Sensibilisation et initialisation à la sécurité

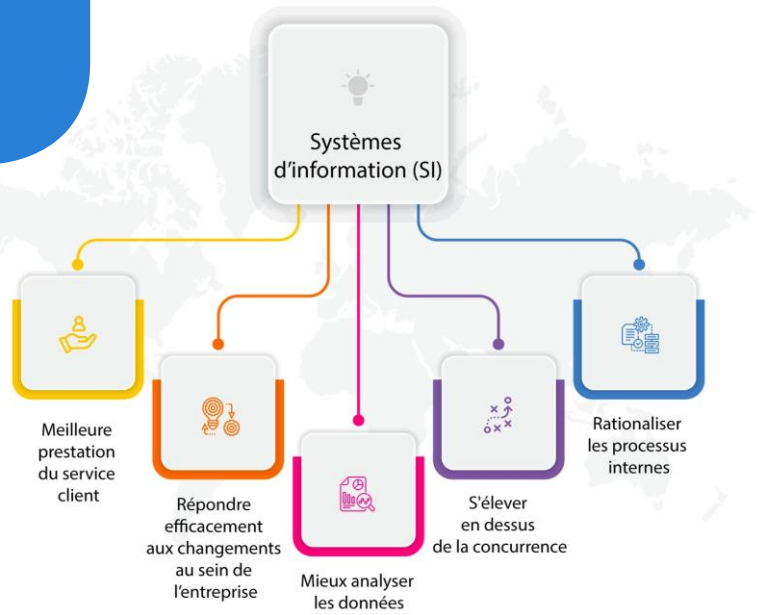
Notions de base

Concepteur Développeur d'Applications

Afpa
se former, avancer

Les enjeux de la sécurité

1. Préambule
2. Les enjeux
3. Pourquoi les pirates s'intéressent aux S.I. ?
4. La nouvelle économie de la cybercriminalité
5. Les impacts sur la vie privée
6. Les infrastructures critiques
7. Quelques exemples d'attaques

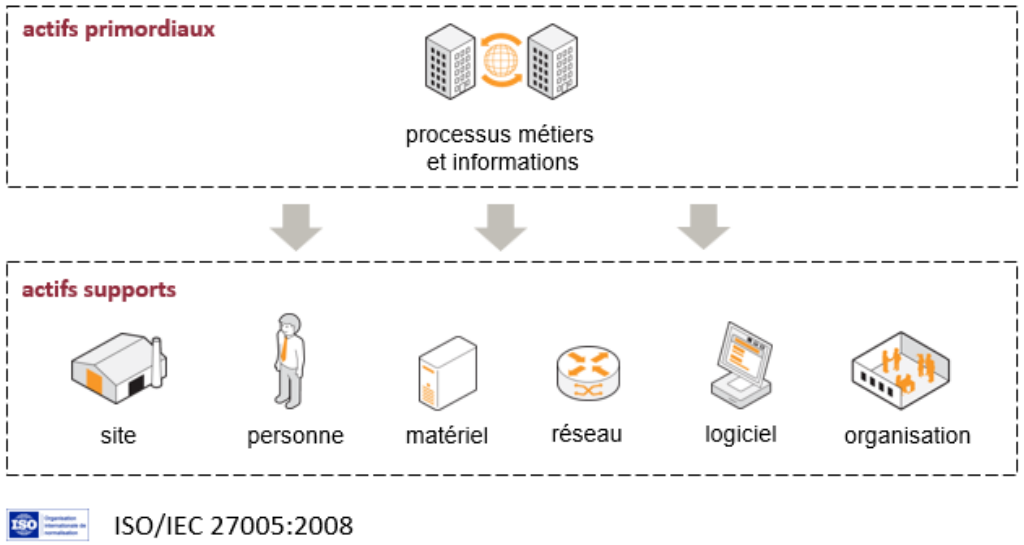


Préambule

Bien distinguer le SI d'une entreprise d'un système informatique ou d'un système d'exploitation

- Le Système d'information (SI)
  - C'est un ensemble des ressources destinées à collecter, classifier, stocker, gérer, diffuser les informations au sein d'une organisation.
  - Il représente une large surface d'exposition aux attaques, qu'il faudra prendre en compte globalement dans une approche sécurité.
- C'est le "nerf de la guerre" pour toutes organisations.

