Master Informatique – parcours SIS
sebastien.duval@loria.fr

Sécurité des Systèmes d'Information

Chapitre 1 : Notions de base

2025/2026

Supports basés sur le cours de Laurent Vigneron

Plan du chapitre

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 (F)**
6. **Avènement du RGPD**
7. **RGPD… et ensuite… - international, NIS2**

1. Les enjeux de la sécurité des S.I.

a) Préambule
b) Les enjeux
c) Pourquoi les pirates s'intéressent aux S.I. ?
d) L'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.

D'après vous ?

C'est quoi un S.I. ?

1. Les enjeux de la sécurité des S.I.

a. Préambule

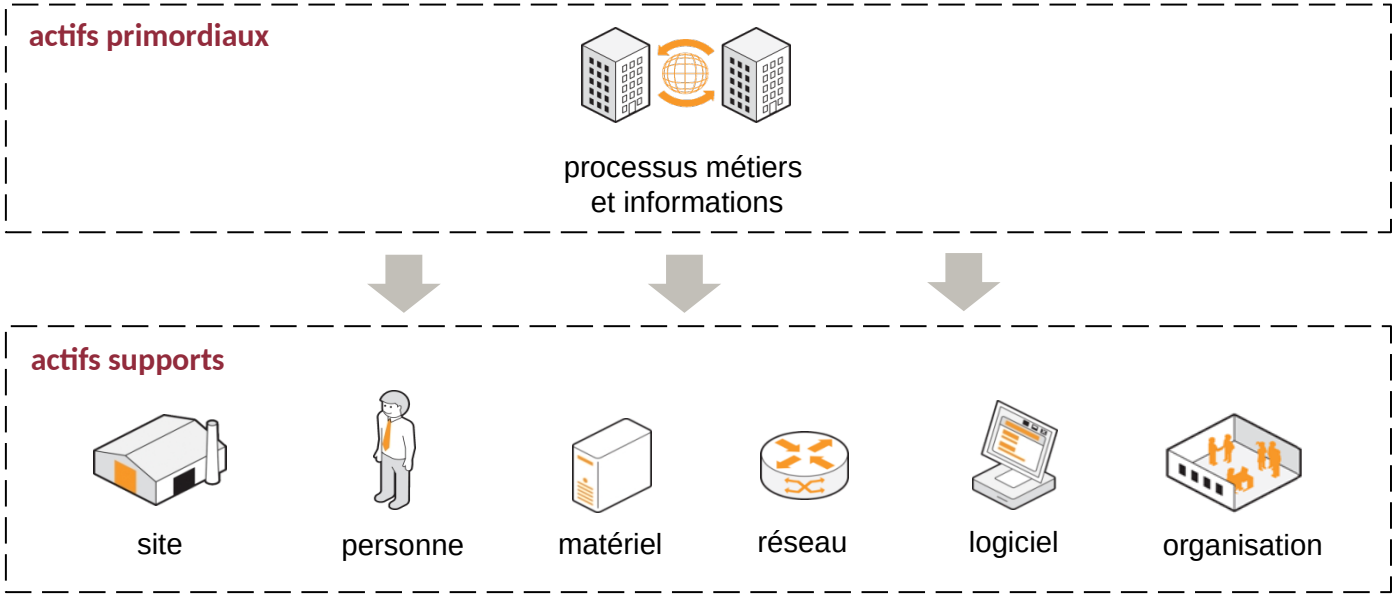
- Système d'Information (S.I.)
  - Ensemble des ressources destinées **à collecter, classifier, stocker, gérer, diffuser les informations** au sein d'une organisation
  - Mot clé : information, c'est le « nerf de la guerre » pour toutes les entreprises, administrations, organisations, etc.

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

1. Les enjeux de la sécurité des S.I.

a. Préambule

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



ISO/IEC 27005:2008

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

1. Les enjeux de la sécurité des S.I.

b. Les enjeux

- La sécurité a pour objectif de **réduire les risques** pesant sur le système d'information, pour **limiter leurs impacts** sur le fonctionnement et les activités métiers des organisations…

- La gestion de la sécurité au sein d'un système d'information n'a pas pour objectif de faire de l'obstruction. Au contraire :

  – Elle **contribue à la qualité de service que les utilisateurs** sont en droit d'attendre

  – Elle **garantit au personnel le niveau de protection** qu'ils sont en droit d'attendre

1. Les enjeux de la sécurité des S.I.

D'après vous ?

Quels départements d'une entreprise sont impactés par la sécurité des SI ?

1. Les enjeux de la sécurité des S.I.

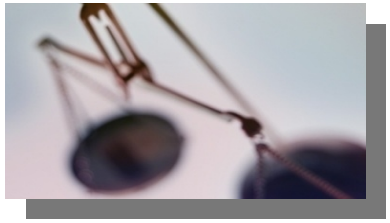
b. Les enjeux

Impacts financiers

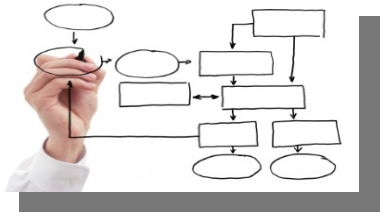
Impacts sur l'image et la réputation

Sécurité des S.I.

Impacts juridiques et réglementaires



Impacts organisationnels



1. Les enjeux de la sécurité des S.I.

D'après vous ?

Pourquoi les pirates s'intéressent-ils aux S.I. des organisations ou à l'ordinateur d'individus ?

1. Les enjeux de la sécurité des S.I.

c. Pourquoi les pirates s'intéressent-ils aux S.I. des organisations ou à l'ordinateur d'individus ?

- Les motivations évoluent
  - Années 1980 et 1990 : 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 à l'ordinateur d'individus ?

- **Gains financiers** (accès à de l'information, puis monétisation et revente)
  - Utilisateurs, méls
  - Organisation interne de l'entreprise
  - Fichiers clients
  - Mots de passe, n° de comptes bancaire, de cartes bancaires
  - Rançons

- **Utilisation de ressources** (puis revente ou mise à disposition en tant que « service »)
  - Bande passante & espace de stockage (hébergement de musique, films et autres contenus)
  - Zombies (botnets)

- **Chantage**
  - Déni de service
  - Modification/divulgation de données

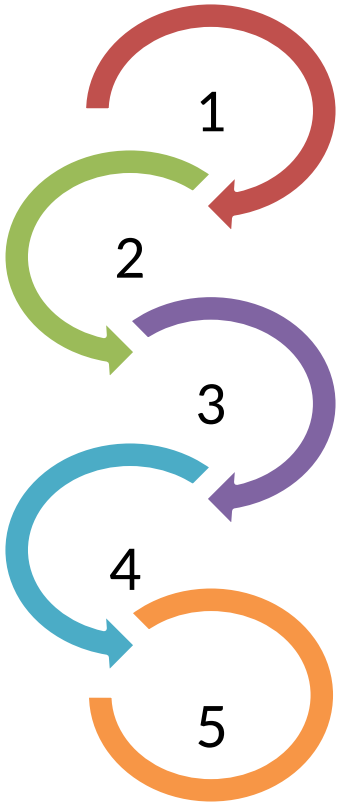
- **Espionnage**
  - Industriel / concurrentiel
  - Étatique

…

1. Les enjeux de la sécurité des S.I.

d. L'économie de la cybercriminalité

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



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

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

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

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

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

1. Les enjeux de la sécurité des S.I.

d. L'économie de la cybercriminalité

- Quelques éléments du marché de la cybercriminalité…
  - Générateurs de numéros valides de CB
  - Revente d'informations de CB réelles (10% du solde du compte)
  - Location de botnets pour provoquer des attaques de déni de service
  - Location de malwares pour intercepter des données confidentielles
- Tout cela avec
  - Une assistance des utilisateurs
  - Des critères de durée et de puissance faisant varier les tarifs
  - Possibilité d'abonnements
  - …

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 / 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 récent (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 faire preuve de discernement lors de l'usage d'Internet/smartphones…

1. Les enjeux de la sécurité des S.I.

f. 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, finance, industrie.

- Ces organisations sont classées comme **Opérateur d'Importance Vitale (OIV).** La liste exacte est classifiée (donc non disponible au public).
- Obligation de renforcer la sécurité des SI critiques (**Systèmes d'Information d'Importance Vitale**, **SIIV**)

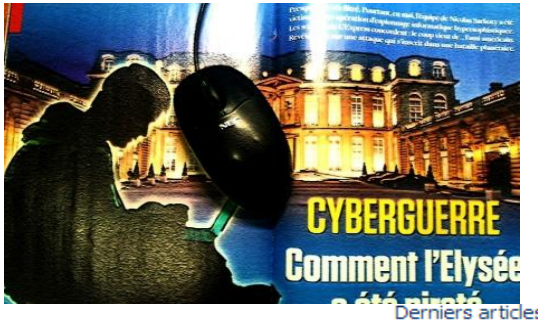
1. Les enjeux de la sécurité des S.I.

D'après vous ?

Connaissez-vous quelques attaques informatiques célèbres / récentes ?

1. Les enjeux de la sécurité des S.I.

g. Quelques exemples d'attaques (les classiques)



Actualités > Société

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

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

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

Tweet +1 5

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.

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

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

Le centre allemand de recherche spatiale cible d'une cyberattaque

Agence France-Presse

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

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

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

Abonnez-vous à partir de 1 € Réagir Classer Partager

Ukraine : le mystérieux virus Snake infecte les ordinateurs du gouvernement

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

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

Illustration. Un mystérieux virus a été réactivée ces derniers jours et vise les ordinateurs ukrainiens. | LP/ Olivier Arandel

1. Les enjeux de la sécurité des S.I.

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.

Gibraltar: un incendie interrompt des services de paris en ligne

AFP, 20/04 23:31 CET

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

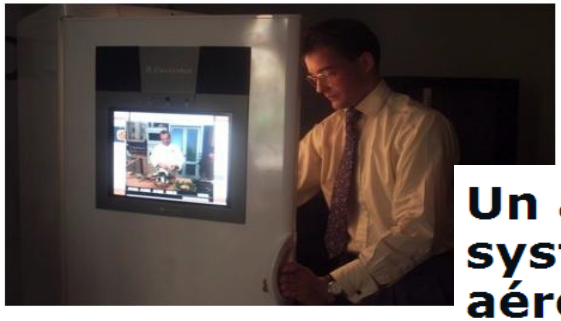
10:12 - vendredi 19 octobre 2012 - Par Johann Mise - Source : France Info

Zoom

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)



Une panne informatique paralyse Wall Street pendant 3 heures

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

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 S.I.

Sony Pictures Entertainment

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

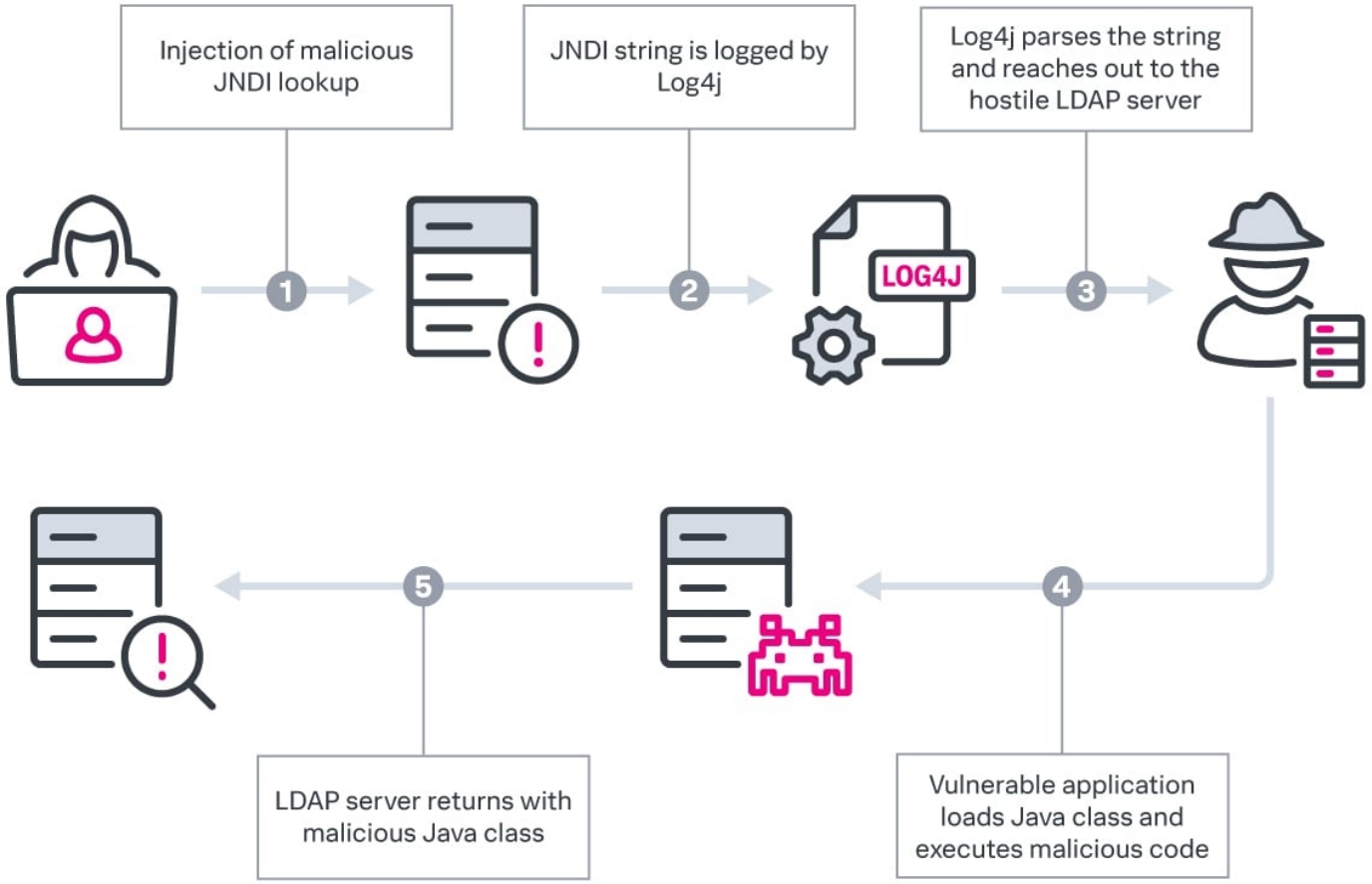
- GOP pour Guardian of Peace
- Des données internes ont été publiées contenant :
  - les numéros de sécurité sociale et les numérisations de passeport appartenant aux acteurs et directeurs.
  - des mots de passe internes
  - des scripts non publiés
  - des plans marketing
  - des données légales et financières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

