;
 - identifier les moyens de protection et des corrections ;
 - enrichir leur base antivirale avec ces informations.

Éviter d'exécuter les scans gratuits depuis les pages Internet vous indiquant que votre ordinateur est infecté.

3. SÉCURISER LES TERMINAUX

c. *Antivirus / Antimalware / Antispyware*

▪ Doivent être configurés de manière à :

- Télécharger automatiquement les nouvelles signatures (base antivirale) ;
- Être toujours actif (faire attention si votre antivirus est désactivé) ;
- Scanner tout l'ordinateur sans exception de répertoires / fichiers ;
- Effectuer des analyses complètes de manière périodique ;
- Analyser automatiquement de nouveaux périphériques tel que les clés USB ;
- Analyser les emails (entrants et sortants) et la messagerie instantanée.

▪ Limites

- Il n'y a pas de base exhaustive pour les virus ;
- Un code malveillant peut sévir dans un système disposant d'un antivirus et y demeuré indétecté ;
- Les antivirus ne détectent que les virus dont les signatures sont « connues » ;
- De très nombreux codes malveillants sont créés chaque jour.

L'antivirus n'est pas une « arme absolue ». La mise à jour des systèmes et des applications, ainsi qu'une bonne hygiène informatique sont indispensables.

3. SÉCURISER LES TERMINAUX

d. Symptômes de présence des codes malveillants

- Ralentissement
 - du terminal : exemple pendant l'arrêt et le redémarrage ;
 - du débit : la bande passante semble partagée.
- Ouvertures régulières de fenêtres de pop-up et de publicités ;
- Modification de la configuration de votre navigateur web
 - Modification de votre page d'accueil ou de votre moteur de recherche ;
 - Exemple : Snapdo.
 - Présence de nouvelles extensions que vous n'avez pas installées.
- Surconsommation des ressources
 - Réduction de l'espace libre sur disque sans raison ;
 - surcharge du processeur.
- L'antivirus/antimalware ou pare-feu est désactivé sans votre intervention ;
- Les mises à jour système/antivirus/antimalware échouent systématiquement ;
- Messagerie
 - vos contacts (amis/famille) reçoivent des messages que vous n'avez pas envoyés ;
 - votre boîte d'envoi contient des messages que vous n'avez pas envoyé.

3. SÉCURISER LES TERMINAUX

e. Protéger les données

- Lors des échanges par mail
 - chiffrer les pièces jointes ou les données sensibles
 - exemple : AxCrypt, Zed Container ;
 - envoyer le mot de passe (Clé) par un autre moyen : SMS.
- Lors de l'usage du Cloud
 - utiliser des logiciels spécialisés pour protéger/chiffrer vos données dans le Cloud (DropBox, Box, SkyDrive...).



- En effectuant des sauvegardes
 - disque externe ;
 - Cloud.

Chiffrer vos données sensibles avant de les stocker.

3. SÉCURISER LES TERMINAUX

f. Durcissement de configuration des équipements

- Modifier les mots de passe des comptes par défaut ;
 - exemple : administrateur.
- Désinstaller les logiciels/services inutiles (exemple : partage de fichiers) ;
- Désactiver les ports/lecteurs non utilisés ;
 - port série / port USB ;
 - lecteur de disquette ;
 - désactiver le « débogage USB » sur les téléphones.
- Mettre un mot de passe BIOS lors de la phase de démarrage ;
 - Lors du démarrage du poste, appuyer sur « F2 » pour rentrer dans le Setup ;
 - Aller dans l'onglet « Security » pour saisir les mots de passe.
- Désactiver le boot sur des périphériques externes (clé USB, CD Rom) ;
 - Dans le setup (Touche « F2 » lors du démarrage), configurer l'ordre de démarrage pour avoir le disque dur en premier.
- Activer la journalisation.



4. GÉRER LES UTILISATEURS

- a) Attribution de privilèges
- b) Rôles utilisateur
- c) Mots de passe
- d) Autres méthodes d'authentification
- e) Sensibilisation des utilisateurs
- f) Spam
- g) Phishing / Spear phishing / Social engineering
- h) Réagir en tant que victime

4. GÉRER LES UTILISATEURS

a. *Attribution de privilèges : grands principes*

- « Moindre privilège » : n'attribuer aux utilisateurs que les droits dont ils ont besoin pour effectuer leurs tâches ;
 - ne pas donner les privilèges importants à tous les utilisateurs, seulement à ceux qui en ont besoin ;
 - Exemple : le privilège « Administrateur »
 - pour un visiteur qui a juste besoin d'accéder à Internet : ne pas lui donner un accès aux disques ou aux applications sensibles.
- « Besoin d'en connaître » : donner les accès et les privilèges appropriés aux utilisateurs :
 - donner accès seulement aux données nécessaires aux utilisateurs ;
 - restreindre l'accès aux répertoires contenant les données sensibles.

4. GÉRER LES UTILISATEURS

a. Attribution de priviléges : recommandations

- Attribuer les comptes aux utilisateurs de manière nominative ;
 - Un utilisateur = un compte ;
 - Tracer les actions effectuées par chaque utilisateur ;
 - Éviter les comptes partagés entre plusieurs utilisateurs.
- Faire signer une charte d'utilisation du SI, informant sur :
 - La conduite à tenir lors de l'usage du SI ;
 - Actions encouragées :
 - Utiliser son poste pour des recherches, pour le travail qui est confié ;
 - protéger ses moyens d'accès : badge, identifiant, etc.
 - Actions interdites :
 - installer des logiciels malveillants / arrêter les outils de détection de codes malveillants ;
 - porter atteinte à un autre utilisateur du SI.
 - Les conditions et les règles d'utilisation des ressources du S.I. ;
 - Les responsabilités de l'utilisateur et ceux de l'entreprise/université ;
 - Les sanctions internes, pénales, civiles encourues ;
- Sous Windows, la commande « **GPEDIT.msc** » permet de configurer de manière fine les droits des utilisateurs.

4. GÉRER LES UTILISATEURS

a. Attribution de privilèges : procédures d'attribution / retrait de privilèges

- Définir une procédure d'attribution/retrait de privilèges.
 - Tenir à jour une liste des droits attribués à chaque utilisateur ;
 - Chaque nouveau compte utilisateur doit être créé en respectant les principes d'attribution de privilège ;
 - Au besoin, chaque utilisateur doit avoir son répertoire personnel et sa boite aux lettres ;
 - Lorsque qu'un utilisateur n'a plus besoin d'accéder au système (démission, changement de poste...), la procédure de retrait de droit doit :
 - Décrire la désactivation de son compte et la suppression de son compte ;
 - Décrire la procédure de retrait des accès aux locaux (badge, clés).

4. GÉRER LES UTILISATEURS

b. Rôles utilisateur

- Le rôle « **administrateur** » : ayant les privilèges les plus élevés sur le système. Il peut être de plusieurs types :
 - Administrateur système : en charge de l'administration des systèmes, de la gestion des disques ;
 - Administrateur réseau : en charge des équipements réseaux, des règles de filtrage ;
 - Administrateur sécurité : en charge de la journalisation, de la supervision.
- Le rôle « **utilisateur** » : ayant le droit d'utiliser le système et d'accéder à des répertoires sensibles ;
- Le rôle « **invité** » : ayant peu de droits, et pas d'accès aux répertoires contenant les informations sensibles.

4. GÉRER LES UTILISATEURS

c. Mots de passe : politique de mots de passe

- Définir une politique de mot de passe qui oblige à
 - Créer un mot de passe complexe :
 - différent d'un mot sorti du dictionnaire ;
 - différent d'une date de naissance (celle de votre conjoint, enfant...) ;
 - différent d'une partie du nom d'utilisateur, du nom, ou du prénom, etc.
 - Avoir un mot de passe d'au moins **8** caractères (**10** pour les admin) ;
 - Changer régulièrement les mots de passe (tous les 6 mois) ;
 - la fréquence des changements dépend de la sensibilité des systèmes accédés, par exemple le code pour accéder en ligne à son compte bancaire sera changé plus régulièrement.
 - Utiliser un mot de passe pour déverrouiller l'écran de veille.
- Consulter les recommandations élaborées par l'ANSSI.

<http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/mot-de-passe.html>

4. GÉRER LES UTILISATEURS

c. Mots de passe : mémorisation

- Ne pas choisir le même mot de passe pour différents comptes.
 - Même si ce principe devient difficile à respecter au vu du nombre de mots de passe que les utilisateurs doivent se rappeler ;
 - A minima, **ne jamais réutiliser son mot de passe de messagerie**. Le compte email devient en effet le pivot numérique de chacun.
 - En cas de perte de mot de passe, c'est souvent grâce à la boite email que l'on est en mesure d'en régénérer un nouveau ;
 - L'email sert aux sites marchands pour nous identifier lors de l'ouverture d'un compte ;
 - Si le compte email se fait pirater, c'est une partie significative de la vie numérique de l'utilisateur qui est affectée (usurpation d'identité, suppression malveillante de documents, changement forcé de mots de passe et impossibilité de les régénérer...).

4. GÉRER LES UTILISATEURS

c. Mots de passe : aide-mémoire

- Aide-mémoire pour construire des mots de passe complexes :
 - Choisir une phrase comme mot de passe, on parle encore de « **passphrase** ».
 - Exemple : « Aujourd'hui je vais à l'aéroport. »
 - Ne garder que la première lettre de chaque mot puis un mot complet
 - Ajvàlaéroport
 - remplacer « s » par « \$ », les « e » par « 3 » ;
 - Ajvàl@3r0port
- Le mot de passe est personnel et doit être mémorisé
 - ne pas écrire les mots de passe sur les post-it ;
 - Il existe des solutions pour stocker les mots de passe sous forme sécurisée (voir diapositive suivante).

Les outils pour deviner les mots de passe, prennent parfois en compte le remplacement de « a » par « @ ».

4. GÉRER LES UTILISATEURS

c. Mots de passe : stockage des mots de passe

- Toujours stocker les mots de passe sous forme chiffrés
 - Mauvais exemple : Sony, répertoire nommé « Password » et contenant les mots de passe « en clair » ;
 - Utiliser des « porte-feuilles » de mots de passe :
 - Dashlane - KeyPass – 1Password ;
 - ou créer votre « porte-feuille », chiffré et protégé par un mot de passe fort.
 - **Ne pas enregistrer les mots de passe sur les navigateurs Web.**



Face aux limites des mots de passe et à leur difficulté d'utilisation, de nouveaux moyens d'authentification sont proposés.

4. GÉRER LES UTILISATEURS

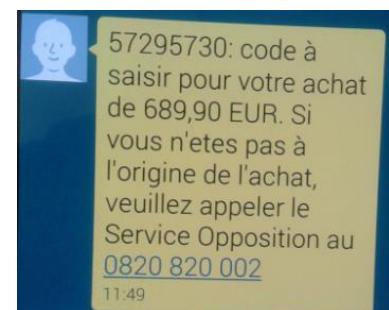
d. Autres méthodes d'authentification

- Biométrie ;
 - permet l'authentification par la lecture des attributs physiques peu changeant d'une personne : empreinte digitale, voix, rétine, etc. ;
- Carte à puce + code pin ;
- SSO : Single Sign-On ;
 - L'utilisation du SSO permet d'éviter que les utilisateurs aient à ressaisir leurs mots de passe (utilisation d'un seul formulaire d'authentification pour accéder à différents services).
- OTP(One Time Password).
 - Généré à chaque demande et utilisable une seule fois. Sa durée de validité très courte :



Token Safenet

- un OTP peut être un code de validation de paiement en ligne reçu par sms ;
- ou généré par un générateur matériel de jetons sécurisés.



4. GÉRER LES UTILISATEURS

e. *Sensibilisation des utilisateurs*

- Se tenir informé de l'actualité liée à la sécurité :
 - des vulnérabilités publiées ;
 - fuite d'information : Sony ;
 - « scam » arnaques sur Internet : arnaque à la nigériane, etc.
- Faire attention aux pièces jointes (même pour les expéditeurs connus).
 - télécharger d'abord et faire un scan avec l'antivirus, avant d'ouvrir la pièce jointe.

4. GÉRER LES UTILISATEURS

e. Sensibilisation des utilisateurs

- Désactiver l'exécution des liens hypertextes et l'affichage des images dans les mails ;
 - Il est préférable de copier et coller le lien hypertexte dans le navigateur. En effet, une technique dans le phishing consiste à faire afficher un lien qui paraît légitime à la lecture, mais qui pointe en fait vers une site malveillant. Cette technique ne fonctionne que si on clique sur le lien.
- Faire attention aux ralentissements/lenteurs de son poste ;
- Applications web : penser à cliquer sur le bouton déconnecter lorsqu'on a fini de surfer sur le site afin de désactiver le cookie ;
- Déconnecter son poste lors qu'il n'est pas utilisé.

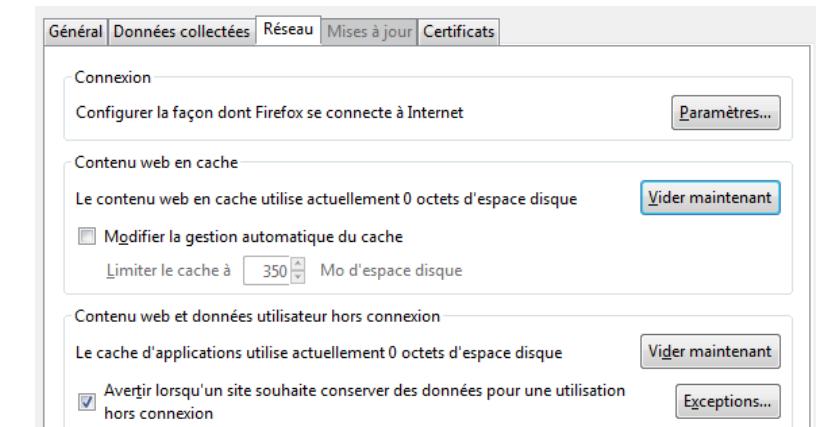
4. GÉRER LES UTILISATEURS

e. Sensibilisation des utilisateurs

- Éviter les sites dont les certificats proposés ne sont pas reconnus ;



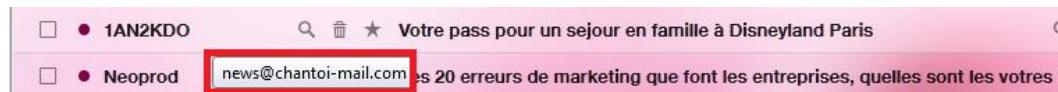
- Dans la mesure du possible, naviguer toujours en « https »
 - Cela est d'autant plus important sur les hotspots publics !
- Effacer régulièrement l'historique de navigation, les fichiers temporaires, les cookies votre navigateur Web.



4. GÉRER LES UTILISATEURS

f. Spam

- Traiter le spam
 - protéger son adresse mail ;
 - au besoin, créer une adresse poubelle : xxx@yopmail.com ;
 - marquer les mails indésirables comme tel afin d'affiner la politique de détection des spams ;
 - ne pas ouvrir les spams, et ne pas cliquer sur les liens contenus.
- Faire attention aux mails envoyés dont l'émetteur est inconnu ;



- Faire attention aux contenus des mails.

P. St, You are receiving this message because you opted-in your email address
@yahoo.com to receive emails from diploe.antsy.bgxxtbx.com.

If you would like to be removed from our mailing list, please [click here](#).

To ensure ongoing optimal receipt of these communications, please add
customerservice@tabard.bgxxtbx.com to your address book.

If, for any reason, this promotion is not capable of running as planned, sponsor reserves the right to
cancel, terminate, modify or suspend the promotion. This includes, but is not limited to, infection by
computer virus, bugs, tampering, unauthorized intervention, fraud, technical failures or any other causes
beyond the control of the sponsor. Why did the Onion Price Go Up So Suddenly?. . Because Rajnikant
Ordered An Onion Dosa. ! :)

4. GÉRER LES UTILISATEURS

g. Phishing / Spear phishing / Social engineering

- Ne pas donner suite au mail, coup de fil vous demandant de :
 - Rappeler rapidement votre conseiller bancaire alors que vous ne l'avez pas contacté ;
 - Donner des informations personnelles parce que vous avez gagné un voyage, un prix, etc.
 - D'envoyer votre mot de passe/code bancaire/code pin par mail sous le prétexte urgent :
 - d'éviter la fermeture de votre adresse mail (car vérification en cours) ;
 - de valider l'existence de votre carte bancaire désactivée, etc.
 - De faire un transfert d'argent à un de vos contacts dans le besoin à l'étranger.

En cas de doute, renseignez-vous mais ne répondez pas au mail.

4. GÉRER LES UTILISATEURS

g. Phishing / Spear phishing / Social engineering

- Limiter les informations que vous partagez par les réseaux sociaux ou mail ;
 - Date de départ en voyage ;
 - <http://pleaserobme.com> : sur la base de tweet (position) indique les maisons vides.
 - Informations personnelles ;
 - Données (photos/vidéos) potentiellement compromettantes ;
 - Chantage menant à des suicides d'adolescents « **chantage à webcam** »
 - « Le jeune homme, prénommé Gauthier, a mis fin à ses jours le 10 octobre après avoir été victime d'un chantage sur [Facebook](#) de la part d'une jeune fille avec qui il venait de faire virtuellement connaissance. »
 - En janvier, Cédric, 17 ans, s'est pendu dans sa chambre à Marseille, 3 mois après avoir été piégé au cours d'un "plan webcam".
- Quelques liens utiles :
 - <http://www.arnaque-chantage-webcam.com/>
 - <http://www.laveudunet.com/>
 - <http://blog.mavieprivee.fr/post/34628211803/chantage-a-la-webcam>.

4. GÉRER LES UTILISATEURS

h. Réagir en tant que victime

- Ne jamais payer de rançons ;
- En cas de chantage / usurpation d'identité / atteinte à la réputation :
 - Ne communiquez plus avec l'escroc ;
 - bloquer ses messages / son contact.
 - Signalez et recevez de l'aide ;
 - faire bloquer ce contact sur le site du chat, ou sur Facebook ou Skype ;
 - exercer le droit à l'oubli sur Google : https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=fr;
 - signaler : <https://www.internet-signalement.gouv.fr/>
 - pour les mineurs : <http://www.netecoute.fr/>
- En cas de ransomware (rançongiciel) :
 - En entreprise ou à l'université : signalez aux responsables informatiques ;
 - A la maison : rechercher de l'aide sur des sites et forums spécialisés :
 - <http://stopransomware.fr/nettoyer-son-ordinateur/>
 - Les sites d'éditeurs de solutions antivirales : Symantec, etc.
- Porter plainte à la police ou à la gendarmerie.

5. SÉCURISER PHYSIQUEMENT

- a) Protection physique des locaux
- b) Imprimantes / Photocopieuses
- c) Sécuriser les équipements

5. SÉCURISER PHYSIQUEMENT

a. Protection physique des locaux

- Protéger physiquement les locaux contenant les biens sensibles :
 - Contrôler l'accès aux locaux : usage de badges par exemple ;
 - Utiliser des alarmes pour identifier les intrusions ;
 - Protéger les clés ou badges dans des coffres par exemple.
- Les prises d'accès réseau doivent être protégées de manière à être inaccessibles aux visiteurs/personnes mal intentionnées ;
 - Si les prises d'accès réseau doivent être exposées, ne pas les connecter au réseau. Mais plutôt le faire au besoin et désactiver ensuite.
- Protéger contre les incidents environnementaux :
 - Incendie : extincteur, détecteur de fumée, etc.
 - Inondation : s'installer en zone non inondable, surélever les éléments, etc.
 - Panne électrique : utiliser des onduleurs, etc.

5. SÉCURISER PHYSIQUEMENT

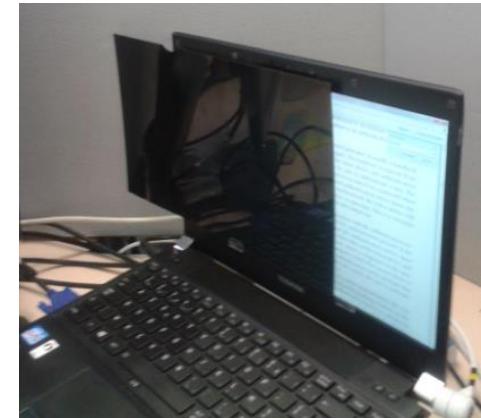
b. Imprimantes / Photocopieuses

- Faire attention lors des photocopies à ne pas oublier les originaux ;
- Aller rapidement retirer les documents imprimés pour éviter que des informations sensibles soient révélées ;
- Ne pas oublier que les imprimantes disposent :
 - De disques durs ;
 - D'historique des impressions : dont les titres de documents pourraient être révélateurs ;
 - De configuration IP pouvant être usurpée.
- Les documents papiers sensibles doivent détruits à la déchiqueteuse ;
- Les imprimantes ne doivent être accessibles depuis Internet.

5. SÉCURISER PHYSIQUEMENT

c. Sécuriser les équipements

- Attacher avec un câble de sécurité les équipements le permettant ;
- Protéger l'accès aux équipements :
 - Avoir un code/mot de passe pour restreindre l'accès à son équipement :
 - lecteur d'empreinte ou signe sur téléphone ;
 - code PIN ou mot de passe ;
 - Demander un code/mot de passe pour sortir de la veille.
- Verrouiller son écran en cas d'inactivité de quelques minutes ;
- Faire attention aux médias USB :
 - Des clés USB piégées sont parfois offertes ou abandonnées ;
 - Toujours scanner (anti-virus) une clé USB avant de l'utiliser.
 - Utiliser les filtres de confidentialité d'écran ;
 - Écran d'ordinateur (fixe, portable) ;
 - Écran de téléphone.



6. CONTRÔLER LA SÉCURITÉ DU S.I.

- a) Contrat/Maintenance/Professional Services
- b) Surveiller/Superviser
- c) Incidents de sécurité
- d) Plans de secours
- e) Audit

6. CONTRÔLER LA SÉCURITÉ DU S.I.

a. *Contrat/Maintenance/Professional Services*

- Lors de l'achat de :
 - matériel : souscrire à des contrats de maintenance ou d'assurance pour vous garantir une assistance en cas de difficulté ;
 - application : souscrire à des contrats de support et d'assistance.
 - niveau 1 : description et enregistrement du problème rencontré. Conseil/information basique ;
 - niveau 2 : intervention de technicien ;
 - niveau 3 : intervention d'expert.
- SLA (Service Level Agreement) : indique le niveau de service garanti par le prestataire pour une prestation de service donnée.
 - Exemple : couverture 3G ou 4G.

6. CONTRÔLER LA SÉCURITÉ DU S.I.

a. *Contrat/Maintenance/Professional Services*

- Cyber-assurance : est une assurance visant à indemniser et assister les victimes de cyber-attaque (fuite de données, attaque à la e-réputation...) :
 - Exemple : AXA propose pour les particuliers « Protection Familiale Intégr@ale »
 - Noter que la souscription d'une assurance est considérée comme une mesure de sécurité permettant de réduire les risques portant sur l'entreprise (au même titre qu'une assurance habitation n'empêchera pas un incendie, mais compensera/limitera les pertes financières de la victime).

Souscrire à des services d'assurance/support/maintenance pour les composants sensibles.

6. CONTRÔLER LA SÉCURITÉ DU S.I.

b. Surveiller / Superviser

- Activer la journalisation d'évènements ;
 - Enregistrer les tentatives d'accès réussies ou pas ;
 - Enregistrer les tentatives de modifications d'informations sensibles ;
 - Etc.
- Consulter les journaux d'évènements ;
- Définir une politique de supervision :
 - définir les seuils : au-delà de tel taux d'occupation du disque, recevoir une alerte ;
 - Définir le type d'alerte souhaité : SMS, mail, etc.

6. CONTRÔLER LA SÉCURITÉ DU S.I.

c. *Incidents de sécurité : catégories d'incidents*

- Divulgation d'information personnelle ;
 - carte de crédit, vol d'identité, numéro de sécurité sociale, etc.
- Déni de service ;
 - entrant ou sortant.
- Activité causée par un code malveillant ;
 - Vers, virus, keylogger, Rootkit.
- Enquête et activité criminelle ;
 - Vol de terminal, fraude, pornographie infantile.
- Non respect de la politique de sécurité ;
 - partage de mot de passe.
- Défacement Web ;
 - Redirection de site, défaçtement d'un site internet.
- Vulnérabilité non corrigée.
 - système/application vulnérable, non application d'un correctif important.

6. CONTRÔLER LA SÉCURITÉ DU S.I.

c. *Incidents de sécurité : gestion des incidents de sécurité*

- Un processus de gestion des incidents de sécurité permet de :
 - Réagir rapidement et de réduire l'impact en cas d'incident ;
 - Améliorer la prévention et la sensibilisation ;
 - Déetecter et d'identifier les incidents ;
 - Améliorer le niveau de sécurité.
- Exemple de réaction en cas d'une infection virale :
 - déconnecter le poste du réseau ou d'Internet, sans l'éteindre ;
 - S'assurer que l'antivirus/antimalware est à jour avec les dernières signatures ;
 - Exécuter le scan complet (en « mode sans échec » par exemple) avec un antivirus ;
 - Contacter un spécialiste au besoin ;
 - Chercher à identifier la cause.

La norme ISO 27035 décrit le processus de gestion des incidents.

6. CONTRÔLER LA SÉCURITÉ DU S.I.

d. Plan de secours

- Avoir un plan de secours en cas de dysfonctionnement important (électrique, télécom...) :
 - Double alimentation :
 - pour un téléphone : batterie de secours ;
 - ordinateur/serveur : onduleur, batterie de secours, groupe électrogène.
 - Accès Internet :
 - utiliser son téléphone comme modem en cas de dysfonctionnement de sa Box ;
 - En entreprise, souscription à une offre Internet comme ligne de secours fournie par un opérateur différent.
 - Avoir une sauvegarde de ses données en cas de panne de son disque dur.
- En entreprise, il y a des :
 - PRA : Plan de Reprise d'Activité qui permet de « reprendre » après une interruption inattendue comme la perte d'un site de travail ;
 - Exemple : utilisateur d'un site de secours « B » et déplacement du personnel en cas d'incendie dans le site principal « A »
 - PCA : Plan de Continuité d'Activité qui permet de s'assurer que l'activité ne s'arrêtera pas ;
 - Exemple : usage d'une architecture réseau redondée en haute disponibilité.
 - Routeur en actif/actif.
 - Les PCA et les PRA doivent être testés et mis à jour régulièrement.

6. CONTRÔLER LA SÉCURITÉ DU S.I.

e. Audit : informations générales

- Un audit peut porter sur tout ou partie du S.I., une application, etc.
- Le but de l'audit est généralement :
 - d'évaluer le niveau de sécurité par rapport à un référentiel (interne ou à une norme) ;
 - obtenir un agrément ou une certification :
 - ASIP Santé, PCI-DSS, 27001, etc.
 - trouver des faiblesses et les corriger :
 - site Web ;
 - application développée « in-house »
- L'audit peut être réalisé par :
 - des experts appelés « auditeur sécurité », « pen-testeur »
 - des sociétés spécialisées.
- Un cadre légal et contractuel est requis pour les audits :
 - Pour les audits de site Web, il faut l'accord du propriétaire du site (par exemple l'association étudiante), de l'hébergeur du site (OVH ou l'université) et parfois celui de l'opérateur ;
 - L'auditeur doit indiquer à partir de quelles adresses IP publiques son audit sera effectué ;
 - L'auditeur doit s'engager à ne pas provoquer d'incident de sécurité (déni de service par exemple) au cours de son audit.

6. CONTRÔLER LA SÉCURITÉ DU S.I.

e. Audit : types d'audit

- **Audit de conformité pour déterminer les écarts par rapport à un référentiel :**
 - Politique de sécurité interne ou exigences de sécurité d'un cahier de charge ;
 - Norme internationale : exemple 27001, PCI-DSS, ASIP Santé.
- **Audit en vue de l'obtention d'un(e) certification/agrément :**
 - Audit physique des datacenters pour obtention d'un agrément SAS 70 ;
 - Audit 27001 en vue de démontrer la bonne application des principes de la norme.
- **Audit Technique.**
 - « Boite noire » ou « Pentest » : sans aucun accès, on évalue le système (site web par exemple) du point de vue d'un attaquant quelconque ;
 - « Boite grise » ou « test du stagiaire » : on dispose de quelques informations et on essaye d'élever ses priviléges ;
 - « Boite blanche » pour faire des « audits de configuration » par exemple. On dispose d'accès, y compris administrateur et on évalue le système par rapport à un référentiel ;
 - « Forensic » ou « Post-mortem » : effectuer sur un système après une attaque.