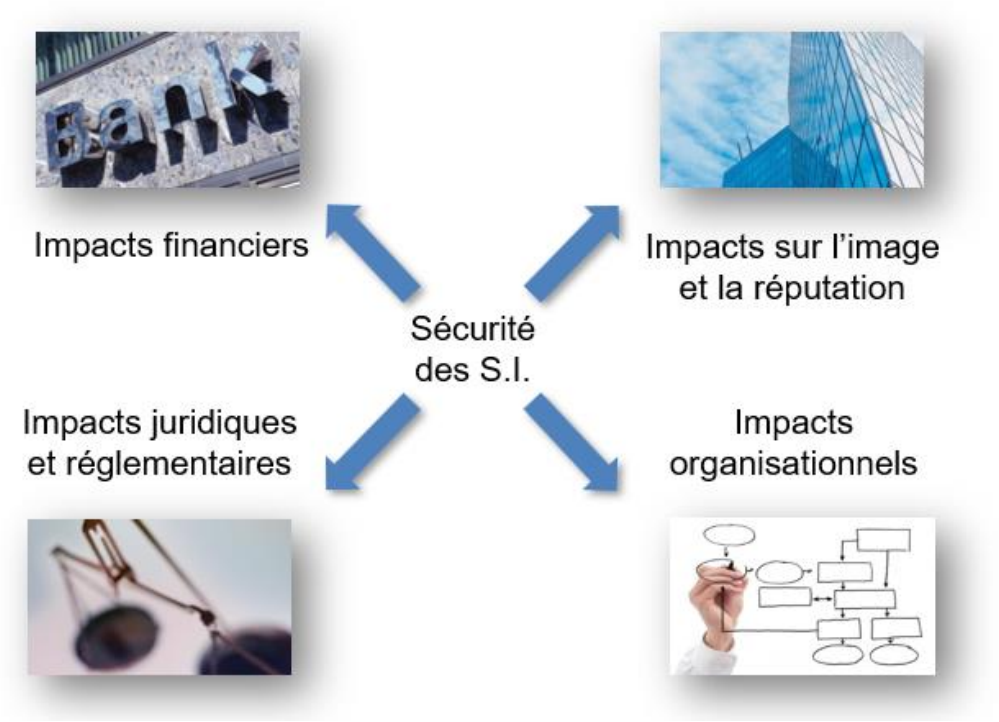
Préambule



ISO/IEC 27005:2008

- Le système d'information d'une organisation contient un ensemble d'actifs :
  - Les actifs primordiaux se rapportent au savoir-faire et à l'activité de l'entreprise : Processus métiers et informations sensibles (brevets, secrets industriels)
  - Les actifs supports se rapportent aux différents sites, le personnel, les matériels utilisés.
- Tous les actifs de l'organisation doivent être protégés. Norme ISO:IEC 27005 de gestion des risques.
- *Exemples :*
  - *cela ne sert à rien de mettre en œuvre une authentification si le mot de passe est envoyé en clair dans le réseau de l'entreprise…*
  - *Cela ne sert à rien de encrypter les données sensibles si celles-ci peuvent être accessibles sur papier…*
  - *Education du personnel à la sécurité*

Les enjeux



- Réduire les risques à un niveau acceptable pour limiter les impacts et non pas les éliminer
  - Risque zéro impossible.
- Une politique de sécurité doit être adaptée en fonction du domaine de l'entreprise et proportionnée les moyens de défense au niveau voulu.
  - Adhésion des utilisateurs et du personnel.
  - Ne pas gêner les utilisateurs et les salariés de l'entreprise dans leur quotidien.
- *Exemples :*
  - *Impacts juridiques et réglementaires : responsabilité de l'entreprise*
  - *Impacts sur l'image et la réputation : crédibilités de l'entreprise*
  - *Impacts organisationnels : attaques par déni de service - indisponibilité de l'entreprise*

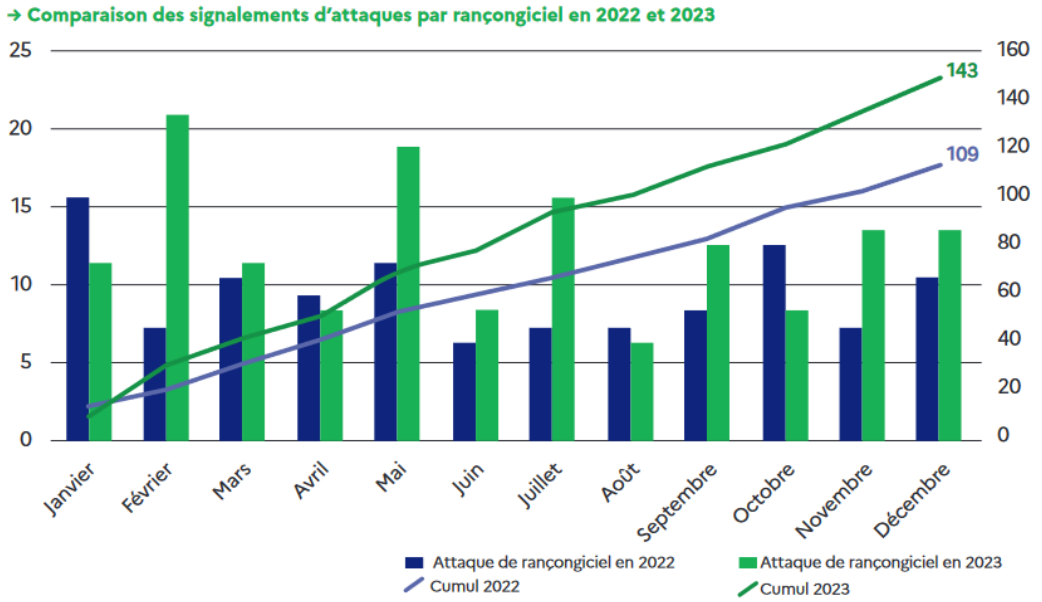
Pourquoi les pirates s'intéressent aux S.I. ?