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

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

1. Les enjeux de la sécurité des S.I.

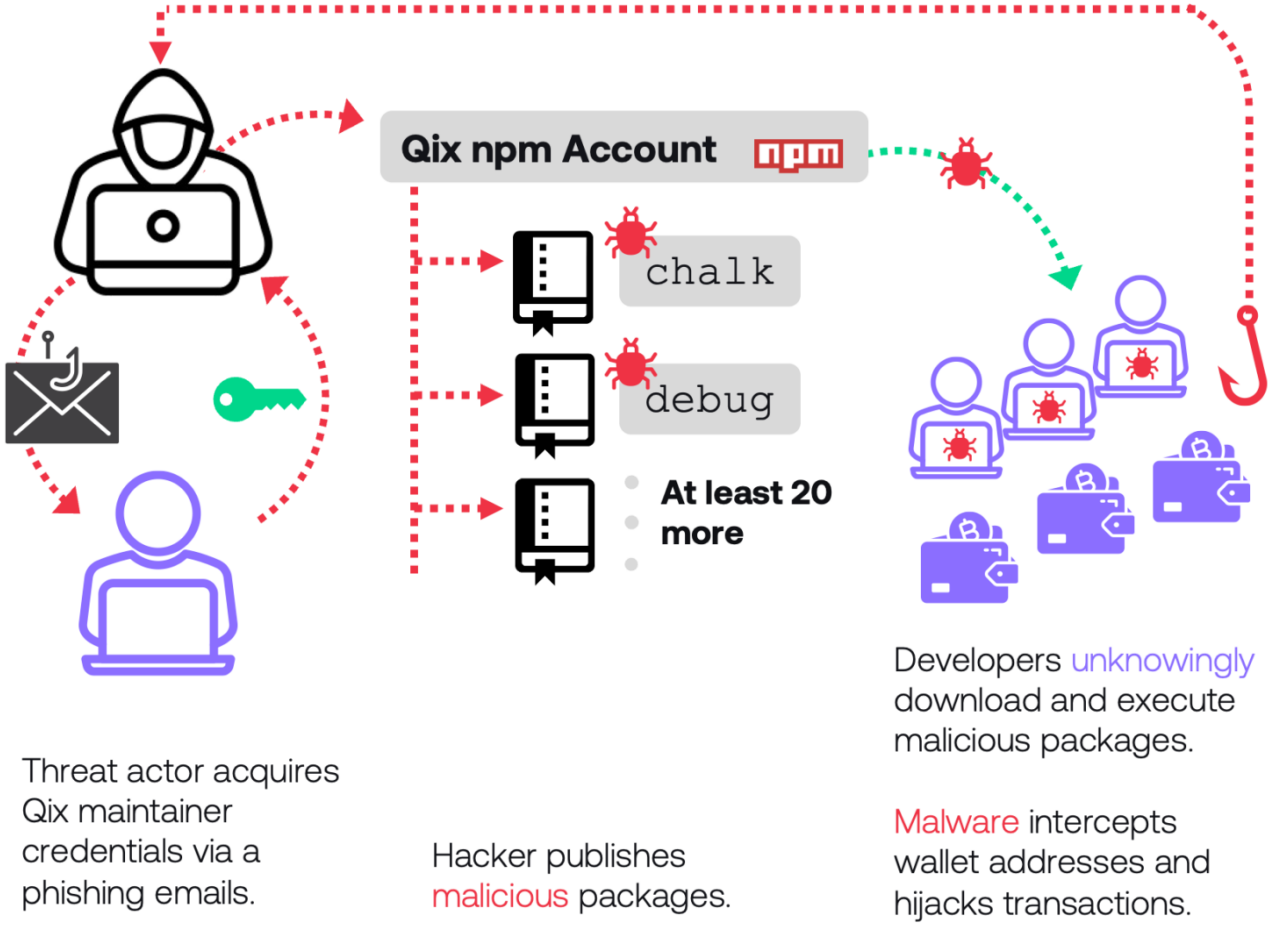
Attaque de log4j (2021 – logs Apache – Java)



- Reverse-shell
- Dans une bibliothèque de log usuelle de tous les serveurs Java
- +34 % de cyberattaques en 2021, majoritairement attribué au passage par cette attaque

1. Les enjeux de la sécurité des S.I.

Shai-Hulud – npm supply-chain attack (sep. 2025)



- Attaque en cours (depuis le 08/09/25)
- Phishing sur Josh Junon, mainteneur de 40 librairies fondamentales de Javascript (e.g. fonts de base, couleurs, …)
- Librairies infectées, téléchargées automatiquement par npm (car dépendances usuelles)
- Le virus :
  - Récupère tous les tokens de connexion du serveur npm infecté
  - Rend publics tous les repos git
  - Installe les packages npm infectés dans tous les repos Javascript trouvés et les push→ de plus en plus de repos infectés et téléchargés

Conséquences :

- 34 % de npm infecté
- ~ 3 milliards de téléchargements par semaine
- Les devs ne savent pas s'ils sont infectés (dépendances de dépendances)
- Exfiltration de données + cryptominers

https://www.exiger.com/perspectives/a-single-compromise-threatened-34-percent-of-npm/

1. Les enjeux de la sécurité des S.I.

Attaque d'hôpital en Allemagne par rançongiciel (2020)

- 9-10-11/09/2020
- Chiffrement de 30 serveurs de l'hôpital de Düsseldorf
- Exploit d'une vulnérabilité d'un VPN de Citrix
- Les attaquants ont réparé l'attaque en apprenant qu'ils attaquaient un hôpital
- 1ère mort civile (officielle) due à une cyberattaque (la personne serait sans doute morte sous peu sans ça...)

La source de l'attaque reste à déterminer.
La Russie est soupçonnée d'être à l'origine de l'attaque.

1. Les enjeux de la sécurité des S.I.

Les universités sont aussi ciblées !

Forum Général
Forum ForEva
Contacts

Espace étudiants

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

> **Poster un nouveau message** <

Liste des messages postés
pages 1 2 3 4 5 6 7 8 9 10

 # HACKED BY SWAN HACKED BY SWAN HACKED BY SWAN HACKED BY SWAN HACKED BY SWAN HACKED BY SWAN

Défacement de site

Vol de données personnelles

TheWMURChannel.com

Dartmouth Computer Hackers

POSTED: 4:07 PM EDT August 1, 2004

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

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

1. Les enjeux de la sécurité des S.I.

Les universités sont aussi ciblées !

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.

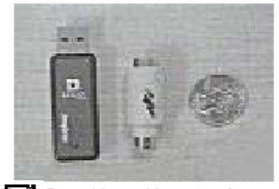
The student attended Clements High School, 4200 Elkins Dr., in the Fort Bend Independent School District.

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

Note des lecteurs: **5.0**/5

Rebond pour fraude externe

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

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

1. Les enjeux de la sécurité des S.I.

Les universités sont aussi ciblées !… pourquoi ???

- Réseaux avec de nombreuses informations sensibles
  - Données financières des étudiants et du personnel
  - Numéros de sécurité sociale
  - Recherche de haut niveau
- Sécurisation difficile
  - Préférence pour le libre accès
  - Équilibre entre faciliter l'échange d'idées et protéger la propriété intellectuelle
  - Nombreux points d'accès aux réseaux car beaucoup d'utilisateurs
  - Beaucoup d'appareils personnels utilisés
  - Difficulté de distinguer véritables menaces / activités bénignes

1. Les enjeux de la sécurité des S.I.

Les universités sont aussi ciblées !… pourquoi ???

- Défauts de la culture du libre accès
  - Étudiants se sentant peu responsables de leurs actions sur le réseau
  - Attaques d'ingénierie sociale très efficaces (via Twitter, Instagram… ou même Reddit ou ChatGPT)
- Stratégie pour protéger un tel réseau
  - Surveiller l'intérieur du réseau pour neutraliser les attaques déjà infiltrées, en complément de
  - Rechercher les menaces connues sur le périmètre du réseau

1. Les enjeux de la sécurité des S.I.

2023, passage d'un cap en France

D'après la gendarmerie, depuis janvier 2023, plus de **50 %** de l'argent obtenu par les criminels vient de cyberattaques.

1. Les enjeux de la sécurité des S.I.

D'après vous ?

Connaissez-vous des façons de gagner de l'argent avec un malware ?

1. Les enjeux de la sécurité des S.I.

Vols de données en 2014

- L'année 2014 a été l'année de tous les records en matière de fuite de données.

(infographie par www.silicon.fr)

Mais ça, c'était avant…

1. Les enjeux de la sécurité des S.I.

En 2017, les ransomwares

- But : obtenir le paiement d'une rançon
- Moyen : chiffre des données et les rend inutilisables
- Fort essor avec le développement des cryptomonnaies (Bitcoin, Monero, Electroneum,…)

- WannaCry (mai 2017) a coûté 7Md€, mais rapporté que 80k€ (0,13 % de payeurs)

  → coût important pour les cibles, peu rentable pour les attaquants

- Tendance : pas de déchiffrement, même si rançon payée…
- Aujourd'hui : beaucoup utilisés pour attaquer les hôpitaux dans les pics COVID, mais globalement moins utilisés

  (utilisateurs savent que la rançon ne sert à rien, la police a progressé, les antivirus ont progressé, ...)

1. Les enjeux de la sécurité des S.I.

D'après vous ?

Est-ce qu'on peut prendre une assurance pour être dédommagé en cas de ransomware ?

Techniquement, ça marche comment, un ransomware ?

1. Les enjeux de la sécurité des S.I.

En 2018, le cryptojacking

- But : produire (miner) de la cryptomonnaie
- Moyen : détournement de la puissance d'appareils

- Mise au point de cryptominers, malwares permettant de produire de la cryptomonnaie
- Fort essor depuis que ces outils sont devenus légers (fichier JavaScript chargé sur le navigateur Web)
  - Rapporte peu unitairement, mais
  - Utilisable à grande échelle (peu de contraintes sur les appareils contaminés)
  - mi-2018 : 40 % des entreprises touchées

1. Les enjeux de la sécurité des S.I.

En 2018, le cryptojacking

- Conséquences pour les entreprises
  - Perte de performance des systèmes compromis
  - Augmentation de la consommation d'énergie
    → forte augmentation des coûts

- Éditeurs de logiciels de sécurité bloquent les scripts de minage identifiés
  - Mais difficiles à identifier (empreinte faible, signature changeante, chargé dans la mémoire vive)
  - Moyen : étudier la consommation d'énergie et l'activité des processeurs
- L'utilisation de logiciels à jour permet en général d'éviter le cryptojacking

1. Les enjeux de la sécurité des S.I.

En 2019, des évolutions…

- Automatisation des attaques d'ingénierie sociales
  - Machine learning pour améliorer leur efficacité
- Moins de cryptominers
  - Baisse des taux des cryptomonnaies
  - Arrêt de Coinhive
  - Guerre entre logiciels de minage pour s'octroyer les ressources

    Concurrence : la taille du butin à gagner par minage n'a pas bougé, mais il y a plus de cryptominers → moins à gagner par personne
- Protection des données au cœur des entreprises
- Généralisation de la protection des données personnelles
- Intérêt croissant pour les équipements domestiques intelligents

1. Les enjeux de la sécurité des S.I.

Aujourd'hui

- Plus vraiment de « mode » en particulier : on trouve un peu de tout
- Il faut s'attendre à un nouveau type d'exploitation des attaques dans les années qui viennent

- Développement du « Malware as a Service » (parallèle avec « Software as a Service ») :
  - Entreprises de pirates informatiques (RH, recrutement, mutuelles, …) de centaines d'employés
  - Recherche et développement d'attaques informatiques
  - Mise à disposition de ressources / points d'entrées dans des SI piratés
  - Département de vente à des clients conscients ou inconscients de ce qu'ils achètent

1. Les enjeux de la sécurité des S.I.

Quelques exemples d'attaques « du futur »

Cyberattaques sur la voiture connectée

Exemple : Prise de contrôle du système de frein

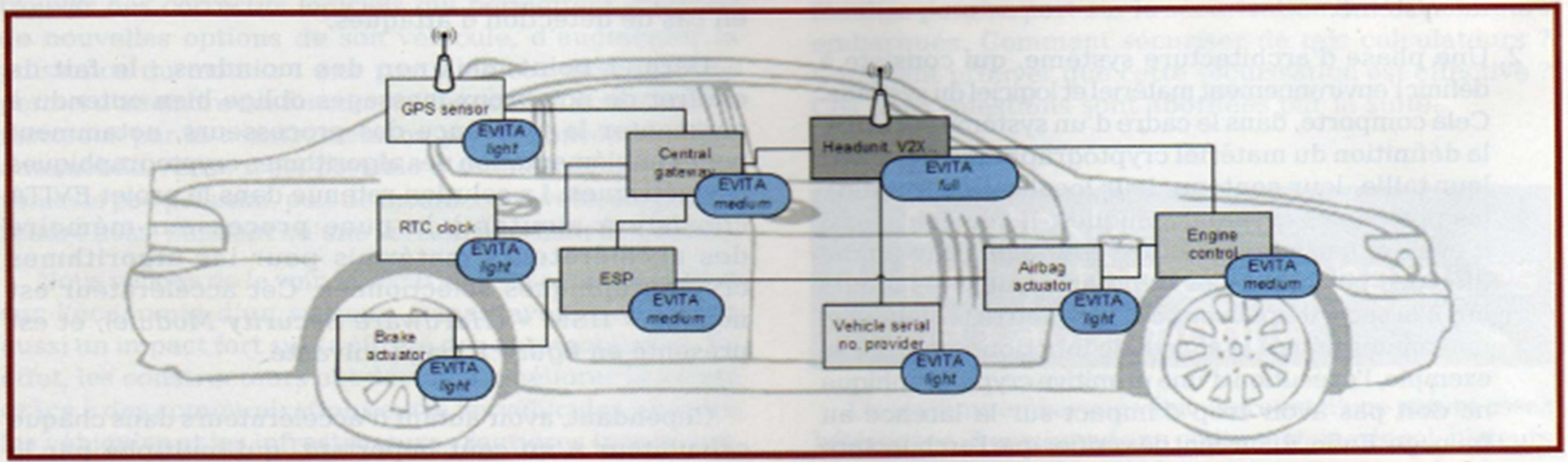
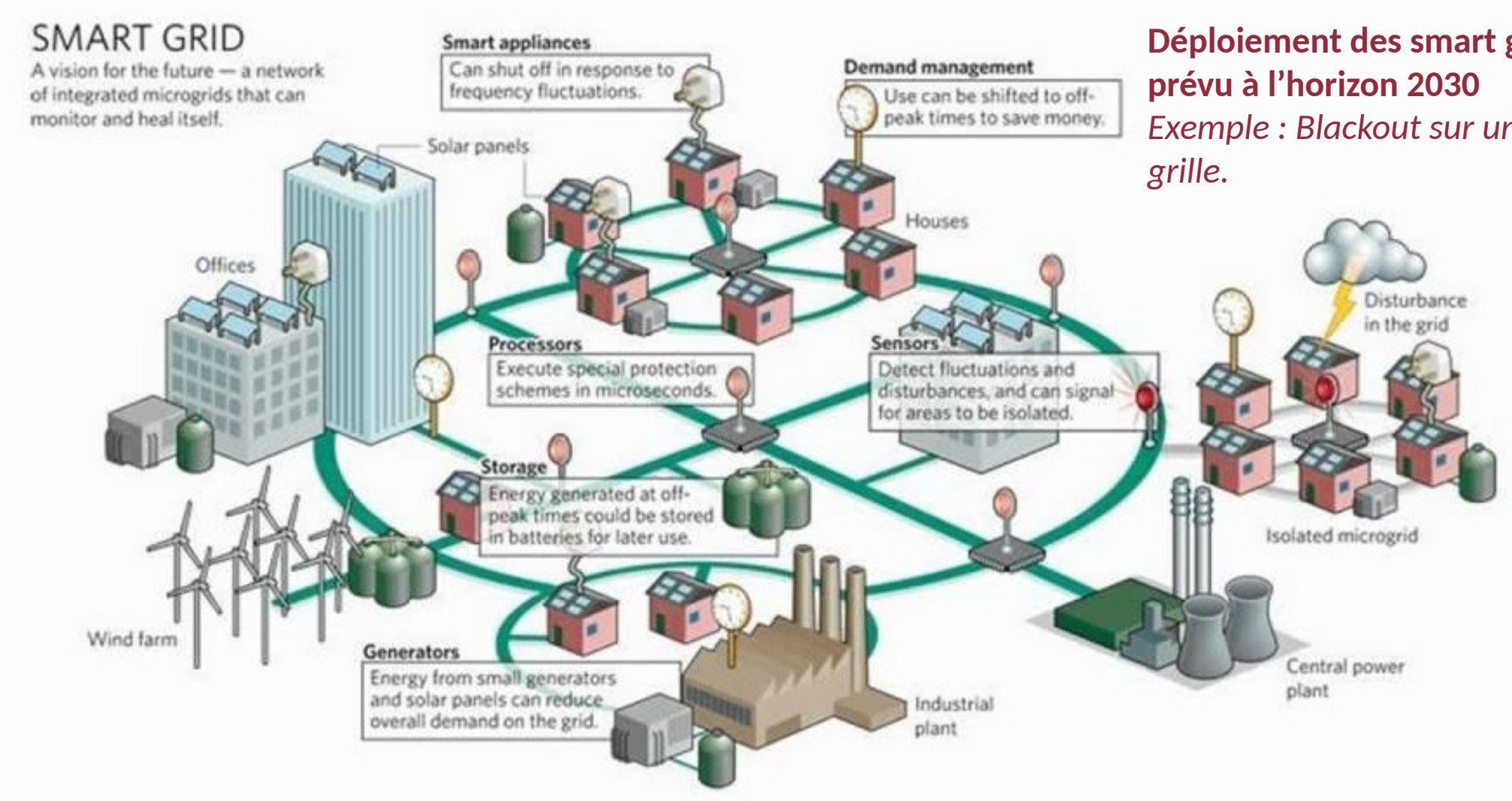


Figure 2 : Les modules de sécurité HSM sont ajoutés à tout calculateur embarqué. Selon la nature du calculateur, une version simplifiée du HSM peut être implantée afin de réduire le coût de l'architecture.

