

RÉPUBLIQUE DÉMOCRATIQUE DU CONGO MINISTÈRE  
DE L'ENSEIGNEMENT SUPÉRIEUR ET UNIVERSITAIRE



---

" MISE EN PLACE D'UN SYSTÈME DE SECURITE DANS  
UN SERVEUR WEB "

---

Par : **Tshibangu Ntumba Kenny**

Travail de fin d'études présenté en vue de l'obtention du grade de : licencié en  
Sciences Informatiques

Option : Réseau et Infrastructure

Année Académique 2022-2023



# Table des matières

<b>1</b>	<b>Introduction Générale</b>	<b>1</b>
1.1	La cybersécurité	1
1.1.1	Pourquoi la cybersécurité est-elle importante?	1
1.2	Qu'est-ce qu'un serveur?	2
1.2.1	Les défis de sécurité associés aux serveurs	2
1.2.2	Les meilleures pratiques pour sécuriser les serveurs :	2
1.3	Contexte de recherche	3
1.4	Solution technique	3
1.5	Problématique	3
1.6	Méthodologie	4
1.7	Techniques	4
1.7.1	La Recherche sur Internet :	4
1.7.2	La Recherche Documentaire :	4
1.7.3	La Recherche Expérimentale :	4
1.8	Limitation	4
1.9	Objectif	4
<b>2</b>	<b>Les Serveurs</b>	<b>5</b>
2.1	Définitions	5
2.2	Les Serveurs Web	6
2.2.1	Quelques vulnérabilités Sur Les Serveurs Web	7
2.3	Serveurs de Messageries	7
2.3.1	Quelques vulnérabilités Sur Les Serveurs de Messageries	8
2.4	Serveur de fichiers	9
2.4.1	Quelques vulnérabilités Sur Les Serveurs de Fichier	10
2.5	Serveur de Base de Données	10
2.5.1	Quelques vulnérabilités Sur Les Serveurs de Base De Données	12
2.6	Serveur d'Application	12
2.6.1	Quelques vulnérabilités Sur Les Serveurs d'Application	13
2.7	Serveur DNS	14
2.7.1	Quelques vulnérabilités Sur Les Serveurs DNS	15
2.8	Serveur de Jeu	15
<b>3</b>	<b>La CyberSécurité et La Sécurité Informatique</b>	<b>18</b>
3.1	La CyberSécurité	18
3.1.1	Définition	18
3.1.2	Pourquoi la cybersécurité est-elle nécessaire?	20
3.1.3	Comment les risques de cybersécurité sont-ils mesurés?	20
3.1.4	Cybersécurité avec défense en profondeur (DEP)	21
3.1.5	Comment mettre en œuvre la cybersécurité	23

3.2	But	23
3.3	objectif	23
3.4	La Sécurité Informatique	24
3.4.1	Définition	24
3.5	La sécurité informatique, pour quoi faire?	26
3.6	Types de sécurité informatique	27
3.7	Sécurité informatique et sécurité des informations, quelle différence?	28
3.8	Sécurité informatique et cybersécurité, quelle différence?	28
3.9	Risques associés à la sécurité informatique	28
3.10	Bonnes pratiques en matière de sécurité informatique	29
<b>4</b>	<b>La Configuration Du Serveur Web (ISS) Et La Sécurisation de ce dernier</b>	<b>32</b>



# Table des figures

2.1	Une Salle Serveur . . . . .	5
2.2	Le Schéma d'un serveur Web . . . . .	7
2.3	Schéma d'un Serveur de Messagerie . . . . .	8
2.4	Schéma De Serveur De Fichier . . . . .	9
2.5	Schema De Serveur De Base De Données . . . . .	11
2.6	Schéma D'un serveur D'application . . . . .	13
2.7	Schéma d'un Serveur DNS . . . . .	14
2.8	Un Schema de Serveur de Jeu . . . . .	16
3.1	Un Tableau Illustrant Les Impact . . . . .	21
3.2	Un Schéma Illustrant Le DEP . . . . .	22
3.3	Le CyberSecurity Framework . . . . .	24
3.4	Les Différents Points Englobés par La sécurité Informatique . . . . .	26
3.5	. . . . .	30

**Résumé**

Résume

# Chapitre 1

## Introduction Générale

### 1.1 La cybersécurité

est la pratique consistant à protéger les systèmes, les réseaux et les données contre tout accès, utilisation, divulgation, perturbation, modification ou destruction non autorisés. C'est un domaine critique dans le monde d'aujourd'hui, car notre dépendance à l'égard de la technologie ne cesse de croître.

Les serveurs sont des composants essentiels de toute infrastructure de cybersécurité. Ils fournissent un emplacement central pour le stockage et le traitement des données et peuvent être utilisés pour héberger des applications et des services utilisés par les employés, les clients et les partenaires.

Ce travail fournira une introduction à la cybersécurité et aux serveurs. Il couvrira les sujets suivants :

- Les bases de la cybersécurité
- Les différents types de serveurs
- Les défis de sécurité associés aux serveurs
- Les bonnes pratiques de sécurisation des serveurs

À la fin de ce travail, vous aurez une compréhension de base de la cybersécurité et des serveurs. Vous serez en mesure d'identifier les risques de sécurité associés aux serveurs et vous serez en mesure de mettre en place les meilleures pratiques pour protéger vos serveurs.

#### 1.1.1 Pourquoi la cybersécurité est-elle importante ?

La cybersécurité est importante car elle protège notre infrastructure critique, nos informations personnelles et nos actifs financiers. Ces dernières années, un certain nombre de cyberattaques très médiatisées ont causé des dommages importants.

Par exemple, l'attaque du ransomware WannaCry en 2017 a infecté plus de 200 000 ordinateurs dans 150 pays.

L'attaque a causé des milliards de dollars de dégâts et perturbé des services essentiels tels que les



hôpitaux et les écoles.

## 1.2 Qu'est-ce qu'un serveur ?

Un serveur est un ordinateur qui fournit des ressources à d'autres ordinateurs sur un réseau. Les serveurs peuvent être utilisés pour stocker des données, exécuter des applications et fournir des services tels que la messagerie électronique, le partage de fichiers et l'impression.

### 1.2.1 Les défis de sécurité associés aux serveurs

Les serveurs sont une cible courante pour les cyberattaques car ils contiennent des données précieuses et sont souvent connectés à Internet.

Certains des défis de sécurité associés aux serveurs incluent :

- **Malware** : un malware est un logiciel conçu pour endommager un système informatique. Les logiciels malveillants peuvent être utilisés pour voler des données, installer des portes dérobées ou perturber les opérations.

- **Phishing** : Le phishing est un type d'attaque d'ingénierie sociale qui est utilisé pour inciter les utilisateurs à révéler leurs informations personnelles, telles que des mots de passe ou des numéros de carte de crédit.

- **Attaques par déni de service (DoS)** : les attaques DoS sont conçues pour submerger un serveur de trafic, le rendant indisponible pour les utilisateurs légitimes.

- **Violations de données** : Les violations de données sont des incidents au cours desquels des données sensibles sont volées dans un système informatique.

Les violations de données peuvent avoir un impact significatif sur les entreprises, car elles peuvent entraîner des pertes financières, la perte de clients et une atteinte à la réputation.

### 1.2.2 Les meilleures pratiques pour sécuriser les serveurs :

Il existe un certain nombre de meilleures pratiques qui peuvent être utilisées pour sécuriser les serveurs. Certaines des meilleures pratiques les plus importantes incluent :

- **Maintenez vos logiciels à jour** : les mises à jour logicielles incluent souvent des correctifs de sécurité qui peuvent aider à protéger votre serveur contre les vulnérabilités connues.

- **Utilisez des mots de passe forts** : Les mots de passe doivent comporter au moins 12 caractères et doivent inclure un mélange de lettres majuscules et minuscules, de chiffres et de symboles.

- **Activer l'authentification à deux facteurs** : L'authentification à deux facteurs ajoute une couche de sécurité supplémentaire en demandant aux utilisateurs de saisir un code sur leur téléphone en plus de leur mot de passe.

- **Utilisez un pare-feu** : Un pare-feu peut aider à protéger votre serveur contre tout accès non autorisé. Sauvegardez vos données régulièrement : Des sauvegardes régulières peuvent aider à minimiser les dommages causés par une violation de données.

En suivant ces meilleures pratiques, vous pouvez aider à protéger vos serveurs contre les cyberattaques.

## 1.3 Contexte de recherche

Ce travail s'appuie sur les différents domaines de la Cybersécurité qui actuellement est déjà devenu un des points plus important dans le domaine de l'informatique Une Solution simple et pratique peut être proposée ; Pour rendre le serveur Plus sur et plus sécurisé

## 1.4 Solution technique

La solution la plus proche et la moins vorace en ressource serait de mettre en place un système de securite qui respecte le nécessaire des normes de securites dans un serveur web actuel.

## 1.5 Problématique

Sur un Serveur web il existe plusieurs sortes de vulnérabilités par lesquels on peut facilement y accéder Comme :

- **L'injection SQL** : en bref c'est une attaque qui consiste a insérer du code SQL malveillant dans les entrées d'un formulaires ...

- **Cross-Site Scripting(XSS)** : Comme son nom l'indique c'est une faille de securite qui permet un attaquant d'injecter du code malveillant dans une page web ou de faire une redirection vers un site frauduleux

Et j'en passe ;

Voici les quelques questions que nous allons nous poser tout au long de ce travail :

- Quel est le descriptif d'un bon système de securite ?
- Quels sont les systèmes de securites que nous allons utiliser ?
- Sur quel type de serveur web ce système sera efficace ?

## 1.6 Méthodologie

Pour arriver a une solution plausible nous allons utiliser une procédure qui va nous permettre d'installer des machines virtuelles ; différentes machines virtuelles configurée de différentes façon ; et tester différentes approches de sécurisation de serveurs et même essayer de les combinées pour voir si le résultat est solide .

