RÉSUMÉ THÉORIQUE – FILIÈRE DÉVELOPPEMENT DIGITAL

M108 - S'INITIER À LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

45 heures

SOMMAIRE

1. **Introduire la sécurité informatique**
   - Introduire la notion de sécurité
   - Comprendre les types d'attaques des systèmes informatiques
   - Se prémunir d'une quelconque tentative de piratage
2. **Assurer la confidentialité des données**
   - Confidentialiser les données clients
   - Maitrise des règles de protection des données utilisateurs
   - Protéger les données utilisateurs
3. **Protéger les applications Web**
   - Sécuriser un service
   - Utiliser les firewalls

MODALITÉS PÉDAGOGIQUES

1

LE GUIDE DE SOUTIEN

Il contient le résumé théorique et le manuel des travaux pratiques

2

LA VERSION PDF

Une version PDF est mise en ligne sur l'espace apprenant et formateur de la plateforme WebForce Life

3

DES CONTENUS TÉLÉCHARGEABLES

Les fiches de résumés ou des exercices sont téléchargeables sur WebForce Life

4

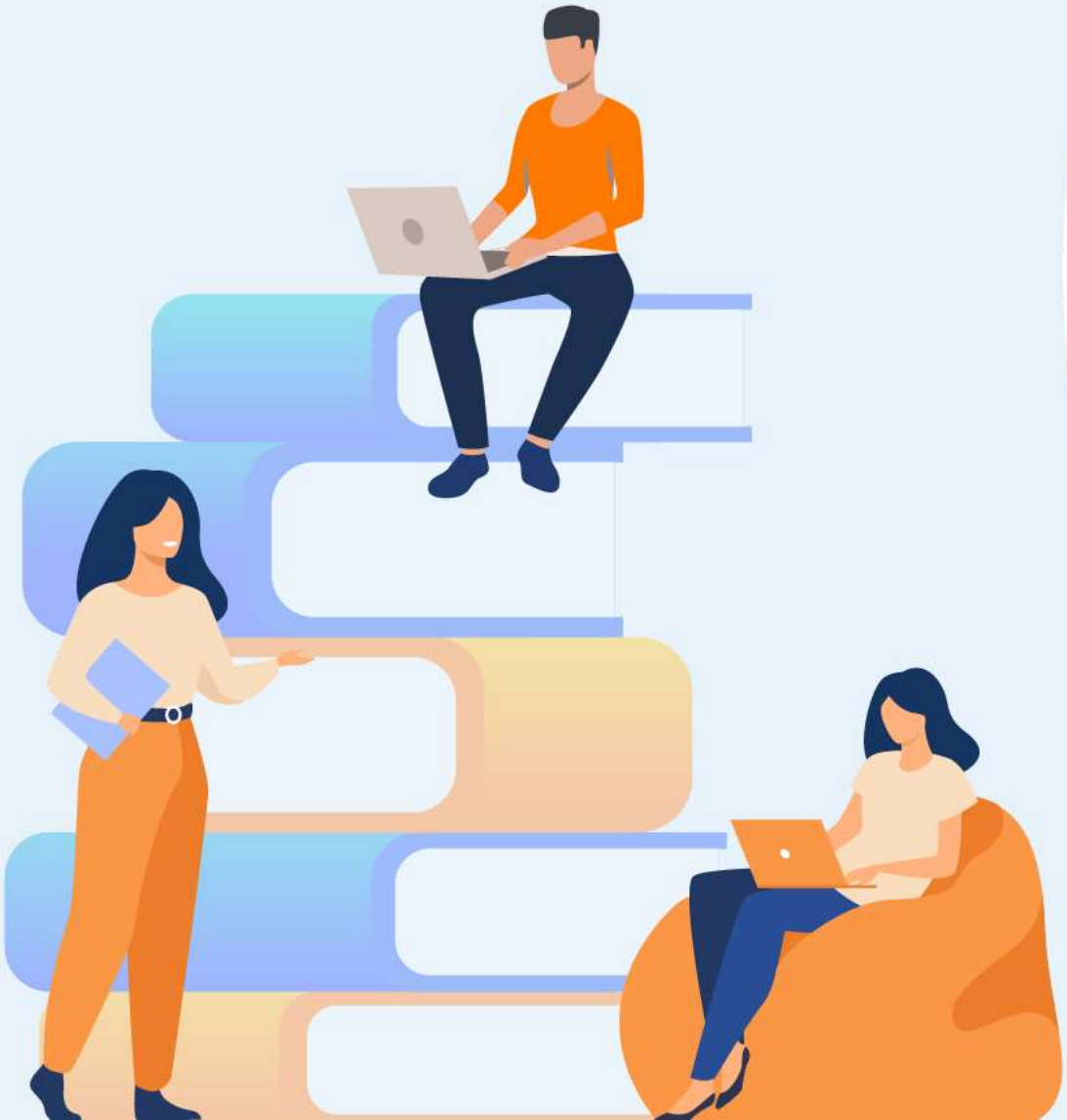
DU CONTENU INTERACTIF

Vous disposez de contenus interactifs sous forme d'exercices et de cours à utiliser sur WebForce Life

5

DES RESSOURCES EN LIGNES

Les ressources sont consultables en synchrone et en asynchrone pour s'adapter au rythme de l'apprentissage



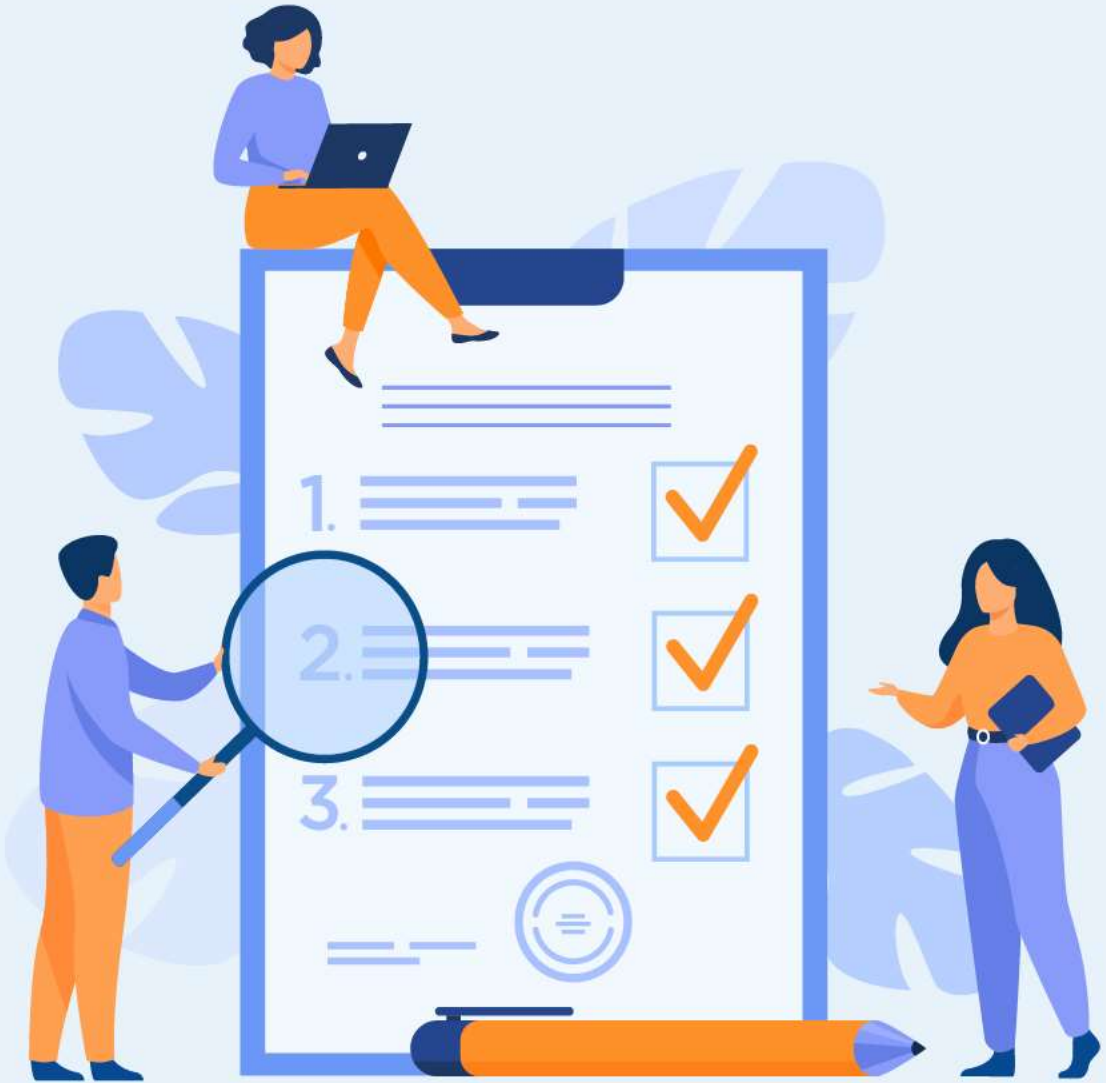
PARTIE 1

Introduire la sécurité informatique

Dans ce module, vous allez :

- Découvrir la notion de sécurité informatique
- Connaitre les différents types des attaques et des virus
- Maitriser les techniques et outils de protection

10 heures



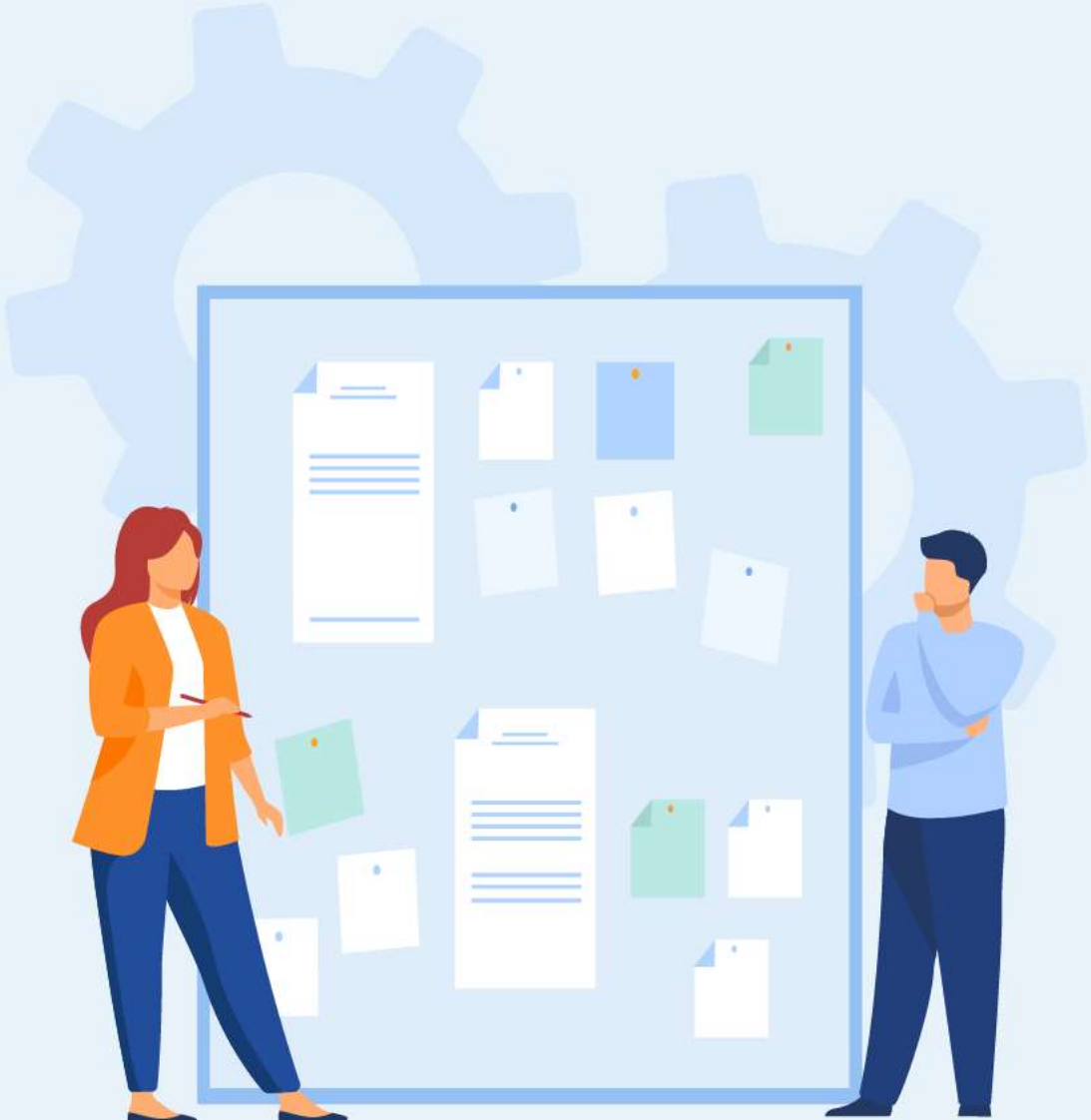
CHAPITRE 1

Introduire la notion de sécurité

Ce que vous allez apprendre dans ce chapitre :

- La notion de sécurité informatique
- Les types de failles et attaques
- Les types de virus
- La notion de Copyright

03 heures



CHAPITRE 1

Introduire la notion de sécurité

1. **La notion de sécurité informatique**
2. Les types de failles et attaques
3. Les types de virus
4. La notion de Copyright

PARTIE 1

Définition

La sécurité informatique est l'ensemble des systèmes, des stratégies et des moyens techniques mise en place pour protéger un système informatique contre toute utilisation, violation, intrusion ou vol de données. Tout en respectant ses trois (3) :

- **La confidentialité** : C'est la protection contre **l'accès non autorisé aux informations**.
- **Intégrité** : C'est la protection contre **la modification non autorisée des informations**. Même si un pirate ne peut pas lire vos données, il peut les corrompre ou les modifier de manière sélective pour causer des dommages ultérieurs.
- **Disponibilité** : C'est la protection contre le **déni d'accès aux informations**. Même si un pirate ne peut pas accéder à vos données ou les modifier, il peut vous empêcher d'y accéder ou de les utiliser.