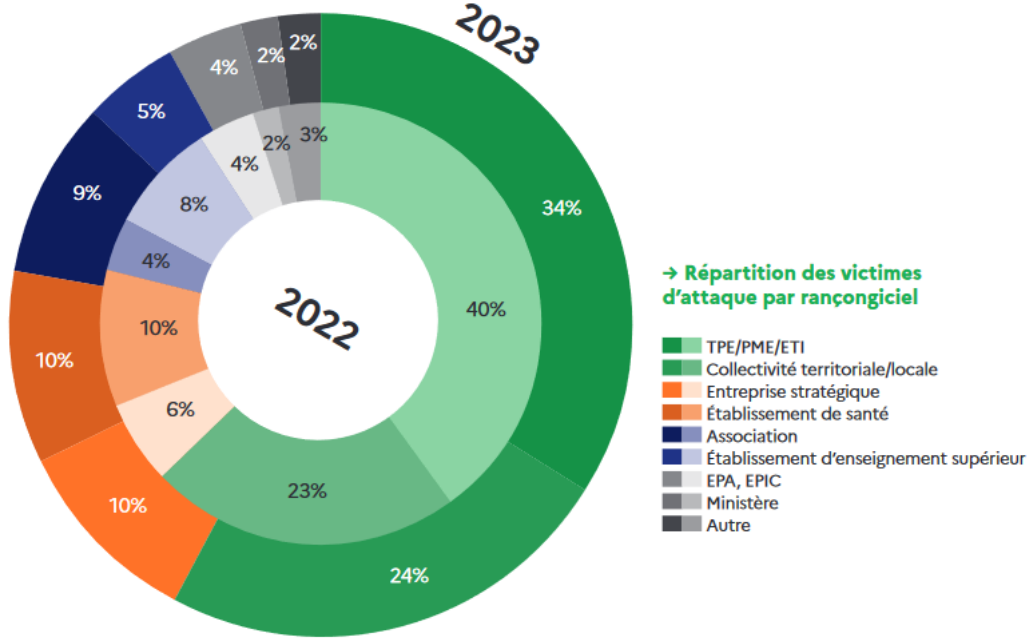
- Motivations :
  - De nos jours, majoritairement des actions organisées et réfléchies.
    - L'appât du gain
    - Les hacktivistes https://fr.wikipedia.org/wiki/Hacktivisme
    - Politiques, religieuses, etc..
    - Espionnage
    - Attaquer un état
    - Chantage
    - Utilisation de ressources pour revente ou mise à disposition (botnet, site de téléchargement)

- Nouvelle économie :
  - Une majorité des actes de délinquance réalisés sur Internet sont commis par des groupes criminels organisés, professionnels et impliquant de nombreux acteurs
    - Développement de programmes malveillants
    - Exploitation et de la commercialisation de services d'attaques informatiques
    - Hébergeurs de contenus malveillants
    - Vente de données volées
    - Intermédiaires financiers

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

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-001.pdf





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

Impacts sur la vie privée

- Diffamation
- Divulgation d'informations personnelles
- Harcèlement
- Usurpation d'identité
- Perte définitive de données
- Impacts financiers
- …

Impacts sur les infrastructures critiques

- Organisations classées Opérateur d'importance Vitale (OIV)
  - Liste classifiée gérée par l'Etat Français
  - Secteurs étatiques : civil, militaire, justice…
  - Secteurs de la protection des citoyens : santé, gestions de l'eau, alimentation
  - Secteurs de la vie économique et sociale : énergie, communication, électronique, audiovisuel, transports, finances, industrie.

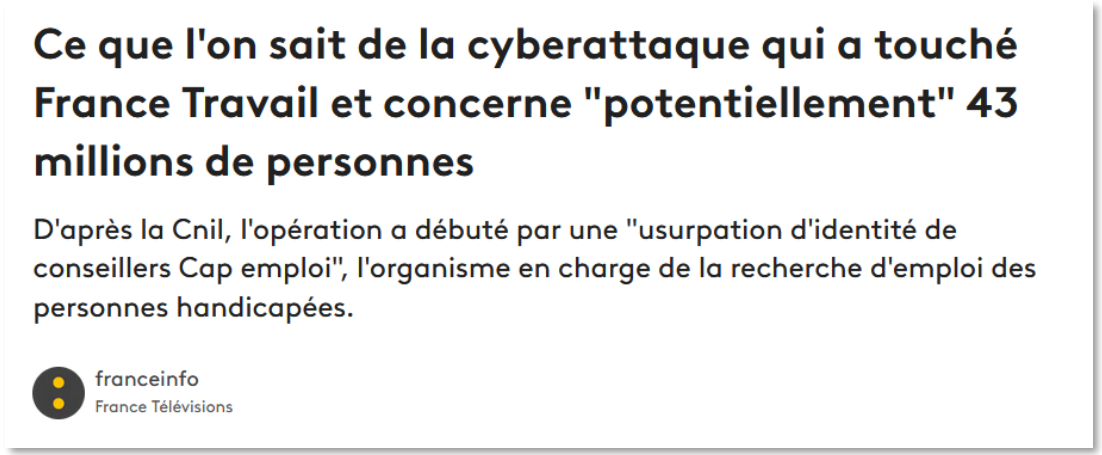
Pourquoi les pirates s'intéressent aux S.I. ?