## 1.7 Techniques

Pour ce travail la technique appropriée sera :

### 1.7.1 La Recherche sur Internet :

Parcourir les différents sites et forums qui proposent des travaux similaires aux miens , des vidéos et tutoriels pour les différentes configurations a faire pour ce travail ...

### 1.7.2 La Recherche Documentaire :

Utiliser les différents livres,revues ,archives ; Qui , en les utilisant pourront m'aider a atteindre mon but , ma solution solide .

### 1.7.3 La Recherche Expérimentale :

Faire des petites expérimentation sur mes machines virtuelles configurées comme des serveurs web

## 1.8 Limitation

Dans ce travail nous allons nous limiter a utiliser :

(En fonction de l'évolution de mon travail ce point va se remplir ).

## 1.9 Objectif

L'objectif visé dans ce travail est de pouvoir mettre en place un système de securite capable de remplir le travail nécessaire qui est actuellement demandé sur les serveurs web ;

De configurer un serveur web assez performant pour remplir les prérequis nécessaire qui sont demandés par la communauté des développeurs Web qui sont majoritairement amenés a utiliser les Serveurs Web Pour héberger leurs sites internet .

# Chapitre 2

## Les Serveurs

### 2.1 Définitions



FIGURE 2.1 – Une Salle Serveur

Les serveurs sont des ordinateurs ou des systèmes informatiques qui fournissent des services ou des ressources à d'autres ordinateurs ou utilisateurs sur un réseau. Ils peuvent être utilisés pour stocker des données, héberger des sites Web, exécuter des applications et bien plus encore. Il existe différents types de serveurs, tels que les serveurs de fichiers, les serveurs de messagerie, les serveurs de bases de données et les serveurs de jeux en ligne. Les serveurs sont souvent utilisés pour fournir des services à distance, ce qui permet aux utilisateurs d'y accéder à partir de n'importe où dans le monde. Dans ce point ci-après nous allons la plupart des sortes de serveurs les plus rependus

### Fonctionnement

Le serveur fonctionne en réseau; Peu importe sa mission, il a pour fonction d'écouter les requêtes formulées par les ordinateurs clients et de les traiter s'il le peut, en communiquant une information ou en donnant accès à un logiciel ou un fichier à l'utilisateur qui en a besoin.

Pour fonctionner correctement, le serveur doit être en mesure de vérifier certaines informations.

Il est en effet configuré pour autoriser l'accès à une liste précise d'utilisateurs, sur des plages horaires

définies ou à choisir qui peut lire, modifier ou supprimer des fichiers.

Cela implique que chaque ordinateur client soit identifiable et puisse recevoir la réponse du serveur selon la méthode attendue.

## Rôles

**Stockage** : Les serveurs stockent de grandes quantités de données, telles que des fichiers, des bases de données et des applications.

Ces données sont accessibles aux utilisateurs ou à d'autres serveurs du réseau. Les serveurs peuvent effectuer des calculs complexes, tels que ceux nécessaires à la recherche scientifique ou à la modélisation financière.

Cela permet aux autres ordinateurs du réseau de se concentrer sur d'autres tâches.

Les serveurs facilitent la communication entre les utilisateurs et les autres ordinateurs du réseau. Cela peut se faire par le biais du courrier électronique, du partage de fichiers ou de la navigation sur le web.

Les serveurs peuvent assurer la sécurité du réseau, par exemple en authentifiant les utilisateurs et en cryptant les données.

Outre ces rôles généraux, les serveurs peuvent être spécialisés dans des tâches spécifiques. Par exemple, un serveur web est un type de serveur qui héberge des sites web. Un serveur de base de données est un type de serveur qui stocke et gère des bases de données.

Le rôle spécifique d'un serveur dépend des besoins du réseau. Cependant, tous les serveurs ont pour objectif commun de fournir des services aux autres ordinateurs du réseau.

## Sortes De Serveur

1. Serveur Web
2. Serveur de Messagerie
3. Serveur de fichiers
4. Serveur de base de données
5. Serveur d'applications
6. Serveur de virtualisation
7. Serveur DNS
8. Serveur de sauvegarde
9. Serveur de jeu
10. Serveur de médias

## 2.2 Les Serveurs Web

Les serveurs Web sont des ordinateurs ou des programmes informatiques qui fournissent des pages Web aux clients qui les demandent via un navigateur Web. Ils sont utilisés pour héberger des sites Web et distribuer du contenu en ligne. Les serveurs Web peuvent exécuter différents types de logiciels, tels que Apache, Nginx, Microsoft IIS et bien d'autres. Les pages Web sont généralement créées en utilisant des langages de programmation Web tels que HTML, CSS et JavaScript. Les serveurs Web peuvent également exécuter des applications Web, telles que des forums en ligne, des blogs, des magasins en ligne et bien plus encore.

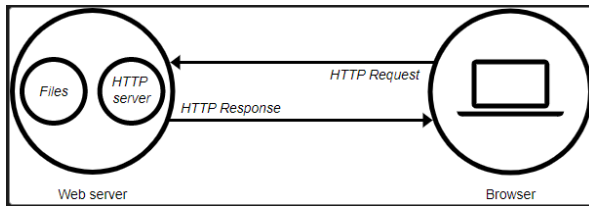


FIGURE 2.2 – Le Schéma d'un serveur Web

### 2.2.1 Quelques vulnérabilités Sur Les Serveurs Web

Il y a plusieurs vulnérabilités qui peuvent affecter un serveur web, en voici quelques exemples :

- **Injection SQL** : Cette vulnérabilité permet à un attaquant d'injecter du code SQL malveillant dans une requête pour détourner le contrôle de la base de données.
- **Cross-site scripting (XSS)** : Cette vulnérabilité permet à un attaquant d'injecter du code malveillant dans une page Web pour voler des informations d'authentification ou d'autres données sensibles.
- **Vulnérabilités du serveur HTTP** : Les serveurs HTTP tels que Apache, Nginx et IIS peuvent être vulnérables à des attaques telles que les dénis de service (DoS) et les dénis de service distribués (DDoS).
- **Mauvaise configuration** : Une mauvaise configuration du serveur web peut permettre aux attaquants d'accéder aux fichiers sensibles ou d'exécuter du code malveillant.
- **Vulnérabilités du CMS** : Les systèmes de gestion de contenu tels que WordPress et Drupal peuvent être vulnérables à des attaques telles que les injections SQL et les attaques de force brute.

Il est important de mettre en place des mesures de sécurité adéquates pour protéger les serveurs web contre ces vulnérabilités potentielles, telles que la mise à jour régulière de la sécurité du système et l'utilisation de logiciels de sécurité pour détecter et prévenir les attaques potentielles. Les développeurs de sites web doivent également être conscients des meilleures pratiques de sécurité, telles que la validation des entrées utilisateur et l'utilisation de l'encodage pour se protéger contre les attaques XSS.

## 2.3 Serveurs de Messageries

Un serveur de messagerie est un type de serveur qui est utilisé pour envoyer et recevoir des courriers électroniques (e-mails). Les serveurs de messagerie sont essentiels pour le fonctionnement du courrier électronique car ils sont responsables de la distribution des messages entre les différents utilisateurs.

Il existe deux types principaux de serveurs de messagerie : le serveur SMTP (Simple Mail Transfer Protocol) et le serveur POP (Post Office Protocol).

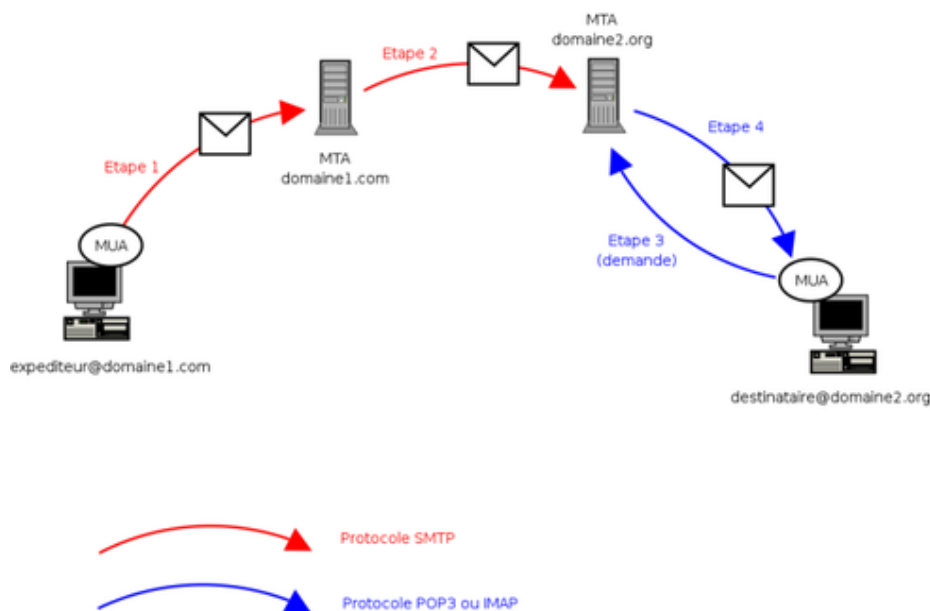


FIGURE 2.3 – Schéma d'un Serveur de Messagerie

Le serveur SMTP est utilisé pour envoyer des courriers électroniques. Lorsqu'un utilisateur envoie un e-mail, le client de messagerie envoie le message au serveur SMTP, qui se charge de le transférer au serveur de messagerie du destinataire.

Le serveur POP est utilisé pour récupérer les courriers électroniques sur le serveur de messagerie. Les clients de messagerie utilisent le protocole POP pour se connecter au serveur de messagerie et récupérer les messages qui leur sont destinés.

Il existe également un autre protocole appelé IMAP (Internet Message Access Protocol) qui est utilisé pour accéder aux messages sur le serveur de messagerie sans les télécharger sur l'ordinateur local. IMAP permet aux utilisateurs de se connecter à leur boîte de réception depuis n'importe quel ordinateur ou appareil connecté à Internet.

