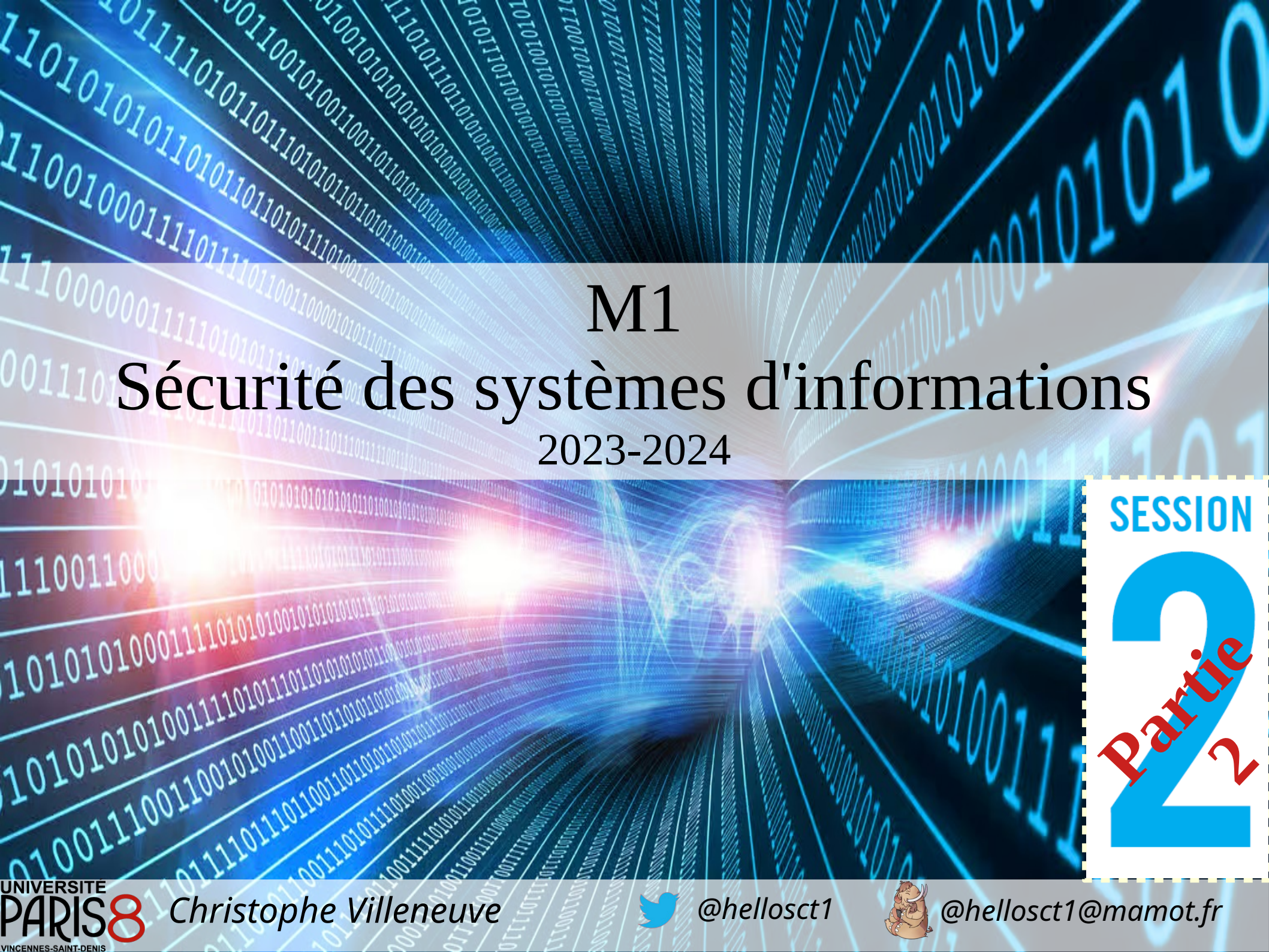


M1
Sécurité des systèmes d'informations
2023-2024

SESSION 2
Partie 2

UNIVERSITE PARIS 8 VINCENNES-SAINT-DENIS
Christophe Villeneuve
@hellosct1
@hellosct1@mamot.fr

Aujourd’hui : Session 2 : Notions de base

- Les détections des vulnérabilités
- Correction TP 1
  - Formulaire d’identification sécurisé
- Les enjeux de la sécurité des S.I.
- Besoin de sécurité : Preuve
- Les notions des vulnérabilités
- Les règles en France
- ...

- Détections vulnérabilités
- Correction TP 1
- Les enjeux de la sécurité
- Besoins de sécurité
- Notions des vulnérabilités
- Panorama des menaces
- Les règles en France

Introduction aux critères DIC (1/3)

- Se poser les bonnes questions

Comment définir le niveau de sécurité d'un bien du S.I. ?

Comment évaluer si ce bien est correctement sécurisé ?

Introduction aux critères DIC (2/3)

- 3 critères pour répondre à cette problématique

Disponibilité

Propriété d'**accessibilité au moment voulu** des biens par les personnes autorisées
→ le bien doit être disponible durant les plages d'utilisation prévues

Intégrité

Propriété d'**exactitude et de complétude** des biens et informations
→ une modification illégitime d'un bien doit pouvoir être détectée et corrigée

Confidentialité

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

Introduction aux critères DIC (2/4)

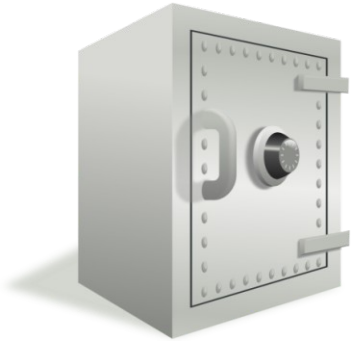
- 1 critère complémentaire

Preuve

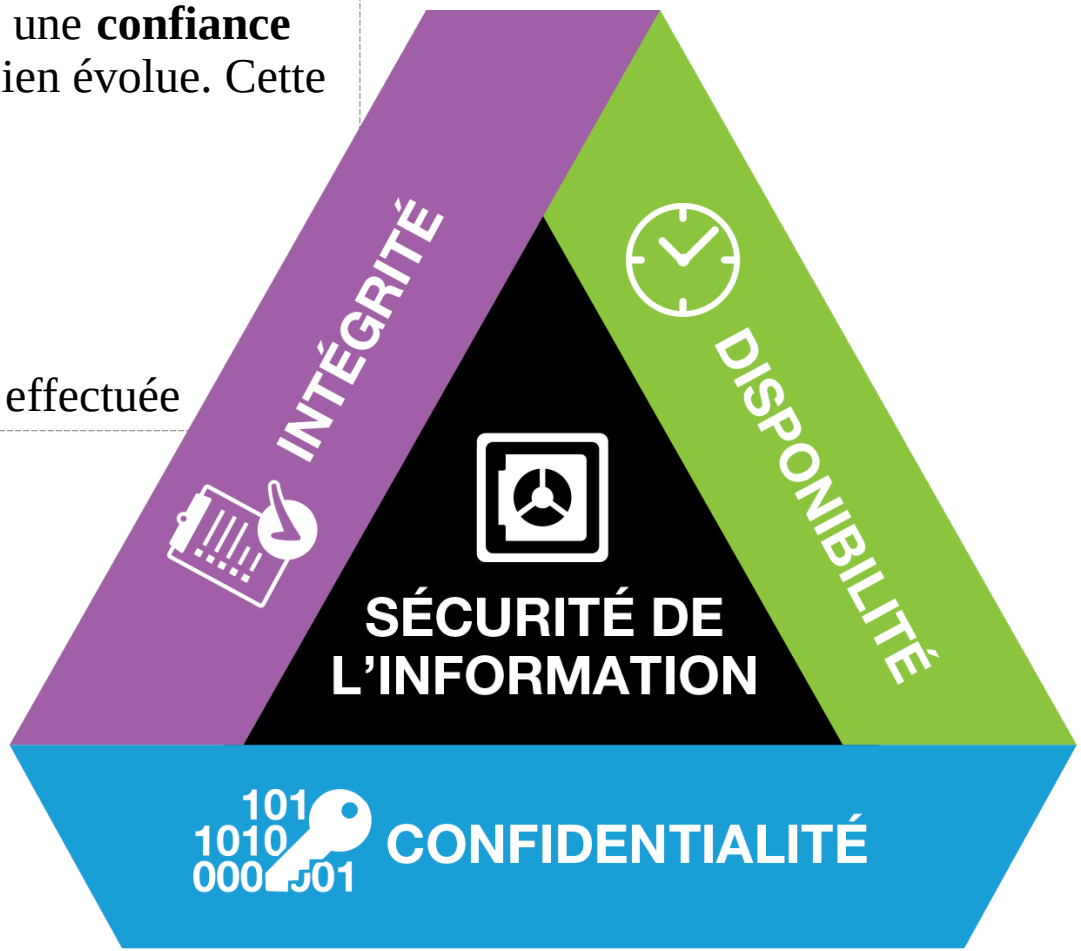
Propriété d'un bien permettant de retrouver, avec une **confiance suffisante**, les circonstances dans lesquelles ce bien évolue. Cette propriété englobe

Notamment :

- La **traçabilité** des actions menées
- L'**authentification** des utilisateurs
- L'**imputabilité** du responsable de l'action effectuée



Bien à protéger



Sûreté VS sécurité (1/4)

- Significations différentes en fonction du contexte.
- L’interprétation de ces expressions
  - Varie en fonction de la sensibilité de chacun.

