Introduction aux attaques informatiques

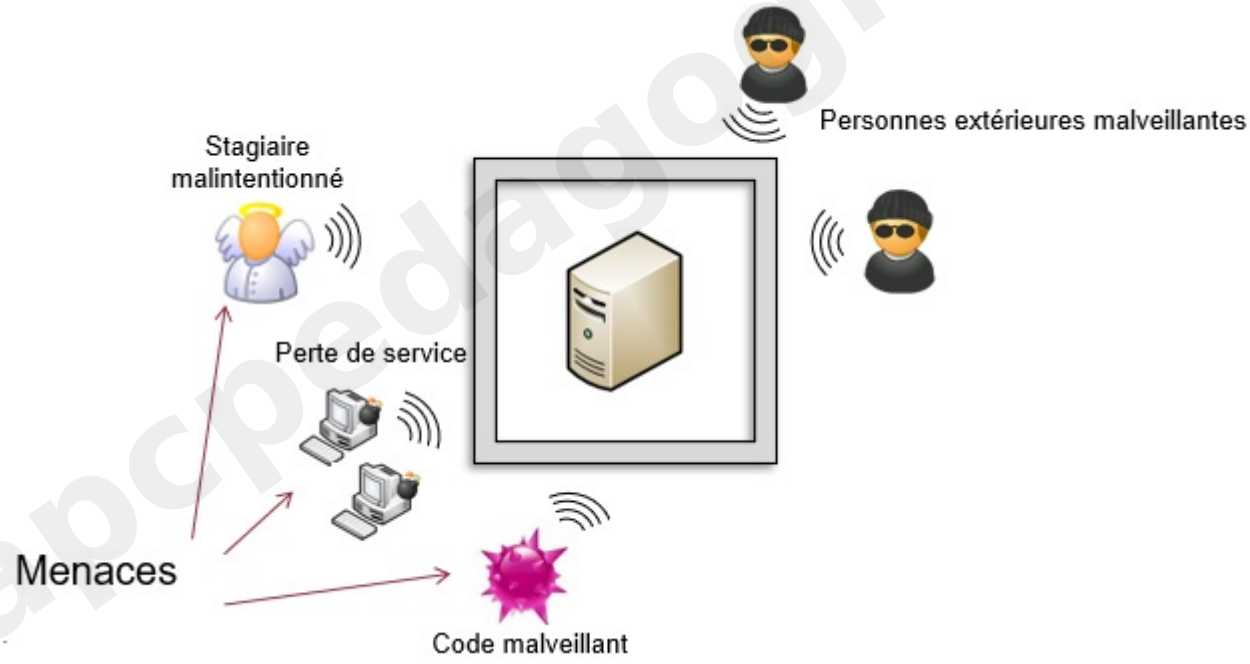
[sommaire]

1. ## Objectifs

- Le but de ce tutoriel est ainsi de donner un aperçu des menaces, des motivations éventuelles des pirates, de leur façon de procéder, afin de mieux comprendre comment il est possible de limiter les risques.

- ## Notions de menace, vulnérabilité, attaque

1. **Les menaces informatiques**



- **Une menace est une cause potentielle d'un incident, qui pourrait entrainer des dommages sur un bien si cette menace se concrétisait.**
- Une Menace est un danger qui existe dans l'environnement d'un système indépendamment de celui-ci : accident, erreur, malveillance passive si elle porte sur la confidentialité, malveillance active si elle modifie le contenu de l'information ou le comportement des systèmes de traitement.

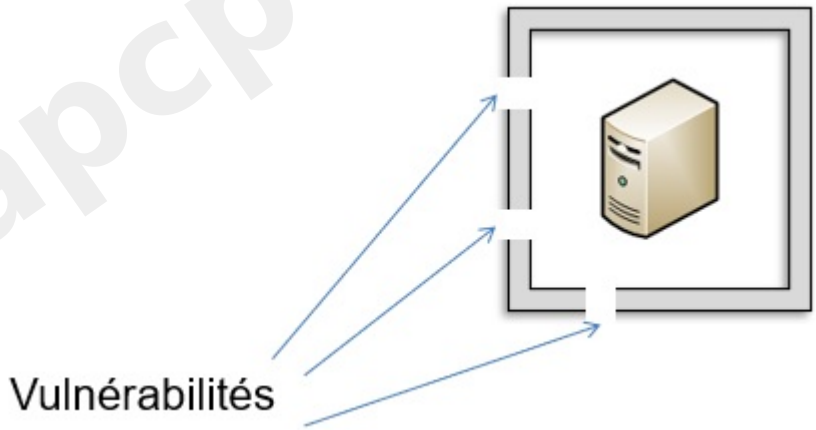
apcpedagogie.com

- Une menace fait référence à un incident susceptible de nuire à un système ou à l'ensemble de votre organisation. Il existe trois principaux types de menaces:

1. les menaces naturelles (par exemple, les inondations ou une tempête),
2. les menaces non intentionnelles (par exemple, un employé qui accède par erreur à une information erronée)
3. les menaces intentionnelles.

