Leçon 2 : Les menaces, risques et vulnérabilités

Équipe Pédagogique Réseau Informatique@ UVCI
2018

Mai 2018
Version 1.0

Table des matières

I - Objectifs **3**

II - Menaces d'un système **4**

1. Typologies des menaces 4

2. Exercice : Question 1 6

3. Exercice : Question 2 6

III - Vulnérabilités **7**

1. Types de vulnérabilités 7

2. Exercice : Exercices 9

IV - Risques de sécurité **10**

1. Notions liés au risque 10

2. Exercice 11

V - Solutions des exercices **12**

Objectifs

A la fin de cette leçon, vous serez capable de :

- Identifier les menaces d'un système informatique
- Évaluer les risques de sécurité
- Identifier les vulnérabilités.

Menaces d'un système

Objectifs

Identifier les menaces d'un système informatique

1. Typologies des menaces

Définition : Menace

Une menace est un danger qui existe dans l'environnement d'un système indépendamment de celui-ci. Les menaces aux systèmes informatiques sont de nos jours variées et redoutables.

Plusieurs menaces existent.

Les menaces contre le système d'information entrent dans l'une des catégories suivantes :

- atteinte à la disponibilité des systèmes et des données,
- destruction de données,
- corruption ou falsification de données,
- vol ou espionnage de données,
- usage illicite d'un système ou d'un réseau,
- usage d'un système compromis pour attaquer d'autres cibles.

1) Menaces humaines

Pirate : Personne commettant des actes illégaux lies à l'informatique.

Hacker

Personne apte à modifier astucieusement un objet pour le destiner à un autre usage que celui prévu initialement.

White hat Hacker

Consultants, administrateurs se servant de leurs compétences pour résoudre des problèmes en avertissant la personne ou l'organisme concerné d'un problème de sécurité.

Black hat Hacker

Créateurs de virus, cyber espions, cyber-terroristes et cyber-escrocs. Ils ont une nette préférence pour les actions illégales.

Remarque

white hats ne signifient pas hommes gentils et les black hats les méchants. De nombreux White hats ne servent que leurs intérêts alors que d'autres Black hats protègent ceux des autres...

Script kiddies

pirate néophyte utilisateur de scripts écrits par d'autres.

2) Autres menaces

D'autres types de menaces sont les suivantes.

a) La fuite de données

La fuite de données peut provenir d'une infiltration du réseau ou provenir d'un employé de l'entreprise. Dans ce second cas, elle peut être intentionnelle (vente des données de l'entreprise) ou due à une négligence (navigation sur des sites non sécurisées).

b) Phishing

l'hameçonnage (phishing) : un courrier électronique dont l'expéditeur se fait généralement passer pour un organisme financier et demandant au destinataire de fournir des informations confidentielles.

c) Le DDos

Déni de service (Denial Of Service (DOS)), vise à rendre indisponible un service, un système, un réseau.

Le DDOS est plusieurs DOS.

d) Virus informatique (Computer Virus)

Un virus informatique est un type de logiciel malveillant caché dans un logiciel légitime. Chaque fois qu'un utilisateur ouvre le logiciel infecté, il permet au virus de se propager. Il agit discrètement et se réplique à une vitesse fulgurante grâce aux échanges de données, que ce soit par une clé USB ou un réseau informatique.

e) Ver informatique (Computer Worm)

Le virus ne doit pas être confondu avec un ver informatique, qui se répand sur le réseau Internet. Ce dernier peut s'installer sur un ordinateur à partir d'un courriel, par téléchargement d'un fichier ou par messagerie instantanée. Il est beaucoup plus courant que le virus informatique de nos jours.

f) Logiciel espion ou cheval de Troie (Spyware ou Trojan Horse)

