Introduction à la sécurité informatique

Équipe Pédagogique Réseau Informatique@ UVCI
2018

Mai 2018
Version 1.0

Table des matières

Objectifs

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

- Définir les concepts fondamentaux pour la compréhension de la sécurité
- Identifier les services de sécurité

Concepts fondamentaux

Objectifs

- Définir les concepts fondamentaux pour la compréhension de la sécurité

1. Définitions et principes

1) Enjeux des réseaux informatiques

La sécurité concerne toute entreprise, tout site disposant d'outils informatiques permettant de communiquer. Quel que soit le degré de confidentialité des données, l'enjeu de la sécurité n'est jamais nul pour une entreprise. Voici une liste d'évènements pouvant déranger le bon fonctionnement de toute entreprise :

- indisponibilité des ressources 80 % du temps pour cause de réinstallation suite à une compromission

- utilisation des ressources du réseau, payées cher à 99 % par des sites pirates (site warez) et indisponibilité pour leurs propres besoins

- mise en liste noire par les correspondants pour avoir négligé un serveur de messagerie qui autorise le relais

- mise en cause des machines de l'entreprise dans la compromission de tel ou tel site renommé.

Fondamental

Quel que soit le site considéré, il existe toujours une exigence minimale de fonctionnement qui justifie la mise en place de mesures de sécurité adaptées.

Il est important que les responsables de l'entreprise soient directement impliqués dans la définition des enjeux de la sécurité informatique.

Il est indispensable de rappeler clairement aux utilisateurs quels sont les objectifs de l'entreprise, pour aboutir à un consensus sur l'arbitrage nécessaire entre convivialité et sécurité.

2) Menace

Des centaines de millions de machines sont aujourd'hui connectées sur l'Internet. Même si la plupart des internautes sont inoffensifs, il en existe que l'envie de nuire ou de jouer amènera à s'attaquer à des machines, même assez bien protégées. À cette fatalité statistique s'ajoute le sentiment d'impunité dont jouira un pirate qui s'attaque à votre machine, à partir d'une machine connecté à des milliers de km de chez vous. Les pirates utilisent donc de nombreuses astuces pour se protéger.

3) Principaux facteurs de motivation des pirates

Les principaux facteurs de motivation des pirates sont les suivants :

a) le goût du défi

Ccertains pirates aiment prouver leur habileté et l'étendue de leurs connaissances;

b) l'appât du gain

Certains sont appâtés par les rémunérations qu'offrent des entreprises peu scrupuleuses qui souhaitent saboter l'outil de travail informatique de leur concurrent et/ou lui dérober des informations confidentielles (devis, plans, secrets industriels...) ;

c) Le profit

La volonté de détourner à son profit des ressources informatiques dont on ne dispose pas (puissance de calcul, espace disque, connexion rapide au réseau...);

d) La méconnaissance

La *méconnaissance des conséquences et des risques* encourus par des pirates aveuglément hostiles.

Définition : Sécurité informatique

La Sécurité est l'état qui résulte de l'absence de risque.

La sécurité informatique consiste à la prévention, la protection contre l'accès aux informations par des personnes non autorisées. C'est le processus de maintien d'un système à un niveau acceptable contre les risques.

4) Objectifs de la sécurité informatique

La sécurité informatique vise trois objectifs principaux :

- La *confidentialité* des données
- L'*intégrité* des données
- La *continuité* des services.

Ces trois objectifs se résument en CIA (Confidentiality, Integrity and Availability).

5) Principe de la sécurité

Toute sécurité repose sur les mêmes principes.

a) Le secret

b) L'isolation

c) Authentification :

d) L'accréditation et la classification

e) La minimisation

f) La surveillance

g) La désinformation

h) La formation, l'information, la sanction.

6) Moyens de la sécurité informatique

Plusieurs techniques sont utilisées pour assurer les objectifs de la sécurité informatique.

a) Cryptologie

Science qui a pour objectif principal de cacher des informations (informations stockées dans des fichiers comme des mots de passe ou informations transitant sur les réseaux). Elle est utilisée aussi pour vérifier l'intégrité des données ou pour l'authentification.

b) Sécurité physique

Cela constitue une mesure primordiale de sécurité. Par exemple, fermer les serveurs à clé.

c) Systèmes d'authentification

Utilisation de mots de passe, systèmes biométriques pour l'identification.

d) Droits

Les droits associés aux fichiers limitent leur accès aux personnes non autorisées. Ce système est couramment utilisé pour la sécurisation des ordinateurs sous Unix/Linux.

e) Sommes de contrôle

Elle vérifie l'intégrité des fichiers. Elle permet par exemple de détecter la présence de logiciels malveillants.

f) Pare-feu

Il permet de filtrer les paquets qui entrent ou sortent d'un réseau. Il constitue un outil de sécurité important.

g) Sauvegardes

Les sauvegardes régulières constituent un outil de sécurité aussi important. Elles permettent de retrouver les données perdues après une attaque.

h) Audit des principaux événements du système (connexion réussie ou échouée)

Cela garantit le suivi des règles de sécurité et permet de détecter des tentatives d'intrusion.

Remarque

La confiance est obligatoire pour garantir l'efficacité des mécanismes de sécurité mis en place.