Ces principes sont liés aux états de l'information et à certaines mesures de sécurité. **Le cube de McCumber** représente cette relation d'une manière très simple.

La triade de sécurité de l'information Confidentialité, Intégrité, Disponibilité(CID).

Le Cube de McCumber

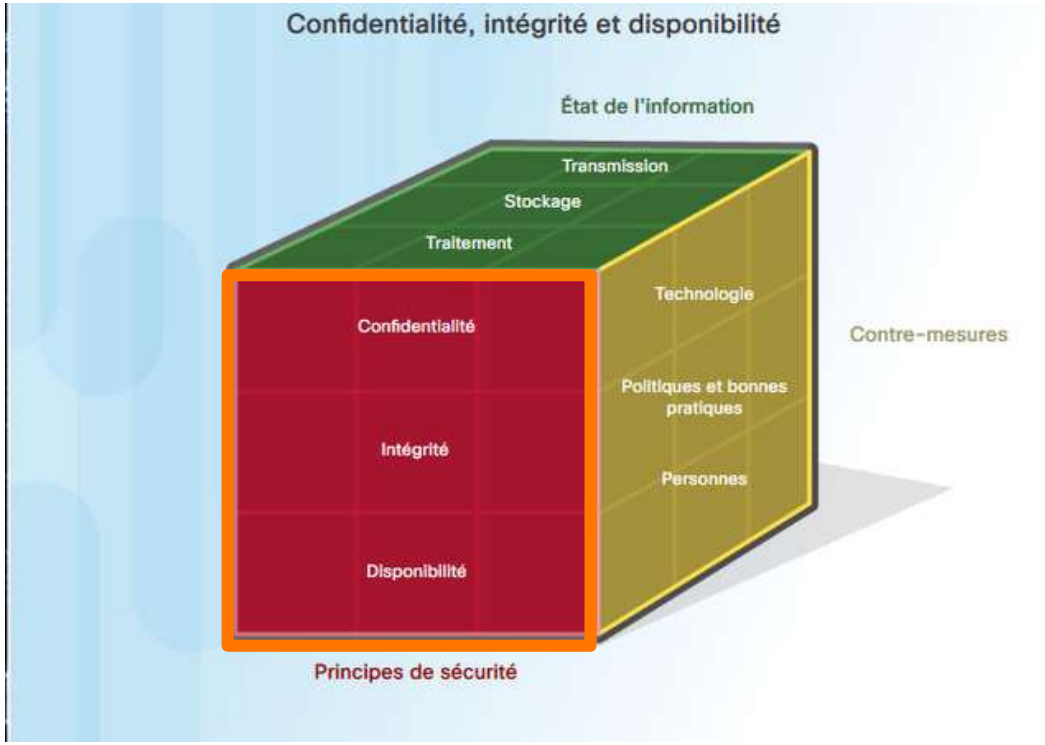
Le Cube de la sécurité informatique (également appelé Cube de McCumber) est un outil développé par ***John McCumber***, l'un des premiers experts de la sécurité informatique , afin d'aider à gérer la protection des réseaux, des domaines et de l'Internet.

Ce Cube a trois dimensions et ressemble un peu à un cube de Rubik.

John McCumber
UCLA European Languages & Transcultural Studies

Les principes de la sécurité

La première dimension du cube de la cybersécurité identifie les objectifs identifiés précédemment et qui sont les principes fondamentaux de la triade de la **CID**. Notamment **la confidentialité, l'intégrité et la disponibilité.**



*Le Cube de McCumber est conçu pour répondre à la sécurité informatique. Le contour orange entour la face des **principes de la sécurité***

PARTIE 1

PARTIE 1

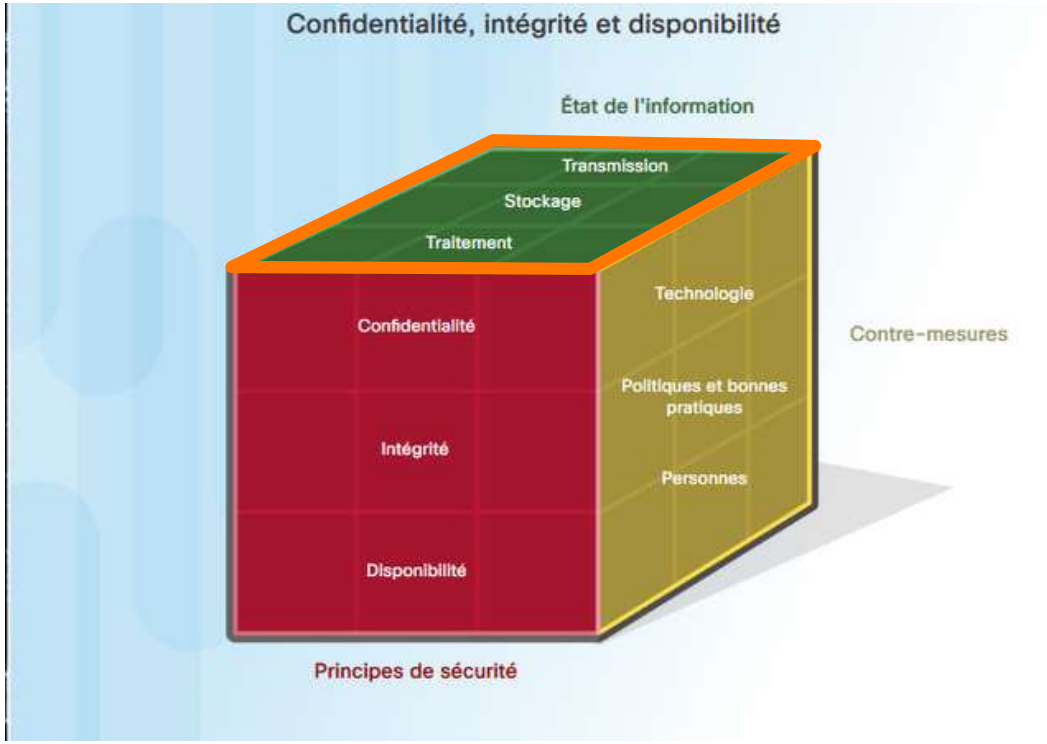
Les états de l'information

La deuxième dimension du Cube de la sécurité informatique traite le problème de la protection des données durant ces différentes états possibles :

•**Transmission** : transfert de données entre systèmes d'information - également appelé données en transit (DET).

•**Stockage** : Données au repos (DAR), telles que celles stockées en mémoire ou sur un disque dure.

•**Traitement** : réalisation d'opérations sur des données afin d'atteindre un objectif souhaité.



*Le Cube de McCumber est conçu pour répondre à la sécurité informatique. Le contour orange entour la face des **états de l'information***

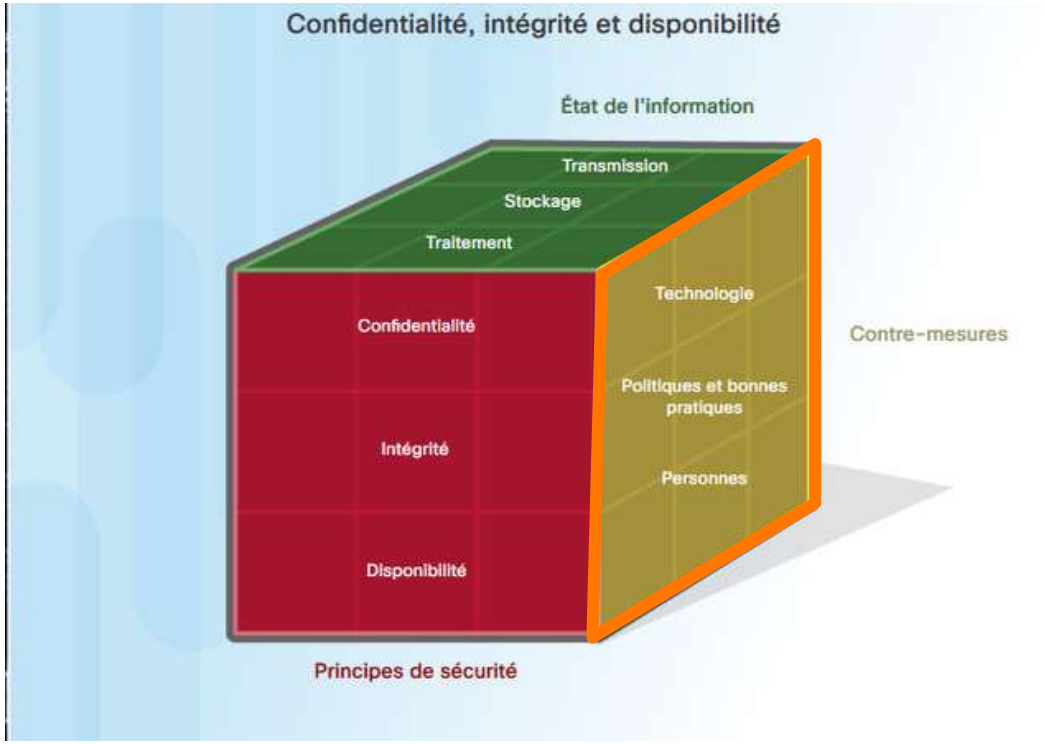
PARTIE 1

Mesures de protection de la cybersécurité (Contre-mesures)

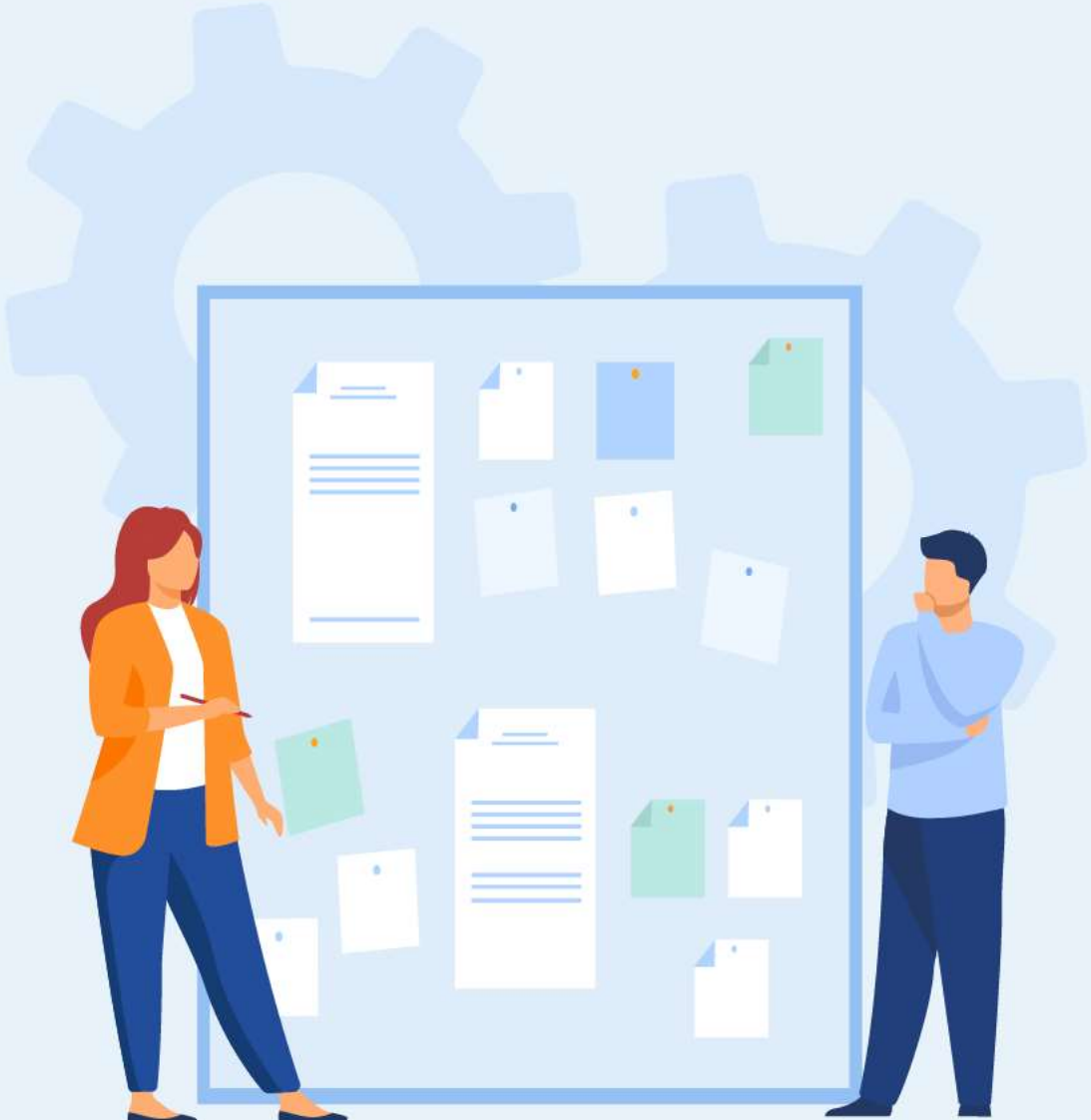
La troisième dimension du cube de McCumber définit les compétences et les disciplines auxquelles un professionnel de la sécurité informatique peut faire appel. Tout en veillant toujours de rester du "bon côté" de la loi.

