La sécurité par l'enseignement supérieur des NTIC

Cybersécurité des Systèmes Industriels

Loïc Rouquette

Séquencement pédagogique

Déroulé (6CM / 6TP)

I. Introduction Générale à la Sécurité des Systèmes d'Information (2h)

II. Aspects Systèmes & Matériels (2h CM)

III. Aspects Réseaux & Applications (2h CM)

IV. Introduction à la méthode EBIOS (3h TP)

V. Analyse EBIOS (3h TP)

VI. Partiel (1h)

Objectifs

À la fin du cours, vous devrez être capable de:

– **Énumérer** les différents organismes responsables de la cybersécurité en France ;

– **Énumérer** les différents aspects de la cybersécurité ;

– **Cartographier** les éléments d'un système d'information ;

– **Déterminer** des axes d'amélioration en termes de sécurité pour un SI.

Évaluation

Projet

→ TP de 3h en binôme avec compte rendu.

→ Sujet Analyse EBIOS d'une entreprise

Partiel

→ 1h sur la partie cours magistraux avec une étude de cas.

Notions

Licence

Enjeux de la cybersécurité

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.

Préambule

→ Le S.I. d'une organisation contient un ensemble d'actifs :

actifs primordiaux

Processus métiers
& Informations

actifs supports

Site Personne Matériel Réseau Logiciel Organisation

Préambule

→ Le S.I. d'une organisation contient un ensemble d'actifs :

actifs primordiaux

Processus métiers

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

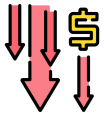
actifs supports

Site Personne Matériel Réseau Logiciel Organisation

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

Les enjeux



Impacts financiers

Impact sur l'image et la réputation

Sécurité des S.I.

Impacts juridiques et réglementaires

Impacts organisationnels

Pourquoi les pirates s'intéressent aux *Système d'information* (S.I.) ?

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

Pourquoi les pirates s'attaquent aux S.I. ?

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

La nouvelle économie de la cybercriminalité

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

1. des groupes spécialisés dans le développement de programmes malveillants et virus informatiques
2. des groupes en charge de l'exploitation et de la commercialisation de services permettant de réaliser des attaques informatiques
3. 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
4. des groupes en charge de la vente des données volées, et principalement des données de carte bancaire
5. des intermédiaires financiers pour collecter l'argent qui s'appuient généralement sur des réseaux de mules

La nouvelle économie de la cybercriminalité

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

de 2 à 10$ le prix moyen de commercialisation des **numéros de cartes bancaires** en fonction du pays et des plafonds

5$ le tarif moyen de location pour 1 heure d'un **botnet**, système permettant de saturer un site internet

2.399$ le prix de commercialisation du **malware** « Citadel » permettant d'intercepter des numéros de carte bancaire (+ un abonnement mensuel de 125 $)

Impacts sur la vie privée

- Impact sur l'image / le caractère / la vie privée
  - Diffamation de caractère
  - Divulgation d'informations personnelles
  - Harcèlement / cyber-bullying
- Usurpation d'identité
  - « Vol » et réutilisation de logins/mots de passe pour effectuer des actions au nom de la victime
- Perte définitive de données
  - malware récents (rançongiciel) : données chiffrées contre rançon
  - connexion frauduleuse à un compte « cloud » et suppression malveillante de l'ensemble des données
- Impacts financiers
  - n° carte bancaire usurpé et réutilisé pour des achats en ligne
  - Chantage (divulgation de photos ou d'informations compromettantes si non paiement d'une rançon)

Ces impacts – non exhaustifs – ne signifient pas qu'il ne faut pas utiliser Internet, loin de là ! Il faut au contraire apprendre à anticiper ces risques et à faire preuve de discernement lors de l'usage d'Internet/smartphones…

Les infrastructures critiques

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

Quelques exemples d'attaques

Stuxnet (2010)

- Ver découvert en 2010 qui aurait été conçu par la NSA.
  - Dégradation des installations nucléaire Iranienne (pourtant coupées d'Internet)
  - Utilisation d'une faille zéro day sur Windows
  - Réplication du malware sur internet avec l'appartiton de nouvelles variantes : DuQu, Flame, Petya

Piratage de Sony (2014)

- Scénario probable :
  1. Phishing repérage sur LinkedIn ;
  2. Campagne de phishing sur les personnes repérées demandant à déverrouiller son AppleID ;
  3. Utilisation des informations pour s'authentifier sur Microsoft System Center Configuration Manager ;
  4. Enjoy !

Quelques exemples d'attaques

Locky (2016)

- Ransomware par fichier Word en pièce jointe ;
- Chiffrement de l'intégralité des disques ;
- **90.000** postes infectés.

Wanncry (2017)

- Exploitation d'une faille de sécurité sur les versions antérieures à Windows 10 ;
- Accés et verrouillage des données ;
- **230.000** postes infectés.

Propriétés de la cybersécurité

Introduction aux critères DIC

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**.

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.

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

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...

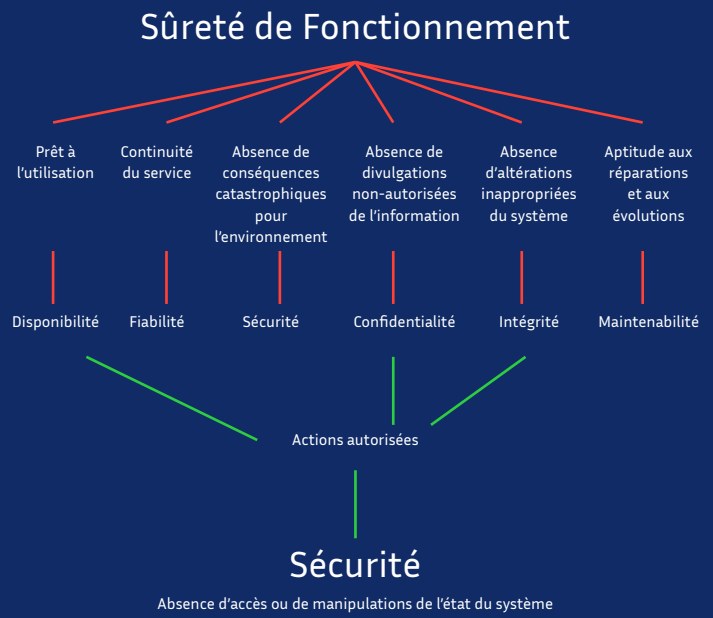
Sécurité

- Protection contre les actions malveillantes volontaires
- Exemple de risque : blocage d'un service, modification d'informations, vol d'informations
- 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, filtrages...

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.



Exemple d'évaluation DICP

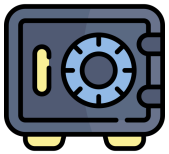
Ainsi, pour évaluer si un bien est correctement sécurisé, il faut auditer son niveau de Disponibilité, Intégrité, Confidentialité et de Preuve. L'évaluation de ces critères sur une échelle permet de déterminer si ce bien est correctement sécurisé.

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

→ Interne : inhérente au métier de l'entreprise

→ 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.

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.

Mécanisme de sécurité pour atteindre les besoins DICP

		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 lecture/écriture/ suppression aux ressources personnes dument habilitées.		✓	✓	✓
Sécurité physique des équipements et locaux	Mécanismes de protection destinés à protéger l'intégrité physique du matériel et des bâtiments/bureaux.	✓	✓	✓	

Mécanisme de sécurité pour atteindre les besoins DICP

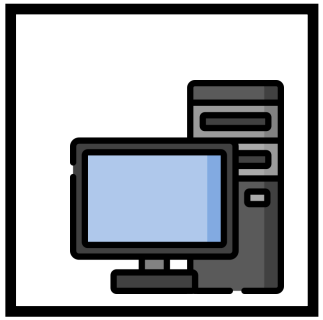
		D	I	C	P
Capacité d'audit	Mécanismes organisationnels destinés à s'assurer de l'efficacité et de la pertinence des mesures mises en œuvre. Participe à l'amélioration continue de la sécurité du S.I.	✓	✓	✓	✓
Clauses contractuelles avec les partenaires	Mécanismes organisationnels destinés à s'assurer que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

Menaces, Vulnérabilités & Attaques

Notion de « Vulnérabilité »

Vulnérabilité : **Faiblesse au niveau d'un bien**

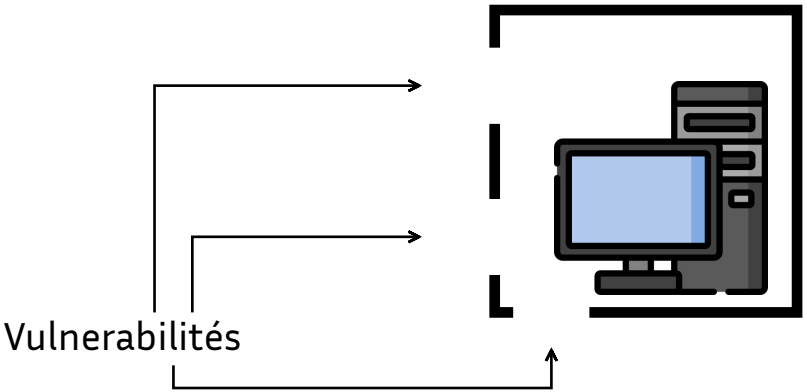
Au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation du bien.