La liste des hôpitaux touchés par une cyberattaque en 2022 :

- **Clinique Léonard de Vinci de Chambray-les-Tours** : attaque par ransomware le 7 janvier. Les malfaiteurs ont demandé 500 000 euros de rançons.
- **Cité sanitaire de Saint-Nazaire** : attaquée le 12 janvier, les patients sont privés de télévision, d'Internet et de communication avec leurs proches.
- **Hôpital de Castelluccio, Ajaccio** : touché par un ransomware le 28 mars, les soins de radiologie et oncologie étaient suspendus.
- **L'hôpital de Saint-Dizier et de Vitry-le-François** : victimes d'un ransomware le 19 avril. Les auteurs exigeaient une rançon de 1,2 million d'euros.
- **Centre hospitalier de Mâcon** : touché le 27 mai.
- **Centre hospitalier de Corbeil-Essonnes :** attaque par ransomware le 20 août, revendiquée par Lockbit. Demande de rançon de 1 million d'euros.
- **Hôpital de Cahors** : cyberattaque le 12 septembre.
- **Maternité des Bluets, Paris XIIIe** : touchée par un ransomware le 9 octobre, revendiqué par Vice Society.
- **Hôpital André-Mignot, Versailles** : attaque par ransomware le 3 décembre.
- **Centre hospitalier d'Argenteuil (déjoué)** : tentative d'intrusion début décembre.
- **CHU Nice (déjoué)** : touché le 3 décembre, le pare-feu a bloqué l'opération.

https://www.numerama.com/cyberguerre/1208398-cyberattaques-la-liste-des-regions-departements-et-villes-impactes-en-2022.html

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



Ce que l'on sait de la cyberattaque qui a touché France Travail et concerne "potentiellement" 43 millions de personnes

D'après la Cnil, l'opération a débuté par une "usurpation d'identité de conseillers Cap emploi", l'organisme en charge de la recherche d'emploi des personnes handicapées.

franceinfo
France Télévisions

https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/ce-que-l-on-sait-de-la-cyberattaque-qui-a-touche-france-travail-et-concerne-potentiellement-43-millions-de-personnes_6423817.html

Cyberattaque chez Viamedis et Almerys : ce que l'on sait du vol de données de plus de 33 millions d'assurés en France

L'état civil, le numéro de Sécurité sociale et des informations sur la mutuelle ont été dérobés, a révélé mercredi la Cnil. En revanche, les informations bancaires ou médicales ne feraient pas partie des données volées.

franceinfo avec AFP
France Télévisions

https://www.francetvinfo.fr/sante/cyberattaque-chez-viamedis-et-almerys-ce-que-l-on-sait-du-vol-de-donnees-de-plus-33-millions-d-assures-en-france_6352741.html

Les besoins de sécurité

1. Les critères DIC
2. Besoin de sécurité : « Preuve »
3. Différences entre sureté et sécurité
4. Exemple d’évaluation DICP
5. Mécanisme de sécurité pour atteindre les besoins DICP

Critères DIC

3 critères pour l'accès aux données

- **D**isponibilité
  - 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)
- **I**ntégrité
  - Propriété d'exactitude et de complétude des biens et informations (i.e. une modification illégitime d'un bien doit pouvoir être détectée et corrigée)
- **C**onfidentialité
  - Propriété des biens de n'être accessibles qu'aux personnes autorisées

Besoin de sécurité : Preuve

Les trois premiers critères sont des besoins de sécurité essentiels. Le quatrième critère, la Preuve, est une mesure de la sécurité d'un système

- **P**reuve
  - Propriété d'un bien permettant de retrouver, avec une confiance suffisante, les circonstances dans lesquelles ce bien évolue.
  - Le critère de Preuve est indispensable pour qu'un système informatique ait une valeur juridique
  - Cette propriété englobe :
    - **La traçabilité** des actions menées (logs)
    - **L'authentification** des utilisateurs
    - **L'imputabilité** du responsable de l'action effectuée

