# Introduction à la Sécurité Informatique

Grégoire Roumache

Décembre 2019

## 1 Principes de sécurité informatique

- **Système d'information** (SI) = ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information. Composé de 2 sous-systèmes:
  - sous-système social = structure organisationnelle et des personnes liées au SI
  - sous-système technique = technologies (hardware, software)
- **Système informatique** = outil au service du SI.
- Objectif de la sécurité = réduire les risques et limiter leurs impacts sur le fonctionnement des organisations.
- Enjeux et impacts de la sécurité des SI:
  - impacts financiers,
  - impacts sur l'image et la réputation,
  - impacts juridiques et réglementaires,
  - impacts organisationnels.
- Sécurité des SI — Domaines d'applications:
  - sécurité du web,
  - sécurité des données,
  - sécurité des applications,
  - sécurité des réseaux,
  - sécurité du système d'exploitation,
  - sécurité physique.
- Sûreté v.s. Sécurité — au-delà du vocabulaire, garder à l'esprit les 2 facettes du danger:
  - les accidents involontaires,
  - les actions malveillantes volontaires.
- Le raisonnement de Mr X est le suivant: "comme j'ai, à tout moment, une copie de mon fichier dans le cloud, mon ordinateur est sécurisé". Qu'en pensez-vous ?

> Faux: l'ordinateur peut toujours être piraté. Et il y a des risques particuliers à utiliser le cloud, ex: l'entreprise qui gère le cloud fait faillite.

- 3 objectifs principaux à ne pas perdre de vue:

  1. **Confidentialité**

     > A et B échangent un message. Ils doivent rester les seuls à en connaître le contenu.
     > Danger = accès non-désiré à l'information (accidentel ou intentionnel)

  2. **Intégrité**

     > A et B échangent un message. B le reçoit tel que A l'a envoyé (non-modifié).
     > Danger = altération non-désirée de l'information (accidentelle ou intentionnelle)

  3. **Disponibilité**

     > Les systèmes informatiques doivent rester opérationnels pour permettre l'accès constant à la ressource souhaitée.
     > Danger = non-disponibilité (accidentelle ou intentionnelle)

- Autres objectifs importants — la triade AAA:

  4. **Authentification**

     > A et B doivent disposer d'un moyen technique de prouver qui ils sont.
     > Danger = usurpation d'identité

  5. **Autorisation**

     > A, B et C accèdent à un fichier. C peut le lire, B peut aussi le modifier et A peut également le supprimer.
     > Danger = accès non-autorisé ou accès avec de mauvaises autorisations

  6. **Accounting** (= journalisation/auditabilité)

     > Le système doit fournir un outil permettant de dire qui fait quoi.
     > Danger = incapacité de déterminer qui ou comment on utilise les ressources du SI
     > Remarque: **Attention** au lien étroit entre cet objectif et la loi (tracker les utilisateurs...).

- Derniers objectifs:

  7. **Autenticité**

     > A envoie un message à B. B doit avoir une preuve que c'est bien A qui l'a envoyé.

  8. **Non-répudiation** (irrévocabilité)

     > Empêcher une entité (personne, entreprise) de nier une action accomplie.
     > Danger = nier volontairement des actions accomplies ou des engagements pris.

- Authentification v.s. Identification
  - Identification = répondre à la question: "qui êtes vous ?".
  - Authentification = en apporter la preuve.
- Causes de l'évolution des risques:
  - multiplication des systèmes d'informations,
  - démocratisation des outils informatiques,
  - généralisation des accès à Internet,
  - complexité des architectures,
  - diversification de la nature des données,
  - professionnalisations des acteurs malveillants, ...
- Motivations des attaques:

  - raisons politiques,
  - idéologiques,
  - financières,
  - ludiques, ...