Les serveurs de messagerie peuvent être configurés pour fournir des fonctionnalités supplémentaires telles que la sécurité des messages, la gestion des spams et des virus, la gestion des listes de diffusion, etc. Les serveurs de messagerie sont également souvent intégrés à des suites de collaboration pour permettre le partage de calendriers, de contacts, de tâches, etc.

### 2.3.1 Quelques vulnérabilités Sur Les Serveurs de Messageries

Il existe plusieurs vulnérabilités potentielles qui peuvent affecter les serveurs de messagerie. Voici quelques exemples :

- **Injection de code** : Les attaquants peuvent exploiter des vulnérabilités dans le serveur de messagerie pour injecter du code malveillant dans les e-mails, qui peuvent ensuite être utilisés pour exécuter des attaques de phishing, des attaques de logiciels malveillants ou d'autres types d'attaques.

- **Attaques de force brute** : Les attaquants peuvent tenter de deviner les identifiants de connexion des utilisateurs en utilisant des attaques de force brute, qui impliquent l'utilisation de programmes pour tester toutes les combinaisons de noms d'utilisateur et de mots de passe possibles.

- **Attaques par déni de service (DoS) :** Les attaquants peuvent lancer des attaques par déni de service (DoS) contre le serveur de messagerie pour le rendre indisponible, ce qui peut empêcher les utilisateurs d'accéder à leurs e-mails ou de les envoyer.

- **Vulnérabilités de sécurité :** Les serveurs de messagerie peuvent avoir des vulnérabilités de sécurité connues qui peuvent être exploitées par les attaquants pour accéder à des données sensibles, tels que des courriels confidentiels ou des informations d'identification.

- **Vulnérabilités de configuration :** Les serveurs de messagerie peuvent avoir des vulnérabilités de configuration qui peuvent être exploitées par les attaquants pour accéder à des données sensibles, tels que des listes de contacts, des calendriers et des tâches.

Il est important de mettre en place des mesures de sécurité adéquates pour protéger les serveurs de messagerie contre ces vulnérabilités potentielles, telles que la mise à jour régulière de la sécurité du système et l'utilisation de logiciels de sécurité pour détecter et prévenir les attaques potentielles. Les utilisateurs doivent également être éduqués sur les meilleures pratiques de sécurité, telles que la création de mots de passe forts et l'utilisation de l'authentification à deux facteurs pour protéger leurs comptes de messagerie.

## 2.4 Serveur de fichiers

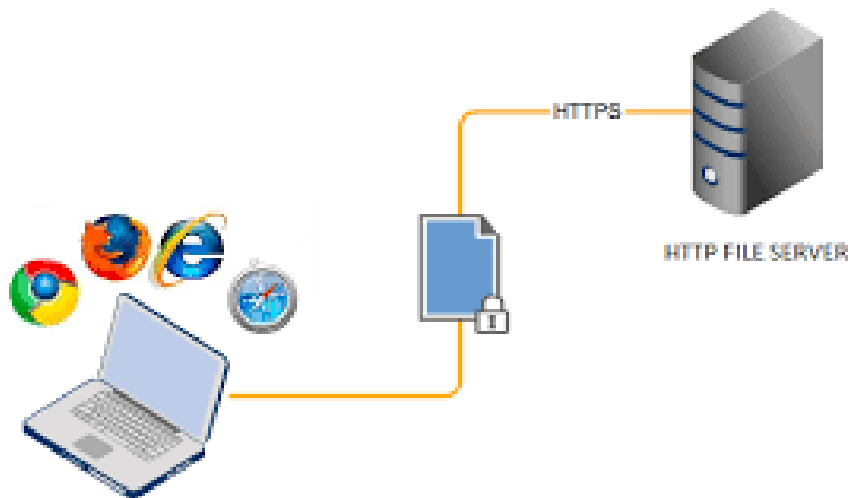


FIGURE 2.4 – Schéma De Serveur De Fichier

Un serveur de fichiers est un type de serveur qui stocke des fichiers et des dossiers, et permet à des utilisateurs de les accéder et de les partager via un réseau. Les serveurs de fichiers peuvent être configurés pour fournir différentes fonctionnalités, telles que :

1. **Partage de fichiers :** Les utilisateurs peuvent accéder aux fichiers stockés sur le serveur et les partager avec d'autres utilisateurs du réseau.
2. **Gestion des droits d'accès :** Les administrateurs peuvent définir des autorisations d'accès pour chaque utilisateur ou groupe d'utilisateurs, afin de contrôler qui peut accéder à quels fichiers.



3. Sauvegarde de données : Les serveurs de fichiers peuvent être configurés pour effectuer des sauvegardes régulières des fichiers stockés, afin de protéger les données contre la perte ou la corruption.
4. Synchronisation de fichiers : Les utilisateurs peuvent synchroniser des fichiers entre le serveur de fichiers et leur ordinateur local, pour assurer une cohérence des données.
5. Accès à distance : Les utilisateurs peuvent accéder aux fichiers stockés sur le serveur de fichiers à partir d'un emplacement distant en utilisant un client de connexion sécurisé.
6. Stockage en nuage : Les serveurs de fichiers peuvent être configurés pour stocker des fichiers dans le cloud, ce qui permet aux utilisateurs d'y accéder à partir de n'importe où avec une connexion Internet.
7. Accès multiplateforme : Les serveurs de fichiers peuvent être configurés pour fournir un accès multiplateforme aux utilisateurs, ce qui permet aux utilisateurs d'accéder aux fichiers à partir de différents systèmes d'exploitation tels que Windows, Mac OS ou Linux.

Les serveurs de fichiers sont couramment utilisés dans les entreprises pour stocker et partager des fichiers entre les employés, mais ils peuvent également être utilisés dans des environnements domestiques pour stocker et partager des fichiers entre les membres de la famille.

### 2.4.1 Quelques vulnérabilités Sur Les Serveurs de Fichier

Il existe plusieurs vulnérabilités potentielles qui peuvent affecter les serveurs de fichiers. Voici quelques exemples :

1. Vulnérabilités de sécurité : Les serveurs de fichiers peuvent avoir des vulnérabilités de sécurité connues qui peuvent être exploitées par les attaquants pour accéder à des données sensibles, telles que des fichiers confidentiels ou des informations d'identification.
2. Vulnérabilités de configuration : Les serveurs de fichiers peuvent avoir des vulnérabilités de configuration qui peuvent être exploitées par les attaquants pour accéder à des données sensibles, telles que des fichiers de configuration ou des répertoires de fichiers.
3. Attaques par déni de service (DoS) : Les attaquants peuvent lancer des attaques par déni de service (DoS) contre le serveur de fichiers pour le rendre indisponible, ce qui peut empêcher les utilisateurs d'accéder aux fichiers hébergés sur ce serveur.
4. Attaques de force brute : Les attaquants peuvent tenter de deviner les identifiants de connexion des utilisateurs en utilisant des attaques de force brute, qui impliquent l'utilisation de programmes pour tester toutes les combinaisons de noms d'utilisateur et de mots de passe possibles.
5. Fuites de données : Les serveurs de fichiers peuvent être vulnérables aux fuites de données, qui peuvent se produire lorsque des données sensibles sont stockées de manière inappropriée ou lorsque des utilisateurs non autorisés y ont accès.

Il est important de mettre en place des mesures de sécurité adéquates pour protéger les serveurs de fichiers contre ces vulnérabilités potentielles, telles que la mise à jour régulière de la sécurité du système et l'utilisation de logiciels de sécurité pour détecter et prévenir les attaques potentielles. Les utilisateurs doivent également être éduqués sur les meilleures pratiques de sécurité, telles que la création de mots de passe forts et l'utilisation de l'authentification à deux facteurs pour protéger leur accès aux fichiers stockés sur le serveur de fichiers.

## 2.5 Serveur de Base de Données

Un serveur de base de données est un type de serveur qui stocke des données et fournit des services pour gérer ces données. Il permet aux utilisateurs de stocker, d'organiser, d'accéder et de gérer des données de manière efficace et sécurisée.

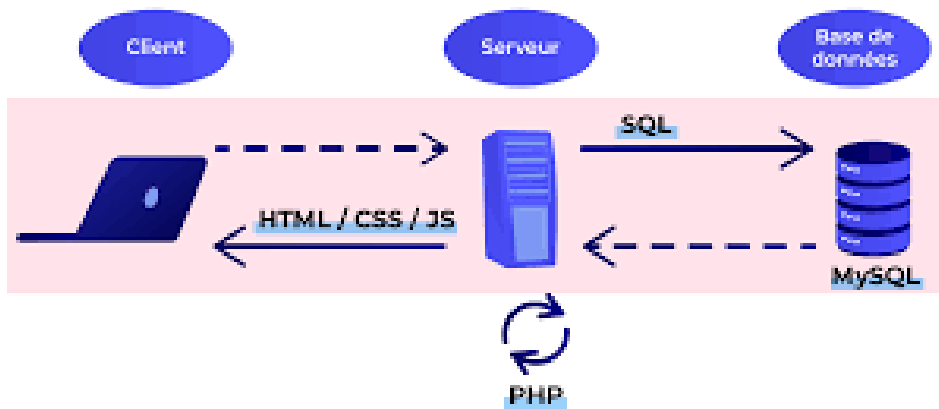


FIGURE 2.5 – Schema De Serveur De Base De Données

Les serveurs de base de données sont utilisés pour stocker des informations sur des produits, des clients, des transactions financières, des employés, des stocks, etc. Ils sont également utilisés pour alimenter des applications qui nécessitent un accès rapide et efficace aux données, telles que les sites web, les applications mobiles, les systèmes de gestion de la relation client (CRM), les systèmes de gestion de la chaîne d'approvisionnement (SCM), etc.