- Une menace (threat) représente une action susceptible de nuire dans l'absolu, tandis qu'une vulnérabilité (vulnerability, appelée parfois faille ou brèche) représente le niveau d'exposition face à la menace dans un contexte particulier. La contre-mesure (ou parade), elle, représente l'ensemble des actions mises en œuvre en prévention de la menace.
- Il existe de nombreux exemples de menaces intentionnelles comprenant des logiciels espions, des logiciels malveillants, des sociétés de logiciels publicitaires ou les actions d'un employé mécontent. D'ailleurs, les vers et les virus sont également considérés comme des menaces, car ils pourraient potentiellement nuire à votre organisation en les exposant à une attaque automatisée, par opposition à une attaque perpétrée par des humains.
- Les contre-mesures ne sont généralement pas uniquement des solutions techniques mais également des mesures de formation et de sensibilisation à l'attention des utilisateurs, ainsi qu'un ensemble de règles clairement définies.
- Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, et donc de connaître et de prévoir la façon de procéder de l' « ennemi ».

- **Les vulnérabilités**



- Dans le domaine de la sécurité informatique, une vulnérabilité ou faille est 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

apcpedagogie.com

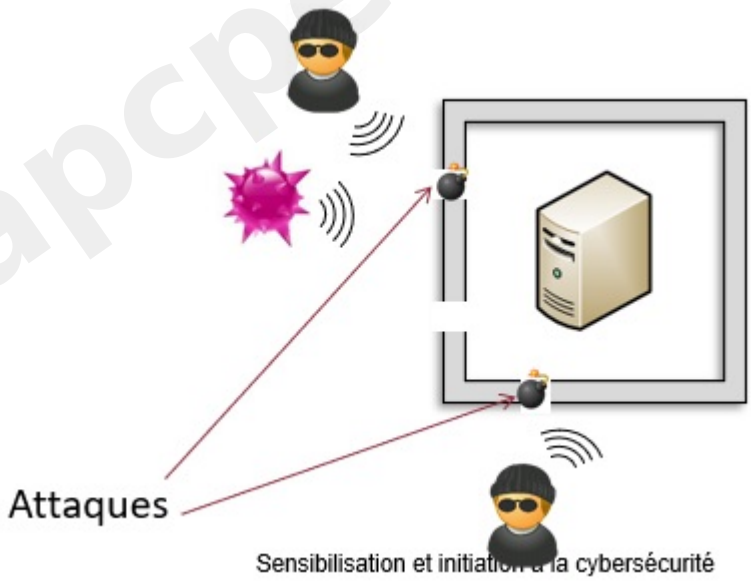
données qu'il contient.

> ***Une vulnérabilité est une faiblesse au niveau d'un bien (au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation du bien).***

- Par exemple, lorsqu'un membre de l'équipe démissionne et que vous oubliez de désactiver son accès aux comptes externes, de modifier ses identifiants, votre entreprise reste ouverte aux menaces intentionnelles. Cependant, la plupart des vulnérabilités sont exploitées par des attaquants automatisés et non par un humain.
- Tester les vulnérabilités est essentiel pour assurer la sécurité continue de vos systèmes en identifiant les points faibles et en élaborant une stratégie pour réagir rapidement.
- Les exemples de vulnérabilités courantes sont Cross-site Scripting, l'injection SQL, les configurations erronées du serveur, les données sensibles transmises en texte brut et l'utilisation de progiciels comportant des vulnérabilités connues.

> ***Menace et vulnérabilité – ces termes sont liés à la cybersécurité et aux cyberattaques. Une menace est un agent qui peut causer du perturbation à l'organisation cible. Une vulnérabilité est une faiblesses ou lacunes d'un programme de sécurité pouvant être exploitées par des menaces pour obtenir un accès non autorisé à une ressource.***

- **Les attaques informatiques**



apcpedagogie.com

- **Une attaque est une 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.**
- Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.
- Une attaque est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.
- Une attaque ne peut avoir lieu (et réussir) que si le bien est affecté par une vulnérabilité.
- Sur Internet des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de pirates informatiques.
- Afin de contrer ces attaques, il est indispensable de connaître les principaux types d'attaques afin de mieux s'y préparer.

