Sécurité informatique

Université Alioune Diop de Bambey (UADB)

UFR SATIC-Département TIC

L3 SRT

Année académique 2022-2023

Objectifs du cours

- Ce cours a pour objectif de permettre aux participants de connaître la théorie et les bases de la sécurité des systèmes et réseaux informatiques ainsi que les principaux algorithmes de cryptographie.
- Objectifs intermédiaires :
  - Etudier les principales risques, menaces, failles et attaques passives/actives par intrusion ou déni de service ;
  - Connaître les mécanismes de défense matérielle (firewall, DMZ, VPN …) et logicielle basée sur le chiffrement ;
  - Maîtriser la cryptologie et connaître les algorithmes de chiffrement les plus couramment utilisés ;
  - Préconiser et mettre en œuvre des méthodes de protection des échanges de données basés sur des méthodes de filtrage des accès de tunneling ou de chiffrement ;
    - Vérification de l'intégrité des informations par hachage,
    - Authentifier des entités communicantes par signature,
    - Vérifier identité des émetteurs des clés échangés (clés publiques)
    - Générer de certificats de type X509 pour les échanges entre clients et serveurs.
  - Proposer des outils de prévention et de détection d'attaques dans un réseau ;

Plan du cours

- Chapitre 1 : Introduction à la sécurité informatique
  - Motivations et objectifs de la sécurité
  - Types et périmètres de sécurité, facteurs d'insécurité (vulnérabilité), risques et menaces de sécurité
- Chapitre 2 : Différentes types d'attaques des réseaux
  - Attaques actives/passives
  - Techniques d'intrusion (programmes malveillants, …)/Déni de service (DOS et DDOS)
- Chapitre 3 : Protection de l'information par cryptographie
  - Chiffrement symétrique : méthodes classiques (Substitutions et Transpositions et Variantes)
  - Chiffrement symétrique (DES, 3DES, AES) et asymétrique (RSA, …) modernes
- Chapitre 4 : Applications de la cryptographie
  - Hachage, signature numérique, authentification, certificats
- Chapitre 5 : Protocoles de sécurité
  - protocoles associés aux VPN et au chiffrement des informations,
  - protocoles pour sécuriser les applications et protocoles pour authentification.
- Chapitre 6 : Moyens de préventions et architectures sécurisées
  - Firewall, IDS/IPS
  - NAT, DMZ, Proxys, VPN

Chapitre 1 : Introduction à la sécurité

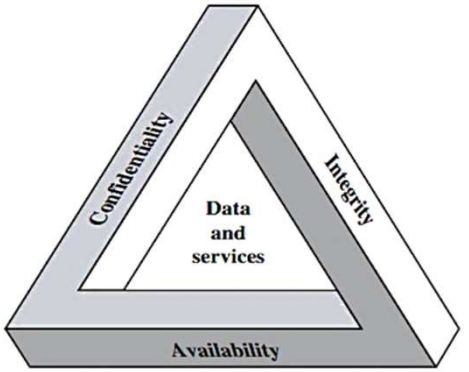
C’est quoi la sécurité?

Introduction à la sécurité

- Sécurité informatique : ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles.
- Développement de l'Internet ⟹ sécurité de l'information est aujourd'hui une véritable préoccupation pour les entreprises, opérateurs privés et administration.
- Entreprises ouvrent leur système d'information à leurs partenaires ou fournisseurs. Il est donc important de
  - connaître les ressources de l'entreprise (données médicales, financières, techniques pouvant être très convoitées) à protéger,
  - contrôler les communications entre le réseau interne et l'extérieur tout en respectant à la fois les besoins des utilisateurs et des applications.
- La confiance des utilisateurs passe par la sécurisation des transactions.
  - atteinte à l'image de l'entreprise,
  - perte de confiance des clients,
  - perte de recettes,
  - engagement de la responsabilité légale, …
- La sécurité est couteuse en moyens, en temps et surtout en ressources humaines.
- Politiques de sécurité basées sur des jugements humains et doivent de plus en plus être révisées en permanence pour s'adapter aux nouvelles attaques.

Objectifs de la sécurité

- Pour limiter les vulnérabilités, la sécurité vise généralement les objectifs suivants:
  - La **confidentialité** consiste à assurer que seules les personnes autorisées ont accès aux ressources et empêcher toute divulgation non autorisée d'informations sensibles.
  - L'**intégrité** permet de se protéger contre toute modification non autorisée d'information.
  - La **disponibilité** vise à garantir à tout moment l'accès à un service ou à des ressources.



CIA triad

- L'imputabilité est la possibilité d'attribuer une action à son auteur.
- La non-répudiation permet de s'assurer qu'une transaction a effectivement eu lieu et qu'aucun des correspondants ne peut la nier.
- L'audit permet l'enregistrement, le contrôle et l'évaluation de la sécurité.
- Authentification est un des moyens qui permet de garantir la confidentialité.