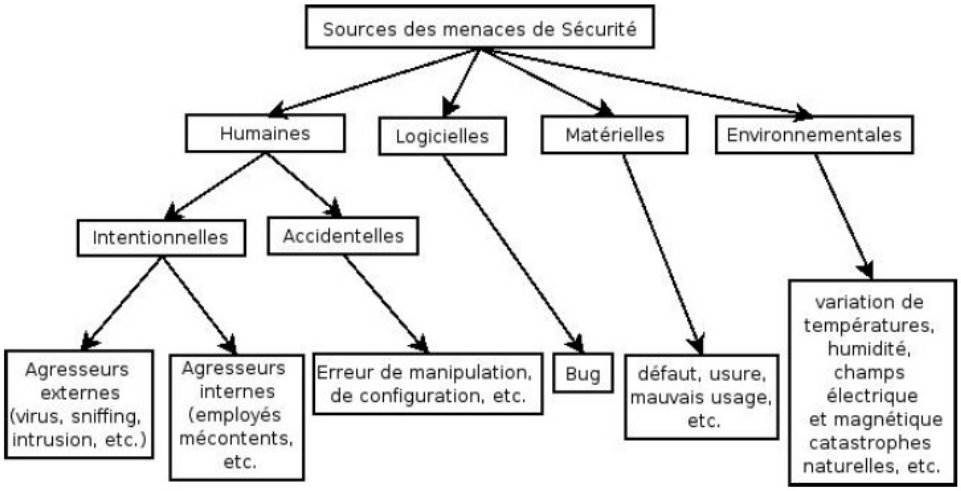
Les virus classiques ont cédé le pas depuis une dizaine d'années à un type particulier de logiciel malveillant, les logiciels espions ou chevaux de Troie. Ceux-ci infectent silencieusement l'ordinateur grâce à une application en apparence légitime. Une fois dans l'ordinateur, le logiciel peut faire ce qu'il veut : enregistrer les mots de passe ou accéder à la caméra pour enregistrer les moindres faits et gestes de l'utilisateur.

g) Vol d'appareils portatifs ou mobiles (Theft)

S'il n'est pas adéquatement protégé, il est facile d'extirper le contenu d'un appareil tombé entre de mauvaises mains ou de l'utiliser pour accéder aux réseaux de l'entreprise.

h) Ransomwares

Elle constitue la version numérique du racket. Elle consiste à prendre en otage les données d'une entreprise. Dans cette attaque, il est impossible d'ouvrir les fichiers car chiffrés par les pirates jusqu'au paiement d'une rançon. Cette menace est aussi appelée rançongiciel.



Sources de menaces

2. Exercice : Question 1

[Solution n°1 p 12]

Exercice

Quelle phrase définit le mieux le mot hameçonnage ?

- ○ A) Une technique d'analyse du trafic réseau
- ○ B) Une méthode de recherche d'informations sur Internet
- ○ C) Un système d'envoi massif de courriers électroniques
- ○ D) Une procédure de collecte de données par formulaire sécurisé
- ○ F) Un procédé frauduleux permettant de collecter des informations personnelles

3. Exercice : Question 2

[Solution n°2 p 12]

Donner dans liste ci-dessous des motivations des hackers.

- ☐ A) prendre connaissance des données
- ☐ B) modifier les données
- ☐ C) paralyser les services et le réseau
- ☐ D) modifier le réseau

Vulnérabilités

II

Objectifs

- Identifier les vulnérabilités.

1. Types de vulnérabilités

Définition

Ce sont les failles (faiblesses) de sécurité dans un système qui le rend sensible à une menace.

Tout système vu dans sa globalité présente des vulnérabilités, qui peuvent être exploitables ou non.
S'il n'y a pas de vulnérabilité, il n'y a pas d'attaque.
C'est un état dans un système informatique qui permet:
- A un attaquant d'exécuter des commandes
- A un attaquant de se faire passer pour une autre entité.

Catégories de vulnérabilités

Les vulnérabilités sont classées en trois catégories :
- Dues à la conception (des logiciels ou matériels)
- Dues à l'implémentation (une erreur dans le logiciel ou le matériel)
- Dues à la configuration.