Sûreté VS sécurité (2/4)

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…

Sûreté VS sécurité (3/4)

Ensemble des mécanismes

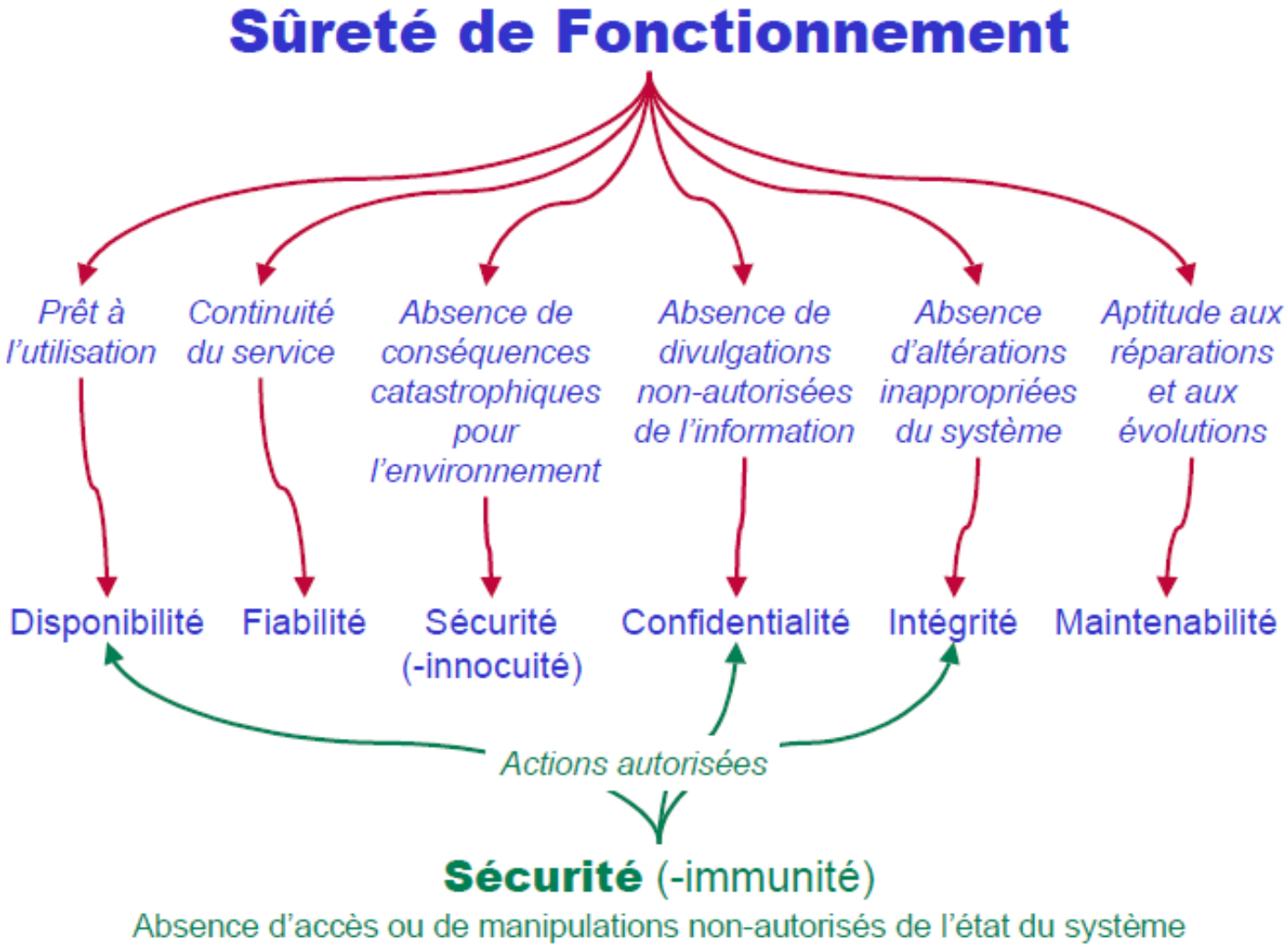
- Sûreté
  - Mis en place pour assurer la continuité de fonctionnement du système dans les conditions requises.
- Sécurité
  - Destinés à protéger l'information des utilisateurs ou processus
    - n'ayant pas l'autorisation de la manipuler
    - d’assurer les accès autorisés.

Le périmètre de chacune des 2 notions n’est pas si clairement délimité dans la réalité

Exemple :
Voiture connectée
→ on cherchera la sécurité & la sûreté.

Sûreté VS sécurité (4/4)

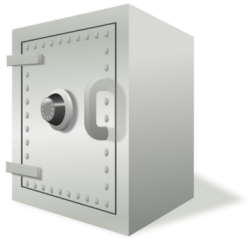
Ensemble des mécanismes



Exemple d’évaluation DICP (1/2)

- Pour évaluer si un bien est correctement sécurisé
  - 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’origine du besoin attendu :
  - Interne : inhérente au métier de l’entreprise
  - externe : issue des contraintes légales qui pèsent sur les biens de l’entreprise.



- 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**

Exemple d'évaluation DICP (2/2)

Avec un site simple (statique) Une entreprise veut 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 connaitre ses services au public

- **Confidentialité** — **Faible**

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

- **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)

- **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.

Mécanismes de sécurité (1/2)

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

Mécanismes de sécurité (2/2)

		D	I	C	P
Capacité d'audit	Mécanismes organisationnels destinés à s'assurer de l'efficacité et de la pertinence des mesures mises en œuvre. Participe à l'amélioration continue de la sécurité du S.I.	X	X	X	X
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	X	X	X	X
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.	X	X	X	X

A retenir

- Le besoin de la sécurité par le preuve

  Implique :

- Une vision de sécurité et/ou sûreté
  - Disponibilité
  - Intégrité
  - Confidentialité
  - Preuve

EXERCICE

Durée 30 minutes

En groupe

Rejoindre le groupe associé au prénom

- A à C
  - https://hebdo.framapad.org/p/a-c-a63i
- D à M
  - http://hebdo.framapad.org/p/d-m-a63i
- N à R
  - https://hebdo.framapad.org/p/n-r-a63i
- S à Z
  - https://hebdo.framapad.org/p/s-z-a63i

En groupe

Marie, David, et les copains de David

EXERCICE

- Le numéro de téléphone de Marie
  - Marie est la petite amie de David

- La valeur de cette information, pour David, peut se mesurer suivant différents critères

- Définir les critères DICP de ce numéro ?

Questions à se poser ?

- Disponibilité
  - Est-il important pour David de disposer du numéro de téléphone de Marie ?
- Intégrité
  - A quel point est-il important que l'information soit la bonne ?
- Confidentialité
  - Est-il important que le numéro de Marie soit connu de David seulement ?
- Preuve
  - Quelqu'un a volontairement modifié le numéro de Marie, supposons que David veuille trouver qui lui a fait ce sale coup, pour se méfier à l'avenir du copain en question.

Critères DIC : solution

- Disponibilité
- Intégrité
- Confidentialité
- Preuve

- Marie ← TEL → David
- Comportement avec les copains de David
- Varie suivant les besoins
- Classer le numéro
  - Prioritaire ?

Critères DIC : solution

- Disponibilité
- Intégré
- Confidentialité
- Preuve

- Si Marie change de N°
- David appelle sur l'ancien N°
- Changement volontaire ou pas du numéro

Critères DIC : solution

- Disponibilité
- Intégrité
- **Confidentialité**
- Preuve

- Si David veut garder le N° de Marie pour lui
  - Protection
  - Mot de passe
  - Bruler le papier
  - Papier dans un coffre
- Risque de vol par les copains

Critères DIC : solution

- Disponibilité
- Intégrité
- Confidentialité
- Preuve

- David a prété son Tel
- Par les logs
- Sauvegarde régulière
- ...

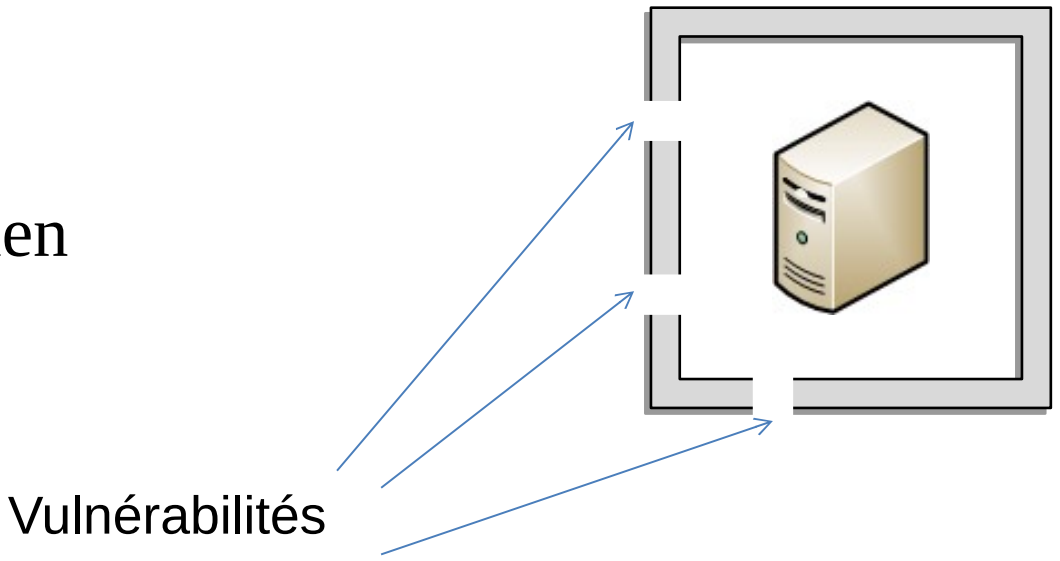
- Détections vulnérabilités
- Correction TP 1
- Les enjeux de la sécurité
- Besoins de sécurité
- Notions des vulnérabilités
- Panorama des menaces
- Les règles en France

Notions de !!!