Notion de « Vulnérabilité »

Vulnérabilité : **Faiblesse au niveau d'un bien**

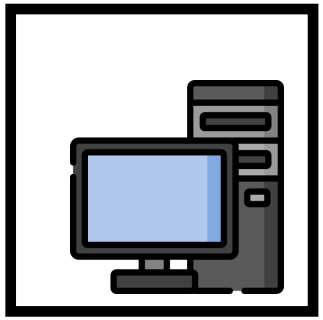
Au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation du bien.



Notion de « Menace »

Menace : **Cause potentielle d'un indicent**

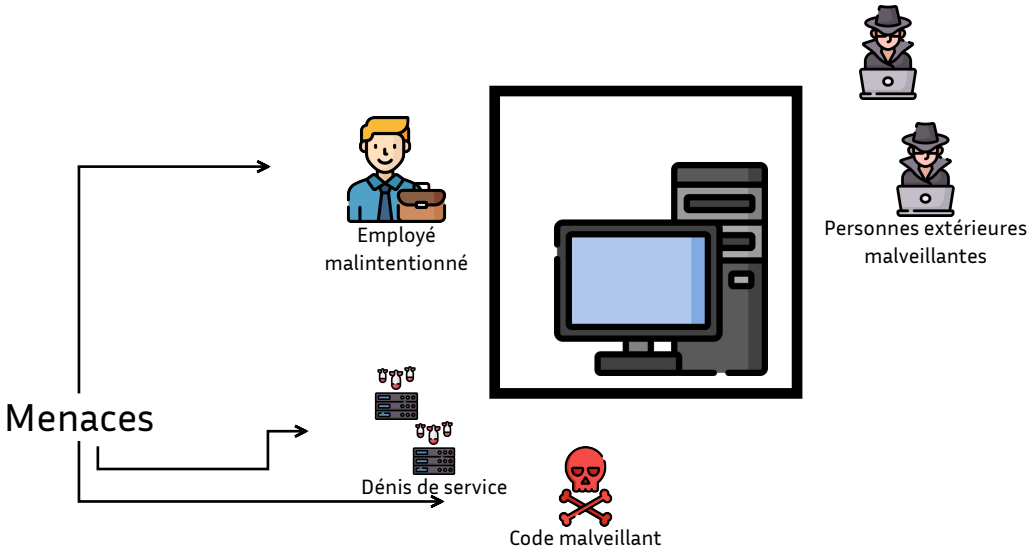
Ce qui pourrait entrainer des dommages sur un bien si cette menace se concrétisait.



Notion de « Menace »

Menace : **Cause potentielle d'un indicent**

Ce qui pourrait entrainer des dommages sur un bien si cette menace se concrétisait.



Notion d’ « Attaque »

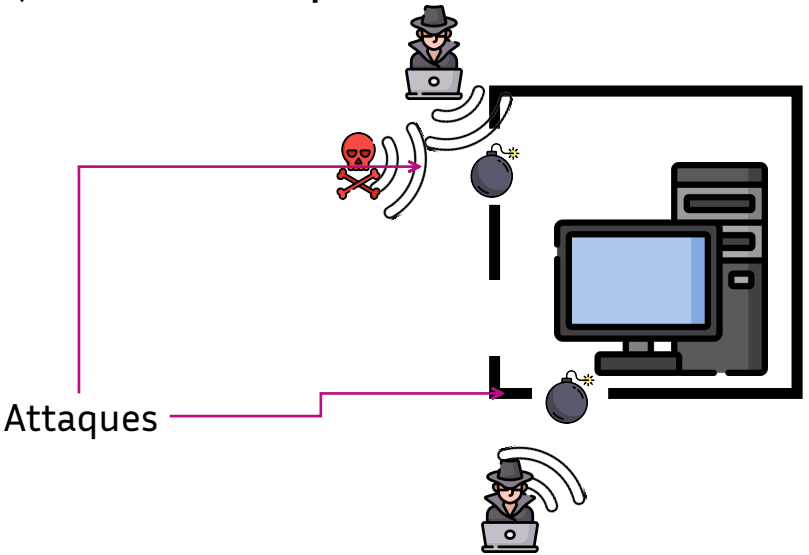
Attaque : **Action malveillante**

Action 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**.

Notion d' « Attaque »

Attaque : **Action malveillante**

Action 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**.



Notion d' « Attaque »

Une attaque ne peut donc avoir lieu (et réussir) que si le bien est affacté 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 maitriser
ces vulnérabilités plutôt que de viser un objectif 0 inatteignable.

Exemple de vulnérabilité lors de la conception d'une application

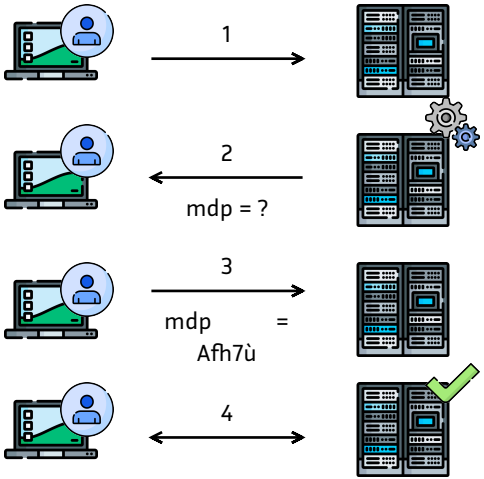
Contournement de l'authentification dans l'application VNC

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

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

Illustration d'un usage normal de l'application vulnérable

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



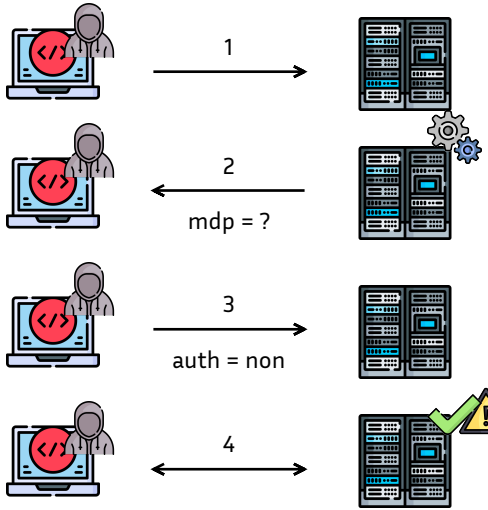
Le serveur détermine le mode d'authentification (aucune authentification, mot de passe, certificat, etc.) et envoie cette demande d'authentification à l'utilisateur demandeur.

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.

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

L'attaquant 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.

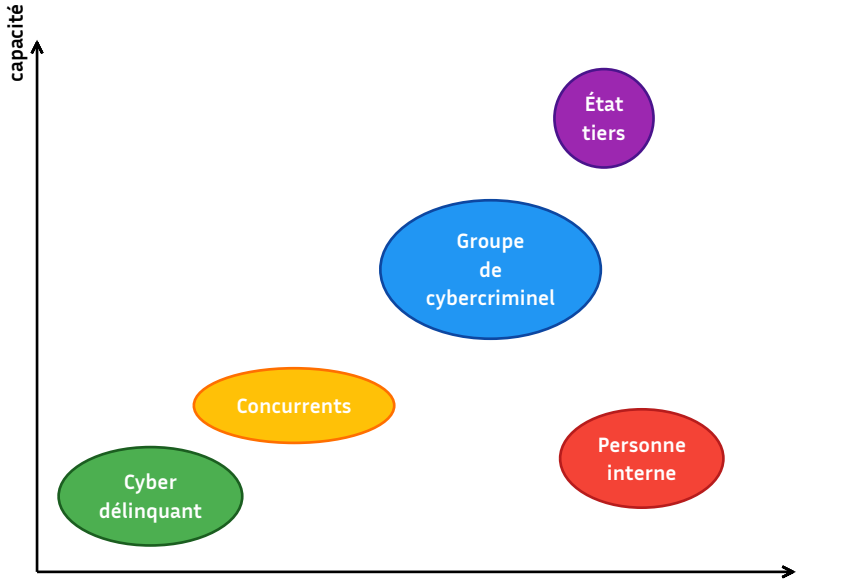
L'attaquant choisit de s'authentifier avec le mécanisme de son choix, et non pas avec le mécanisme choisi par le serveur. Ici il choisit la méthode « pas d'authentification ».