Ces compétences et disciplines sont :

- **Politiques et bonnes pratiques** : contrôles administratifs, tels que les directives de gestion, qui fournissent une base pour la mise en œuvre de l' assurance de l'information au sein d'une organisation. (exemples : politiques d'utilisation acceptable ou procédures de réponse aux incidents) - également appelées opérations .
- **Personnes** : s'assurer que les utilisateurs des systèmes d'information sont conscients de leurs rôles et responsabilités en matière de protection des systèmes d'information et sont capables de suivre les normes.
- **Technologie** : solutions logicielles et matérielles conçues pour protéger les systèmes d'information (exemples : antivirus, pare-feu, systèmes de détection d'intrusion, etc.)



*Le Cube de McCumber est conçu pour répondre à la sécurité informatique. Le contour orange entour la face des **Contre-mesures***



CHAPITRE 1

Introduire la notion de sécurité

1. La notion de sécurité informatique
2. **Les types de failles et attaques**
3. Les types de virus
4. La notion de Copyright

C’est quoi une attaque informatique ?

Les attaques informatique (ou Cyberattaques) sont des actions offensives visant les systèmes, les infrastructures ou les réseaux informatiques, ou même des ordinateurs personnels. En utilisant diverses méthodes et moyens, pour voler, modifier ou détruire des données ou des systèmes informatiques.

La cybersécurité est la méthode de protection des réseaux, des systèmes informatiques et de leurs composants contre tout accès numérique non autorisé.

Maintenant que vous savez ce qu'est une cyberattaque, examinons les différents types de cyberattaques.

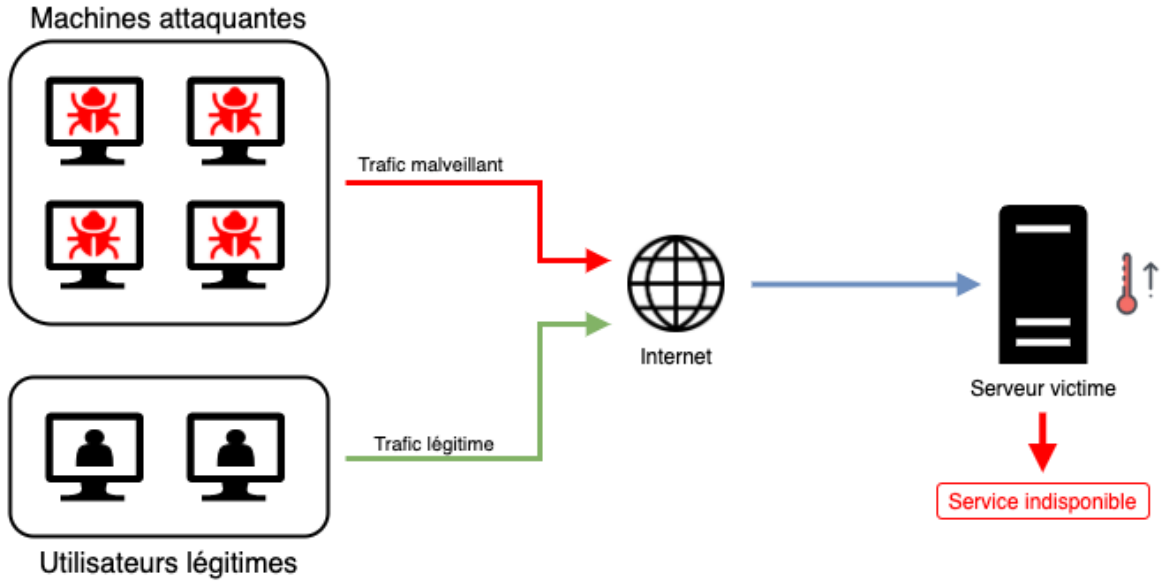


Figure 1 : Un schéma montrant un exemple d’une cyber attaque qui montre comment l’attaquant augment le trafic vers la machine cible et par conséquence elle devienne indisponible

PARTIE 1

PARTIE 1

les différents types de cyberattaques

Il existe de différents types de cyberattaques. Si nous connaissons ces différents types, il nous devient plus facile de protéger nos réseaux et nos systèmes informatique. Ici, nous examinerons de près les principales cyberattaques.

Les attaques par déni de service (DoS) et par déni de service distribué (DDoS) :

- Une attaque DoS est une attaque qui a comme but de submerger les ressources d'un système ou une application a fin de le rendre indisponible,
- Une attaque DDoS (attaque de déni de service distribué) a aussi le même concept de submerger les ressources d'un système, mais elle est exécutée à partir d'autres machines hôtes infectées par un logiciel malveillant contrôlé par l'attaquant.
- Les types d'attaques **DoS** et **DDoS** les plus courantes sont les attaques **SYN flood**, les attaques **Teardrop**, les attaques **par rebond**, **le ping de la mort** et les **botnets**.

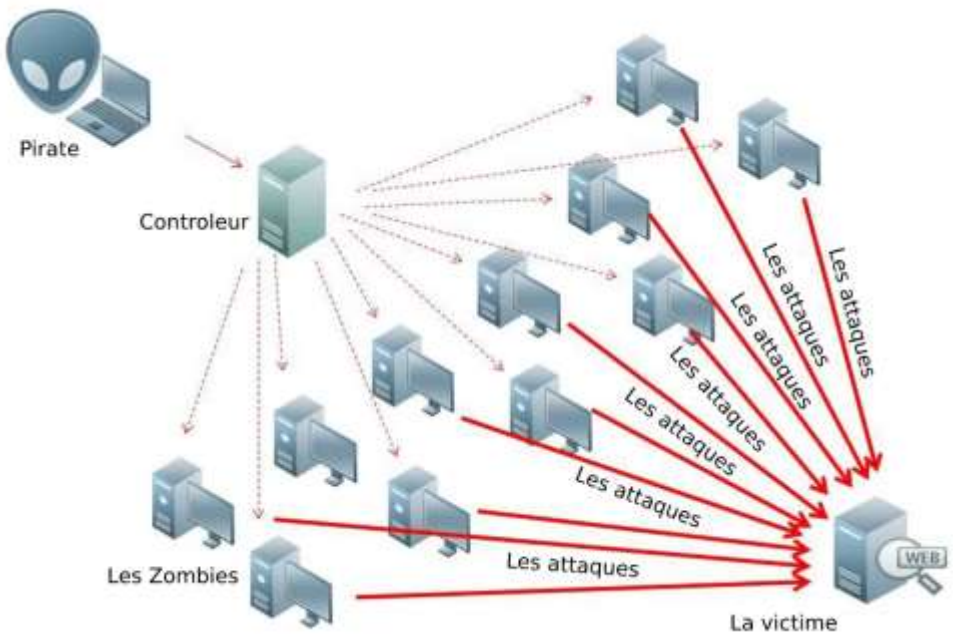


Figure 1 : Principe des attaques DDoS. Le pirate utilise un serveur contrôleur qui contrôle des machine infectées par un logiciel malveillant pour envoyer des requêtes multiple et submerge la machine cible.

Attaque de l'homme au milieu (MitM) :

Une attaque d'homme du milieu (MITM) est un terme général désignant le moment où un pirate se positionne dans une conversation entre un utilisateur et une application ou un site web, soit pour écouter, soit pour se faire passer pour l'une des parties, ce qui donne l'impression qu'il s'agit d'un échange normal d'informations.

D'une manière générale, une attaque MITM équivaut à un facteur qui ouvre votre relevé bancaire, pour noter les détails de votre compte, puis referme l'enveloppe et la livre à votre porte.

Malware :

Le terme "malware" englobe différents types d'attaques, notamment les logiciels espions, les virus et les vers. Les logiciels malveillants utilisent une vulnérabilité pour pénétrer dans un réseau lorsqu'un utilisateur clique sur un lien dangereux "planté" ou une pièce jointe dans un e-mail, ce qui installera un logiciel malveillant dans le système.

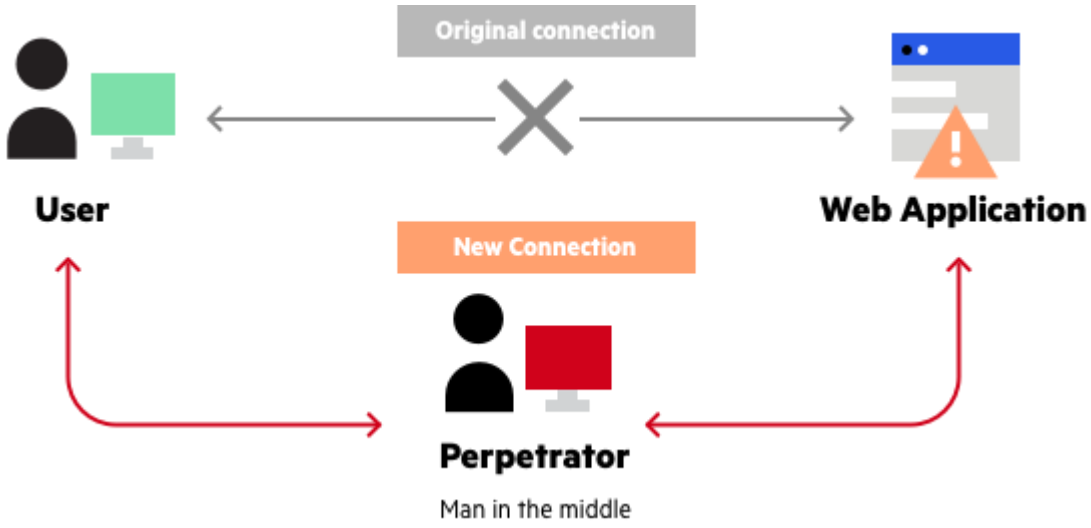


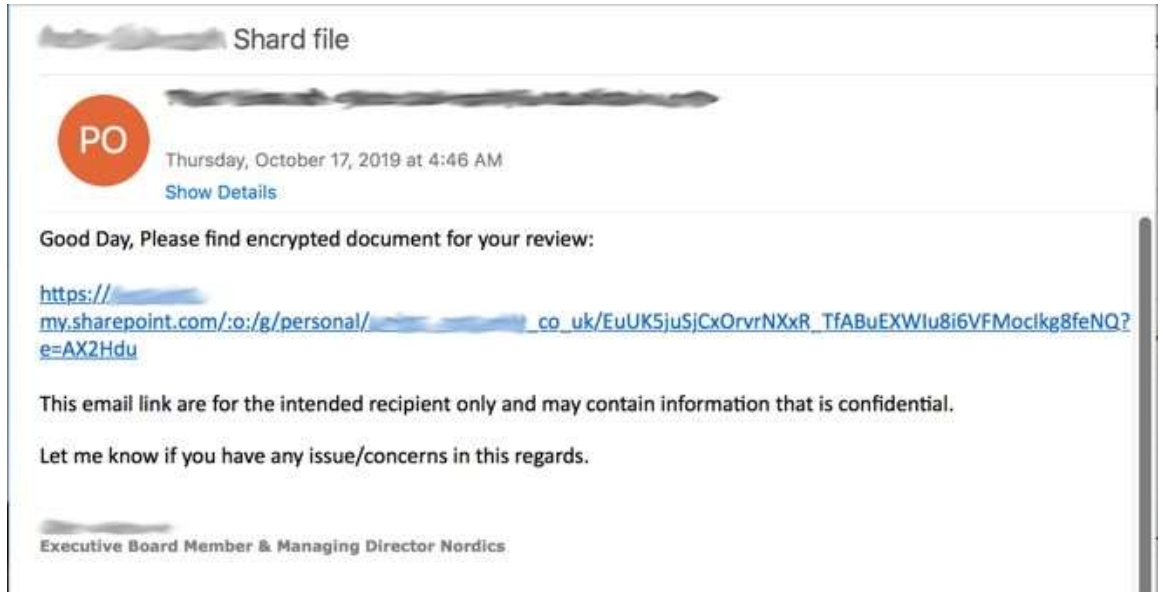
Figure 1 : le pirate se positionne au milieux de la conversation entre l'utilisateur et l'application pour récupérer et contrôler les données envoyées et recrevées par les deux parties

PARTIE 1

Hameçonnage :

Les attaques par hameçonnage sont extrêmement courantes et consistent à envoyer des quantités massives de mails frauduleux à des utilisateurs peu méfiants, déguisés en provenance d'une source fiable.

