Ministère de l'Enseignement Supérieur et de la Recherche Scientifique Université 08 Mai 1945 - Guelma

Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie Département d'Informatique

3eme année LMD

Sécurité Informatique

Chapitre 1 : Généralités

Chargé du cours : Bada Mousâab

Bada.mousaab@gmail.com

Année Universitaire 2015-2016

1. *Introduction générale :*

Les exigences de la sécurité de l'information au sein des organisations ont conduit à **deux changements majeurs** au cours des dernières décennies.

Avant l'usage généralisé d'équipements informatiques, la sécurité de l'information était assurée par des moyens physiques (classeurs fermés par un cadenas).

Avec l'introduction de l'ordinateur, le besoin d'outils automatisés pour protéger des fichiers et autres informations stockées est devenu évident. Ce besoin est accentué pour un système accessible via un téléphone public ou un réseau de données. On donne à cette collection d'outils conçus pour protéger des données et contrecarrer les pirates le nom de *sécurité informatique*.

Le second changement majeur qui affecte la sécurité est l'introduction de systèmes distribués et l'utilisation de réseaux et dispositifs de communication pour transporter des données entre un terminal utilisateur et un ordinateur, et entre ordinateurs. Les mesures de sécurité des réseaux sont nécessaires pour protéger les données durant leur transmission. On parle alors de *sécurité des réseaux*.

2. *Définition de base :*

2.1. La sécurité :

La sécurité informatique c'est ***l'ensemble des moyens*** mis en œuvre pour ***minimiser la vulnérabilité*** d'un système ***contre des menaces*** accidentelles ou intentionnelles.

Attention !!!

a) Sureté = " Safety"

Protection de systèmes informatiques **contre les accidents dus à l'environnement**, **les défauts du système, etc...**

b) Sécurité = "Security"

Protection des systèmes informatiques **contre des actions malveillantes intentionnelles**.

2.2. La vulnérabilité

Une **vulnérabilité** (en anglais « *vulnerability*», appelée parfois *faille* ou *brèche*) est un point où un système est sensible à une attaque malveillante. Il s'agit ***d'une faiblesse*** de sécurité de ***nature logique*** ou ***physique*** pouvant être exploitée pour causer des pertes ou des dommages.

Une vulnérabilité peut découler, par exemple, d'une erreur d'implémentation ou une mauvaise conception du système, erreur susceptible d'être exploitée, pour nuire au système (pénétration, refus de service, etc.).

Elle peut également provenir d'une mauvaise configuration. Elle peut enfin avoir pour origine une insuffisance de moyens de protection des biens critiques, comme l'utilisation de flux non chiffrés, l'absence de protection par filtrage de paquets, etc.

2.3. Menace :

L'ensemble des actions qui peuvent **exploiter les vulnérabilités** d'un système (ses faiblesses) pour **lancer des attaques** sur ce système.
Le danger peut être une personne (un pirate du système ou un espion), un objet (une pièce défectueuse de l'équipement)

2.3.1. Les menaces passives

L'intrus est limité à l'écoute et l'analyse du trafic échangé sans modification des données transmis ou altération du fonctionnement du système. L'intention de l'intrus peut être la connaissance des informations confidentielles des utilisateurs ou bien la connaissance des informations relatives au réseau ou aux systèmes pour se préparer à une attaque active. Ce type de menace est difficile à détecter puisque l'intrus n'apporte aucune modification sur les informations échangées.

2.3.2. Les menaces actives

L'intrus tente de supprimer ou modifier les messages transmis sur le réseau. Il peut aussi injecter son propre trafic ou rejouer d'anciens messages pour perturber le fonctionnement du réseau ou provoquer un déni de service.

2.4. Contre-mesure (Mesure de sécurité) :

L'ensemble des actions mises en œuvre en **prévention** de la menace.
Les contre-mesures à mettre en œuvre ne sont pas uniquement des solutions techniques mais également des mesures de formation et de sensibilisation à l'intention des utilisateurs, ainsi qu'un ensemble de règles clairement définies.