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

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 « auth = non » est effectivement une authentification qui est toujours correcte).

Panorama des Menaces

Les sources potentielles de menaces



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

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

Exposition : opportunités et intérêts de la source de menaces

Panorama de quelques menaces

Hameçonnage & Ingénierie sociale

Fraude interne

Violation d'accès non autorisé

Virus informatique

Déni de service distribué

Hameçonnage & Ingénierie sociale

Ingénierie sociale

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

→ pour dérober directement des informations confidentielle, ou

→ pour introduire des logiciels malveillants dans le système d'information de la banque

Hameçonnage & Ingénierie sociale

Ingénierie sociale

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

→ pour dérober directement des informations confidentielle, ou

→ pour introduire des logiciels malveillants dans le système d'information de la banque

Téléphone Internet Emails

Hameçonnage & Ingénierie sociale

Ingénierie sociale

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

→ pour dérober directement des informations confidentielle, ou

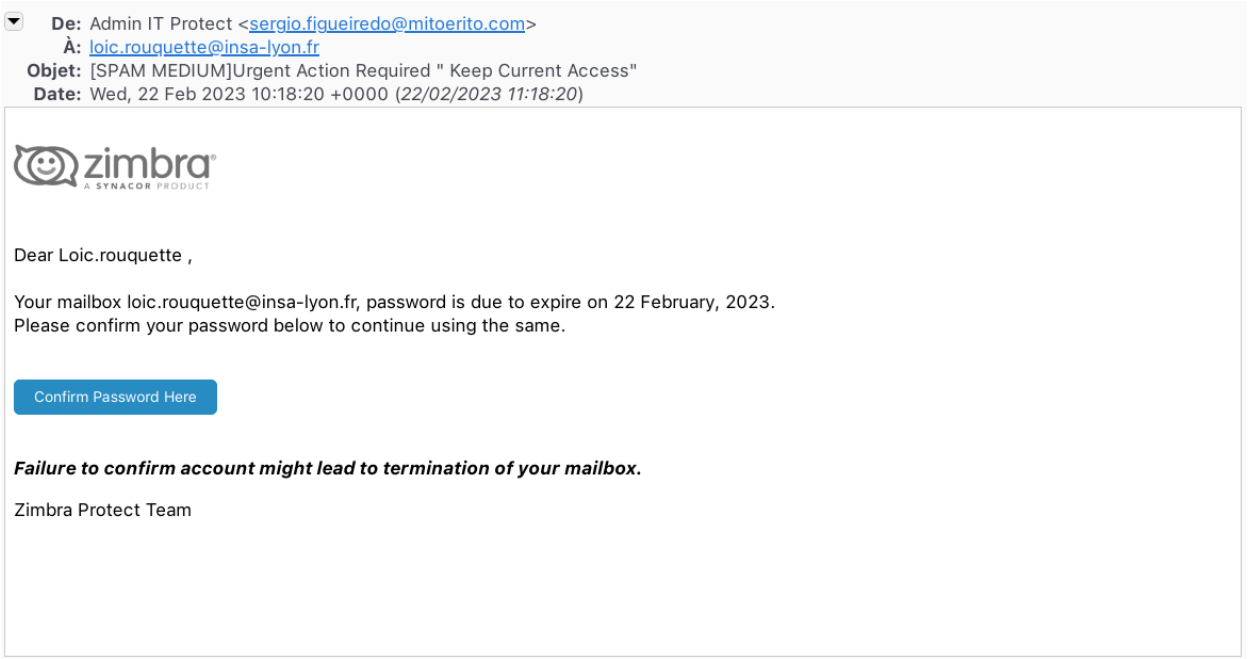
→ pour introduire des logiciels malveillants dans le système d'information de la banque

Téléphone Internet Emails

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

Hameçonnage & Ingénierie sociale

Exemple de phishing



De: Admin IT Protect <sergio.figueiredo@mitoerito.com>
À: loic.rouquette@insa-lyon.fr
Objet: [SPAM MEDIUM]Urgent Action Required " Keep Current Access"
Date: Wed, 22 Feb 2023 10:18:20 +0000 (*22/02/2023 11:18:20*)

zimbra
A SYNACOR PRODUCT

Dear Loic.rouquette ,

Your mailbox loic.rouquette@insa-lyon.fr, password is due to expire on 22 February, 2023.
Please confirm your password below to continue using the same.

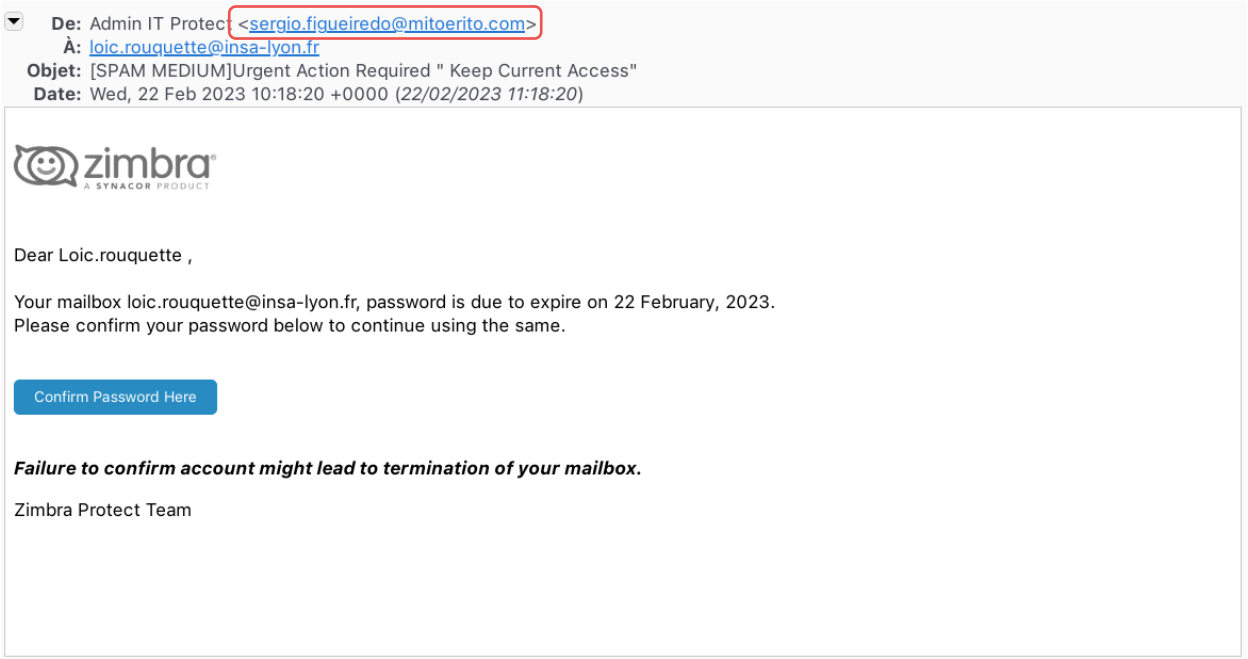
Confirm Password Here

Failure to confirm account might lead to termination of your mailbox.

Zimbra Protect Team

Hameçonnage & Ingénierie sociale

Exemple de phishing



De: Admin IT Protect <sergio.figueiredo@mitoerito.com>
À: loic.rouquette@insa-lyon.fr
Objet: [SPAM MEDIUM]Urgent Action Required " Keep Current Access"
Date: Wed, 22 Feb 2023 10:18:20 +0000 (*22/02/2023 11:18:20*)

zimbra
A SYNACOR PRODUCT

Dear Loic.rouquette ,

Your mailbox loic.rouquette@insa-lyon.fr, password is due to expire on 22 February, 2023.
Please confirm your password below to continue using the same.