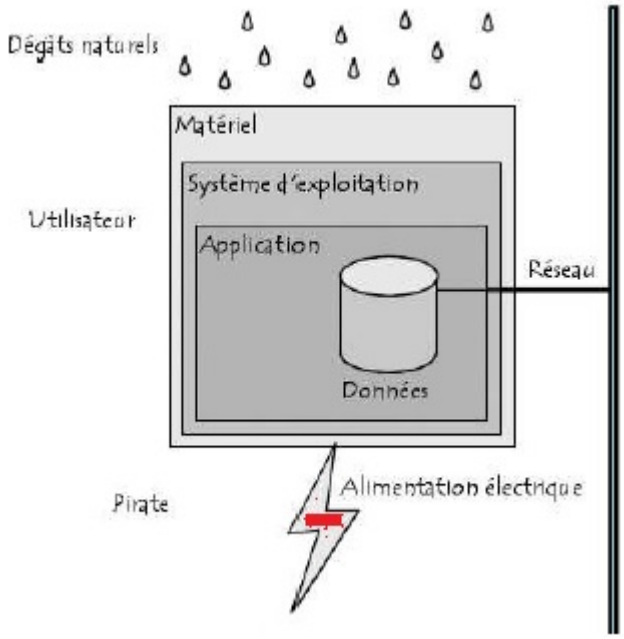
Les motivations des attaques sont de différentes sortes :

- obtenir un accès au système ;
- voler des informations, tels que des secrets industriels ou des propriétés intellectuelles ;
- glaner des informations personnelles sur un utilisateur ;
- récupérer des données bancaires ;
- s'informer sur l'organisation (entreprise de l'utilisateur, etc.) ;
- troubler le bon fonctionnement d'un service ;
- utiliser le système de l'utilisateur comme « rebond » pour une attaque ;
- utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

Les types d'attaques

- Les systèmes informatiques mettent en œuvre différentes composantes, allant de l'électricité pour alimenter les machines au logiciel exécuté via le système d'exploitation et utilisant le réseau.
- Les attaques peuvent intervenir à chaque maillon de cette chaîne, pour peu qu'il existe une vulnérabilité exploitable. Le schéma suivant rappelle très sommairement les différents niveaux pour lesquels un risque en matière de sécurité existe.

apcpedagogie.com



- Il est ainsi possible de catégoriser les risques de la manière suivante :
  - **Accès physique** : il s'agit d'un cas où l'attaquant à accès aux locaux, éventuellement même aux machines :
    - coupure de l'électricité ;
    - extinction manuelle de l'ordinateur ;
    - vandalisme ;
    - ouverture du boîtier de l'ordinateur et vol de disque dur ;
    - écoute du trafic sur le réseau ;
    - ajout d'éléments (clé USB, point d'accès WiFi...).
  - **Interception de communications** :
    - vol de session (session hijacking) ;
    - usurpation d'identité ;
    - détournement ou altération de messages.
  - **Dénis de service** : il s'agit d'attaques visant à perturber le bon fonctionnement d'un service. On distingue habituellement les types de déni de service suivant :
    - exploitation de faiblesses des protocoles TCP/IP ;
    - exploitation de vulnérabilité des logiciels serveurs.
  - **Intrusions :**
    - balayage de ports ;
    - **élévation de privilèges** : ce type d'attaque consiste à exploiter une vulnérabilité d'une application en envoyant une requête spécifique, non prévue par son concepteur, ayant pour effet un comportement anormal conduisant parfois à un accès au système avec les droits de l'application. Les attaques par débordement de tampon (buffer overflow) utilisent ce principe.

apcpedagogie.com

        - **Maliciels** (virus, vers et chevaux de Troie).
    - **Ingénierie sociale** :
        - Dans la majeure partie des cas le maillon faible est l’utilisateur lui-même ! En effet, c’est souvent lui qui, par méconnaissance ou par duperie, va ouvrir une brèche dans le système, en donnant des informations (mot de passe par exemple) au pirate informatique ou en exécutant une pièce jointe. Ainsi, aucun dispositif de protection ne peut protéger l’utilisateur contre les arnaques, seuls le bon sens, la raison et un peu d’informations sur les différentes pratiques peuvent lui éviter de tomber dans le piège ! La montée en puissance des réseaux sociaux sur le Web a donné encore plus d’importance à ce type d’attaque, Attaque par ingéniérie sociale).
    - **Trappes** :
        - il s'agit d’une porte dérobée (backdoor) dissimulée dans un logiciel, permettant un accès ultérieur à son concepteur.

- ## Exercices d'application

    [h5p id="50"]

Cours Administration et sécurité des sites web

Source : https://apcpedagogie.com/introduction-aux-attaques-informatiques · téléchargé le 04/11/2026 · © APC Pédagogie · apcpedagogie.com

apcpedagogie.com