- 3 Notions :
  - Vulnérabilité
  - Menace
  - Attaque

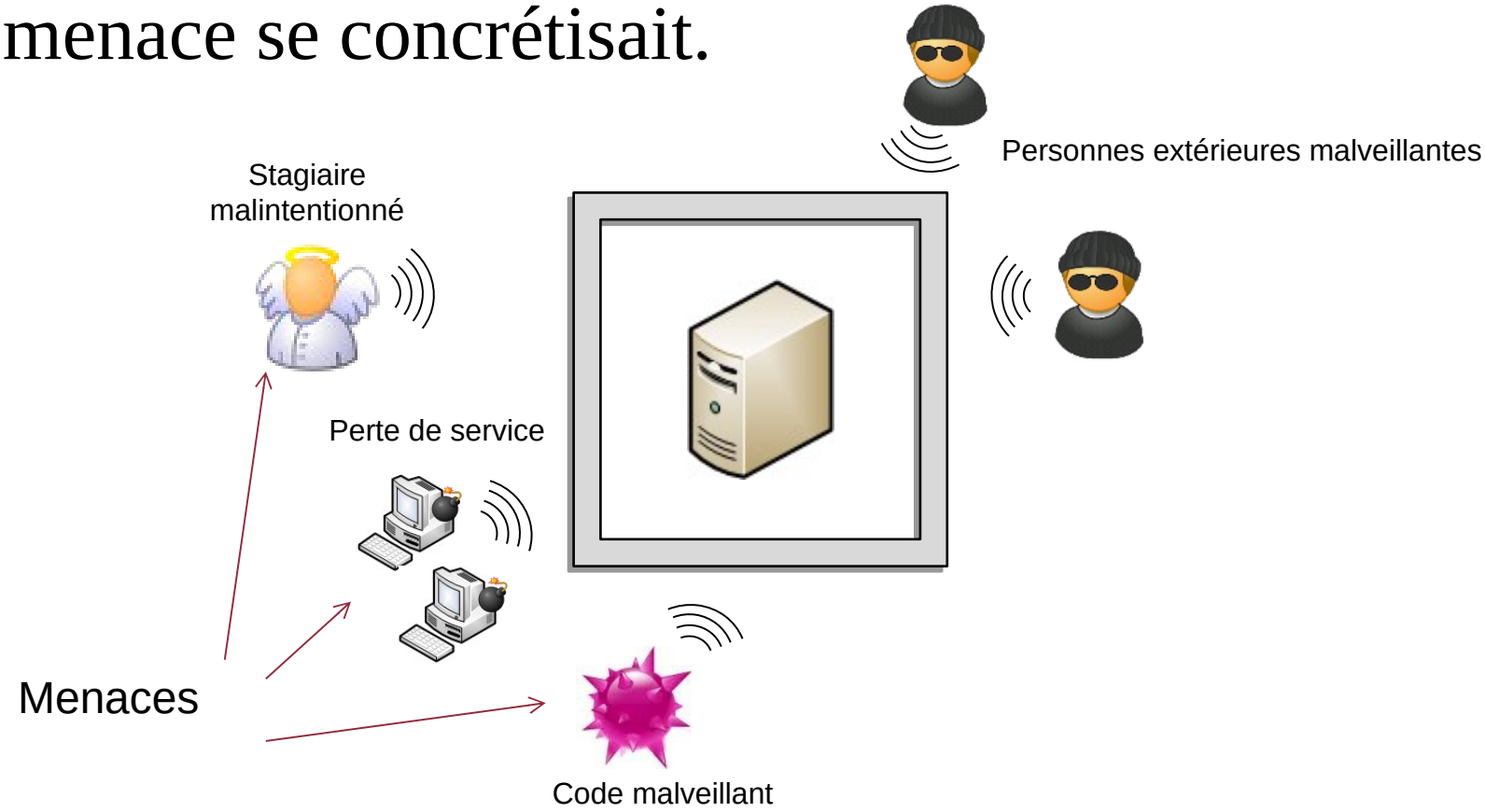
Notion de « Vulnérabilité »

- 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



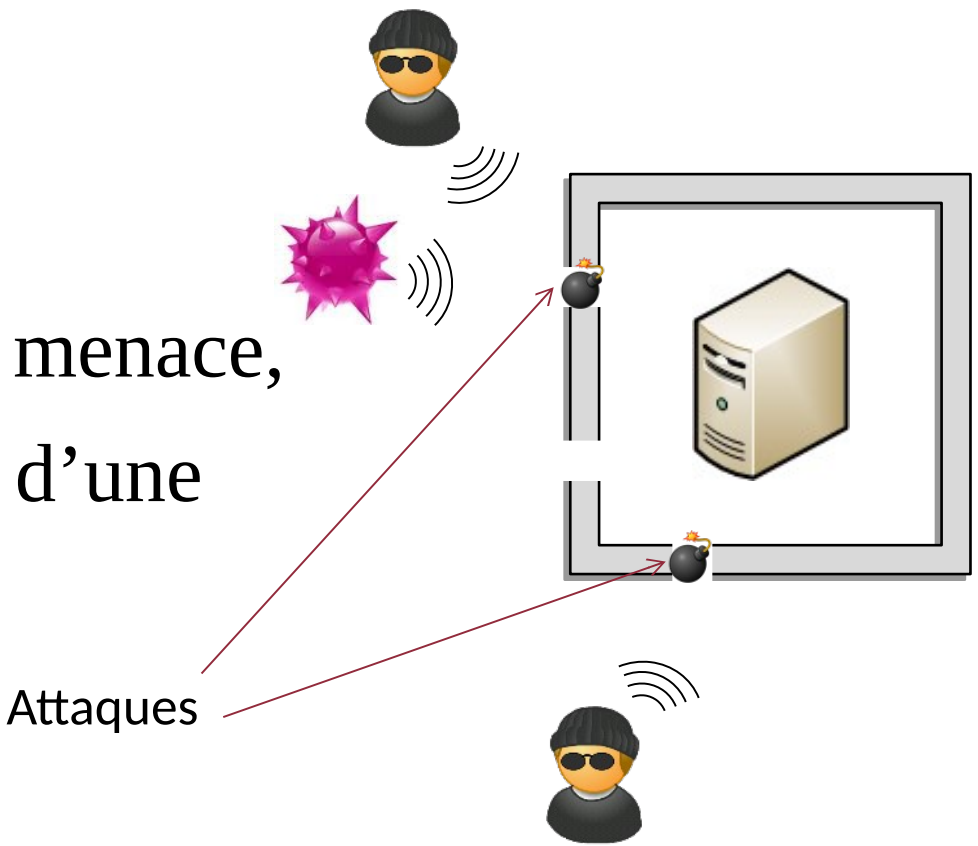
Notion de « Menace »

- Menace
- Cause potentielle d’un incident
  - Qui pourrait entraîner des dommages sur un bien si cette menace se concrétisait.



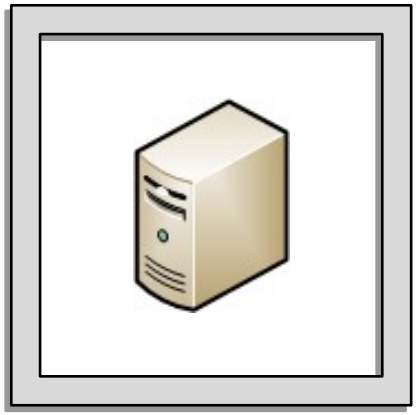
Notion d'« Attaque »

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



Notion d’« Attaque »

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



Rôle de l’expert Sécurité

- Objectif principal
  - S’assurer que le S.I.
    - ne possède pas de vulnérabilité
- Au quotidien
  - Etre en mesure de maîtriser ces vulnérabilités

Objectif « 0 » est inatteignable

Exemple de vulnérabilité : VNC

2006

- Contournement de l'authentification
  - dans l’application VNC
- VNC est une application
  - Prise en main sur une machine distance,
    - Après qu’il se soit authentifié.
- Faille :
  - Contournement de l'authentification
    - dans l’application VNC

Description de la vulnérabilité

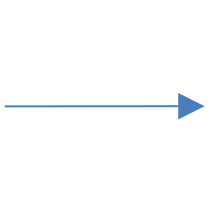
- L’application permet
  - A un utilisateur de se connecter à distance sur une machine
    - Partage de bureau
    - Travailler à distance sur cette machine
- En 2006 → Vulnérabilité critique détecté
  → Possible de se connecter à distance
    - sur cette application sans avoir besoin de s’authentifier

Failles corrigées depuis 2006

Illustration d’un usage normal de l’application vulnérable

Description du fonctionnement <u>normal</u> de l’application

L’utilisateur effectue une demande de connexion au serveur depuis son PC client



mdp = ?

