Cours: Sécurité Informatique

Chapitre 01 : Introduction à la sécurité

2022-2023

Objectifs du Cours

- A l ’issue de ce cours, vous aurez des idées sur les disciplines de la sécurité informatique :
  - Introduction/sensibilisation à la problématique de la sécurité.
  - Se familiariser avec le **vocabulaire** de la sécurité informatique.
  - **identification** des concepts de base de la sécurité informatique.
  - **Distinction** entre les différents aspect de sécurité.
  - Connaissance des différents techniques de sécurisation des systèmes d’information.

Chapitre 01: Introduction à la sécurité

Introduction

- Avec le développement de l'utilisation d'internet, de plus en plus d'entreprises ouvrent leur **système d'information** à leurs partenaires, il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information.
- **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.

Problématique

- Les SI évoluent dans un milieu « hostile » :
  - Concurrence économique.
  - Piratage.
  - Systèmes non-fiables.
  - Catastrophes climatiques.
  - Environnement politique.
  - Actes de destruction intentionnelle, accidentelle.
  - …
- Mise en place indispensable d'une Politique de prise en compte des risques $\Rightarrow$ **Sécurisation des SI**.

1.1 - Définitions

Sécurité informatique:

- La **sécurité des systèmes d'information** (**SSI**) ou plus simplement **sécurité informatique**, est l'ensemble des moyens **techniques**, **organisationnels**, **juridiques** et **humains** nécessaires visant à empêcher l'**utilisation non autorisée**, le **mauvais usage**, la **modification** ou le **détournement** du système d'information.

- Assurer la sécurité du système d'information est une activité du management du système d'information.

Différences entre sureté et sécurité

- « Sécurité » et « Sûreté » ont des significations différentes en fonction du contexte:

- **Sécurité :** Protection contre les **actions malveillantes volontaires**. C'est donc un 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 : modification d'informations, vol d'information, blocage d'un service, etc.

Différences entre sureté et sécurité

- **Sûreté :** Protection contre les **dysfonctionnements** et **accidents involontaires**. Elle consiste en un ensemble de mécanismes mis en place pour assurer la **continuité de fonctionnement** du système dans les conditions requises.

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

1.2 - Principaux concepts de sécurité informatique

- **Vulnérabilité:** Une faille ou une faiblesse dans un système informatique permettant à un attaquant de porter atteinte à **l'intégrité** de ce système, c'est-à-dire à son fonctionnement normal, à la **confidentialité** ou à **l'intégrité des données** qu'il contient.
- Elle provient dans la majorité des cas d'une faiblesse dans la conception d'un système d'information (SI), d'un composant matériel ou d'un logiciel, de la réalisation, de l'installation, de la configuration ou de l'utilisation du composant.
- **Sensibilité:** plus l'information est stratégique, plus elle a de valeur, plus elle doit être confidentielle et plus elle est sensible.

1.2 - Principaux concepts de sécurité informatique

- **Menace:** Les éléments nuisibles à une source sont appelés menaces, ou une **cause potentielle d'incident**, qui pourrait entrainer des **dommages** au système ou à l'organisation.
  - Code malveillant (virus…)
  - Personnes extérieures malveillantes (pirates…)
  - Perte de service
  - Stagiaire malintentionné
- La menace tentera d'être imperceptible afin d'y rester le plus longtemps possible sans être détectée.
- **Intrusion :** Opération qui consiste à accéder, sans autorisation, aux données d'un système informatique ou d'un réseau, en contournant ou en désamorçant les dispositifs de sécurité mis en place.

1.2 - Principaux concepts de sécurité informatique

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

- Une attaque ne peut donc avoir lieu (et réussir) que si le bien est affecté par une vulnérabilité.

- Ainsi, tout le travail des experts de 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.*

1.2 - Principaux concepts de sécurité informatique

- **Risque :** danger, inconvénient possible, sinistre éventuel …

- En sécurité c'est la possibilité qu'une menace exploite une vulnérabilité et crée un impact.

  Vulnérabilité × Menace = Risque

- Le risque informatique se mesure à la fois par la probabilité d'occurrence d'une menace et par le montant de la perte suite à sa réalisation.