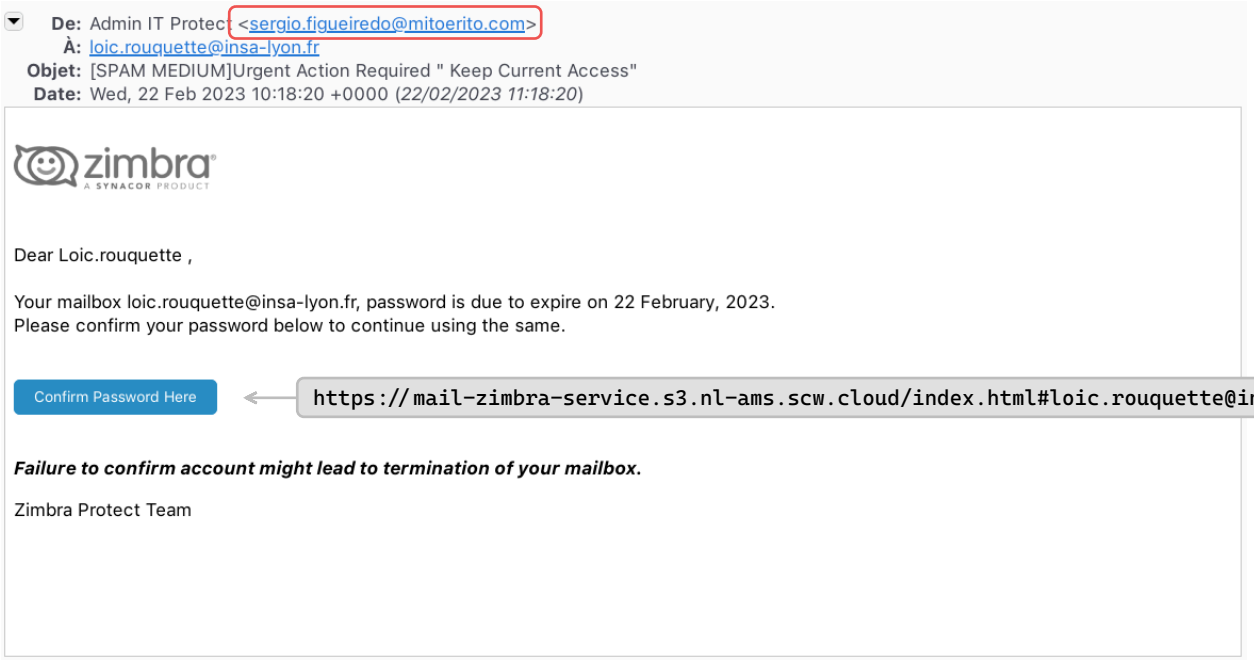
Confirm Password Here

Failure to confirm account might lead to termination of your mailbox.

Zimbra Protect Team

Hameçonnage & Ingénierie sociale

Exemple de phishing



De: Admin IT Protect <sergio.figueiredo@mitoerito.com>
À: loic.rouquette@insa-lyon.fr
Objet: [SPAM MEDIUM]Urgent Action Required " Keep Current Access"
Date: Wed, 22 Feb 2023 10:18:20 +0000 (*22/02/2023 11:18:20*)

zimbra
A SYNACOR PRODUCT

Dear Loic.rouquette ,

Your mailbox loic.rouquette@insa-lyon.fr, password is due to expire on 22 February, 2023.
Please confirm your password below to continue using the same.

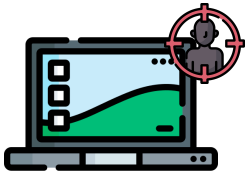
Confirm Password Here ← `https://mail-zimbra-service.s3.nl-ams.scw.cloud/index.html#loic.rouquette@insa-lyon.fr`

Failure to confirm account might lead to termination of your mailbox.

Zimbra Protect Team

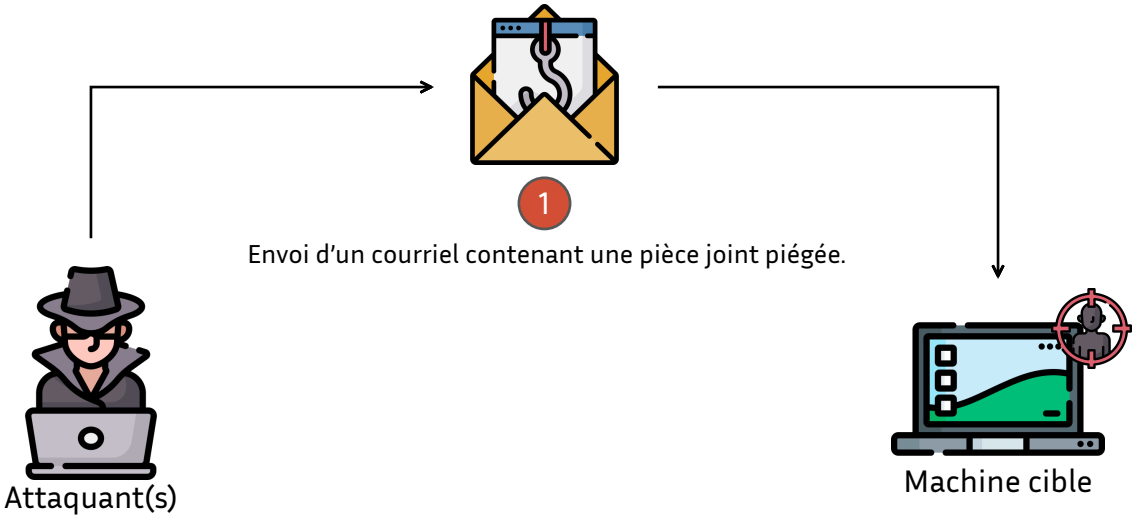
Déroulement d'une attaque avancée

Attaquant(s)