Les serveurs de bases de données peuvent être configurés pour fournir différentes fonctionnalités, telles que :

1. Langage de requête : Les serveurs de bases de données prennent en charge des langages de requête tels que SQL (Structured Query Language) pour interroger et récupérer les données stockées.
2. Gestion des transactions : Les serveurs de bases de données prennent en charge la gestion des transactions pour garantir l'intégrité des données et éviter les conflits.
3. Gestion des utilisateurs et des droits d'accès : Les administrateurs peuvent définir des autorisations d'accès pour chaque utilisateur ou groupe d'utilisateurs, afin de contrôler qui peut accéder à quelles données.
4. Sauvegarde et restauration : Les serveurs de bases de données peuvent être configurés pour effectuer des sauvegardes régulières des données stockées, afin de protéger les données contre la perte ou la corruption.
5. Réplication des données : Les serveurs de bases de données peuvent être configurés pour répliquer les données sur plusieurs serveurs, pour améliorer la disponibilité et la redondance des données.
6. Sécurité des données : Les serveurs de bases de données peuvent être configurés pour fournir des fonctionnalités de sécurité avancées, telles que le chiffrement des données, l'authentification à deux facteurs, etc.

Les serveurs de bases de données sont couramment utilisés dans les entreprises pour stocker et gérer des données importantes, mais ils peuvent également être utilisés dans des environnements domestiques pour stocker et gérer des données personnelles telles que les finances, les contacts, les photos, etc.

### 2.5.1 Quelques vulnérabilités Sur Les Serveurs de Base De Données

Il existe plusieurs vulnérabilités potentielles qui peuvent affecter les serveurs de bases de données. Voici quelques exemples :

1. Injection SQL : Les attaquants peuvent exploiter des vulnérabilités dans le serveur de base de données pour injecter du code SQL malveillant, qui peut permettre aux attaquants de prendre le contrôle du serveur de base de données, de modifier ou de supprimer des données, ou encore d'accéder à des informations confidentielles.
2. Vulnérabilités de sécurité : Les serveurs de bases de données peuvent avoir des vulnérabilités de sécurité connues, telles que la configuration par défaut de mots de passe faibles, qui peuvent être exploitées par les attaquants pour accéder à des données sensibles.
3. Attaques par déni de service (DoS) : Les attaquants peuvent lancer des attaques par déni de service (DoS) contre le serveur de base de données pour le rendre indisponible, ce qui peut empêcher les utilisateurs d'accéder aux données stockées sur ce serveur.
4. Vulnérabilités de configuration : Les serveurs de bases de données peuvent avoir des vulnérabilités de configuration qui peuvent être exploitées par les attaquants pour accéder à des données sensibles, telles que des informations de connexion ou des fichiers de configuration.
5. Fuites de données : Les serveurs de bases de données peuvent être vulnérables aux fuites de données, qui peuvent se produire lorsque des données sensibles sont stockées de manière inappropriée ou lorsque des utilisateurs non autorisés y ont accès.

Il est important de mettre en place des mesures de sécurité adéquates pour protéger les serveurs de bases de données contre ces vulnérabilités potentielles, telles que la mise à jour régulière de la sécurité du système et l'utilisation de logiciels de sécurité pour détecter et prévenir les attaques potentielles. Les développeurs de bases de données doivent également être conscients des meilleures pratiques de sécurité, telles que la validation des entrées utilisateur et l'utilisation de l'authentification à deux facteurs pour protéger l'accès aux données stockées sur le serveur de bases de données.

## 2.6 Serveur d'Application

Un serveur d'application est un type de serveur qui héberge des applications et fournit des services d'application aux clients. Les serveurs d'application sont essentiels pour les entreprises qui développent et déploient des applications commerciales, car ils fournissent une plateforme pour exécuter et gérer ces applications de manière efficace et sécurisée.

Les serveurs d'application peuvent être utilisés pour héberger une grande variété d'applications, telles que les applications de commerce électronique, les applications de gestion de contenu, les applications de gestion de la relation client (CRM), les applications de gestion de la chaîne d'approvisionnement (SCM), les applications de collaboration, etc.

Les serveurs d'application peuvent fournir différentes fonctionnalités, telles que :

1. Gestion de la connectivité : Les serveurs d'application peuvent gérer la connectivité entre les applications et les différents systèmes d'information, tels que les bases de données, les systèmes de fichiers, les services web, etc.
2. Gestion des transactions : Les serveurs d'application peuvent gérer les transactions pour garantir l'intégrité des données et éviter les conflits.
3. Gestion de la sécurité : Les serveurs d'application peuvent fournir des fonctionnalités de sécurité avancées pour protéger les applications et les données contre les menaces potentielles.
4. Gestion des sessions : Les serveurs d'application peuvent gérer les sessions pour assurer la continuité des services aux utilisateurs lorsqu'ils passent d'une page à l'autre ou lorsqu'ils se connectent à l'application à partir de différents appareils.

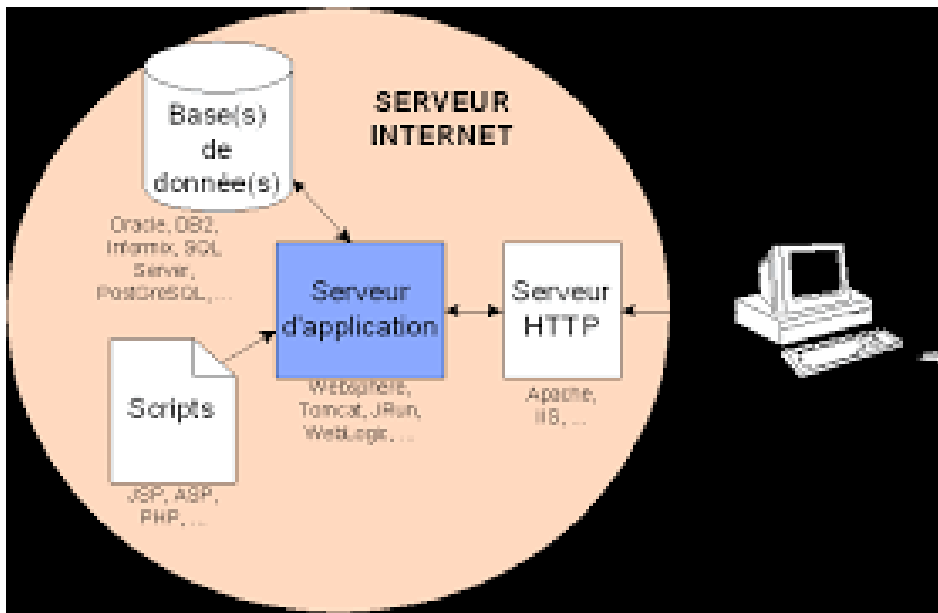


FIGURE 2.6 – Schéma D'un serveur D'application

5. Gestion des performances : Les serveurs d'application peuvent surveiller et optimiser les performances de l'application pour assurer une expérience utilisateur rapide et fluide.

Les serveurs d'application sont souvent utilisés en conjonction avec d'autres outils de développement et de déploiement, tels que les serveurs web, les bases de données, les outils de développement intégrés (IDE), les systèmes de contrôle de version, etc.

### 2.6.1 Quelques vulnérabilités Sur Les Serveurs d'Application

Il existe plusieurs vulnérabilités potentielles qui peuvent affecter les serveurs d'application. Voici quelques exemples :

1. Vulnérabilités de sécurité : Les serveurs d'application peuvent avoir des vulnérabilités de sécurité connues, telles que des failles dans les algorithmes de chiffrement ou des vulnérabilités dans les bibliothèques tierces, qui peuvent être exploitées par les attaquants pour accéder à des données sensibles ou prendre le contrôle du serveur.
2. Attaques par déni de service (DoS) : Les attaquants peuvent lancer des attaques par déni de service (DoS) contre le serveur d'application pour le rendre indisponible, ce qui peut empêcher les utilisateurs d'accéder aux applications hébergées sur ce serveur.
3. Injection de code : Les attaquants peuvent exploiter des vulnérabilités dans le serveur d'application pour injecter du code malveillant dans les applications, qui peuvent ensuite être utilisées pour exécuter des attaques de phishing, des attaques de logiciels malveillants ou d'autres types d'attaques.
4. Vulnérabilités de configuration : Les serveurs d'application peuvent avoir des vulnérabilités de configuration qui peuvent être exploitées par les attaquants pour accéder à des données sensibles, telles que des informations de connexion ou des fichiers de configuration.
5. Fuites de données : Les serveurs d'application peuvent être vulnérables aux fuites de données, qui peuvent se produire lorsque des données sensibles sont stockées de manière inappropriée ou

lorsque des utilisateurs non autorisés y ont accès.

Il est important de mettre en place des mesures de sécurité adéquates pour protéger les serveurs d'application contre ces vulnérabilités potentielles, telles que la mise à jour régulière de la sécurité du système et l'utilisation de logiciels de sécurité pour détecter et prévenir les attaques potentielles. Les développeurs d'applications doivent également être conscients des meilleures pratiques de sécurité, telles que la validation des entrées utilisateur et l'utilisation de l'authentification à deux facteurs pour protéger les applications hébergées sur le serveur d'application.

## 2.7 Serveur DNS

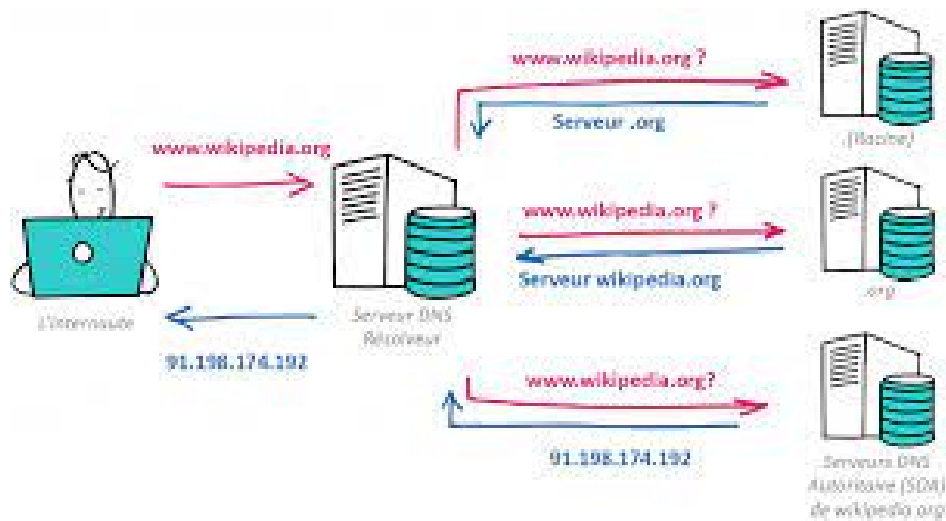


FIGURE 2.7 – Schéma d'un Serveur DNS

Un serveur DNS (Domain Name System) est un type de serveur qui permet de traduire les noms de domaine en adresses IP. Les noms de domaine sont des identificateurs textuels, tels que "google.com" ou "facebook.com", qui sont plus faciles à mémoriser que les adresses IP numériques qui identifient les ordinateurs et les serveurs sur Internet.