1. Les enjeux de la sécurité des S.I.

Quelques exemples d'attaques « du futur »



Déploiement des smart grid prévu à l'horizon 2030

Exemple : Blackout sur une grille.

1. Les enjeux de la sécurité des S.I.

Conséquences du Covid-19 !

- Développement massif de solutions en ligne (achat, télétravail, communication)
- Beaucoup de nouveaux utilisateurs d'Internet inexpérimentés

Apprendre d'un exemple : Cybercriminalité en lien avec l'épidémie [Interpol]

- **Escroqueries en ligne + hameçonnage**
  - Ex : [Trend Micro] 907.000 messages d'hameçonnage thématiques (médicaments, mesures fiscales, aides d'urgence) utilisant des logiciels malveillants comme Emotet, Trickbot et Cerberus
- **Malwares pour désorganiser** (rançongiciels et dénis de service distribué)
  - Basés surtout sur Cerber, NetWalker et Ryuk
- **Malwares de contrôle à distance (chevaux de Troie / reverse shell)**
  - Forte propagation grâce à Emotet, 13% des organisations touchées dans le monde
  - Trickbot était souvent associé aux incitations liées à l'épidémie

Leçon : les attaques de masses ne sont pas originales – faciles à identifier puis contrer

1. Les enjeux de la sécurité des S.I.

Apprendre d'un exemple : Cybercriminalité en lien avec l'épidémie [Interpol]

- **Mésinformation** (fake news) ***[notez : classé comme cybercriminel]***
  - Beaucoup de théories du complot
  - Thèmes les plus récurrents :
    - L'action des autorités publiques
    - La propagation dans la population
    - Les informations générales d'ordre médical
    - Les acteurs de premier plan
    - Les théories du complot
    - Le mode de transmission du virus
    - La préparation de la population
    - La mise au point d'un vaccin
    - ...
  - Diffusion par les médias sociaux (WhatsApp, Facebook, Twitter, …)

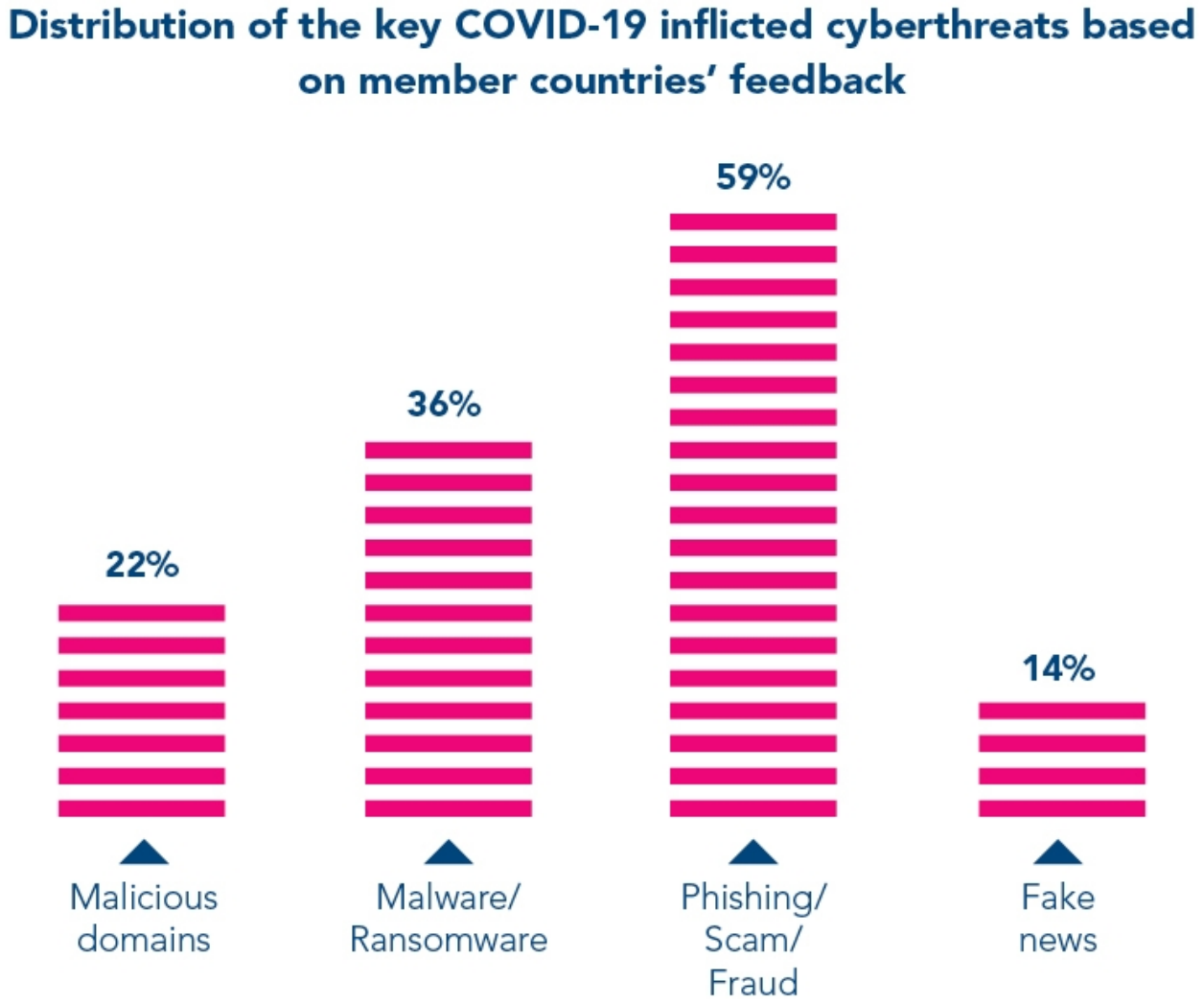
1. Les enjeux de la sécurité des S.I.

D'après vous ?

D'après vous, quel type d'attaque a été le plus populaire lors de l'explosion de la pandémie Covid ?

1. Les enjeux de la sécurité des S.I.

Répartition de ces menaces [Interpol]



1. Les enjeux de la sécurité des S.I.

Et si vous voulez avoir une liste d'attaques récentes, il suffit d'ouvrir un site d'information…

Par exemple, https://www.20minutes.fr/dossier/cyberattaque

- 05-20/09 : SFR, Cultura, assurance retraite... victimes de fuites de données
- 19/09 : Hackers iraniens fuitent données de campagne de Trump
- Début 09 : journal La Croix, université Paris-Saclay paralysés
- 05/08 : Grand Palais victime de rançongiciel
- JO : 548 événements de cybersécurité
  - https://cyber.gouv.fr/actualites/bilan-cyber-des-jeux-olympiques-et-paralympiques-de-paris-2024

Pas uniquement des attaques :

- 08/09/22 : Les assureurs pourront rembourser la rançon d'une cyberattaque
- 2022-2025 : directive européenne NIS2 (suite du RGPD)

1. Les enjeux de la sécurité des S.I.

Il y a des activités informatiques en zone grise, pas (encore?) classées comme criminelles :

- Copie du fonctionnement d'un logiciel (le code, l'art, les dialogues, tout ça est protégé par le droit d'auteur, mais pas le fonctionnement)
- Copie d'un site Web (idem)
- Copie / enregistrement des données publiques d'un site Web (e.g. site de vente en ligne). Ça s'appelle du ***scraping***.
- …

<u>C'est techniquement intéressant :</u>

- Pas de protection légale → bataille **technique** pour protéger / copier les logiciels et données publiques

1. Les enjeux de la sécurité des S.I.

Ça bouge à Nancy !

Exemple 1 : **Assises universitaires Droit et Cybersécurité** du 04/07/22 à Nancy (1ère rencontre mondiale entre ces domaines), où une question majeure était de faire évoluer le droit du domaine.
2è édition : le 26 octobre 2023, centre Prouvé (près de la gare)

https://assisescyber.loria.fr/

Il y avait du monde : général en charge de l'armée cyber, commandant en charge de la police cyber, ministres, préfets, vice-président de l'ANSSI, vice-président de la CNIL, des professeurs de droit, Antoine Joux et Véronique Cortier, …, vice-président de France Assureurs
Très productif et visiblement le début d'une longue série de rencontres !

Exemple 2 : l'ANSSI et la région Grand-Est ont signé la création d'un **centre ANSSI CSIRT** (centre d'intervention en cas d'attaque informatique sur des entreprises civiles) en Grand-Est, et Nancy a été choisie ! Ça a ouvert début 2023.

Exemple 3 : création d'un **Campus Cyber** Grand-Est, dont le cœur est à Nancy ! Ouvert début 2024. Rencontres : entreprises, administrations, chercheurs, ...

1. Les enjeux de la sécurité des S.I.

Tendances actuelles : l'IA

Disclaimer :

« Intelligence Artificielle » c'est un buzz-word de commerciaux, vague exprès pour que tout puisse rentrer dedans.

Entre informaticiens, faisons l'effort de dire de quoi on parle.

D'après vous ?

C'est quoi l'IA

1. Les enjeux de la sécurité des S.I.

Tendances actuelles : l'IA

Intelligence artificielle :
Façon sexy de dire **« statistiques assistées par ordinateur »**.
Ce n'est pas rien : les statistiques modernes, c'est une science inventée en France dans les années 1700 qui a été l'un des piliers de la révolution industrielle.

Statistiques :
Science dont le but est d'approximer une règle générale à partir de cas particuliers : on échantillonne des cas d'exemple et on en déduit une formule générale (approximée).

En gros :
Les statistiques, c'est la **solution du bourrin** : plutôt que de réfléchir pour comprendre le problème, on teste plein de fois sur des exemples et on espère que ça donne une règle pas trop mal pour le cas général.
= **Remplacer la réflexion par beaucoup de données et de puissance de calcul** : adapté aux ordinateurs.
Pratique pour résoudre des petits problèmes faciles (ne pas passer du temps sur un problème qu'on n'a à gérer qu'une fois et sur lequel on n'a pas besoin d'une solution optimale).

1. Les enjeux de la sécurité des S.I.

Tendances actuelles : l'IA

Grandes familles d'outils en IA (non-exhaustif) :

- Algorithmes gloutons d'optimisation (descente de gradient, recuit-simulé, etc)
  très mathématiques, il faut d'abord modéliser le problème avec des math, pas toujours pratique mais bien compris.
- Algorithmes sans mémoire / markoviens (Monte-Carlo, Las Vegas, etc)
  Très appréciés en finance par exemple.
- Apprentissage « profond » (réseaux de neurones, etc)
  - statistiques sur des graphes
  - opérations simplissimes + énorme quantité de données
  - processeurs ultra-parallélisés avec opérations élémentaires, type GPU
  - Simples d'utilisation, pas de mathématiques dures, efficace sur ordin → tendance !
- IA « générative » (GPT, etc) : apprendre à générer du contenu multimédia
  - Généralement algos « profonds »

1. Les enjeux de la sécurité des S.I.

Tendances actuelles : l'IA

Pour la sécu !

En attaque :

- Automatiser les attaques avec des bases de données d'attaques connues.
- Imiter des humains : phishing avancé automatisé.

En défense :

- Apprendre à quoi « ressemble une attaque », ou à quoi « ressemble un logiciel malveillant » (e.g. dans les antivirus).

Limitation :

L'IA est adaptée aux problèmes statistiques simples (très courants).
Mais il y a des problèmes difficiles ! Par exemple, la sécurité informatique repose sur la cryptographie dont les problèmes sont difficiles. L'IA est inefficace sur la cryptographie.

1. Les enjeux de la sécurité des S.I.

Tendances actuelles : l'IA

Note sans rapport avec la SSI :

Les IA génératives, c'est pratique mais :

- C'est cher en énergie
- Il faut beaucoup de données (pas le cas de tous les problèmes)
- Entraîné sur Internet :
  L'IA a un « niveau moyen d'Internet ». C'est bien sur certaines choses (informatique de base, développement, mise en forme de documents, contenus multimédias).

  Pas fou sur les sujets spécialisés !
  IA ~ étudiant de master avec 14/20 de moyenne
- Bossez bien en master, vous ferez mieux qu'une IA !

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

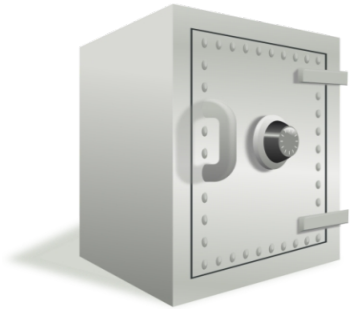
2. Les besoins de sécurité

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

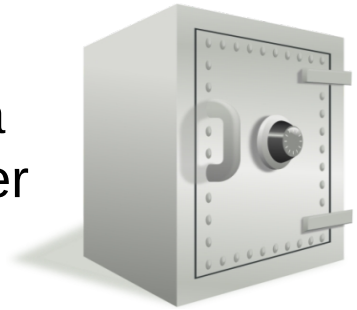
2. Les besoins de sécurité

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

Utile par exemple pour suivre les actions d'un attaquant

2. Les besoins de sécurité

D'après vous ?