3. *Concepts de base (objectifs de la sécurité informatique) :*

La sécurité de l'information s'articule autour de quelques concepts fondamentaux, à savoir ***la confidentialité, l'intégrité, la disponibilité, l'authenticité, l'autorisation et la traçabilité.***

Les trois premiers, souvent référencés via l'acronyme anglais CIA (*Confidentiality, Integrity, Availability*), forment **les buts fondamentaux** visés par la sécurité de l'information.

3.1. Confidentialité :

C'est la propriété qui assure que **seuls les utilisateurs autorisés, dans des conditions prédéfinies, ont accès** aux informations. C'est-à-dire garder les informations secrètes sauf pour les personnes auxquels elles sont destinées.

L'un des moyens pour garantir la confidentialité des données est le chiffrement des données (la cryptographie) et le contrôle d'accès (Autorisation).

3.2. Intégrité

Une information est dite intègre (honnête) si l'on est capable de prouver avec quasi certitude qu'elle n'a pas été modifiée ou corrompue, soit accidentellement, soit de manière malveillante.

L'un des moyens pour assurer l'intégrité est l'utilisation des empreintes digitales (cryptographie).

3.3. Disponibilité

Un système d'information assure de la disponibilité s'il est capable de garantir un fonctionnement correct durant les périodes prévues d'utilisation. Cela implique notamment de la résilience aux pannes ainsi que la capacité à absorber efficacement des pics de charge.

3.4. Authenticité

Une information est dite ***authentique*** si l'on est capable d'en identifier l'origine d'une manière quasi certitude.

L'authentification désigne le processus visant à confirmer qu'un commettant est bien celui qu'il prétend être. Il existe quatre facteurs d'authentification qui peuvent être utilisés pour confirmer l'identité d'un commettant :

- utiliser une information que seul le commettant connaît : mot de passe.
- utiliser une information unique que seul le commettant possède : l'empreinte.
- utiliser une information que seul le commettant peut produire: CryptoCard (authentification renforcées)

3.5. Autorisation

Un mécanisme d'autorisation est responsable de spécifier et de vérifier les droits d'accès a une ressource quelconque dans un système d'information

3.6. Traçabilité

Un mécanisme de traçabilité est responsable de s'assurer que l'historique des actions en relation avec une information donnée (création, lecture, modification, etc.) puisse être relié de manière univoque avec une entité préalablement identifiée.

4. ***Principes fondamentaux :***

En ayant ces principes en tête lors de la conception, de l'implémentation ou la configuration d'un système informatique, d'un réseau ou d'une application logicielle, on pourra éviter de nombreuses vulnérabilités.

4.1. Moindre privilège (à faire) :

Lorsqu'un système d'information permet de segmenter les privilèges alloués à ses utilisateurs, un principe de base consiste à ne donner que les permissions minimales nécessaires pour effectuer une tache donnée. Cela évite qu'un adversaire capable de détourner le fonctionnement de ce système puisse abuser de permission non nécessaire.

4.2. Défense en profondeur :

Un mécanisme de sécurité, comme tout autre système d'information, peut être mal conçu ou mal configuré, et ainsi ne pas être capable de remplir sa tache de manière attendue. Le principe de défense en profondeur prône le fait de ne pas faire reposer la sécurité d'un système sur un seul mécanisme de protection. L'application de ce principe vise ainsi à éviter qu'un système de protection devienne un point individuel de défaillance.

4.3. Participation des utilisateurs et la simplicité :

Tout système d'information sera ***in fine*** en contact avec des utilisateurs. Souvent, les mécanismes de sécurité mis en place vont à l'encontre de la productivité de ces utilisateurs et si ces mécanismes sont trop lourds pour ces derniers, des stratégies pour les contourner seront rapidement mises en place.

4.4. Goulet d'étranglement :

Le mot ***goulet***, qui fait référence à l'entrée étroite d'un port, exprime parfaitement l'idée sous-jacente a ce principe : *il est nécessaire de concentrer les flux d'information entrant et sortant d'un système complexe* en quelques points faisant office de goulets d'étranglement pour être capable de les protéger ou de les analyser.