SENSIBILISATION ET INITIATION À LA CYBERSÉCURITÉ

Module 3 : les aspects réseau et applicatifs

PLAN DU MODULE

- 1. La sécurité du protocole IP**
- 2. Sécurisation d'un réseau**
- 3. Les bases de la cryptographie**
- 4. La sécurité des applications web**

1. LA SÉCURITÉ DU PROTOCOLE IP

- a) Préambule
- b) Exemple d'attaque par réflexion
- c) Exemples d'écoute de trafic
- d) Exemple de modification du routage des datagrammes IP
- e) Sécurisation du protocole IP

1. LA SÉCURITÉ DU PROTOCOLE IP

a. Préambule

Lorsqu'ils ont été conçus, le protocole IP et les protocoles associés (TCP, UDP, ICMP, routage...) n'ont pas pris en compte la sécurité

- « Concept sécurité » inconnu à l'époque, personne n'imaginait que ces protocoles pourraient être détournés à des fins malveillantes ;
- **Aucun mécanisme de sécurité n'est donc implémenté au sein de ces protocoles.**

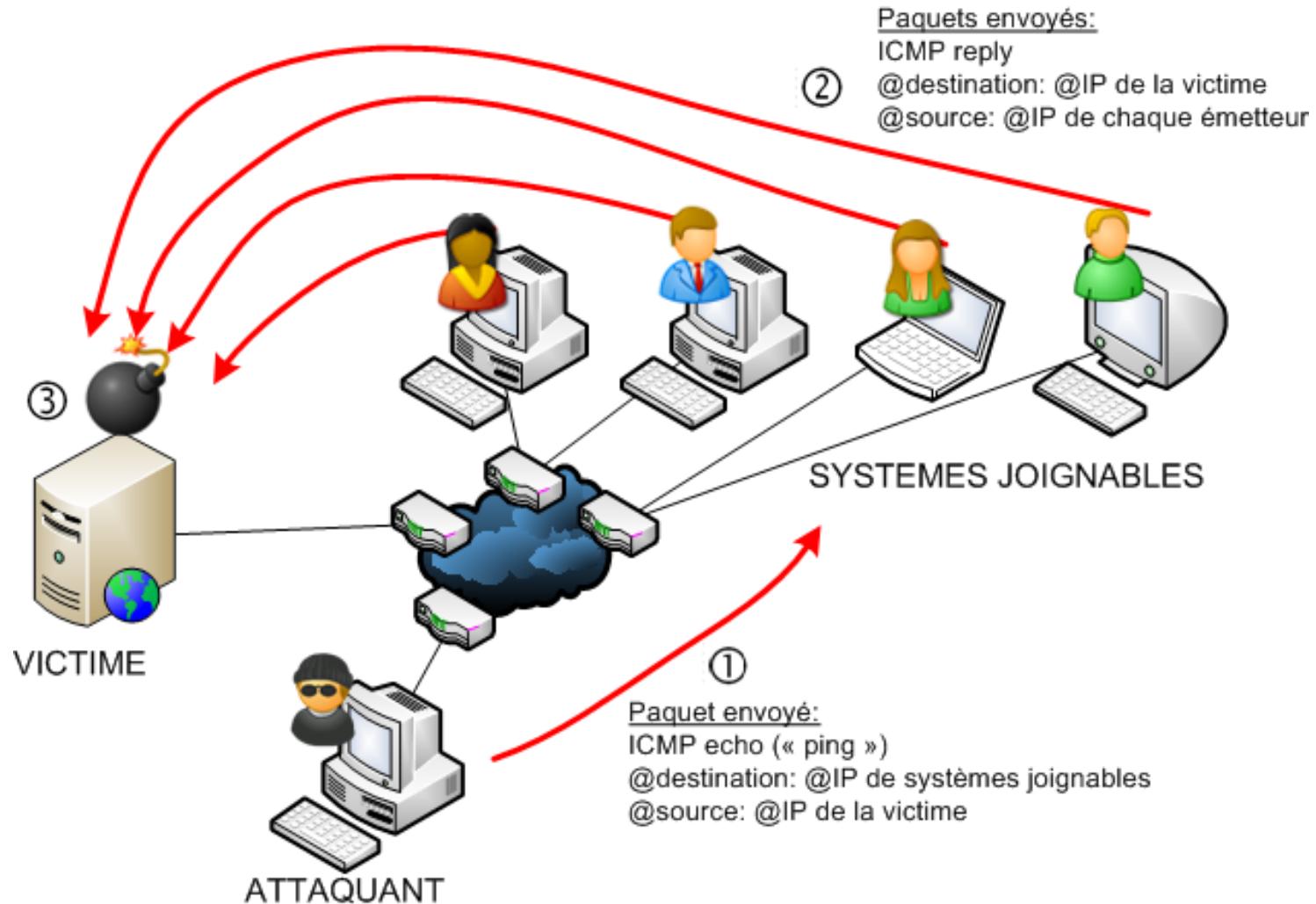
Quelques exemples de faiblesses de ces protocoles

- **Absence d'authentification des émetteurs et récepteurs** d'un datagramme : usurpation d'adresse IP possible ;
- **Absence de chiffrement des données**, celles-ci sont donc transmises en clair. Un hacker positionné sur un réseau peut donc écouter les connexions et accéder aux données ;(Man In The Middle)
- **Le routage des datagrammes peut être modifié** de façon à rediriger les datagrammes vers un autre destinataire ;
- Note : l'exploitation de ces faiblesses nécessite des prérequis techniques, i.e. elles ne sont pas systématiquement applicables à tous les réseaux.

Les diapositives suivantes illustrent ces faiblesses.

1. LA SÉCURITÉ DU PROTOCOLE IP

b. Exemple d'attaque par réflexion



1. LA SÉCURITÉ DU PROTOCOLE IP

b. Exemple d'attaque par réflexion

But de l'attaque

- porter atteinte aux performances d'un système cible (déni de service).

Quelles sont les caractéristiques de l'attaque ?

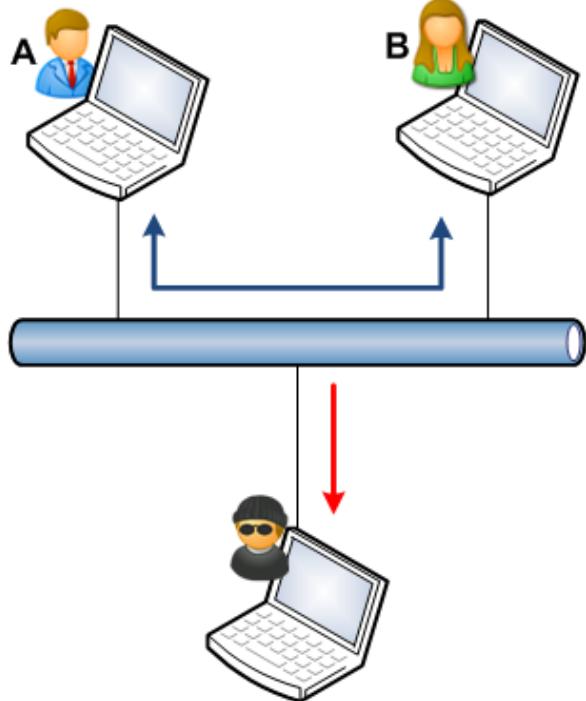
- usurpation d'adresse IP ;
- réflexion de trafic en ayant recours à des systèmes tiers « innocents ».

Séquences de l'attaque

- ① Un attaquant envoie des paquets PING à des systèmes tiers joignables en indiquant l'@IP de la future victime comme @IP source ;
- ② Chaque système pense ainsi recevoir un PING de la part d'un système distant, et chacun va répondre à ce PING ;
- ③ Avec suffisamment de ressources, l'attaquant sera en mesure de faire générer suffisamment de trafic pour affecter les performances de la victime.

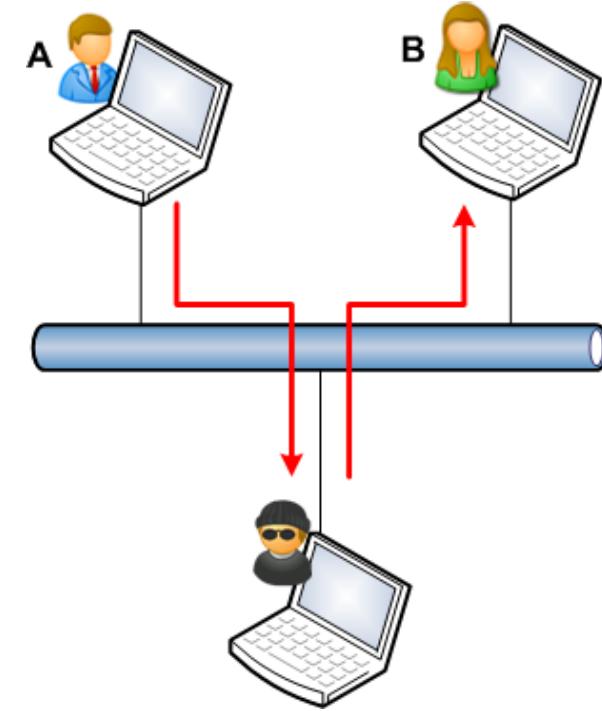
1. LA SÉCURITÉ DU PROTOCOLE IP

c. Exemples d'écoute de trafic



Ecoute passive

L'attaquant est en mesure d'écouter les conversations entre A et B (atteinte à la **confidentialité** des échanges).

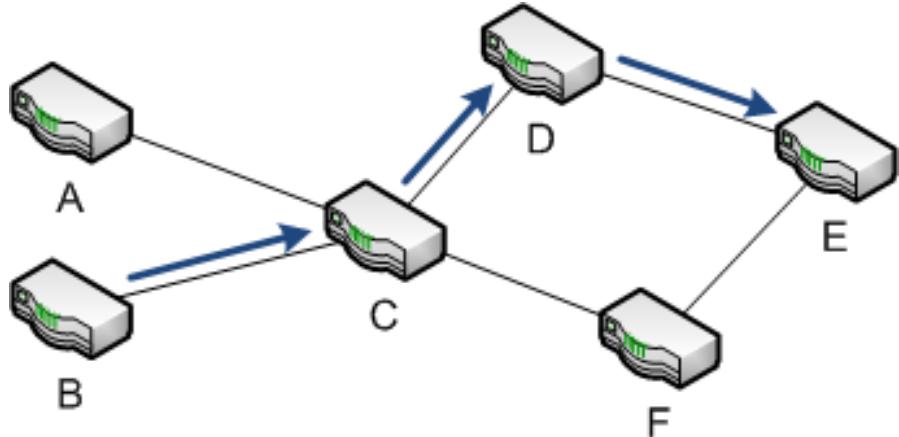


Ecoute active

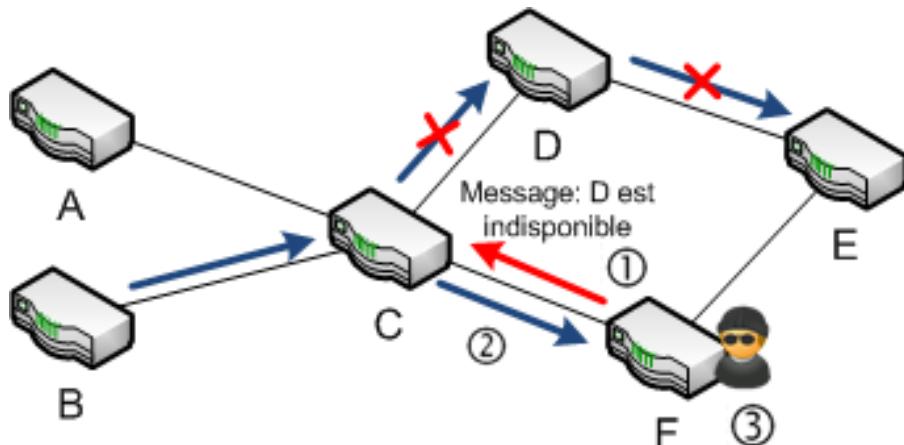
L'attaquant est en mesure de s'insérer dans la conversation entre A et B sans que ceux-ci le sachent (atteinte à la **confidentialité** et à l'**intégrité** des échanges).

1. LA SÉCURITÉ DU PROTOCOLE IP

d. Exemple de modification du routage des datagrammes IP



Chaque routeur possède une table de routage qui indique vers quel routeur voisin transmettre les datagrammes. Cette table peut être mise à jour dynamiquement en fonction des événements réseaux (protocoles BGP, RIP, OSPF, etc.).



But de l'attaque : **dérouter les paquets** à destination du réseau E, vers le réseau F maitrisé par l'attaquant.

Méthode :

- ① L'attaquant utilise une faiblesse du protocole de routage pour indiquer au routeur C que le routeur D est indisponible, et que le routeur F peut router les paquets vers E ;
- ② le routeur C transfère donc à F les paquets pour E, afin qu'ils puissent être routés à destination ;
- ③ Selon le but visé par l'attaquant, celui-ci peut décider de router ou non les paquets vers E.

1. LA SÉCURITÉ DU PROTOCOLE IP

e. Sécurisation du protocole IP

Ainsi, il est nécessaire de **mettre en œuvre des mécanismes de sécurité complémentaires** afin de réduire et maîtriser les risques émanant des protocoles historiques régissant les réseaux.

Exemple de mécanismes :

- Chiffrement des communications ;
- Authentification des entités ;
- Cloisonnement réseau ;
- Filtrage ;
- Dimensionnement adapté des infrastructures ;
- Règles de renforcement des configurations des équipements ;
- Supervision des équipements ;
- etc.

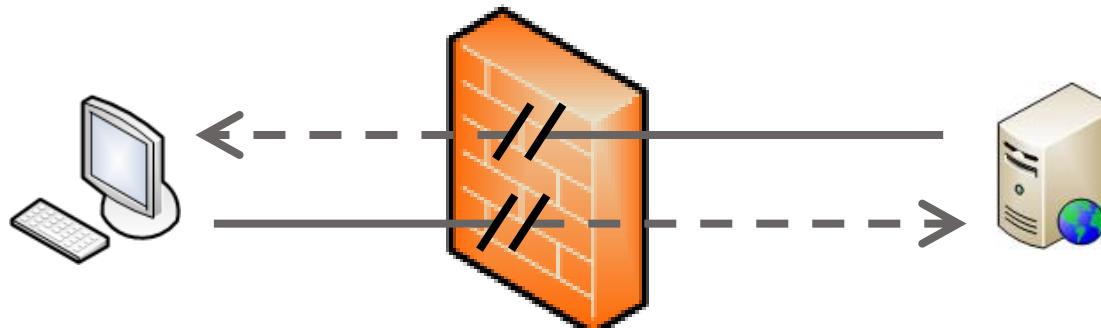
2. SÉCURISATION D'UN RÉSEAU

- a) Pare-feu
- b) Répartiteur de charge
- c) Anti-virus
- d) IDS et IPS
- e) VPN
- f) Segmentation
- g) Exemple pratique de sécurisation avec un réseau simple

2. SÉCURISATION D'UN RÉSEAU

a. Pare-feu

- **Équipement en coupure entre 2 ou plusieurs réseaux ;**
- Inspecte les paquets réseaux entrants et sortants d'un réseau à l'autre ;
- Implémente un **mécanisme de filtrage basé sur des règles** : il ne transmet donc que les paquets réseaux qui respectent les règles de filtrage implémentées dans la configuration du pare-feu.



Pour chaque flux entrant ou sortant, le pare-feu interroge ses règles de filtrage pour déterminer s'il doit laisser le paquet réseau ou non.

2. SÉCURISATION D'UN RÉSEAU

a. Pare-feu

Règles de filtrage :

- Historiquement, elles étaient basées sur les couches basses de la pile protocolaire (réseau, transport), et portaient uniquement sur les paramètres comme les adresses IP et les ports TCP/UDP ;
- Les pare-feu sont également capables de filtrer selon les données de la **couche applicative** (protocole et contenu des données). Ex. : HTTP, SMTP, DNS, etc.
 - Les **proxy et reverse-proxy peuvent être vus comme des pare-feu applicatifs dédiés**. Ils permettent **d'analyser finement** les flux applicatifs (par exemple la navigation web des utilisateurs ou les flux web entrants sur un server de e-commerce).
- Un anti-virus ou un mécanisme de détection d'intrusion peuvent également être implémentés sur le pare-feu de façon à détecter un malware en transit ou certaines attaques.

Avantage sécurité :

- L'exploitant d'un réseau peut donc restreindre le trafic entrant et sortant aux seules connexions qu'il estime légitime. Toutes les autres connexions sont donc bloquées.

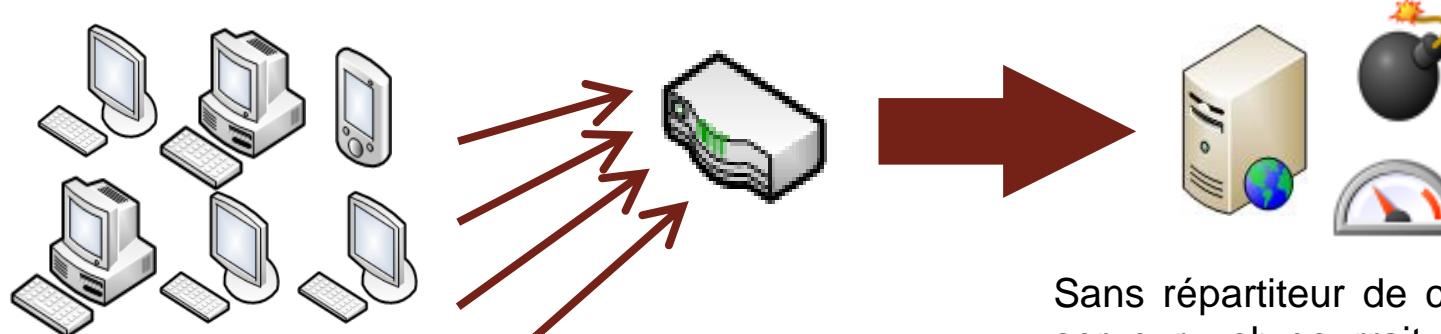
2. SÉCURISATION D'UN RÉSEAU

b. Répartiteur de charge

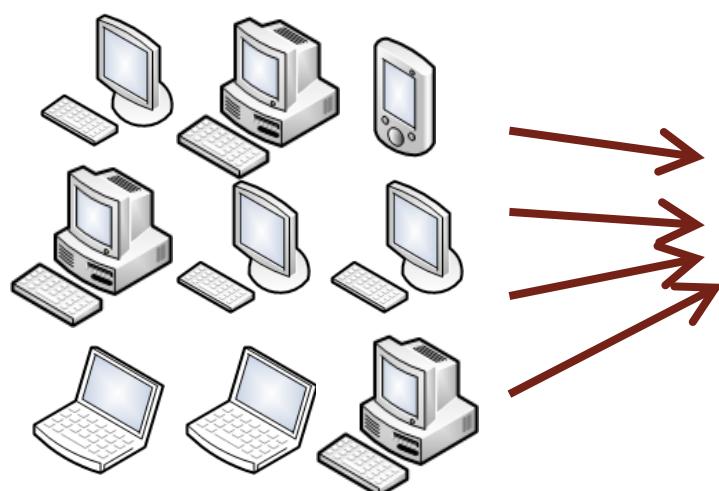
- « Load-balancer » en anglais ;
- Équipement rencontré sur les grosses infrastructures où les serveurs doivent faire face à de très fortes bandes passantes et charges élevées de trafic ;
- Équipement chargé de **répartir/distribuer la charge réseau** en fonction des caractéristiques de celui-ci et de la disponibilité des serveurs ;
- Avantage sécurité : permet de mieux se protéger contre les **dénis de service distribués**.

2. SÉCURISATION D'UN RÉSEAU

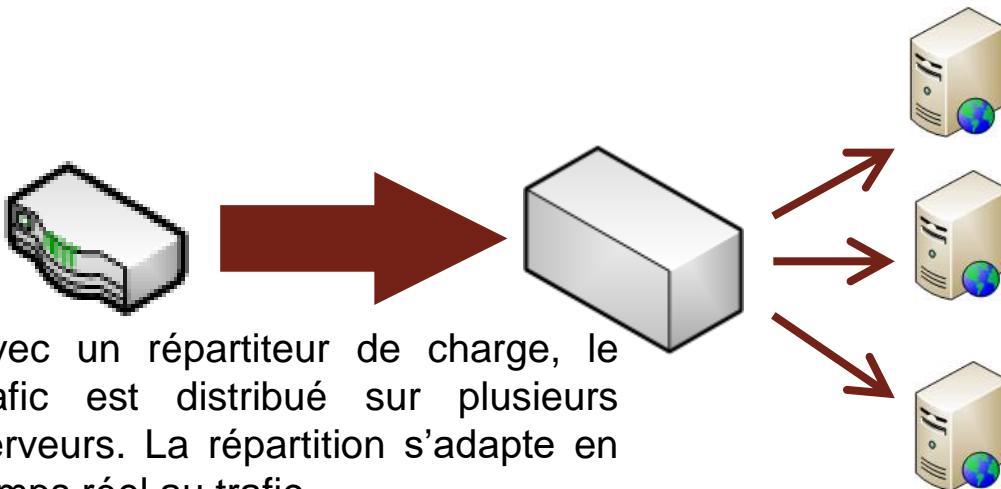
b. Répartiteur de charge



Sans répartiteur de charge, ce seul serveur web pourrait ne plus pouvoir faire face aux nombreuses demandes, et devenir indisponible.



Avec un répartiteur de charge, le trafic est distribué sur plusieurs serveurs. La répartition s'adapte en temps réel au trafic.



2. SÉCURISATION D'UN RÉSEAU

c. Anti-virus

Logiciel chargé de détecter et stopper les **malware connus** :

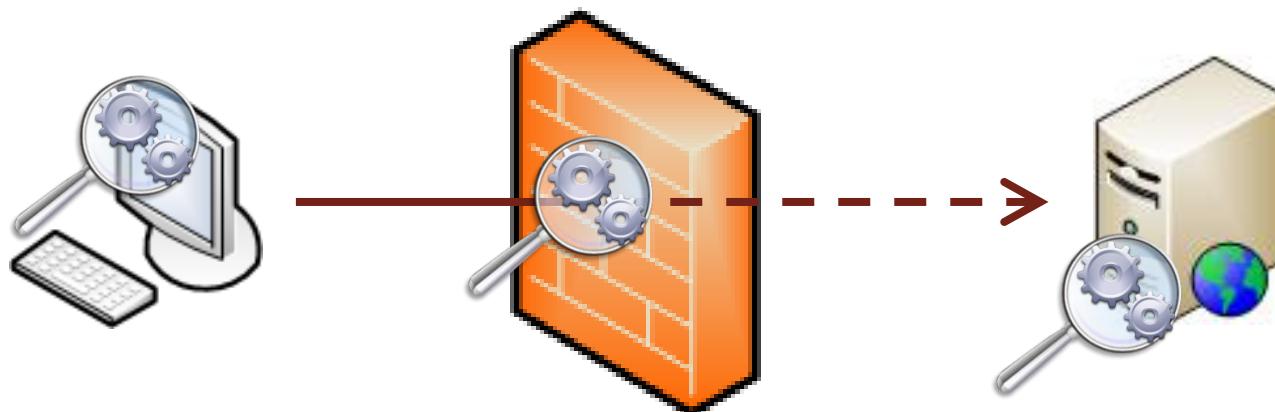
- Virus, vers, *keylogger* (enregistreur de frappe), chevaux de Troie, etc.
- Ces logiciels fonctionnent en général avec une base de données qui contient les signatures des malware connus. Ils analysent en permanence les fichiers et les exécutables du système hébergeant l'anti-virus ;
- **Limite des anti-virus** : ils ne détectent (en général) que les malware déjà répertoriés par les éditeurs. Ainsi, les nouveaux virus ou les malware ciblés ne sont souvent pas détectés. D'autre part, il est impératif que l'anti-virus soit mis à jour quotidiennement.

2. SÉCURISATION D'UN RÉSEAU

c. Anti-virus

Un anti-virus peut être déployé :

- En **local** : sur un système (poste de travail ou serveur) afin de détecter les virus affectant cette machine ;
- En **coupure des flux réseaux** : sur un pare-feu afin d'analyser les flux réseau et détecter les malware avant même qu'ils n'atteignent leur cible. Ce fonctionnement peut être assimilé à un IDS (Intrusion Detection System), mécanisme présenté dans la section suivante.



2. SÉCURISATION D'UN RÉSEAU

d. *IDS et IPS*

IDS **I**ntrusion **D**etection **S**ystem

IPS **I**ntrusion **P**revention **S**ystem

Chargés d'analyser le trafic réseau pour y **déetecter des tentatives d'intrusion** :

- soit en analysant le comportement des flux réseaux ;
- soit en se basant sur une base de signatures identifiant des données malveillantes (principe similaire à celui des anti-virus).

En cas de détection d'une intrusion :

- Les **IDS alertent** les administrateurs, libre à eux d'intervenir ou non ;
- Les **IPS bloquent** les flux réseau concernés.

Les IDS/IPS demandent un configuration fine et maintenue :

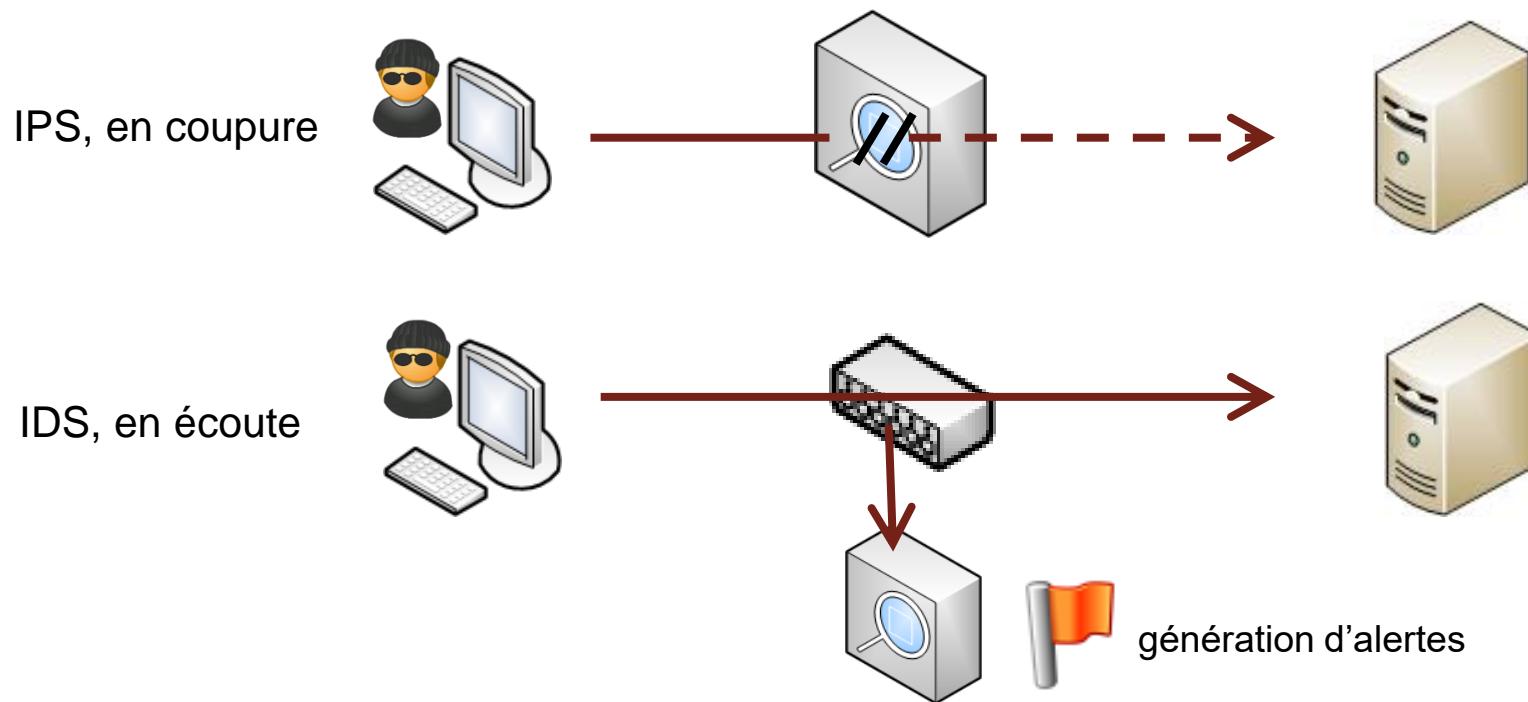
- Ils sont en effet connus pour présenter de nombreux faux-positifs (i.e. ils détectent à tort une tentative d'intrusion) ;
- De plus, les IDS/IPS basés sur des signatures ne peuvent détecter que les intrusions dont les caractéristiques techniques sont déjà connues et référencées.

2. SÉCURISATION D'UN RÉSEAU

d. IDS et IPS

Un IDS peut être soit en coupure du flux réseaux, soit **positionné en écoute**.

Un IPS doit forcément être en **coupure du flux** de façon à pourvoir bloquer le trafic lorsque cela est nécessaire.



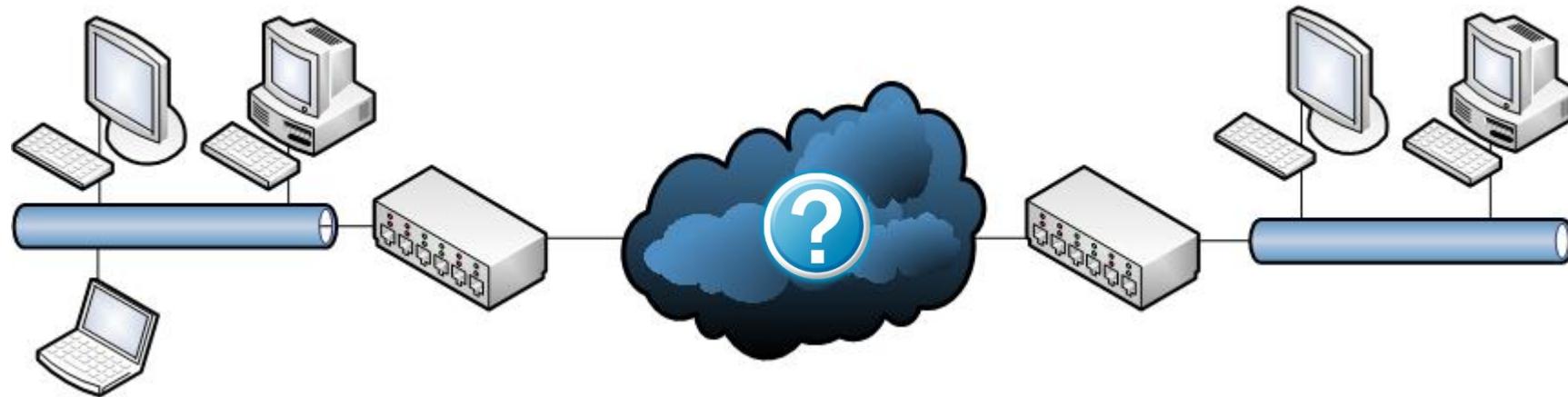
2. SÉCURISATION D'UN RÉSEAU

e. VPN

VPN **V**irtual **P**rivate **N**etwork

Un VPN est un **réseau virtuel** qui permet à **deux réseaux distants de communiquer en toute sécurité**, y compris si la communication s'effectue via des réseaux inconnus et auxquels nous ne faisons pas confiance.

Exemple avec une entreprise qui possède deux sites distants et qui ont besoin de communiquer entre eux via internet : comment faire passer les flux en toute sécurité via Internet que l'on ne maîtrise pas ?



2. SÉCURISATION D'UN RÉSEAU

e. VPN

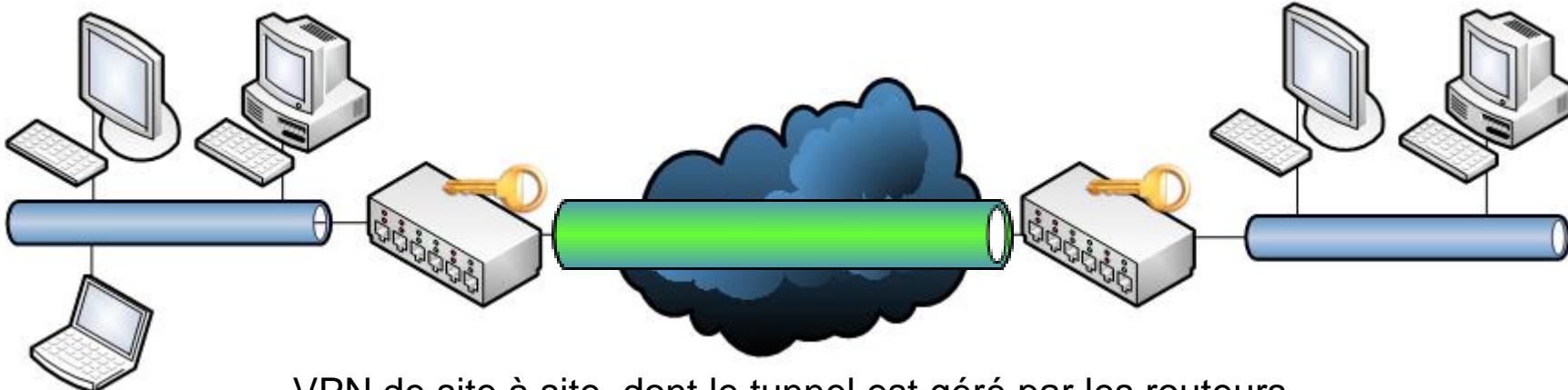
Solution : grâce à des mécanismes cryptographiques, appliquer un **chiffrement des données, ainsi qu'un motif d'intégrité, à tous les flux entre les 2 sites**. On obtient ainsi un **tunnel virtuel** qui ne contient que des données chiffrées et protégées en intégrité :

- Les données qui passent sur Internet sont donc chiffrées et non compréhensibles par un attaquant qui écouterait les flux ;
- En cas de modification malveillante des flux, le mécanisme d'intégrité permettra au destinataire de déterminer que les données reçues ne sont pas intègres, et qu'il ne faut donc pas traiter ces données.