Quelle différence entre sécurité et sûreté ?
(security vs safety)

2. Les besoins de sécurité

c. Différences entre sûreté et sécurité

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

Sûreté

Protection contre les dysfonctionnements et accidents involontaires

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

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

Parades : sauvegarde, dimensionnement, redondance des équipements…

Sécurité

Protection contre les actions malveillantes volontaires

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

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

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

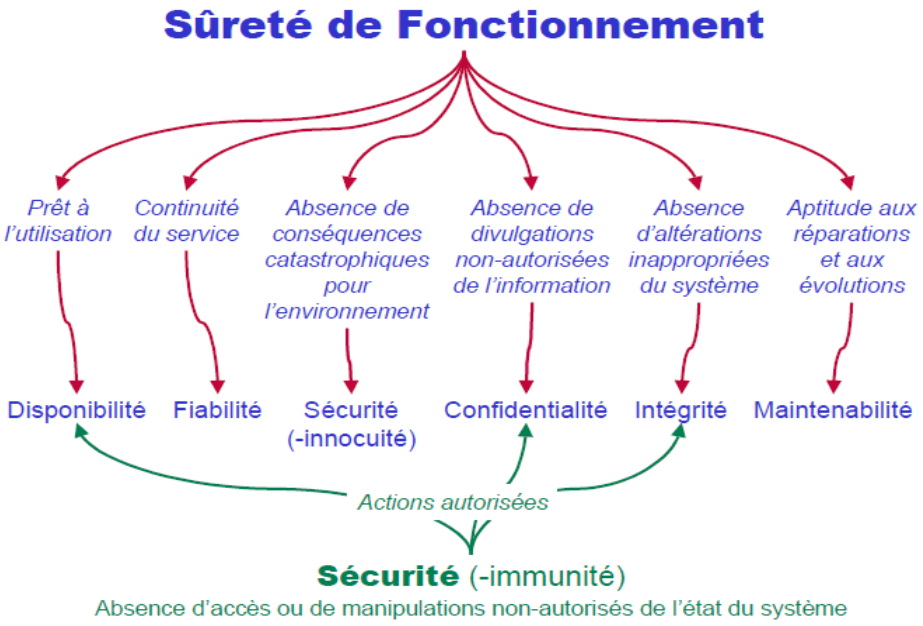
2. Les besoins de sécurité

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

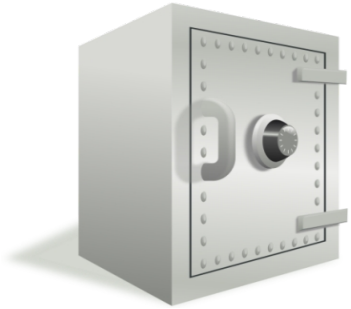
d. Exemple d'évaluation DICP

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 connaitre ses services au public

Intégrité = **Très fort**

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

Serveur web

Confidentialité = **Faible**

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

Preuve = **Faible**

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

2. Les besoins de sécurité

e. Mécanismes de sécurité pour atteindre les besoins DICP

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

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

2. Les besoins de sécurité

e. Mécanismes de sécurité pour atteindre les besoins DICP

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

2. Les besoins de sécurité

e. Mécanismes de sécurité pour atteindre les besoins DICP

Ce tableau est un bon résumé des mécanismes de sécurité
C'est un élément à connaître par cœur.

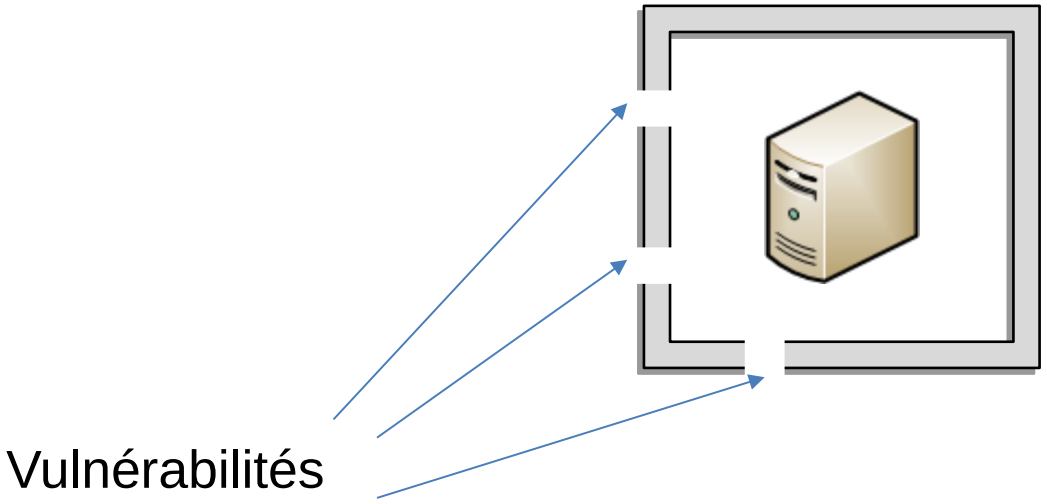
3. Notions de vulnérabilité, menace, attaque

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 »

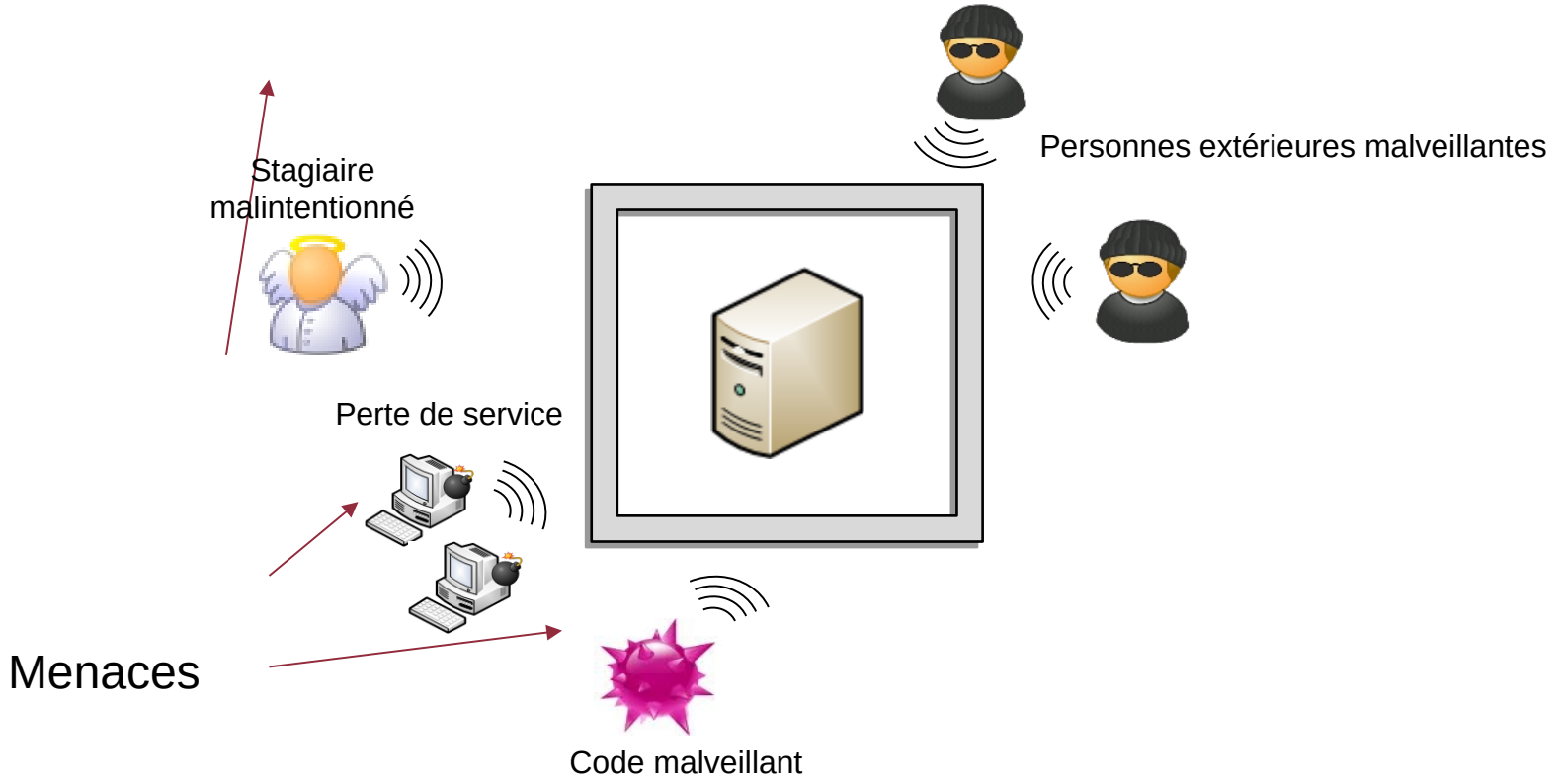
- **Vulnérabilité**
- **Faiblesse au niveau d'un bien** (au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation du bien).



3. Notions de vulnérabilité, menace, attaque

b. Notion de « Menace »

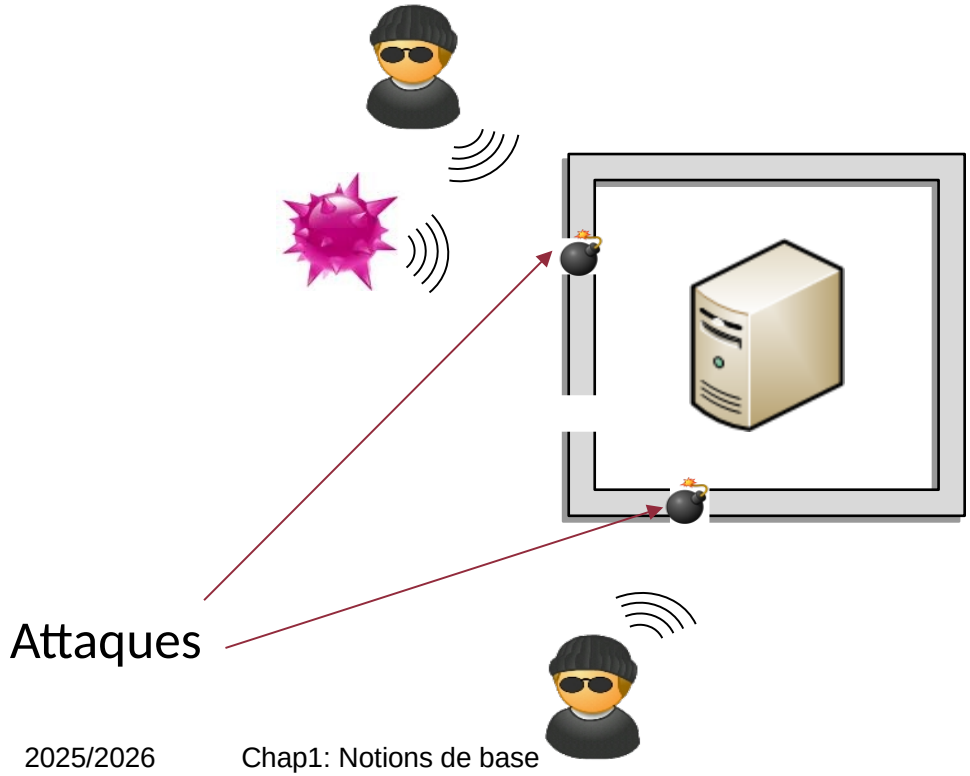
- **Menace**
- **Cause *potentielle* d'un incident**, qui pourrait entraîner des dommages sur un bien si cette menace se concrétisait.



3. Notions de vulnérabilité, menace, attaque

c. Notion d'« Attaque »

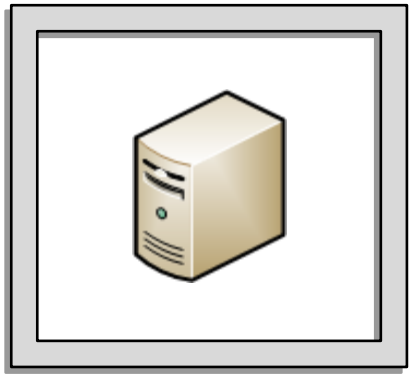
- **Attaque**
- **Action malveillante** destinée à porter atteinte à la sécurité d'un bien. Une attaque représente la **concrétisation d'une menace**, et nécessite **l'exploitation d'une vulnérabilité.**



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 (Virtual Network Computing)

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

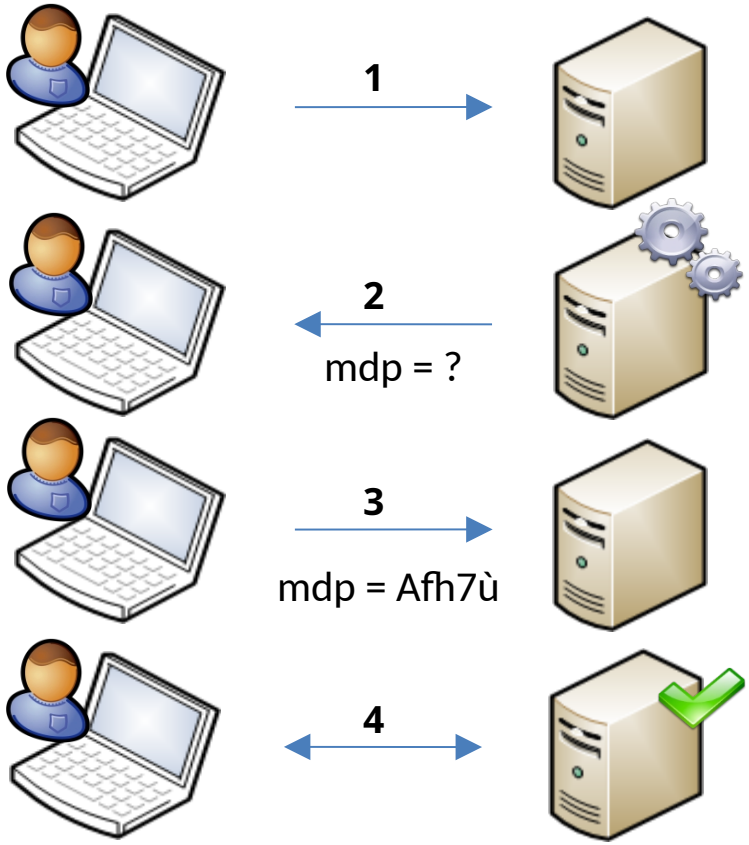
- La vulnérabilité décrite dans les planches suivantes est corrigée depuis de nombreuses années. Elle est symptomatique d'une **vulnérabilité dans la conception d'une application.**
- L'application permet en temps normal à un utilisateur de se connecter à distance sur une machine pour y effectuer un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

3. Notions de vulnérabilité, menace, attaque

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

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

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



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

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

Référence : CVE-2006-2369

3. Notions de vulnérabilité, menace, attaque

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

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

1

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

2

mdp = ?