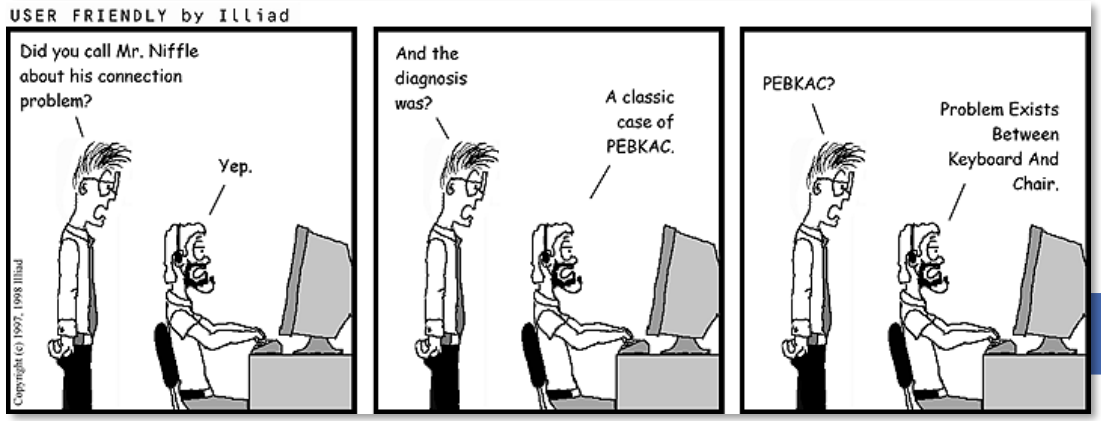
Différences entre sûreté et sécurité

Sûreté

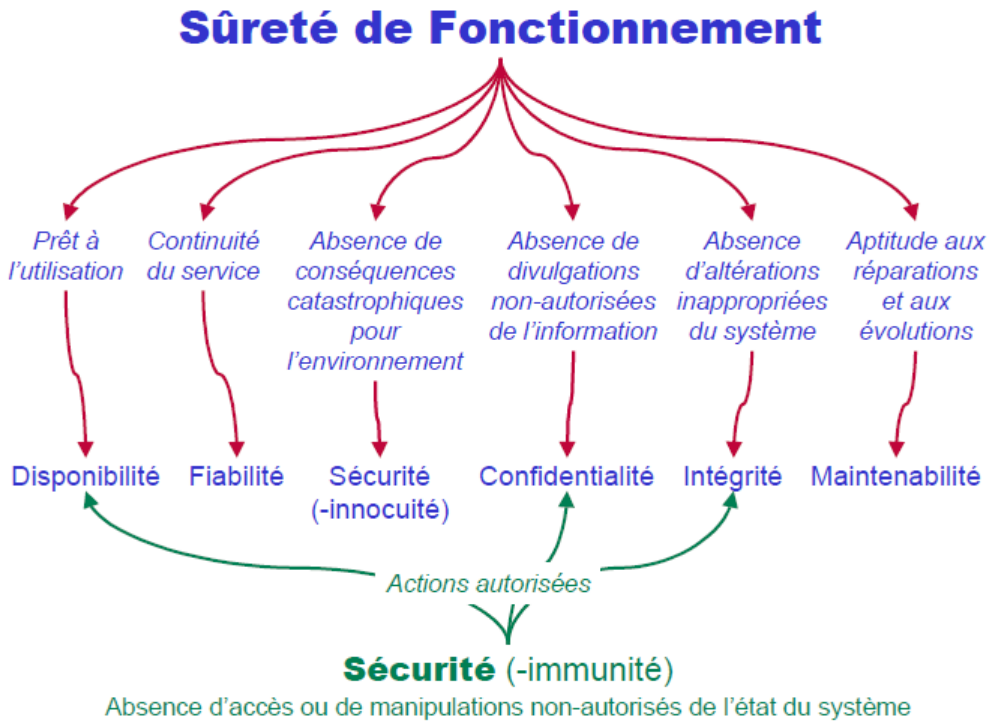
- Protection contre les dysfonctionnements et accidents involontaires
  - Saturation d'un point d'accès, panne d'un disque, erreur d'exécutions
  - Parades : sauvegarde, redondance des équipements
- La « sûreté » d'un logiciel : il est bien conçu, bien codé et fonctionne comme prévu dans son cahier des charges, dans des conditions normales d'utilisation.
  - Erreurs de saisies
  - Parades : contrôle des saisies, gestion des exceptions et des cas d'erreurs

Sécurité

- Protection contre les actions malveillantes volontaires
  - Blocage d'un service, modification d'informations, vol d'informations
  - Parades : contrôles des accès, veille sécurité, correctifs, …
- La « *sécurité* » d'un logiciel : sa capacité à résister à des utilisateurs et des actions malveillantes.



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.

Exemple d'évaluation DICP

Exemple du site Web statique

- **Disponibilité et Intégrité**: ce sont ses atouts majeurs. Un site perd une bonne partie de ses visiteurs à chaque indisponibilité. Et c'est encore pire s'il est « défacé » avec des faux produits, des prix erronés.
- **Confidentialité et preuve** : faible, puisqu'il est par nature public et que l'utilisateur ne fait que consulter les informations.
    - Forte : C'est bien sûr très différent pour un site dynamique de commerce en ligne, où il faut garantir la confidentialité de l'achat et sa preuve juridique (validation de la carte bancaire).