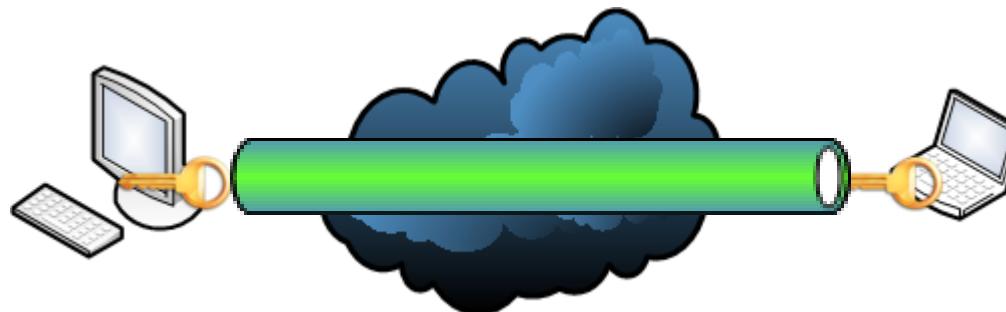
Il existe différents types de VPN, représentés sur les diapositives suivantes.

2. SÉCURISATION D'UN RÉSEAU

e. VPN



VPN de site à site, dont le tunnel est géré par les routeurs
IPsec – au niveau de la couche Internet

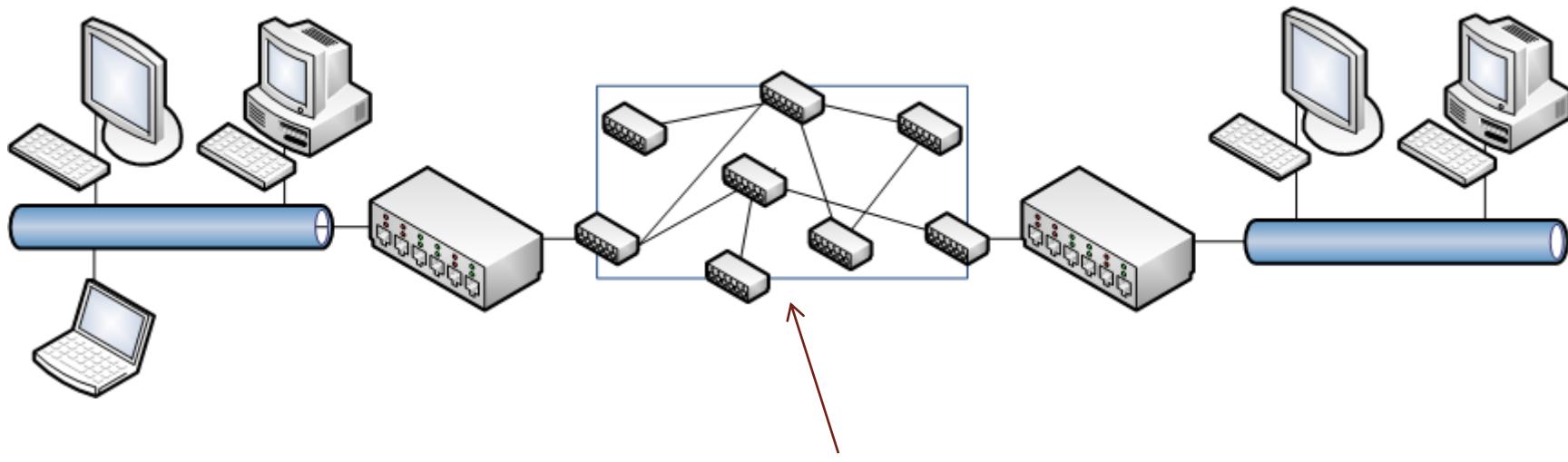


VPN entre systèmes
TLS – au niveau de la couche Transport

2. SÉCURISATION D'UN RÉSEAU

e. VPN

Il existe également des VPN qui n'ont pas recours à de la cryptographie, mais qui font appel aux infrastructures d'opérateurs. Dans ce cas, la protection du réseau est assurée par l'opérateur.



Réseau opérateur **MPLS**, dont le cœur est inaccessible aux clients se connectant sur ce réseau

2. SÉCURISATION D'UN RÉSEAU

f. Segmentation

Un principe majeur de la Sécurité est celui du **moindre privilège** :

On ne doit donner les droits d'accès à une ressource qu'aux seules personnes/entités ayant un besoin légitime d'y accéder.

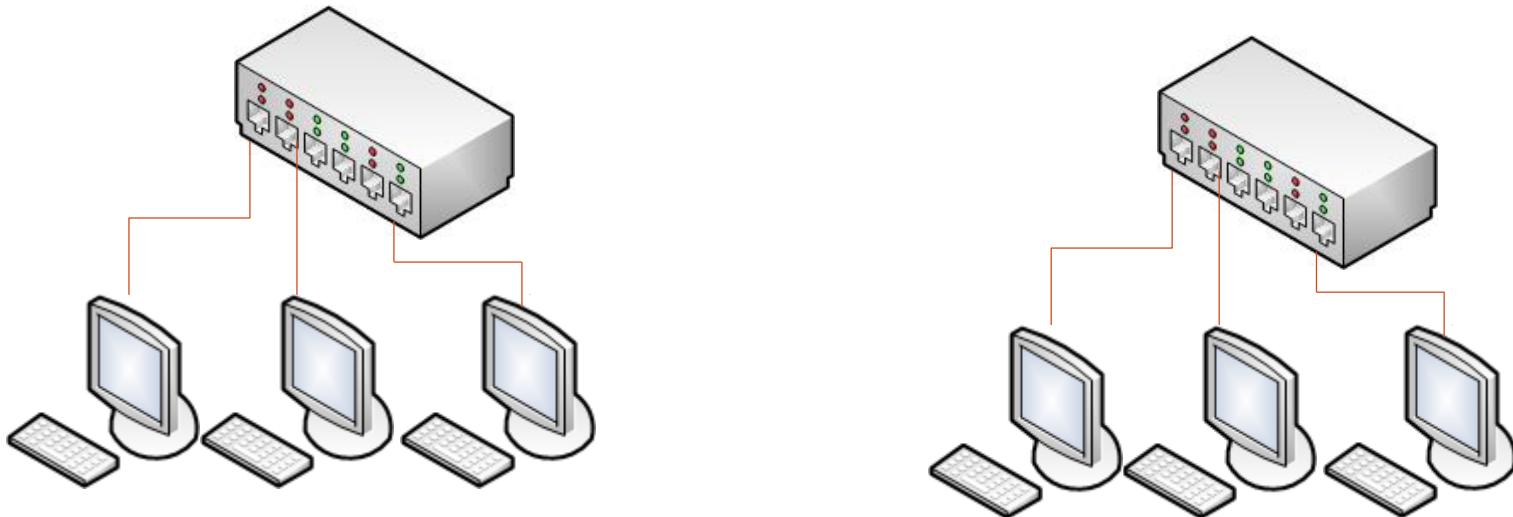
Appliqué au domaine réseau, il est donc fait **recours à de la segmentation** afin de séparer le réseau en différentes zones.

Les droits d'accès à ces zones doivent ensuite être **filtrés** afin de n'autoriser que les flux nécessaires entre chaque zone.

2. SÉCURISATION D'UN RÉSEAU

f. Segmentation

Il existe plusieurs techniques pour procéder à de la segmentation. La technique la plus évidente : implémenter deux réseaux distincts non connectés.



Implémentation de deux réseaux physiques différents, non connectés.

Avantage : **étanchéité réseau parfaite** (aucune communication possible entre ces deux zones).
Inconvénient : adapté à certains réseaux très sensibles seulement, **peu adapté aux réseaux d'entreprise** qui ont besoin de communiquer.

2. SÉCURISATION D'UN RÉSEAU

f. Segmentation

Autre technique de segmentation : **VLAN** (Virtual LAN).

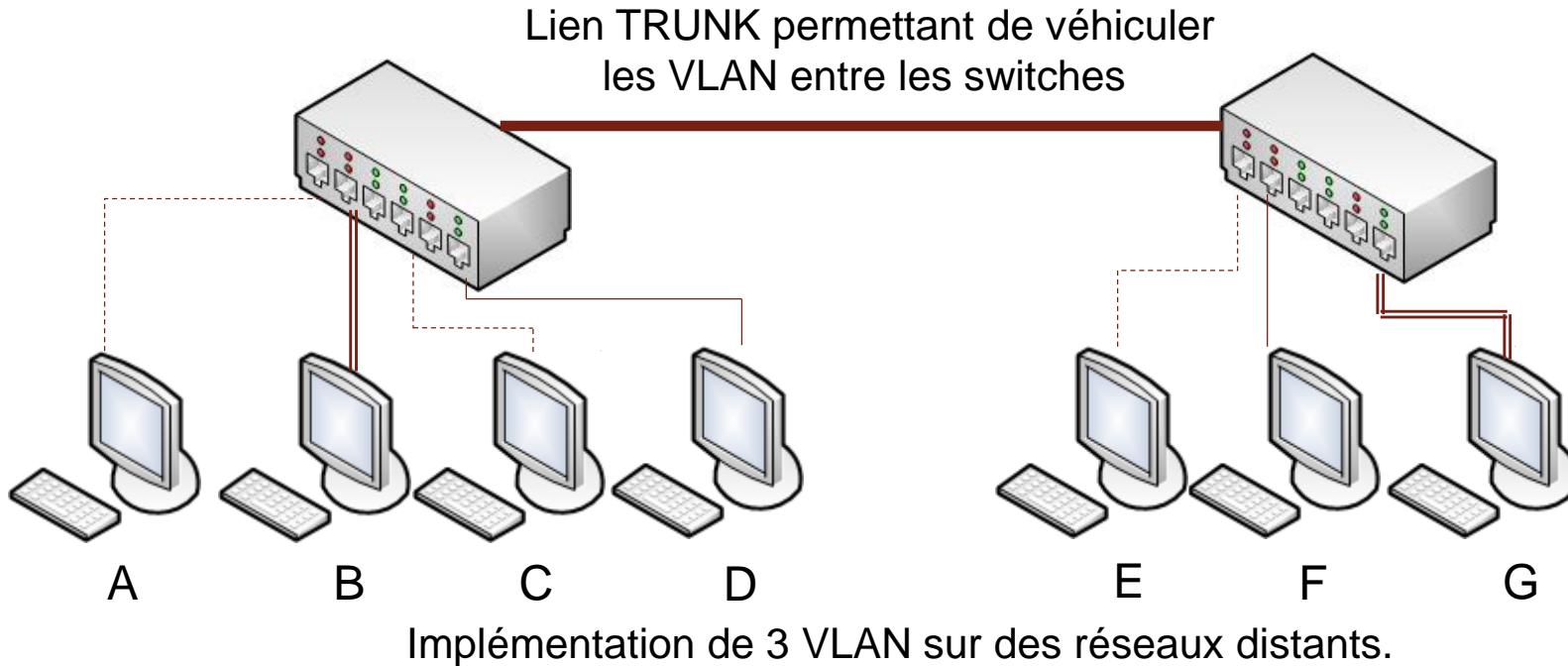
Les VLAN sont des **réseaux virtuels implémentés par les switches**. Ceux-ci **restreignent la communication entre systèmes selon des règles configurées** sur l'équipement réseau :

- La segmentation peut se faire grâce aux ports Ethernet de chaque switch (on affecte un VLAN particulier à chaque port des switches, les deux switches étant reliés entre eux par un lien TRUNK afin de véhiculer les étiquettes des VLAN) ;
- La segmentation aussi se faire grâce aux adresses MAC des systèmes.
 - Attention : les adresses MAC des cartes réseaux pouvant facilement être modifiées par les utilisateurs, le filtrage sur les adresses MAC est à considérer – logiquement – avec précaution car le niveau de sécurité effectif est limité.

Voir exemple sur la diapositive suivante.

2. SÉCURISATION D'UN RÉSEAU

f. Segmentation



VLAN 1. Les machines B et G sont segmentées des autres systèmes et peuvent communiquer entre-elles deux seulement.

VLAN 2. Les machines A, C et E sont segmentées des autres systèmes et peuvent communiquer entre-elles seulement.

VLAN 3. Les machines D et F sont segmentées des autres systèmes et peuvent communiquer entre-elles deux seulement.

2. SÉCURISATION D'UN RÉSEAU

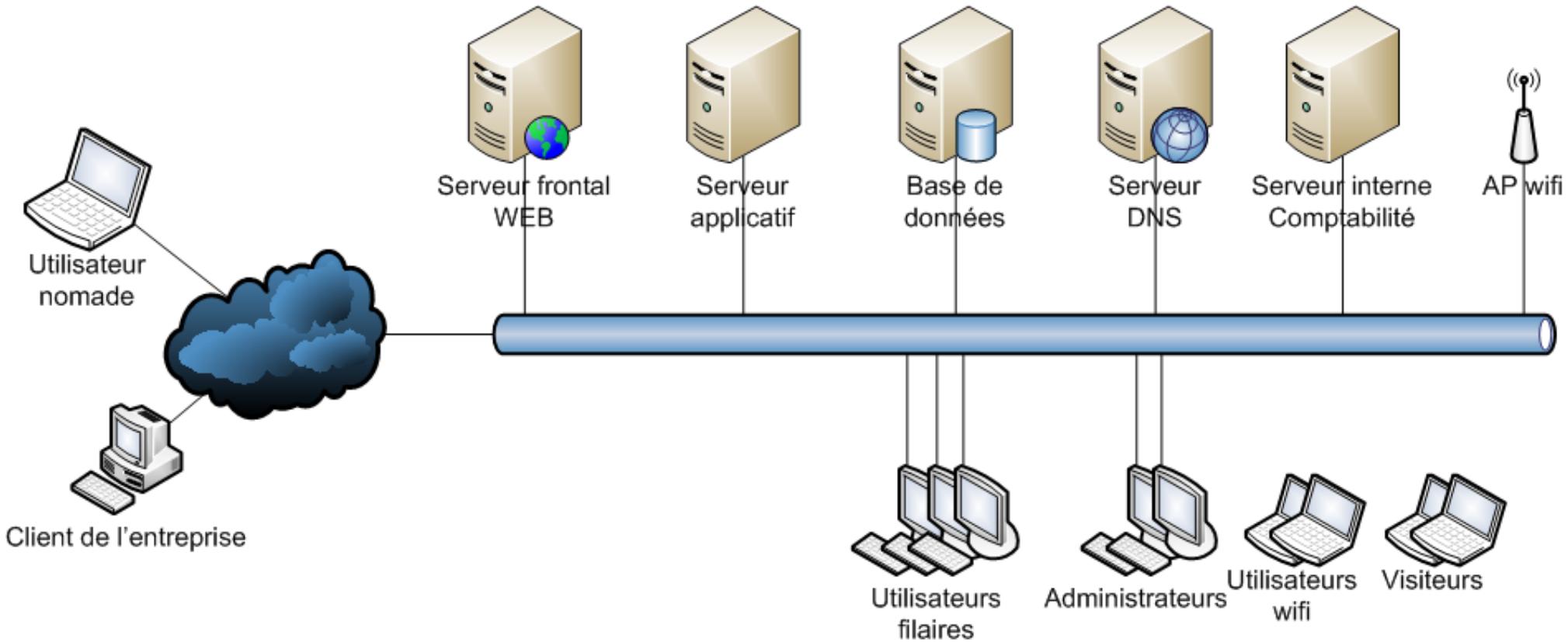
g. Exemple pratique de sécurisation avec un réseau simple

Prenons l'exemple d'un réseau d'entreprise « à plat ». Caractéristiques de cette entreprise :

- Elle fournit un **site WEB de e-commerce** ;
- Certains employés se connectent sur le **réseau local filaire**, d'autres se connectent en **wifi** ;
- Certains employés sont **nomades** et doivent donc se **connecter à distance** ;
- Il existe deux catégories principales d'utilisateurs : les **utilisateurs « standard »** et les **administrateurs** du S.I. ;
- Afin de fonctionner, l'entreprise possède également des **serveurs internes** (comptabilité, wiki, etc.) ;
- L'entreprise souhaite permettre à ses **visiteurs** de se connecter en **wifi** afin de naviguer sur internet.

2. SÉCURISATION D'UN RÉSEAU

g. Exemple pratique de sécurisation avec un réseau simple



Réseau « à plat », avant sécurisation

2. SÉCURISATION D'UN RÉSEAU

g. Exemple pratique de sécurisation avec un réseau simple

Voyons comment nous allons pouvoir sécuriser ce réseau.

- Note : il existe plusieurs façons d'améliorer la sécurité de ce réseau, nous en présentons ici uniquement les grandes lignes. Cet exercice n'est ni exhaustif ni la seule solution possible.

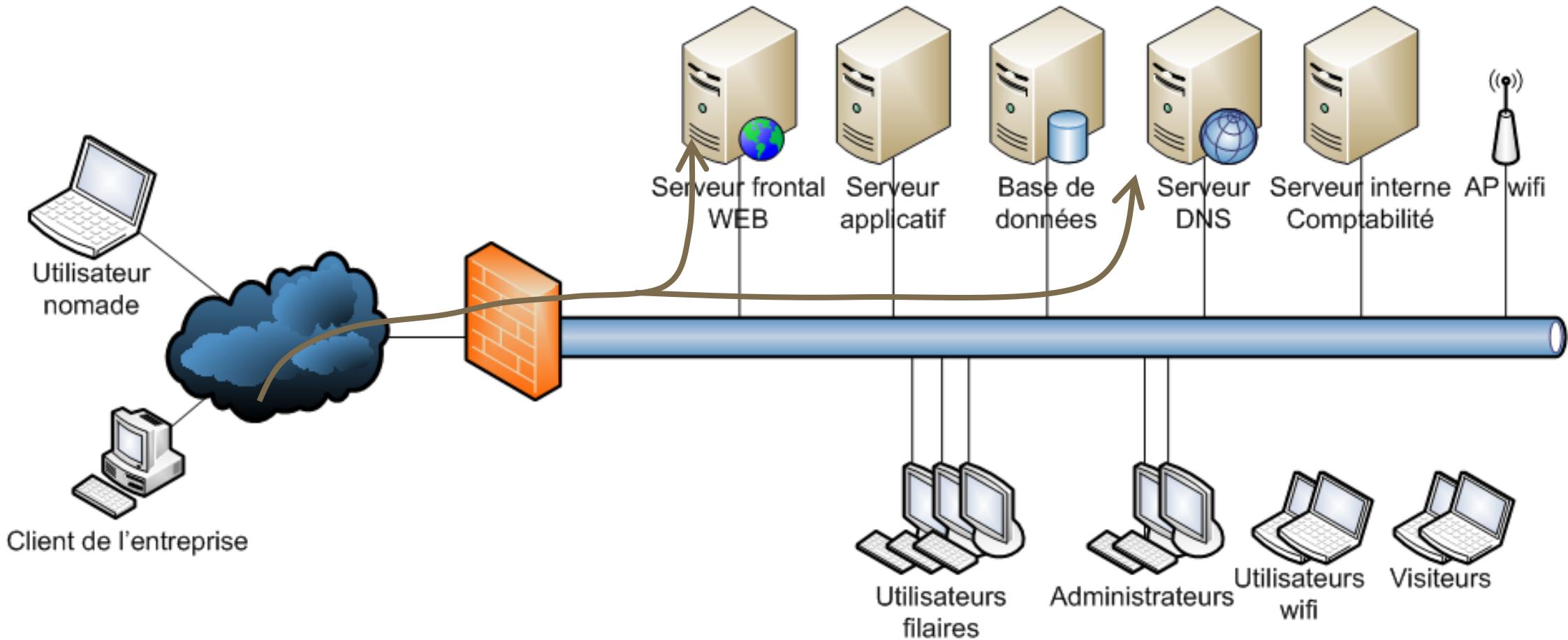
Parmi les nombreuses faiblesses architecturales de ce réseau, nous pouvons identifier au moins le problème suivant :

- Le réseau est **directement connecté à Internet**, i.e. tous les systèmes et utilisateurs et systèmes peuvent communiquer avec l'extérieur (attention aux **fuites de données !**) et **tout Internet peut se connecter sur notre réseau interne.**

Corrigeons cela en implémentant un **pare-feu** en frontal qui va autoriser uniquement les flux entrants vers le serveur WEB (TCP/80 et TCP/443) et le serveur DNS (UDP/53 et TCP/53). Ainsi, Internet ne pourra plus accéder au reste du réseau interne.

2. SÉCURISATION D'UN RÉSEAU

g. Exemple pratique de sécurisation avec un réseau simple



Réseau « à plat », avec un pare-feu en frontal

2. SÉCURISATION D'UN RÉSEAU

g. Exemple pratique de sécurisation avec un réseau simple

Le pare-feu empêche – certes – la connexion directe entre internet et le réseau interne, mais :

- Au cas où le serveur WEB présente une **vulnérabilité**, un hacker présent sur Internet peut potentiellement **prendre la main sur ce serveur**, puis **rebondir ensuite sur le réseau interne**.

Nous allons donc **segmenter** notre réseau en **différentes zones de criticité**, notamment :

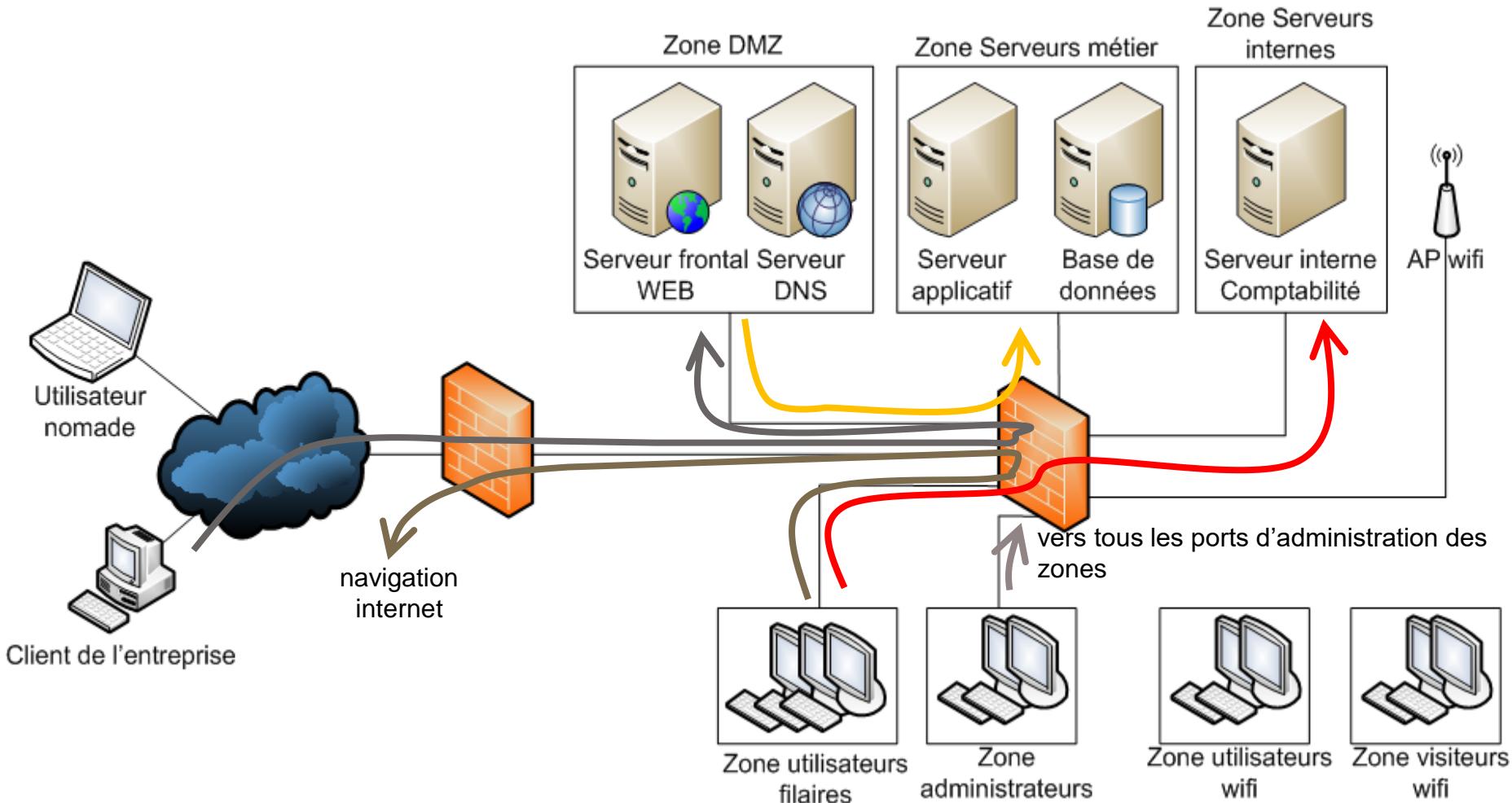
- Une **DMZ (zone démilitarisée)** destinée à héberger tous les serveurs qui doivent être accessibles depuis internet, et uniquement ceux-ci. Ainsi, en cas de faille dans le serveur web, un attaquant aurait plus de difficultés pour rebondir sur le réseau interne ;
- Une zone destinée aux **serveurs internes** de l'entreprise ;
- Une zone pour les **postes de travail filaires des utilisateurs** ;
- Une zone pour les **postes de travail wifi des utilisateurs** ;
- Une zone pour les **postes wifi des visiteurs** ;
- Une zone pour les **postes de travail des administrateurs**, car ceux-ci ont besoin d'accéder à des interfaces d'administration (RDP, SSH...).

Afin que cette segmentation réseau soit efficace, nous faisons **passer tous les flux** (y compris internes) **par un deuxième pare-feu (interne)** afin que seuls les flux que nous allons configurer soient autorisés.

- Note : on observe malheureusement souvent des réseaux segmentés mais non filtrés. Cela ne sert à rien en terme de sécurité, car toutes les zones peuvent communiquer entre-elles.

2. SÉCURISATION D'UN RÉSEAU

g. Exemple pratique de sécurisation avec un réseau simple

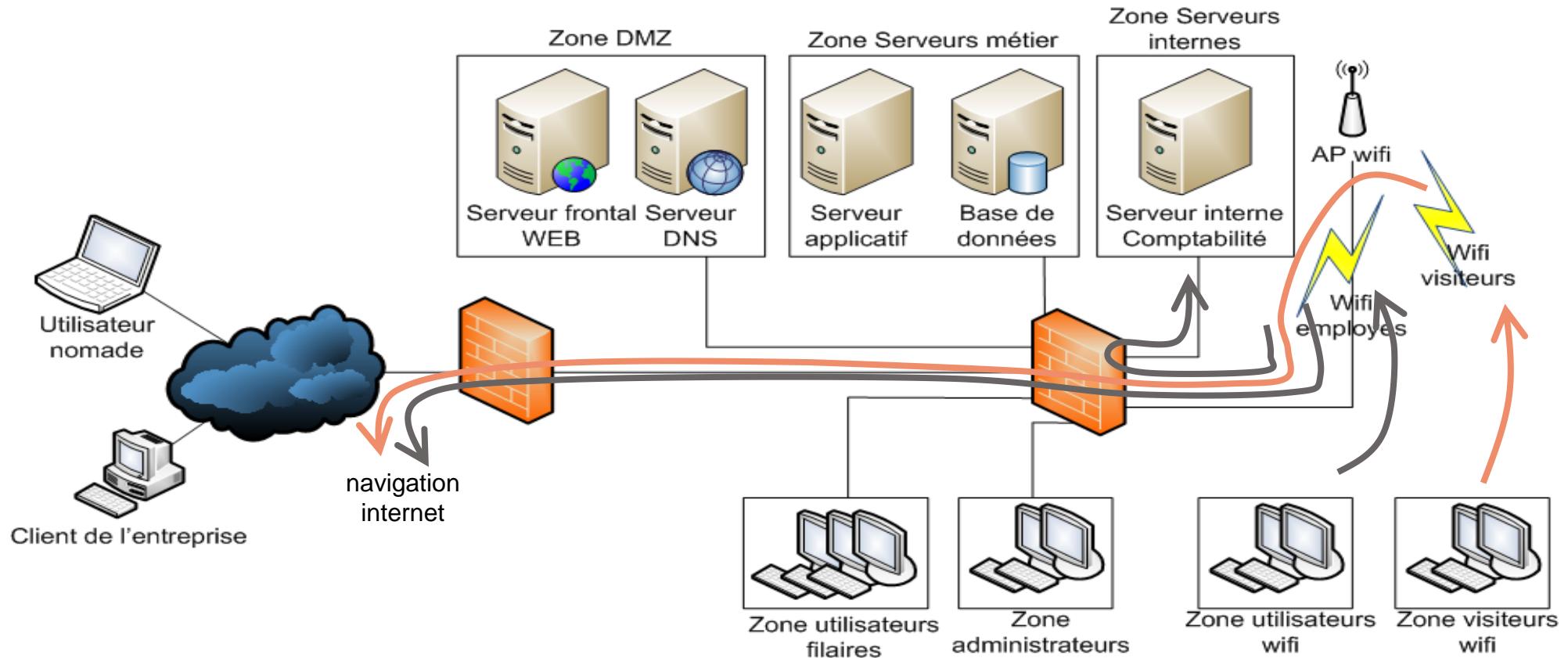


Réseau avec des zones segmentées, et un filtrage systématique via le pare-feu, y compris pour les flux internes.

2. SÉCURISATION D'UN RÉSEAU

g. Exemple pratique de sécurisation avec un réseau simple

Le point d'accès wifi doit être accessible aux visiteurs et aux employés internes. Puisque le besoin d'accès aux ressources est différent pour ces 2 populations, nous allons donc implémenter deux SSID (**deux réseaux wifi distincts**, portés par le même point d'accès, et dont le pare-feu filtrera les flux).