- **Vulnérabilité** = faiblesse au niveau d'un bien (au niveau de la conception, réalisation, installation, configuration, utilisation).
- **Menace** = cause potentielle d'un incident.
- **Risque** = menace × vulnérabilité
- Criticité = probabilité du risque × impacts (= $P_{risque} \times impacts$)
  Remarque: la priorité est mise sur les mesures qui préviennent les événements les plus critiques.
- **Attaque** = action malveillante destinée à porter atteinte à la sécurité d'un bien. C'est la concrétisation d'une menace, elle exploite une vulnérabilité.
- **Qui fait quoi ?**
  - Black Hats = hacker malintentionné
  - Grey Hats = hacker parfois éthique et parfois pas
  - White Hats = hacker éthique
  - Script Kiddies = hacker inexpérimenté, utilise des programmes/scripts développés par d'autres
  - Cyber terroriste = personne détruisant de manière systématique des systèmes informatiques pour atteindre un but politique grâce à la menace ou l'intimidation
  - Hacktiviste = piratage informatique dans le but de favoriser des changements politiques ou sociétaux
  - Crackers = hacker qui casse des protections de sécurité (ex: logiciel avec clé d'enregistrement)
  - Carder = hacker qui pirate des cartes de crédit
  - Phreaker = personne exploitant frauduleusement les systèmes téléphoniques
  - **RSSI** = Responsable de la Sécurité des Systèmes d'Information
- Méthodologie du hacker:
  1. collecte de l'information
  2. intrusion
  3. (option) garantir un accès plus facile dans le futur
  4. reconnaissance interne
  5. (option) mouvement
  6. exécution de l'action voulue
  7. (option) couvrir les traces
- Différents types d'attaques:
  - Virus = programme malveillant qui se réplique et modifie des données/programmes
  - Ver = programme malveillant qui se réplique (sans modifier les données/programmes)
  - Cheval de Troie = programme malveillant caché à l'intérieur d'un programme à l'allure légitime
  - Spyware = logiciel "espion", récolte des informations sur le système ou l'utilisateur
  - Adware = force l'utilisateur à regarder des pubs ou se rend sur des sites pour générer des revenus publicitaires
  - Spam (pourriel) = messages envoyés à des fins publicitaires ou malveillantes
  - Ransomware = chiffre les données sur l'ordinateur et demande une rançon pour les déchiffrer
  - Phishing = site se faisant passer pour un site web authentique pour voler des données de connexion
  - DoS - DDoS = empêche ou limite fortement la capacité d'un système à fournir le service attendu
  - MitM (man in the middle) = interception des échanges entre 2 parties légitimes

## 2 Guide d'hygiène informatique

- Citer une technique permettant le cloisonnement des réseaux.

  > VLAN, switch, firewall, cloisonnement physique (= séparation physique)

- À qui est destiné une charte informatique ?

  > Destinée aux utilisateurs des systèmes informatiques, généralement mise à disposition des employés par l'employeur.
  > Dans le cas de l'hénallux, elle est signée par les représentants syndicaux (des profs et de l'administration) et la direction mais pas par une organisation représentant les étudiants.

- Journalisation:
  - De quoi s'agit-il ?

    > C'est l'enregistrement séquentiel dans un fichier ou une base de données de tous les événements affectant un processus particulier (application, activité d'un réseau informatique...).

  - Comment rendre son utilisation optimal ?

    > Tout enregistrer (toutes les applications ouvertes et quelles actions l'utilisateur prend, etc.).

  - Quelle est la différence avec le monitoring ?

    > monitoring = surveillance/mesure d'une activité informatique en temps réel (ex: mesurer les performances)
    > Autrement dit,
    > * monitoring = analyse en temps réel
    > * journalisation = enregistrement pour analyse plus tard

- **Définition**:
  - RSSI = Responsable de la Sécurité des Systèmes d'Information
  - Infogérant = prestataire **externe** de gestion ou d'exploitation d'un système informatique
  - Risques SSI = Risques de Sécurité des Systèmes d'Information
  - Hébergement mutualisé = serveurs informatiques dont les ressources sont attribuées dynamiquement à un ensemble d'utilisateurs
  - Appel d'offre = procédure permettant à un commanditaire de faire le choix de l'entreprise la plus à même de réaliser une prestation de travaux, fournitures ou services. Le but est de mettre plusieurs entreprises en concurrence.

- Notion intéressante: plan d'assurance sécurité PAS.

  > Remarque: PAS = Plan d'Assurance Sécurité.
  > Le PAS a pour but de préciser comment les prestataires se conforment aux exigences de cybersécurité définies par le maître d'ouvrage.

- Relais applicatifs
  - Autre terme pour *relai applicatif*.

    > Proxy (= logiciel intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges)

  - Protocole les utilisant fréquemment.

> HTTP (plus généralement, couche application: http, ssh, ftp, etc.)

- De quoi découlent les politiques de sécurité ?

> politiques de sécurité = plan d'actions définies pour maintenir un certain niveau de sécurité
> Elle découle de la stratégie de l'entreprise (??)

- Que veut dire "les procédures doivent être formalisées" ?

> Les procédures doivent être précises, nettes et exclure tout malentendu.
> Remarque: procédure = manière spécifiée d'effectuer un ensemble de tâches.

- Comptes services, utilisateurs et d'administration:
  - Quelle est la nomenclature pour identifier les comptes ?

    > "il est souhaitable de définir et d'utiliser une nomenclature simple et claire pour identifier les comptes de services et les comptes d'administration"

  - Donner un exemple (logiciel = Tech3d, utilisateur = Céline Heliot, admin IT = Louis Renard).

    > Noms des comptes:
    > * Céline Heliot = user-celine-heliot
    > * Louis Renard = admin-louis-renard
    >
    > Objectifs = connaître directement les droits des comptes àpd leurs noms.