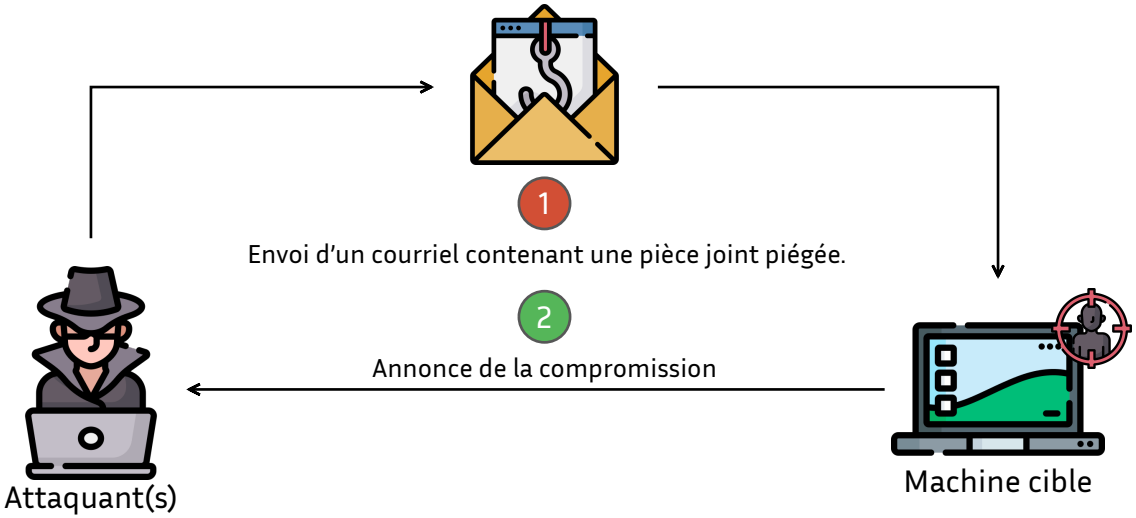


Machine cible

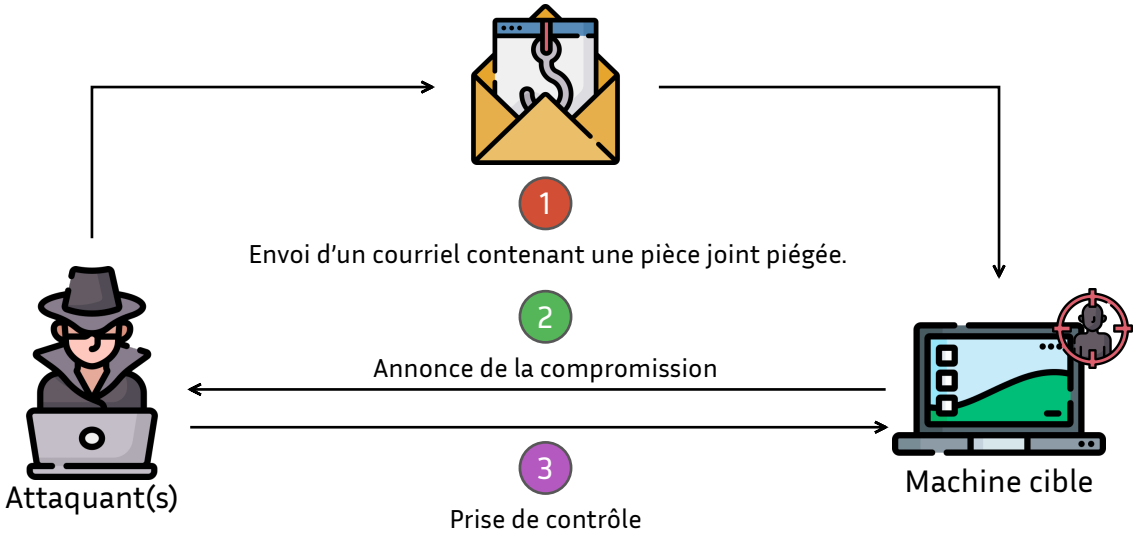
Déroulement d'une attaque avancée



Déroulement d'une attaque avancée



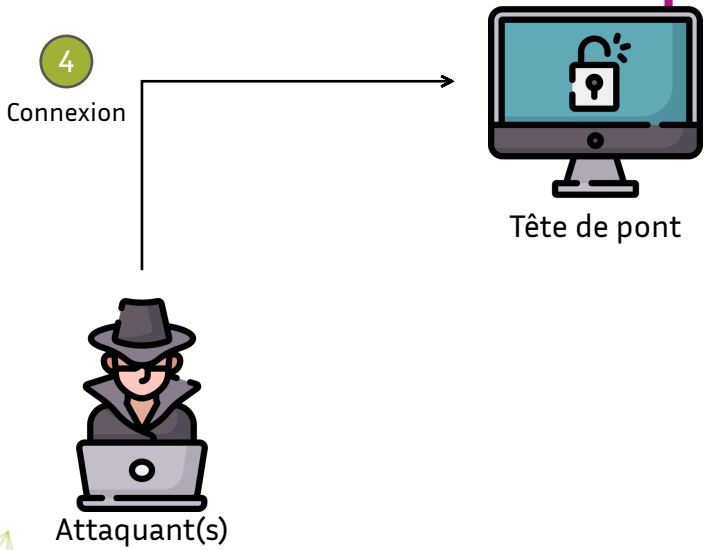
Déroulement d'une attaque avancée



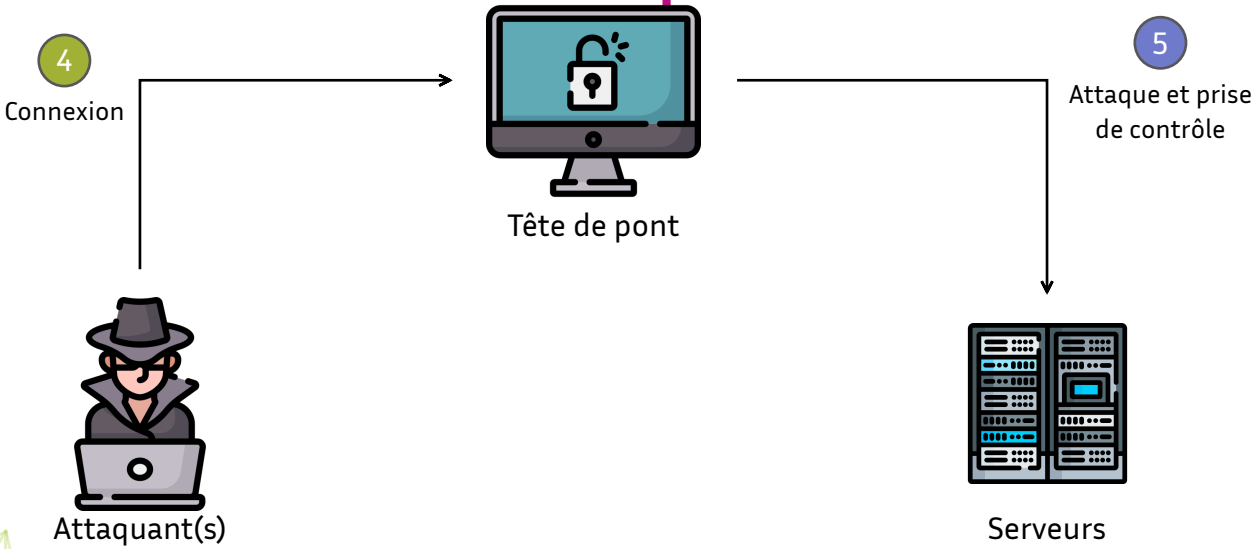
Déroulement d'une attaque avancée

Attaquant(s)