Deux réseaux wifi, dont les flux sont filtrés différemment.

2. SÉCURISATION D'UN RÉSEAU

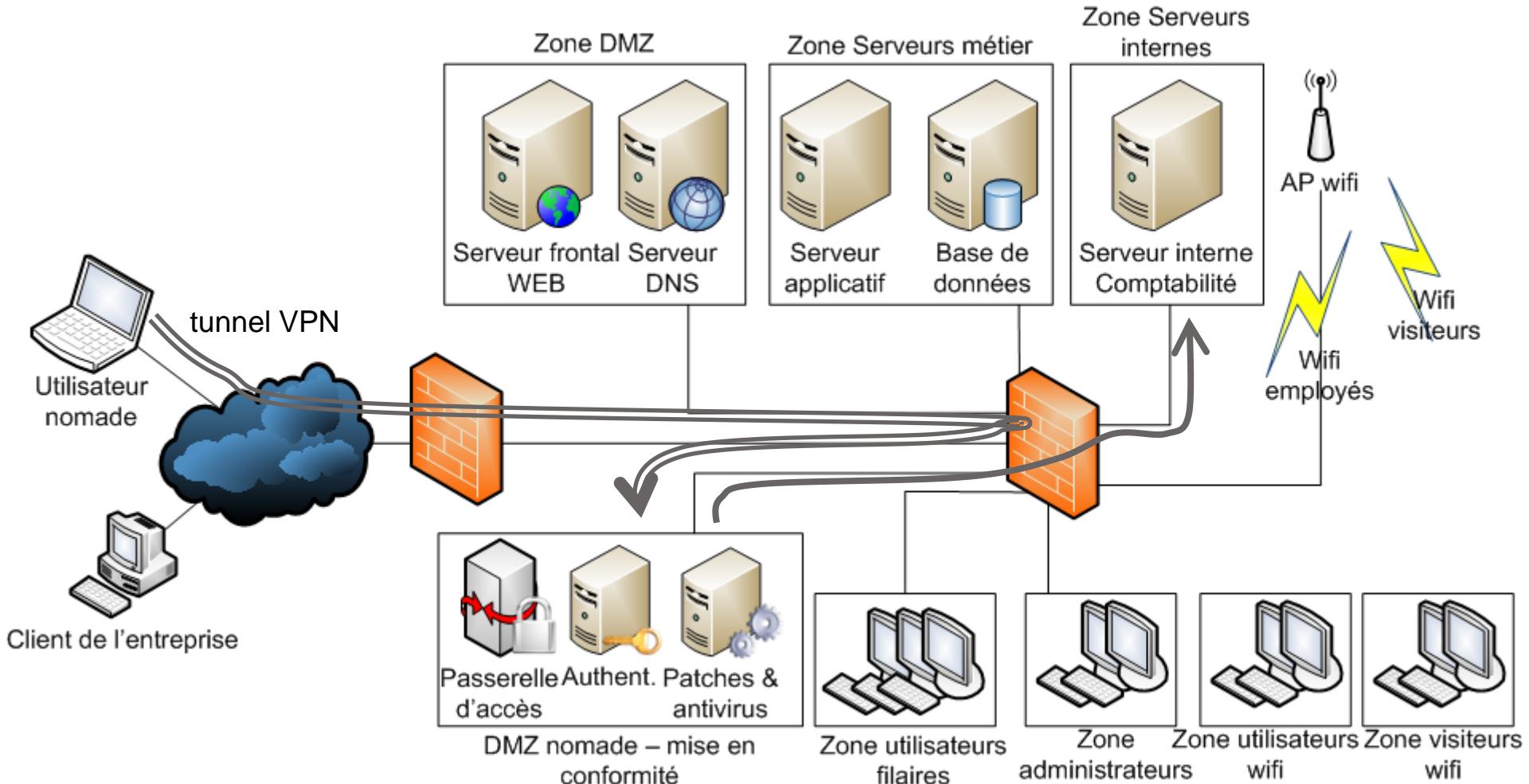
g. Exemple pratique de sécurisation avec un réseau simple

Nous devons également permettre aux **utilisateurs nomades de se connecter** au réseau interne depuis internet. Cela se fait via une DMZ spécifique, appelée zone de mise en conformité, dont le rôle est le suivant :

- Fournir l'interface d'accès au réseau interne depuis internet, en général via un **tunnel VPN** ;
- **Vérifier que le poste nomade et son utilisateur sont habilités** pour se connecter à distance ;
- **Vérifier le niveau de sécurité du poste** avant d'autoriser la connexion (**patches et anti-virus à jour** notamment) ;
- Si tout est OK, alors **autoriser les flux vers les zones internes** (et seulement celles qui sont nécessaires pour le métier), toujours en passant par le **pare-feu**.

2. SÉCURISATION D'UN RÉSEAU

g. Exemple pratique de sécurisation avec un réseau simple



Réseau avec DMZ de mise en conformité pour les postes nomades.

2. SÉCURISATION D'UN RÉSEAU

g. Exemple pratique de sécurisation avec un réseau simple

Enfin, il serait souhaitable de **mieux filtrer le trafic WEB** entrant et sortant :

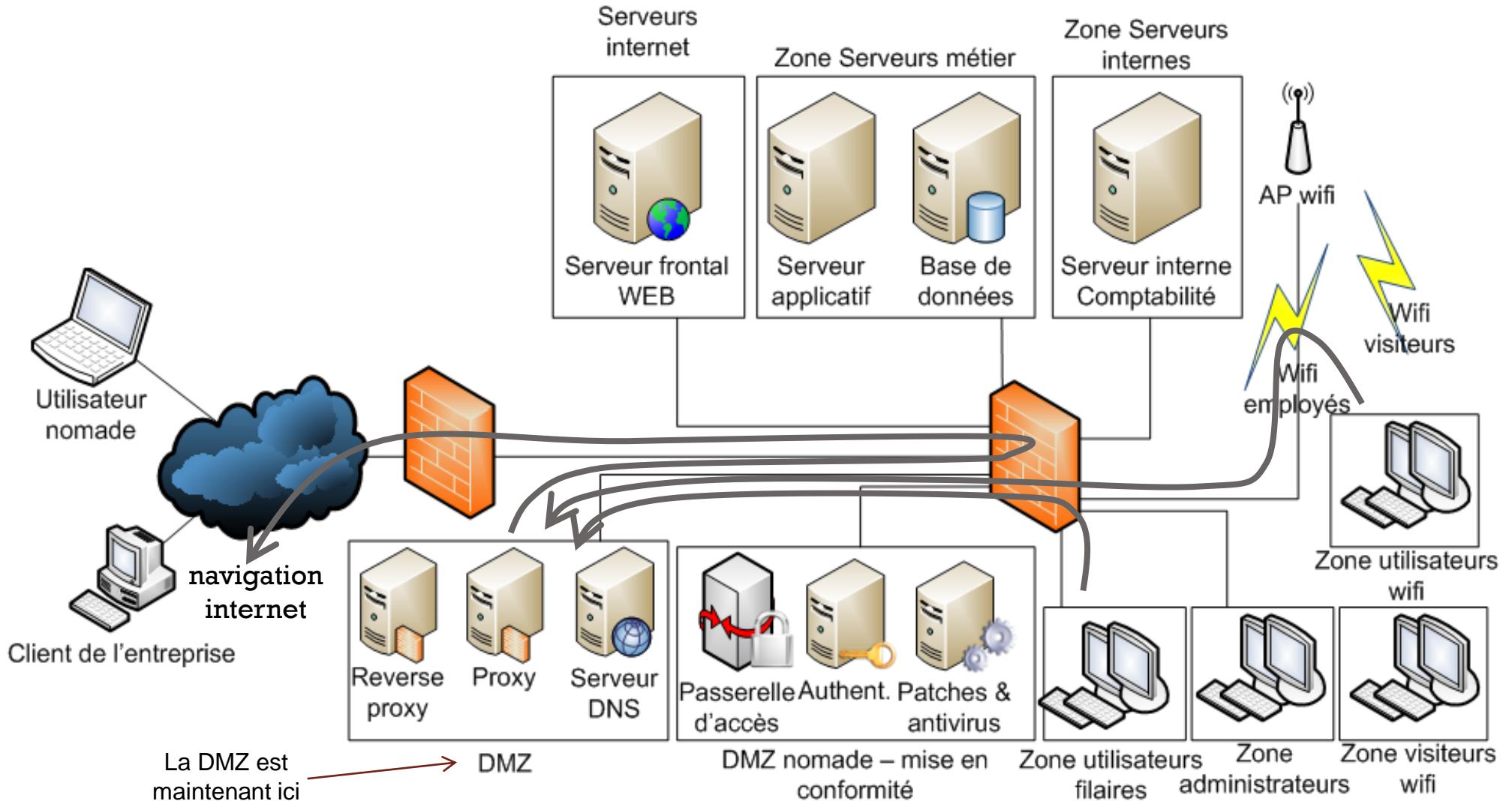
- **Trafic sortant** : définir les catégories de sites WEB que les employés sont autorisés à naviguer, implémenter une liste blanche ou noire de sites autorisés/interdits ;
- **Trafic entrant** : analyser les requêtes WEB d'internet vers le serveur de e-commerce afin d'intercepter les requêtes malveillantes (injection, malware, etc.).

Nous allons donc recourir à un **proxy pour analyser les flux sortants**, et **un reverse-proxy pour analyser les flux entrants**. Ces équipements étant en coupure, ils empêchent donc les postes de travail des utilisateurs d'être connectés directement à Internet tout en leur permettant de naviguer sur les sites autorisés. Même remarque pour le serveur WEB : celui-ci n'est plus connecté directement sur Internet, c'est le reverse-proxy qui est maintenant en frontal.

Puisque les proxies et reverse-proxies sont en frontal Internet, ce sont donc eux qu'il faut **placer dans la DMZ** maintenant.

2. SÉCURISATION D'UN RÉSEAU

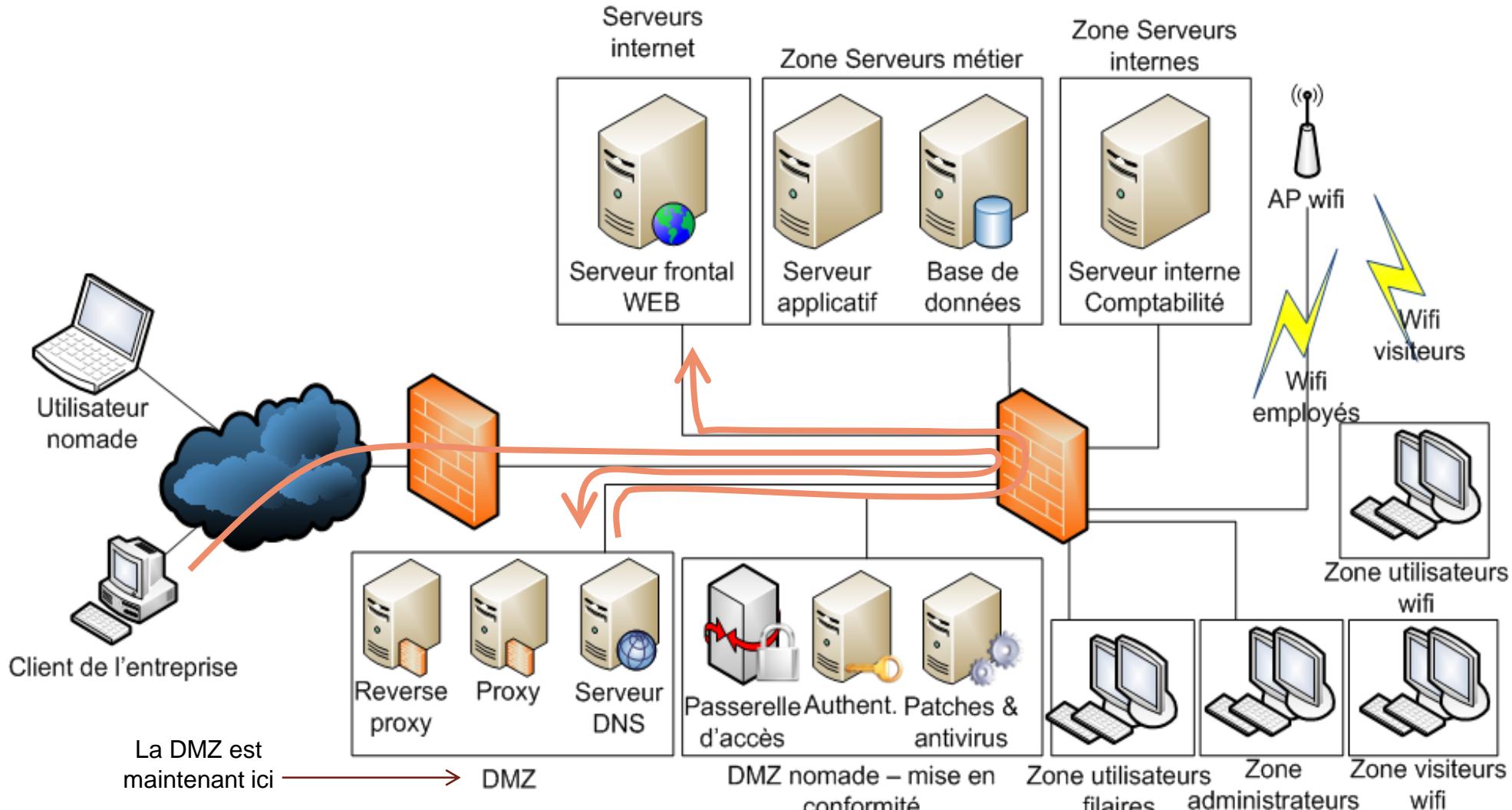
g. Exemple pratique de sécurisation avec un réseau simple



Réseau avec un proxy et un reverse-proxy en coupure des flux de/vers Internet

2. SÉCURISATION D'UN RÉSEAU

g. Exemple pratique de sécurisation avec un réseau simple



Réseau avec un proxy et un reverse-proxy en coupure des flux de/vers Internet.

3. LES BASES DE LA CRYPTOGRAPHIE

- a) Vocabulaire
- b) Un peu d'histoire
- c) Chiffrement symétrique
- d) Chiffrement asymétrique
- e) Chiffrement symétrique vs Chiffrement asymétrique
- f) Signature électronique
- g) Certificats électroniques
- h) Jetons cryptographiques

3. LES BASES DE LA CRYPTOGRAPHIE

a. Vocabulaire

La cryptographie est une discipline consistant à manipuler des données de telle façon que les services suivants puissent être fournis :

Intégrité

Objectif : s'assurer que les données n'ont pas été modifiées sans autorisation.

Remarque : dans les faits, la cryptographie ne s'attache pas vraiment à empêcher une modification de données, mais plutôt à fournir un moyen sûr de détecter une modification malveillante.

Confidentialité

Objectif : ne permettre l'accès aux données qu'aux seules personnes autorisées.

Preuve (authentification et non-répudiation)

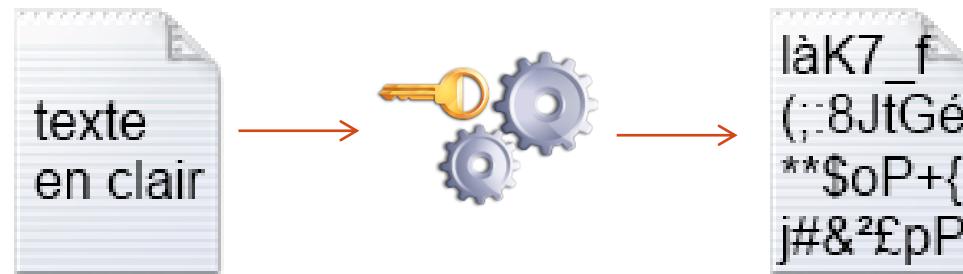
Objectif : fournir un moyen de preuve garantissant la véritable identité des entités ainsi que l'imputation de leurs actions.

3. LES BASES DE LA CRYPTOGRAPHIE

a. Vocabulaire

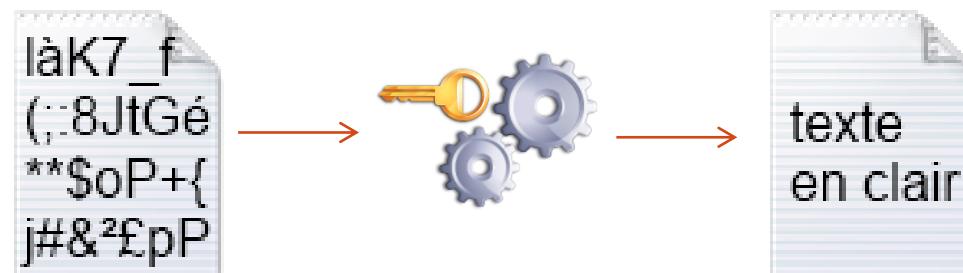
Chiffrer

Transformer une donnée de telle façon qu'elle devienne incompréhensible. Seules les entités autorisées pourront comprendre cette donnée chiffrée.



D chiffrer

Transformer une donn e pr c d m ment chiffr e pour reconstituer la donn e d'origine. Seules les entit s autoris es ont la capacit  de proc der   cette action.



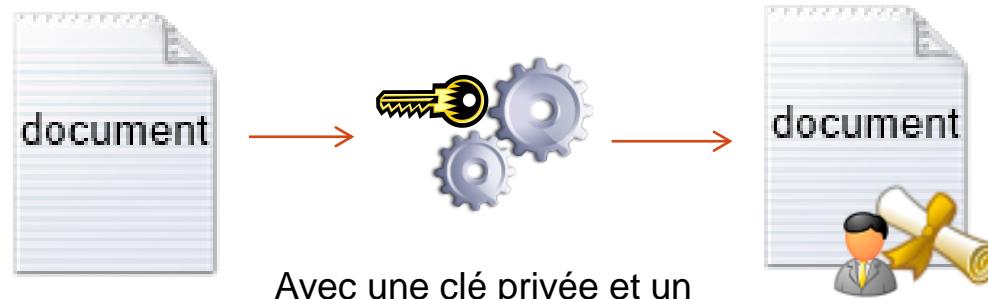
Recours   un algorithme
et   une cl 
cryptographique.

3. LES BASES DE LA CRYPTOGRAPHIE

a. Vocabulaire

Signer

Créer une signature électronique unique à la donnée et à son auteur. La signature lie donc la donnée d'origine et son auteur.



Avec une clé privée et un message en entrée, on obtient une signature en sortie

Vérifier la signature

S'assurer que la donnée d'origine n'a pas été modifiée et que son auteur est authentifié. Si la signature n'est pas valide, alors il ne faut pas faire confiance au document.



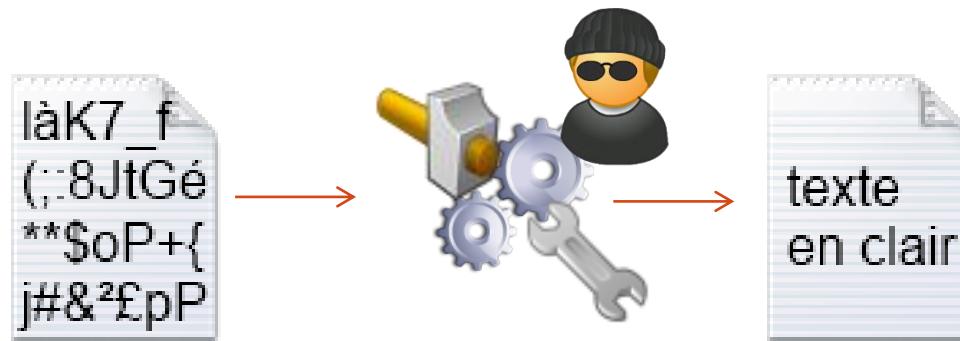
Avec la clé publique, la signature et le message en entrée, on obtient un verdict OK/NOK en sortie

3. LES BASES DE LA CRYPTOGRAPHIE

a. Vocabulaire

Décrypter

Reconstituer la donnée d'origine en tentant de « casser » la donnée chiffrée ou l'algorithme cryptographique.



Crypter

La notion de crypter n'existe pas. Il s'agit d'un abus de langage.

3. LES BASES DE LA CRYPTOGRAPHIE

b. Un peu d'histoire : « Les codes »

• Le code de Mary Stuart

- Mary Stuart est arrêtée en 1586, pour le meurtre de son mari. En fait, c'était surtout un prétexte car beaucoup de sujets considéraient que c'était elle la souveraine légitime de l'Angleterre et non Elizabeth.
- Toutes les lettres que Mary écrivait et recevait depuis sa semi-captivité étaient interceptées, ouvertes, recopiées avant d'être acheminées à leur destinataire par Sir Francis Walsingham, Premier secrétaire de la reine Elizabeth
- Il confie le décryptement à Thomas Phelipps.
- Le 17 juillet 1586, Mary Stuart écrit une lettre qui signera son arrêt de mort et où elle s'exprime ouvertement à propos de l'assassinat de la reine Elizabeth
- Walsingham en voulait plus. Il eut l'idée, pour démanteler complètement le réseau, d'introduire de faux post-scriptum dans les lettres adressées à Mary pour qu'elle écrive les noms des conspirateurs. Trop confiante en son code, elle le fit.
- Le 15 octobre 1586, Marie Stuart est jugée pour trahison, accusée d'avoir pris part à un complot tendant à assassiner la reine Elizabeth, afin de s'emparer elle-même de la couronne d'Angleterre.

3. LES BASES DE LA CRYPTOGRAPHIE

- Le chiffre utilisé était constitué de 23 symboles qui remplaçaient les lettres de l'alphabet (sauf j, v et w), ainsi que de 36 symboles représentant des mots ou des phrases. Il y avait en outre quatre nulles et un symbole qui signifiait que la lettre suivante était une lettre doublée.

a b c d e f g h i k l m n o p q r s t u x y z
o †

Nulles ff.—.—.d. Dowbleth σ

and for with that if but where as of the from by
z ɔ 4 4 4 3 ɔ 2 3 3 x ɔ

so not when there this in wich is what say me my wyrt
ɔ x + ɔ 6 x ɔ ɔ m n m m o

send lře receave bearer I pray you Mte your name myne
ř o ř ř T L H — R ř ss

3. LES BASES DE LA CRYPTOGRAPHIE

- À la cour d'Espagne au 17e siècle, les jeunes filles étaient très surveillées. Elles créèrent un code avec les mouvements de leur éventail.



3. LES BASES DE LA CRYPTOGRAPHIE

- Le code Morse (du nom de Samuel Morse, son inventeur)
 - Code télégraphique utilisant un alphabet conventionnel fait de traits et de points, et, quant au son, de longues et de brèves



A	--	N	--	0	-----
B	----	O	---	1	-----
C	---	P	---	2	-----
D	-..	Q	-..-	3	-----
E	.	R	-..	4	-----
F	-.-.	S	...	5	-----
G	---	T	-	6	-----
H	U	...	7	-----
I	..	V	...	8	-----
J	-.-.	W	---	9	-----
K	---	X	---	.	-----
L	-.-.	Y	---	,	-----
M	--	Z	---	?	-----

3. LES BASES DE LA CRYPTOGRAPHIE

- Le code Navajo

- Connaissant l'extrême difficulté de la langue navajo, Philip Johnston, un ingénieur installé à Los Angeles, eut l'idée que cette pourrait être utilisée comme un code pratiquement incompréhensible.
- Si chaque bataillon du Pacifique était doté d'une paire d'indigènes comme opérateurs radio, la sécurité des communications serait garantie.
- Le codage en langue navajo avait pourtant un défaut majeur: cette langue n'offre pas d'équivalent au langage militaire moderne. Afin d'éviter les ambiguïtés, les marines décidèrent d'établir un lexique de mots navajos pour remplacer les termes anglais autrement impossibles à traduire.
- L'impénétrabilité du code navajo est due à l'appartenance du navajo à la famille des langues Na-Dene, qui n'a aucun lien avec une quelconque langue européenne ou asiatique. Un verbe, par exemple, n'est pas conjugué seulement en accord avec son sujet, mais aussi avec son complément d'objet.
- 420 Navajos étaient employés au code.
- c'est l'un des rares codes de l'histoire à n'avoir jamais été brisé

3. LES BASES DE LA CRYPTOGRAPHIE

La stéganographie

- La stéganographie (« écriture couverte »)
 - Contrairement à la cryptographie, qui chiffre des messages de manière à les rendre incompréhensibles, la stéganographie (en grec «l'écriture couverte») cache les messages dans un support

La stéganoraphie

JEUDI 4 MARS 2004 - PREMIÈRE ÉDITION N° 7095 - WWW.LIBERATION.FR

L'Es Selon Gianni Vattimo, philosophe, la nouvelle chrétienneté sera laïque cahier central

Libération

Chantage sur les rails

Depuis deux mois, un mystérieux «groupe AZ» menace la SNCF d'attentats et réclame de l'argent à l'Etat. Une bombe a été désamorcée sur la ligne Paris-Toulouse. **Page 2**

Mon gros loup, ne prenons pas de risques inutiles, le plus tôt sera le mieux. Donne moi tes instructions
Suzy

Comment «Libé» a servi de boîte aux lettres

La police a utilisé les petites annonces pour contacter les maîtres chanteurs. **Page 3**

Loi Perben 2: deux articles retoqués
Le Conseil constitutionnel a conservé deux dispositions, sans toucher au fond de la loi sur le crime organisé. **Page 1**

MONDÉ
La femme de Dutroux accusée
Etats-Unis: Super Tuesday pour Kerry

SOCIÉTÉ
Cesare Battisti libéré

ÉCONOMIE
VU: le cours de l'action manipulé sous Messier

TELEVISION
Deneuve sur divan

Rebonds
Contre l'intelligence exclusive

Par XAVIER DARCOS

Autour des élections municipales de mars prochain, le 1er mai marquera le retour à l'ordre dans les rues de Paris. Mais ce n'est pas tout. Il s'agit également d'un rendez-vous avec l'avenir. L'avenir de l'Europe, en particulier l'avenir de l'Union européenne, qui devrait être consacré à l'élaboration d'un nouveau traité. Cela nécessitera de nombreuses discussions et négociations entre les différents pays membres de l'UE. Mais il est également important que les citoyens soient informés et participent à ces discussions. C'est pourquoi nous avons décidé de publier cette interview de Xavier Darcos, ancien ministre de l'Intérieur et actuel député de Paris, qui nous parle de son projet de réforme de l'administration publique.

La stéganographie

Cher ami, Je suis toute émue de vous dire que j'ai bien compris l'autre jour que vous aviez toujours une envie folle de me faire danser. Je garde le souvenir de votre baiser et je voudrais bien que ce soit une preuve que je puisse être aimée par vous. Je suis prête à montrer mon affection toute désintéressée et sans calcul, et si vous voulez me voir ainsi vous dévoiler, sans artifice, mon âme toute nue, daignez me faire visite, nous causerons et en amis franchement je vous prouverai que je suis la femme sincère, capable de vous offrir l'affection la plus profonde, comme la plus étroite amitié, en un mot : la meilleure épouse dont vous puissiez rêver. Puisque votre âme est libre, pensez que l'abandon où je vis est bien long, bien dur et souvent bien insupportable. Mon chagrin est trop gros. Accourez bien vite et venez me le faire oublier. A vous je veux me soumettre entièrement.

- Alfred de Musset a répondu ceci :



Quand je mets à vos pieds un éternel hommage,
Voulez-vous qu'un instant je change de visage ?
Vous avez capturé les sentiments d'un cœur
Que pour adorer forma le Créateur.
Je vous chéris, amour, et ma plume en délire
Couché sur le papier ce que je n'ose dire.
Avec soin de mes vers lisez les premiers mots,
Vous saurez quel remède apporter à mes maux.

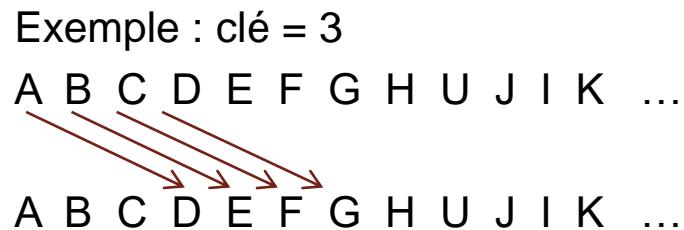
3. LES BASES DE LA CRYPTOGRAPHIE

b. Un peu d'histoire : « Chiffrement de César »

Exemple d'algorithme cryptographiques historique. Les algorithmes sont maintenant basés sur des fonctions mathématiques.

Chiffrement de César

Méthode : il s'agit ici de « décaler » chaque caractère par un nombre déterminé.



Exercice :

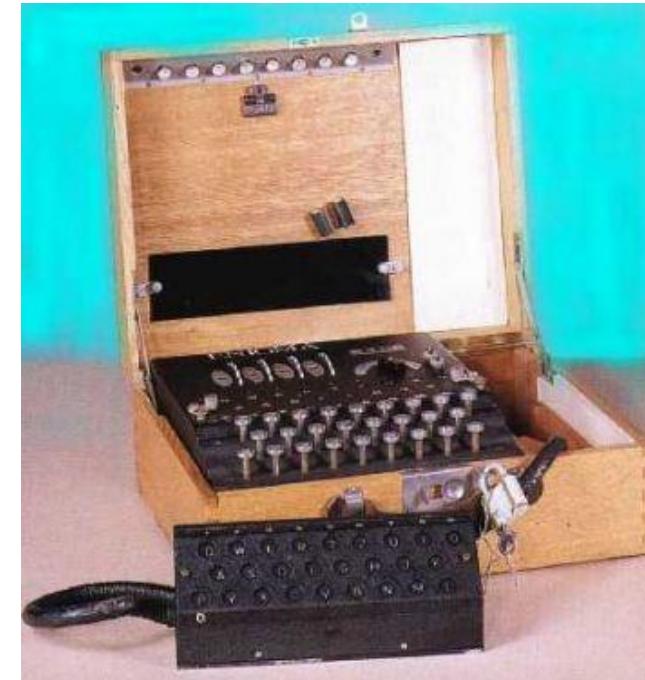
Donnée chiffrée : FBEHUHGX
Quelle est la donnée en clair ?