Mécanisme de sécurité pour atteindre les besoins DICP

Type	Description	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.	✓	✓	✓	

Notions de vulnérabilité, menace, attaque

1. Notion de « Vulnérabilité »
2. Notion de « Menace »
3. Notion d'« Attaque »
4. Exemple de vulnérabilité lors de la conception d'une application

Notion de vulnérabilité

définition

- Une vulnérabilité est une 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).
- *Exemples*
  - *Envoi d'un mot de passe en clair dans un lieu public*
  - *Configuration : Définition d'un mot de passe trop faible*
  - *Réalisation : codage défensif non effectué ou tests non effectués*

Notion de menace

Définition

- Une menace est une cause potentielle d'un incident qui pourrait entrainer des dommages sur un bien si cette menace se concrétisait.
- Un système d’information sécurisé est organisé comme un château fort avec des fossés et un donjon. Il est prévu pour se défendre contre un attaquant extérieur, et il est plus vulnérable contre une menace interne (le « stagiaire malintentionné »).

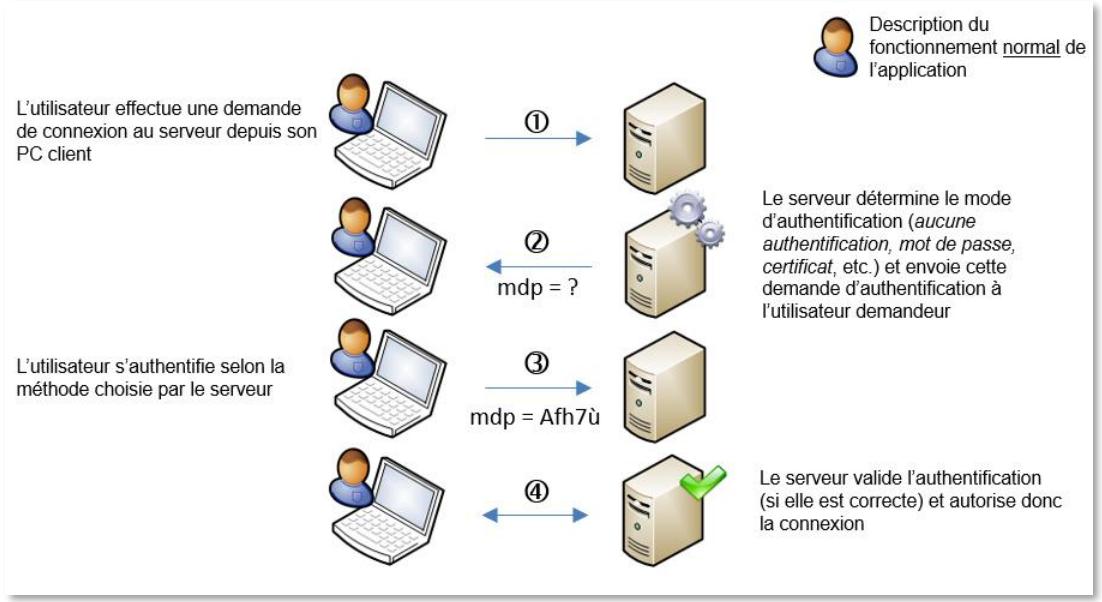
Notion d'attaque

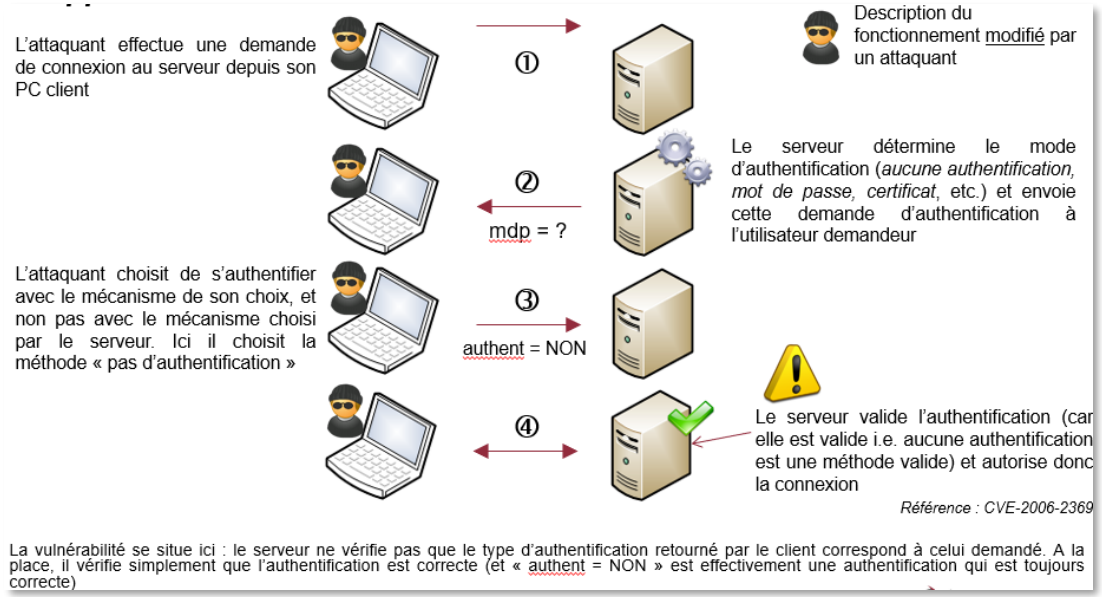
Définition

- Une attaque est une 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.
- Une attaque ne peut donc avoir lieu et réussir que si le bien est affecté par une vulnérabilité.
- **L'objectif final des experts sécurité est de maitriser ces vulnérabilités plutôt que de viser l'objectif 0**