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

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 »

3

authent = NON

4

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

Référence : CVE-2006-2369

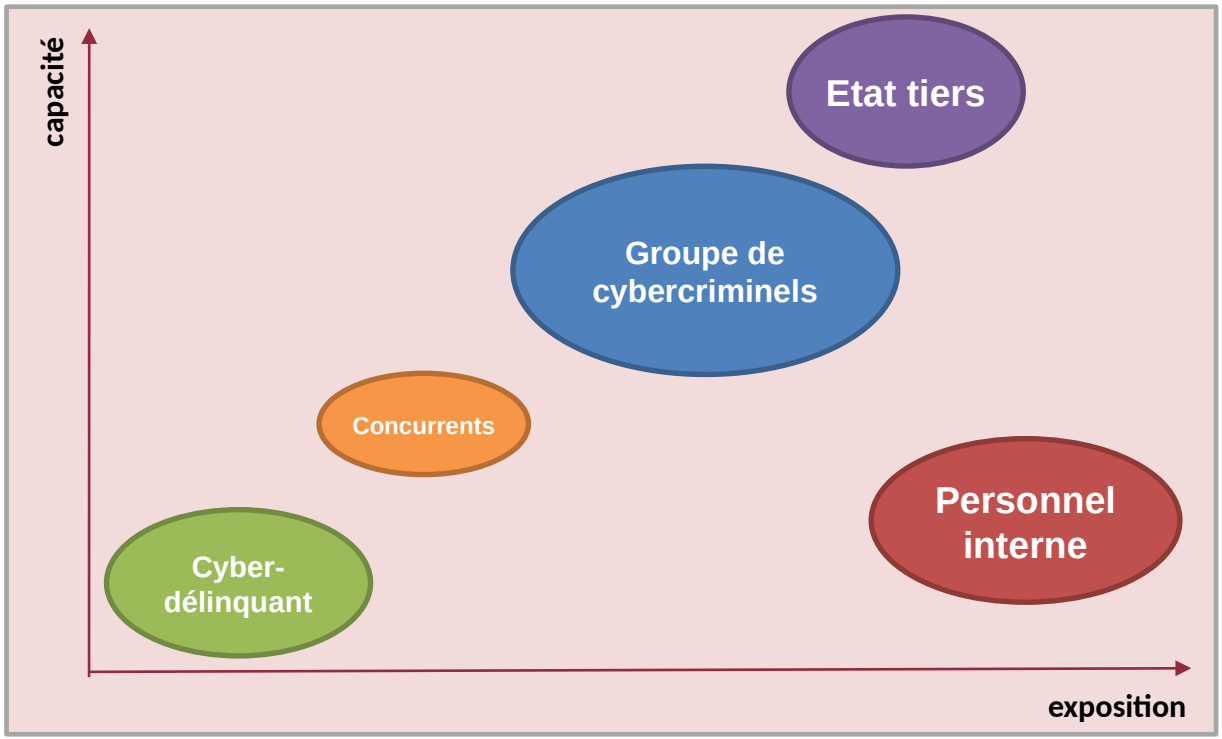
La vulnérabilité se situe ici : le serveur ne vérifie pas que le type d'authentification retourné par le client correspond à celui demandé. A la place, il vérifie simplement que l'authentification est correcte (et « authent = NON » est effectivement une authentification qui est toujours correcte)

4. Panorama de quelques menaces

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

4. Panorama de quelques menaces

a. Sources potentielles de menaces



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

<u>Capacité</u>
degré d'expertise et ressources de la source de menaces

<u>Exposition</u>
opportunités et intérêts de la source de menaces

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

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

4. Panorama de quelques menaces

b. Panorama de quelques menaces

Hameçonnage & ingénierie sociale

Fraude interne

Violation d’accès non autorisé

Virus informatique

Déni de service distribué

4. Panorama de quelques menaces

c. Hameçonnage & ingénierie sociale

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

1. Réception d'un mél 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 toute autre donnée sensible) saisie par le client sur le faux site

4. Panorama de quelques menaces

c. Hameçonnage & ingénierie sociale

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

- pour dérober directement des informations confidentielles, ou
- pour introduire des logiciels malveillants dans le système d'information

par téléphone

par réseaux sociaux

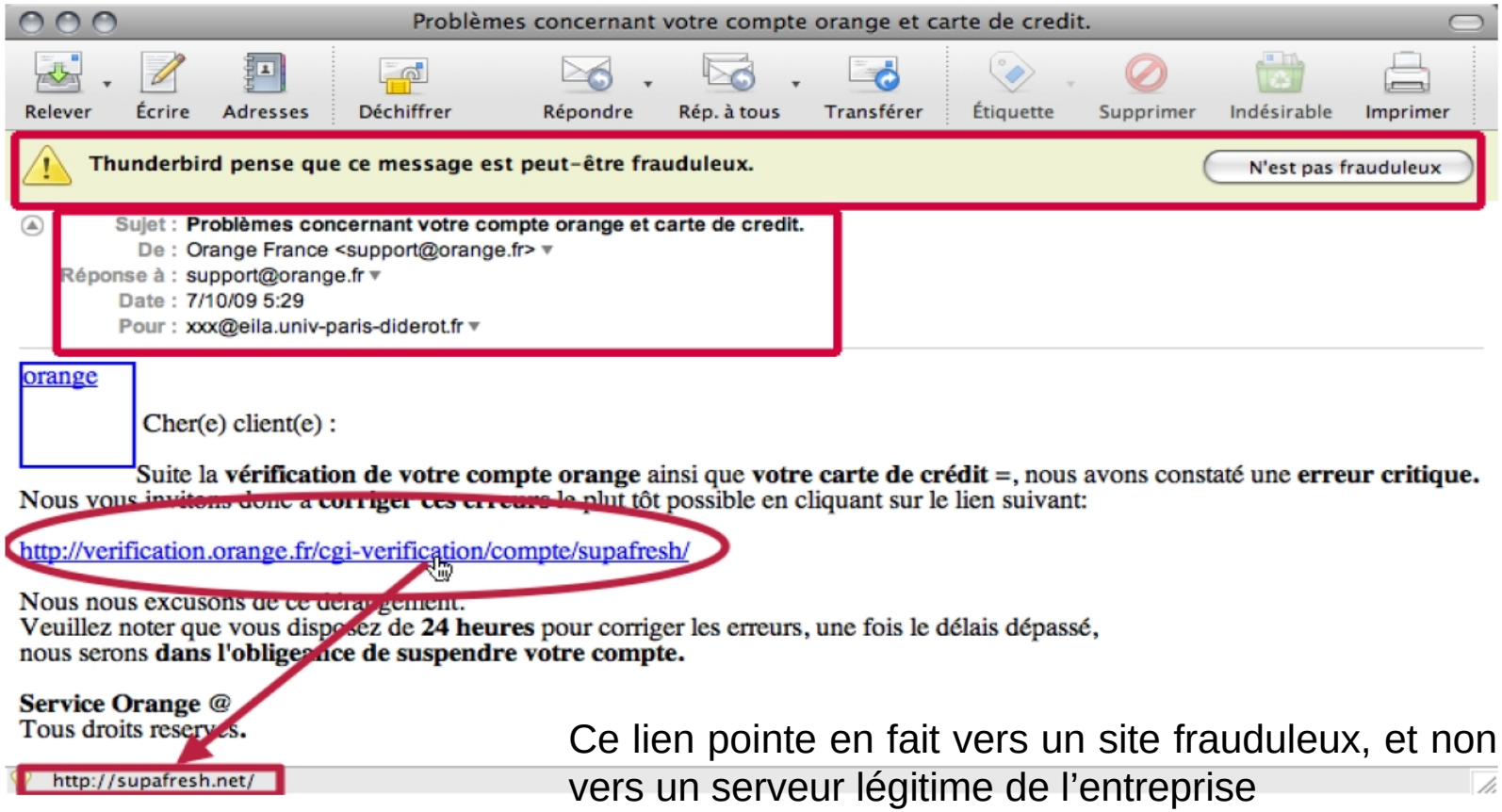
par mél

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…



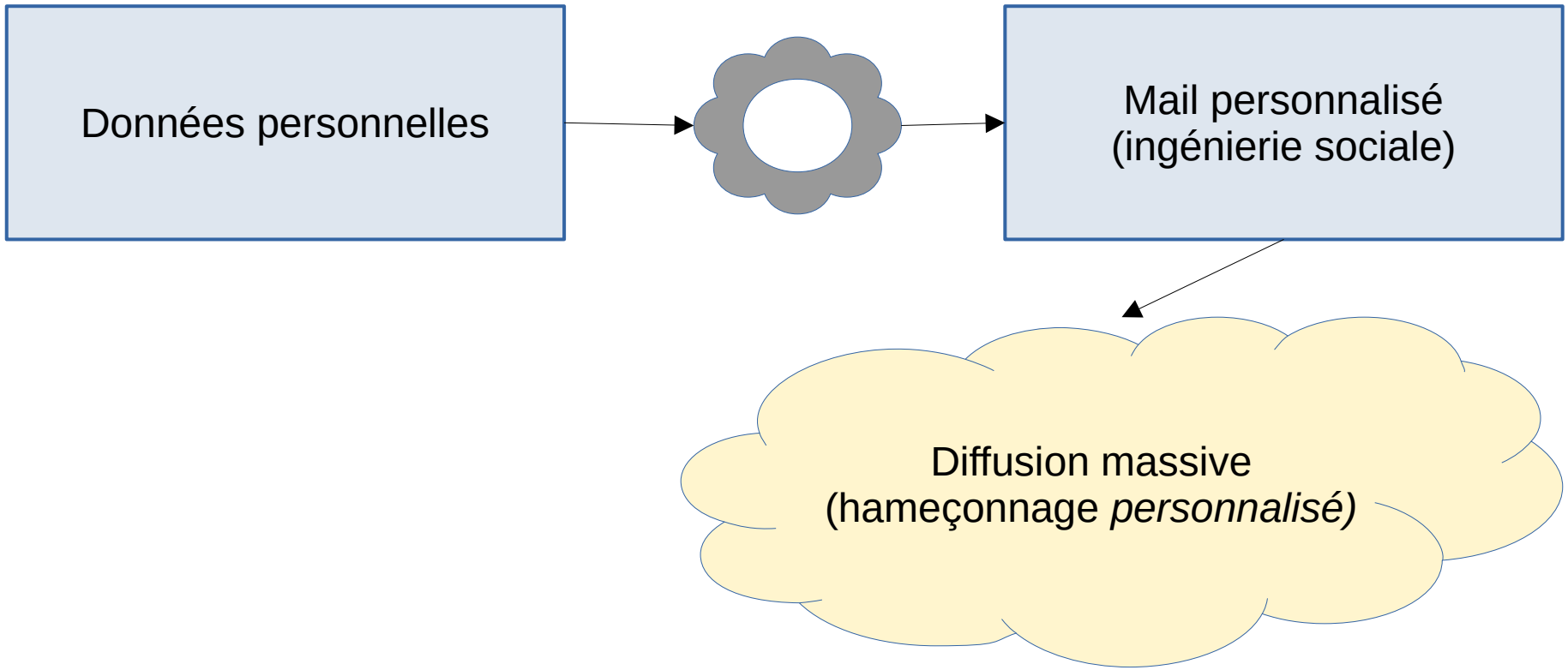
Ce lien pointe en fait vers un site frauduleux, et non pas vers un serveur légitime de l'entreprise

4. Panorama de quelques menaces

c. Hameçonnage & ingénierie sociale

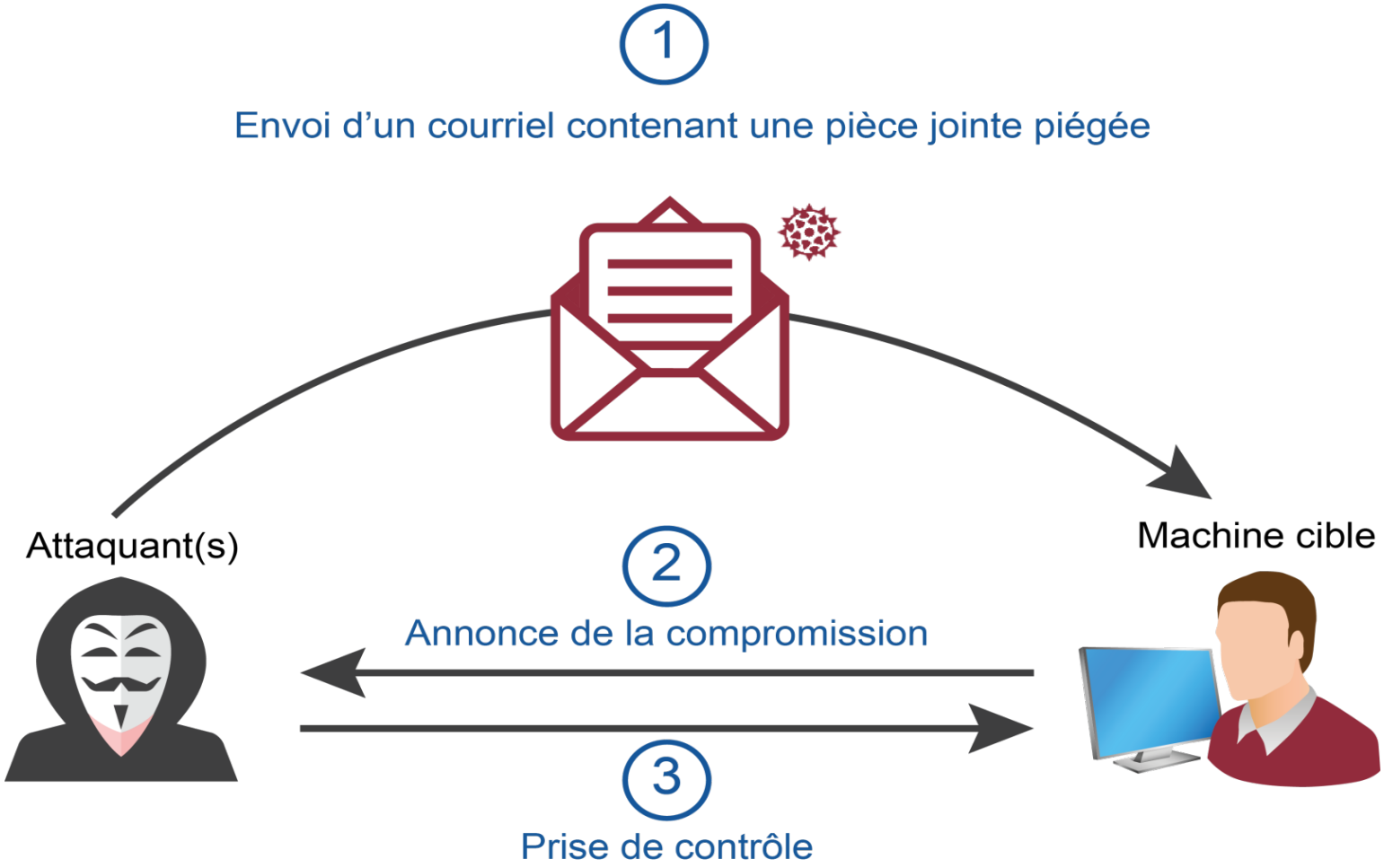
Hameçonnage, ingénierie sociale et IA

La publicité récente autour de l'IA générative (ChatGPT et consorts) donne des idées neuves :