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

L’utilisateur s’authentifie selon la méthode choisie par le serveur

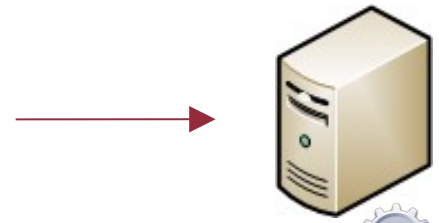
mdp = Afh7ù

Le serveur valide l’authentification (si elle est correcte) et autorise donc la connexion

Référence : CVE-2006-2369

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

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



Description du fonctionnement <u>modifié</u> par un attaquant

mdp = ?

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

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

authent = NON

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

Référence : CVE-2006-2369

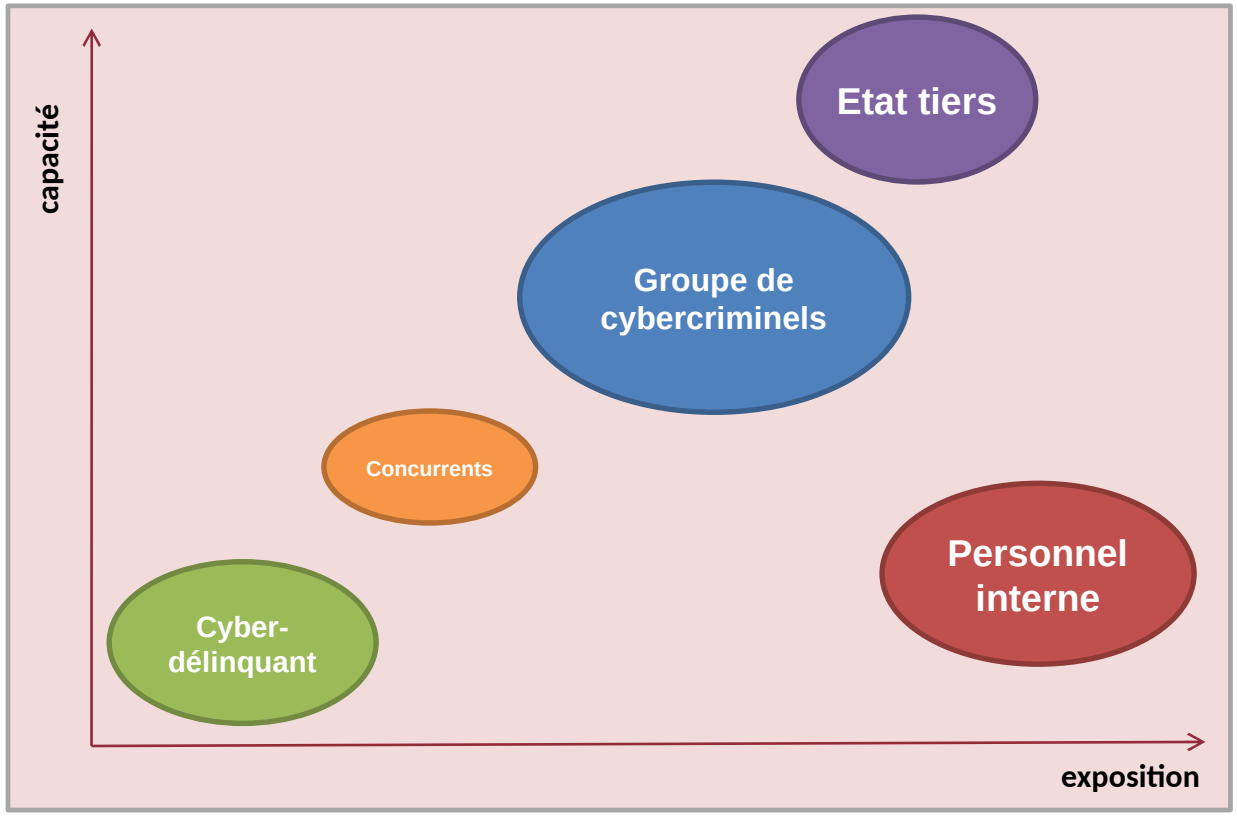
La vulnérabilité se situe ici : le serveur ne vérifie pas que le type d'authentification retourné par le client correspond à celui demandé. A la place, il vérifie simplement que l'authentification est correcte (et « authent = NON » est effectivement une authentification qui est toujours correcte)

En résumé

- Il n’est pas possible de connaître toutes les failles
- Il existe des outils pour aider le S.I.
- Objectif « 0 » est inatteignable

- Détections vulnérabilités
- Correction TP 1
- Les enjeux de la sécurité
- Besoins de sécurité
- Notions des vulnérabilités
- Panorama des menaces
- Les règles en France