Lorsqu'un utilisateur entre un nom de domaine dans son navigateur web, le navigateur envoie une requête DNS au serveur DNS pour obtenir l'adresse IP correspondante. Le serveur DNS répond alors avec l'adresse IP, qui est utilisée pour établir la connexion avec le serveur web correspondant.

Les serveurs DNS sont essentiels pour le fonctionnement d'Internet, car ils permettent aux utilisateurs d'accéder aux sites web et aux services en ligne en utilisant des noms de domaine plutôt que des adresses IP numériques. Les serveurs DNS sont également utilisés pour acheminer le courrier électronique et pour fournir d'autres services de réseau.

Les serveurs DNS peuvent être configurés pour fournir différentes fonctionnalités, telles que :

1. Caching de requêtes : Les serveurs DNS peuvent mettre en cache les réponses aux requêtes DNS précédentes pour accélérer les temps de réponse et réduire la charge sur le réseau.

2. Résolution de noms de domaine : Les serveurs DNS peuvent résoudre les noms de domaine en adresses IP en utilisant des bases de données de noms de domaine et des serveurs racines.
3. Redirection de domaine : Les serveurs DNS peuvent être configurés pour rediriger les requêtes vers d'autres serveurs DNS, en fonction des besoins.
4. Sécurité DNS : Les serveurs DNS peuvent implémenter des fonctionnalités de sécurité avancées, telles que DNSSEC (DNS Security Extensions), pour protéger contre les attaques de DNS spoofing et de DNS cache poisoning.
5. Load balancing : Les serveurs DNS peuvent être utilisés pour répartir la charge entre plusieurs serveurs web en redirigeant les requêtes vers différents serveurs en fonction des besoins.

Les serveurs DNS sont souvent gérés par les fournisseurs de services Internet (ISP), les entreprises et les organisations gouvernementales. Les utilisateurs peuvent également configurer leur propre serveur DNS pour fournir une résolution de noms de domaine personnalisée ou pour améliorer la sécurité et la performance de leur réseau local.

### 2.7.1 Quelques vulnérabilités Sur Les Serveurs DNS

Il existe plusieurs vulnérabilités potentielles qui peuvent affecter les serveurs de DNS (Domain Name System). Voici quelques exemples :

1. Attaques par déni de service (DoS) : Les attaquants peuvent lancer des attaques par déni de service (DoS) contre le serveur de DNS pour le rendre indisponible, ce qui peut empêcher les utilisateurs d'accéder aux noms de domaine associés à ce serveur.
2. Vulnérabilités de sécurité : Les serveurs de DNS peuvent avoir des vulnérabilités de sécurité connues qui peuvent être exploitées par les attaquants pour accéder à des données sensibles, telles que des informations de connexion ou des fichiers de configuration.
3. Attaques de cache poisoning : Les attaquants peuvent exploiter des vulnérabilités dans le serveur de DNS pour modifier le contenu du cache DNS, ce qui peut rediriger les utilisateurs vers des sites web malveillants.
4. Vulnérabilités de configuration : Les serveurs de DNS peuvent avoir des vulnérabilités de configuration qui peuvent être exploitées par les attaquants pour accéder à des données sensibles, telles que des informations de connexion ou des fichiers de configuration.
5. Fuites de données : Les serveurs de DNS peuvent être vulnérables aux fuites de données, qui peuvent se produire lorsque des données sensibles sont stockées de manière inappropriée ou lorsque des utilisateurs non autorisés y ont accès.

Il est important de mettre en place des mesures de sécurité adéquates pour protéger les serveurs de DNS contre ces vulnérabilités potentielles, telles que la mise à jour régulière de la sécurité du système et l'utilisation de logiciels de sécurité pour détecter et prévenir les attaques potentielles. Les administrateurs de DNS doivent également être conscients des meilleures pratiques de sécurité, telles que la mise en place de politiques de sécurité strictes pour l'accès au serveur de DNS et la configuration correcte du serveur de DNS pour minimiser les risques d'attaques de cache poisoning.

## 2.8 Serveur de Jeu

Un serveur de jeu est un type de serveur qui permet de fournir des services de jeu en ligne à des joueurs du monde entier. Les serveurs de jeu sont utilisés pour héberger des jeux multijoueurs en ligne, tels que les jeux de tir à la première personne, les jeux de stratégie en temps réel, les jeux de rôle en ligne massivement multijoueurs (MMORPG), les jeux de sport en ligne, etc.

Les serveurs de jeu offrent des fonctionnalités telles que :



FIGURE 2.8 – Un Schema de Serveur de Jeu

1. Hébergement de jeux multijoueurs : Les serveurs de jeu sont utilisés pour héberger des jeux multijoueurs en ligne pour permettre aux joueurs de jouer ensemble sur Internet.
2. Gestion des joueurs : Les serveurs de jeu peuvent gérer les joueurs, les scores, les classements et les statistiques de jeu, ainsi que les opérations de modération pour assurer un environnement de jeu sécurisé et équitable.
3. Optimisation des performances : Les serveurs de jeu peuvent être optimisés pour offrir des performances de jeu optimales, telles que des temps de latence réduits et une faible latence pour une expérience de jeu fluide.
4. Gestion de la bande passante : Les serveurs de jeu peuvent gérer la bande passante pour optimiser les performances de jeu et éviter les problèmes de lag ou de décalage.
5. Gestion des mises à jour : Les serveurs de jeu peuvent gérer les mises à jour de jeu pour maintenir les joueurs à jour avec les dernières fonctionnalités et correctifs de bugs.

Les serveurs de jeu sont utilisés par les développeurs de jeux pour héberger leurs jeux en ligne et fournir des services de jeu en ligne à des millions de joueurs dans le monde entier. Les serveurs de jeu peuvent être exploités directement par les développeurs de jeux ou par des fournisseurs de services tiers spécialisés dans l'hébergement de serveurs de jeu. Les serveurs de jeu sont essentiels pour les jeux multijoueurs en ligne, car ils permettent aux joueurs de jouer ensemble sur Internet, offrant ainsi une expérience de jeu immersive et sociale.

Il existe plusieurs vulnérabilités potentielles qui peuvent affecter les serveurs de jeu. Voici quelques exemples :

1. Vulnérabilités de sécurité : Les serveurs de jeu peuvent avoir des vulnérabilités de sécurité connues qui peuvent être exploitées par les attaquants pour accéder à des données sensibles, telles que des informations de compte de joueur ou des données de paiement.
2. Attaques par déni de service (DoS) : Les attaquants peuvent lancer des attaques par déni de service (DoS) contre le serveur de jeu pour le rendre indisponible, ce qui peut empêcher les joueurs d'accéder au jeu ou de jouer en ligne.
3. Exploits de jeu : Les attaquants peuvent exploiter des vulnérabilités dans le code du jeu pour gagner un avantage injuste sur les autres joueurs, ou pour perturber le jeu pour tous les autres joueurs.
4. Vulnérabilités de configuration : Les serveurs de jeu peuvent avoir des vulnérabilités de configuration qui peuvent être exploitées par les attaquants pour accéder à des données sensibles, telles que des informations de connexion ou des fichiers de configuration.
5. Fuites de données : Les serveurs de jeu peuvent être vulnérables aux fuites de données, qui peuvent se produire lorsque des données sensibles sont stockées de manière inappropriée ou lorsque des utilisateurs non autorisés y ont accès.

Il est important de mettre en place des mesures de sécurité adéquates pour protéger les serveurs de jeu contre ces vulnérabilités potentielles, telles que la mise à jour régulière de la sécurité du système et l'utilisation de logiciels de sécurité pour détecter et prévenir les attaques potentielles. Les développeurs de jeux doivent également être conscients des meilleures pratiques de sécurité, telles que la validation des entrées utilisateur et l'utilisation de l'authentification à deux facteurs pour protéger les comptes de joueur. Les administrateurs de serveurs de jeu doivent également surveiller les activités suspectes et mettre en place des politiques de sécurité strictes pour minimiser les risques d'attaques.

## **Constat**

Si vous remarquez bien que sur tout les serveurs que je viens de citer nous voyons que les attaques comme :

1. L'Attaque Par Déni de Service (DoS).
2. Vulnérabilité de Configuration.
3. Fuites de données.
4. Vulnérabilité de Sécurité .

Dans ce le chapitre qui suit nous allons essayer de parler des méthodes, manières par lesquelles nous pouvons éviter de tomber dans les pièges d'attaques citées ci-hauts .



## Chapitre 3

# La CyberSécurité et La Sécurité Informatique

### 3.1 La CyberSécurité

#### 3.1.1 Définition

La racine « cyber » provient du mot cybernétique, qui avait été formé en français en 1834 pour désigner la « science du gouvernement », à partir du grec Kubernêtiké, signifiant « diriger, gouverner ».