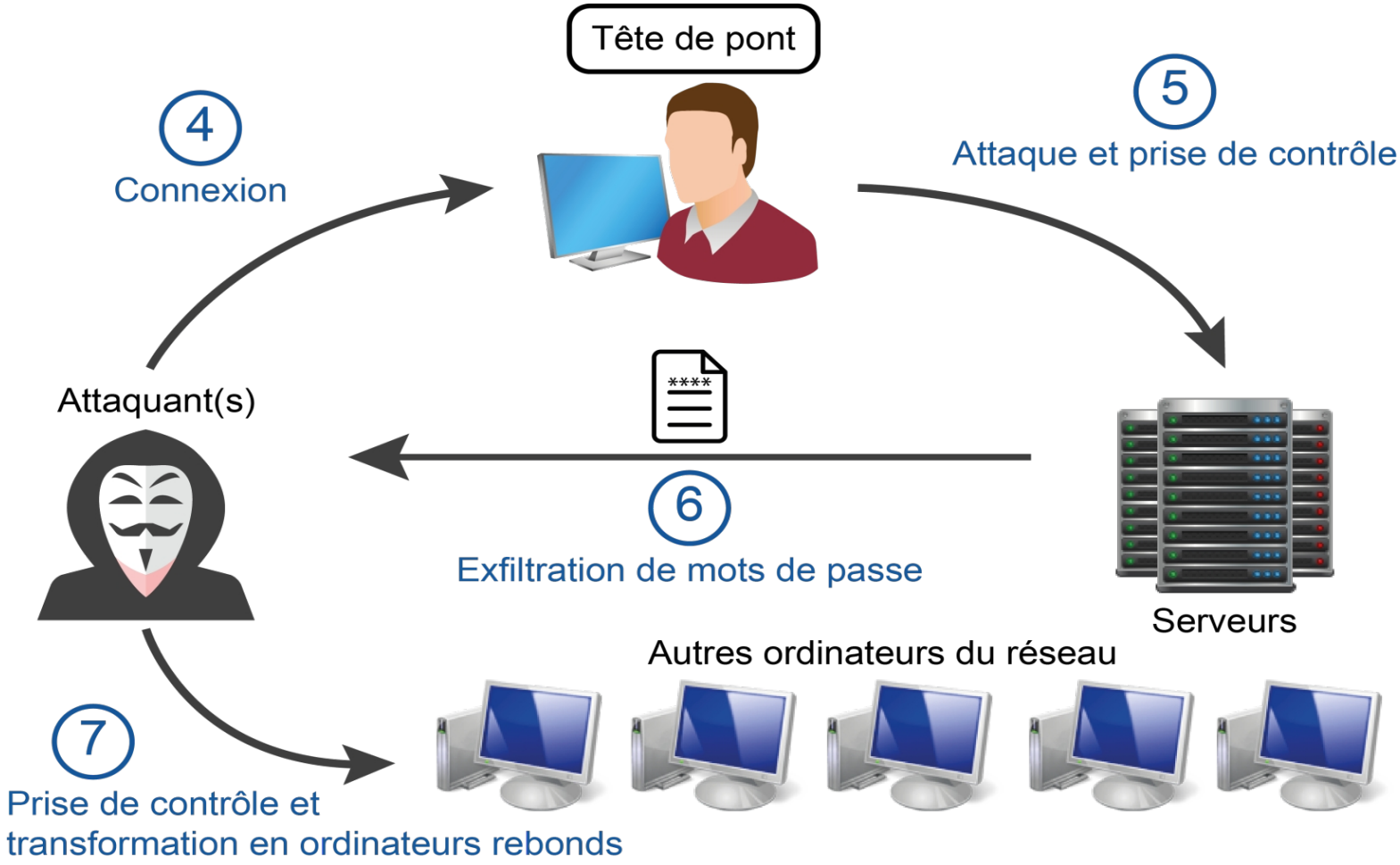
4. Panorama de quelques menaces

d. Déroulement d'une attaque avancée



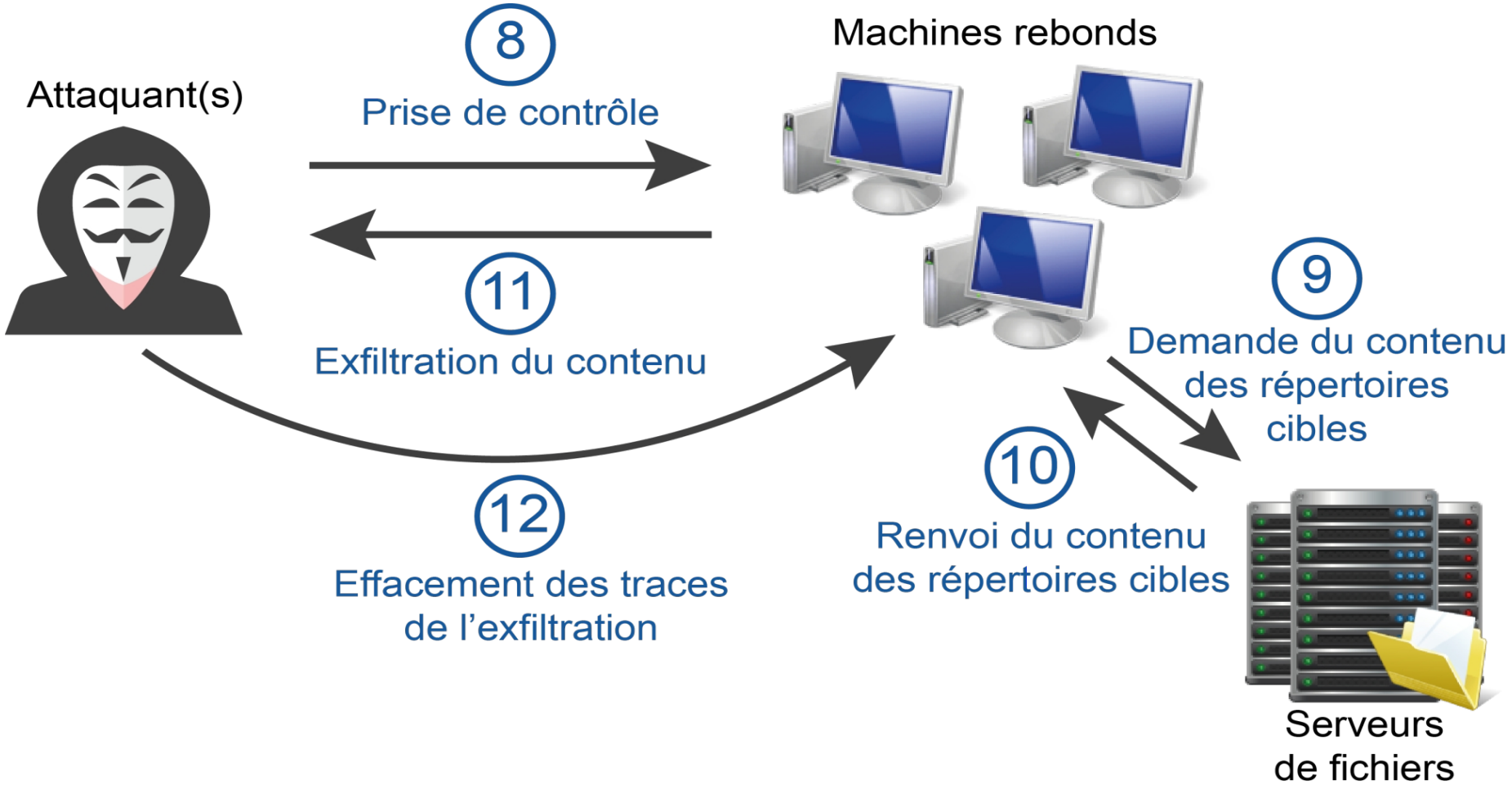
4. Panorama de quelques menaces

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 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.

http://www.wsj.com/articles/apple-celebrity-accounts-compromised-by-very-targeted-attack-1409683803

4. Panorama de quelques menaces

e. Fraude interne

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

Catégories de fraudeurs

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

Vulnérabilités

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

Typologies des fraudes

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

4. Panorama de quelques menaces

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

Des mots de passe simples ou faibles (notamment sans caractères spéciaux comme « ! » ou « _ » et des chiffres) permettent, entre autres, 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.

En pratique :

Longueur > complexité

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

D'après vous ?

Vous utilisez des Active Directory au quotidien ?

À mon sens, Active Directory mériterait aujourd'hui une UE complète (niveau M1), mais on fera sans.

4. Panorama de quelques menaces

g. Virus informatique

Les **virus (*malwares qui se reproduisent automatiquement*)** sont 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

D'après vous ?

C'est quoi un DDoS ?

4. Panorama de quelques menaces

h. Déni de service distribué (DDoS)

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

… une menace majeure et en augmentation pour les sites Internet

34,5 heures
durée moyenne d'une attaque

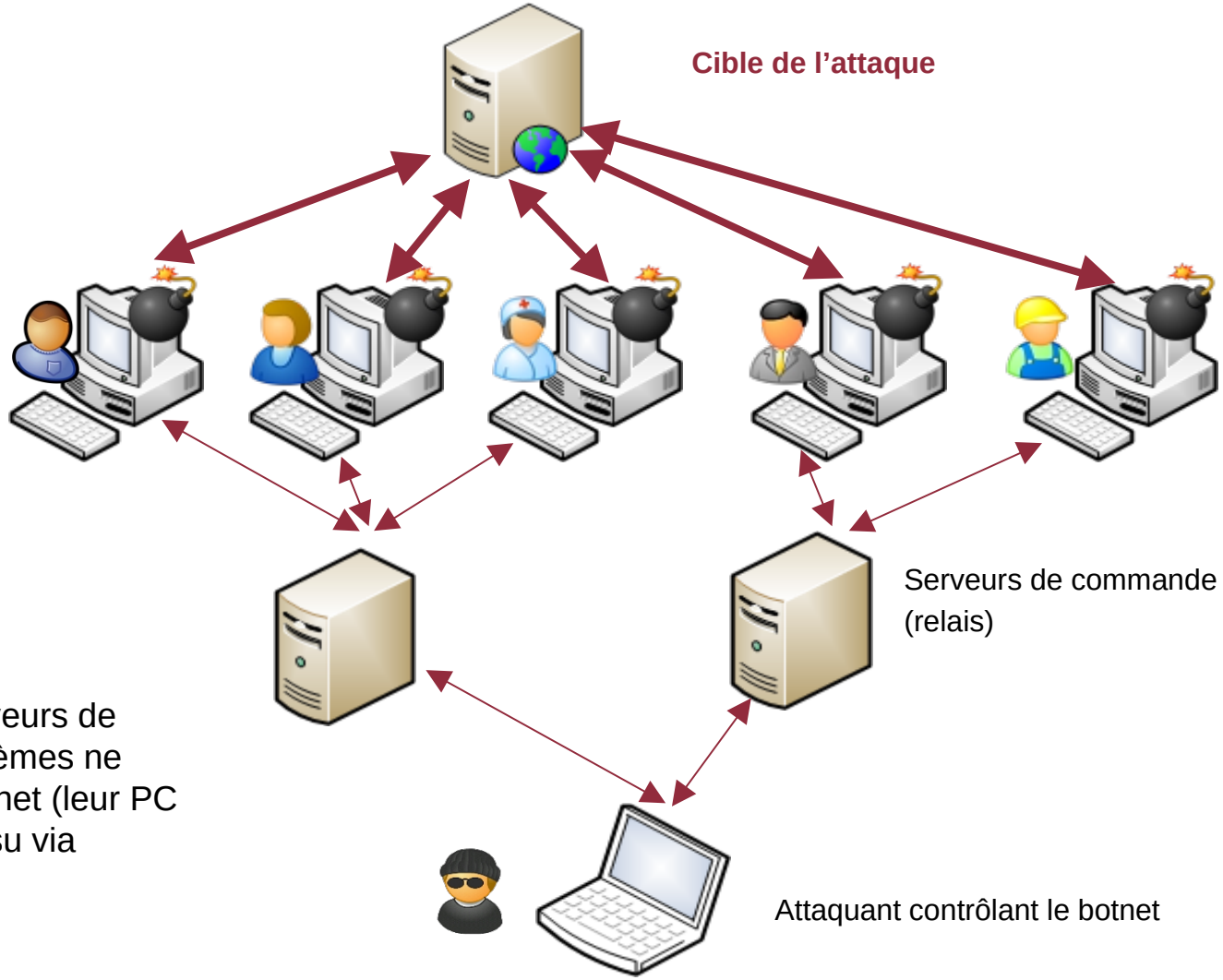
48,25 Gbps
bande passante moyenne d'une attaque

75 % des attaques au niveau infrastructure
25% des attaques au niveau application

4. Panorama de quelques menaces

i. Illustration d'un réseau de botnets

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



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

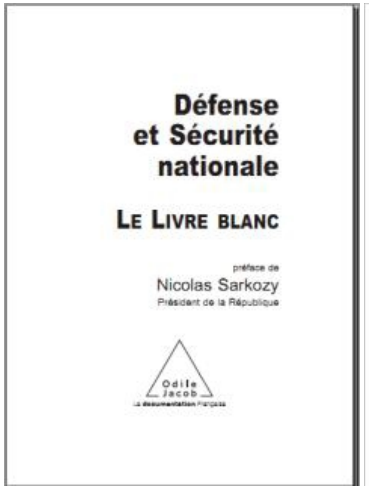
5. Le droit des T.I.C. et l'organisation de la cybersécurité en France

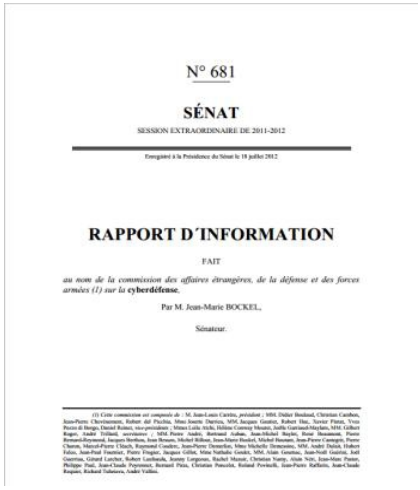
a) L'organisation de la sécurité en France
b) Le contexte juridique
c) Le droits des T.I.C.
d) La lutte contre la cybercriminalité en France
e) Le rôle de la CNIL : La protection des données à caractère personnel

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

a. L'organisation de la sécurité en France

Cyberdéfense : un véritable enjeu de sécurité nationale





« **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)*

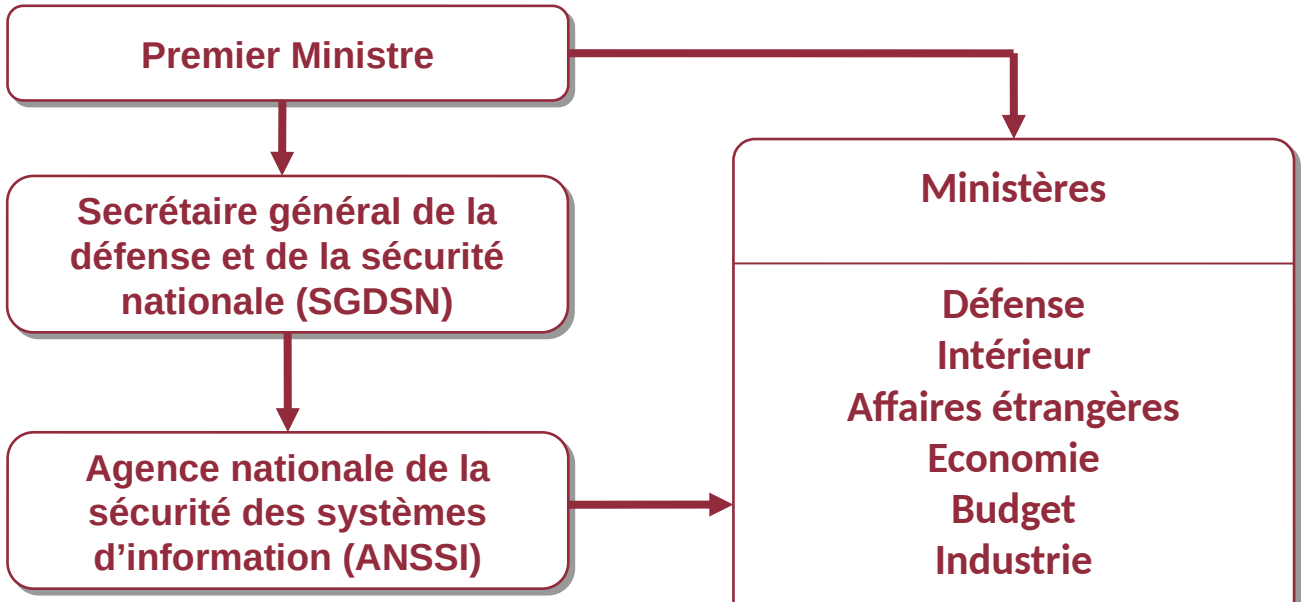
« Le développement de capacités de cyberdéfense militaire fera l'objet ***d'un effort marqué*** *» (Chapitre 7, Les moyens de la stratégie, livre blanc 2013)*