Sources potentielles de menaces



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

- Capacité :
degré d'expertise et ressources de la source de menaces

- Exposition :
opportunités et intérêts de la source de menaces

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

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

Panorama de quelques menaces

Hameçonnage & ingénierie sociale

Fraude interne

Violation d’accès non autorisé

Virus informatique

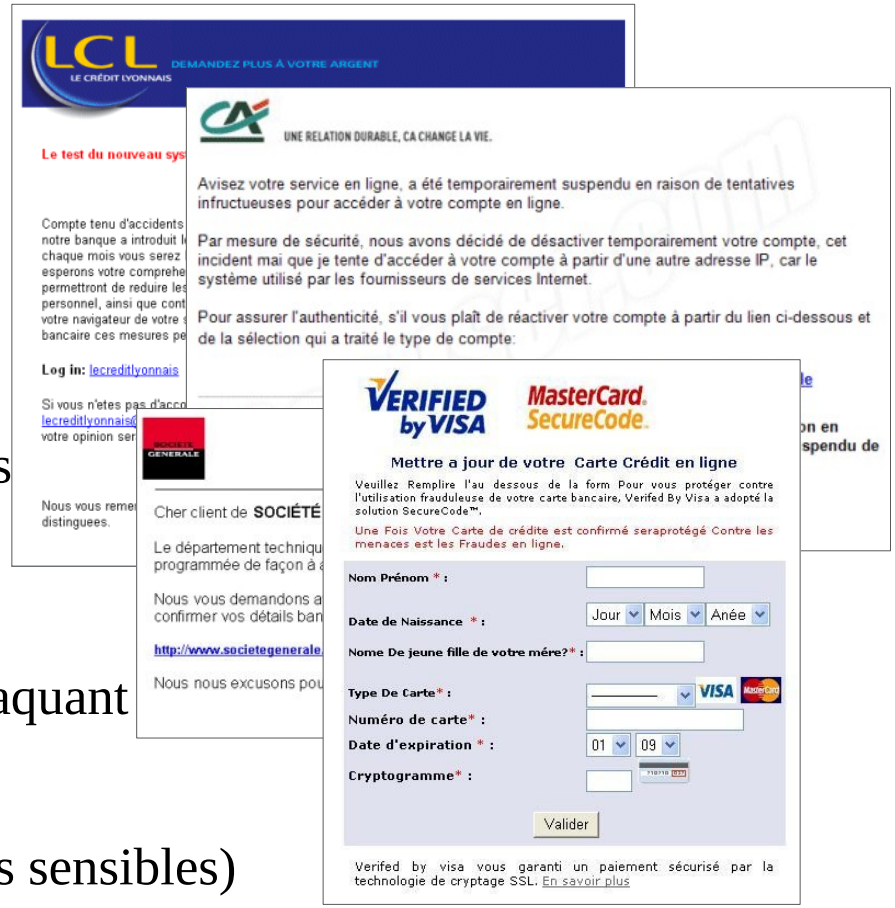
Déni de service distribué

Phishing

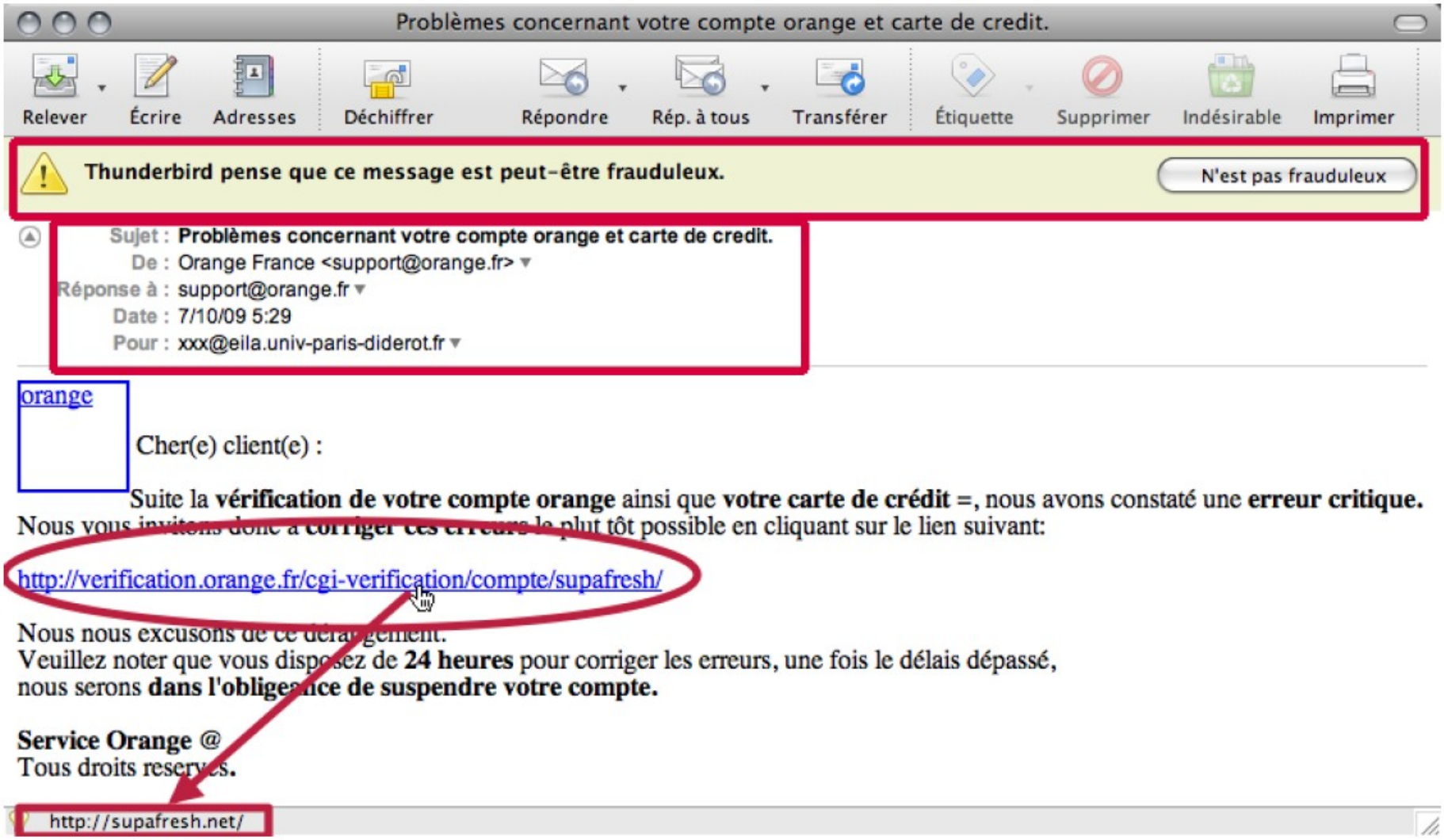
- L’hameçonnage (« phishing »)
  - Attaque de masse vise à abuser de la « naïveté »
    - des clients ou des employés pour récupérer leurs identifiants de banque en ligne ou leurs numéros de carte bancaire…
- Fonctionnement
  - Réception d’un mail
    - Logo et couleurs de l’entreprise
  - Demande effectuer une opération
    - Ex : Mise-à-jour des données personnelles

      ou la confirmation du mot de passe
  - Connexion à un faux-site identique
    - à celui de l’entreprise et contrôlé par l’attaquant
  - Récupération par l’attaquant
    - des identifiants/mots de passe (ou données sensibles)

      saisie par le client sur le faux site



Exemple de phishing



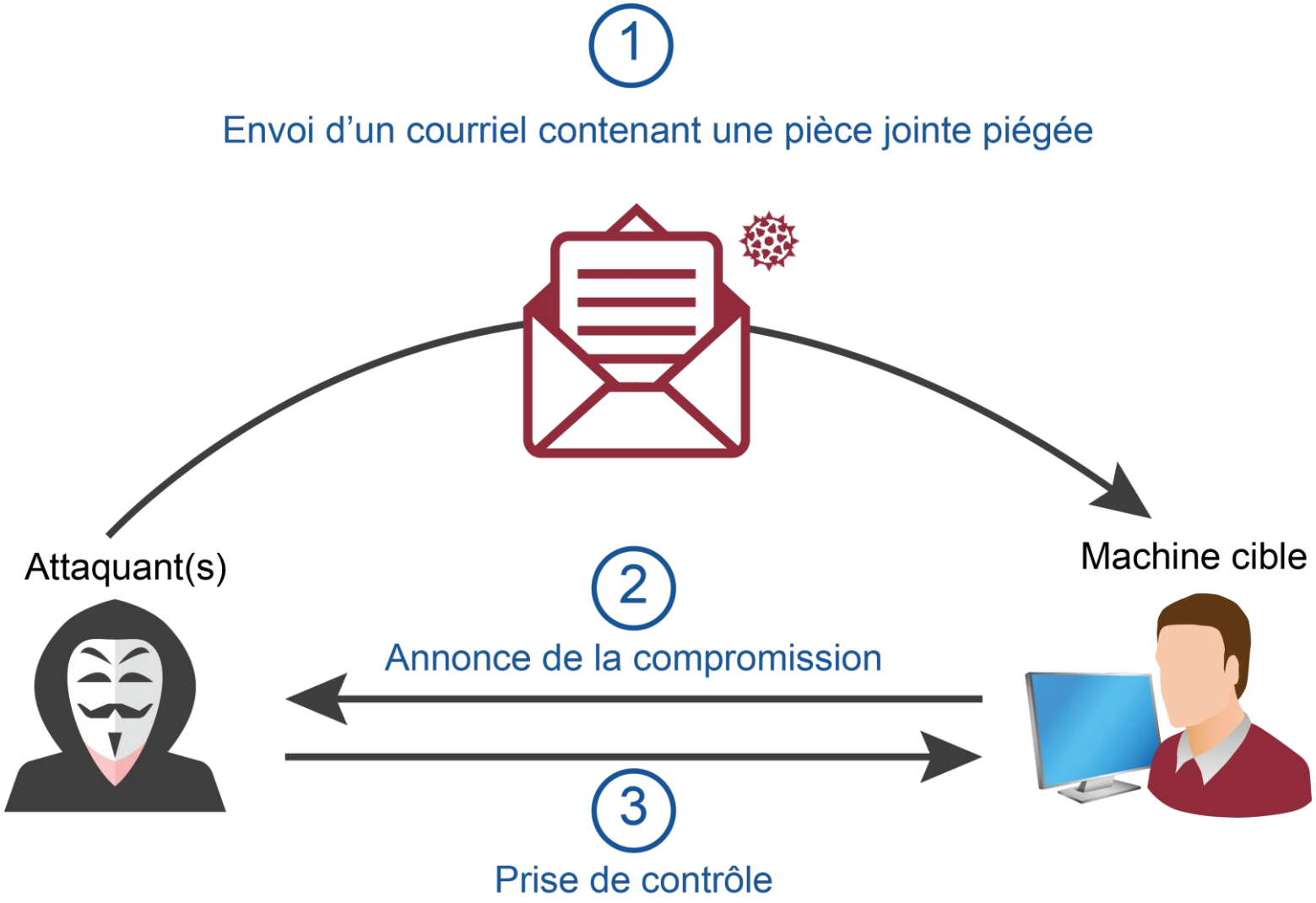
Ingénierie sociale

- Attaque ciblée
  - Téléphonie, messagerie, Réseaux sociaux
  - vise à abuser de la « naïveté » des employés de l'entreprise pour dérober directement :
    - des informations confidentielle
    - pour introduire des logiciels malveillants

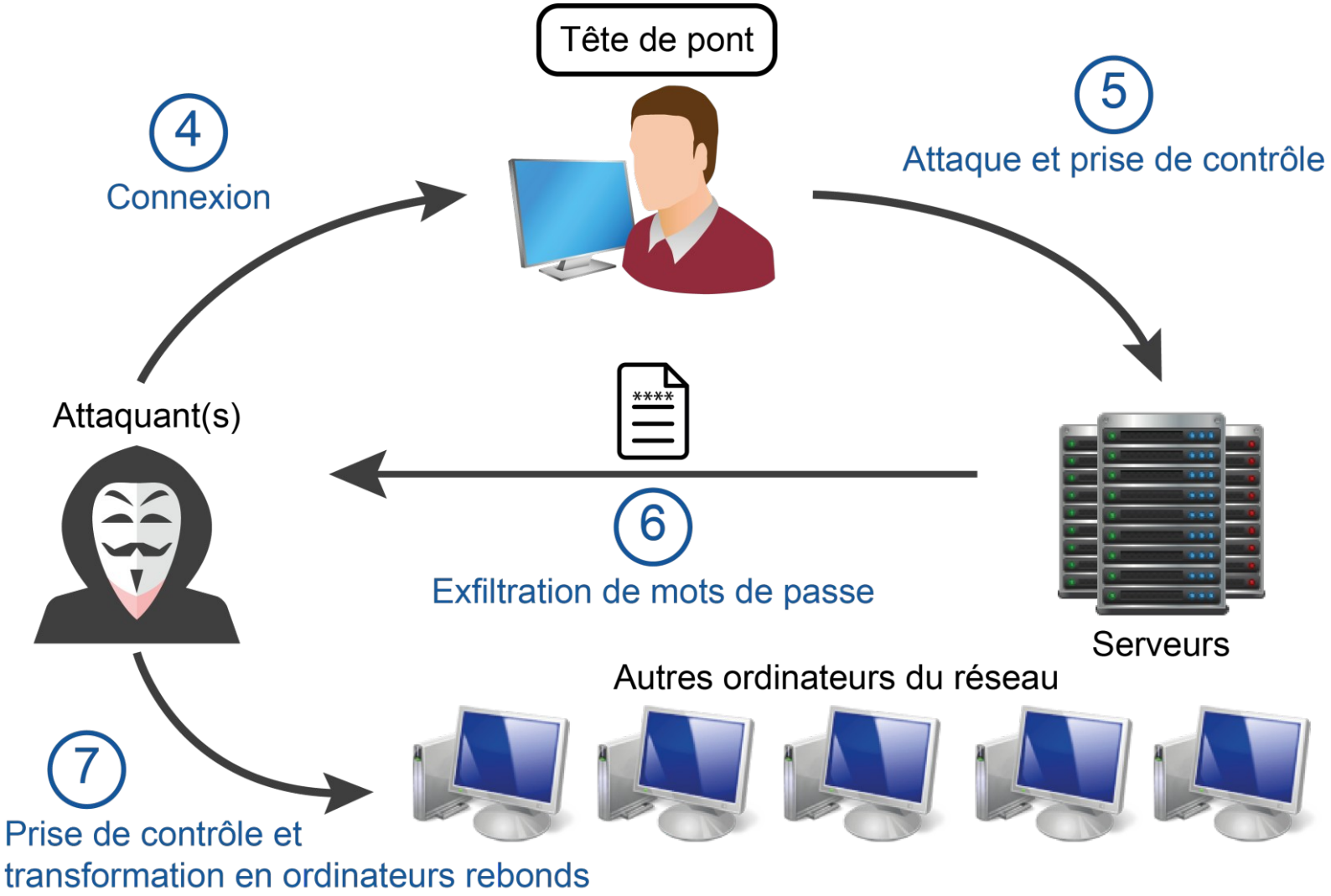
      dans le système d'information de la banque