Terme repris en 1948, par le mathématicien Norman Wiener aux États-Unis à l'origine de la cybernétique (cybernetics), science constituée par l'ensemble des théories relatives au contrôle, à la régulation et à la communication entre l'être vivant et la machine. La cybersécurité, également appelée sécurité informatique ou sécurité des technologies de l'information, est l'ensemble des mesures techniques, organisationnelles et juridiques mises en place pour protéger les systèmes informatiques, les réseaux et les données contre les attaques, les pertes ou les altérations. Elle vise à garantir la confidentialité, l'intégrité et la disponibilité des informations stockées sur les systèmes informatiques, ainsi que la protection de la vie privée et des droits de propriété intellectuelle.

La cybersécurité concerne la sécurité informatique et des réseaux des environnements connectés à Internet et accessibles via le cyberspace. Elle peut être mise en défaut, entre autres, par des cyberattaques informatiques. Du fait de l'usage extensif d'Internet, de nouvelles menaces sont apparues générant des risques additionnels dont les impacts, de niveaux d'importance variables, peuvent affecter les individus, les organisations ou les États.

La cybersécurité est devenue un enjeu majeur dans le monde numérique d'aujourd'hui, où les attaques informatiques sont de plus en plus sophistiquées et fréquentes. Elle est essentielle pour protéger les systèmes informatiques et les données sensibles contre les menaces potentielles et assurer la continuité des activités des organisations qui les utilisent. La cybersécurité est également importante pour protéger les utilisateurs finaux, tels que les consommateurs et les employés, contre les risques de vol d'identité, de fraude en ligne et d'autres formes de cybercriminalité.

Le préfixe « Cyber » est relatif à l'environnement informatique et aux activités rendues possibles par les technologies du numérique et de l'Internet.

Le cyberspace (l'ensemble des infrastructures numériques, des données et des services mis en réseaux) est une extension de notre espace naturel qui reflète notre société avec ses réalités politique, économique,

sociale et culturelle. Mais contrairement à la terre, à la mer, à l'air et à l'espace-extra atmosphérique, le cyberspace est une pure création de l'être humain qui ne relève pas de la nature.

Les points essentiels englobés par la cybersécurité comprennent :

**1. La confidentialité :**

la protection des données contre les accès non autorisés. Cela inclut la protection des données personnelles, des secrets commerciaux, des informations financières et autres informations sensibles.

**2. L'intégrité :**

la protection des données contre les altérations non autorisées. Cela inclut la garantie que les données sont exactes et fiables.

**3. La disponibilité :**

la garantie que les systèmes, les réseaux et les données sont accessibles et fonctionnent correctement, et que les interruptions de service sont minimisées.

**4. L'authenticité :**

la garantie que les utilisateurs sont bien ceux qu'ils prétendent être, et que les données sont bien celles qu'elles prétendent être.

**5. La non-répudiation :**

la garantie qu'une personne ne peut pas nier avoir effectué une action ou avoir envoyé des données.

**6. La résilience :**

la capacité des systèmes et des réseaux à résister aux attaques et à récupérer rapidement en cas d'incident.

**7. La conformité :**

le respect des lois, des réglementations et des normes en matière de sécurité informatique.

**8. La sensibilisation :**

l'éducation et la formation des utilisateurs pour qu'ils comprennent les risques liés à la sécurité informatique et les meilleures pratiques à suivre pour les éviter.

Ces points essentiels sont interconnectés et doivent être pris en compte dans toute stratégie de cybersécurité efficace.

### **3.1.2 Pourquoi la cybersécurité est-elle nécessaire ?**

En 2021, le cybercrime a coûté au monde 6 000 milliards de dollars américains. D'ici 2025, ce coût passera à 10 500 milliards de dollars. Le cybercrime est un problème de plus en plus sérieux, et pour s'y attaquer, il est essentiel de disposer d'un excellent dispositif de cybersécurité.

Les individus, les gouvernements, les entreprises, les organismes à but non lucratif et les établissements d'enseignement risquent tous de subir des cyberattaques et des violations de données. À l'avenir, le nombre d'attaques se multipliera, avec l'évolution des technologies numériques, l'augmentation du nombre d'appareils et d'utilisateurs, les chaînes logistiques mondiales de plus en plus complexes, et le rôle de plus en plus stratégique des données dans l'économie numérique. Pour minimiser le risque d'une attaque et pour sécuriser les systèmes et les données, un solide dispositif de cybersécurité devient vital.

### **3.1.3 Comment les risques de cybersécurité sont-ils mesurés ?**

Le risque de cybersécurité correspond au potentiel de perte ou de préjudice résultant de l'endommagement d'une ressource informatique, susceptible d'entraîner un vol de propriété intellectuelle, une perte financière, une atteinte à la réputation, et des amendes légales ou réglementaires. En mesurant les risques, les entreprises peuvent optimiser les actions permettant de mieux les gérer, et s'assurer ainsi qu'il n'y a pas d'obstacles aux objectifs commerciaux.

**Identifier les ressources et définir leur priorité.** L'évaluation des risques de cybersécurité commence par la compréhension des ressources de l'entreprise et la définition de leur priorité, en établissant celles dont la perte, l'exposition ou l'endommagement pourrait avoir un impact sur les opérations.

**Identifier les vulnérabilités.** Toutes les vulnérabilités susceptibles de laisser une menace causer des dommages sont identifiées à l'aide de l'analyse automatique des vulnérabilités, des tests d'intrusion, ou de l'utilisation d'une base de données de vulnérabilités telle que la [base de données nationale des vulnérabilités du NIST](#).

**Calculer l'impact de la menace.** L'impact probable ou le dommage que pourrait causer une menace à une ressource est calculé et classé comme élevé, moyen ou faible.

**Calculer le risque.**  $\text{Risque} = \text{Menace} \times \text{Vulnérabilité} \times \text{Ressource}$ . À partir de cette équation, l'entreprise peut mesurer chaque risque.

**Créer une matrice de risques pour la planification des corrections.** Enfin, la matrice de risques est établie, les deux axes représentant la probabilité et l'impact.

**Risque = Probabilité x Impact.** À partir de cette valeur, chaque risque est classé comme élevé, moyen ou faible, à la suite de quoi les stratégies de réduction appropriées sont mises en œuvre.

		IMPACT		
		LOW	MEDIUM	HIGH
LIKELIHOOD	HIGH	LOW	MEDIUM	HIGH
	MEDIUM	LOW	MEDIUM	MEDIUM
	LOW	LOW	LOW	LOW

FIGURE 3.1 – Un Tableau Illustrant Les Impact

### 3.1.4 Cybersécurité avec défense en profondeur (DEP)

Il n'existe pas de méthode ou d'outil de cybersécurité capable de défendre de tous les types d'attaque. Voilà pourquoi la cybersécurité avec défense en profondeur (DEP) est essentielle.

Avec la DEP, également connue sous le nom d'« approche forteresse » en matière de cybersécurité, des mécanismes défensifs multiples sont mis en œuvre pour protéger les ressources d'entreprise.

Cette approche multicouche renforce la sécurité globale. De plus, si un mécanisme échoue, les autres

fonctionneront pour prévenir ou stopper les cyberattaques.

Une stratégie de cybersécurité avec DEP inclut différents éléments :

**Logiciel antivirus.** Les solutions antivirus comportant des fonctionnalités heuristiques qui recherchent et signalent les activités suspectes offrent une plus forte protection que les solutions classiques basées sur des signatures.

**Contrôles de sécurité du réseau.** Les pare-feu et les systèmes de protection contre les intrusions peuvent identifier des menaces de sécurité potentielles, et les bloquer à partir de règles de sécurité.

**Solutions d'intégrité des données.** Ces produits vérifient les adresses IP sources pour confirmer que les fichiers entrants proviennent de sources connues et de confiance uniquement.

**Analyse comportementale.** Ces systèmes analysent les comportements des fichiers et des réseaux en fonction de comportements « normaux » prédéfinis. Ils envoient ensuite des alertes ou effectuent des actions automatiques pour bloquer une violation ou l'empêcher de se poursuivre.

**Stratégies et procédures.** Les stratégies de gestion des risques, de gestion de la chaîne logistique, de la réponse aux incidents, etc. permettent de renforcer la cybersécurité.

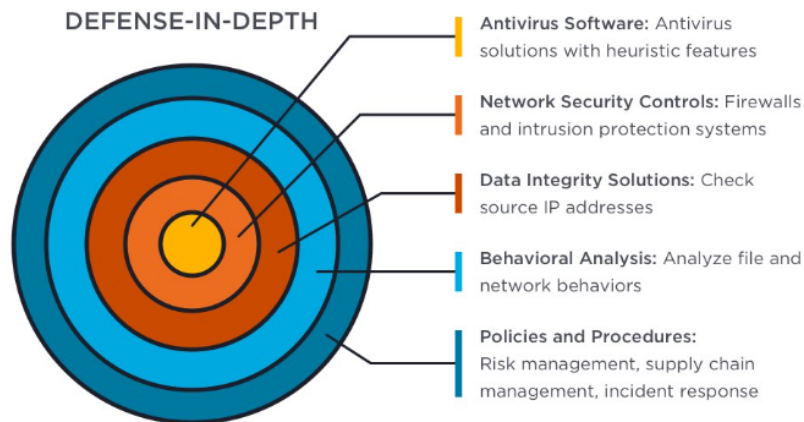


FIGURE 3.2 – Un Schéma Illustrant Le DEP

### 3.1.5 Comment mettre en œuvre la cybersécurité

Le panorama des cybermenaces est en constante évolution. La mise en œuvre d'un solide dispositif de cybersécurité peut donc s'avérer être un véritable défi. Elle n'est toutefois pas impossible, si les entreprises suivent une approche systématique en intégrant les éléments suivants :

**Analyse et gestion des risques.** Une approche basée sur les risques garantit que les équipes de sécurité auront connaissance des risques les plus critiques pour l'entreprise, et pourront adopter l'intervention adéquate pour réduire leur impact éventuel.

**Inventaire et gestion des ressources.** Il est essentiel de comprendre les ressources d'une entreprise pour appréhender et gérer les risques qui menacent ces ressources. Identification et gestion des vulnérabilités.