« Depuis janvier 2022, ***plus de 50 % de l'argent des criminels vient d'attaques informatiques***. *» (Général Marc Boget, Commandant de la Gendarmerie dans le Cyberespace, Nancy 2022)*

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

a. L'organisation de la sécurité en France

Organisation interministérielle :



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

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

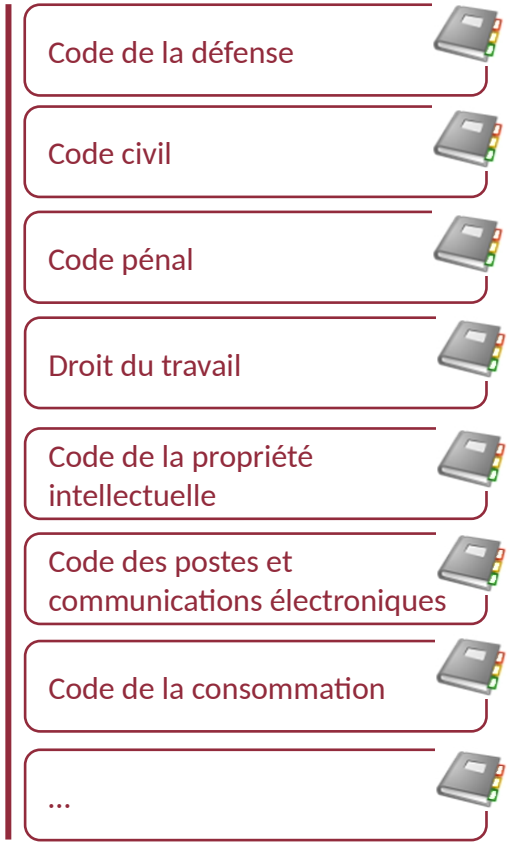
Cybercriminalité

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

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

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

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

d. La lutte contre la cybercriminalité en France

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

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

Jurisprudence sur la définition des STAD : Le réseau Orange (ex-FT), 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

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

f. LCEN

- Loi pour la confiance dans l’économie numérique
- 21 juin 2004
- Loi française (transposition de la directive européenne de 2000)
- E-commerce, vie privée
- Objectif : espace commercial sans frontières pour l’UE

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

f. LCEN

- Loi pour la confiance dans l’économie numérique
- 21 juin 2004
- Loi française (transposition de la directive européenne de 2000)
- E-commerce, vie privée
- Objectif : espace commercial sans frontières pour l’UE

6. Avènement du RGPD

Règlement Général sur la Protection des Données (25/05/2018)

- Simplifie les formalités auprès de la CNIL
- Responsabilité des organismes renforcée
- Doivent assurer une protection optimale des données à tout instant
- Doivent pouvoir démontrer la protection mise en œuvre

https://www.cnil.fr/fr/reglement-europeen-protection-donnees

6. Avènement du RGPD

Mise en œuvre

a. Désigner un pilote
b. Cartographier les traitements de données personnelles
c. Prioriser les actions à mener
d. Gérer les risques
e. Organiser les processus internes
f. Documenter la conformité

6. Avènement du RGPD

a. Désigner un pilote

Pour piloter la gouvernance des données personnelles de la structure.

→ délégué à la protection des données (DPO)

Mission :

- Informer et conseiller le responsable de traitement
- Contrôler le respect du règlement et du droit national
- Conseiller l'organisme (études d'impact sur la protection des données ; exécution)
- Coopérer avec l'autorité de contrôle (point de contact)

6. Avènement du RGPD

b. Cartographier les traitements

Tenir un registre des traitements recensant

- les différents traitements de données personnelles
- les catégories de données personnelles traitées
- les objectifs des traitements de données
- les acteurs (internes ou externes) traitant ces données
- les flux (origine et destination) des données

→ Qui ? Quoi? Pourquoi ? Où ? Jusqu'à quand ? Comment ?

6. Avènement du RGPD

c. Prioriser les actions à mener

- Pour chaque traitement identifié, définir les actions à mener pour se conformer à la loi
- Prioriser selon les risques provoqués par les traitements sur les libertés des personnes concernées
- Points d'attention
  - Vérifier que seules les données strictement nécessaires sont collectées et traitées
  - Identifier la base juridique pour chaque traitement
  - Réviser les mentions d'information
  - Vérifier les clauses contractuelles avec les sous-traitants
  - Prévoir les modalités d'exercice des droits des personnes concernées
  - Vérifier les mesures de sécurité mises en place

6. Avènement du RGPD

d. Gérer les risques

- Analyse d'impact relative à la protection des données (AIPD)
  - Aide à construire des traitements respectueux de la vie privée
  - Repose sur
    - Principes et droits fondamentaux « non négociables »
    - Gestion des risques sur la vie privée
  - Contient
    - Description du traitement étudié et finalités
    - Évaluation de la nécessité et proportionnalité des opérations de traitement
    - Évaluation des risques pour les droits et libertés, et mesures envisagées pour faire face aux risques

6. Avènement du RGPD

d. Gérer les risques

- Critères de détermination du niveau de risque
  - Évaluation ou notation
  - Décision automatisée avec effet juridique
  - Surveillance systématique
  - Données sensibles ou hautement personnelles
  - Données personnelles traitées à grande échelle
  - Croisement d’ensemble de données
  - Données concernant des personnes vulnérables
  - Usage innovant ou nouvelles solutions technologies ou organisationnelles
  - Exclusion du bénéfice d’un droit, d’un service ou contrat

6. Avènement du RGPD

d. Gérer les risques

- Qui participe ?
  - Le responsable de traitement
  - Le délégué à la protection des données
  - Les sous-traitants
  - Les métiers (RSSI, MOA, MOE)
  - Les personnes concernées

6. Avènement du RGPD

e. Organiser les processus internes

- Prendre en compte la protection des données personnelles dès la conception
- Sensibiliser et organiser la remontée d'information
- Traiter les réclamations et demandes des personnes exerçant leurs droits
- Anticiper les violations de données

6. Avènement du RGPD

f. Documenter la conformité

- Doc sur les traitement de données personnelles
  - Registre des traitements
  - AIPD
  - Encadrement des transferts de données hors UE
- Information des personnes
  - Mentions d'information
  - Modèles de recueil des consentements
  - Procédures pour l'exercice des droits
- Contrats établissant les rôles et responsabilités
  - Contrats avec les sous-traitants
  - Procédures internes en cas de violation de données
  - Preuves de consentement des personnes concernées

6. Avènement du RGPD

Conclusion

- Révolution au sein des entreprises
- Mise en place obligatoire sous peine de lourdes sanctions
- Tout le monde concerné !
- Mais des questions restent posées…
  - Comment l'application va-t-elle être suivie ?
  - Moyens humains pour gérer les plaintes ?
  - *Mais possibilité de lancer des actions de groupe contre les entreprises*

6. Avènement du RGPD

D'après vous ?

7 ans après la création du RGPD, ça marche ?

7. RGPD… et ensuite… - international,NIS2

Premier pas vers une loi internationale

- Aux USA, le droit constitutionnel au respect de la vie privée n'existe pas
- Questions des entreprises américaines
  - *Le RGPD va-t-il nous impacter ?* Oui, obligatoirement
  - *Comment l'éviter ?* Impossible, aligner sa stratégie dessus
- *California Consumer Privacy Act* (CCPA) votée en 2018, appliquée depuis 2020
  - Californie : 5^{e} puissance économique mondiale, donc influente → Un tournant majeur dans le respect de la vie privée aux USA, d'autres états s'y mettent doucement
- Au Canada, *Personal Information Protection and Electronic Documents Act*
- Au Brésil, loi similaire (LGPD) votée en 2018, en cours d'application
- Le Japon a signé un accord avec l'Europe
- La Chine est sur la même voie (mais plus difficile en raison de la censure sur Internet)
- En Europe, une grosse mise-à-jour arrive : **NIS2**

→ ***Les GAMAM n'ont qu'à bien se tenir…***

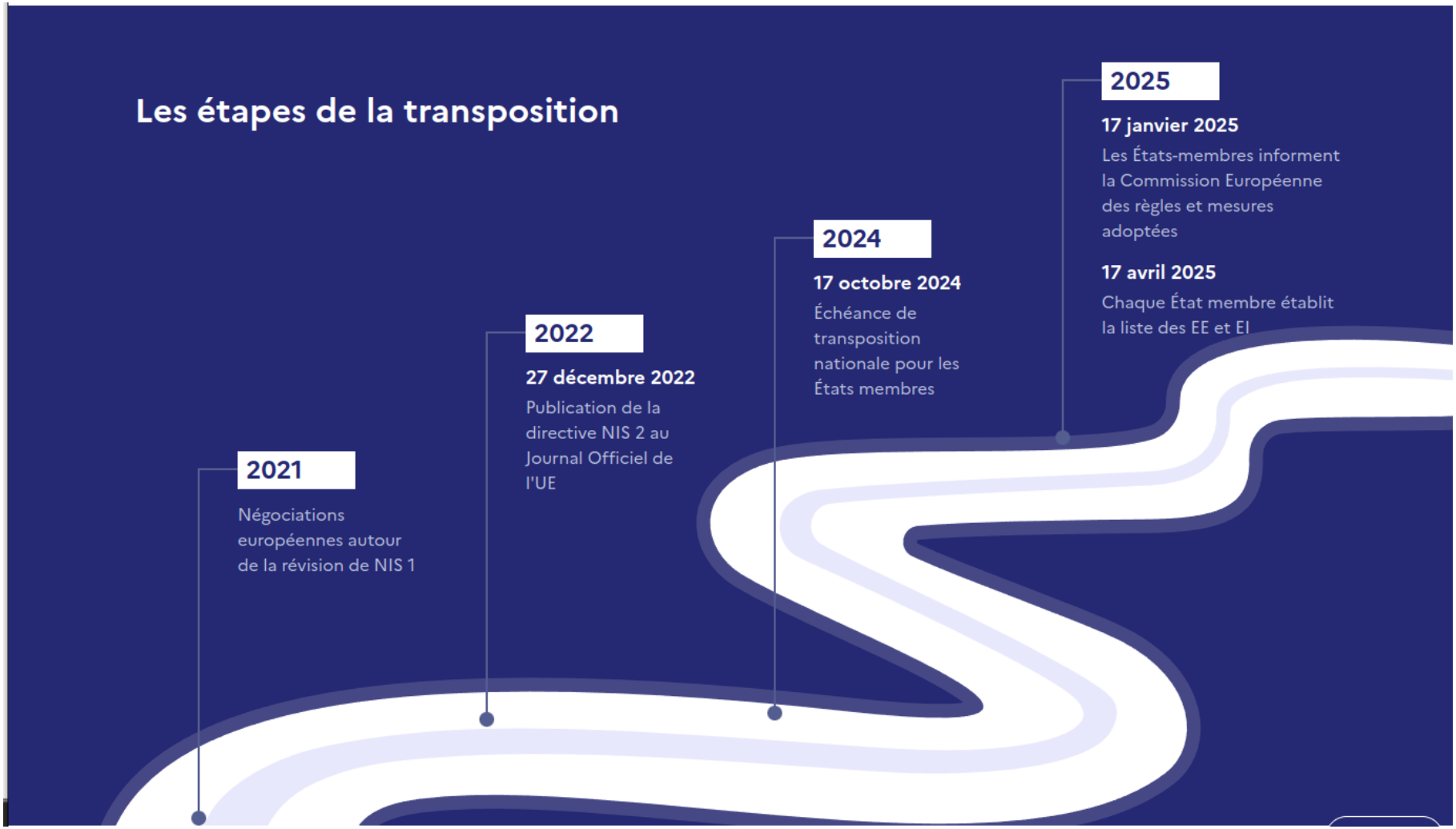
7. RGPD… et ensuite… - international,NIS2

NIS2 : « Sécurité des réseaux et des systèmes d'Information »

- Directive de l'UE pour « sécuriser les tissus économiques et administratifs des pays membres de l'UE »
- Distingue deux types d'entités-cibles :
  - EI : entités importantes (secteur important et taille moyenne)
  - EE : entités essentielles (secteur important et grande entreprise)
  - (en gros, l'UE reproduit le système français des OIV et OSE)
- Ces entités ont des devoirs spécifiques
  - Sous peines de sanctions financières jusqu'à 2 % du chiffre d'affaires mondial
  - Doivent rendre des comptes à l'ANSSI
- cf. https://monespacenis2.cyber.gouv.fr/
- C'est l'une des principales préoccupations des grosses entreprises d'IT en Europe en ce moment !

7. RGPD… et ensuite… - international,NIS2

NIS2 : « Sécurité des réseaux et des systèmes d'Information »



7. RGPD… et ensuite… - international,NIS2

ICANN – Internet corporation for assigned names and numbers

- Structure d'Internet
- Organisme à but non-lucratif
- **Soumis au droit <u>californien</u>**
- Gère la structure d'Internet :
  - Noms de domaine (ils ont supprimé le .iq de l'Irak par exemple)
  - Fonctionnement des adresses IP

7. RGPD… et ensuite… - international,NIS2

Déclaration Universelle des Droits de l'Homme (déclaratif) + Pacte international relatif aux droits civils et politiques (ONU)

https://treaties.un.org/doc/Publication/UNTS/Volume%20999/volume-999-I-14668-French.pdf

Article 17.

1. Nul ne sera l'objet d'immixtions **arbitraires** ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.

2. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.

Note : le terme **arbitraire** est essentiel : il implique qu'on peut obtenir accès aux informations, mais seulement de façon **ciblée** et **justifiée**. Grosso modo, il faut un mandat d'un juge. On n'a pas le droit de contrôler par défaut.

Charte des Droits Fondamentaux de l'Union Européenne (UE)

https://www.europarl.europa.eu/charter/pdf/text_fr.pdf

Article 7.

Toute personne a droit au respect de sa **vie privée** et familiale, de son domicile et de ses **communications**.

Article 8.

1. Toute personne a droit à la protection des **données à caractère personnel** la concernant.

2. Ces données doivent être **traitées loyalement**, à des **fins déterminées** et sur la base du **consentement** de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'**accéder aux données** collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une **autorité indépendante**.
(en France, c'est la CNIL)

7. RGPD… et ensuite… - international,NIS2

En France,

La violation du secret des correspondances est punie d’1 an de prison et 45 000 € d’amende.

Alourdi jusqu’à 3 ans de prison si une personne facilite cette violation dans le cadre de ses fonctions.