- **Définitions**:
  - SSID Wi-Fi = nom du wifi
  - 802.1X = protocole d'identification wifi avec nom d'utilisateur et mot de passe (comme à l'hénallux)
- Condensat de mot de passe:
  - Autre terme plus utilisé.

    > hash

  - Est-ce robuste ?

    > oui, si on utilise une bonne fonction de hashage

- Authentification:
  - Pourquoi une authentification à 2 facteurs est plus robuste ?

    > Car plus difficile de voler deux facteurs qu'un seul.

  - Authentification multi-facteurs:
    * Quelque chose que je sais,
    * Quelque chose que je possède,
    * Quelque chose que je suis.
  - Le dernier facteur d'authentification (ce que je suis) est-il une bonne idée ?

    > Non. Une fois que ce facteur est compromis, il est difficile à changer, vu qu'on ne peut pas se changer soit même.

  - Qu'est-ce qu'une carte RFID ?

    > Une carte de radio-identification.

  - Donner un exemple de "Mécanisme de mots de passe à usage unique avec jeton physique".

> Lorsqu'on utilise le PC banking, le lecteur de carte créé un mot de passe à usage unique.

- Qu'est-ce qu'une application ou un serveur métier ?

> Une application métier sert à gérer l'activité de l'entreprise. L'application est existante ou développée selon les besoins métiers.

- Pourquoi le *backup* doit se faire sur des équipements déconnectés ?

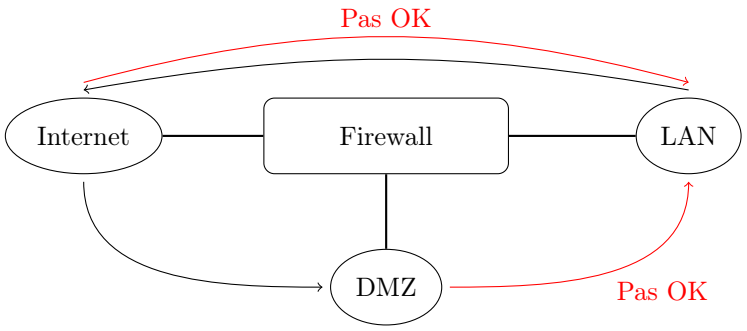
> Si ils sont connectés, ils sont vulnérables et on perd l'avantage de faire un backup.

- À quoi correspondent les ports que le document recommande de bloquer:
  - 135, 445 et 3389 pour Windows,
  - 22 pour Linux ?

> Ce sont les ports qui permettent de prendre le contrôle à distance de l'ordinateur.

- "les infrastructures d'hébergement Internet doivent être physiquement cloisonnées de toutes les infrastructures du système d'information qui n'ont pas vocation à être visibles depuis Internet"
  Quelle technique se cache derrière cette recommandation ?

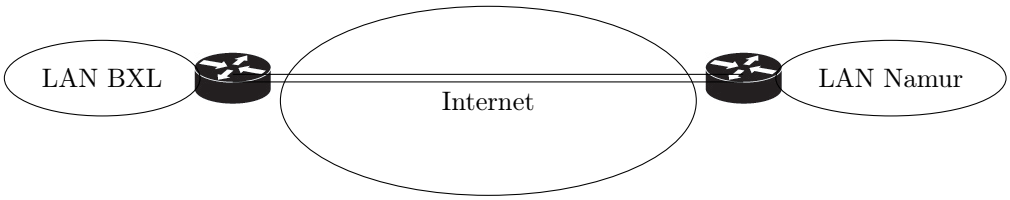
> Le pare-feu (firewall).




Remarque: DMZ = zone démilitarisée, peut contenir des serveurs web, ftp, smtp.

- Qu'est-ce qu'un tunnel « site à site » ? Sur quel appareil monter un tel tunnel ?

> C'est un tunnel VPN qui sert à communiquer de manière sécurisée sur internet. On monte ce tunnel sur des routeurs.



- Qu'est-ce qu'un serveur mandataire inverse ?

  > serveur mandataire inverse = reverse proxy
  >
  > - proxy = serveur permettant à un utilisateur d'accéder à internet
  > - reverse proxy = serveur permettant à un utilisateur d'internet d'accéder à des ressources internes

- Que sont les enregistrements DNS: MX, SPF, DKIM, DMARC ?

  > Des enregistrements mails (ex: MX = mail exchanger record).

- Quels outils pour la délégation de privilèges ?

  > **(??)**

- Quel est le risque de chiffrer ses données ?

  > De perdre la clé de déchiffrement.

- **Définitions**:
  - Adhérence logicielle = interdépendance entre programmes qui ont besoin les uns des autres pour fonctionner
  - Corrélation = lien, rapport réciproque
  - Protocole NTP = Network Time Protocol
  - EBIOS = méthode d'analyse de risque de l'ANSSI