Les vulnérabilités doivent être identifiées et corrigées dès que possible, en particulier si elles sont critiques et peuvent véritablement nuire à l'entreprise.

**Déploiement de la gestion des accès et identités.** Pour éviter à la fois les attaques de l'intérieur et de l'extérieur, il est essentiel de protéger et de contrôler l'accès aux services, aux systèmes et aux données.

**Sécurité des données.** L'ensemble des données organisationnelles doit être protégé de tout accès ou utilisation non autorisés.

**Gestion des incidents.** Une bonne gestion des incidents peut réduire l'impact et les dommages causés par les incidents de sécurité.

**Sécurité de la chaîne logistique.** Il est essentiel d'identifier et d'appréhender de manière cohérente les risques et vulnérabilités sur les réseaux tiers.

**Formation des salariés.** Selon une étude IBM, l'erreur humaine est responsable de 49 pourcent des violations. Une autre étude de la Stanford University estime que les erreurs humaines, en particulier celles des salariés, est à l'origine de 88 pourcent des violations. Les salariés utilisent souvent des mots de passe faibles, se font avoir par les e-mails d'hameçonnage, ou n'installent pas les mises à jour de sécurité sur leurs appareils. Il est vital de former le personnel aux bonnes habitudes de cybersécurité pour bénéficier d'une solide protection.

L'identification, l'évaluation et la mesure des risques sont des composantes importantes de la mise en place d'un programme de cybersécurité. Sans ces étapes essentielles, les entreprises ne pourront sans doute pas mettre en œuvre un dispositif solide, ni améliorer leur posture de sécurité.

## 3.2 But

Le but concret de la cybersécurité est de protéger les systèmes informatiques, les réseaux, les programmes et les données contre les attaques, les dommages, les modifications ou les fuites non autorisées. La cybersécurité vise à prévenir les cyberattaques, à détecter les violations de sécurité, à réduire les dommages potentiels et à réagir efficacement en cas d'incident de sécurité.

## 3.3 objectif

L'objectif concret de la cybersécurité est de protéger les systèmes informatiques, les réseaux, les programmes et les données contre les attaques, les dommages, les modifications ou les fuites non autorisées. La cybersécurité vise à prévenir les cyberattaques, à détecter les violations de sécurité, à réduire



FIGURE 3.3 – Le CyberSecurity Framework

les dommages potentiels et à réagir efficacement en cas d'incident de sécurité.

En 2020, le vol de données et les cyberattaques arrivaient à la 6e et à la 7e place des risques mondiaux les plus importants en termes de probabilité de survenue.

En 2021, les hackers continuent d'exploiter la pandémie de COVID-19 et le passage au télétravail opéré en conséquence.

Ainsi, les cyberattaques ont augmenté de 21 pourcent dans le monde entier. La cybersécurité joue un rôle crucial pour se tenir à distance de telles menaces et des personnes malveillantes.

Les cybercriminels recherchent constamment le talon d'Achille des systèmes informatiques d'entreprise.

Pour éviter d'être victimes de cyberattaques, les entreprises doivent mettre en œuvre les outils, les technologies et le personnel adéquats en matière de cybersécurité.

## 3.4 La Sécurité Informatique

### 3.4.1 Définition

La sécurité informatique est l'ensemble des mesures techniques, organisationnelles et juridiques mises en place pour protéger les systèmes informatiques, les réseaux et les données contre les attaques, les pertes ou les altérations. Elle vise à garantir la confidentialité, l'intégrité et la disponibilité des informations stockées sur les systèmes informatiques, ainsi que la protection de la vie privée et des droits de propriété intellectuelle.

La sécurité informatique englobe un large éventail de domaines, tels que la sécurité des réseaux, la sécurité des systèmes d'exploitation, la sécurité des applications, la sécurité des données, la sécurité

physique, la gestion des identités et des accès, la conformité aux normes de sécurité, la surveillance et la détection des incidents de sécurité, ainsi que la réponse aux incidents de sécurité.

La sécurité informatique est devenue un enjeu majeur dans le monde numérique d'aujourd'hui, où les attaques informatiques sont de plus en plus sophistiquées et fréquentes. La mise en place d'une politique de sécurité informatique efficace est donc essentielle pour protéger les systèmes informatiques et les données sensibles contre les menaces potentielles et assurer la continuité des activités des organisations qui les utilisent.



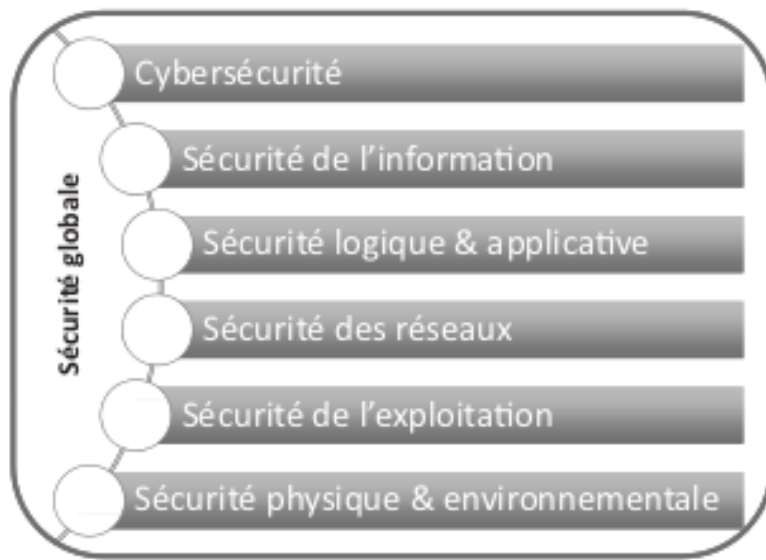


FIGURE 3.4 – Les Différents Points Englobés par La sécurité Informatique

La sécurité informatique englobe plusieurs domaines d'applications :

1. sécurité physique et environnementale ;
2. sécurité de l'exploitation ;
3. sécurité des réseaux ;
4. sécurité logique, sécurité applicative et sécurité de l'information ;

### 3.5 La sécurité informatique, pour quoi faire ?

La dernière décennie a été marquée par la migration de pratiquement tous les aspects des activités d'une entreprise vers un environnement en ligne. Dès lors, chaque entreprise se retrouve exposée à un risque de cyberattaque, dont le but peut être de voler des informations sensibles, telles que des données clients et des détails de paiement, des éléments de propriété intellectuelle et des secrets commerciaux, ou tout simplement de porter atteinte à la réputation de l'entreprise.

Par ailleurs, la généralisation du télétravail, la migration vers le cloud et la prolifération des appareils connectés offrent aux pirates informatiques et autres cybercriminels des possibilités quasi infinies d'attaques. Cette surface d'attaque élargie, combinée à la sophistication croissante des cyberadversaires numériques, a imposé aux entreprises de renforcer et d'actualiser leurs pratiques de sécurité afin de protéger leurs ressources basées dans le cloud en particulier.

Dans une certaine mesure, la sécurité informatique est une question de droit. En effet, dans certains pays, la loi impose aux entreprises d'investir dans le développement et l'implémentation de concepts de sécurité informatique, tandis que d'autres pays ont fixé des normes strictes en matière de confidentialité et de protection des données.

## 3.6 Types de sécurité informatique

La sécurité informatique est un terme générique qui désigne tout plan, mesure ou outil destiné à protéger les ressources numériques d'une entreprise. La sécurité informatique comprend plusieurs éléments :

**La cybersécurité** a pour but d'assurer la protection des ressources numériques (réseaux, systèmes, ordinateurs, données, etc.) contre les cyberattaques.

**La sécurité des endpoints, ou protection des endpoints**, est l'approche qui vise à protéger les endpoints (ordinateurs de bureau, ordinateurs portables, terminaux mobiles, etc.) contre les activités malveillantes.

**La sécurité du cloud** regroupe la stratégie et les solutions de protection contre les cybermenaces de l'infrastructure cloud, ainsi que de tout service ou application hébergé dans l'environnement cloud.

**La sécurité des applications** couvre toutes les mesures mises en place pour réduire la vulnérabilité des applications et ainsi empêcher tout vol, fuite ou compromission de données ou de code au sein de l'application.

**La sécurité du réseau** désigne les outils, les technologies et les processus utilisés pour protéger le réseau et l'infrastructure critique contre les cyberattaques et les activités malveillantes. Elle inclut un ensemble de mesures préventives et défensives conçues pour refuser tout accès non autorisé aux ressources et aux données.

**La sécurité des conteneurs** est le processus continu de protection des conteneurs, y compris du pipeline des conteneurs, de l'infrastructure de déploiement et de la supply chain, contre les cybermenaces.

**La sécurité de l'IoT** est une subdivision de la cybersécurité qui couvre la protection, la surveillance et la neutralisation des menaces ciblant l'Internet des objets (IoT) et le réseau de terminaux IoT connectés qui collectent, stockent et partagent des données via Internet.

### 3.7 Sécurité informatique et sécurité des informations, quelle différence ?

Bien que la sécurité informatique soit parfois confondue avec la sécurité des informations, il s'agit de deux concepts bien distincts. La principale différence réside dans la forme dans laquelle les données sont stockées et, par extension, dans la manière dont elles sont protégées.

La sécurité des informations consiste à protéger les données, quelle que soit leur forme. Il peut s'agir de protéger les données stockées par voie électronique, ainsi que de mesures de sécurité physiques telles que le verrouillage des armoires de classeurs ou des clés d'accès aux bureaux.

La sécurité informatique concerne quant à elle la protection des données et autres ressources exclusivement sous forme numérique.

### 3.8 Sécurité informatique et cybersécurité, quelle différence ?

Il importe également de faire la distinction entre sécurité informatique et cybersécurité.

La cybersécurité fait référence à la protection de l'entreprise contre tout accès non autorisé et toute attaque malveillante.

Par comparaison, la sécurité informatique revêt un caractère plus large. Elle couvre notamment toute fonctionnalité permettant de protéger et de préserver la confidentialité, l'intégrité et la disponibilité des données contre toute menace numérique.