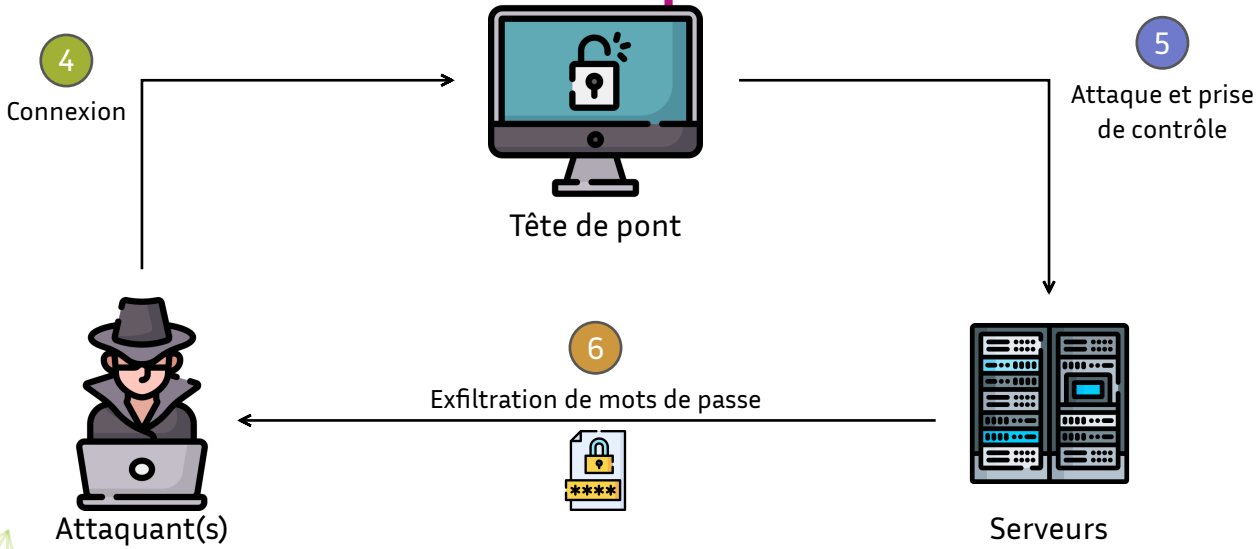
Déroulement d'une attaque avancée



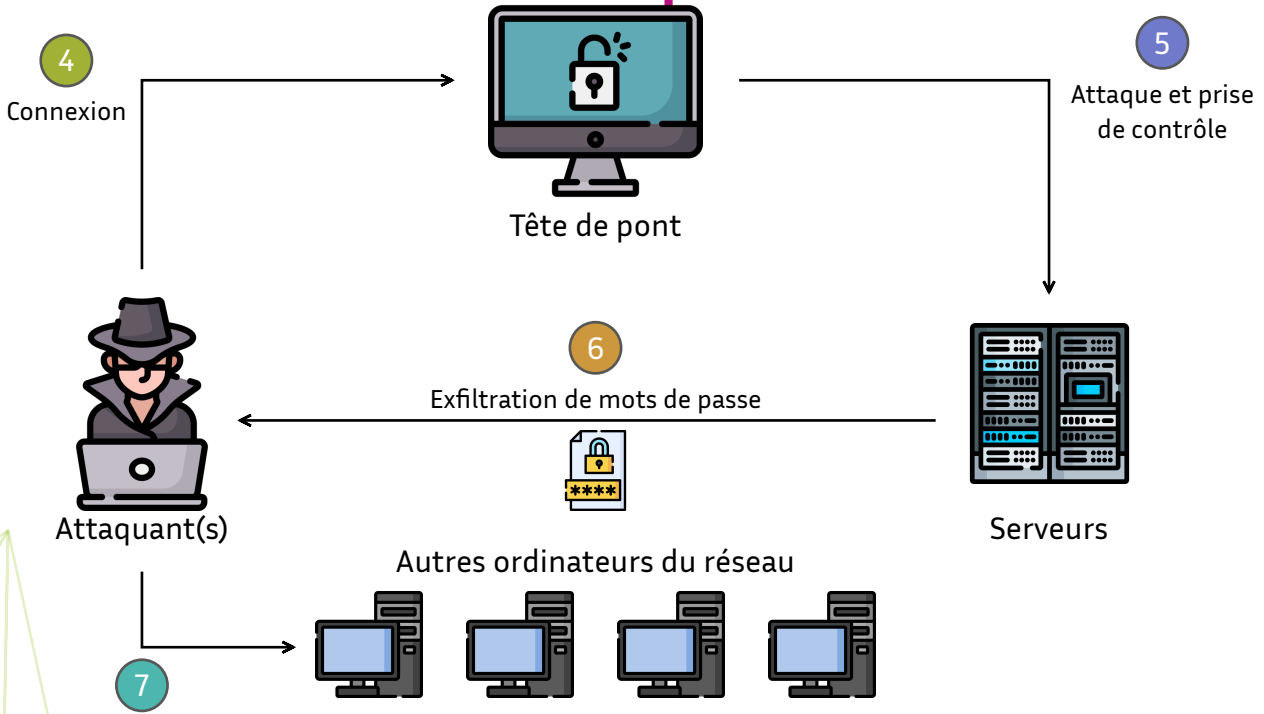
Déroulement d'une attaque avancée



Déroulement d'une attaque avancée



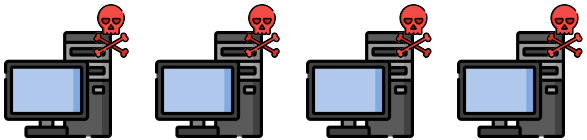
Déroulement d'une attaque avancée



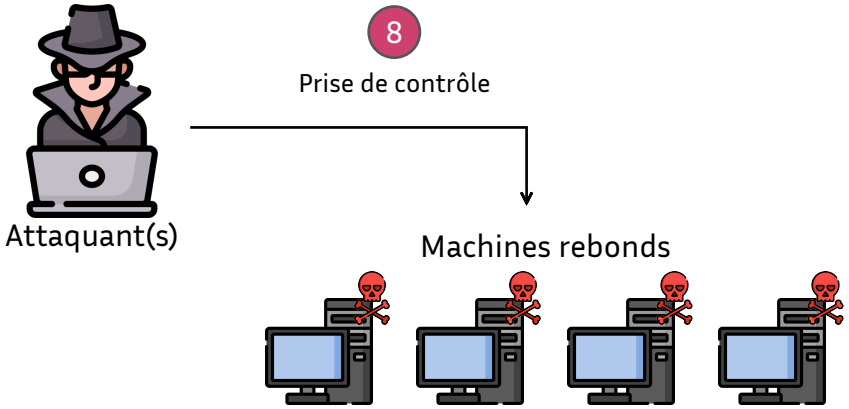
Déroulement d'une attaque avancée

Attaquant(s)

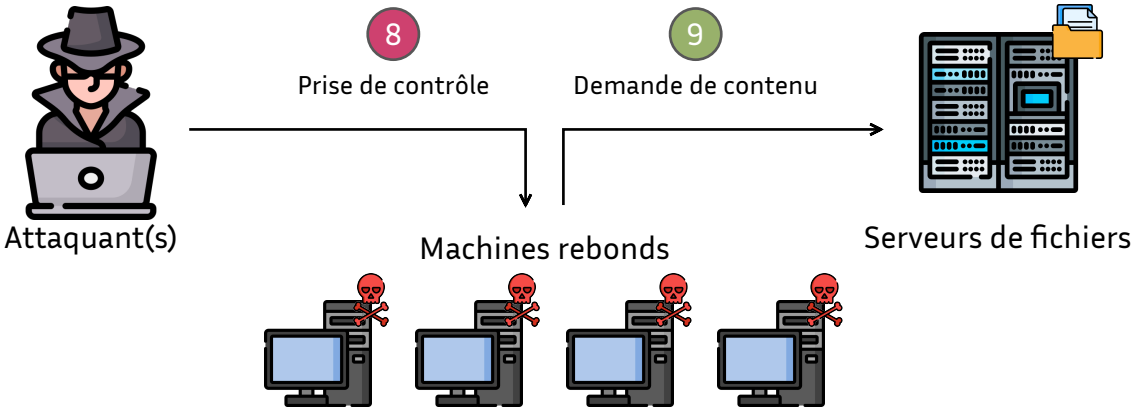
Machines rebonds



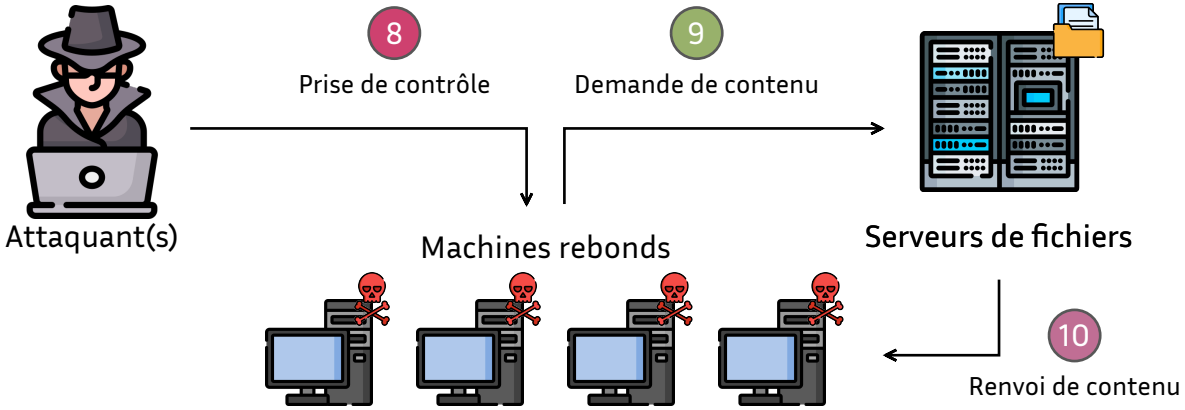
Déroulement d'une attaque avancée



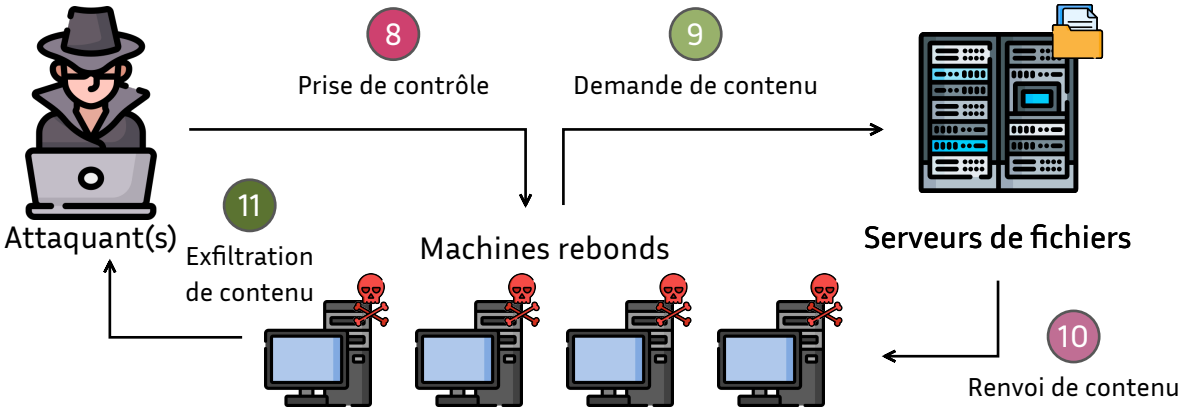
Déroulement d'une attaque avancée



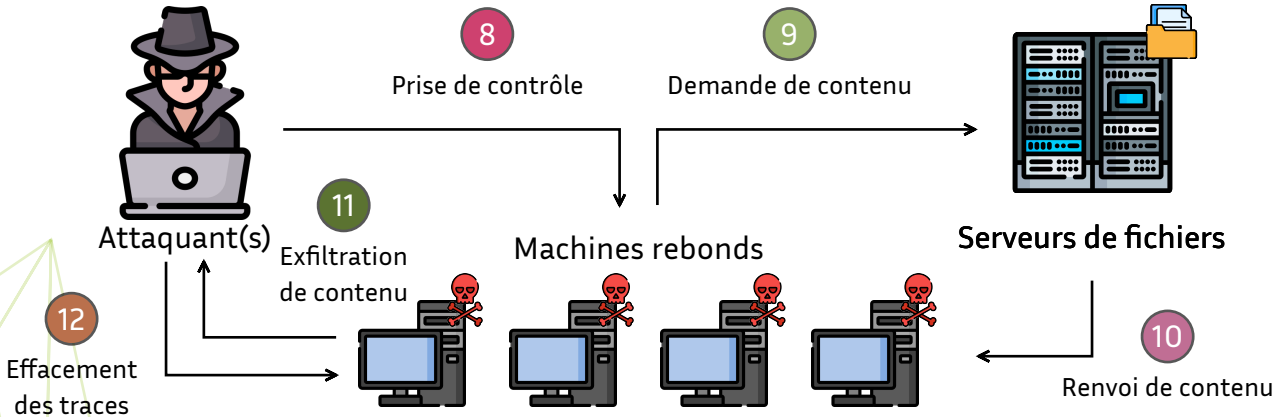
Déroulement d'une attaque avancée



Déroulement d'une attaque avancée



Déroulement d'une attaque avancée



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
  - → question de sécurité.

Le nombre de tentatives de mots de passe avant verrouillage du compte était trop élevé.

- → permettant des attaques par « brute force ».

Il semblerait que l'attaque soit de type « social engineering ».

- → permettant de répondre aux questions de sécurité.

Fraude interne

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

Catégorie des fraudeurs

- Frodeur 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 deas avoirs de l'entreprise
- La création de fausses opérations
- La personne qui fausse ses objectifs pour augmenter sa rémunération

Violation d'accès non-autorisé

Mots de passe faibles

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

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

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

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

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.