4.5. Interdiction par défaut :

L'application de ce principe, plus largement connu sous le terme du principe de la liste blanche : *exige que toute activité soit interdite par défaut* dans un premier temps, **puis** que dans un second temps *l'on permette les activités tolérées*.

4.6. Maillon faible :

Tout système de traitement de l'information un peu complexe comporte de nombreuses parties interagissant entre elles, que ce soit un réseau de communication, un système d'exploitation ou une application logicielle.

Ces parties possèdent souvent *des niveaux de sécurité différents*. **Le principe du maillon faible** stipule qu'un adversaire visera à attaquer donc en priorité au maillon le plus faible afin de compromettre un système complexe.

4.7. Plantage sécurisé :

Fréquemment, un système informatique se trouve dans des conditions ne lui permettant plus de mener sa tâche a bien, parce qu'il ne dispose plus de mémoire, d'espace disque, ou parce qu'un système tiers dont il a besoin est temporairement indisponible.
Dans ce cas, il est nécessaire que le traitement de ces cas d'exception n'induise pas de vulnérabilité.

4.8. Sécurité par l'obscurité :

Une erreur souvent commise est de faire reposer la sécurité d'un système sur la difficulté supposée d'en effectuer la retro-conception.

Un exemple typique violant ce principe est le codage en dur d'un mot de passe dans un logiciel. Le développeur imagine que comme le mot de passe n'est pas visible de manière explicite, il ne tombera pas dans les mains d'un adversaire.

5. La gestion de la sécurité de l'information

Il est bon de se rappeler que la sécurité informatique ne se résume pas à trouver des solutions techniques à des problèmes. Pour pouvoir garantir la confidentialité, l'intégrité, et la disponibilité de l'information, il faut développer des stratèges. Celles-ci peuvent inclure des aspects non techniques comme l'attribution de responsabilité, la formation, etc.

5.1. normes de sécurité :

Une norme de sécurité forme l'ensemble complet « **avec peu de technique : juste le quoi ?** » qui décrit tous les aspects de la gestion de la sécurité de l'information. Elle permet aussi de faire certifier une société afin de démontrer qu'elle gère d'une manière efficace la sécurité de l'information.

ISO 27002 :

La norme ISO 27002 décrit d'une manière détaillée des directions à suivre pour la gestion de la sécurité de l'information. ***C'est un document de référence pour la création d'une politique de sécurité.***

Les points essentiels décrits dans ce document sont :

- l'organisation de la sécurité de l'information
- la sécurité des ressources humaines
- la gestion des actifs
- contrôle d'accès
- cryptographie
- sécurité physique et environnementale
- sécurité liée a l'exploitation

- sécurité de communications
- développement et maintenance des systèmes d'information
- relation avec les fournisseurs
- etc...

5.2. politique de sécurité :

Une politique de sécurité décrit l'ensemble des règles qui sont appliquées (selon le besoin : on choisi un sous ensemble de la norme ISO 27002), pour atteindre le niveau de sécurité souhaité ***sans dire comment le faire.***

5.3. L'implémentation d'un système de gestion de sécurité:

Ils décrivent comment les politiques sont mises en œuvre. Pour cela on peut utiliser un catalogue de sécurité. On appel le résultat de cette implémentation : un standard.

5.4. Catalogues de sécurité :

Les catalogues de sécurité de base constituent un répertoire de menace et des mesures de sécurités pour sécuriser un système d'information typique. Contrairement à une norme, les catalogues de sécurité décrit ***comment*** les mesures de sécurité doivent être mis en œuvre.

Ex : *IT-Grundschutz-Kataloge* décrit d'une manière détaillée:

- **Les menaces :** Plus de 250 menaces comme :
  - Les évènements externes (feux, eau, ...).
  - Les défauts organisationnels (manque de formation, manque de documentation).
  - Erreurs humaines
  - Défaut techniques (bogues, pannes,...)
  - Actes délibérés Piratage, espionnage, fraude
- **Les mesure de sécurité :** Plus de 600 contre-mesures

5.5. Critères communs :

Les critères communs sont une collection de critères à l'aide desquels on peut évaluer le niveau de sécurité d'un system. Cette évaluation peut se faire avec différents niveaux d'assurance de l'évaluation (EAL) qui donne lieu à un certificat d'un niveau correspondant.