  Risque = Probabilité × Potentiel de dommages

1.2 - Principaux concepts de sécurité informatique

Contre-mesures : Les mécanismes permettant de garantir la sécurité d'un système d'information, ils peuvent être :

1) Sécurité physique et environnemental (incendie, énergie, salles sécurisées, postes de travail des personnels, …)
2) Sécurité logique:
   - Qualité des développements logiciels et des tests de sécurité.
   - Mise en œuvre adéquate de la cryptographie pour assurer l'intégrité et la confidentialité.
   - Procédures de contrôle d'accès logique, d'authentification.
   - Procédures de détection de logiciels malveillants, de détection. d'intrusions et d'incidents.
   - Procédures de sauvegarde et de restitution des informations.
   - Validation et audit des programmes.
   - Classification des données et leurs sensibilités.

1.2 - Principaux concepts de sécurité informatique

Contre-mesures : (suite)

3) Sécurité des infrastructures (accès au réseau et du transport de l'information, sécurité de la gestion des noms, des adresses, du routage, des transmissions, ...)

4) Formation et sensibilisation des utilisateurs aux problèmes de sécurité.

1.3- Objectifs de la sécurité informatique :

- Un système d'information a besoin de mécanismes de sécurité qui ont pour objectif d'assurer les **objectifs** (**services**) suivants:
- La **confidentialité**: faire en sorte que l'information ne soit accessible qu'aux personnes autorisées à en savoir,
  - Seulement les personnes autorisées peuvent « comprendre / avoir accès » les données protégées.
- L'**intégrité**: Propriété d'exactitude et de complétude des biens et données (i.e. une altération (modification) totale ou partielle des données doit pouvoir être détectée et corrigée).
- La **disponibilité**: continuité de service et accessibilité à tout moment dans la plage d'utilisation prévue.

1.3- Objectifs de la sécurité informatique :

- L'**Authenticité**: Assure que l'identité d'une personne ou l'origine des données est indéniable et véridique.
- La **Non-répudiation**: Assure qu'une personne ne peut pas refuser d'avoir effectué une opération sur des données, l'auteur d'un acte ne peut nier l'avoir effectué.
  - L'engagement est contractuel et juridique, l'entité ne peut pas revenir en arrière.
- Cette propriété englobe notamment :
  - La **traçabilité** des actions menées.
  - L'**imputabilité** du responsable de l'action effectuée.
  - L'**authentification** des utilisateurs.

1.4- Menaces informatiques

Attaque:

En informatique une attaque est une tentative d'atteinte à des systèmes d'information réalisée dans un but malveillant.

- Elle peut avoir pour objectif de voler des données, de détruire, endommager ou altérer le fonctionnement normal de systèmes d'information en employant des ordinateurs en réseau.
- Les programmes malveillants ou indésirables s'exécutant à l'insu de l'utilisateur.

1.4- Menaces informatiques

Attaque: (suite)

Les attaques peuvent être classés en deux catégories principales:

- Attaques passives: atteinte à la confidentialité (prélèvement par copie, écoute de l'information sur les voies de communication, elles sont souvent indétectable, mais une prévention est possible).
- Attaques actives: tentent à modifier des données ou des messages, à s'introduire dans des équipements réseau ou à perturber le bon fonctionnement de système (modification, DoS, virus, ver, etc.…).

1.4- Les menaces informatiques

Les logiciels malveillants: (malware en anglais) est un logiciel développé dans le but de nuire à un système informatique.

- peuvent être classés en fonction des trois mécanismes suivants :
  - le mécanisme de propagation,
  - le mécanisme de déclenchement,
  - la charge utile.
- **Virus:** Un virus informatique est un logiciel autoréplicatif conçu pour se propager sur d'autres ordinateurs en s'insérant dans des logiciels ou documents légitimes, appelés « hôtes ».
  - Il se répand par tout moyen d'échange de données numériques, comme les réseaux informatiques ou les périphériques de stockage externes (clés USB, disques durs, etc.).

1.4- Les menaces informatiques

Les logiciels malveillants:

- **Ver:** Un ver est un programme capable de se propager et de se dupliquer par ses propres moyens sans contaminer de programme hôte.
- Un ver, contrairement à un virus informatique, n'a pas besoin d'un programme hôte pour se reproduire. Il exploite les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction.

1.4- Les menaces informatiques

Les logiciels malveillants:

- **Cheval de Troie :** un cheval de Troie est une version modifiée d'un logiciel légitime qui contient une fonctionnalité malveillante. Son but est de faire entrer cette fonctionnalité malveillante sur l'ordinateur et de l'installer à l'insu de l'utilisateur.
- Le programme contenu est appelé la charge utile. Il peut s'agir de n'importe quel type de malware : virus, keylogger, logiciel espion ou publicitaire... C'est ce malware qui va exécuter des actions au sein de l'ordinateur victime.