2. Exercice : Exercices

[Solution n°1 p 10]

Exercice : Question 1

Choisir dans la liste ci-dessous, les réponses qui résument les principaux objectifs de la sécurité informatique :

- ☐ A) empêcher l'utilisation des ressources réseau ou informatiques de façon générale
- ☐ B) empêcher la divulgation non-autorisée de données
- ☐ C) accroître l'utilisation des ressources et données de l'entreprise
- ☐ D) empêcher la modification non-autorisée de données
- ☐ E) empêcher l'utilisation non-autorisée des ressources réseau ou informatiques de façon générale

Exercice : Question 2

Quel sigle anglais résume les objectifs de la sécurité informatique ?

Exercice : Question 3

L'interruption du fonctionnement d'un serveur de l'entreprise correspond à une atteinte à : (choisir une bonne réponse)

- ◯ A) l'authenticité
- ◯ B) l'intégrité
- ◯ C) la continuité
- ◯ la confidentialité

Services de la sécurité

II

Objectifs

- Identifier les services de sécurité

1. Différents secteurs de la sécurité

La sécurité se subdivise en plusieurs secteurs dans une société.

1) Sécurité globale

La sécurité globale s'occupe de la sécurité des locaux, des documents papiers, du personnel dirigeant. Ce secteur de la sécurité est très proche de la sécurité militaire par ses moyens et ses objectifs.

2) Sécurité du réseau

Le réseau étant le cœur du système d'information d'une entreprise, le responsable de la sécurité réseau est le plus souvent le responsable de la sécurité informatique. La sécurité réseau concerne les pare-feu, les techniques pour éviter toute intrusion au réseau et le choix global des stratégies de sécurisation.

3) Sécurité des serveurs

Ce secteur concerne la sécurité des serveurs de l'entreprise (bases de données, web...). Sa mise en œuvre nécessite la connaissance des techniques de sécurisation offerte par les systèmes d'exploitation et les applications.

2. Définitions des Services de Sécurité

Pour remédier aux failles et pour contrer les attaques, la sécurité informatique se base sur un certain nombre de services qui permettent de mettre en place une réponse appropriée à chaque menace.

Voici les services de sécurité les plus importants

1) Authentification

Permet de vérifier l'identité revendiquée par une entité, ou l'origine d'un message, ou d'une donnée.

2) Confidentialité

Permet de se protéger contre la consultation abusive des données par des entités tierces indésirables.

3) Contrôle d'intégrité

Permet de vérifier qu'une donnée n'a pas été modifiée par une entité tierce (accidentellement ou intentionnellement).

4) Contrôle d'accès

Permet de vérifier que toute entité n'accède qu'aux services et informations pour lesquelles elle est autorisée.

5) Non répudiation

Permet de se protéger contre la contestation d'envoi et de réception de données lors d'une communication.

3. Exercice : Exercices

[Solution n°2 p 10]

Exercice : Question 1

Le schéma d'authentification est : (choisir une bonne réponse)

- ◯ A) un service de sécurité informatique
- ◯ B) un moyen de sécurité informatique
- ◯ C) un algorithme de sécurité informatique

Exercice : Question 2

Lorsqu'on vérifie que les données d'un système n'ont pas été modifiées, on dit : (choisir une réponse)

- ◯ A) qu'on gère le contrôle l'accès aux données
- ◯ B) qu'on gère la confidentialité des données
- ◯ C) qu'on gère l'intégrité des données

Exercice : Question 3

La sécurité consistant à détecter ou éviter l'intrusion dans le système est appelée :

Exercice : Question 4

La confidentialité est :

- ◯ A) la garantie que les données échangées ne sont compréhensibles que pour les deux entités
- ◯ B) la garantie que les données échangées ne peuvent pas être modifiées

Solutions des exercices

> Solution n°1

Exercice p. 7

Question 1

- [ ] A) empêcher l'utilisation des ressources réseau ou informatiques de façon générale
- [x] B) empêcher la divulgation non-autorisée de données
- [ ] C) accroître l'utilisation des ressources et données de l'entreprise
- [x] D) empêcher la modification non-autorisée de données
- [x] E) empêcher l'utilisation non-autorisée des ressources réseau ou informatiques de façon générale

Question 2

CIA

Question 3

- ( ) A) l'authenticité
- ( ) B) l'intégrité
- (•) C) la continuité
- ( ) la confidentialité

> Solution n°2

Exercice p. 9

Question 1

- ( ) A) un service de sécurité informatique
- (•) B) un moyen de sécurité informatique
- ( ) C) un algorithme de sécurité informatique

Question 2

- ( ) A) qu'on gère le contrôle l'accès aux données
- ( ) B) qu'on gère la confidentialité des données
- (•) C) qu'on gère l'intégrité des données

Question 3

sécurité du réseau

Question 4

- (●) A) la garantie que les données échangées ne sont compréhensibles que pour les deux entités
- ( ) B) la garantie que les données échangées ne peuvent pas être modifiées

Bibliographie

1. Stéphane Lohier, Dominique Présent ; Réseaux et transmissions, 6è édition, DUNOD 2016

Danièle Dromard, Dominique Seret ; Architecture des réseaux, collection Synthex, 2009 Pearson Education France, ISBN : 978-2-7440-7385-4