3. LES BASES DE LA CRYPTOGRAPHIE

b. Un peu d'histoire : « Machine Enigma »

Présentation des machines Enigma

- Machine initiale conçue au début du XX^e siècle. Elle a bénéficié de plusieurs évolutions et versions, et a été utilisée par les Allemands pendant la seconde guerre mondiale ;
- Les machines Enigma ressemblent à des machines à écrire, avec un clavier destiné à un opérateur, un tableau de sortie (panneau lumineux), plusieurs rotors, un réflecteur et un tableau de connexion ;
- La méthode de chiffrement est basée sur de la substitution :
 - L'opérateur tape le message en clair. Chaque lettre du message en clair est remplacée par une autre lettre dans le message chiffré (les lettres chiffrées s'allument sur le tableau de sortie au fur et à mesure de la frappe en clair de l'opérateur) ;
 - L'utilisation des rotors a pour conséquence qu'une lettre en clair sera être substituée par des lettres différentes tout au long du message chiffré.



source image : <http://museeradiomili.com/cryptographie/>

3. LES BASES DE LA CRYPTOGRAPHIE

b. Un peu d'histoire : « Machine Enigma »

Les fonctions d'une machine Enigma

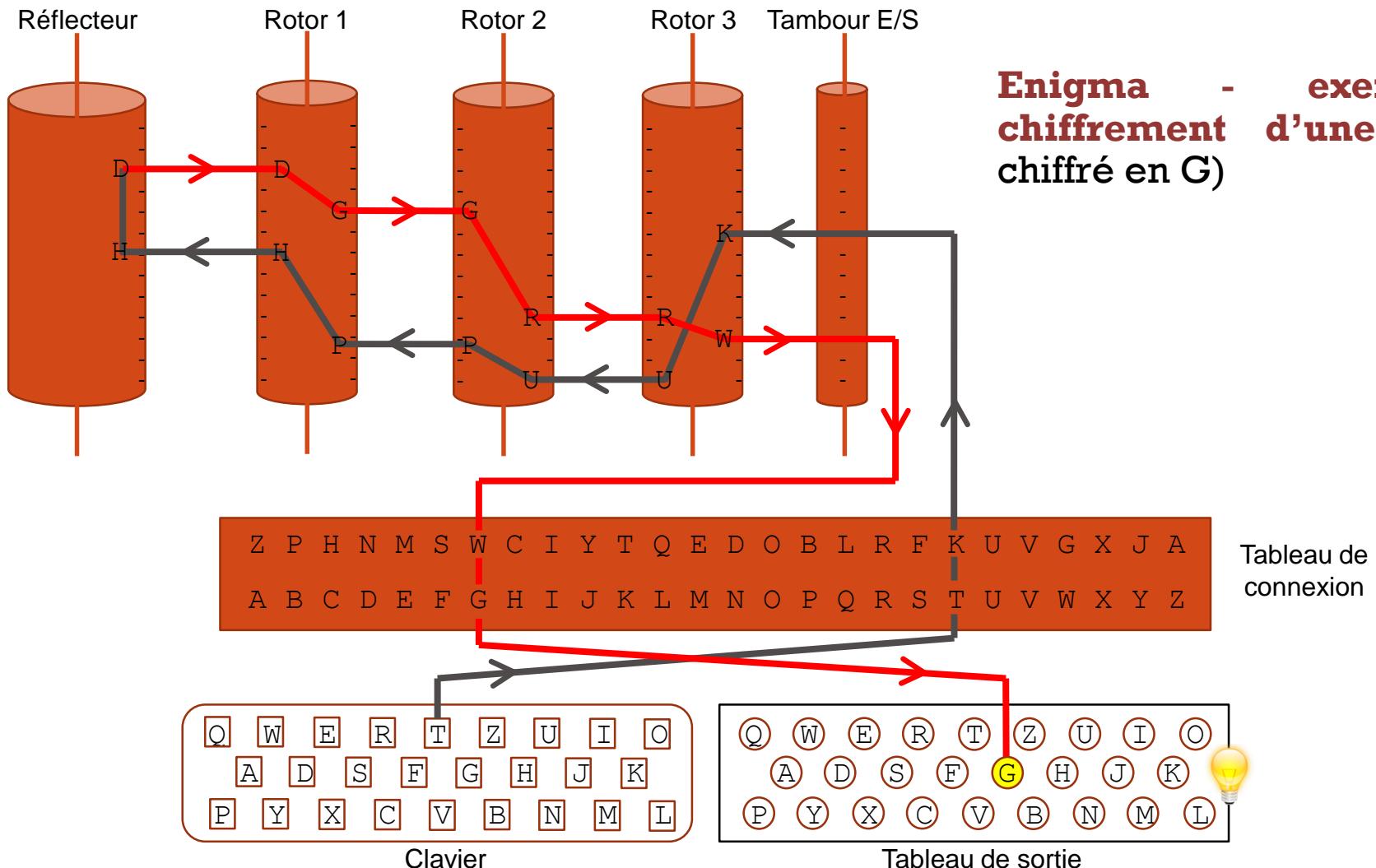
- Tableau de connexion
 - Se situe avant l'entrée sur le brouilleur ;
 - Effectue des permutations simples.
- De 3 à 6 rotors (selon le modèle)
 - Permutations aléatoires des lettres de l'alphabet ;
 - Le rotor tourne à chaque lettre tapée ;
 - Lorsque le premier rotor a fait un tour (26 positions), le second rotor tourne d'un cran, et ainsi de suite.
- Le réflecteur
 - Dernière permutation 2 à 2 des lettres avant de les faire retraverser les rotors et le tableau de connexion.



source images : https://interstices.info/jcms/jalios_5127/accueil

3. LES BASES DE LA CRYPTOGRAPHIE

b. Un peu d'histoire : « Machine Enigma »



3. LES BASES DE LA CRYPTOGRAPHIE

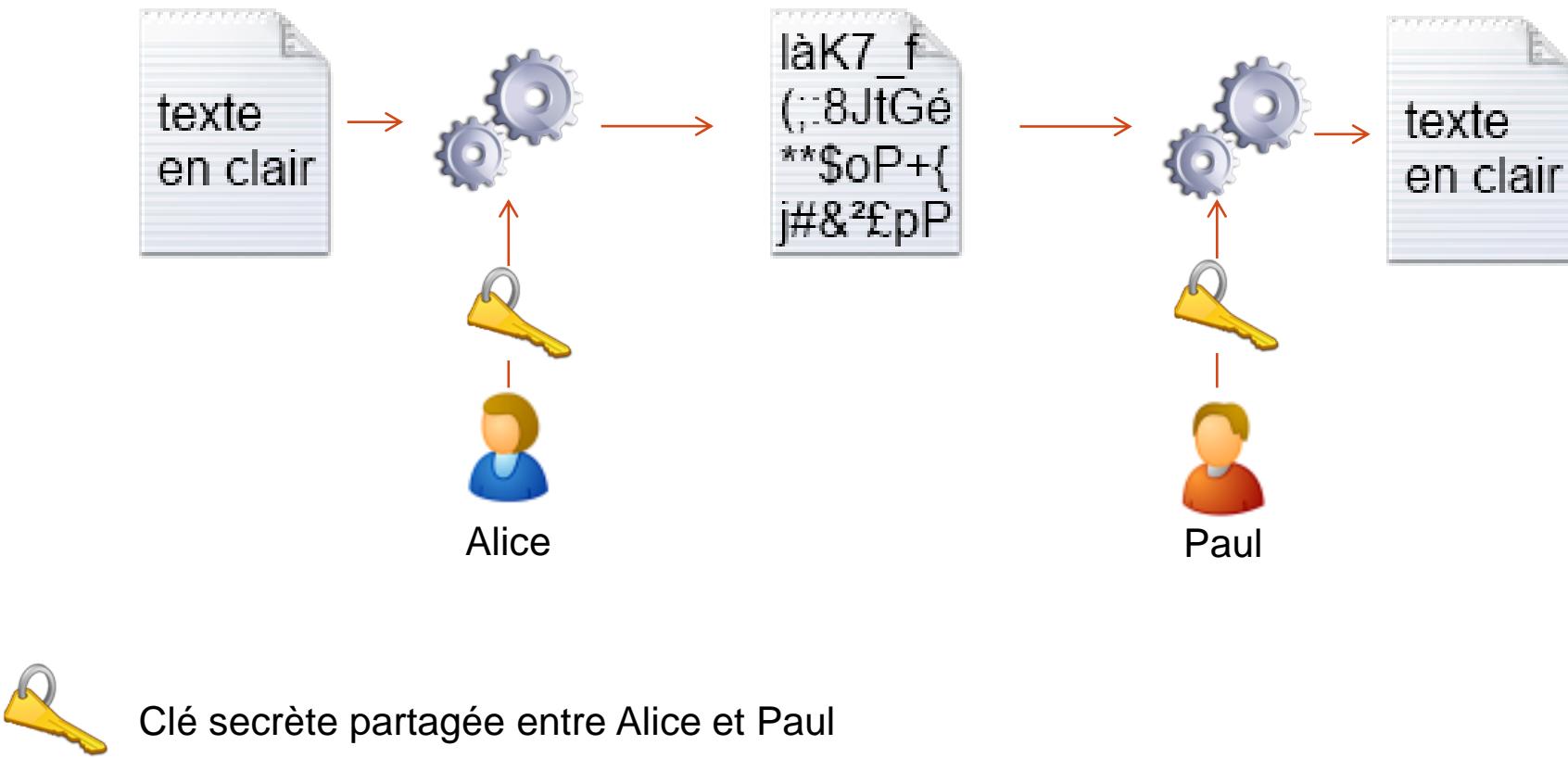
c. Chiffrement symétrique

- La clé utilisée pour le chiffrement est la **même** que celle utilisée pour le déchiffrement ;
- Cette clé doit être **secrète** : seules les personnes habilitées doivent posséder cette clé, sinon la confidentialité du message n'est plus assurée !

3. LES BASES DE LA CRYPTOGRAPHIE

c. Chiffrement symétrique

- Exemple : Alice souhaite envoyer un message confidentiel à Paul



3. LES BASES DE LA CRYPTOGRAPHIE

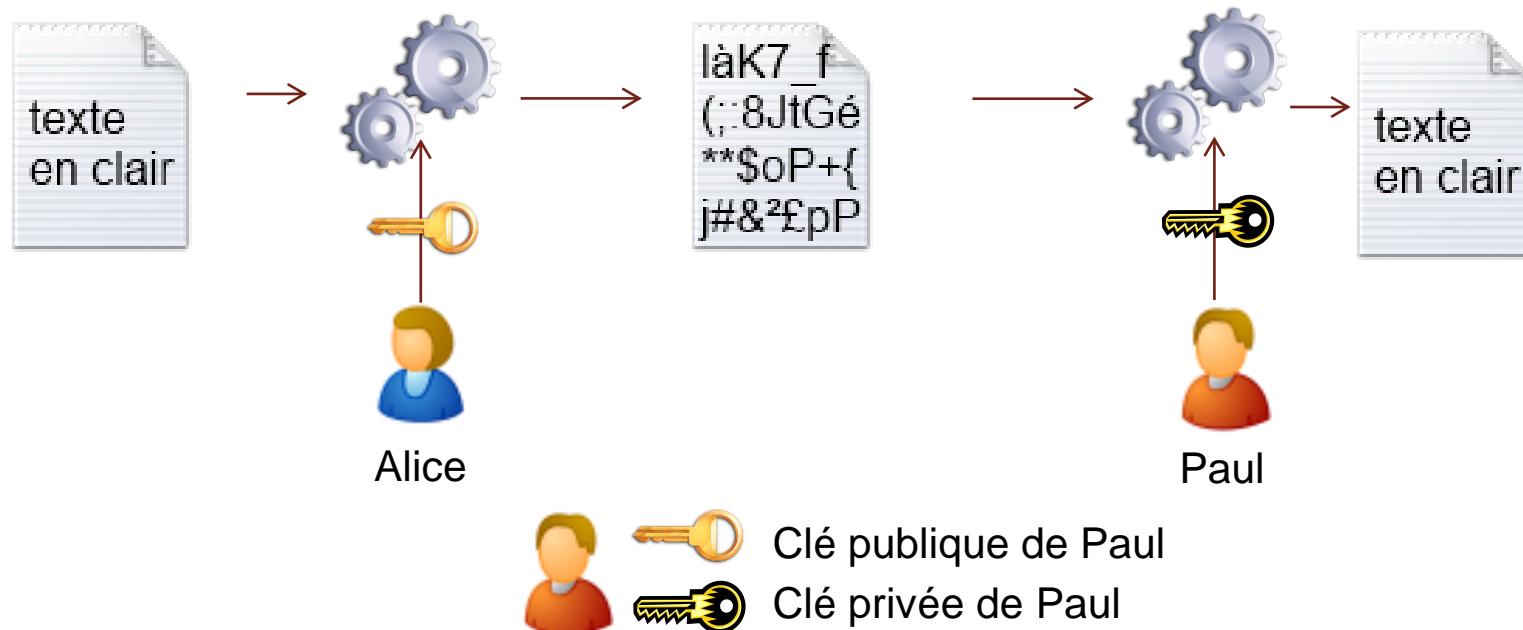
d. Chiffrement asymétrique

- La clé utilisée pour le chiffrement est **différente** de celle utilisée pour le déchiffrement. Il est nécessaire d'utiliser 2 clés :
 - Clé publique : comme son nom l'indique, cette clé est publique et peut être donnée à tout le monde ;
 - Clé privée : cette clé doit être personnelle et connue de son seul propriétaire. Elle ne doit jamais être divulguée !
- Ces deux clés sont mathématiquement liées
 - La connaissance de la clé publique ne permet pas de calculer de manière efficace la clé privée (attention à la taille de la clé, qui doit être suffisamment longue) ;
 - Chaque personne doit donc posséder 2 clés : une clé privée (confidentielle) et une clé publique qu'il peut divulguer à tout le monde.

3. LES BASES DE LA CRYPTOGRAPHIE

d. Chiffrement asymétrique

- Exemple : Alice souhaite envoyer un message confidentiel à Paul
 - Alice chiffre le message avec la clé publique de Paul ;
 - Paul déchiffre le message grâce à sa privée ;
 - Notes :
 - Alice ne pourra jamais (et n'aura jamais besoin de) utiliser la clé privée de Paul puisque celle-ci est confidentielle à Paul !
 - Alice n'a pas besoin d'utiliser ses clés personnelles dans cet exemple de chiffrement sans signature.



3. LES BASES DE LA CRYPTOGRAPHIE

e. Chiffrement symétrique vs Chiffrement asymétrique

Chiffrement symétrique

Avantages

- Rapidité des opérations (adapté à du trafic en temps réel) ;
- Clés courtes (256 bits suffisent actuellement) ;

Chiffrement asymétrique

- Facilité d'échange des clés : les seules clés qui ont besoin d'être échangées sont des clés publiques (dont il faut assurer la protection en intégrité) ;

Inconvénients

- Difficulté d'échange sécurisé des clés secrètes : comment le faire en protégeant ce secret ?

- Lenteur des opérations (peu adapté à du trafic en temps réel) ;
- Grande taille des clés (2048 bits minimum actuellement) ;

Exemples d'algorithmes sûrs (janvier 2015)

- AES.

- RSA.

3. LES BASES DE LA CRYPTOGRAPHIE

f. Signature électronique

Rappel de l'objectif : **s'assurer de la non-modification d'une donnée**, et **s'assurer de l'identité de son auteur**. Si la signature n'est pas valide, cela indique que l'auteur « n'est pas le bon » ou que la donnée reçue n'est pas celle que son auteur avait signé.

Notes :

- **La signature électronique n'assure pas la confidentialité des données**, mais leur intégrité et la notion de preuve ;
- **Lorsque l'on chiffre un message, il est fortement recommandé de le signer également** afin d'assurer l'intégrité du message.

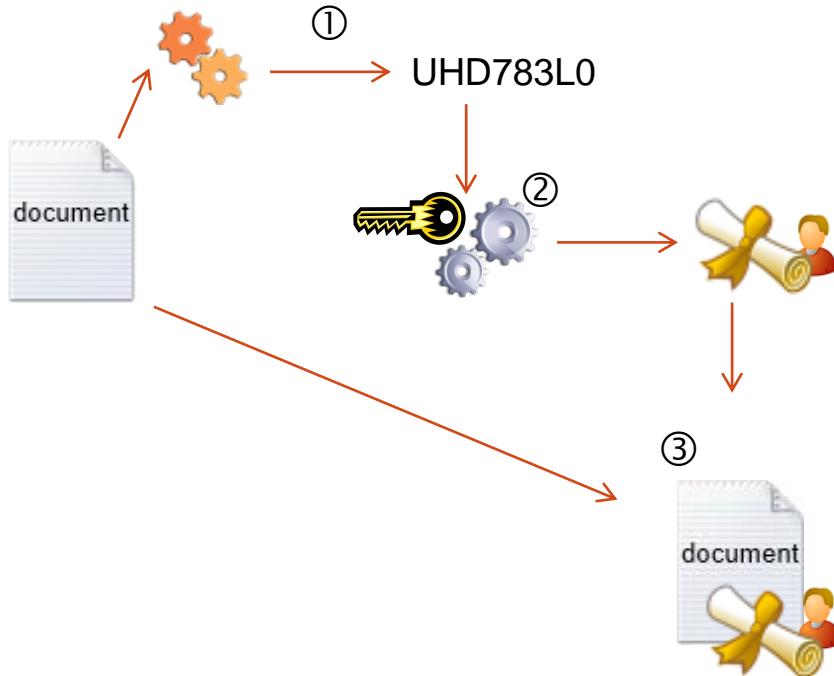
3. LES BASES DE LA CRYPTOGRAPHIE

f. Signature électronique : principe

1. Le signataire d'un message génère – grâce à un algorithme cryptographique spécifique – une valeur unique calculée à partir du message que l'on souhaite signer : un condensat (un haché) ;
 - Les algorithmes de calcul de condensat sont publics et ne gèrent pas de secret, donc tout le monde peut les utiliser et calculer les mêmes condensats à partir d'un même message ;
 - Deux messages différents ne peuvent pas donner lieu au même condensat.
2. Le signataire utilise l'algorithme de signature, qui prend en entrée sa clé privée et le condensat précédent, pour produire une signature électronique ;
3. Le signataire envoie (ou stocke) le message et la signature électronique, permettant ainsi à un lecteur d'en prendre connaissance ;
4. Le lecteur calcule lui-même le condensat du message en clair ;
5. Le lecteur utilise l'algorithme de vérification de signature, qui prend en entrée la clé publique du signataire, le condensat et la signature, pour rendre un verdict. Si le verdict est négatif, alors il ne faut pas faire confiance au message reçu (celui-ci ne correspond pas — pour une raison que l'on ignore — au message du signataire).

3. LES BASES DE LA CRYPTOGRAPHIE

f. Signature électronique : illustration



Etapes de la signature :

- ① Le signataire génère le condensat unique associé au message ;
- ② Le signataire utilise l'algorithme de signature, qui prend en entrée sa clé privée et le condensat précédent, pour produire une signature électronique ;
- ③ Le signataire envoie (ou stocke) le message et la signature électronique, permettant ainsi à un lecteur d'en prendre connaissance ;

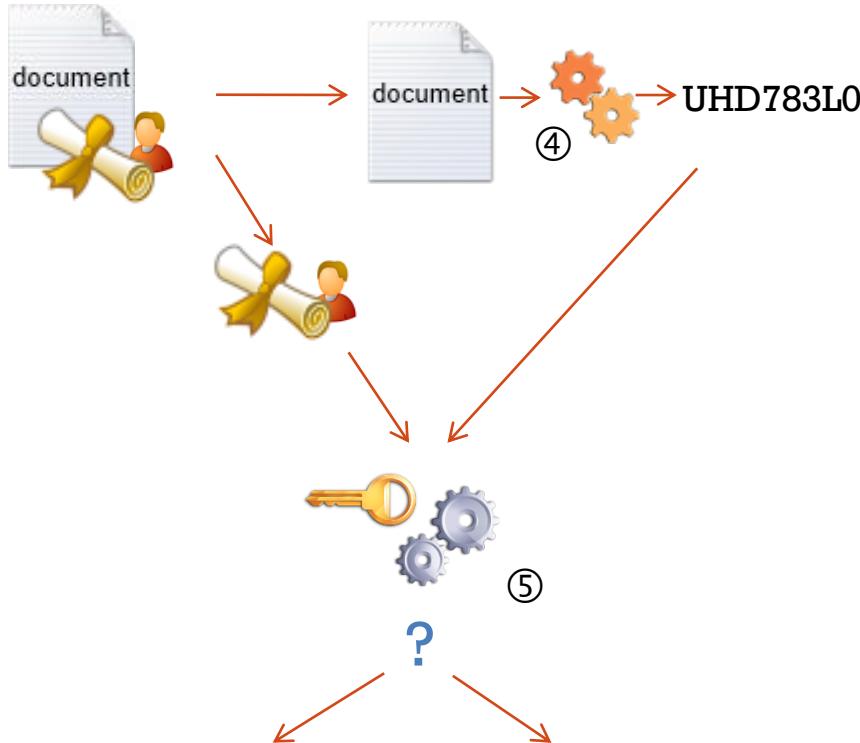
La vérification par le destinataire/lecteur est décrite sur la diapositive suivante.



- Clé publique du signataire
Clé privée du signataire

3. LES BASES DE LA CRYPTOGRAPHIE

f. Signature électronique : illustration



✓ La signature est valide.
Le message est intègre.

✗ La signature est
invalide. Le message
n'est pas intègre.

Etapes de la vérification de la signature par un lecteur/destinataire :

- ④ Le lecteur calcule le condensat du message en clair ;
- ⑤ Le lecteur utilise l'algorithme de vérification de signature, qui prend en entrée la clé publique du signataire, le condensat et la signature, pour rendre un verdict. Si le verdict est négatif, alors il ne faut pas faire confiance au message reçu (celui-ci ne correspond pas — pour une raison que l'on ignore — au message du signataire).



Clé publique du signataire
Clé privée du signataire

3. LES BASES DE LA CRYPTOGRAPHIE

g. Certificats électroniques

Un aspect important n'a pas été traité jusqu'à maintenant :



Clé publique de Paul



Clé privée de Paul

Les interlocuteurs de Paul ont besoin d'utiliser sa clé publique. Comment peuvent-ils **être certains que la « clé publique de Paul » appartient effectivement à Paul** et qu'elle n'a pas été générée frauduleusement en son nom ? Autre exemple, comment les visiteurs d'un site web bancaire peuvent **être certains que le site web est légitime** et qu'il ne s'agit pas d'un site frauduleux imitant celui d'une banque ?

- Solution : utilisation de certificats électroniques.

3. LES BASES DE LA CRYPTOGRAPHIE

g. Certificats électroniques

Un certificat est un **fichier électronique** qui comprend notamment :

- La **clé publique** d'un individu (ou d'une entité ou d'un nom de domaine) ;
- Les détails de cet individu (ou de cette entité) : nom, prénom, nom de domaine, etc. ;
- La **signature par un tiers de confiance**, chargé de garantir que le propriétaire de la clé publique a été vérifié et – par conséquent – l'authenticité de la clé publique vis-à-vis de son propriétaire. La signature porte sur l'identité du détenteur et la clé publique afin d'assurer l'intégrité de l'ensemble ;
- D'autres informations telles que l'usage de la clé, les dates de validité, des informations concernant la révocation, etc.

Le tiers de confiance, une autorité de certification, en charge de :

- **Vérifier l'identité** de la personne demandant à créer le certificat ;
- **Créer le certificat** après vérification, **puis le signer** (avec la clé privée de l'autorité de certification) ;
- **Tenir à jour une liste des certificats qui ont été révoqués** (par exemple si la clé a été compromise).

3. LES BASES DE LA CRYPTOGRAPHIE

g. Certificats électroniques

Comment connaitre les autorités de certification ?

- Elles sont directement intégrées par les éditeurs dans les systèmes d'exploitation et/ou les navigateurs ;
- L'utilisateur est également libre de rajouter l'autorité de certification de son choix si il choisit de faire confiance à des certificats signés par une autorité non-intégrée dans son navigateur.

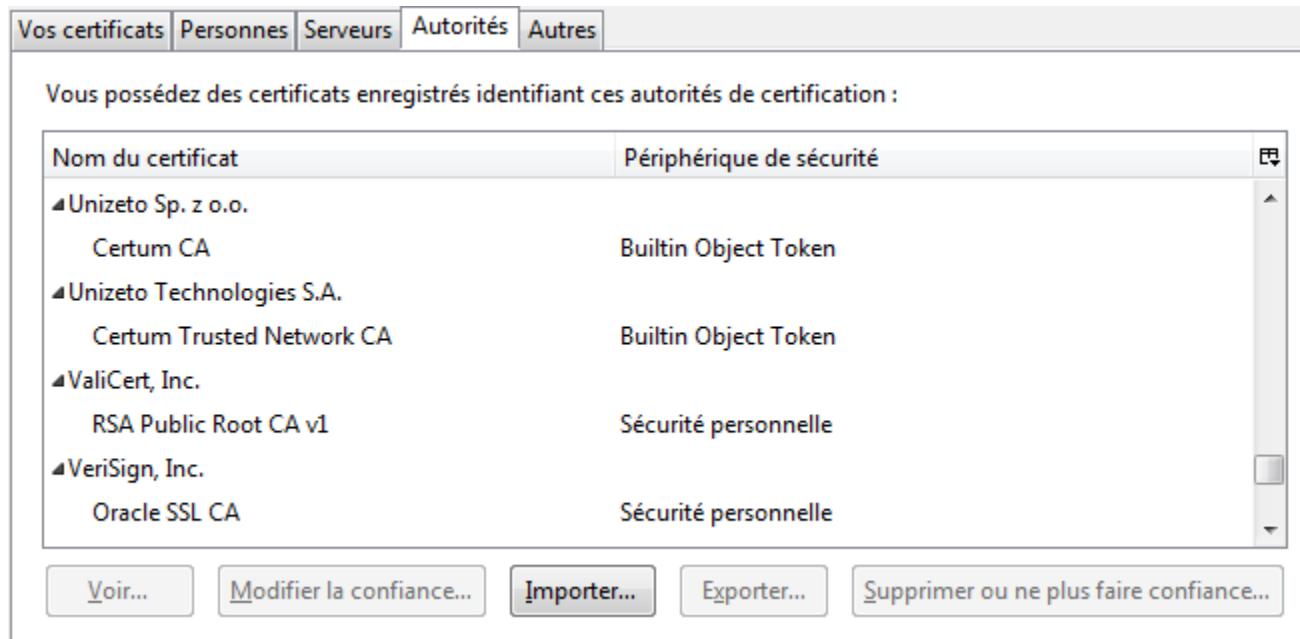


Image : magasin de certificats de Firefox

3. LES BASES DE LA CRYPTOGRAPHIE

g. Certificats électroniques

Exemple d'un certificat pour le site web www.france-universite-numerique-mooc.fr

Les détails techniques du certificat, la clé et la signature se trouvent dans **Détails**

Détenteur de la clé publique

Autorité de certification

Dates de validité du certificat

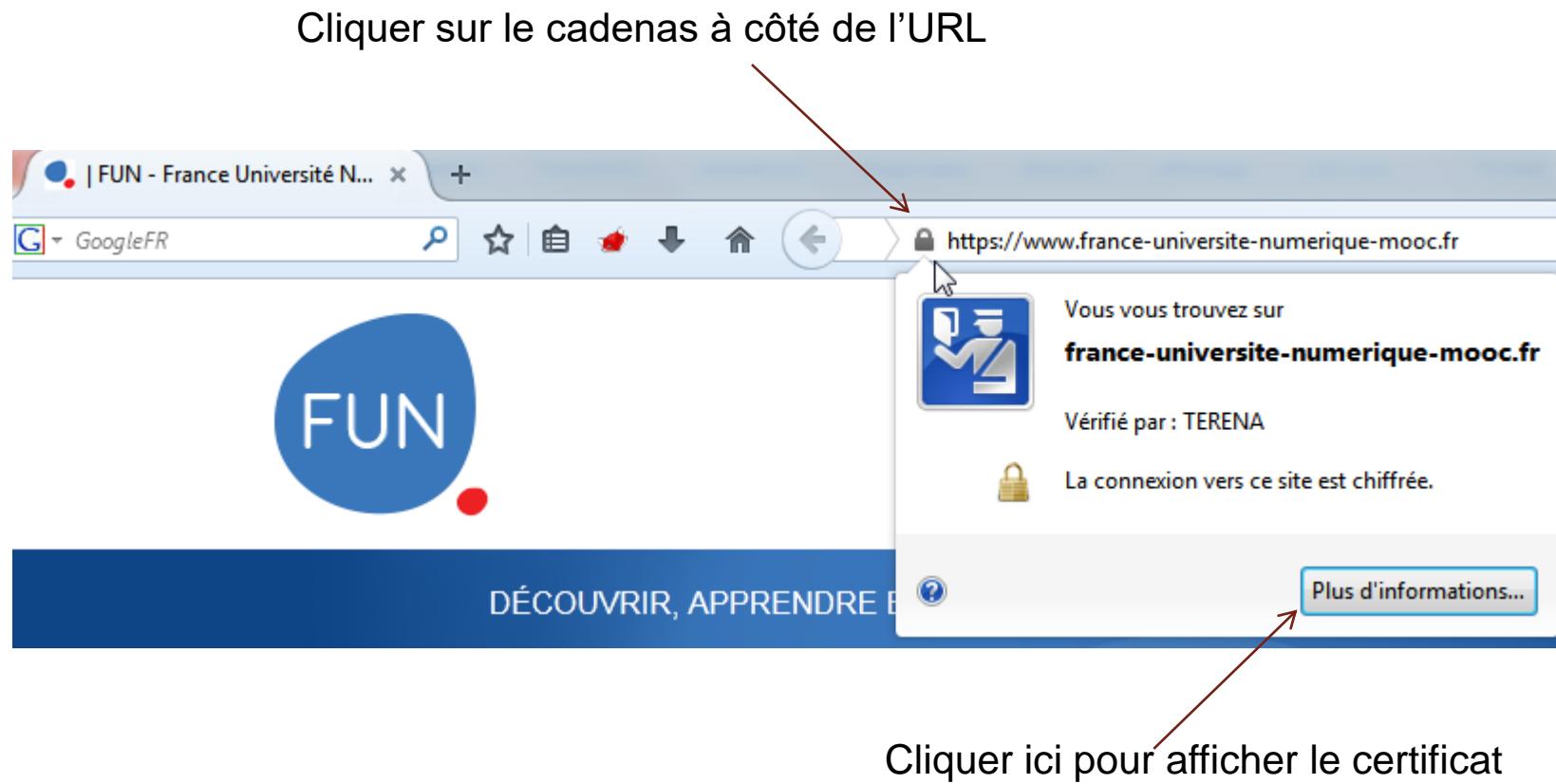
Général	Détails
	<p>Ce certificat a été vérifié pour les utilisations suivantes :</p> <p>Certificat client SSL Certificat serveur SSL</p>
	<p>Émis pour</p> <p>Nom commun (CN) : www.france-universite-numerique-mooc.fr Organisation (O) : <Ne fait pas partie du certificat> Unité d'organisation (OU) : Domain Control Validated Numéro de série : 00:EE:CE:37:A0:F9:50:16:57:BC:0A:C2:4B:A8:9F:0E:41</p>
	<p>Émis par</p> <p>Nom commun (CN) : TERENA SSL CA Organisation (O) : TERENA Unité d'organisation (OU) : <Ne fait pas partie du certificat></p>
	<p>Période de validité</p> <p>Débute le : 08/10/2013 Expire le : 08/10/2016</p>
	<p>Empreintes numériques</p> <p>Emprinte numérique SHA-256 : 6E:D0:7E:51:A4:2A:86:97:A0:A8:C0:70:9C:32:E8:8B: 16:B3:89:22:A2:C5:AE:5A:FE:35:99:0E:B3:79:10:EB Emprinte numérique SHA1 : 86:22:89:4F:FB:7B:9F:45:DF:B0:89:C0:A6:C0:83:DF:F6:2E:0B:9A</p>

3. LES BASES DE LA CRYPTOGRAPHIE

g. Certificats électroniques

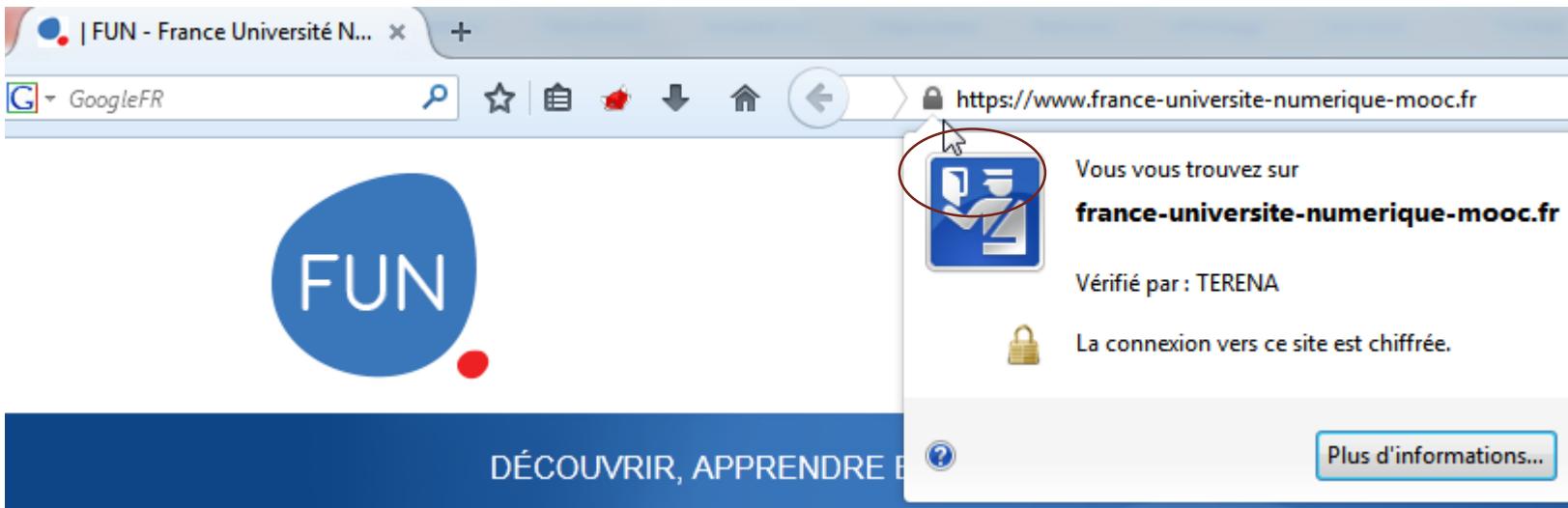
Où trouver les certificats dans un navigateur ?