Exemples de vulnérabilités

- Bogues dans les logiciels
- Mauvaises configurations
- Erreurs humaines
- Services permis et non utilisés
- Virus et chevaux de Troie
- Saturation de la liaison d'accès à internet
- Installation des logiciels et matériels par défaut
- Mises à jours non effectuées
- Mots de passe inexistants ou par défaut
- Services inutiles conservés
- Traces inexploitées.
- Pas de séparation des flux opérationnels des flux d'administration des systèmes
- Procédures de sécurité obsolètes

- Eléments et outils de test laissés en place dans les configurations en production
- Authentification faible
- Télémaintenance sans contrôle fort

Attaques

Les attaques (exploits) représentent les moyens d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas exploitables.

Il existe quatre catégories d'attaques : interruption, interception, modification, fabrication.

a) Interruption

Un atout du système est détruit ou devient indisponible ou inutilisable.

C'est une attaque portée à la disponibilité. Il peut s'agir d'une personne, d'un programme ou d'un ordinateur.

Une écoute téléphonique dans le but de capturer des données sur un réseau, ou la copie non autorisée de fichiers ou de programmes en sont des exemples.

La destruction d'une pièce matérielle (tel un disque dur), la coupure d'une ligne de communication, ou la mise hors service d'un système de gestion de fichiers en sont d'autres exemples.

b) Interception

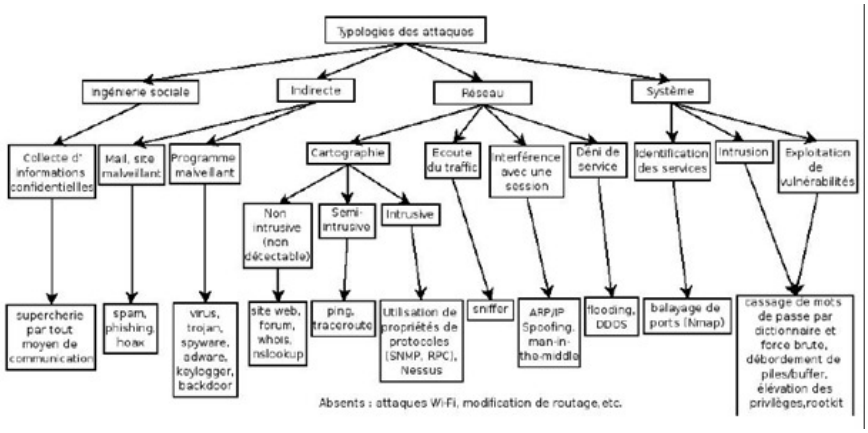
Une tierce partie non autorisée obtient un accès à un atout. C'est une attaque portée à la confidentialité.

c) Modification

Une tierce partie non autorisée obtient accès à un atout et le modifie de façon (presque) indétectable. Il s'agit d'une attaque portée à l'intégrité. Changer des valeurs dans un fichier de données, altérer un programme de façon à bouleverser son comportement ou modifier le contenu de messages transmis sur un réseau sont des exemples de telles attaques.

d) Fabrication

Une tierce partie non autorisée insère des contrefaçons dans le système. C'est une attaque portée à l'authenticité. Il peut s'agir de l'insertion de faux messages dans un réseau ou l'ajout d'enregistrements à un fichier.



Typologie des attaques

Les contre-mesures :

Ce sont les procédures ou techniques permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique (auquel cas il peut exister d'autres attaques sur la même vulnérabilité).

2. Exercice : Exercices

[Solution n°3 p 12]

Exercice : Question 1

Donner dans la liste ci-dessus ce qu'un virus peut menacer :

- [ ] La confidentialité des données
- [ ] Le fonctionnement de l'écran
- [ ] Le fonctionnement des programmes
- [ ] La ROM de l'ordinateur
- [ ] L'Intégrité des données

Exercice : Question 2

La mise hors de service des imprimantes d'une entreprise est :

- ◯ A) une attaque visant la modification
- ◯ B) une attaque visant l'interruption
- ◯ C) un risque
- ◯ D) une menace
- ◯ E) une vulnérabilité

Risques de sécurité

Objectifs

Évaluer les risques de sécurité

1. Notions liés au risque

Les menaces engendrent des risques et coûts humains et financiers :

- perte de confidentialité de données sensibles,

- indisponibilité des infrastructures et des données,

- dommages pour le patrimoine intellectuel et la notoriété.