Ces e-mails frauduleux ont souvent l'apparence d'être légitimes, mais ils lient le destinataire à un fichier ou un script malveillant conçu pour permettre aux attaquants d'accéder à votre appareil afin de le contrôler ou de recueillir des informations, d'installer des scripts/fichiers malveillants ou d'extraire des données comme que des informations bancaire.

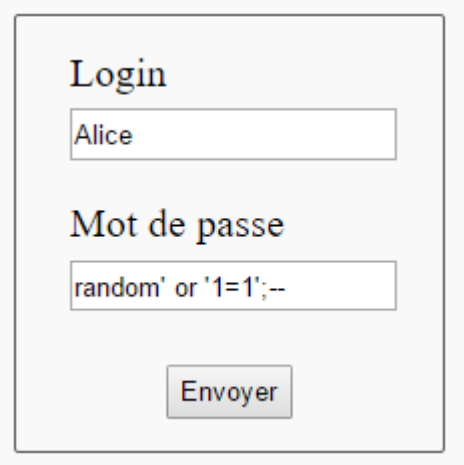


Dans l'exemple ci-dessous, une fausse notification SharePoint est générée depuis un compte Microsoft 365 corrompu qui envoie une notification par message.
Source : [Anatomie d'un email de phishing (vadesecure.com)]

PARTIE 1

Injections SQL :

Il s'agit d'un pirate qui insère un code malveillant dans un serveur en utilisant le langage de requête du serveur (SQL) pour pousser le serveur à fournir des données protégées. Ce type d'attaque consiste généralement à soumettre un code malveillant dans un commentaire ou un champ de recherche non protégé d'un site web. Des pratiques de codage sécurisées, telles que l'utilisation d'instructions préparées avec des requêtes paramétrées, constituent un moyen efficace de prévenir les injections SQL.



Ici, on injecte du SQL dans le formulaire de saisie du mot de passe. En effet, on tape n'importe quelle mot de passe associé à Alice (vu qu'on ne le connait pas), puis on ajoute : or '1==1';--.

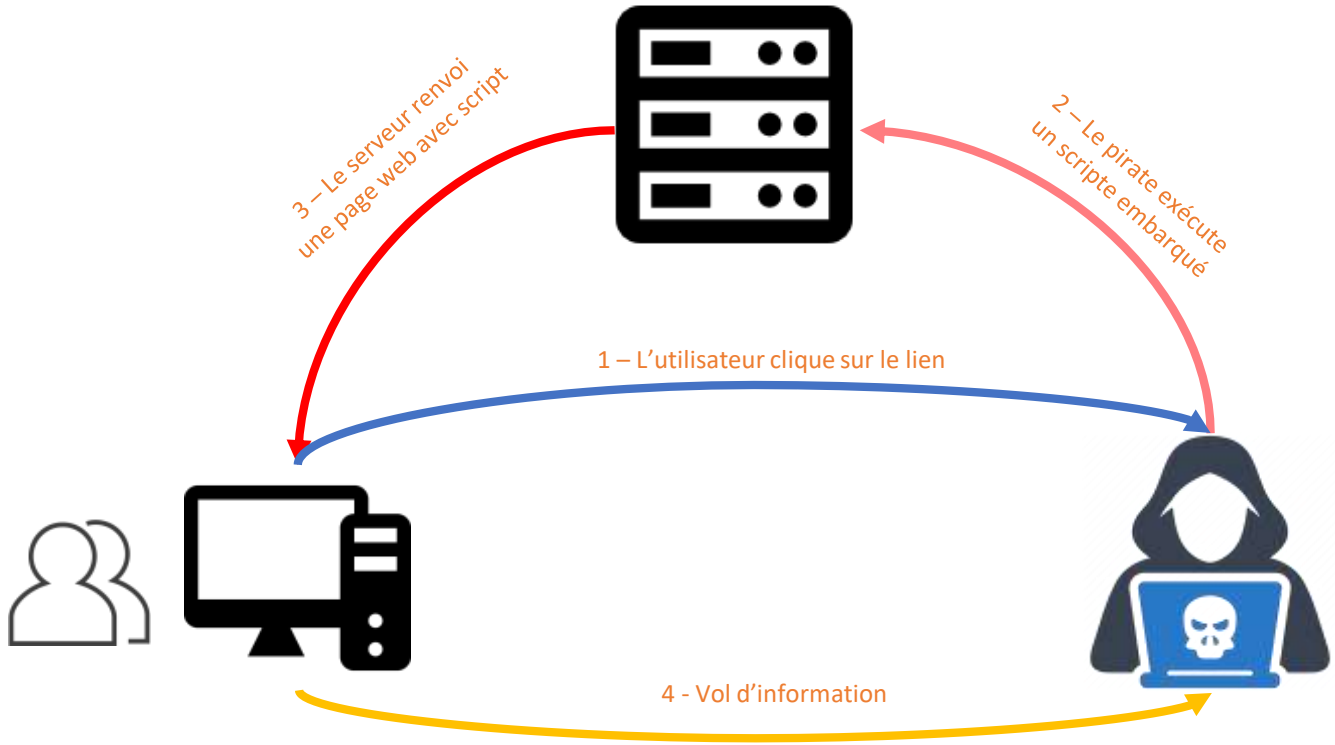
```
<source style="border: 1px dashed #2f6fab;background-color: #f9f9f9;font-size: 127%;padding: 1em;" lang="sql"> SELECT * FROM Users WHERE name='Alice' AND password = 'random' or '1=1';--'; </source>
```

PARTIE 1

Cross-site Scripting (XSS) :

Une attaque par cross-site scripting envoie des scripts malveillants dans le contenu de sites web fiables. Le code malveillant se joint au contenu dynamique qui est envoyé au navigateur de la victime. Généralement, ce code malveillant consiste en un code Javascript exécuté par le navigateur de la victime, mais il peut inclure du Flash, du HTML et du XSS.

Exemple d'une attaque XSS par réflexion (reflected XSS). Elle s'appuie sur le fait que l'application Web affiche ce que l'utilisateur vient de saisir dans un formulaire dans une page de résultat. Le navigateur de la victime exécute alors le code frauduleux généré dans la page de résultat. Tous les champs de formulaire sont donc une faille de sécurité potentielle que l'attaquant peut exploiter par XSS.



PARTIE 1

Rootkits

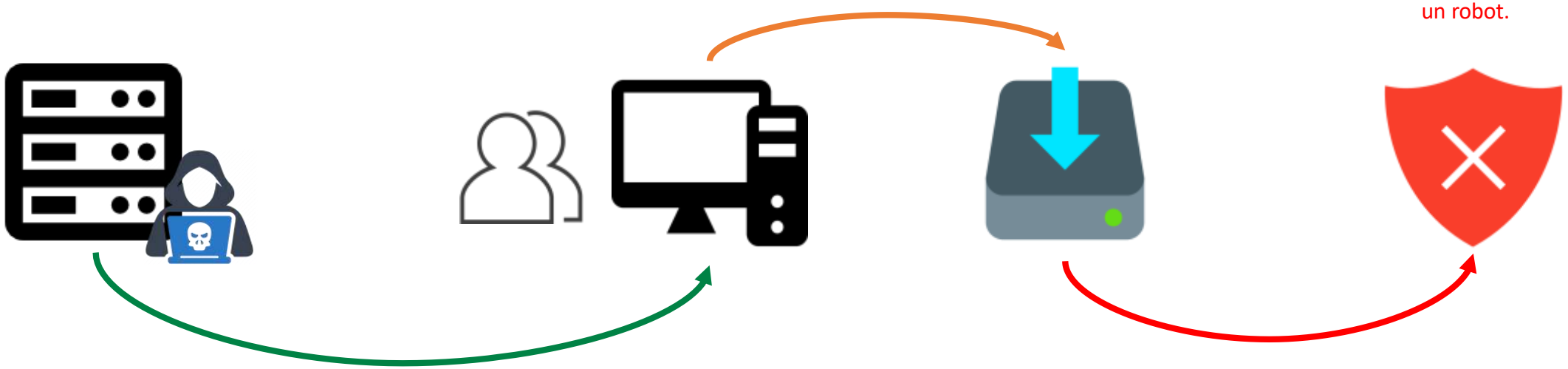
Les rootkits sont installés à l'intérieur d'un logiciel légitime, où ils peuvent obtenir le contrôle à distance et l'accès au niveau de l'administration d'un système. L'attaquant utilise ensuite le rootkit pour voler des mots de passe, des clés, des informations d'identification et récupérer des données critiques.

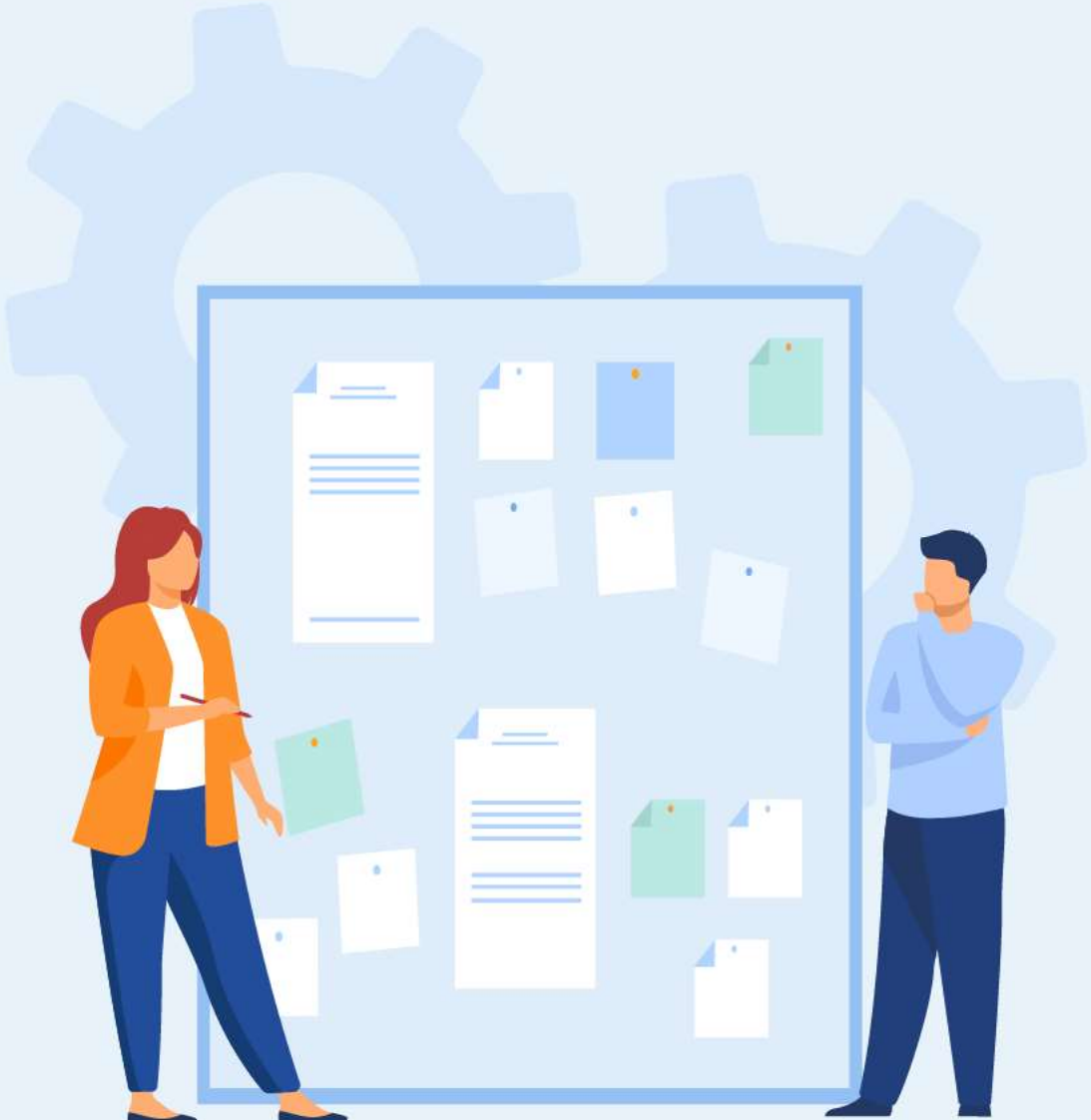
Une série de scripts PHP infectés sont conservés sur le site Web de l'attaquant.