EAL 1 : testé fonctionnement.
ELA 2 : testé structurellement.
EAL 3 : testé et vérifié méthodiquement « Apple Mac OS X , CISCO Catalyst 6500 switches»
EAL 4 : conçu, testé et vérifié méthodiquement « Windows server 2008, Oracle database »
EAL 5 : conçu de façon semi-formelle et testé
EAL 6 : conception vérifiée de façon semi-formelle et testé.
EAL 7 : conception vérifiée de façon formelle et testé.

TD 1

Exercice1 :

Une application de banque électronique utilise un système d'authentification de ses clients qui repose sur un identifiant, un mot de passe, et un Authentifieur qui génère un nombre de 10 chiffres toutes les minutes.

Quelles sont les menaces du coté du client ? Essayer d'en identifier au moi 4 .

Exercice 2 :

En tant que spécialiste en sécurité logicielle, vous êtes amené à travailler dans un projet de développement d'une base de données devant stocker des informations médicales sensibles et les mettre a disposition du personnel médical d'un hôpital.

Quels sont les objectifs de sécurité d'une telle application en donnant des explications.

Exercice 3 :

1. expliquer les termes suivants :
    a. Niveau de sécurité de base.
    b. Certification de sécurité.
    c. Politique de sécurité.
2. Indiquer à quel terme de la question précédente se rapporte principalement chacune des références suivantes :
    a. Catalogues de sécurité du BSI allemand.
    b. ISO 27002.
    c. ISO 15408.

Solution :

Exercice1

1. un espion de clavier (keylogger) installer sur le poste du client capable de récupérer les identifiants statiques et dynamiques entrés par l'utilisateur.

2. Interception ou manipulation du contenu des communications entre le client et le serveur, soit au niveau du navigateur (man in the browser) ou soit au niveau du réseau (man in the middle : homme au milieu)

3. des menaces physiques visant à induire ou à forcer le client à divulguer ses identifiants

4. Le vol physique de l'authentifieur + une attaque par force brute contre les identifiants du client.

Exercice 2 :

- Confidentialité : protection du stockage (sans oublier les sauvegarde) : chiffrement + contrôle d'accès basé sur l'authentification forte.
- On peut ajouter aussi un mécanisme de traçabilité parce qu'on a utilisé le contrôle d'accès

- L'intégrité : comme les informations sont sensible, il faut assurer que l'information n'a pas été modifier d'une manière accidentelle ou intentionnel

- La disponibilité : il n'est pas envisageable qu'un chirurgien ayant besoin d'une information spécifique au sujet du patient qu'il opère ne puisse pas y accéder parce que la base est en panne.

Exercice3 :

a. On définit les termes proposés :

- ***le niveau de sécurité de base*** présente l'ensemble des mesures de sécurité nécessaire à la protection d'un système d'information contre les menaces usuelles.
- ***La certification de sécurité*** atteste qu'un produit donné (une application, un system d'exploitation, un réseau de communication, etc.) vérifie des critères défini selon une norme spécifique.
- ***Politique de sécurité :*** est l'ensemble des règles générales ayant but de contrôler et limiter les risques lies a l'utilisation d'un system d'information.

b.

- ***Catalogues de sécurité du BSI allemand (IT- Grundshutz Kataloge) :*** ce manuel *concret et technique* est un catalogue de menace et de mesures de sécurité. Donc ce manuelle est utile afin d'établir un *niveau de sécurité de base.*

- **ISO 27002 :** cette norme décrit d'une manière détaillée (non technique) des directions à suivre pour la gestion de la sécurité de l'information. Cette norme permet de *définir une politique de sécurité*.

- **Common Criteria (ISO 15408)** : cette norme international définit des critères de sécurité permettant d'évaluer *d'une manière homogène* des produits liés à la : - confidentialité – l'authenticité – et l'intégrité ***afin d'attribuer une certification***