Les risques peuvent se réaliser si les systèmes menacés présentent des vulnérabilités.

Il est possible de préciser la notion de risque en la décrivant comme le produit d'un préjudice par une probabilité d'occurrence :

risque = préjudice × probabilité d'occurrence

Cette formule exprime qu'un événement dont la probabilité à survenir est assez élevée, par exemple la défaillance d'un disque dur, mais dont il est possible de prévenir le préjudice (pertes) qu'il peut causer par des sauvegardes régulières, représente un risque acceptable ; il en va de même pour un événement à la gravité imparable, comme l'impact d'un météorite de grande taille, mais à la probabilité d'occurrence faible.

1) Impact

C'est la conséquence sur l'entreprise de la réalisation d'une attaque.

2) Risque

C'est la combinaison de la réalisation d'une menace et des pertes qu'elle peut engendrer. Ainsi la probabilité qu'une menace particulière puisse exploitée une vulnérabilité donnée du système peut être élevée avec un impact nul, donc un risque moins élevé.

3) Identification des éléments sensibles

La gestion des risques nécessite l'identification des éléments sensibles de l'architecture et analyser les risques qui leur sont associés.

Quelques éléments sensibles :

- Matériels (ordinateurs, équipements réseaux, etc.)

- Données (bases de données, sauvegardes, etc.)

- Systèmes (l'exploitation des matériels)

- Réseaux (l'échange des données)

- Logiciels (sources des programmes, services démons (DNS, FTP,...), applications web, etc.)

- Personnes (salariés, personnel en régie, etc.).

2. Exercice

[Solution n°4 p 13]

Exercice : Question 1

Si les mesures de prévention contre un préjudice sont effectives et efficaces et le nombre d'occurrences de l'événement assez élevé, on peut dire que :

- ◯ A) le risque est acceptable
- ◯ B) le risque n'est pas acceptable

Exercice : Question 2

Quelle expression définit le mieux la notion de risque ?

- ◯ A) Menace
- ◯ B) Vulnérabilité
- ◯ C) Menace + Vulnérabilité
- ◯ D) Menace + Vulnérabilité + Impact

Solutions des exercices

> Solution n°1

Exercice p. 6

Exercice

- ○ A) Une technique d'analyse du trafic réseau
- ○ B) Une méthode de recherche d'informations sur Internet
- ○ C) Un système d'envoi massif de courriers électroniques
- ○ D) Une procédure de collecte de données par formulaire sécurisé
- ◉ F) Un procédé frauduleux permettant de collecter des informations personnelles

> Solution n°2

Exercice p. 6

- ☑ A) prendre connaissance des données
- ☑ B) modifier les données
- ☑ C) paralyser les services et le réseau
- ☐ D) modifier le réseau

> Solution n°3

Exercice p. 9

Question 1

- ☑ La confidentialité des données
- ☑ Le fonctionnement de l'écran
- ☑ Le fonctionnement des programmes
- ☐ La ROM de l'ordinateur
- ☑ L'Intégrité des données

Question 2

- ○ A) une attaque visant la modification
- ◉ B) une attaque visant l'interruption
- ○ C) un risque
- ○ D) une menace

- ○ E) une vulnérabilité

> Solution n°4

Exercice p. 11

Question 1

- ◉ A) le risque est acceptable
- ○ B) le risque n'est pas acceptable

Question 2

- ○ A) Menace
- ○ B) Vulnérabilité
- ○ C) Menace + Vulnérabilité
- ◉ D) Menace + Vulnérabilité + Impact