La machine de la victime est infectée en visitant le site web.

Le malware obtient les privilèges et s'installe dans le système.

Le malware désactive les services de sécurité et transforme le système en un robot.





CHAPITRE 1

Introduire la notion de sécurité

1. La notion de sécurité informatique
2. Les types de failles et attaques
3. **Les types de virus**
4. La notion de Copyright

Qu'est-ce qu'un virus informatique ?

Un virus informatique est un morceau de code intégré dans un programme légitime et il est créé avec la capacité de s'auto-répliquer en infectant d'autres programmes sur un ordinateur. Tout comme la façon dont les humains attrapent un rhume ou une grippe, il peut rester en sommeil à l'intérieur du système et s'activer lorsque vous vous y attendez le moins. Il peut s'agir de pièces jointes à des e-mails, de téléchargements de fichiers, d'installations de logiciels ou de liens non sécurisés.


Messages / Chats


Emails

Site Web

Sources possibles infection initiale

Clé USB Infectée


Un Ordinateur infecté

Sources possibles infection initiale

Les virus informatiques peuvent infecter votre ordinateur de différentes manières. Mais certaines sont plus répandues que d'autres. L'illustration ci-dessus présente les moyens les plus courants par lesquels les virus s'introduisent dans un appareil.

PARTIE 1

Types courants de virus informatiques

Les cybercriminels, ou pirates, volent de mieux en mieux nos données confidentielles et les virus qui se créent évoluent rapidement. Il existe des millions de virus dans le monde, mais voici quelques types les courants :

Virus infectant les fichiers

- Virus qui s'attache à un programme exécutable. Il est également appelé virus parasite qui infecte généralement les fichiers avec les extensions .exe ou .com. Certains infecteurs de fichiers peuvent écraser les fichiers hôtes et d'autres peuvent endommager le formatage de votre disque dur.

Macro-virus

- Ce type de virus se trouve généralement dans des programmes tels que Microsoft Word ou Excel. Ces virus sont généralement stockés dans le cadre d'un document et peuvent se propager lorsque les fichiers sont transmis à d'autres ordinateurs, souvent par le biais de pièces jointes.

Pirate de navigateur

- Ce virus cible et modifie les paramètres de votre navigateur. **Il est souvent appelé virus de redirection de navigateur** car il redirige votre navigateur vers d'autres sites Web malveillants que vous n'avez pas l'intention de visiter. Ce virus peut poser d'autres menaces telles que la modification de la page d'accueil par défaut de votre navigateur.

Virus du secteur de démarrage

- Ces virus sont autrefois courants lorsque les ordinateurs sont démarrés à partir de disquettes. Aujourd'hui, ces virus se retrouvent distribués sous forme de supports physiques tels que les disques durs externes ou USB. Si l'ordinateur est infecté par un virus de secteur d'amorçage, il se charge automatiquement dans la mémoire permettant le contrôle de votre ordinateur.

Virus polymorphe

- Un virus polymorphe est un morceau de code caractérisé par le comportement suivant – cryptage, auto-multiplication et modification d'un ou plusieurs composants de lui-même afin qu'il reste insaisissable. Il est conçu pour éviter la détection car il est capable de créer des copies modifiées de lui-même.

Virus résident

- Un virus résident se stocke dans la mémoire de votre ordinateur, ce qui lui permet d'infecter des fichiers sur votre ordinateur. Ce virus peut interférer avec votre système d'exploitation, entraînant la corruption de fichiers et de programmes.

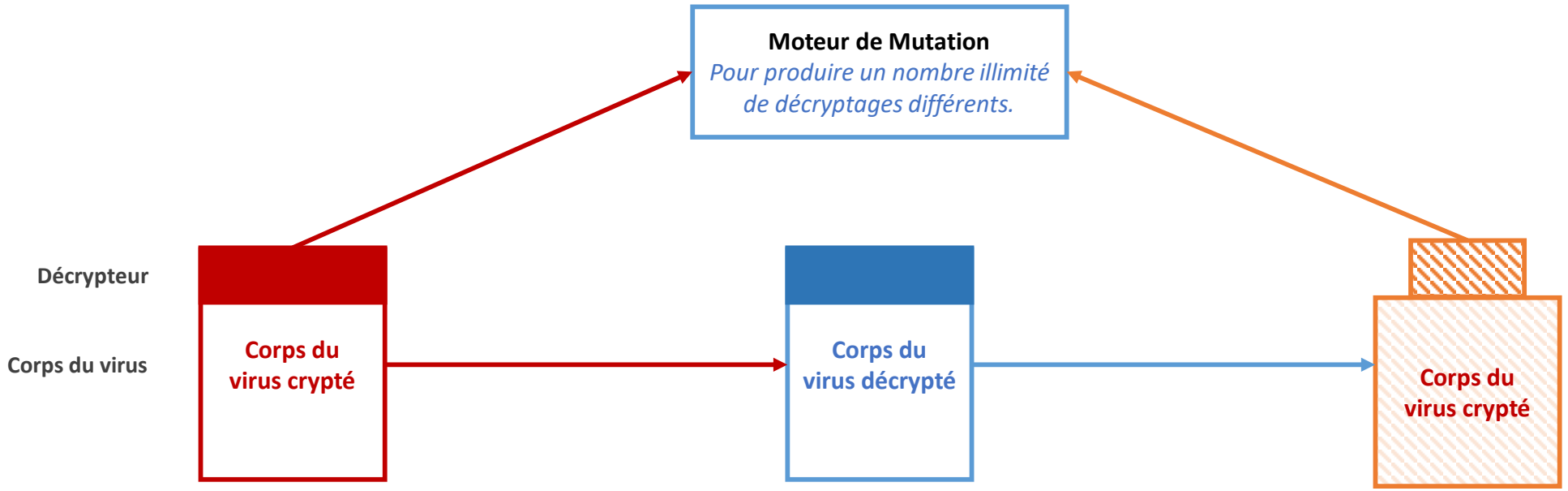
Virus multipartite

- Un virus multipartite est un type de logiciel malveillant à action rapide qui attaque simultanément le secteur d'amorçage et les fichiers exécutables d'un appareil. Les virus multipartites sont souvent considérés comme plus problématiques que les virus informatiques traditionnels en raison de leur capacité à se propager de plusieurs manières.

Pirate de navigateur

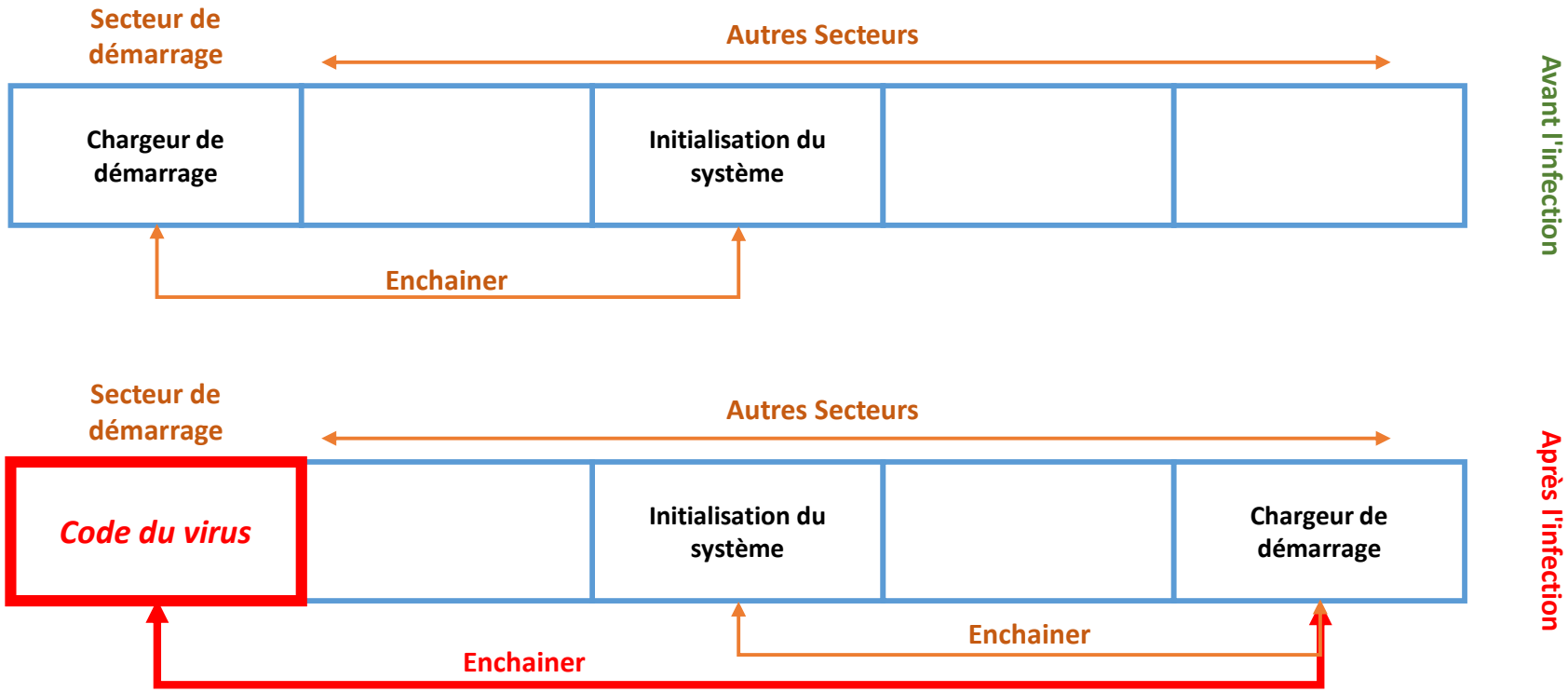
- Ce virus cible et modifie les paramètres de votre navigateur. **Il est souvent appelé virus de redirection de navigateur** car il redirige votre navigateur vers d'autres sites Web malveillants que vous n'avez pas l'intention de visiter. Ce virus peut poser d'autres menaces telles que la modification de la page d'accueil par défaut de votre navigateur.

Exemple : virus polymorphe



Comme nous pouvons le voir ci-dessus, les logiciels malveillants polymorphes modifient constamment leurs caractéristiques identifiables afin d'échapper à la détection. De nombreuses formes courantes de logiciels malveillants peuvent être polymorphes, notamment les virus, les vers, les robots, les chevaux de Troie ou les keyloggers.