Cela peut notamment inclure la protection contre les problèmes de sécurité non malveillants en soi, comme un composant matériel défaillant ou une configuration incorrecte du système.

### 3.9 Risques associés à la sécurité informatique

Les risques associés à la sécurité informatique peuvent être divisés en deux catégories : les perturbations du système et les attaques malveillantes ciblées.

Une perturbation du système peut consister en une interruption temporaire des activités de l'entreprise induite par un composant système tel qu'un composant matériel défectueux, une panne réseau ou une faille logicielle. Face à une telle situation, l'entreprise s'expose à des pertes de revenus résultant de son incapacité à fonctionner ou de l'atteinte possible à sa réputation.

Si la préservation du fonctionnement du système constitue une composante majeure de la sécurité informatique, la protection contre les cyberattaques est plus importante encore dans la mesure où la plupart de ces attaques visent à accéder à des données ou autres informations sensibles ou à les dérober. Voici quelques cyberattaques courantes :

1. **Virus informatiques** : les virus informatiques sont des programmes malveillants qui peuvent se propager à d'autres ordinateurs et causer des dommages aux fichiers et aux données. Les virus peuvent se propager via des e-mails, des pièces jointes, des sites web malveillants ou des supports de stockage infectés.
2. **Logiciels malveillants** : les logiciels malveillants, tels que les chevaux de Troie, les vers, les spywares, les rootkits, les ransomwares, etc., sont conçus pour infecter les systèmes informatiques et causer des dommages aux données et aux fichiers.

3. **Phishing** : le phishing est une technique d'ingénierie sociale qui vise à tromper les utilisateurs en les incitant à divulguer des informations personnelles ou confidentielles telles que des mots de passe, des numéros de carte de crédit ou des informations bancaires.
4. **Piratage informatique** : le piratage informatique est une activité malveillante visant à infiltrer un système informatique ou un réseau en utilisant des techniques telles que l'exploitation de failles de sécurité, la force brute ou le vol de mots de passe.
5. **Espionnage industriel** : l'espionnage industriel est une activité visant à voler des informations confidentielles telles que des plans de produits, des données de recherche et développement ou des secrets commerciaux.
6. **Cyberterrorisme** : le cyberterrorisme est une forme de terrorisme qui utilise des techniques informatiques pour causer des dommages à des systèmes informatiques, des réseaux ou des infrastructures critiques.
7. **Cyber-espionnage** : le cyber-espionnage est une activité visant à recueillir des informations confidentielles sur les gouvernements, les entreprises ou les individus à des fins d'espionnage.
8. **Réseaux de robots ou botnets** Un réseau de robots est un ensemble d'ordinateurs compromis supervisés via un canal de commande et contrôle. La personne qui exploite l'infrastructure de commande et contrôle, à savoir le maître des robots ou botmaster, utilise ces ordinateurs compromis, ou robots, pour lancer des attaques destinées à faire tomber le réseau d'une cible, à injecter des logiciels malveillants, à collecter des identifiants ou à exécuter des tâches gourmandes en puissance de calcul.

### 3.10 Bonnes pratiques en matière de sécurité informatique

La prévalence du terme « sécurité informatique » ne signifie nullement que la sécurité est un « problème informatique ». Ce n'est pas non plus un problème qui sera résolu uniquement à l'aide de solutions technologiques.

Pour élaborer une stratégie de cybersécurité à la fois complète et efficace, les entreprises doivent tenir compte des règles, des processus et des technologies mis en œuvre dans l'ensemble des fonctions métier. Par ailleurs, les utilisateurs du réseau doivent être correctement formés aux comportements responsables en ligne, ainsi qu'à la détection des signes d'attaques réseau courantes.

Dans le monde connecté actuel, une stratégie de cybersécurité globale est absolument essentielle. Les stratégies de cybersécurité les plus efficaces combinent ressources humaines et solutions technologiques avancées, telles que l'intelligence artificielle (IA), le Machine Learning (ML) et d'autres formes d'automatisation intelligente, afin d'améliorer la détection des activités anormales et de réduire le délai d'intervention et de correction.

#### Une stratégie de sécurité IT doit intégrer les éléments suivants :

**La détection et l'intervention sur les endpoints (EDR)** forment une solution complète qui identifie et contextualise toute activité malveillante afin d'aider l'équipe de sécurité à prioriser les efforts de réponse et de correction en cas de compromission de sécurité.

**La détection et l'intervention managées (MDR)** sont un service de cybersécurité qui allie technologie et expertise humaine pour mettre en place des opérations de Threat Hunting, de surveillance et d'intervention. La MDR a pour principal avantage de favoriser une identification rapide des cybermenaces et d'en limiter les répercussions sans avoir à augmenter les effectifs.

**La réponse à incident** consiste en une série d'étapes mises en place pour prévenir, détecter et bloquer les compromissions de données, ainsi que pour restaurer les systèmes. Elle aboutit généralement à l'établissement d'un plan de réponse à incident qui décrit les étapes et procédures que l'organisation devra suivre en cas d'incident de sécurité.

**Un antivirus de nouvelle génération (NGAV, Next-Generation Antivirus)** combine intelligence artificielle, détection des comportements, algorithmes de Machine Learning et atténuation des exploits, afin d'anticiper et de prévenir immédiatement toutes les menaces de sécurité, connues comme inconnues.

**Un test d'intrusion** consiste en une simulation d'attaque réelle visant à tester les capacités de détection et de réponse de l'entreprise.

### Qu'attendre d'un antivirus de nouvelle génération ?

Un antivirus de nouvelle génération efficace doit s'appuyer sur des technologies innovantes pour faire face à des cyberadversaires qui changent constamment de tactiques, techniques et procédures pour s'infiltrer dans les entreprises, qu'il s'agisse de malwares de base ou zero day, ou encore d'attaques avancées sans logiciels malveillants. Les fonctionnalités de prévention à privilégier sont les suivantes :

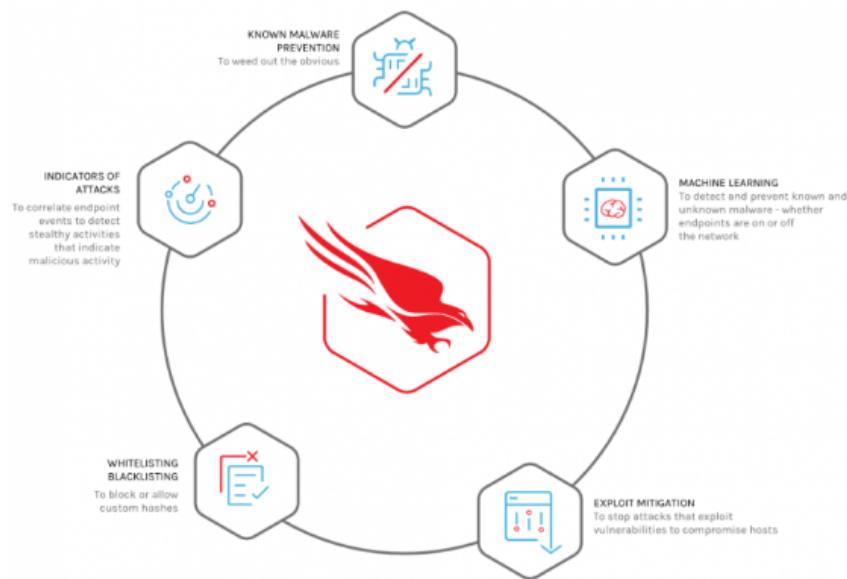


FIGURE 3.5 –

#### 1. Prévention des logiciels malveillants connus et inconnus

a) **Protection antimalware sans fichiers de signatures** La protection antimalware sans fichiers de signatures utilise des algorithmes de Machine Learning pour déterminer la probabilité qu'un fichier soit malveillant. Les nouvelles menaces sont bloquées en temps réel et la rentabilité est immédiate.

b) **Machine Learning** Le Machine Learning peut détecter et contrer les logiciels malveillants connus et inconnus, que les endpoints soient connectés au réseau ou non. Il détecte les indicateurs d'attaque de manière plus rapide et précise, élimine les ransomwares et comble les failles laissées par les antivirus d'ancienne génération.

## 2. Prévention des attaques sans logiciels malveillants

a). Indicateurs d'attaque Les indicateurs d'attaque mettent en corrélation les événements se produisant au niveau des endpoints afin de détecter les activités furtives, signes d'intentions malveillantes.

Une solution s'appuyant sur une analyse hors ligne rétrospective pour identifier les indicateurs d'attaque est incapable de rester au fait des dernières cybermenaces, en plus de nécessiter des ressources considérables.

Les algorithmes en ligne qui exploitent le Machine Learning et n'ont pas besoin d'un ensemble complet de données pour effectuer des analyses pertinentes sont à la fois plus rapides, plus efficaces et plus performants.

b) Blocage des exploits Les malwares ne sont pas toujours distribués au moyen de fichiers. Les attaques basées sur des macros, des commandes d'exécution, des chargeurs en mémoire et d'autres techniques sans fichiers sont en effet de plus en plus courantes.

Le blocage des exploits permet de détecter et de bloquer les exploits dès qu'ils se produisent.

## 3. Intégration de la cyberveille L'intégration de la cyberveille permet de déterminer immédiatement l'origine, l'impact et la gravité des attaques dans l'environnement et apporte les conseils nécessaires pour une intervention décisive et une résolution rapide.

## 4. Solution native au cloud L'architecture cloud est une composante fondamentale des antivirus de nouvelle génération.

Un NGAV basé dans le cloud peut être totalement opérationnel en quelques secondes, et ce sans redémarrage, mise à jour des signatures, configuration ni acquisition d'une nouvelle infrastructure.

Les algorithmes peuvent traiter en direct l'activité des endpoints et exposer les fichiers malveillants et les comportements suspects en temps quasi réel, sans incidence sur les performances des endpoints.

## Chapitre 4

# La Configuration Du Serveur Web (ISS) Et La Sécurisation de ce dernier