Types et périmètres de sécurité

- La sécurité informatique peut être divisée en 2 grands domaines :
  - sécurité organisationnelle : concerne la politique de sécurité d'une société
    - ✓ code de bonne conduite,
    - ✓ méthodes de classification et de qualification des risques,
    - ✓ plan de secours,
    - ✓ plan de continuité,
    - ✓ ….
  - sécurité technique : mise en œuvre toutes les recommandations et plans dans le domaine technique de l'informatiq
- Le périmètre de la sécurité est très vaste :
  - sécurité personnelle et sécurité physique des locaux,
  - sécurité des systèmes d'information et sécurité de l'information,
  - sécurité des communications,
  - sécurité des réseaux,
  - sécurité dans le développement d'applications,
  - Sécurité des systèmes d'exploitation,
  - …
- La plupart des incidents de sécurité surviennent par le réseau, et visent le réseau.

Facteurs d'insécurité

- Une formation du personnel est indispensable (règles de sécurité, déontologie, ...) pour une bonne sécurité.
- Les problèmes de sécurité qu'on peut rencontrer sur un réseau d'entreprise ou sur Internet relèvent d'abord de la responsabilité des victimes avant d'être imputables aux hackers.
- Plus de 50% des problèmes de sécurité ont pour origine les utilisateurs internes qui mettent le réseau en danger par leur comportement :
  - installation intempestives de logiciels de sources douteuses,
  - mauvaise utilisation du lecteur de courrier (en ouvrant automatiquement les fichiers attachés),
  - mots de passe "basique", "prêt" de mot de passe
  - trou dans le réseau par ignorance (modem, wifi) ou volontairement (utilisation à distance)

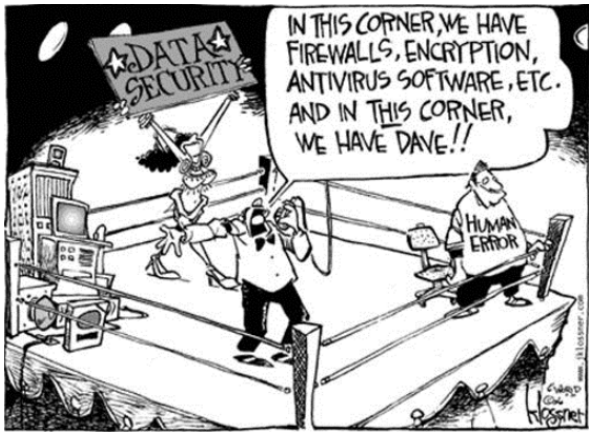
Notions importantes sur la sécurité

- Vulnérabilités (faiblesses) : degré de faiblesse inhérent à tout réseau ou périphérique. 3 types :
  - Faiblesses technologiques
  - Faiblesses de configuration
  - Faiblesses dans la stratégie de sécurité
- Menaces : viennent d'individus intéressés par l'exploitation des faiblesses de sécurité.
  - Les menaces engendrent des risques et coûts humains et financiers.
  - Les risques peuvent se réaliser si les systèmes menacés présentent des vulnérabilités.
- Attaques : variété d'outils, de scripts et de programmes permettant de lancer des attaques contre des réseaux et leurs périphériques.
- Risques : Quoi protéger ?
  - Données : contre divulgation, altération, perte ou dégradation
  - Ressources (serveur, disques, …) : contre le refus de service.
  - Réputation de l'entreprise et des personnes : contre usurpation d'identité.

$$risque = \frac{menace \times vulnérabilité \times sensibilité}{contre - mesure}$$

Etude des risques et menaces

- Origines des risques
  - ***Risques accidentels***
    - Risques matériels accidentels (incendie, explosion, inondation, ...)
    - Vol et sabotage
    - Panne et dysfonctionnement de matériel ou de logiciel de base
  - ***Risques d'erreur*** (saisie, transmission, exploitation, conception et réalisation)
  - ***Risques de malveillance***
    - Fraude, sabotage immatériel
    - Indiscrétion (espionnage industriel ou commercial), détournement d'informations
    - Détournement de logiciels (piratage)
    - Grève, départ de personnel stratégique
  - ***Risques humains***
    - Facteur humain