1.4- Les menaces informatiques

Les logiciels malveillants:

- **Logiciel espion:** Un logiciel espion, un mouchard ou un espiogiciel est un logiciel malveillant qui s'installe dans un ordinateur ou autre appareil mobile, dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, sans que l'utilisateur en ait connaissance.
  - **Enregistreur de frappe (keylogger):** programme généralement invisible installé sur le poste d'un utilisateur et chargé d'enregistrer à son insu ses frappes clavier;
  - **Le Rootkit:** ensemble de logiciels permettant généralement d'obtenir les droits d'administrateur sur une machine,
- **Logiciel de publicité indésirable (Adware) :** logiciel de publicité indésirable qui peut générer des annonces pop-up ou la redirection d'un navigateur à un site commercial.

1.4- Les menaces informatiques

- **Origine des attaques :** Une attaque peut émaner de personnes isolées, d'un groupe de pirates, de vastes organisations ayant des objectifs géopolitiques, de concurrents ou simplement de script kiddies (amateurs).

Les différents types d'attaques

1) Hameçonnage «phishing» & ingénierie sociale: consiste à exploiter la «faille humaine» en piégeant les victimes pour récupérer leurs mots de passe, identifiants de banque en ligne, numéros de carte bancaire, …

1) Réception d'un mail utilisant le logo et les couleurs de l'entreprise.
2) Demande pour effectuer une opération comme la mise-à-jour des données personnelles ou la confirmation du mot de passe.
3) Connexion à un faux-site identique à celui de l'entreprise et contrôlé par l'attaquant.
4) Récupération par l'attaquant des identifiants/mots de passe (ou tout autre donnée sensible) saisie par le client sur le faux site.

Les différents types d'attaques

1) Hameçonnage «phishing» & ingénierie sociale:

- Exemple de phishing d'un compte facebook.
- Le lien pointe en fait vers un site frauduleux, et non pas vers un serveur légitime de l'entreprise.

Les différents types d'attaques

2) Sniffing : Le reniflage (en anglais Sniffing) est une technique qui consiste à analyser le trafic réseau.

- Lorsque deux ordinateurs communiquent entre eux, il y a un échange d'informations (trafic). Mais, il est toujours possible qu'une personne malveillante récupère ce trafic. Elle peut alors l'analyser et y trouver des informations sensibles.
- Parmi les solutions :
  - Utiliser de préférence un switch (commutateur) plutôt qu'un hub.
  - Utiliser des protocoles chiffrés pour les informations sensibles comme les mots de passe.
  - Utiliser un détecteur de sniffer.

Les différents types d'attaques

3) Attaques DoS :

- Une «**attaque par déni de service**» («**Denial of Service**», **DoS**) est un type d'attaque qui consiste à saturer un site Web par des requêtes pour le mettre « hors-service » .
- Il s'agit la plupart du temps d'attaques à l'encontre des serveurs d'une entreprise, afin qu'ils ne puissent être utilisés et consultés.
- Le but d'une telle attaque n'est pas de récupérer ou d'altérer des données, mais de nuire à la réputation de sociétés ayant une présence sur internet et éventuellement de nuire à leur fonctionnement.
- Le principe des attaques par déni de service consiste à envoyer des paquets inutiles afin de provoquer une saturation ou un état instable des machines victimes et de les empêcher ainsi d'offrir leurs services réseau.

Les différents types d'attaques

3) Attaques DoS :

- DOS local (épuisement des ressources)
  - Saturation de l'espace disque (répertoires récursifs, …)
  - boucle infinie de fork()
  - …
- DOS par le réseau (consommation de bande passante)
  - Flags TCP illégaux
  - SYN flood
  - …
- Parmi les solutions de protection contre les attaques par déni de service:
  - Installation de modules complémentaires (exemple : Apache propose le module **mod_evasive** pour contrer les attaques DoS)
  - Utilisation d'un Firewall

Les différents types d'attaques

4) Usurpation d'identité (Spoofing) :