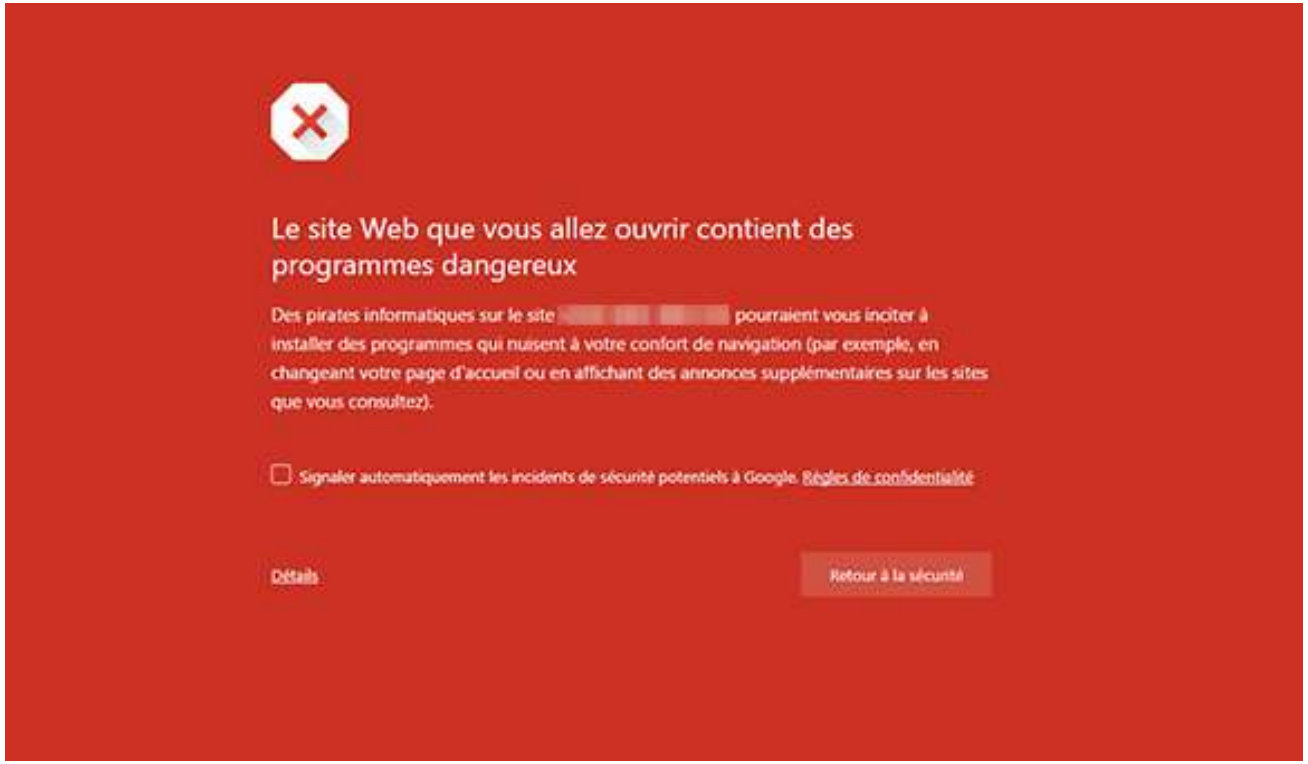
Exemple : virus de secteur de démarrage



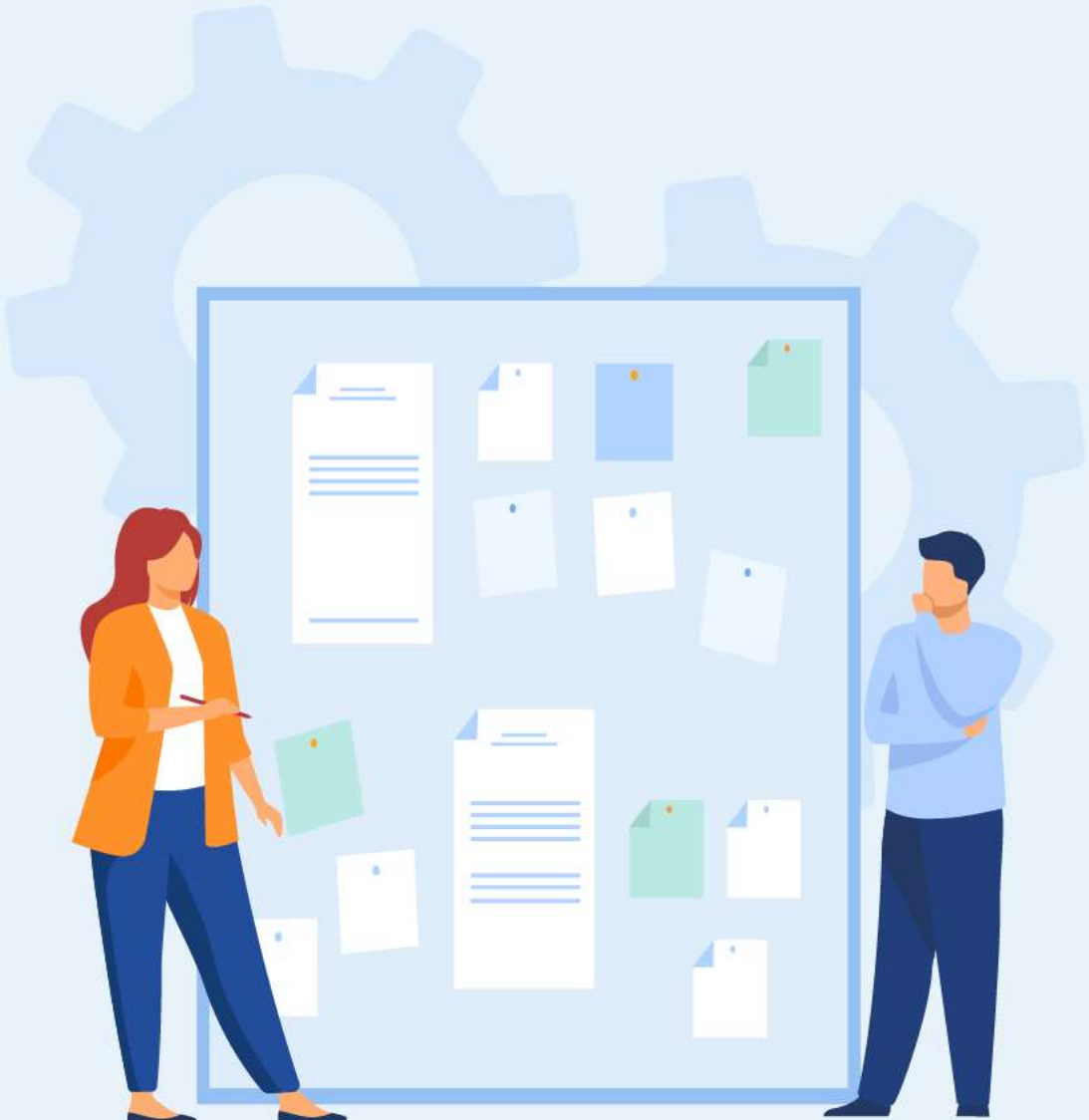
Ce virus infecte le secteur du MBR (Master Boot Record) du périphérique de stockage. Tout support, qu'il soit amorçable ou non, peut déclencher ce virus. Ces virus injectent leur code dans la table de partition du disque dur. Il s'introduit ensuite dans la mémoire principale lorsque l'ordinateur redémarre.

PARTIE 1

Exemple : pirate de navigateur



Cette information récoltée et affichée par le navigateur provient directement du moteur Google. Cette situation est le résultat de fichiers infectés par un virus, trojan ou autre malware et qui se trouve sur votre site web.



CHAPITRE 1

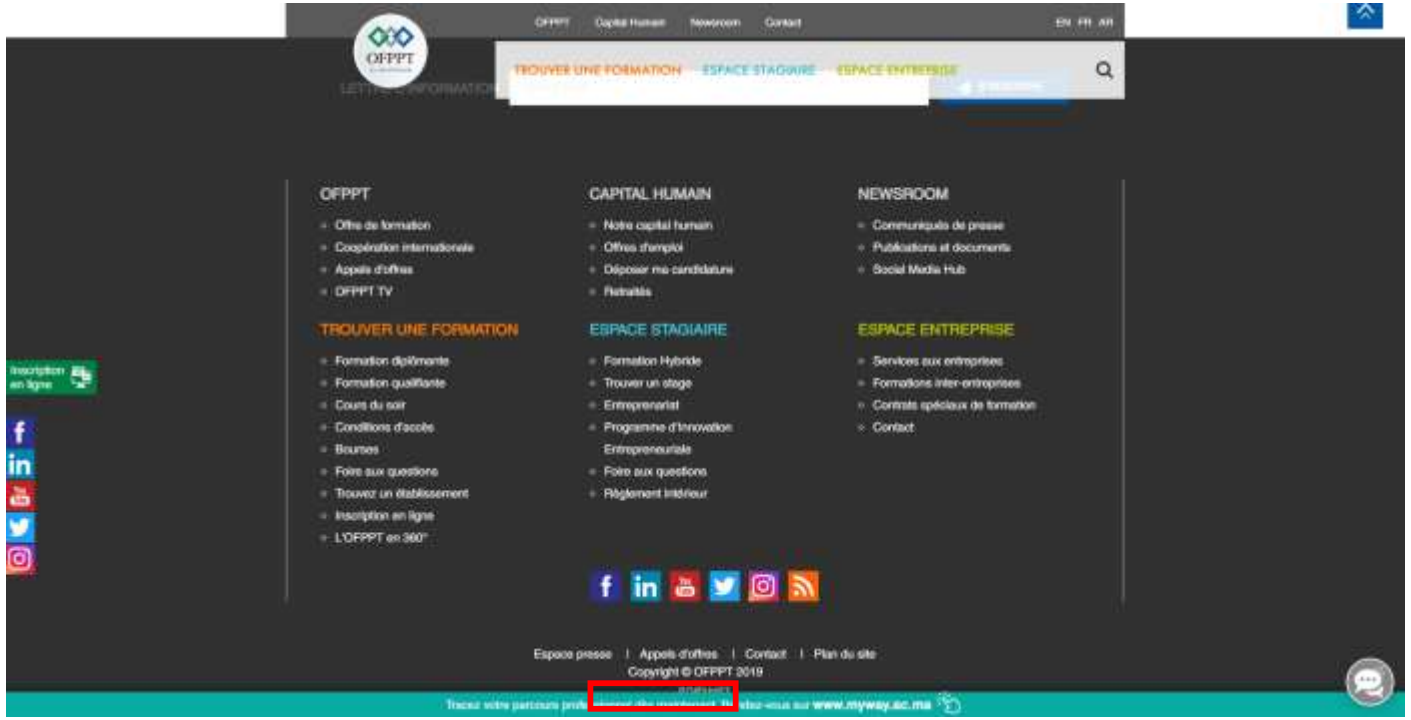
Introduire la notion de sécurité

1. La notion de sécurité informatique
2. Les types de failles et attaques
3. Les types de virus
4. **La notion de Copyright**

PARTIE 1

C’est quoi le Copyright

Le droit d'auteur **(Copyright)** est un terme juridique décrivant la propriété du contrôle des droits d'utilisation et de distribution de certaines œuvres d'expression créative, notamment les livres, les vidéos, les films cinématographiques, les compositions musicales et les programmes informatiques.

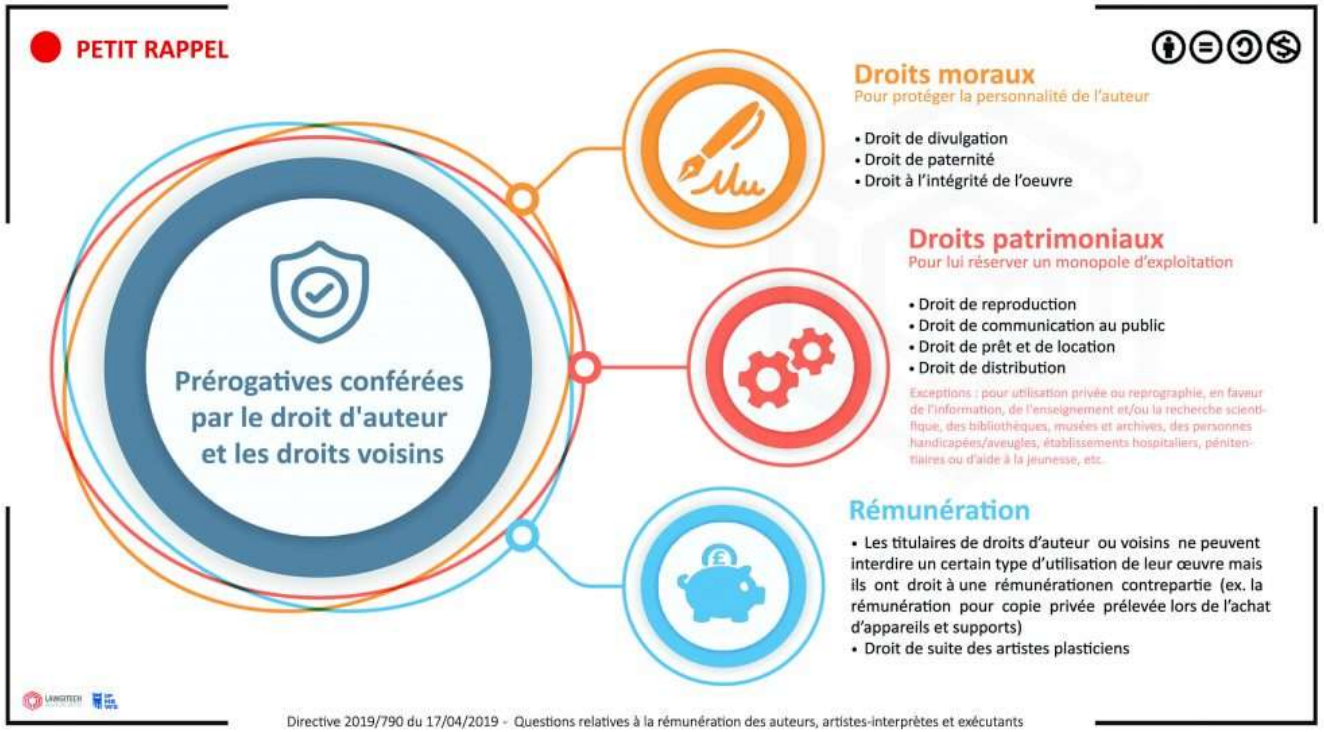


Sur le site de l'OFPPT, le copyright est déclaré en bas de page, ce qui signifie que tout le contenu de ce site est la propriété de l'OFPPT.