Exemple de vulnérabilité lors de la conception d'une application

Exemple : en 2006 : Contournement de l'authentification dans l'application VNC



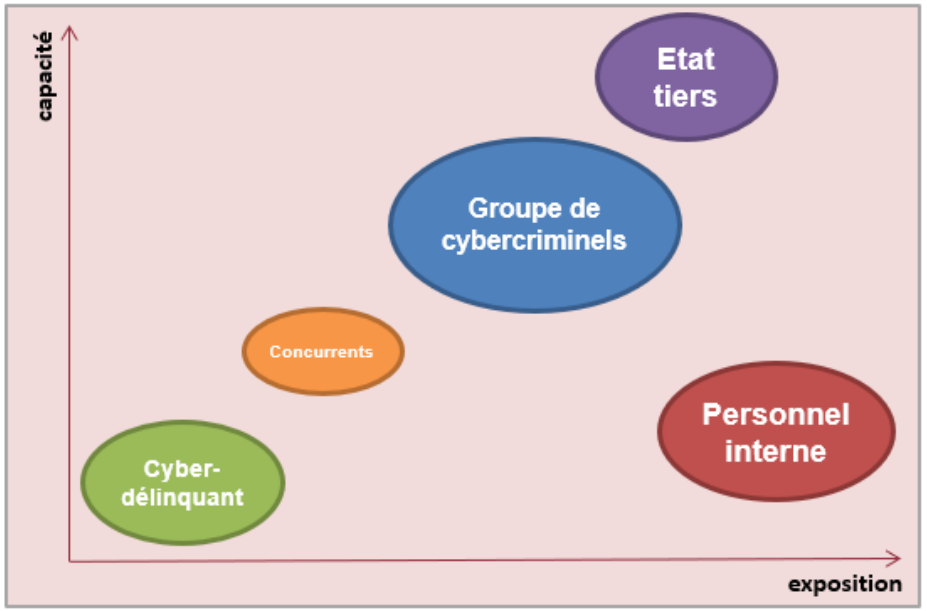


Panorama de quelques menaces

1. Les sources potentielles de menaces
2. Panorama de quelques menaces
3. Hameçonnage & ingénierie sociale
4. Déroulement d'une attaque avancée
5. Violation d'accès non-autorisé
6. Fraude interne
7. Virus informatique
8. Déni de service Distribué (DDoS)
9. Illustration d'un réseau de botnets

Panorama de quelques menaces

Sources potentielles de menaces



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

Un schéma pour lutter contre les idées reçues.

- A noter :
  - Le hacker ou cyber-délinquant individuel est au bas de l'échelle des menaces, car il est à l'extérieur de l'entreprise et a relativement peu de connaissances et de ressources techniques pour mener à bien ses attaques
  - Le personnel interne a un accès plus direct aux ressources de l'entreprise, et constitue une menace plus importante
  - Les états sont des menaces importantes, car ils ont des ressources techniques considérables et une motivation (espionnage militaire ou industriel).

Panorama

Hameçonnage & ingénierie sociale

- Ces deux attaques visent le même objectif : récupérer des données confidentielles, à des fins d'escroquerie ou de prise de contrôle du système d'information.
  - Le phishing ou Hameçonnage comporte toujours une partie technique. Il faut construire un faux site Web qui se fait passer pour le vrai, et qui va capturer l'identifiant et le mot de passe
  - L'ingénierie sociale n'a pas nécessairement de partie technique. On peut appeler l'ingénieur système, en se faisant passer pour un collègue en clientèle qui a oublié le mot de passe système.

Panorama

Fraude interne

- La fraude interne est un sujet tabou pour les entreprises, mais un véritable sujet d'importance !
- La plus dangereuse, car l'attaquant est déjà dans les murs et la plupart des dispositifs de défense sont ciblés pour des attaquants extérieurs.

Panorama

Violation d’accès non autorisé - mot de passe faible

- C’est une attaque simple mais répandue, qui vise à la fois les entreprises et les individus.
- Une sécurité s’écroule s’il y a au moins un maillon faible
  - il ne sert à rien de bien concevoir et coder un logiciel avec une méthode d’authentification fiable, si à la fin l’administrateur choisit « abc » ou « toto » comme mot de passe système
- Solutions
  - Double authentification
  - One time password

Panorama

Violation d’accès non autorisé - intrusion

- La compromission d’un domaine d'un Active Directory signifie que certains comptes sont piratés et que des utilisateurs malveillants peuvent se connecter sur les postes de travail et/ou les serveurs du domaine.
- Solutions
  - Cloisonnement des réseaux
  - Test d'intrusion

Panorama

Virus, Déni de service et Botnet

- Les virus informatiques constituent des attaques massives, de plus en plus ciblant un secteur d'activités, de plus en plus sophistiqués et furtifs.
  - Cheval de troie
- Déni de service (DDoS) constitue une attaque ciblée d'un service en le saturant de requêtes web pour le mettre hors service à l'aide de botnets, réseaux d'ordinateurs infectés et contrôlés par les attaquants.

