Compétences visés :

• Définir les concepts fondamentaux de la sécurité informatique (confidentialité, disponibilité, intégrité, non répudiation)

• Définir les concepts de cybercriminalité, cyber sécurité

• Décrire les techniques de protection des données

Introduction

Avec le développement de l'utilisation d'internet, de plus en plus d'entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs, 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. Il en va de même lors de l'ouverture de l'accès de l'entreprise sur internet.
La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. La sécurité informatique vise à réduire au maximum le risque qui est une combinaison des notions (menace, vulnérabilité et contre-mesure). La menace représente le type d'action susceptible de nuire dans l'absolu, tandis que la vulnérabilité (en anglais « vulnerability », appelée parfois faille ou brèche) représente le niveau d'exposition face à la menace dans un contexte particulier. Enfin la contre-mesure est l'ensemble des actions mises en œuvre en prévention de la menace.

I. Objectifs de la sécurité informatique

La sécurité informatique vise généralement cinq principaux objectifs :

• L'intégrité, c'est-à-dire garantir que les données sont bien celles que l'on croit être ; consiste à déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).

• La confidentialité, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées ; consiste aussi à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction.

• La disponibilité, permettant de maintenir le bon fonctionnement du système d'information ; L'objectif de la disponibilité est de garantir l'accès à un service ou à des ressources.

• La non répudiation, permettant de garantir qu'une transaction ne peut être niée ; La non-répudiation de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction.

• L'authentification, consistant à assurer que seules les personnes autorisées aient accès aux ressources. L'authentification consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées.

II. Les attaques

Il existe quatre catégories principales d'attaque :

• Les attaques par l'accès. C'est une tentative d'accès à l'information par une personne non autorisée.

Exemples : Sniffing cette attaque est utilisée par les pirates informatiques pour obtenir des mots de passe.

Craquage de mot de passe il consiste à faire de nombreux essais jusqu'à trouver le bon mot de passe

• **Les attaques par modification,** elle consiste, pour un attaquant à tenter de modifier des informations. Quelques exemples de ce type d'attaque : Virus, et les vers etc… **(Un vers est un programme caché dans un autre qui peut s'exécuter et se reproduire en infectant d'autres programmes ou d'autres ordinateurs il se déplace à travers un réseau.)**

• **Les attaques par déni de service,** elle consiste à envoyer des milliers de messages depuis des dizaines d'ordinateurs, dans le but de submerger les serveurs d'une société, de paralyser pendant plusieurs heures son site Web et d'en bloquer ainsi l'accès aux internautes.

Exemple :
Le flooding, Cette attaque consiste à envoyer à une machine de nombreux paquets IP de grosse taille.
Le smurf, c'est une attaque qui s'appuie sur le ping et les serveurs de broadcast. On falsifie d'abord son adresse IP pour se faire passer pour la machine cible.

• **Les attaques par répudiation.** La répudiation est une attaque contre la responsabilité. Autrement dit, **la répudiation consiste à tenter de donner de fausses informations ou de nier qu'un événement ou une transaction se soit réellement passé.**

Ces attaques sont basées sur les types de virus suivant :

• virus: un programme malveillant ayant pour but de nuire au bon fonctionnement de l'ordinateur.

• Ver(worm): programme malveillant qui se propage en utilisant un réseau informatique (comme Internet)

• cheval-de-troie (trojan): un programme malveillant qui ouvre une porte dérobée dans un système afin de l'exploiter ultérieurement.

• Spam: courrier indésirable envoyé dans l'intention de créer des deni de service, ou alors de distraire et de faire oublier l'essentiel.

III. Concepts de cyber sécurité et cyber criminalité

La cyber-sécurité renvoie à la protection des personnes, des idées et des données dans le cyber espace. La sécurisation des données informatiques ou cyber sécurité, passe par une sécurisation des matériels et logiciels informatiques constituant le support de transmission, de stockage et de traitement de l'information.

L'augmentation de la sécurité des matériels et logiciel informatique, permettrait donc d'augmenter la sécurité des informations.

Deux types de personnes animent ces concepts :

• **Black hat hacker :** pirate des systèmes informatiques, s'introduisant de façon furtive ou masquée pour voler des informations sensibles ou créer des dénis de service. Ces genres de personnes font dans ce qu'on appelle cybercriminalité (le fait d'utiliser ses connaissances informatiques pour commettre des délits des actes préjudiciables).