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

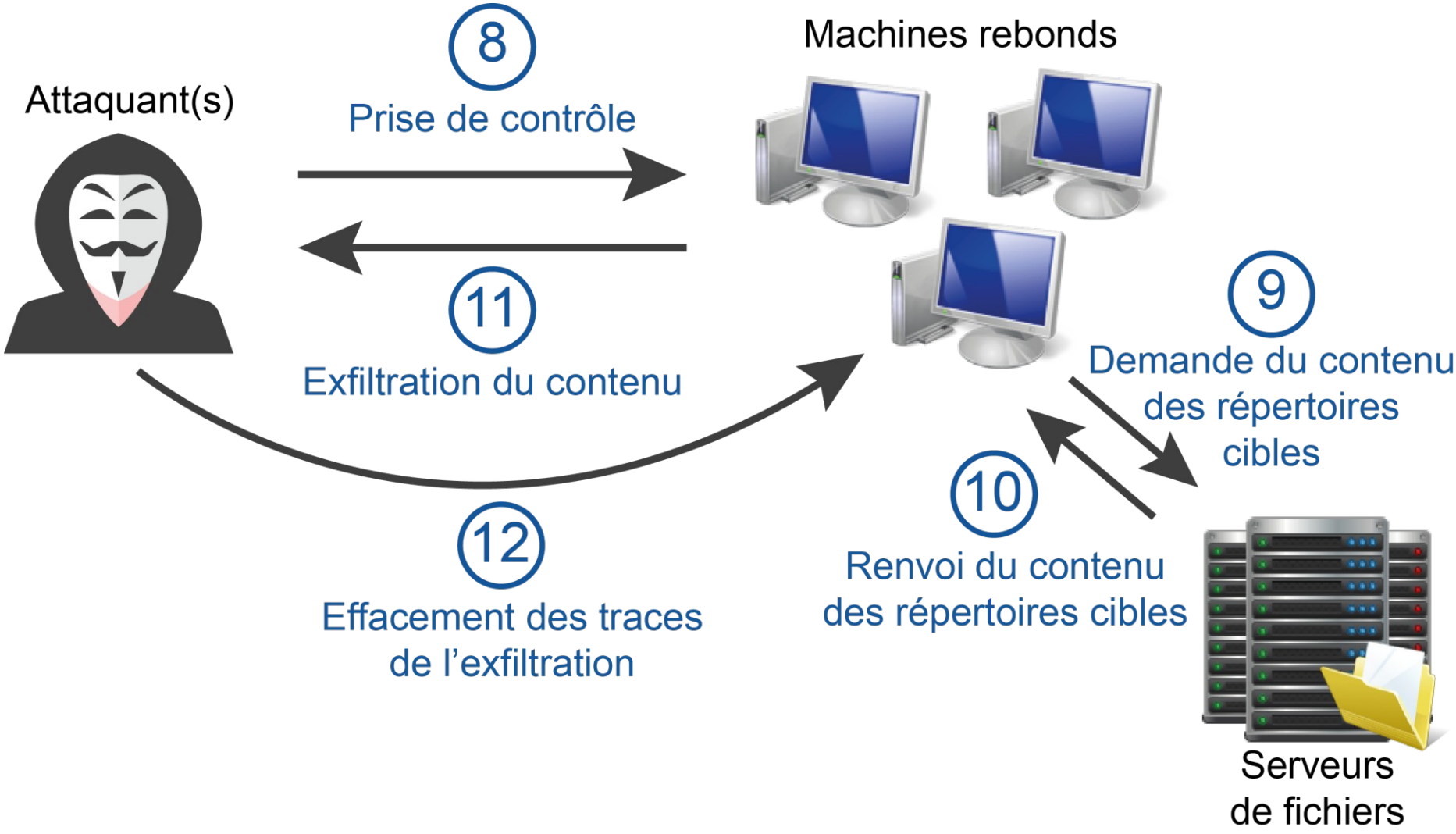
Déroulement d’une attaque avancée (1/3)



Déroulement d'une attaque avancée (2/3)



Déroulement d’une attaque avancée (3/3)



Exemple : Déroulement d'une attaque avancée

Des photos intimes d'acteurs, chanteurs, présentateurs célèbres stockées sur iCloud d'Apple ont été diffusées en ligne.
Les célébrités incluaient Jennifer Lawrence, Kate Upton, Rihanna, Kim Kadarshian, Selena Gomez entre autres.

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

Fraude interne

- « Sujet tabou » pour les entreprises

  mais un véritable sujet d'importance !

Catégories de fraudeurs

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

→

Vulnérabilités

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

→

Typologies des fraudes

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

Violation d’accès non autorisé : mots de passe faibles

- Des mots de passe simples ou faibles permettent
  - aux 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.
- Réflexion sur l’utilisation des mots de passe :
  - les mots de passe constituent une faiblesse significative pour la cybersécurité.
- Autres moyens d’authentification émergent
  - But : Libérer les individus des problématiques des mots de passe.
  - Ex : la biométrie, les tokens USB, les matrices papier, la vérification via un code SMS, etc.

Violation d’accès non autorisé : Intrusion (1/2)

- Les intrusions informatiques
  - Constituent des « attaques ciblées »
  - Exploitent une ou des vulnérabilité(s) technique(s) pour dérober des informations confidentielles
    - ex. : mots de passe, carte bancaire…
    - 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
  - Les applications sensibles internes

Violation d’accès non autorisé : Intrusion (2/2)

- 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

tests d’intrusion Orange Consulting 2012-2013

Virus informatique

- Constituent des « attaques massives »
- But :
  - A devenir de plus en plus ciblés sur un secteur d'activité
    - télécommunication, banque, défense, énergie, etc.
  - A devenir de plus en plus sophistiqués et furtifs

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
- …

Déni de service distribué (DDoS)

- Constitue une « attaque ciblée »
- Consiste à saturer un site Web de requêtes
  - pour le mettre « hors-service »
  - A l'aide de « botnets »
  - Réseaux d'ordinateurs infectés et contrôlés par les attaquants