Violation d'accès non-autorisé

Intrusion

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

80% des domaines Active Directory sont compromis en 2h

75% des comptes 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.

Virus informatique

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

→ à devenir de plus en plus ciblés sur un secteur d'activité (télécommunication, banque, défense, énergie, etc.)

→ à devenir de plus en plus sophistiqués et furtifs

Les principaux vecteurs d'infection :

→ Message avec pièce-jointe

→ Support mobile

→ Site Web malveillant ou piratés

→ Partages réseaux ouverts, systèmes vulnérables

Conséquences :

→ Installation d'un « cheval de Troie » pour accéder au poste de travail à distance

→ Récupération de données ciblées : cartes bancaires, identifiants/mots de passe...

→ Surveillance à distance des activités : capture des écrans, des échanges, du son ou de la vidéo !

→ Destruction des données des postes de travail

→ Chiffrement des données pour une demande de rançon

Déni de service Distribué (DDoS)

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

34.5h

durée moyenne d'une attaque

48.28Gbps

bande passante moyenne d'une attaque

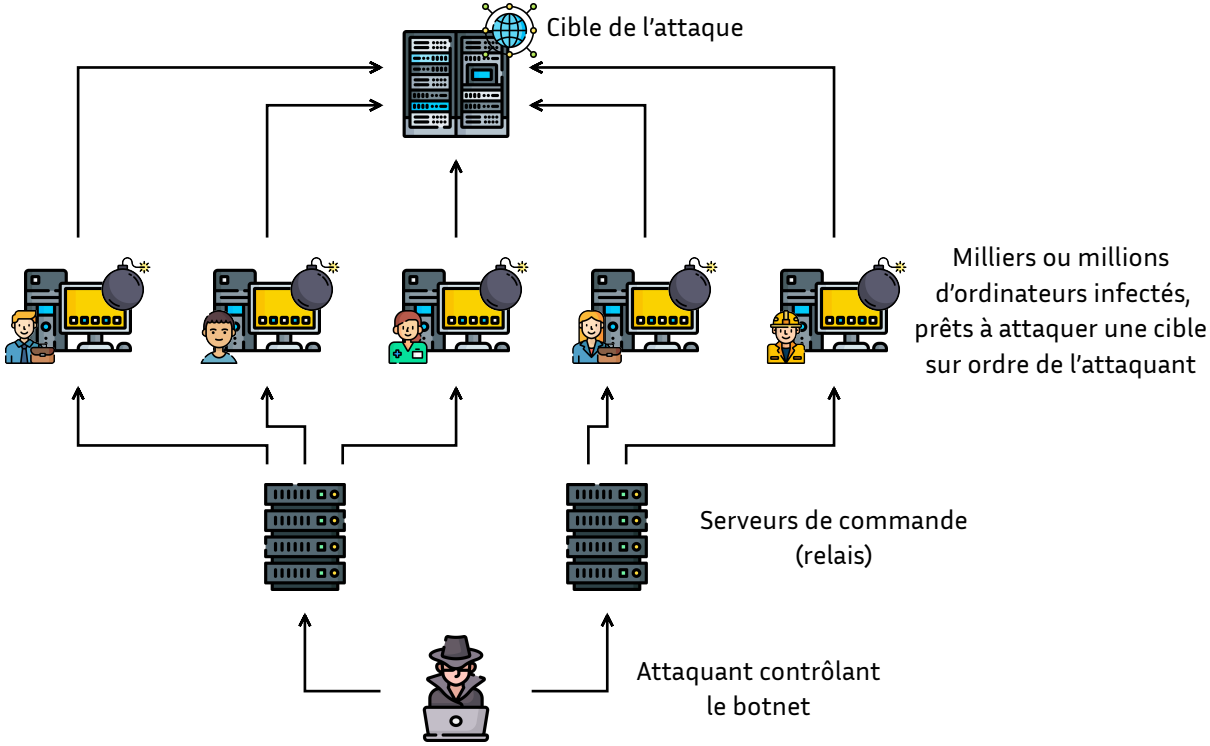
75%

des attaques au niveau infrastructure

25%

des attaques au niveau application

Illustration d'un réseau de botnets



Droit des *Technologies de l'information et de la communication* (TIC) & Organisation de la sécurité en France

L'organisation de la sécurité en France

Cyberdéfense : un véritable enjeu de sécurité nationale

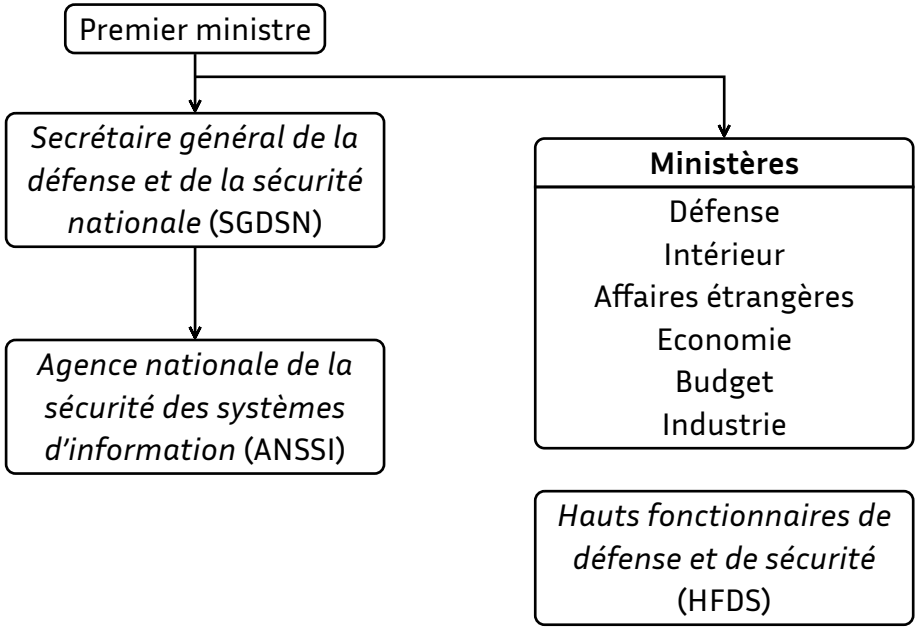
« **Les cyberattaques**, parce qu'elles n'ont pas, jusqu'à présent, causé la mort d'hommes, n'ont pas dans l'opinion l'impact d'actes terroristes. Cependant, dès aujourd'hui, et plus encore à l'horizon du Livre blanc, elles constituent **une menace majeure, à forte probabilité et à fort impact potentiel**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

— Chapitre 4, Les priorités stratégiques, livre blanc 2013

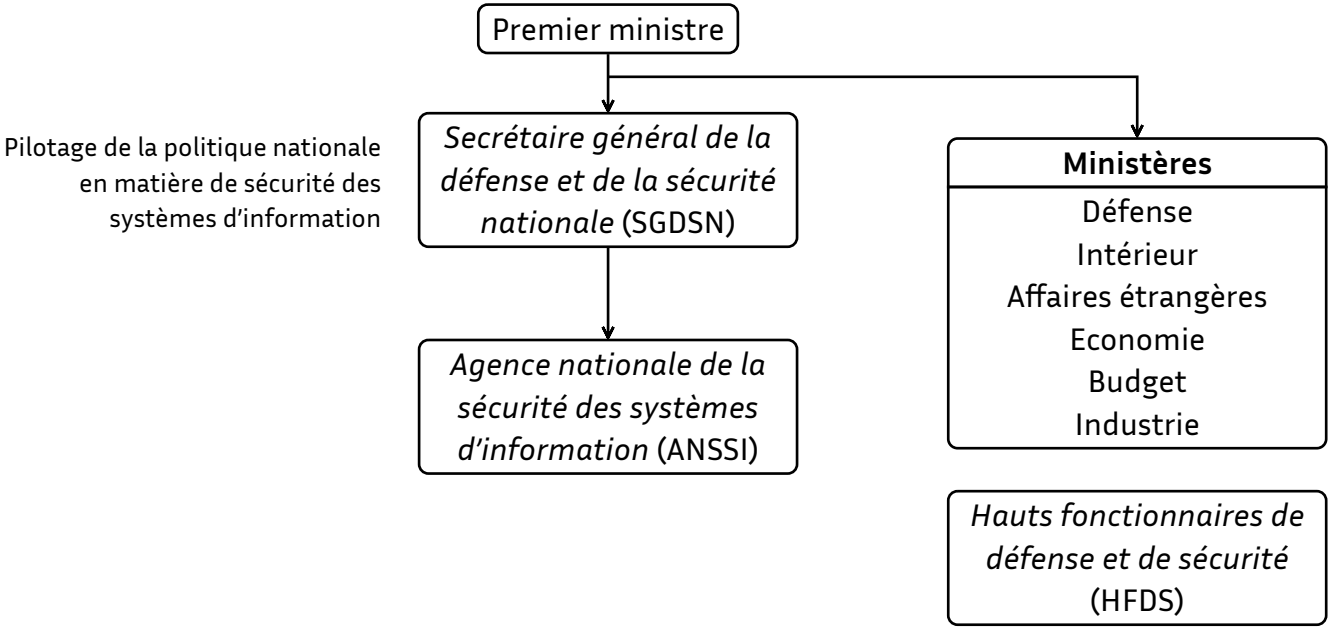
« Le développement de capacités de cyberdéfense militaire fera l'objet **d'un effort marqué** »