Exemple avec Firefox pour ouvrir le certificat d'un site WEB



3. LES BASES DE LA CRYPTOGRAPHIE

g. Certificats électroniques



Puisque le certificat du site WEB est disponible et valide, cela amène donc deux avantages à l'utilisateur, caractéristiques du HTTPS

- Nous sommes confiants que **le site WEB est légitime** (i.e. le certificat a été vérifié et signé par une autorité de certification de confiance) ;
- Puisque le certificat contient la clé publique du site WEB, nous pouvons donc **chiffrer nos connexions vers ce site** (méthode : chiffrement avec la clé publique du destinataire comme nous l'avons vu au préalable dans ce cours).

3. LES BASES DE LA CRYPTOGRAPHIE

h. Jetons cryptographiques (tokens)

- Les jetons sont utilisés pour **stocker des clés privées** (cryptographie asymétrique) ou **secrètes** (cryptographie symétrique) ;
- Puisqu'un jeton contient une information sensible (une clé privée ou secrète), il faut donc **protéger ce jeton** pour que seules les personnes habilitées puissent l'utiliser ;
- Exemples de jetons et leurs moyens de protection (ainsi que leur niveau de sécurité) :
 - **Fichier sur disque**, associé à un mot de passe connu de l'utilisateur seulement (exemple avec l'application libre GPG) ;
 - **Jeton USB**, associé à un mot de passe (exemple de nombreux produits commerciaux qui utilisent un jeton physique pour authentifier un utilisateur sur un poste de travail) ;
 - **Carte à puce**, associée à un mot de passe simple (exemple des cartes bancaires avec un code PIN permettant d'authentifier le propriétaire de la carte avant d'autoriser la transaction).
 - Afin d'éviter qu'une personne malveillante ne découvre facilement le mot de passe simple, on impose un verrouillage de la carte à puce après 3 tentatives infructueuses.



4. LA SÉCURITÉ DES APPLICATIONS WEB

- a) Usurpation d'identité via les cookies
- b) Injection SQL

4. LA SÉCURITÉ DES APPLICATIONS WEB

a. *Usurpation d'identité via les cookies*

Comme toutes les applications, les applications web sont sujettes à des vulnérabilités. Nous allons en voir deux d'entre elles :

- une faiblesse basée sur les cookies ;
 - Ce qui permet – par exemple – à un attaquant de contourner un mécanisme d'authentification.
- une faiblesse basée sur un code source mal développé.
 - Ce qui permet – par exemple – à un attaquant de contourner un mécanisme d'authentification, d'accéder à des données pour les divulguer ou les corrompre.

4. LA SÉCURITÉ DES APPLICATIONS WEB

a. *Usurpation d'identité via les cookies*

Les cookies sont des fichiers gérés par les navigateurs web afin de stocker (et réutiliser) des informations concernant l'utilisateur, par exemple :

- son identifiant ;
- ses préférences d'affichage et de disposition de la page web.

Les cookies sont nécessaires pour toutes les pages web dynamiques qui nécessitent d'identifier ou d'authentifier l'utilisateur, en permettant notamment la mise en œuvre de sessions :

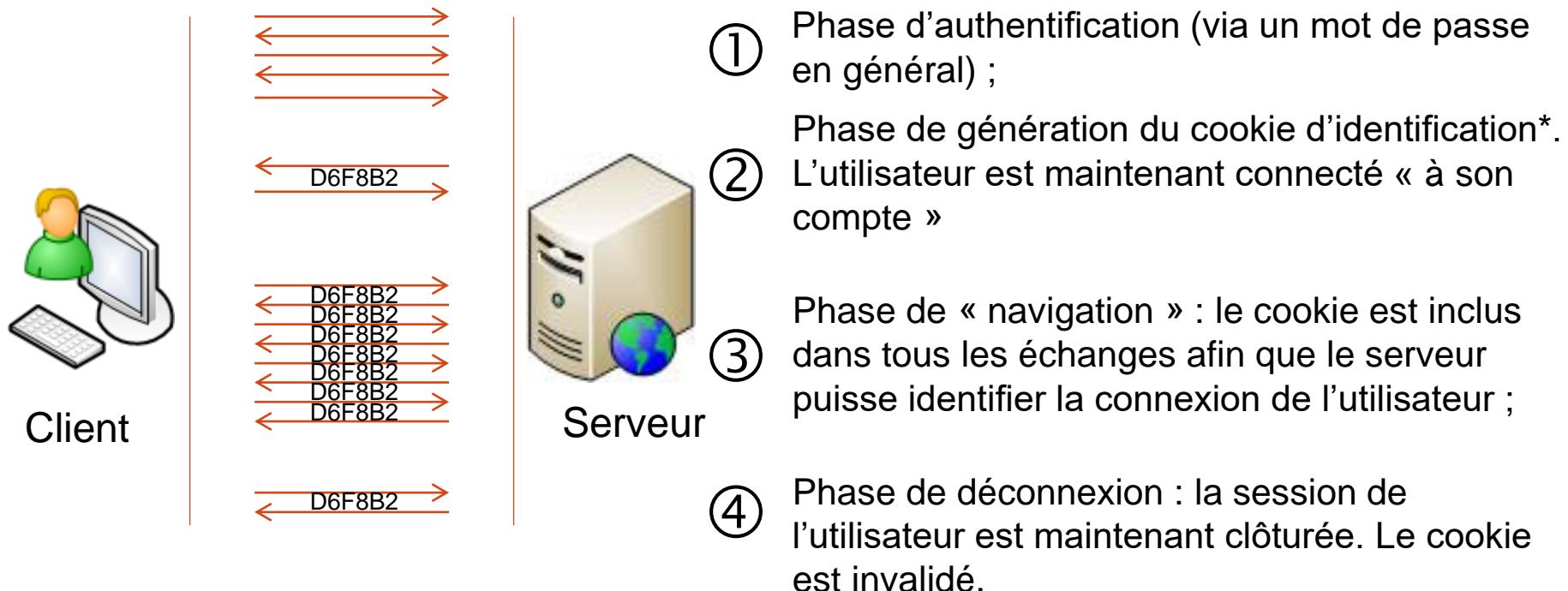
- les sites marchand (afin d'afficher le panier de l'utilisateur connecté) ;
- les sites bancaires (afin d'afficher le solde du compte de l'utilisateur connecté et non pas celui d'un autre client) ;
- les sites « en général » (afin d'afficher des publicités ciblées sur notre navigation).

Il est possible – sous certaines conditions – d'usurper l'identité d'un utilisateur sur un site web si on arrive à récupérer son cookie d'identification.

4. LA SÉCURITÉ DES APPLICATIONS WEB

a. Usurpation d'identité via les cookies

Fonctionnement habituel d'une connexion sur un site web nécessitant une authentification (site marchand, site bancaire, etc.) :

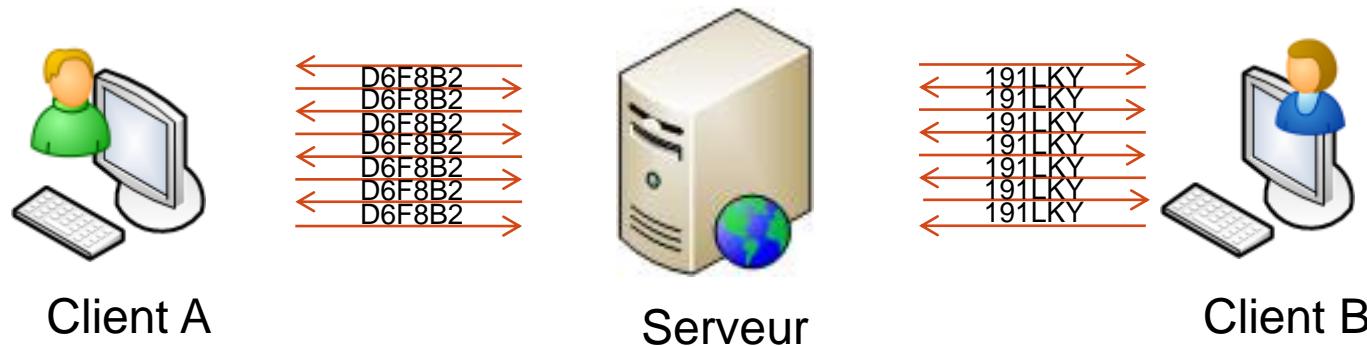


- Un cookie d'identification est en fait une chaîne de caractères aléatoire et unique, suffisamment longue pour qu'elle ne puisse pas être générée deux fois par erreur.
Exemple d'un cookie d'identification : D6F8B2BE3ED3040D9A3C10-D6F8B2A305D048B9

4. LA SÉCURITÉ DES APPLICATIONS WEB

a. Usurpation d'identité via les cookies

A tout moment d'une connexion, chaque utilisateur du site web possède donc son propre cookie, unique à lui. Le serveur est donc en mesure d'identifier à qui appartient chaque connexion, et donc d'afficher les pages web qui lui sont propres.

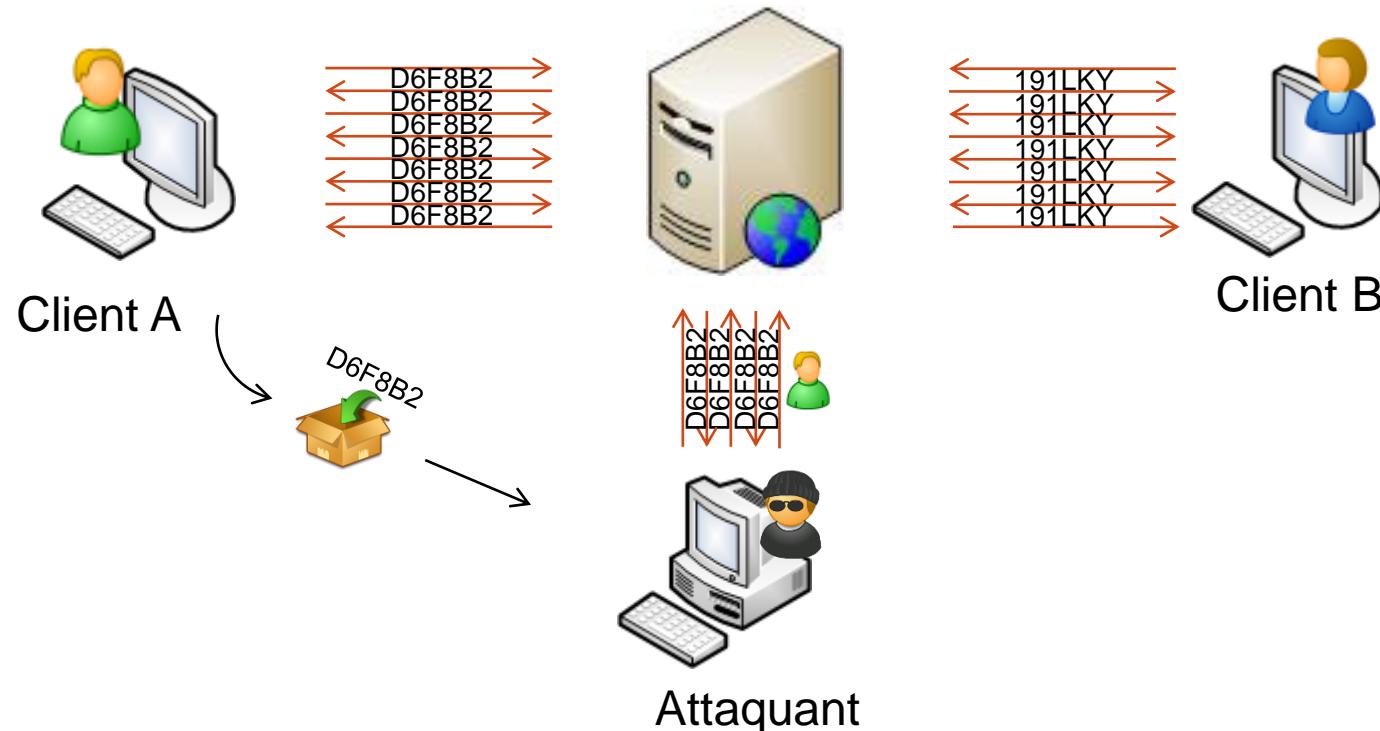


4. LA SÉCURITÉ DES APPLICATIONS WEB

a. Usurpation d'identité via les cookies

Mais que se passe-t-il si un attaquant arrive à dérober le cookie d'un utilisateur et se connecte au même serveur ?

- Il se fait passer pour l'utilisateur dont il a dérobé le cookie au près du serveur applicatif ! Il usurpe donc l'identité de la victime et accède à son compte.



4. LA SÉCURITÉ DES APPLICATIONS WEB

a. *Usurpation d'identité via les cookies*



L'attaquant peut dérober un cookie d'identification par différents moyens :

- soit en écoutant le trafic réseau HTTP et en interceptant les données applicatives, dont le cookie ;
 - Moyen de protection : l'utilisateur doit **s'assurer que le site auquel il est connecté utilise du HTTPS** (le cookie est donc chiffré pendant le transport).
- soit en dérobant le cookie sur le poste de travail en utilisant une vulnérabilité du système ;
 - Moyen de protection : l'utilisateur doit **sécuriser son système d'exploitation et ses logiciels** correctement (services inutiles désactivés, installation des mises à jours de sécurité, anti-virus, etc. voir le module 2 pour plus d'informations).
- soit en dérobant le cookie sur le poste de travail via des méthodes d'ingénierie sociale ciblées sur l'utilisateur ;
 - Moyen de protection : l'utilisateur doit **être sensibilisé aux méthodes d'ingénierie sociale** (phishing, spam, etc.) afin de « ne pas tomber dans le panneau »
- soit en dérobant le cookie via une faille sur le serveur ;
 - Moyen de protection : l'exploitant du serveur doit **suivre les bonnes pratiques de sécurisation et du maintien en condition de sécurité** du serveur, ainsi que les **bonnes pratiques de développement applicatif**.



4. LA SÉCURITÉ DES APPLICATIONS WEB

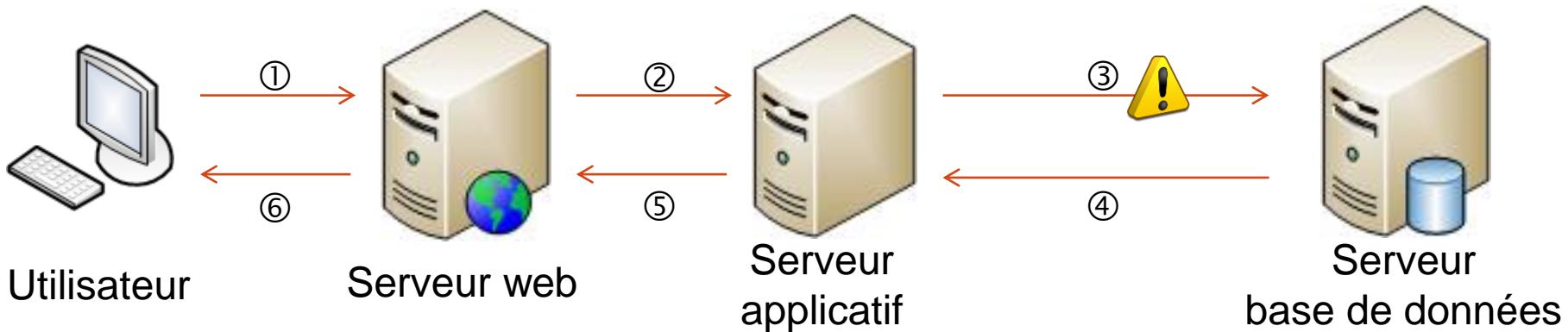
b. Injection SQL

- Une attaque par injection SQL permet à un **attaquant d'interagir directement avec la base de données** d'un site web (alors que l'accès à cette base est bien entendu interdite) ;
- L'objectif de ce type d'attaque est en général de **contourner le mécanisme d'authentification, d'accéder ou de modifier frauduleusement les données** confidentielles de la base (mots de passe, téléphones, numéro de carte bancaire, etc.) ;
- Il existe de multiples variantes possibles, la diapositive suivante présente un exemple de contournement d'authentification d'une page web.

4. LA SÉCURITÉ DES APPLICATIONS WEB

b. Injection SQL

Architecture standard logicielle d'un site web faisant appel à une base de données



- ① Le navigateur client demande l'affichage d'une page ;
- ② Le serveur web transfère la demande au serveur applicatif ;
- ③ Le serveur applicatif génère une requête SQL afin de récupérer les informations nécessaires ;
- ④ Le serveur base de données retourne le résultat de la requête au serveur applicatif ;
- ⑤ Le serveur applicatif transmet au serveur web les informations nécessaires à la création de la page à afficher ;
- ⑥ Le serveur web envoie les pages HTML au navigateur client.

4. LA SÉCURITÉ DES APPLICATIONS WEB

b. Injection SQL

- L'objectif d'une attaque de type injection SQL consiste à détourner la requête SQL de l'étape 3 (diapositive précédente), et – en fonction du contexte – créer sa propre requête SQL malveillante ;
- La diapositive suivante illustre comment une telle attaque peut être menée à partir d'un navigateur client.

4. LA SÉCURITÉ DES APPLICATIONS WEB

b. Injection SQL

Formulaire WEB :

Entrez votre identifiant et votre mot de passe puis cliquez sur Connexion :

The form consists of two input fields: 'Login' and 'Mot de passe', both with placeholder text. Below them is a large, dark red rectangular button labeled 'Connexion'.

\$user contient le login renseigné dans le formulaire par l'utilisateur.
\$mdp contient le mot de passe.

La requête SQL permettant de vérifier le login et le mot est la suivante :

```
select count(*) from user where user='$user' and mdp='$mdp'
```

Ainsi, une requête légitime serait la suivante :

```
select count(*) from user where user='thomas' and mdp='cykUfl9an'
```

4. LA SÉCURITÉ DES APPLICATIONS WEB

b. Injection SQL

Formulaire WEB :

Entrez votre identifiant et votre mot de passe puis cliquez sur Connexion.

The form is composed of three main elements: a 'Login' field, a 'Mot de passe' field, and a large 'Connexion' button.

Mais que se passe-t-il si un attaquant rentre précisément les chaînes de caractères suivantes ?

Login : azerty

Mot de passe : **abcd' or 1=1/***

La requête SQL `select count(*) from user where user='$user' and mdp='$mdp'`

devient donc :

```
select count(*) from user where user='azerty' and mdp='abcd' or 1=1/*'
```

Cette condition est toujours vraie !

4. LA SÉCURITÉ DES APPLICATIONS WEB

b. *Injection SQL*

- La condition étant toujours vraie, la requête est donc toujours valide, quel que soit le mot de passe renseigné par l'attaquant !
 - Les caractères /* sont utilisés pour ignorer la fin de la requête légitime.
- La faiblesse réside ici dans le code applicatif : les **données** renseignées par l'utilisateur (i.e. un attaquant dans notre scénario) **ne sont pas vérifiées/validées** ; elles sont au contraire utilisées telles quelles sans aucune vérification préalable qu'elles sont « inoffensives »
- Comment s'en protéger ?
 - **Valider systématiquement chaque donnée** extérieure avant de l'utiliser ;
 - Recourir à des requêtes préparées (connues sous le nom de « **prepared statements** »), qui ont l'avantage d'être plus résistantes aux injections ;
 - D'une façon générale, **respecter les bonnes pratiques de développement** recommandées par l'industrie concernant le code PHP, Java, etc.

SENSIBILISATION ET INITIATION À LA CYBERSÉCURITÉ

- **Module 4 : La gestion de la cybersécurité au sein d'une organisation**

PLAN DU MODULE

- 1. Intégrer la sécurité au sein d'une organisation**
- 2. Intégrer la sécurité dans les projets**
- 3. Difficultés liées à la prise en compte de la sécurité**
- 4. Métiers liés à la cybersécurité**

1. INTÉGRER DE LA SÉCURITÉ AU SEIN D'UNE ORGANISATION

- a) Préambule
- b) Panorama des normes ISO 2700x
- c) Système de Management de la Sécurité de l'Information (27001)
- d) Code de bonnes pratiques pour le management de la sécurité de l'information (27002)
- e) Gestion des risques (27005)
- f) Classification des informations
- g) Gestion des ressources humaines

1. INTÉGRER LA SÉCURITÉ AU SEIN D'UNE ORGANISATION

- a. Préambule
- Les mesures de sécurité à mettre en place dépendent de l'activité, de l'organisation et de la réglementation et des contraintes de son écosystème.
- Afin d'évaluer le niveau de sécurité attendue, les questions suivantes peuvent être posées :
 - Qu'est ce que je veux protéger ?
 - De quoi je veux me protéger ?
 - A quel type de risques mon organisation est exposée ?
 - Qu'est ce que je redoute ?
 - Quelles sont les normes qui s'appliquent à mon organisation ?
- L'organisation peut s'inspirer de la famille de norme internationale ISO 27000 et des guides nationaux (ANSSI, CLUSIF, etc.), voire des politiques de sécurité en usage dans l'État (PSSIE, RGS, etc.) pour mettre en place la sécurité.

1. INTÉGRER LA SÉCURITÉ AU SEIN D'UNE ORGANISATION

- b. Panorama des normes ISO 27K
- Ensemble de normes internationales de sécurité de l'information, destinées à protéger l'information. Elles découlent d'une recherche de consensus commun sur le domaine.
- Néanmoins la conformité à une norme ne garantit pas formellement un niveau de sécurité. Les normes ne prennent pas en compte l'état de l'art récent et les exigences réglementaires.
- Quelques unes des principales normes incluses dans la série 27000 :

27001	• Systèmes de management de la sécurité de l'information
27002	• Code de bonnes pratiques
27004	• Mesures du management de la sécurité
27005	• Gestion des risques
27035	• Gestion des incidents de sécurité
27037	• Traitement des preuves numériques (<i>forensics</i>)
...	• ...

- b. Panorama de normes ISO 2700x
- Dans le cadre de la mise en place de la sécurité au sein d'une organisation :
 - La norme **ISO 27001** permet à une organisation de **mettre en œuvre et d'améliorer le système de management de la sécurité** :
 - Une certification ISO 27001 délivrée par un organisme certificateur accrédité garantie suite à un audit qu'une organisation a bien appliquée les exigences de la norme en matière de sécurité. Cette certification est valable 3 ans, tous les ans un audit de contrôle est effectué.
 - Il peut être exigé à une organisation d'avoir cette certification pour accéder à certains contrats : par exemple un organisme payeur d'aides agricoles européennes.
 - La norme **ISO 27002** définit un ensemble de « **bonnes pratiques** » en matière de sécurité répartie en plusieurs chapitres, l'organisation dispose :
 - d'un référentiel de mise en œuvre ;
 - d'une « check-list » en cas d'audit.
 - La norme **ISO 27005** définit des lignes directrices relatives à la **gestion des risques de sécurité** dans une organisation. Une organisation peut s'appuyer sur ce processus de gestion de risques pour intégrer la sécurité.

▪ c. Système de Management de la Sécurité de l'Information (27001)

Une démarche calquée sur ISO 9000 (**Plan / Do / Check / Act**).

Phase Plan : Fixer des objectifs et des plans d'actions :

- Identification des actifs ou des biens ;
- Analyse de risques ;
- Choisir le périmètre du SMSI :
 - Quel périmètre ? C'est le domaine d'application du SMSI, son choix est libre, mais il doit être circonscrit, ce sont toutes les activités pour lesquelles l'organisation exige de la confiance.
 - Quelle politique de sécurité ?
 - Quel niveau de sécurité : intégrité, confidentialité, disponibilité de l'information au sein de l'organisation ?

Noter que la norme n'impose pas de niveau minimum de sécurité à atteindre.



Attention : une entreprise peut donc être certifiée ISO 27001 tout en ayant défini un périmètre réduit et une politique de sécurité peu stricte.

1. INTÉGRER LA SÉCURITÉ AU SEIN D'UNE ORGANISATION

▪ c. Système de Management de la Sécurité de l'Information (27001)

- **Phase Do :** mise en œuvre et exploitation des mesures et de la politique
 - Établir un plan de traitement des risques ;
 - Déployer les mesures de sécurité ;
 - Former et sensibiliser les personnels ;
 - Déetecter les incidents en continu pour réagir rapidement.
- **Phase Check :** mesurer les résultats issus des actions mises en œuvre
 - Audits internes de conformité et d'efficacité du SMSI (ponctuels et planifiés) ;
 - Réexaminer l'adéquation de la politique SSI avec son environnement ;
 - Suivre l'efficacité des mesures et la conformité du système ;
 - Suivre les risques résiduels.
- **Phase Act :**
 - Planifier et suivre les actions correctrices et préventives.

▪ c. Système de Management de la Sécurité de l'Information (27001)

Avantages

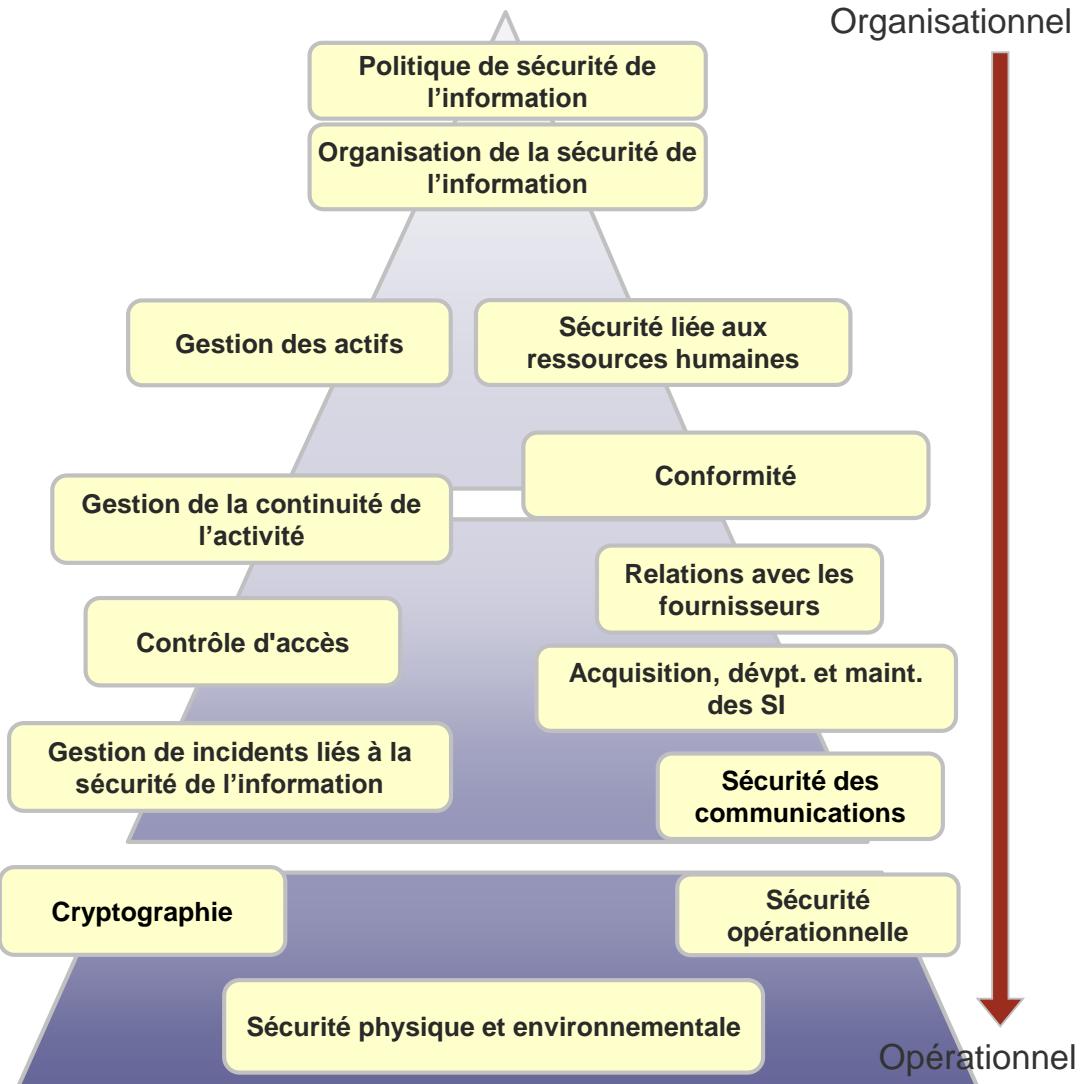
- Description détaillée de la **mise en œuvre des objectifs et des mesures de sécurité** ;
- **Audits réguliers** qui permettent le suivi entre les risques initialement identifiés, les mesures prises et les risques nouveaux ou mis à jour. Objectif : mesurer l'**efficacité** des mesures prises ;
- **Sécurité** : une amélioration continue de la sécurité : donc un niveau croissant de sécurité et de maturité en SSI ;
- Meilleure **maîtrise** des différents **risques** ;
- Élimination des mesures de sécurité non usitées ;
- Amélioration de la **confiance des associés, partenaires & clients** ;
- **Référentiel international** qui facilite les échanges ;
- **Indicateurs** clairs et fiables produisant des éléments de pilotage financier pour les dirigeants.