une menace majeure et en augmentation pour les sites Internet

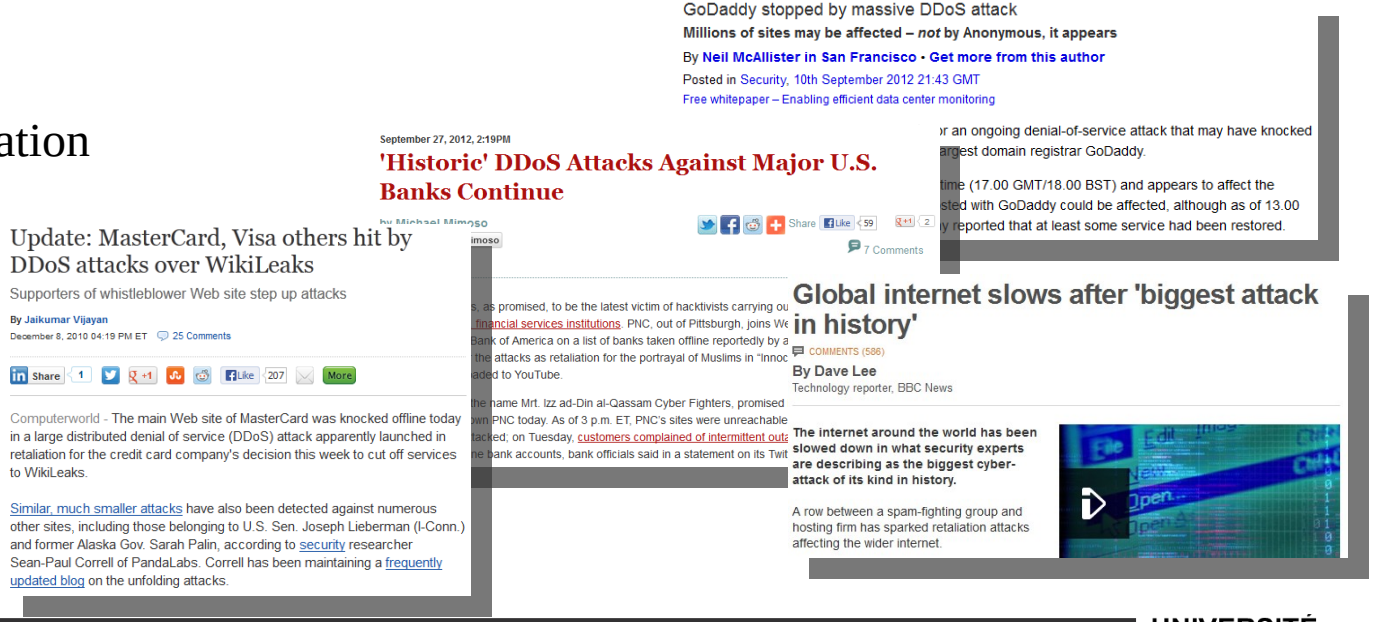
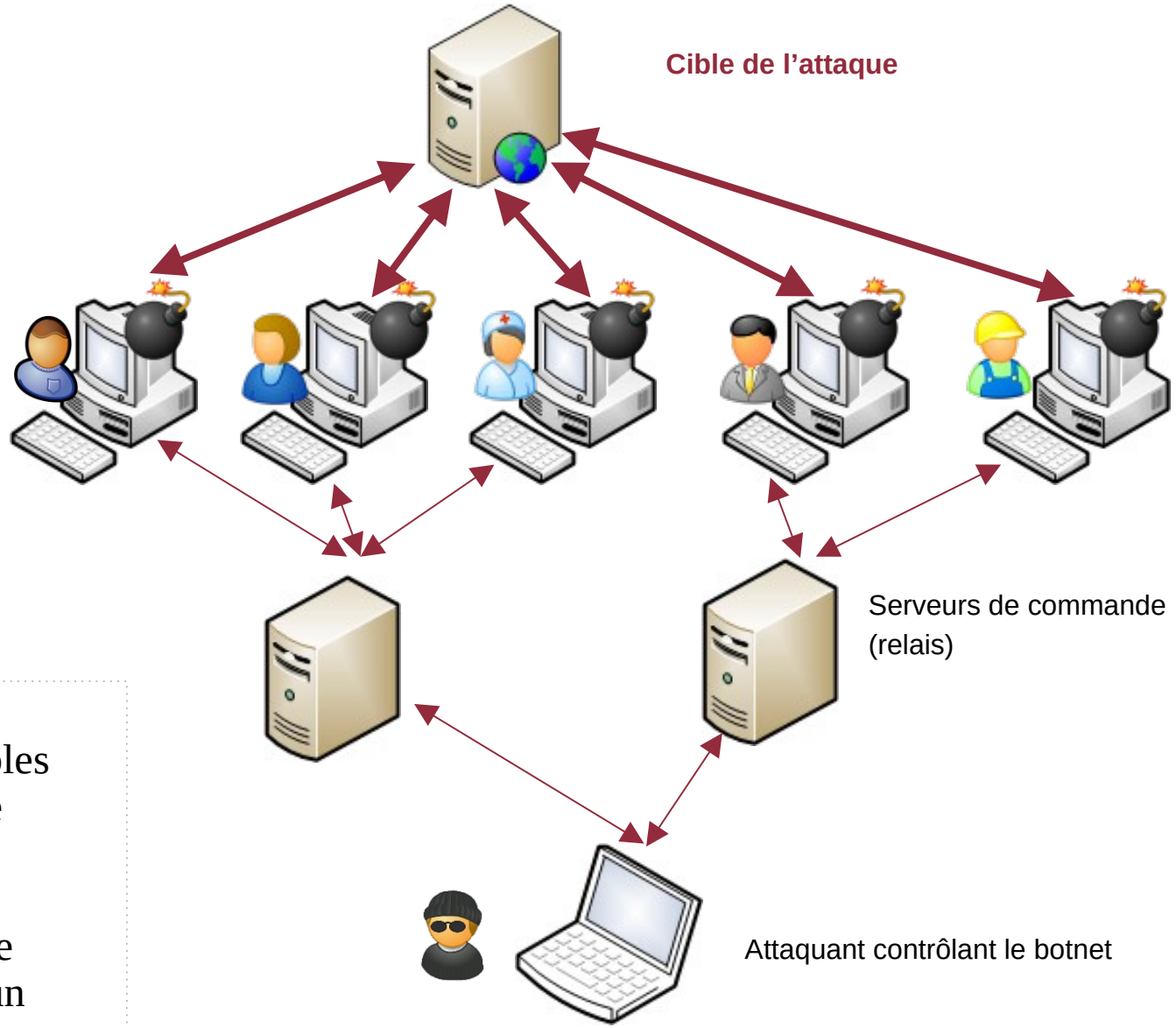


Illustration d’un réseau de botnets

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



Botnet
→ 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

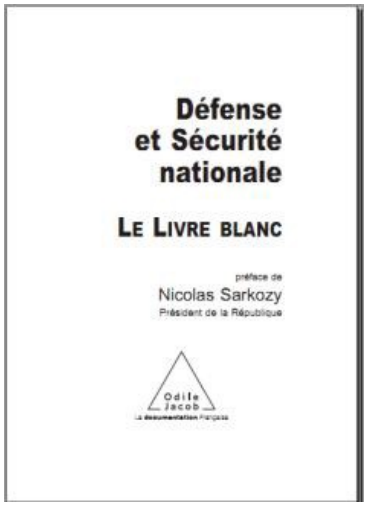
En résumé

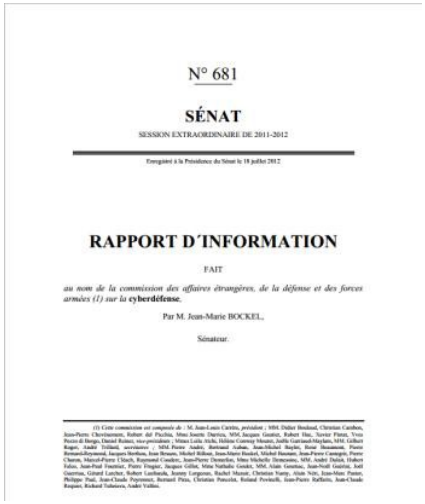
- Les menaces couvrent un large périmètre
- L’imagination des attaquants est sans limite

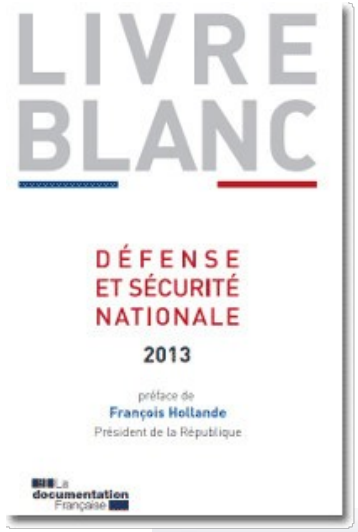
- Détections vulnérabilités
- Correction TP 1
- Les enjeux de la sécurité
- Besoins de sécurité
- Notions des vulnérabilités
- Panorama des menaces
- Les règles en France

L’organisation de la sécurité en France (1/

Cyberdéfense : un véritable enjeu de sécurité nationale







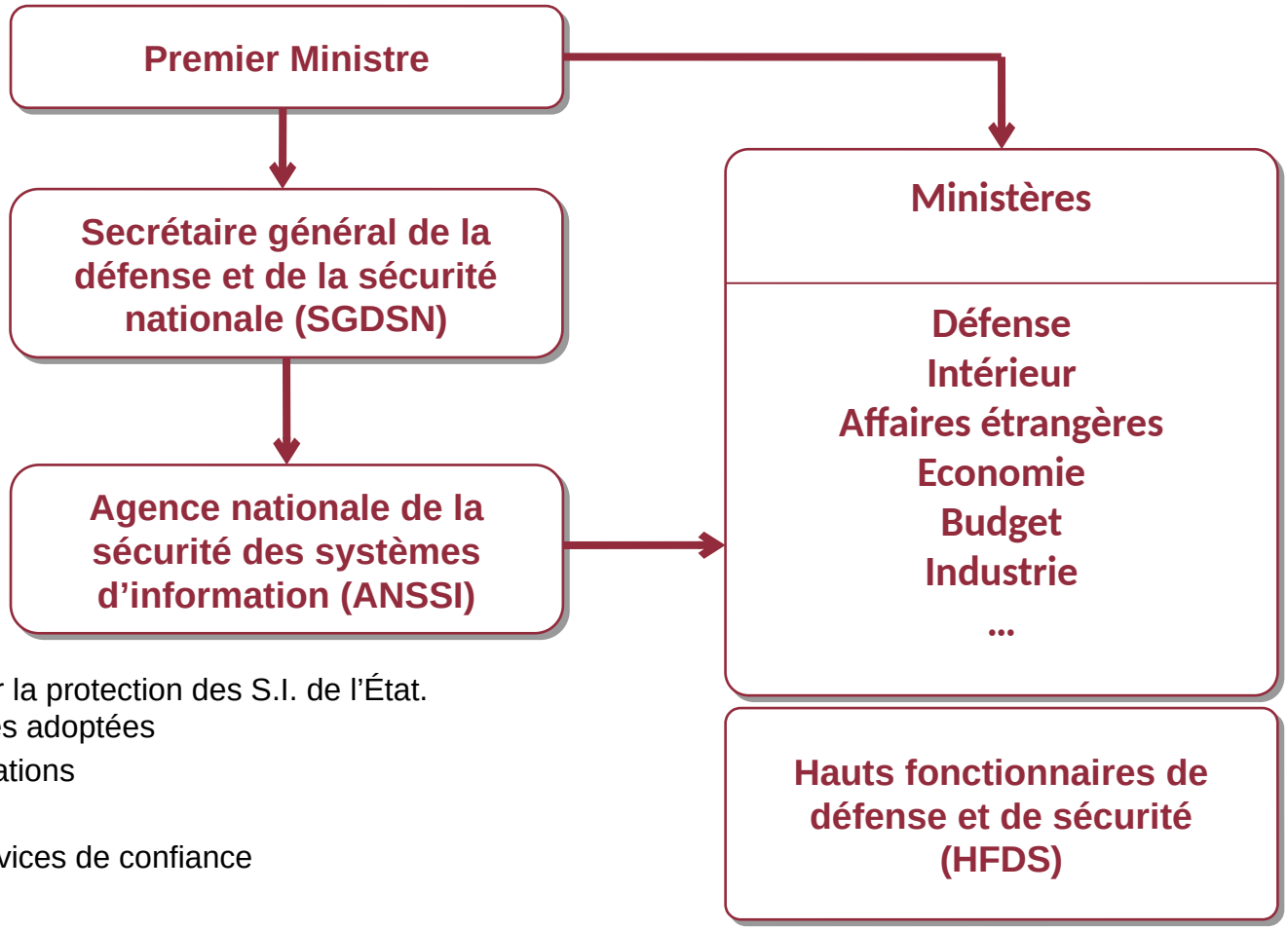
« **Les cyberattaques**, *parce qu’elles n’ont pas, jusqu’à présent, causé la mort d’hommes, n’ont pas dans l’opinion l’impact d’actes terroristes. Cependant, dès aujourd’hui, et plus encore à l’horizon du Livre blanc, elles constituent* **une menace majeure, à forte probabilité et à fort *impact potentiel***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