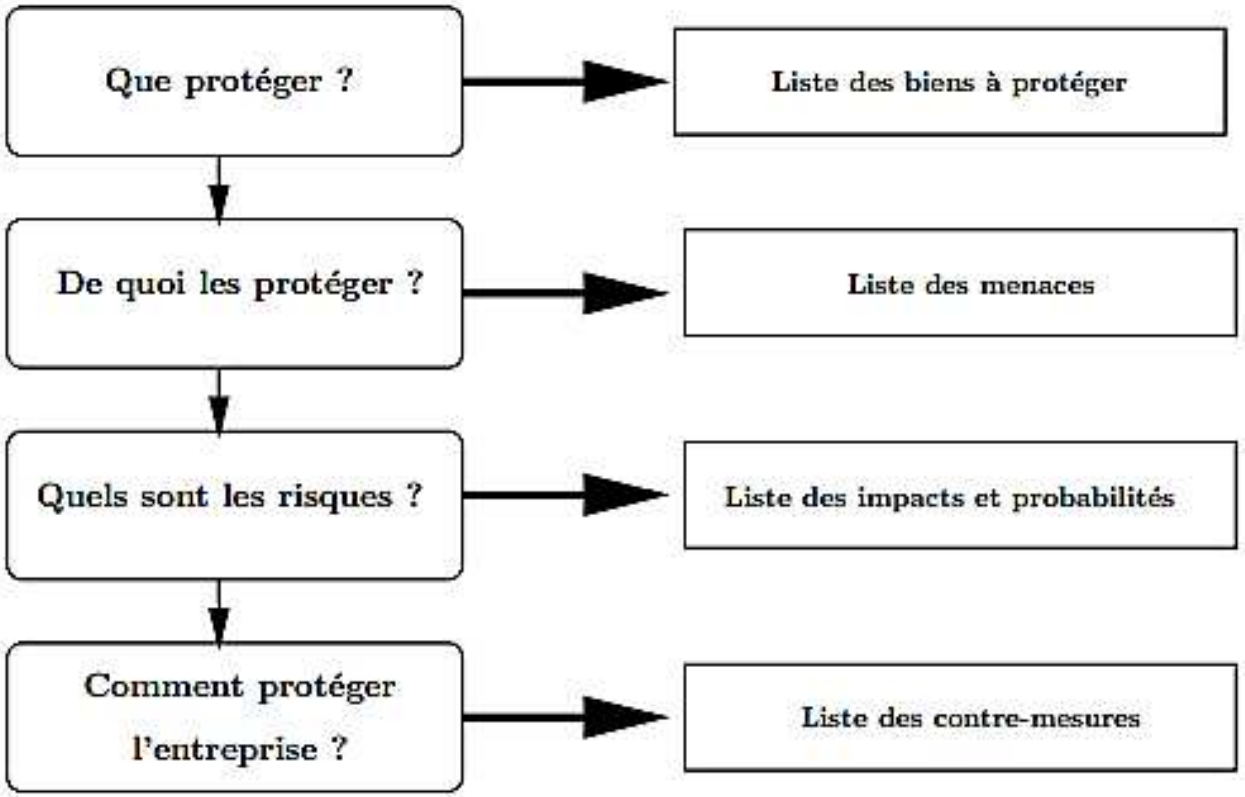


Etude des risques et menaces

- Il est nécessaire de réaliser une analyse de risque en prenant soin d'identifier les problèmes potentiels avec les solutions avec les coûts associés.
- L'ensemble des solutions retenues doit être organisé sous forme d'une politique de sécurité cohérente, fonction du niveau de tolérance au risque.
- On obtient ainsi la liste de ce qui doit être protégé.
- Quelques éléments de base à une étude de risque :
  - Quelle est la valeur des équipements, des logiciels et surtout des informations ?
  - Quel est le coût et le délai de remplacement ?
  - Faire une analyse de vulnérabilité des informations contenues sur les ordinateurs en réseau.
  - Quel serait l'impact sur la clientèle d'une information publique concernant des intrusions sur les ordinateurs de la société ?
- Les attaques exploitent les vulnérabilités du système.

Etude des risques et stratégie de sécurité

- **Stratégie de sécurité**



Etude des risques et stratégie de sécurité

- Les entreprises possédant un réseau local possèdent aussi un accès à Internet, afin d'accéder à la manne d'information et de pouvoir communiquer avec l'extérieur.
- Cette ouverture vers l'extérieur est indispensable et dangereuse en même temps.
- Ouvrir l'entreprise vers le monde signifie aussi laisser place ouverte aux étrangers pour essayer de pénétrer son réseau local, et y accomplir des actions douteuses, de destruction, vol d'informations confidentielles, ...

➢ Des produits existent sur le marché, qui permettent d'éviter ces problèmes. Chacune des technologies ou produits de sécurité d'un réseau a une couverture spécifique.

- Nécessaire de :
  - Disposer d'une sauvegarde de ses données.
  - Faire un audit des accès inutilement ouverts.
  - S'assurer que les comptes d'administration ont des mots de passe sécurisés.
  - Suppression des comptes utilisateurs non utilisés.
  - Désactiver les services non utilisés sur les machines et supprimer les partages de fichiers qui ne sont pas nécessaires.
- 1er stade de sécurité d'un intranet passe par un bon dimensionnement et une bonne gestion du réseau.

Etude des risques et stratégie de sécurité

- Démarche pratique pour la sécurisation d'un SI
- Maturité des entreprises