1. INTÉGRER LA SÉCURITÉ AU SEIN D'UNE ORGANISATION

▪ d. Code de bonnes pratiques pour le management de la sécurité de l'information (27002)

- La norme ISO/IEC 27002:2013 constitue un code de bonnes pratiques. Elle est composée de 114 mesures de sécurité réparties en 14 chapitres couvrant les domaines organisationnels et techniques ci-contre.

- C'est en adressant l'ensemble de ces domaines que l'on peut avoir une approche globale de la sécurité des S.I.



1. INTÉGRER LA SÉCURITÉ AU SEIN D'UNE ORGANISATION

▪ d. Code de bonnes pratiques pour le management de la sécurité de l'information (27002)

- Exemples de mesures sur le chapitre « Contrôle d'accès » :
 - L'accès aux fichiers/répertoires doit être restreint conformément aux politiques de contrôle d'accès :
 - Seuls les professeurs autorisés doivent pouvoir accéder à un répertoire contenant les épreuves des futurs examens/concours.
 - Les propriétaires de l'information doivent vérifier les droits d'accès à intervalles réguliers :
 - Le responsable des concours doit contrôler les droits d'accès au répertoire contenant les épreuves des futurs examens/concours pour s'assurer qu'il n'y a pas d'étudiants qui auraient été rajoutés.
- Exemple de mesures sur le chapitre « Sécurité opérationnelle » :
 - L'installation et la configuration de logiciels doivent être encadrés :
 - Seuls les administrateurs doivent pouvoir installés un logiciel sur un poste.
 - Des sauvegardes doivent êtres régulièrement effectuées et testées :
 - Un espace de sauvegarde des données peut être mis à disposition des utilisateurs.

▪ e. Gestion des risques (27005)

La norme 27005 présente **une démarche** :

- Établissement du contexte de l'analyse des risques ;
- Définition de l'appréciation des risques SSI ;
- Choix pour le traitement du risque SSI ;
- Acceptation du risque ;
- Communication et concertation relative aux risques SSI ;
- Surveillance et revue du risque en SSI.

Avantages

- Définit une démarche rationnelle qui a donné lieu à des méthodes qui fonctionnent ;
- Grande souplesse : utilisée en toutes circonstances, surtout lors des changements ;
- Pragmatique et utilisable seule, elle peut aussi bien convenir aux petites organisations.

Limites

- L'organisation doit définir sa propre approche ;
- Méthodes nécessitant souvent de la formation et non adaptables à toutes les situations ;
- Dépendance vis-à-vis de la cartographie du SI : profondeur, étendue etc. ;
- Tendance à l'exhaustivité ;
- Accumulation de mesures techniques sans cohérence d'ensemble.

■ f. Classification des informations

- La classification selon la confidentialité des informations aide à définir des mesures de protection appropriées pour chaque type d'information.

	Intitulé	Explication	Exemple	Risque
C1	Accès libre	Tout le monde peut y accéder	Informations publiées sur le site internet	Aucun
C2	Accès à l'organisation	Seul le personnel de l'organisation est autorisé à accéder à l'information	Nom, adresse des partenaires et fournisseurs de l'organisation	Atteinte à l'image, gêne passagère
C3	Diffusion limitée	Au sein de l'organisation, seul un groupe de personnes est autorisé comme les membres du même projet	Plan technique d'un nouveau laboratoire ; Listes der personnes admissibles avant publication officielle...	Situation à risques ; pertes financières acceptables
C4	Confidentiel	L'information est accessible à une liste très restreinte d'utilisateurs à titre individuel	Contenu des brevets déposés ; Recherche en cours ; N° de sécurité sociale et noms...	Pertes financières inacceptables, poursuites judiciaires

- f. Classification des informations
- Sur la base des niveaux de confidentialité définis, les mesures suivantes peuvent être implémentées :
 - Une politique de gestion des informations est définie :
 - Création d'un modèle de document indiquant le niveau de confidentialité ;
 - Sensibilisation du personnel et des partenaires à cette politique.
 - Les informations de niveau « **Confidentiel** » doivent être :
 - envoyées par mail de manière chiffrée et le mot de passe communiqué par SMS aux destinataires ;
 - stockées localement dans des conteneurs chiffrés.
 - Les informations de niveau « **Diffusion limitée** » doivent être échangées au travers au travers d'un système documentaire collaboratif ayant des accès nominatifs contrôlés, par exemple MS SharePoint.

g. Gestion des ressources humaines

▪ Avant embauche :

- Sélection des candidats et interviews ;
- Vérification du CV (contacter les anciens employeurs, vérifier les diplômes, certifications...) du candidat ;
- En fonction de la sensibilité du poste, un extrait de casier judiciaire peut être demandé.

▪ Pendant l'embauche :

- Fourniture des accès logiques (création de comptes utilisateurs, accès aux répertoires nécessaires...) et physiques (badges) adaptés à la fonction ;
- Sensibilisation aux politiques et procédures internes de l'organisation ;
- Sensibilisation régulière à la sécurité adaptée aux fonctions ;
- Processus disciplinaire en cas de non respect.

▪ Au terme du contrat de travail :

- Retrait des accès et restitution du matériel fourni (badge, ordinateur, ...).

■ Conclusion

- Une politique de sécurité doit être adaptée à l'organisme et à ses évolutions ;
- la sécurité ne s'improvise pas et nécessite des professionnels ;
- les normes sont une aide pour mettre en œuvre une démarche d'amélioration continue de la sécurité ;
- les normes par nature ne délivrent pas un niveau de sécurité ;
- les normes ne prennent pas en compte toute la sécurité des systèmes d'information.

2. INTÉGRER LA SÉCURITÉ DANS LES PROJETS

- a) Préambule
- b) Sécurité dans l'ensemble du cycle de vie d'un projet
- c) Sécurité prise en compte en fin de développement
- d) Approche par l'analyse et le traitement du risque
- e) Plan d'action SSI

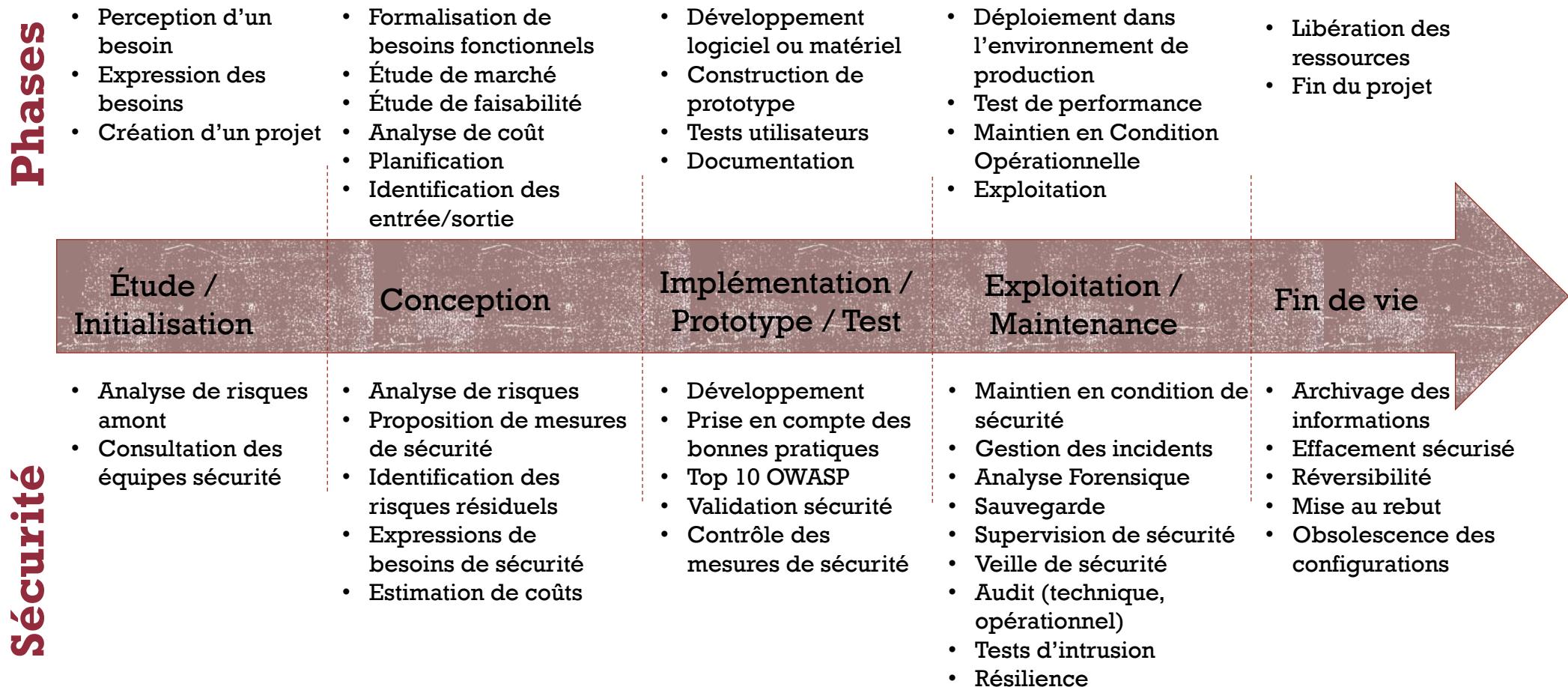
■ a. Préambule

- Il s'agit de bien distinguer :
 - **la sécurité du système d'information** qui est un des objets du projet ;
 - **et la sécurité du projet en lui-même** (diffusion et traitement des informations).
- Concernant la sécurité du SI en lui-même :
 - toute activité étant gérée en mode projet, une bonne intégration de la sécurité dans l'organisation nécessite l'intégration de la sécurité dans chaque projet dans le respect de la réglementation ;
 - isoler les traitements de données sensibles au sein de projet pour avoir une meilleure maîtrise des risques et des mesures de sécurité à mettre en œuvre pour réduire ces risques.

■ a. Préambule

- La sécurité doit être prise en compte dans **toutes les étapes** d'un projet :
 - Application de la démarche d'amélioration continue ;
 - Respect des impératifs et des contraintes notamment juridiques et réglementaires ;
 - Responsabilisation des acteurs, documentations, gestion du temps.

▪ b. Exemple d'intégration de la sécurité dans le cycle de vie d'un projet



▪ c. Sécurité prise en compte en fin de développement

- Exemple d'un projet de développement de site Web :
 - L'audit de sécurité fait le constat que :
 - Les versions de composants logiciels utilisés sont obsolètes et vulnérables ;
 - La base de données n'a pas été correctement isolée, et les tables ont été créées à l'intérieur d'une autre base de données à accès public ;
 - La politique de gestion de mots de passe n'est pas conforme aux bonnes pratiques : création de mots de passe faibles ; stockage de mots de passe en clair...
 - Le niveau de disponibilité attendu pour ce site ne peut être assurer avec l'infrastructure existante.
 - Conséquences :
 - Besoin de rachats de licences logicielles : coût supplémentaire ;
 - Recréation de la base de données sur un espace dédié correctement protégé ;
 - Redéveloppement des modules de gestion des mots de passe : coût supplémentaire ;
 - Modification de l'infrastructure pour assurer le niveau de disponibilité requis.

Délai, coût et effort supplémentaires...

▪ c. Sécurité prise en compte en fin de déploiement

- Exemple d'un projet de construction d'une nouvelle salle devant héberger les serveurs de l'organisation :
 - L'audit de sécurité fait le constat que :
 - Les baies de stockage des serveurs ne se ferment pas à clé ;
 - Pas de mécanisme de contrôle d'accès (lecteur de badge) prévu tracer les accès ;
 - Pas de redondance (alimentation, accès de télécommunications) des équipements ;
 - Aucune alarme anti-intrusion ou incendie n'est prévue ;
 - L'arrivée de câbles dans la salle est exposée à des actes de malveillances ;
 - La salle est construite en zone inondable.
 - Conséquences :
 - Rachat de matériel et d'équipements => coût supplémentaire ;
 - Re-câblage de la salle, et travaux de génie civil à prévoir ;
 - Relocation de la salle ou reconstruction => coût supplémentaire très importante.

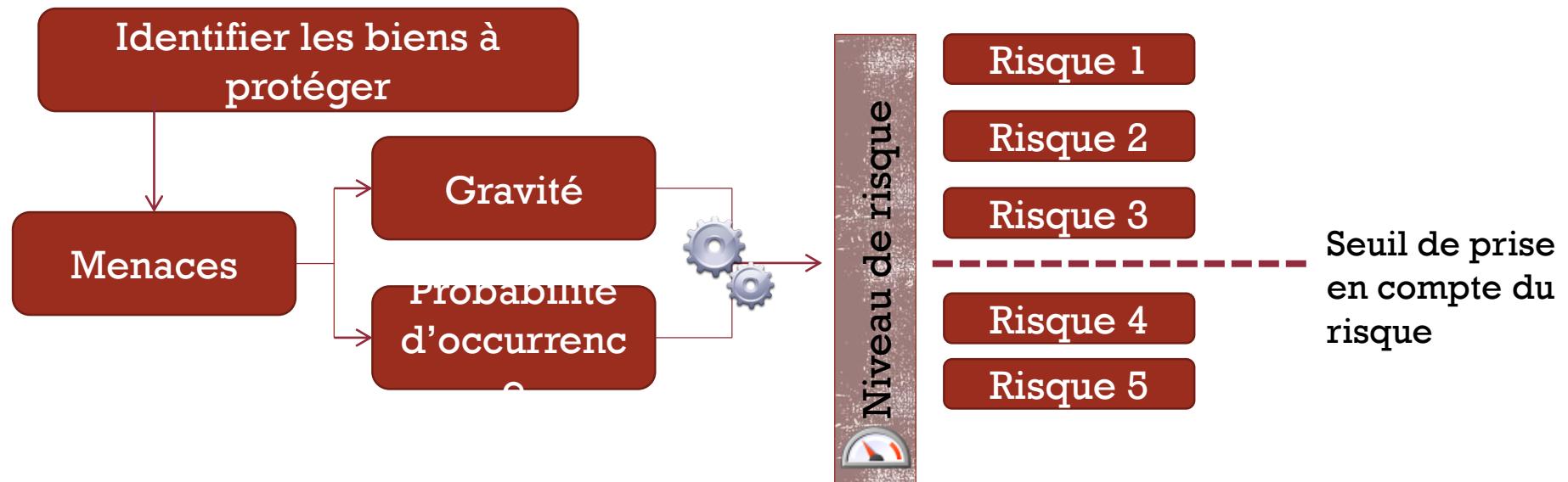
Reconstruction de la salle ou relocation de la salle, délai et coût supplémentaires...

■ d. L'approche par l'analyse et le traitement du risque

- L'analyse de risques doit être effectuée en amont du projet mais doit aussi évoluer au fur et à mesure de l'exploitation du système (analyse de risque dynamique dans la supervision du système (SOC)) et fonction de l'évolution des risques (évolution des vulnérabilités, des menaces, du système d'information).
- L'analyse de risque consiste à :
 - identifier les biens à protéger,
 - analyser de la fréquence et la gravité du danger pour évaluer la criticité du risque,
 - établir une hiérarchisation des risques : fréquence vs gravité,
 - établir un seuil d'acceptabilité pour chacun de ces risques,
 - seuil au-delà duquel le risque doit être pris en compte par les mesures de sécurité.
 - identifier des mesures de sécurité.
- Les mesures ainsi identifiées peuvent constituer un cahier de charges sécurité pour le projet qui soit réalisé en interne ou externalisé.

- d. L'approche par l'analyse et le traitement du risque

Une démarche d'analyse de risque peut être schématisée ci-dessous :

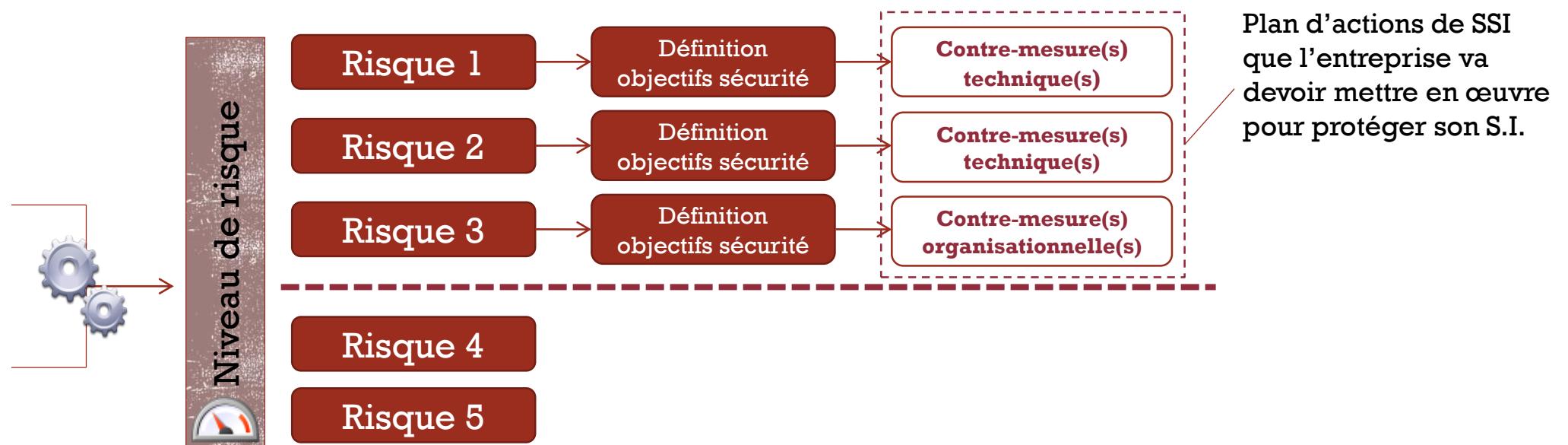


La hiérarchisation des risques permet de déterminer les risques qui :

- doivent absolument être traités et donc réduits par des mesures ;
- ceux qui sont acceptables et avec lesquels le système peut exister.

▪ d. L'approche par l'analyse et le traitement du risque

- Pour les risques dont le niveau est supérieur au seuil de prise en compte :
 - Définir les objectifs de sécurité ;
 - Définir les mesures techniques et organisationnelles qui vont permettre d'atteindre ces objectifs.
- Pour les risques dont le niveau est inférieur au seuil de prise en compte :
 - un **risque résiduel** est le risque subsistant après le traitement de risque (car – par exemple – le coût pour compenser ce risque est trop élevé par rapport au risque encouru).



- d. L'approche par l'analyse et le traitement du risque

Une analyse de risque peut être assez complexe et nécessite rigueur et méthode, il faut notamment trouver le bon niveau abstraction.

Voici 3 exemples de méthodes d'analyses de risque compatibles avec les lignes directrices de l'ISO 27005 :

- **E BIOS** : Expression des Besoins et Identification des Objectifs de Sécurité

développée par le Club E BIOS auquel participe l'ANSSI, l'Agence nationale de la sécurité des systèmes d'information

- **MEHARI** : MEthode Harmonisée d'Analyse de Risques

développée par le CLUSIF, Club de la Sécurité de l'Information Français

- **OCTAVE** : Operationally Critical Threat, Asset, and Vulnerability Evaluation

développée par l'Université de Carnegie Mellon.

e. Plan d'actions SSI

Le défi vis-à-vis de la mise en place des mesures de sécurité est **asymétrique** entre « attaquer » et « défendre » :

- L'attaque peut réussir par l'exploitation d'une seule vulnérabilité ;
- Tandis que la défense doit prendre en compte l'ensemble du système.

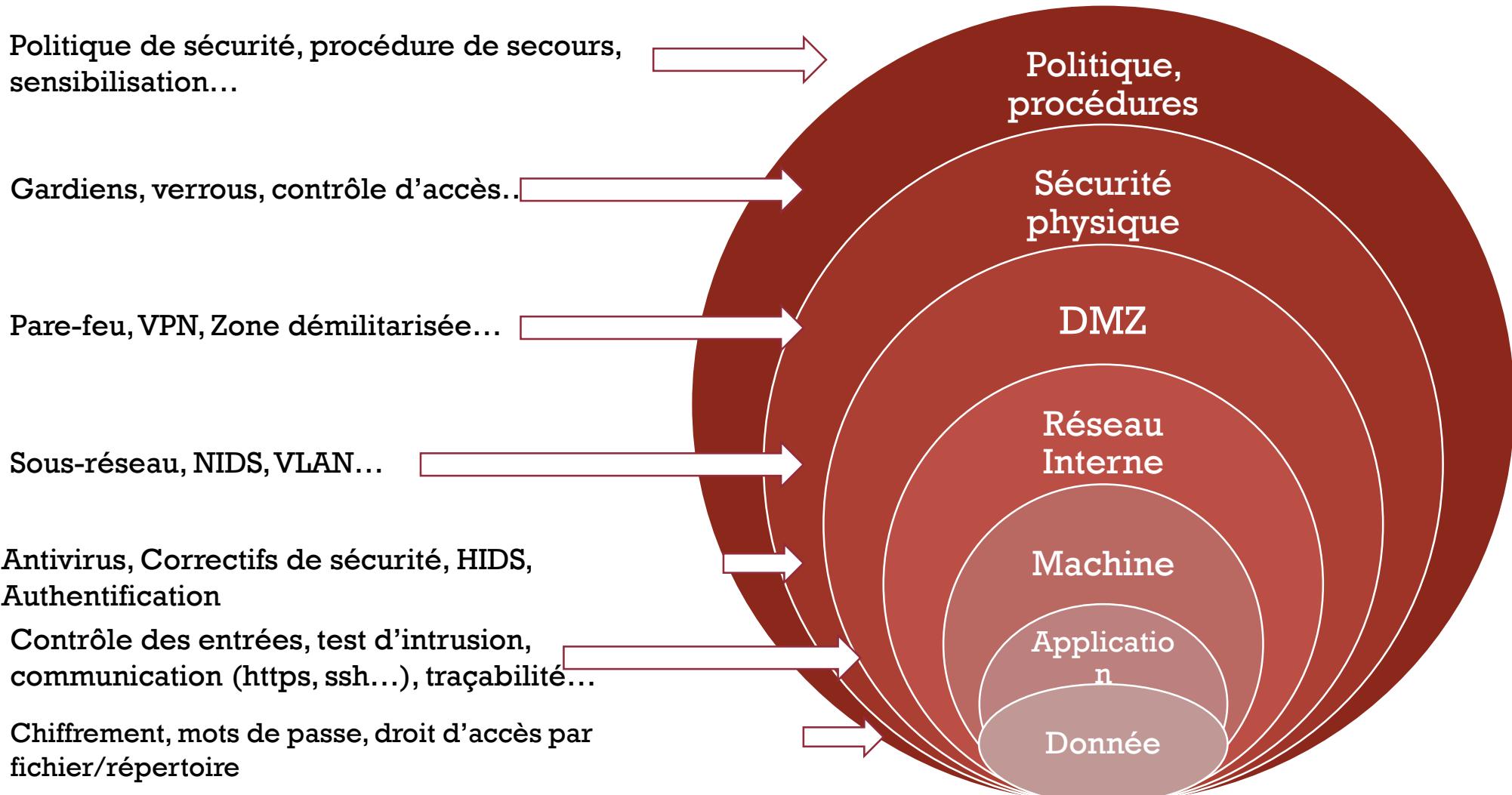
Un plan d'action des mesures de sécurité à mettre en place à l'issue de l'analyse de risques devrait respecter le principe de « **défense en profondeur** » qui recommande :

- d'avoir plusieurs lignes de défenses indépendantes ;
- que chaque ligne constitue une barrière autonome contre les attaques ;
- que la perte d'une ligne de défense implique qu'on passe à un niveau de défense plus fort.

Les objectifs de la défense en profondeur sont :

- prévenir, bloquer, limiter, détecter, alerter, réagir, réparer.

■ e. Plan d'actions SSI



▪ Conclusion

- La sécurité des systèmes d'information : un élément indispensable d'un projet ;
- une sécurité globale et cohérente, et non une accumulation de mesures et de produits de sécurité ;
- une politique de sécurité réaliste et pragmatique ;
- un élément clé : la connaissance du système d'information (cartographie) et de son niveau de sécurité (contrôle, audit) ;
- une difficulté et une nécessité : le maintien en condition de sécurité du système d'information ;
- un accroissement des besoins de sécurité : besoin en compétences et en professionnels.

3. DIFFICULTÉS LIÉES À LA PRISE EN COMPTE DE LA SÉCURITÉ

- a) Compréhension insuffisante des enjeux
- b) Implication nécessaire de la direction
- c) Difficulté pour faire des choix en toute confiance
- d) Délicat arbitrage entre commodité et sécurité
- e) Suivre l'évolution des technologies
- f) Frontières floues entre sphères professionnelle, publique, et privée

3. DIFFICULTÉS LIÉES À LA PRISE EN COMPTE DE LA SÉCURITÉ

- a. Une compréhension insuffisante des enjeux...

...liée à un problème d'éducation

- L'information a une valeur importante pour l'entreprise, pour les concurrents, pour les États. On parle aujourd'hui de « guerre de l'information ».
 - Chaque année des centaines de compagnies en France sont victimes d'espionnage industriel ou économique :
 - Écoute des conversations ;
 - Espionnage des écrans d'ordinateurs ;
 - Social engineering, etc.
 - Des actes aisés dans les transports : train, avion, etc.



Les voyageurs aux USA perdent environ
12 000 pc portables chaque semaine*

*source : Ponemon Institute

3. DIFFICULTÉS LIÉES À LA PRISE EN COMPTE DE LA SÉCURITÉ

- a. Une compréhension insuffisante des enjeux

...liée à un problème de formation

- Des dirigeants qui n'ont pas tous une culture sécurité ;
- Des évolutions vers le poste de « RSSI », sans formation complémentaire adéquate :
 - personnel issu de la technique : administrateur réseau, système...
 - personnel issu de la qualité : responsable qualité... ;
- Un coût lié à la sécurité qui rebute en période de crise :
 - Authentification forte : achats de jetons/carte à puce ;
 - Plan de secours : acheter en double certains équipements ;
 - Personnel : former aux bonnes pratiques en sécurité...

3. DIFFICULTÉS LIÉES À LA PRISE EN COMPTE DE LA SÉCURITÉ

- a. Une compréhension insuffisante des enjeux...

...entraînant de nombreux risques pour l'entreprise ou pour l'organisation

- Perte d'informations essentielles ;
- Arrêt de la production ;
- Détérioration de l'image/réputation ;
- Risques juridiques/réglementaires...

...entraînant de nombreux risques pour les États

- Indisponibilité de services ;
- Perte de crédibilité ;
- Divulgation d'informations sensibles ;
- Risques de conflits avec d'autres États...

3. DIFFICULTÉS LIÉES À LA PRISE EN COMPTE DE LA SÉCURITÉ

- b. L'implication nécessaire de la direction

Rien ne peut se faire sans l'aval de l'exécutif.

Le chef d'entreprise doit être conscient des enjeux de sécurité pour l'avenir de son entreprise :

- Être **proactif** plutôt que réactif. La PSSI est une réflexion stratégique : Elle permet de prévoir l'avenir de l'organisation ;
- **Prendre le temps** de comprendre, ne pas être absorbé que par ses marchés, ses clients, ses concurrents, son relationnel ;
- La sécurité :
 - **va au-delà de la technique**. L'humain joue un rôle central ;
 - **ne doit pas rester un domaine d'experts**. La sécurité est l'affaire de tous et une préoccupation de tous les responsables ;
 - n'est pas seulement une contrainte coûteuse mais **elle est aussi un investissement**, un atout supplémentaire pour l'organisation.

3. DIFFICULTÉS LIÉES À LA PRISE EN COMPTE DE LA SÉCURITÉ

- b. L'implication nécessaire de la direction

Investir dans la sécurité ne suffit pas. Il faut être conscient des enjeux vis-à-vis de l'organisation. La dynamique sécurité viendra de la direction.

- Le dirigeant doit **montrer l'exemple** d'abord en y accordant un intérêt : charismatique, il est le premier à sensibiliser les personnes concernées ;
- **Motiver** son RSSI ou ses administrateurs pour faire appliquer la politique de sécurité de l'organisation et maîtriser leurs systèmes le mieux possible ;
- **Responsabiliser** : en désignant un responsable de la coordination, qui distribuera les tâches au sein des équipes ;
- **Réagir** en cas d'attaque avérée : mettre des ressources à disposition, permettre l'expertise juridique et porter plainte ;
- **Impliquer** ses personnels, les sensibiliser et leur permettre de suivre des formations.

3. DIFFICULTÉS LIÉES À LA PRISE EN COMPTE DE LA SÉCURITÉ

- c. Difficulté pour faire des choix en toute confiance

Il est important de faire des choix éclairés en prenant en compte la sécurité.

"L'implantation en France des chinois Huawei et ZTE pose une question de sécurité nationale"



Par **JM Bockel** (Express Yourself) publié le 01/10/2012 à 15:12, mis à jour à 15:25



Vie privée : La NSA s'octroie un backdoor dans tous les systèmes Windows



Le Gouvernement Chinois a adopté une nouvelle régulation exigeant aux entreprises qui vendent des ordinateurs aux banques chinoises de fournir le code source et de se soumettre à des audits.