7. RGPD… et ensuite… - international,NIS2

USA Patriot Act

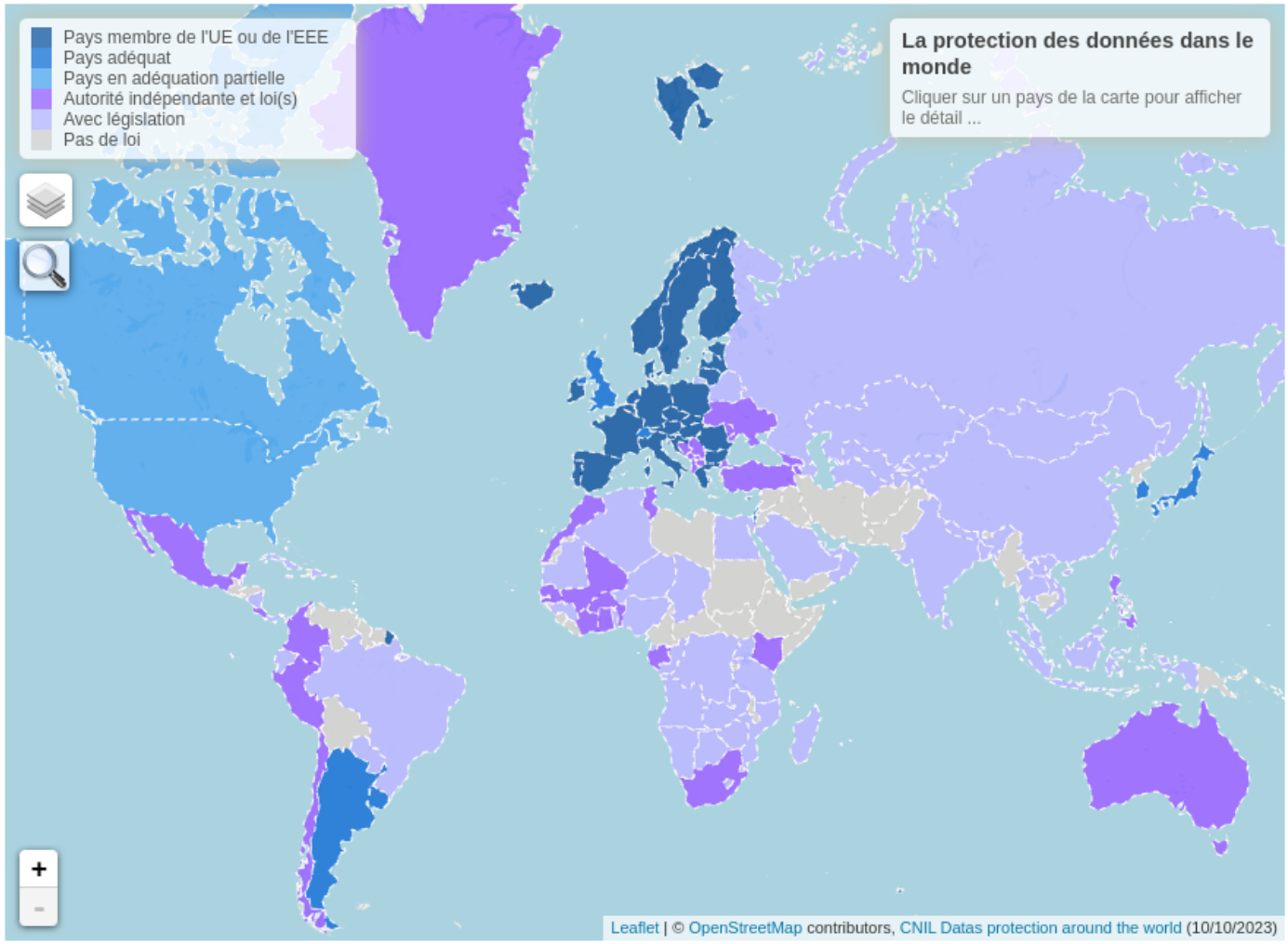
- 2001
- Union et renforcement des USA
- Exceptions à la loi dans un cadre anti-terroriste
  - Accès aux données informatiques des particuliers et entreprises **sans autorisation préalable et sans informer les utilisateurs**
- Renouvelé en 2024 pour la partie surveillance (FISA)

- En France : il faut une autorisation préalable (en gros, un mandat d'un juge) pour une telle enquête

Les USA n'ont pas entièrement intégré les droits de l'Homme dans leurs lois (et ont refusé de signer les droits de l'Enfant), ne partez pas du principe que le droit étasunien protège les données hébergées aux USA.

7. RGPD… et ensuite… - international,NIS2

L'icône « loupe » vous permet de rechercher un pays et de le positionner sur la carte.



Protection des données dans le monde

Carte de la CNIL, retrouvez les détails sur

https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

7. RGPD… et ensuite… - international,NIS2

Le droit ne fait que bouger !

Exemple : depuis août 2022, les assureurs ont le droit de rembourser les rançons de rançongiciels.

D'après vous ?

C'est positif ?

Références liées au chapitre

Glossaire du vocabulaire de cybersécurité
https://cyber.gouv.fr/publications/recommandations-relatives-ladministration-securisee-des-si
https://cyber.gouv.fr/publications/la-cybersecurite-pour-les-tpepme-en-treize-questions
https://cyber.gouv.fr/publications/la-methode-ebios-risk-manager-le-guide
https://cyber.gouv.fr/publications/cyberattaques-et-remediation-les-cles-de-decision

https://cyber.gouv.fr/publications/recommandations-pour-le-reconditionnement-des-ordinateurs-de-bureau-ou-portables
https://cyber.gouv.fr/publications/denis-de-service-distribues-ddos
https://cyber.gouv.fr/publications/les-mesures-cyber-preventives-prioritaires
https://cyber.gouv.fr/publications/sauvegarde-des-systemes-dinformation
https://cyber.gouv.fr/publications/recommandations-de-securite-pour-larchitecture-dun-systeme-de-journalisation
https://cyber.gouv.fr/publications/anticiper-et-gerer-sa-communication-de-crise-cyber
https://cyber.gouv.fr/publications/recommandations-pour-les-architectures-des-si-sensibles-ou-dr
https://cyber.gouv.fr/publications/recommandations-pour-la-protection-des-systemes-dinformation-essentiels
https://cyber.gouv.fr/publications/recommandations-relatives-la-securite-des-systemes-dobjets-connectes
https://cyber.gouv.fr/publications/securisation-des-systemes-de-controle-dacces-physique-et-videoprotection
https://cyber.gouv.fr/publications/attaques-par-rancongiciels-tous-concernes
https://cyber.gouv.fr/publications/cybersecurite-toutes-les-communes-et-intercommunalites-sont-concernees
https://cyber.gouv.fr/publications/securite-numerique-des-collectivites-territoriales-lessentiel-de-la-reglementation
https://cyber.gouv.fr/publications/maitrise-du-risque-numerique-latout-confiance

Nous vivons dans un joli monde, n’est-ce pas ???

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

DÉNIS DE SERVICE DISTRIBUÉS (DDOS *)

1/ LES ATTAQUES DDOS, UNE MENACE PROTÉIFORME

→ Les attaques DDoS peuvent être de plusieurs types :

> **volumétrique** visant à épuiser la bande passante réseau disponible (ex. : attaque consistant à envoyer des paquets depuis de multiples sources vers une cible – UDP *flood* ou ICMP *flood*) ;

> **protocolaire** visant à épuiser les ressources (CPU,RAM) d'une cible en détournant le fonctionnement d'un protocole (ex. : inondation SYN ou TCP, Smurf) ;

> **applicative** visant à épuiser les ressources (CPU,RAM) d'une cible en détournant le fonctionnement d'un service (ex. : attaque DNS *water torture* consistant à requêter massivement des serveurs pour des entrées DNS existantes).

→ **Ces types d'attaque en disponibilité ne sont pas exclusifs** et les attaquants peuvent très facilement et rapidement adapter voire combiner leurs techniques au cours du temps. Par exemple, un attaquant pourra commencer par une attaque volumétrique puis,voyant que sa cible prend des mesures d'atténuation spécifiques, s'adaptera en déclenchant une attaque protocolaire ou autre.

→ Des **mesures préventives et réactives** existent pour en limiter les conséquences. Dans le cas d'une attaque ciblée et très probablement évolutive, l'implication complémentaire d'experts est fortement recommandée pour **une réponse appropriée et spécifique**.

(*) L'acronyme anglais DDoS pour *Distributed Denial of Service* est le plus couramment utilisé.

2/ CONSTRUIRE ET PROTÉGER

→ **Restreindre au strict besoin opérationnel les services exposés à Internet.**

→ **Acquérir et mettre en œuvre un service de protection anti-DDoS dédié à cette seule fonction, et adapté au SI à protéger** :

> auprès de votre prestataire en cas d'hébergement externe, celui-ci pouvant déjà intégrer une prestation anti-DDoS, en fonction de l'offre d'hébergement souscrite ;

> et/ou auprès de vos fournisseurs d'accès à Internet (trou noir, dépollution des flux **) ;

> et/ou auprès d'un fournisseur de service professionnel (déroutement BGP, dépollution des flux **).

Le service mis en œuvre doit **protéger contre les attaques de niveaux 3, 4, 5 et 7 du modèle OSI**, par exemple en permettant un contrôle de débit, une limitation du nombre de requêtes, une protection anti-robot et une reconnaissance d'adresses IP réputées malveillantes.

Dans tous les cas, sa **mise en œuvre collaborative entre client et prestataire** nécessite une prise en main, un paramétrage adapté au trafic de l'entité et aux applications exposées (ex. : seuils de déclenchement d'alerte) et **des tests réguliers** pour s'assurer du bon fonctionnement et de l'absence d'effets de bord. Des procédures doivent être définies.

(**) Par exemple, la dépollution des flux peut faire intervenir des critères de géolocalisation,de conformité protocolaire, d'inspection de paquets et de volumétrie par protocole susceptible d'être utilisé dans les DDoS (ex. : DNS en UDP, NTP, CHARGEN).

V2.0 (04/24)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

→ **Concevoir une architecture des services qui permet de répartir la charge et le trafic sur plusieurs sous-systèmes** (centre de données, mécanismes de bascule réseau, répartiteurs de charge, serveurs distribués, etc.).

→ **Dimensionner une architecture des services en prenant en compte les besoins métiers** qui peuvent fluctuer : bandes passantes, puissances de calcul et mémoire, capacités de stockage.

→ **Concevoir les architectures de telle sorte qu'un service exposé à Internet qui subit une attaque DDoS puisse continuer à être administré malgré cette attaque** (réseau d'administration physiquement dédié, cloisonnement réseau des flux de supervision, etc.).

→ **Concevoir les services exposés à Internet de façon à ce qu'une attaque DDoS sur un service n'ait pas d'impact sur la disponibilité des autres services** (chaînes d'accès Internet distinctes, segmentation des plans d'adressage réseau, hébergeurs distincts, etc.).

→ **Configurer les pare-feux en coupure d'Internet** :

> activer uniquement un filtrage au niveau réseau et transport (niveaux 3 et 4 du modèle OSI) et désactiver les fonctions de filtrage applicatif (niveaux 5 et plus) ;

> réduire les flux UDP entrants au strict nécessaire;

> anticiper la capacité à retirer temporairement le suivi de connexions.

→ **Configurer en aval des pare-feux applicatifs pour protéger les sites Web** en ajustant des limites de session et en appliquant des blocages de requêtes malveillantes.

→ **Protéger les sites Web avec un CDN (*Content Delivery Network*) pour la répartition de charge.** Les CDN permettent la répartition de ressources sur un grand nombre de serveurs, ce qui peut contribuer à améliorer la résistance aux attaques DDoS. **Une attention doit être portée au fait qu'une partie de ces ressources peut être hébergée à l'étranger (impact potentiel en confidentialité).**

2/ ANTICIPER ET RÉAGIR

→ **Mettre en place un dispositif de supervision et détection des attaques DDoS**, afin de détecter au plus tôt une attaque :

> utiliser un dispositif de centralisation des journaux afin de faciliter le diagnostic d'un incident DDoS *a posteriori* ;

> rédiger et tester régulièrement une procédure définissant la marche à suivre en cas d'attaque, en étroite collaboration avec les prestataires de services anti-DDoS. .

→ **Prévoir un mode dégradé pour les activités critiques en cas d'attaque DDoS**, le temps de la remédiation. Intégrer le fait que votre fournisseur d'accès à Internet peut aussi imposer un mode dégradé en cas d'attaque DDoS sur sa propre infrastructure, même si cette attaque ne cible pas directement votre entité.

→ **Faire régulièrement l'inventaire des services ouverts sur Internet** afin d'adapter la procédure de réponse à des attaques DDoS.

→ **Mettre en place un dispositif de gestion des crises**, en lien avec vos prestataires de protection DDoS d'une part et vos responsables communication d'autre part.

→ **Contrôler *a posteriori* les autres alertes de sécurité** générées pendant une attaque DDoS « bruyante », potentiels signes d'une attaque plus discrète et plus grave.

Pour aller plus loin : https://cyber.gouv.fr/guide-ddos

V2.0 (04/24)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

SAUVEGARDE DES SYSTÈMES D'INFORMATION

1/ CONSTRUIRE ET PROTÉGER

→ **Définir une politique de sauvegarde** en identifiant les données critiques pour l'activité de votre entité en précisant la fréquence à laquelle il est important de les sauvegarder.

→ **Considérer les opérations de sauvegarde et de restauration comme des opérations sensibles d'administration** devant bénéficier des protections adéquates : poste d'administration durci, flux dans un réseau d'administration, etc.

→ **Rendre indépendante l'infrastructure de sauvegarde** vis-à-vis des annuaires de production (ex. : Active Directory).

→ **S'assurer du contrôle d'accès des sauvegardes** pour garantir qu'elles ne seront ni modifiées ni altérées et toujours disponibles, en particulier dans le cadre de l'utilisation d'offres de sauvegarde *cloud*.

→ **Être vigilant sur la sensibilité des données sauvegardées** en cas de solution hors-site, dans un *cloud* public ou chez un prestataire externe. Chiffrer les sauvegardes au préalable par vos propres moyens si nécessaire.

→ **Faire évoluer continuellement l'infrastructure de sauvegarde** au même rythme que l'évolution des SI (virtualisation, *cloud*, etc.) et en fonction de l'évolution de la menace. Ne conservez pas une infrastructure obsolète en production.

2/ ANTICIPER ET RÉAGIR

→ **Définir une stratégie de restauration** en lien avec le plan de reprise d'activité et en tenant compte des principaux scénarios d'attaque identifiés sur les SI (rançongiciels, espionnage, etc.). **Réaliser régulièrement des tests de restauration.** Impliquer la direction sur les modes dégradés acceptables en cas de crise cyber.

→ **Ne pas oublier d'inclure les médias d'installation et les configurations** des applications métier dans les sauvegardes.

→ **Réaliser régulièrement et impérativement des sauvegardes hors-ligne** (déconnectées du SI).

→ **Prévoir une procédure d'isolation d'urgence** du système de sauvegarde (serveurs, médias, etc.) en cas de suspicion de compromission ou d'attaque en cours.

→ Après un incident, tenir compte du fait que les sauvegardes peuvent contenir les vecteurs de compromission. **Restaurer à partir de sources de confiance** (images officielles, binaires d'installation signés), contrôler la conformité des configurations, faire un scan antivirus des données.