• **white-hat hacker :** ce sont des « hackers éthiques » des experts en sécurité informatique qui utilisent leurs

capacités à des fin honnêtes éthiques et du côté de la justice. Un hacker white-hat qui trouve une faille de sécurité dans une application la rapportera à son développeur lui permettant ainsi d'améliorer la sécurité de celle-ci avant qu'elle ne soit compromise. Ces genres de personnes font dans ce qu'on appelle cybersécurité **(le fait d'utiliser ses connaissances informatique pour empêcher la défaillance, détecter et fermer les failles d'un système informatique dans une entreprise**).

IV. Protection des données

La protection des données consiste à déployer des moyens et des dispositifs visant à sécuriser le système d'information ainsi que de faire appliquer les règles définies dans la politique de sécurité. Les principaux dispositifs permettant de sécuriser un réseau contre les intrusions sont :

• **Les mots de passe** Lors de la connexion à un système informatique, celui-ci demande la plupart du temps un identifiant (en anglais login ou username) et un mot de passe (en anglais password) pour y accéder. Ce couple identifiant/mot de passe forme ainsi la clé permettant d'obtenir un accès au système. Pour des données sensibles à protéger il est conseillé d'utiliser un mot de passe d'au moins 14 caractères contenant des lettres , des chiffres et des caractères spéciaux.

• **Les systèmes pare-feu**. Dispositif matériel et logiciel qui protège un système informatique connecté à internet des tentatives d'intrusion qui pourraient en provenir.

Le pare feu définit les types de communications autorisés, surveille et contrôle les applications et les flux de données. Néanmoins ce type de dispositif ne protège pas la confidentialité des données circulant sur le réseau.

• **La cryptographie** discipline de la cryptologie s'attachant à protéger les messages en utilisant des clés. La cryptographie vise à rendre le message inintelligible à toutes autres personnes sauf le destinataire du message. Elle permet ainsi de garantir la confidentialité des échanges. On s'appuis généralement sur plusieurs algorithmes cryptographiques tels que DES, RSA, etc..

• **Antivirus** ce sont des programmes permettant de détecter et de neutraliser éliminer tout programme malveillant présent dans l'ordinateur. Il existe plusieurs antivirus telque : Kaspersky, Avast, Norton, Avira etc..

• **Le VPN (Virtual Private Network)** correspond à la mise en place de tunnels sécurisés.

Ce système permet de créer un lien direct entrer des ordinateurs distants qui isole leurs échanges du reste du trafic se déroulant sur le réseau. (permet d'obtenir un niveau de sécurisation supplémentaire dans la mesure où l'ensemble de la communication est chiffrée.

• **Droit d'accès et privilèges** les droits d'accès sont des privilèges attribués à un utilisateur pour accéder à des informations. L'utilisateur peut bénéficier des privilèges suivants : lecture, écriture ou modification, privilège d'administration dans le cas des serveurs ou des appareils de sécurité comme le firewall (pare feu matériel). L'attribution des privilèges peut se faire à un utilisateur spécifique ou à un groupe d'utilisateurs. Il existe plusieurs niveaux de privilèges :

- Le super administrateur : c'est celui qui est propriétaire de tous les dossiers et fichiers du système

- L'administrateur : reçois du super administrateur le droit aussi d'accéder et de modifier les données sur tous les fichiers

- L'invité : dispose d'un accès limité dans le système ; ne peut pas modifier ou accéder aux données dont il n'a pas créé.

Conclusion

La sécurité d'un système informatique doit être abordée selon une approche globale. Ainsi, une porte blindée est inutile dans un bâtiment si les fenêtres sont ouvertes sur la rue.
Cela signifie que la sécurité doit être abordée dans un contexte global et notamment prendre en compte les aspects suivants :

- **La sensibilisation des utilisateurs aux problèmes de sécurité**
- **La sécurité logique, c'est-à-dire la sécurité au niveau des données, notamment les données de l'entreprise, les applications ou encore les systèmes d'exploitation.**
- **La sécurité des télécommunications : technologies réseau, serveurs de l'entreprise, réseaux d'accès, etc.**
- **La sécurité physique, soit la sécurité au niveau des infrastructures matérielles : salles sécurisées, lieux ouverts au public, espaces communs de l'entreprise, postes de travail des personnels, etc.**