Le symbole du droit d'auteur consiste en une lettre "c" dans un cercle, suivie du nom du titulaire du droit d'auteur et de l'année de la première publication de l'œuvre. Par exemple, le symbole du droit d'auteur, suivi de Jane Doe, virgule, 1999, indique que Jane Doe est l'auteur de l'œuvre qui a été publiée pour la première fois en 1999.

C’est quoi un titulaire du droit d'auteur ?

Le droit d'auteur appartient généralement au créateur de l'œuvre en premier lieu. Toutefois, la propriété du droit d'auteur dépend d'un certain nombre de facteurs, tels que le type d'œuvre créée ou la manière dont l'œuvre a été créée, par exemple par un employé dans le cadre de son travail. Déterminer qui est titulaire du droit d'auteur sur une œuvre peut être complexe.



Les titulaires de droits d’auteur disposent de divers types de droits l’égard de leurs œuvres. Il s’agit des droits patrimoniaux, des droits moraux et du droit à une rémunération dans certains cas.
https://lawgitech.eu/

PARTIE 1

Quelle est la durée de protection du droit d'auteur?

Après l'expiration du droit d'auteur d'une œuvre, celle-ci tombe dans le domaine public et peut être utilisée gratuitement et sans restriction. La durée initiale du droit d'auteur était fixée à **14 ans**, avec possibilité de **renouvellement pour 14 ans** supplémentaires. Ce terme a été **doublé en 1831** à **28 ans** plus un **renouvellement de 28 ans**.

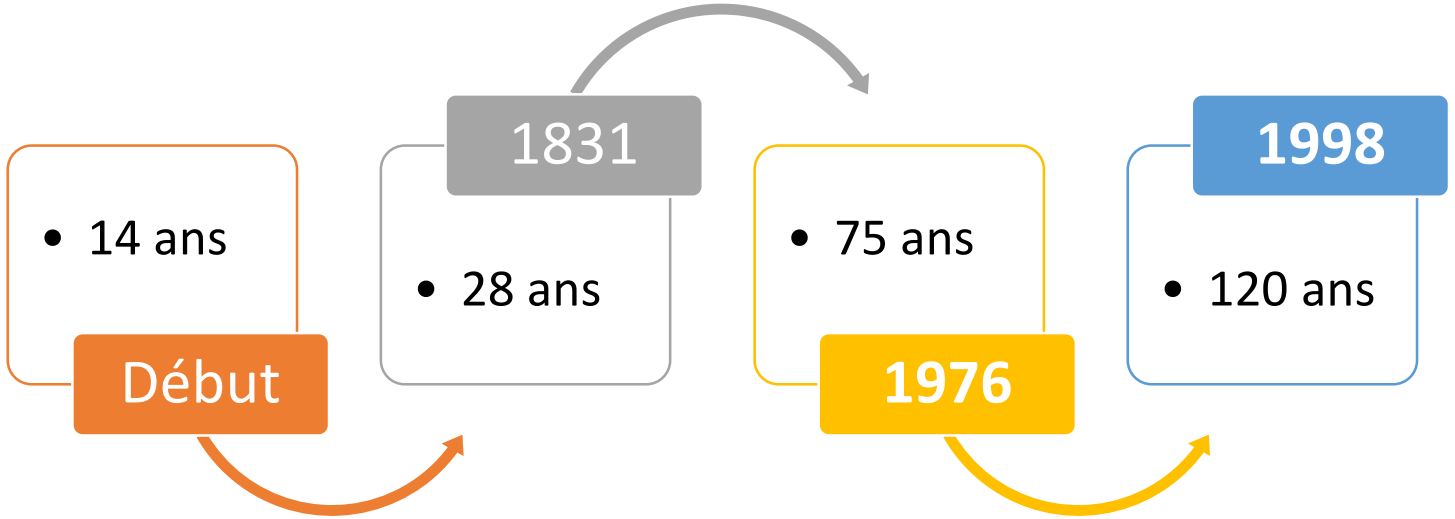
, notamment:

- **la loi sur le droit d'auteur de 1976**, qui a étendu la protection du droit d'auteur à 75 ans ou la vie de l'auteur plus 50 ans ;
- **Copyright Term Extension Act de 1998**, également appelé **Mickey Mouse Protection Act**, qui a prolongé la durée à 120 ans ou la vie de l'auteur plus 70 ans.

Disney Corp., par exemple, est connu comme le groupe le puissant qui bénéficient de durées de protection du droit d'auteur plus longues. Disney a joué un rôle moteur dans l'extension de la protection du droit d'auteur aux États-Unis pour sa souris emblématique et a pris en charge les modifications des conditions de droit d'auteur aux États-Unis

PARTIE 1

Quelle est la durée de protection du droit d'auteur?

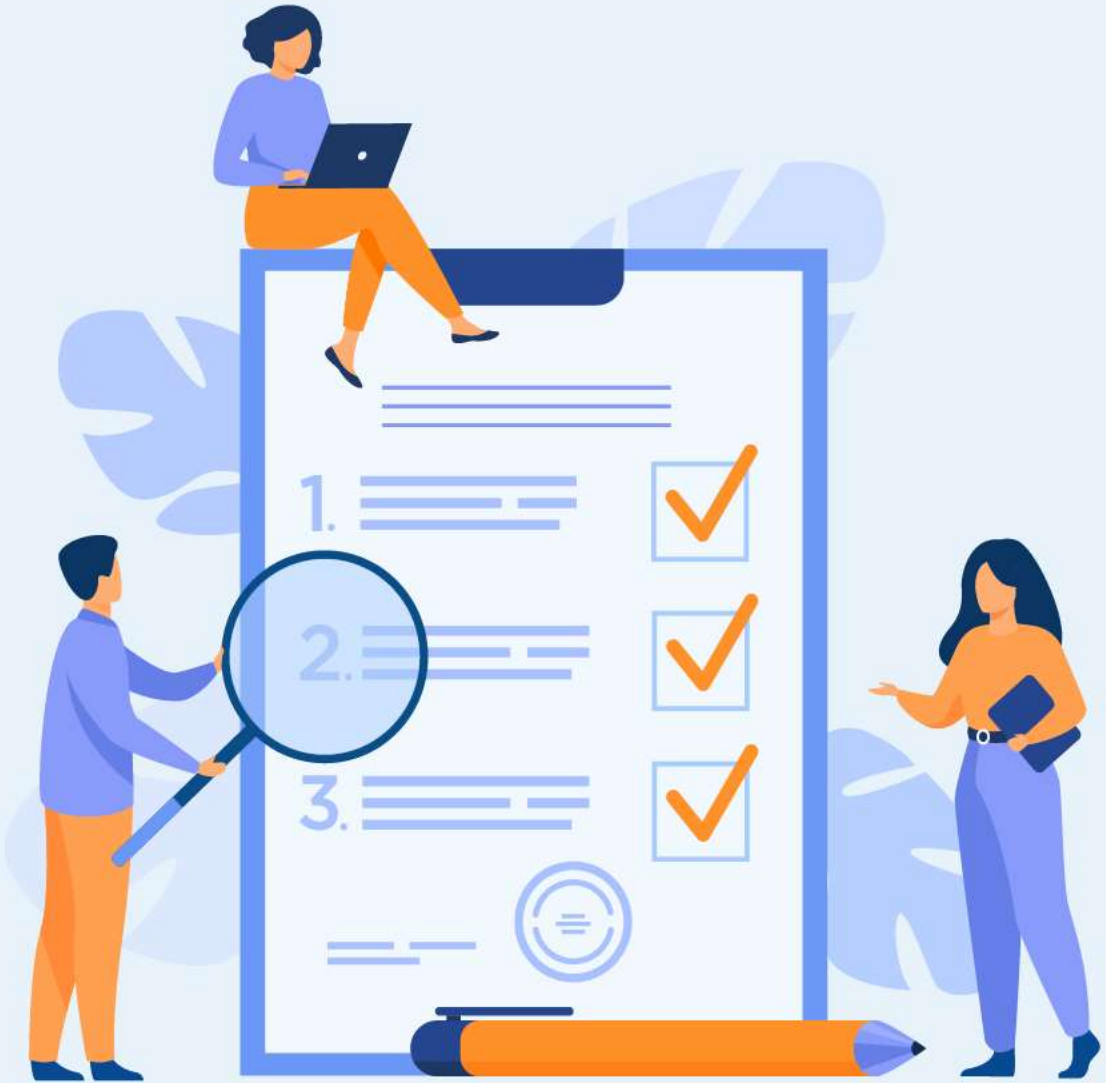


Une ligne du temps montrant la durée du droit d'auteur au fil des ans.

Information

Le Bureau Marocain du Droit d'Auteur est un organisme de gestion collective, créé par Décret N° 2.64.406 du 5 kaada 1384 (8 mars 1965) « est seul chargé de percevoir et de répartir les droits d'auteur sous toutes leurs formes existantes et à venir ». (https://bmda.ma/)

PARTIE 1



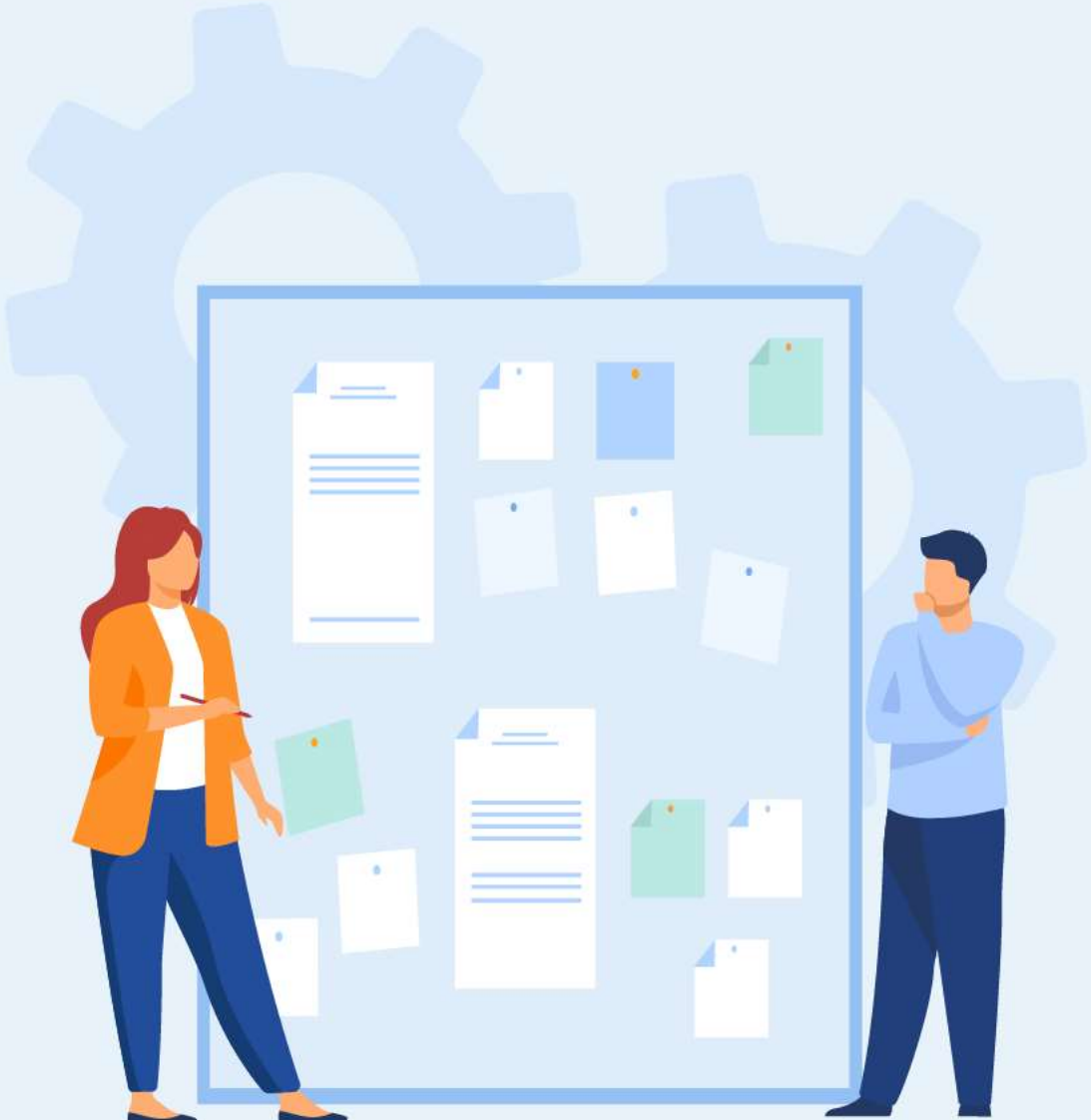
CHAPITRE 2

Comprendre les types d’attaques des systèmes informatiques

Ce que vous allez apprendre dans ce chapitre :