— Chapitre 7, Les moyens de la stratégie, , livre blanc 2013

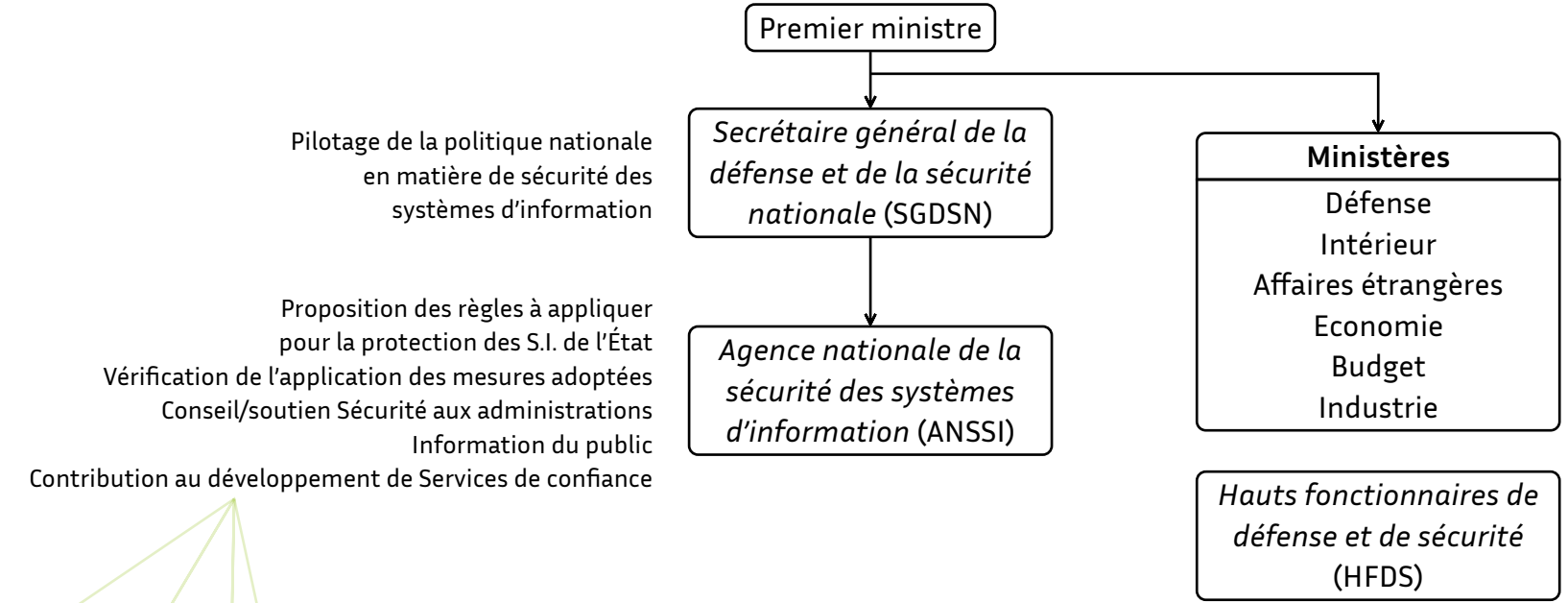
L'organisation de la sécurité en France



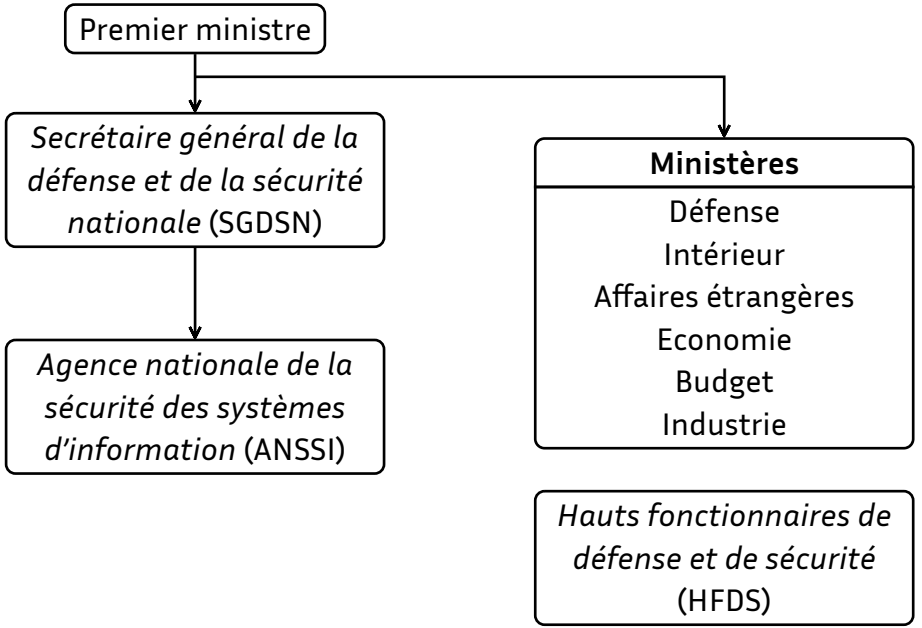
L'organisation de la sécurité en France



L'organisation de la sécurité en France



L'organisation de la sécurité en France

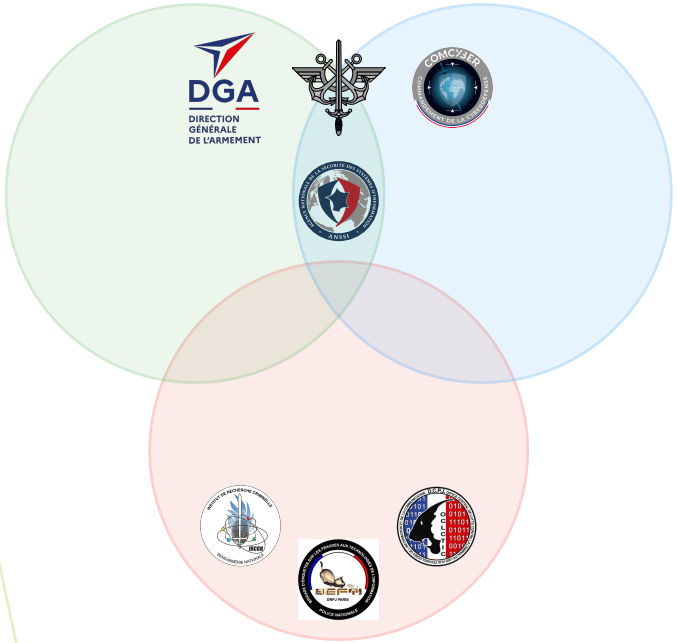


Pilotage de la politique nationale en matière de sécurité des systèmes d'information

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

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

L'organisation de la sécurité en France



Cybersécurité = SSI + Cyberdéfense + Cybercriminalité

DGA
Direction Générale de l'Armement

EMA
États Majors des Armées

ANSSI
Agence Nationale de la Sécurité des Systèmes d'Information

COMCYBER
Commandement de la Cyberdéfense

IRCGN
Institut de Recherche Criminelle de la Gendarmerie Nationale

OCLCTIC
Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication

BEFTI
Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information

Le contexte juridique

Quels domaines doivent être couverts ?

Liberté d'expression

Protection du e-commerce

Protection de la propriété intellectuelle

Protection de la vie privée

Protection des entreprises

Cybercriminalité

… et bien d'autres…

Le droits des T.I.C.

Le droit des *Technologies de l'Information et de la Communication* (T.I.C.) est non codifié : des dizaines de code en vigeurs difficiles d'accès.

- → Au carrefour d'autres droits
- → En évolution rapide et constante
- → Issu de textes de toute nature
- → Caractérisé par une forte construction jurisprudentielle

Nécessite un effort de veille juridique

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.

La lutte contre la cybercriminalité en France

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

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

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

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

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

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

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. »

Le rôle de la CNIL : La protection des 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

Le rôle de la CNIL : La protection des 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).

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)

Sanctions pénales

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)

Sanctions civiles

Dommages-intérêts en fonction du préjudice causé aux personnes concernées.

Sanctions administratives

- → 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

Merci de votre attention