http://www.livreblancdefenseetsecurite.gouv.fr/
http://www.sgdsn.gouv.fr/

L’organisation de la sécurité en France (2/

Organisation interministérielle :



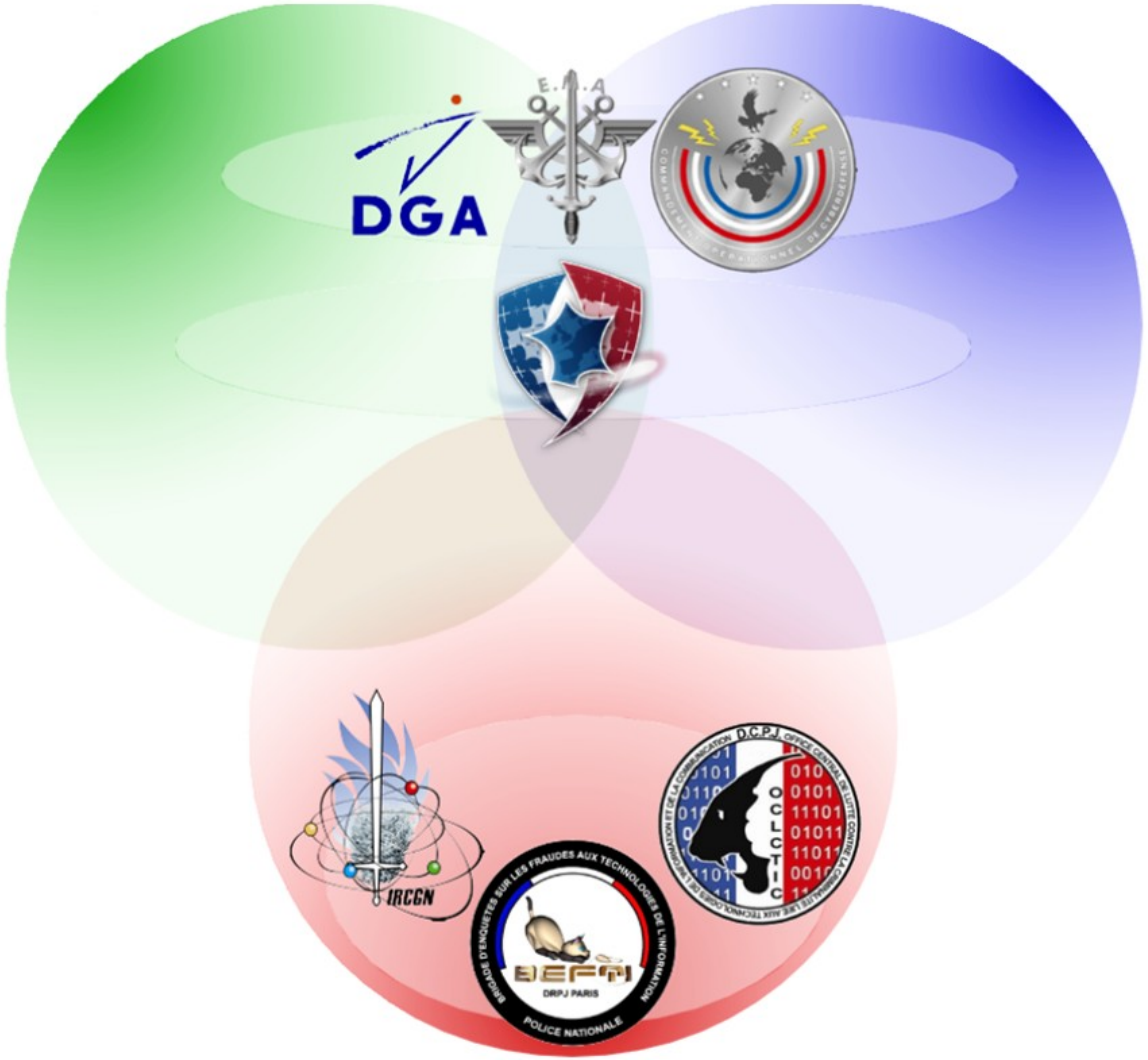
Pilotage de la politique nationale en matière de sécurité des systèmes d’information

Proposition des règles à appliquer pour la protection des S.I. de l’État.
Vérification de l’application des mesures adoptées
Conseil/soutien Sécurité aux administrations
Information du public
Contribution au développement de Services de confiance
…

Coordination de la préparation des mesures de défense (Vigipirate) et chargés de la sécurité des systèmes d'information

L’organisation de la sécurité en France (3/

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”

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
  - …

Le droit des T.I.C (1/2)

- = droit orienté vers les

  Technologies de l'Information et la Communication.

- Objectifs
  - Appréhender les enjeux humains et sociaux
    - liés au développement des technologies
      - de l'information
      - de la communication
  - c'est-à-dire
    - cerner l'impact de la manipulation des TIC sur la société et sur l'homme.

Le droit des T.I.C. (2/2)

- Un droit non codifié : des dizaines de codes en vigueur
- 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.

- Code de la défense
- Code civil
- Code pénal
- Droit du travail
- Code de la propriété intellectuelle
- Code des postes communicat. électroniques
- Code de la consommation
- …

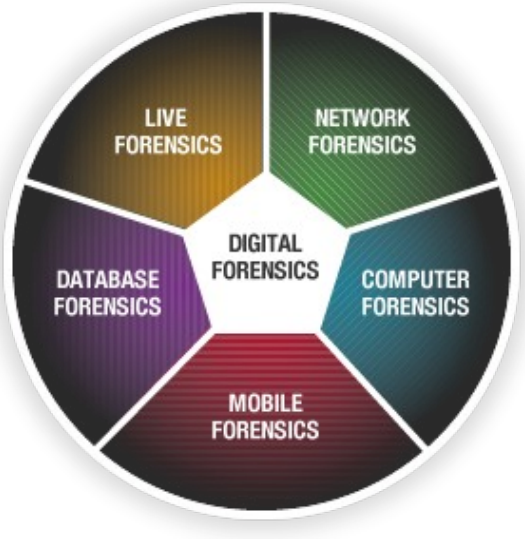
(*) La « jurisprudence » est formée de l'ensemble des décisions de justice , « à tous les étages » de l'ordre judiciaire, ce qui donne lieu parfois à des décisions contradictoires, à l'image de l'évolution de la société.

La lutte contre la cybercriminalité en France (1/4)

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

La lutte contre la cybercriminalité en France (2/4)

- 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.



La lutte contre la cybercriminalité en France (3/4)

- 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

La lutte contre la cybercriminalité en France (4/4)

- 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

Le rôle de la CNIL (1/6)

= La Commission Nationale de l'Informatique et des Libertés

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Chargée :
  - Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles
- 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). »

https://www.cnil.fr/

Le rôle de la CNIL (2/6)

- 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. »

https://www.cnil.fr/

Le rôle de la CNIL (3/6)

- 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

Le rôle de la CNIL (4/6)

- 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).

Le rôle de la CNIL (5/6)

- 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)

Le rôle de la CNIL (6/6)

- 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

En résumé

- Tout le monde doit être au courant des lois

TP 2

- Deadline
  - Le 22 février 2024 23:59
- Énumération structurée (avec détails)
  - Tous les formats acceptés
    - ODT, Docx, PDF, Markdown…
- Sujet :
    - Si vous étiez victime d'une attaque cybercriminelle, quelles pourraient être les conséquences (impacts) sur votre vie privée ?

Rendez-vous au prochain cours

- Merci de votre attention