Les droits des T.I.C et organisation de la cybersécurité en France

1. L’organisation de la sécurité en France
2. Le droit des T.I.C.
3. La lutte contre la cybercriminalité en France
4. Le rôle de la CNIL : La protection des données à caractère personnel

En France

La Cyber Sécurité est devenue un enjeu national, qui justifie d'introduire les concepts et la pratique de la sécurité dans toutes les formations informatiques, dont celles du développement informatique

- La Cyber Sécurité regroupe trois notions :
  - la SSI (Sécurité des systèmes d'information),
  - la Cyber Défense (aspect militaire, attaques étatiques),
  - la Cyber Criminalité (attaques d'individus, de mafia).

L'organisation de la sécurité en France

Organisation interministérielle :

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

Premier Ministre

Secrétaire général de la défense et de la sécurité nationale (SGDSN)

Agence nationale de la sécurité des systèmes d'information (ANSSI)

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

Sensibilisation et initialisation à la cybersécurité

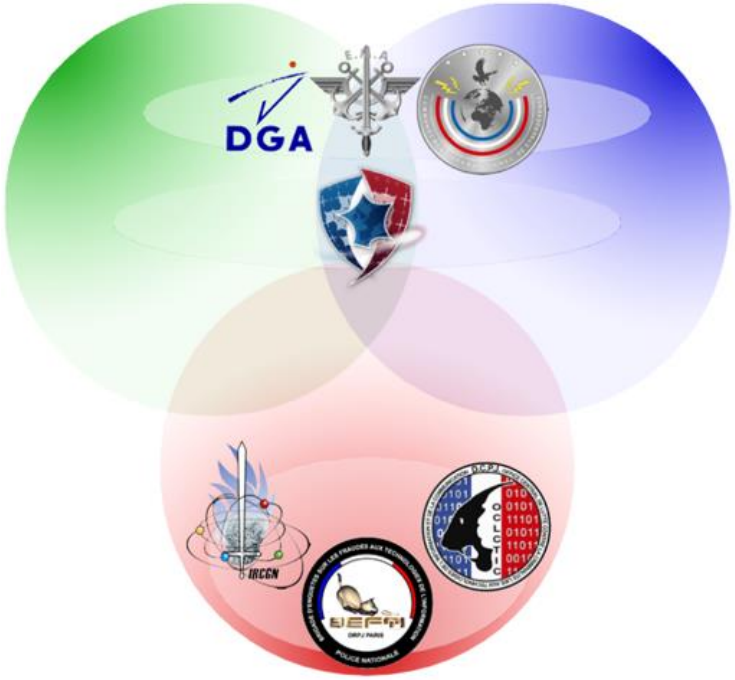
Ministères

Défense
Intérieur
Affaires étrangères
Economie
Budget
Industrie
...

Hauts fonctionnaires de défense et de sécurité (HFDS)

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

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"

*Technologie de l'information et de la communication

Le droit des T.I.C*

Un droit non codifié : des dizaines de codes en vigueur … et difficile d'accès

- Code de la défense
- Code civil
- Code pénal
- Droit du travail
- Code de la propriété intellectuelle
- Code des postes communication électroniques
- Code de la consommation
- …
- D'où la mise en place de droits spécifiques pour les T.I.C depuis quelques années. (HADOPI par exemple)

La lutte contre la cybercriminalité en France

A noter

- L'importance de la condamnation pénale (2 à 5 ans) qui est souvent méconnue du public.
- La définition des délits qui n'est pas intuitive : accéder indument à un système d'information, sans nuire à l'entreprise, est passible de 2 ans de prison ferme.
- Le périmètre de la cybercriminalité qui concerne tous les STAD (Système de Traitement Automatisé de Données) : postes de travail et serveurs mais aussi téléphones, réseau téléphonique, réseau bancaire, disque dur, etc.

CNIL

la Cyber Sécurité vise en général à protéger les systèmes informatiques contre des individus ou des organisations malveillantes.

- La CNIL joue le rôle de contre-pouvoir
- Elle défend le droit des individus face aux moyens informatiques
  - définition des données personnelles admissibles, procédures formalisées de déclaration de fichiers, droit à l'oubli sur Internet.
- https://www.cnil.fr/fr

Liens utiles

La Cyber Sécurité est un métier à part entière, mais c'est aussi une compétence utile pour tout développeur, qu'il faut entretenir, car elle évolue vite !

- il est conseillé de s'intéresser à l'actualité de la sécurité informatique (attaques, vulnérabilités, menaces) en menant une veille technologique personnelle.
- L'ANSSI, organisme de référence français : http://www.ssi.gouv.fr/
- - Le CERT, référence pour les alertes de sécurité : http://www.cert.ssi.gouv.fr/
- - OWASP, référence pour le développement web : https://www.owasp.org

MERCI !

Document produit sur la base des documents suivants :

- **CyberEdu : Sensibilisation et initiation à la cybersécurité (année 2004)**
- **Afpa - Sensibiliser à la sécurité informatique (année 2018)**

Jérôme BOEBION

2024 - v1.0