- L'usurpation (en anglais spoofing) consiste à se faire passer pour quelqu'un d'autre afin d'obtenir des privilèges. Parmi les exemples d'usurpations, on trouve :
  - **Usurpation de l'adresse IP** (IP spoofing) est une technique consistant à remplacer l'adresse IP de l'expéditeur par l'adresse IP d'une autre machine. Cette technique permet ainsi à un pirate d'envoyer des paquets anonymement.
  - **Usurpation de l'adresse e-mail** : Lors de la réception d'un courrier électronique, nous pouvons lire l'adresse de l'expéditeur. Mais, il est possible de changer l'adresse. Ainsi, un pirate peut vous envoyer un mail en usurpant l'adresse de votre supérieur.
  - **Usurpation WEB** : Ceci est le principe du phishing

Les différents types d'attaques

5) 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 (Recherche exhaustive).
  - Outils de cryptanalyse se développent continuellement
  - Internet fournit une ressource massive de calcul parallèle
- Ces outils sont:
  - très efficaces dans le cadre de mots de passe simples,
  - beaucoup moins efficaces dans le cas de mots de passe longs et complexes.

Les différents types d'attaques

5) Violation d'accès non autorisé : intrusion :

- Les intrusions informatiques constituent des « attaques ciblées » qui exploitent une ou des vulnérabilité(s) technique(s) pour accéder à des informations confidentielles (ex. : mots de passe, carte bancaire…) ou prendre le contrôle des serveurs ou postes de travail.

1.4- Les menaces informatiques

6) 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 amovible (clé USB…)
  - Site Web malveillant ou piratés
  - Partages réseaux ouverts, systèmes vulnérables…

1.4- Les menaces informatiques

6) Virus informatique:

… avec comme conséquences potentielles …

- Installation d'un « cheval de Troie » pour accéder au poste de travail à distance.
- Récupération de données ciblées : cartes bancaires, identifiants/mots de passe …
- Surveillance à distance des activités : capture des écrans, des échanges, du son ou de la vidéo !
- Destruction des données des postes de travail.
- Chiffrement des données pour une demande de rançon.
- …

Les différents types d'attaques

7) Attaques par injections SQL:

- Ces attaques sont possibles contre des sites web mal programmés.
- Une injection SQL insert un code SQL dans les requêtes SQL réalisées entre le serveur web et sa base de données.
- Les conséquences de cette attaque peuvent être multiples :
  - Contournement de formulaires d'authentification.
  - Destruction totale de la base de données.
  - Exécution arbitraire de code.
  - …

Les différents types d'attaques

8) Spam :

- Le spam (courriel indésirable) est une communication électronique non sollicitée, en premier lieu via le courrier Électronique.
- Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires et frauduleuses.
- Le spam contient généralement de la publicité.
- Il peut être utiliser pour des escroqueries.

1.5 - Méthodes de défense :

Afin de lutter contre ces différentes attaques, il est d'usage de prendre en considération les points suivants :

- **Chiffrement :** L'utilisation d'algorithmes mathématiques pour transformer les données en une forme illisible...
- **Signature numérique:** algorithmes pour vérifier l'intégrité ou l'origine des données.
- **Bourrage de trafic:** envoie de données inutiles pour faire échouer les tentatives d'analyse de trafic.
- **Contrôle d'accès :** vérifie les droits d'accès d'un acteur aux données.
- **Antivirus, Anti-malware :** protège contre virus, ver, cheval de troie (trojan), adware, etc.

1.5 - Méthodes de défense :

- **Le pare-feu « Firewall »:** un élément (logiciel ou matériel) du réseau informatique contrôlant les communications qui le traversent.
  - Ne protège pas contre un pirate qui utilise une connexion autorisée pour attaquer le système.
  - Ne protège pas contre une attaque venant du réseau intérieur (qui ne traverse pas le Firewall).
- **Détection d'intrusion « (IDS : Intrusion Detection System) » :** repère les activités anormales ou suspectes sur le réseau surveillé.
- **Journalisation ("logs") :** Enregistrement des activités de chaque acteurs.

1.5 - Méthodes de défense :

Et il y a aussi :

- Mises à jour régulières du système d'exploitation et des logiciels de protection.
- Bonnes configurations (modification des identifiants par défaut, choix de mot de passe, changement régulier des mots de passe).
- Et vigilance de l'utilisateur : téléchargement à partir de sites de confiance, exécution de programmes provenant de sources fiables, vérification de l'expéditeur des emails, vérification des URLs.