3. DIFFICULTÉS LIÉES À LA PRISE EN COMPTE DE LA SÉCURITÉ

- c. Difficulté pour faire des choix en toute confiance

Quels sont aujourd’hui les matériels ou logiciels de confiance ?

- Ceux issus de l’industrie nationale vs ceux de nos partenaires de confiance : alliés, fournisseurs ;
- Ceux issus du monde libre (« open source ») ;
- Les matériels qualifiés par l’ANSSI.

Quels sont les organismes de confiance ?

- Les entreprises nationales ou européennes (mais qui sont les actionnaires) ;
- Nos partenaires de longue date ;
- Les autorités gouvernementales ;
- Les prestataires de service qualifiés par l’ANSSI.

3. DIFFICULTÉS LIÉES À LA PRISE EN COMPTE DE LA SÉCURITÉ

- d. Le délicat équilibre entre productivité et sécurité : contexte
- Authentification requise pour chaque application dans l'entreprise
 - Problème pour l'utilisateur : « J'ai besoin de travailler chaque jour avec 5 applications et je dois à chaque fois y saisir un mot de passe différent ».
 - Réaction pour l'utilisateur : « Je note certains mots de passe sur papier ».
- Utiliser une application de chiffrement pour partager les fichiers chiffrés avec des partenaires
 - Problème pour l'utilisateur : l'interface de Crypt&Share n'est pas ergonomique.
 - Réaction de l'utilisateur : « Je vais utiliser Box ou DropBox pour partager les informations avec mes partenaires ».
- Les informations classifiées au niveau 4 (niveau de sensibilité le plus élevé) ne doivent pas sortir du S.I.
 - Problème pour l'utilisateur : J'ai besoin de l'avis d'un prestataire extérieur sur certaines informations de niveau 4.
 - Réaction de l'utilisateur : Déclassification des informations de manière à ne jamais avoir de niveau 4 mais uniquement des niveaux 3 ou 2.

3. DIFFICULTÉS LIÉES À LA PRISE EN COMPTE DE LA SÉCURITÉ

- d. Le délicat équilibre entre productivité et sécurité
- Les usages fondent les pratiques... entre ce qui est acceptable à l'utilisateur, ce qui est nécessaire au bon fonctionnement de l'organisme et ses besoins de sécurité.

D'où l'importance :

- De la **pédagogie** : expliquer à quoi servent les procédures, leurs bienfondés, leur intérêt pour l'organisation ;
- De **l'implication des dirigeants** : qui viendront renforcer ces convictions ;
- De la **prise en compte des remarques et éventuelles oppositions des utilisateurs** : ergonomie, pratique, simplicité de mise en œuvre etc. ;
- La mise en place d'une **charte informatique** signée et connue de tous ;
- De **régulièrement rappeler les règles** : changer les mots de passe, rejouer les procédures, créer une check-list etc. ;
- De sensibiliser en évoquant les incidents réels qui se produisent et peuvent se produire dans l'organisation.

3. DIFFICULTÉS LIÉES À LA PRISE EN COMPTE DE LA SÉCURITÉ

- d. Le délicat équilibre entre productivité et sécurité
- **Écouter les utilisateurs** et prendre en compte leurs besoins lors de l'étude de solutions de sécurité :
 - Proposer des mesures en concertation et avec l'adhésion des utilisateurs concernés autant que possible ;
 - **Former les utilisateurs** pour les aider à prendre en main les nouveaux outils et à bien appliquer les mesures.
- **Tester les procédures**, dans le but d'évaluer son efficacité (applicabilité, réalisation des objectifs, risques encourus) :
 - Éviter de multiplier les moyens de protection si ceux-ci ne sont pas respectés ;
 - il faut parfois investir moins dans la sécurité mais avoir des procédures efficaces.
- **Confier la responsabilité de la sécurité à un collaborateur** qui a le pouvoir ou les ressources pour la faire appliquer.
- Choisir les solutions les plus adaptées à **sa propre structure**, à **son** fonctionnement, au niveau de maturité l'entreprise.

3. DIFFICULTÉS LIÉES À LA PRISE EN COMPTE DE LA SÉCURITÉ

- e. Suivre l'évolution des technologies : le Cloud
 - Les technologies Cloud se popularisent de plus en plus au sein des entreprises. Les raisons évoquées sont diverses et peuvent être :
 - Réduction des coûts
 - Meilleure accessibilité
 - gestion confiée à un tiers
 - Mais les mesures de sécurité et réglementaires constituent toutefois des « freins ».
- Le **SaaS** (Software as a Service) est l'usage du Cloud le plus rencontré en entreprise :
 - SaaS est la fourniture d'applications sous forme de service à la carte. L'application est installée dans le Cloud (Datacenter) et l'utilisateur paye une licence d'utilisation.
- Les utilisateurs finaux souscrivent aujourd'hui à des services SaaS sans l'aval de la direction informatique et en dépit des règles de sécurité. Ils accèdent au SaaS à travers divers terminaux souvent non contrôlés par l'entreprise. On parle alors de « **Shadow IT** » :
 - Dans une entreprise du CAC, le DSI estimait à près de 100 le nombre total d'applications. Un audit de découverte du Cloud a révélé près de 2500 usages SaaS.

3. DIFFICULTÉS LIÉES À LA PRISE EN COMPTE DE LA SÉCURITÉ

▪ e. Suivre l'évolution des technologies : le Cloud

Le recours à des services type Cloud pose de nouvelles problématiques que l'entreprise se doit de résoudre, notamment :

- Le choix d'un fournisseur
 - Est-ce que le fournisseur dispose de certification relatives à l'hébergement (Exemple : SAS 70 II)?
 - Est-ce que le fournisseur est agréé par une autorité nationale?
- Le stockage
 - A qui appartiennent **léggalement** les données lorsqu'elles sont hébergées ?
 - Quelles sont les mesures de protection des données stockées?
 - Les systèmes sont-ils mutualisés avec d'autres clients ou nous sont-ils dédiés ?
 - Qui doit fournir les clés cryptographiques ?
 - Comment les données sont-elles sauvegardées, redondées ?
- Le transport des données
 - Qui fournit l'infrastructure de transport?
 - quels sont les mécanismes de sécurité en place?
- Fin de contrat : réversibilité
 - Que deviennent les données lorsque le contrat expire ? Comment sont-elles restituées au client, supprimées du Cloud et qu'advient-il des données sauvegardées sur bande ?

3. DIFFICULTÉS LIÉES À LA PRISE EN COMPTE DE LA SÉCURITÉ

- e. Suivre l'évolution des technologies : le Cloud
- Les guides suivants peuvent être utiles pour choisir un fournisseur SAAS :
 - Guide Contractuel SAAS : <http://www.syntec-numerique.fr/content/publication-du-guide-contractuel-saas>
 - Recommandations CNIL pour la souscription au SAAS : <http://www.cnil.fr/linstitution/actualite/article/article/cloud-computing-les-conseils-de-la-cnil-pour-les-entreprises-qui-utilisent-ces-nouveaux-services/>
 - Guide de l'ANSSI : « Sécurité de l'externalisation » : <http://www.ssi.gouv.fr/entreprise/bonnes-pratiques/externalisation/>
- Les Cloud Access Security Brokers (CASB) ou les Cloud Security Gateway (CSG) sont des composants logiciels ou matériels qui se situent entre les utilisateurs et le fournisseur SaaS et permettent :
 - de protéger les données des utilisateurs de l'entreprise de manière à ce que l'éditeur SaaS ne puisse les lire ;
 - de gérer les accès et de l'authentification unique (SSO) ;
 - de conserver les données en local via de la tokenisation ou de les chiffrer avant de les envoyer vers le fournisseurs SaaS...

3. DIFFICULTÉS LIÉES À LA PRISE EN COMPTE DE LA SÉCURITÉ

- e. Suivre l'évolution des technologies : le Cloud
- Le Cloud pourrait à terme rendre les autres moyens de sauvegarde désuets :
 - sauvegarder une copie de son S.I. au sein du Cloud permettra à l'organisation de redémarrer une activité saine à tout moment en cas d'incident ;
 - A partir d'une sauvegarde, un espace de travail peut être accessible de n'importe quel endroit du monde pour tous ceux qui y sont autorisés.
- La fédération d'identité est un usage du Cloud qui peut permettre aux entreprises de mieux gérer les identités de ses utilisateurs et de :
 - centraliser les comptes utilisateurs ;
 - d'octroyer et de retirer facilement les droits d'accès sur plusieurs applications en interne ou en externe ;
 - tracer les utilisateurs et leurs actions...

3. DIFFICULTÉS LIÉES À LA PRISE EN COMPTE DE LA SÉCURITÉ

- e. Suivre l'évolution des technologies : le Big Data
- « Big Data » recouvre l'exploitation des données massives impossibles à manipuler avec les outils classiques comme les bases de données.
- Le « Big Data » comme outil de sécurité :
 - Modélisation des comportements et détection des anomalies sur la base de corrélation des données issues du trafic réseau ;
 - Détection possible des attaques persistantes avancées (APT) ;
 - Meilleure efficacité des outils tels que des SIEM, IDS, ou IPS ;
 - Surveillance du trafic réseau pour identifier des botnets.
- Le « Big Data » représente un enjeu pour la sécurité des S.I. :
 - La source de données doit être fiable, et intègre (comme dans toute collecte d'information) ;
 - L'anonymisation des données manipulées représente une véritable difficulté compte tenu de leur volume important ;
 - La localisation des données car le « big data » est souvent exploité dans le « cloud » et les réglementations applicables ;
 - La protection de données exploitées est importante et le chiffrement peut être difficile à assurer. Un vol de données aura une ampleur beaucoup plus importante.

3. DIFFICULTÉS LIÉES À LA PRISE EN COMPTE DE LA SÉCURITÉ

■ f. Des frontières floues entre sphères professionnelle, publique, et privée

Quel est le périmètre de confiance?

- Internet est un réseau mondial ouvert ; dans un monde concurrentiel, il est naturel qu'il soit **source de menaces** ;
- Les réseaux d'entreprises sont des **réseaux internes**, généralement protégés de façon périphérique, mais peu protégés en interne...
- Les multinationales possèdent souvent de **grands réseaux ouverts à des exploitants**, des services de télémaintenance et des sous-traitants qui ont des accès conséquents sur ces réseaux, et qui possèdent eux-mêmes leurs propres informations ;
- De plus, de nombreux « nouveaux » **appareils sont utilisés** (smartphones, tablettes etc.) faiblement sécurisés et connectés directement à Internet (Wifi, 3G/4G, etc.) sans passer par les dispositifs de sécurité de l'entreprise ;
- Les données personnelles peuvent ainsi être présentes sur le réseau d'entreprise.

3. DIFFICULTÉS LIÉES À LA PRISE EN COMPTE DE LA SÉCURITÉ

- f. Des frontières floues entre sphères professionnelle, publique, et privée

BYOD - Focus sur le smartphone personnel (ou la tablette personnelle) :

- Il nous accompagne au travail, lors de nos déplacements ;
 - On le connecte à notre PC de bureau pour le recharger en USB ;
 - Il remplace souvent notre téléphone professionnel, peut-être moins performant ou restreint en terme de fonctionnalités ;
 - Pour des raisons de facilité, on y configure notre messagerie professionnelle, nos contacts, notre emploi du temps... autant d'informations qui peuvent potentiellement être sensibles pour l'entreprise.
-
- La frontière entre nos informations privées et nos informations professionnelles devient donc **très floue** ;
 - Dès que les informations sont stockées sur un smartphone personnel, l'entreprise en perd la maîtrise (l'équipement ne lui appartient pas, elle ne peut pas imposer ses règles...).

3. DIFFICULTÉS LIÉES À LA PRISE EN COMPTE DE LA SÉCURITÉ

- f. Des frontières floues entre sphères professionnelle, publique, et privée

Raconter, partager sa vie privée sur l'Internet c'est y être pour la postérité...

- **Nos données nous échappent dès l'instant où nous les publions** : Dans le meilleur des cas, on pourra effacer notre propre publication, mais on ne pourra pas effacer les multiples copies que l'on ne contrôle pas (droit à l'oubli illusoire par manque de maîtrise de l'information) ;
- C'est permettre à tout inconnu, **d'entrer dans notre sphère privée** ; la restriction des accès aux « amis » n'est qu'illusoire dans l'absolu ;
- c'est permettre aux Ressources Humaines de **filtrer notre CV** ; et déterminer le profil privé du candidat correspondant au profil professionnel recherché ;
- à nos collègues et supérieurs **d'interpréter nos propos...**

3. DIFFICULTÉS LIÉES À LA PRISE EN COMPTE DE LA SÉCURITÉ

- f. Des frontières floues entre sphères professionnelle, publique, et privée

Partager les problèmes que l'on rencontre au travail : personnels, techniques, relationnels ; consulter des sites personnels au travail...

- c'est peut-être mettre en danger son organisation : en offrant à un pirate ou un concurrent des informations précieuses (version d'un logiciel, faille de sécurité, fournisseurs, secrets commerciaux, informations RH...) ;
- transgresser la **déontologie** du travail, ou la **charte de confidentialité** ;
- potentiellement s'exposer à des sanctions en interne qui peuvent aller jusqu'au pénal.

3. DIFFICULTÉS LIÉES À LA PRISE EN COMPTE DE LA SÉCURITÉ

▪ Conclusion

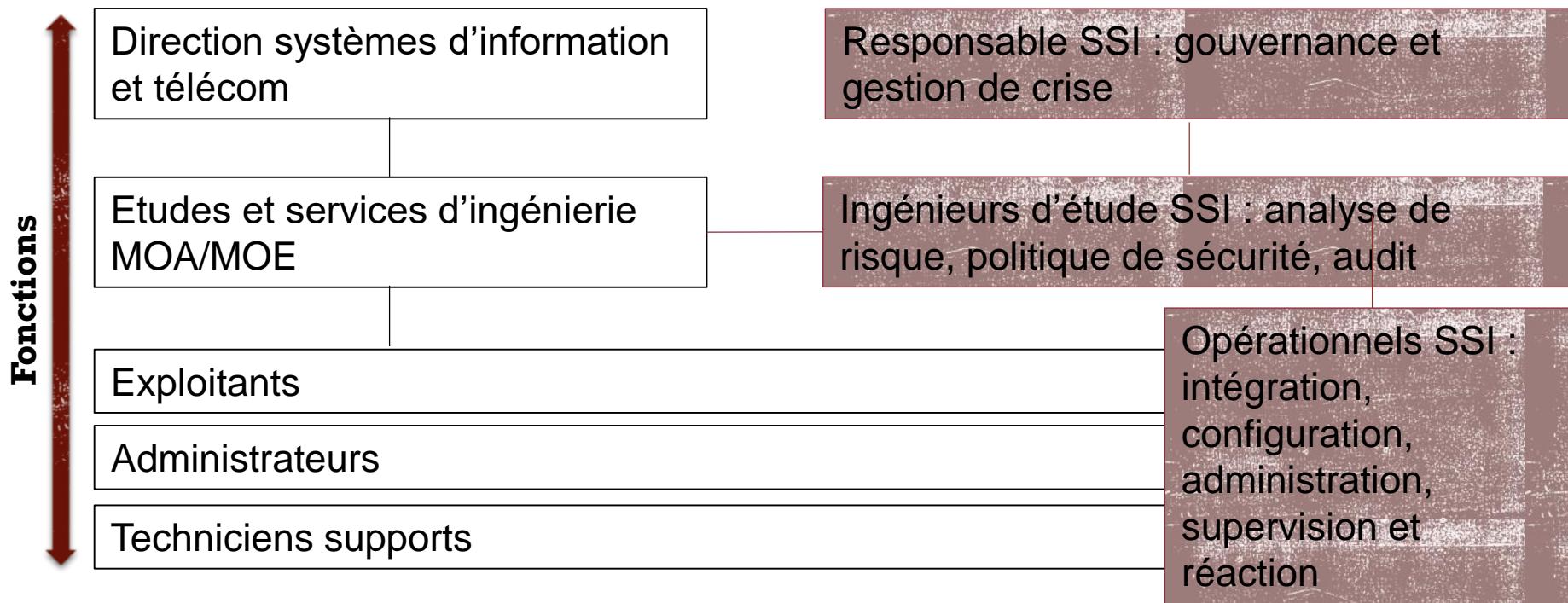
- Évolution des modes, des besoins, des technologies, des habitudes ;
- au-delà des nouveautés, toujours le même problème : la non-prise en compte de la sécurité (développement, implémentation, exploitation, formation) ;
- un périmètre d'attaque et d'accident plus étendu mais peu nouveau ;
- une prise en compte permanente des enjeux et de la sécurité par tous (hygiène informatique) et par le chef d'entreprise ;
- un accroissement des besoins de sécurité : besoin en compétences et en professionnels.

4. LES MÉTIERS EN CYBERSÉCURITÉ

- a) Positionnement des métiers au sein des organisations
- b) Cartographie des métiers et compétence
- c) Profils et carrières
- d) Perspectives d'embauche

▪ a. Positionnement des métiers au sein des organisations

La cybersécurité est transverse à toute activité qui requiert de l'informatique et des réseaux de télécommunications, de la TPE à la multinationale, dans le domaine privé ou public.



▪ a. Positionnement des métiers au sein des organisations

Selon la taille de l'organisation (PME/PMI/Grande entreprise...), les fonctions liées à la cybersécurité nécessitent une charge de travail qui varie. Il est possible d'avoir du personnel à temps partiel ou du personnel dédié à la sécurité.

Et cela sur l'ensemble des couches depuis la gouvernance jusqu'à l'opérationnel : par exemple.

ETP = Équivalent Temps Plein

DSI = Direction des Systèmes d'Information

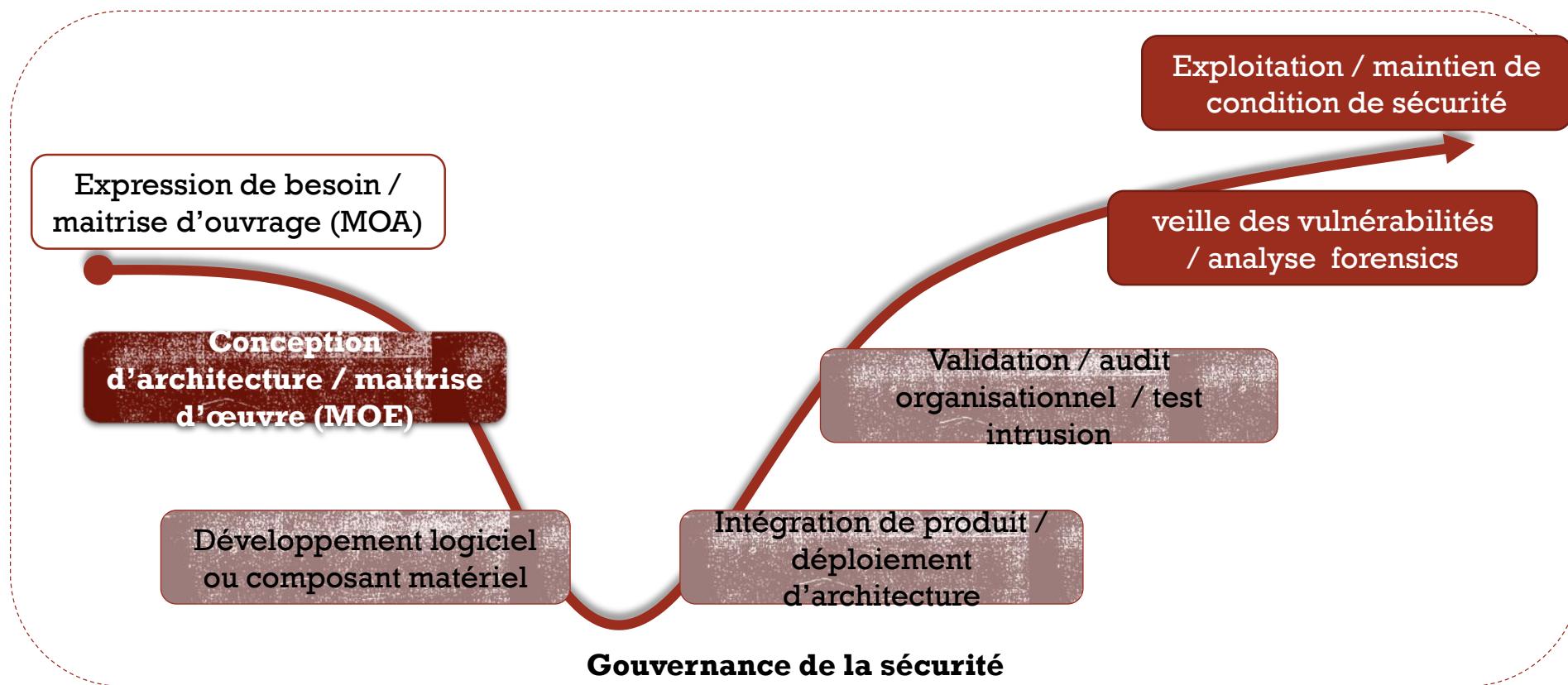
SSI = Sécurité des Systèmes d'Information

PSSI = Politique de Sécurité des Systèmes d'Information

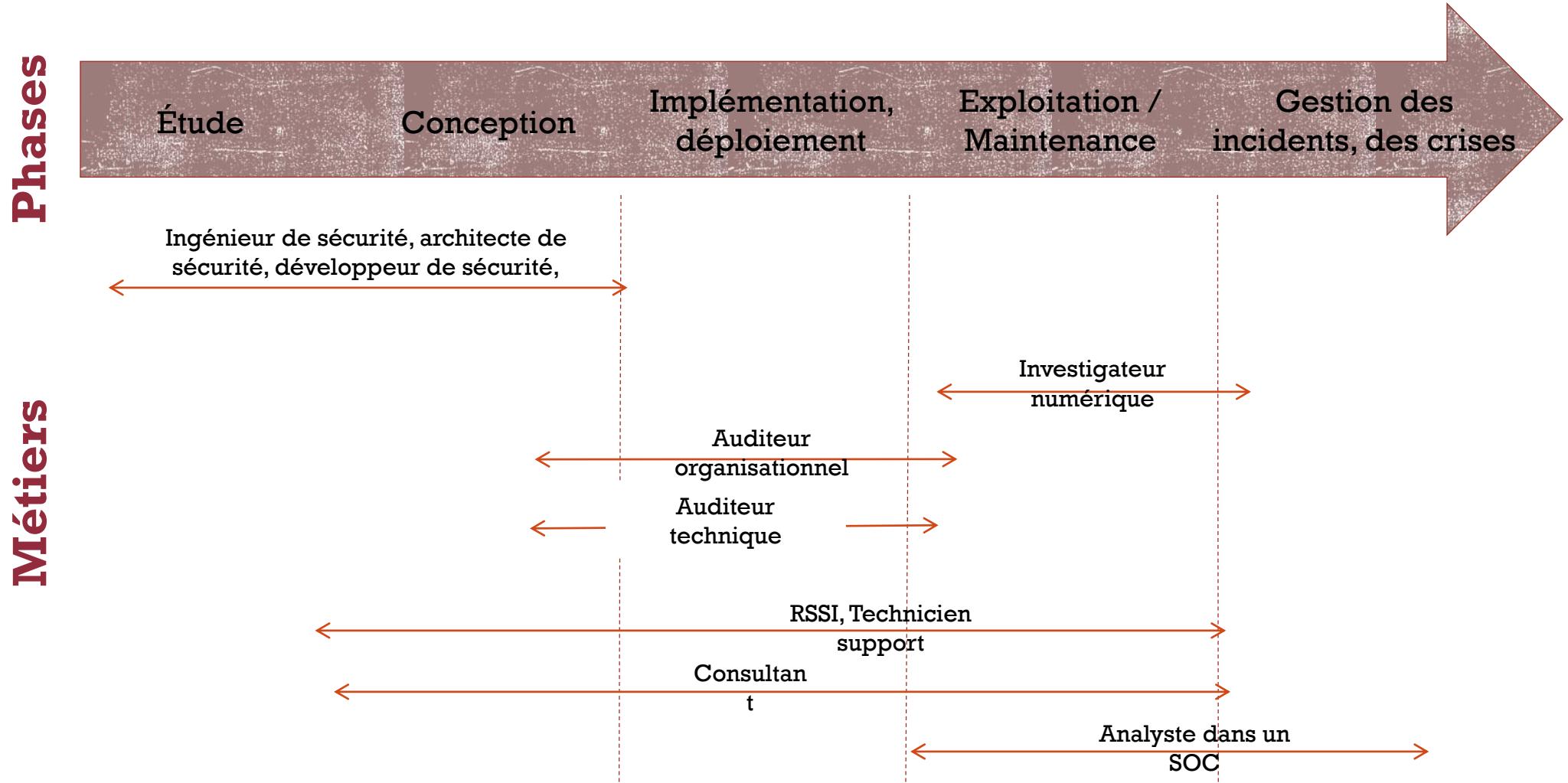
	PME/PMI DSI 15 pers	Grande entreprise DSI 500 pers
Responsable SSI : gouvernance et gestion de crise	$\frac{1}{4}$ ETP du Dir. du S.I.	3 à 5 ETP
Ingénieurs d'étude SSI : analyse de risque, mise en œuvre PSSI, audit...	$\frac{1}{4}$ ETP des études S.I.	5 à 10 ETP
Opérationnels SSI : intégration, configuration, administration, supervision et réaction	1 ETP réparti sur l'exploitation du S.I.	20 à 50 ETP si H24 7/7

■ b. Cartographie des métiers et compétence en SSI

Les métiers se répartissent dans le cycle de vie d'un projet depuis l'expression de besoin jusqu'au retrait de l'exploitation sous la responsabilité de la gouvernance globale de l'organisation.



▪ b. Cartographie des métiers et compétence en SSI



▪ b. Cartographie des métiers et compétence en SSI

Les métiers se répartissent dans les familles de l'informatique et des réseaux.

	Nb année expérience	Compétence technique	Compétence management
Gouvernance des systèmes d'information			
•Responsable ou Directeur	15 à 20	X	XXX
•Chef de projet / Consultant MOA	5 à 15	XX	XX
Conception et déploiement de système d'information			
•Chef de projet / Consultant MOE	5 à 15	XX	XX
•Architecte système	10 à 15	XXX	
Développement logiciel et matériel			
•Architecte/concepteur logiciel/composant	5 à 10	XXX	
•Développeur logiciel (dont cryptologue)	0 à 10	XXX	
Exploitation			
•Technicien système et réseau	0 à 10	XXX	
•Administrateur système et réseau	0 à 10	XXX	X
•Analyste veille/gestion des incidents/forensics	0 à 10	XXX	X
Validation / Audit			
•Auditeur technique SSI (dont test intrusion)	0 à 10	XXX	X
•Auditeur organisationnel SSI	5 à 10	X	X

Compétence requise :
X : peu de compétence
XX : niveau moyen
XXX : forte compétence

4. LES MÉTIERS

■ c. Profils et carrières

- **Responsable de la Sécurité des Systèmes d'Information** (RSSI) : définit la politique de sécurité du SI et veille à son application ; il assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte.
- **Architecte [système, logiciel] sécurité** : l'architecte sécurité structure les choix techniques, technologiques et méthodologiques d'un ensemble [système, logiciel] répondant à des exigences de sécurité.
- **Développeur [produit, logiciel] de sécurité** : le développeur de sécurité assure le sous-ensemble des activités d'ingénierie nécessaires à la réalisation d'éléments [produit, logiciels] répondant à des exigences de sécurité.

4. LES MÉTIERS

■ c. Profils et carrières

- **Technicien ou Administrateur système et réseau :** assure ou est responsable de diverses activités de support, de gestion ou d'administration de la sécurité aux plans techniques ou organisationnel.
- **Analyste :** assure la veille sur les vulnérabilités des produits et logiciel, , recherche et détecte les incidents de sécurité coordonne le suivi de l'application des correctifs.
- **Auditeur Organisationnel :** contrôle la prise en compte de la sécurité au niveau organisationnel sur la gouvernance, les procédures de sécurité notamment vis-à-vis de la norme ISO27K. Il vérifie la conformité des mesures mises en œuvre.
- **Auditeur Technique :** contrôle les configurations des équipements et logiciels. Il est en mesure de pénétrer les défenses d'un système d'information et d'identifier les divers chemins d'intrusions possibles et leurs conséquences. Il vérifie l'efficacité des mesures en place pour protéger le système.

■ c. Profils et carrières

La majeure partie des postes SSI sont occupés actuellement par des personnes ayant une formation informatique ou télécom, s'étant spécialisées au cours de leur carrière par des formations / certifications.

Certaines certifications en SSI peuvent être effectuées en 5 jours et se terminer par un examen comme par exemple :

- ISO 27001 Lead Auditor
- ISO 27001 Lead Implementor
- ISO 27005 Risk Manager
- CISSP : Certified Information System Security Professional
- CEH : Certified Ethical Hacker

On note depuis une dizaine d'années, un accroissement des formations spécialisées en sécurité de niveau bac+4/5. Elles permettent généralement de démarrer une carrière sur des postes qui requièrent des compétences techniques.

Possibilité de progression de carrière depuis la production technique jusqu'à de la direction/management en passant par de la vente ou du marketing de produits/services.

} Compétence Technique : X
Compétence Management : XXX

} Compétence Technique : XXX
Compétence Management : X

} Compétence Technique : XX
Compétence Management : XXX

4. LES MÉTIERS

- d. Perspectives d'embauche
- Métiers avec une forte demande annoncée pour les 15 prochaines années :
 - progression de la virtualisation de IT et des réseaux,
 - révolution digitale des services aux usagers (BToC) et entre entreprise (BtoB),
 - Internet des objets...
- Dans tous les secteurs privés banque, industrie, commerce...
- Ainsi que dans le secteur public : administration, collectivité territoriale, hôpitaux, universités...
- Mais surtout au sein de sociétés de service, principaux employeurs de diplômés depuis 20 ans pour intervenir en sous-traitance ou assistance technique pour les entreprises et les administrations :
 - les organisations tendent à se concentrer sur leur métier et faire de la délégation de service pour les fonctions supports dont la sécurité.

4. LES MÉTIERS

▪ d. Perspectives d'embauche

- Exemples d'organisations spécialisées dans la cybersécurité et qui recrutent :
 - Éditeurs/Constructeurs de produit de sécurité (anti-virus, boitier de chiffrement, pare-feu, ICG...) : développement, marketing et vente ;
 - Tiers de confiance qui exploite des infrastructures pour des clients (produits/services de sécurité en mode IaaS, SaaS) : conception et déploiement, exploitation, marketing et vente ;
 - Sociétés de service/cabinet de conseil : conseil, expertise, audit... ;
 - Organismes étatiques comme l'ANSSI, ministère de la défense (DGSE, Armées), ministère de l'intérieur (DGSI, police judiciaire, gendarmerie nationale), la CNIL : conseil, expertise, audit... ;
 - Entreprises proposant ou gérant des SOC.

MERCI DE VOTRE ATTENTION