- Vulnérabilités des applications Web
- Attaques " Cross Site Scripting " ou XSS
- Attaques sur les sessions (cookie poisonning, session hijacking, ...).
- Exploitation de vulnérabilités sur le frontal HTTP (ver Nimda, faille Unicode, ...)
- Attaques sur les configurations standards (Default Password, Directory Transversal, ...)
- Attaques d’hameçonnage (fishing)
- Attaques DDOS

05 heures



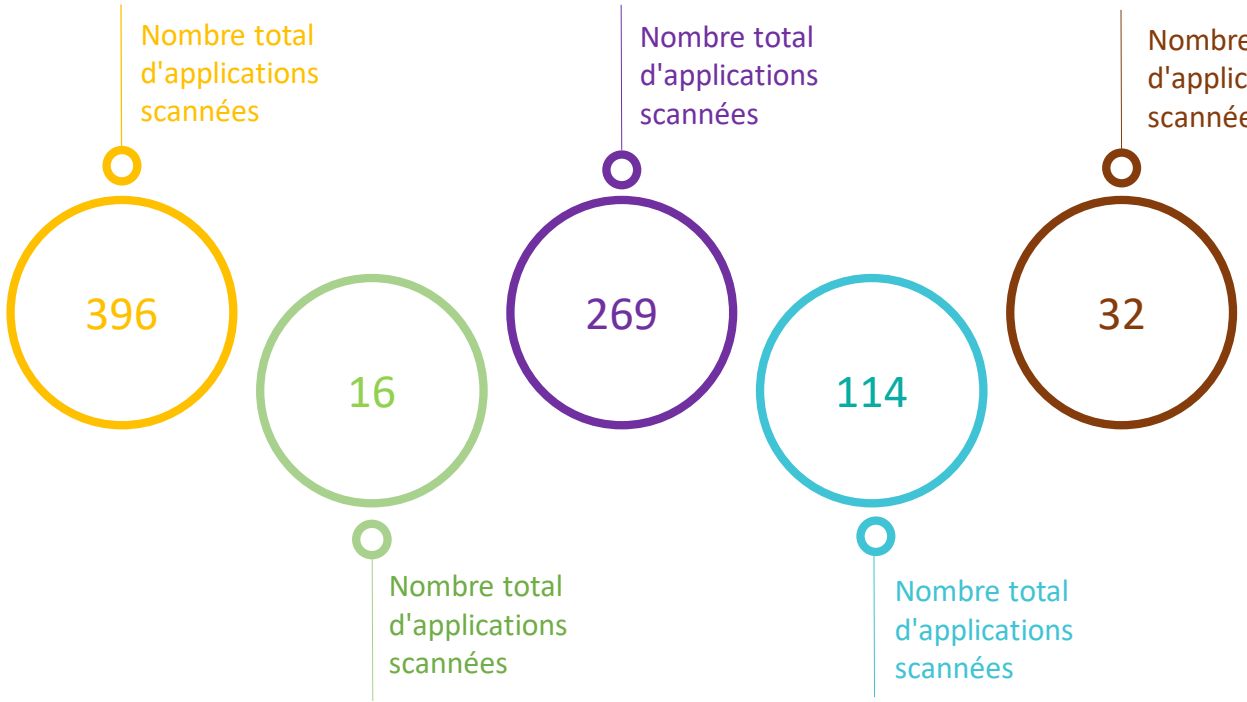
CHAPITRE 2

Comprendre les types d’attaques des systèmes informatiques

1. **Vulnérabilités des applications Web**
2. Attaques " Cross Site Scripting " ou XSS
3. Attaques sur les sessions (cookie poisonning, session hijacking, ...).
4. Exploitation de vulnérabilités sur le frontal HTTP (ver Nimda, faille Unicode, ...)
5. Attaques sur les configurations standards (Default Password, Directory Transversal, ...)
6. Attaques d’hameçonnage (fishing)
7. Attaques DDOS

C'est quoi la vulnérabilité d'une application Web?

La vulnérabilité d'un site web est une faiblesse ou une mauvaise configuration du code d'un site web ou d'une application web qui permet à un attaquant d'obtenir un certain niveau de contrôle du site, et éventuellement du serveur d'hébergement. La plupart des vulnérabilités sont exploitées par des moyens automatisés, tels que les scanners de vulnérabilité et les botnets.



*Selon le site web d'Acunetix, sur les **269** vulnérabilités, un scanner spécifique a détecté les scanners de vulnérabilités web identifiés :*

***180** étaient des vulnérabilités de type Cross-site Scripting. Celles-ci incluent le XSS réfléchi, stocké, DOM Based et XSS via RFI.*
***55** étaient des vulnérabilités par injection SQL. Celles-ci incluent également les injections SQL booléennes et aveugles (basées sur le temps).*
***16** vulnérabilités d'inclusion de fichiers, y compris les inclusions de fichiers locaux et distants.*

PARTIE 1

C'est quoi le OWASP?

L'Open Web Application Security Project (OWASP) est une **fondation à but non lucratif** dédiée à l'amélioration de **la sécurité des logiciels**. L'OWASP fonctionne selon un modèle de « **communauté ouverte** », où tout le monde peut participer et contribuer à des projets, des événements, des discussions en ligne, etc.

C'est un référentiel de tout ce qui concerne **la sécurité des applications Web**, soutenu par les connaissances et l'expérience approfondies de ses contributeurs de la communauté ouverte.

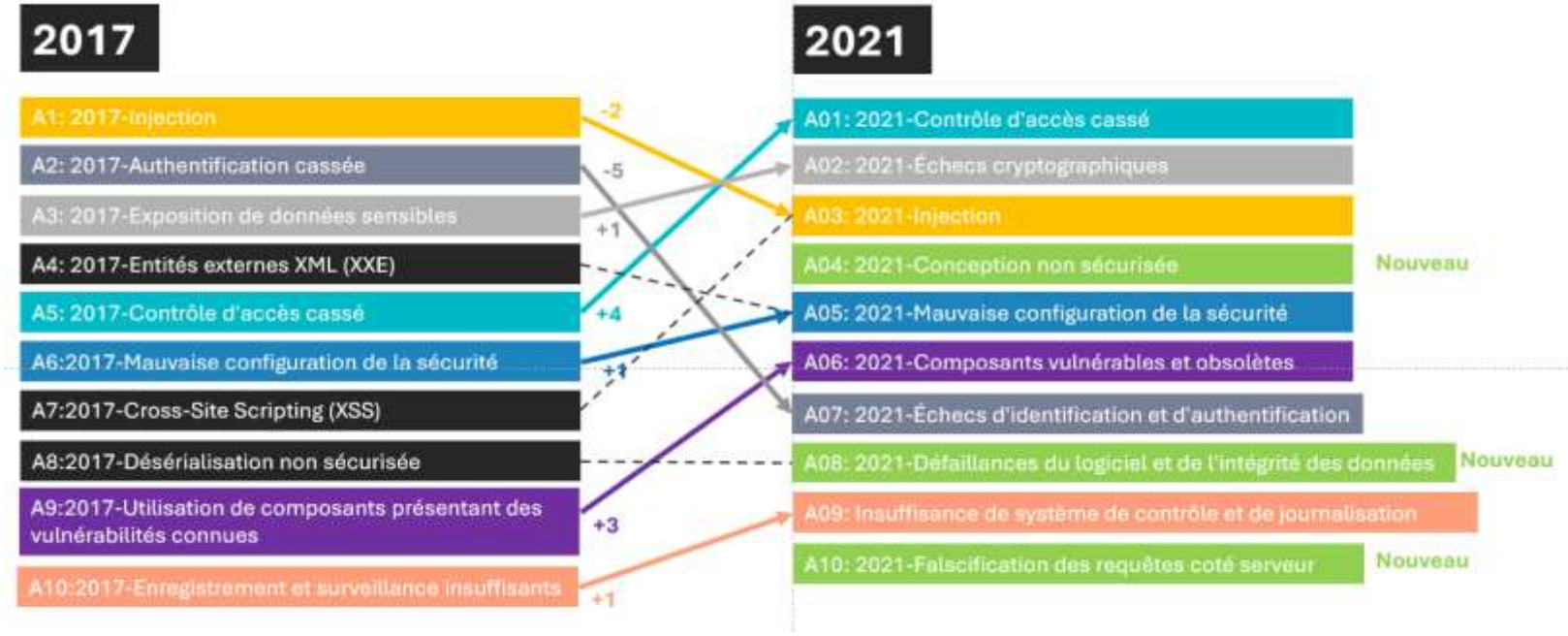
OWASP Top 10 se définit comme un document de sensibilisation standard pour les développeurs et la sécurité des applications Web. Il présente chaque année (après analyse) les top 10 vulnérabilités apps web et mobile les plus critique.

OWASP Top 10 2021 (ce qui a changé) (linkedin.com)

PARTIE 1

Qu'est-ce que le Top 10 de l'OWASP?

OWASP (Open **W**eb **A**pplication **S**ecurity **P**roject) **Top 10** est un **document en ligne** sur le site Web de l'OWASP qui fournit un **classement et des conseils de correction pour les 10 risques de sécurité** des applications Web les plus critiques. **L'objectif du rapport** est d'offrir aux développeurs et aux professionnels de la sécurité **un aperçu des risques les plus répandus** afin qu'ils puissent intégrer les conclusions et les recommandations dans leurs guides de sécurité.



La version la plus récente a été publiée en 2021 et comprenait des modifications importantes par rapport à la version 2017, comme le montre la figure à droite.

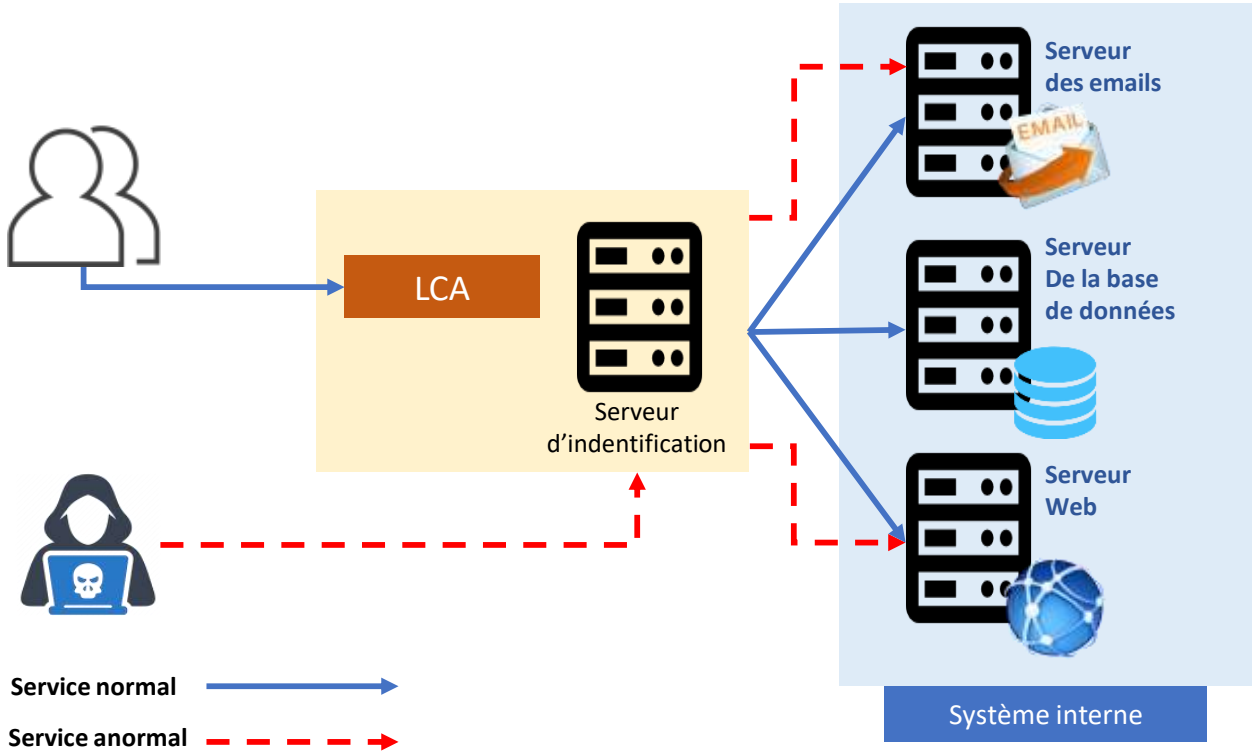
PARTIE 1

Quelles sont les dernières catégories du Top 10 OWASP ?

Contrôles d'accès défaillants

Le contrôle d'accès applique une stratégie telle que les utilisateurs ne peuvent pas agir en dehors de leurs autorisations prévues. Les défaillances entraînent généralement la divulgation, la modification ou la destruction d'informations non autorisées de toutes les données ou l'exécution d'une fonctionnalité métier en dehors des limites de l'utilisateur.

Il est essentiel d'utiliser des **tests d'intrusion** afin de détecter les contrôles d'accès involontaires. **Des modifications de l'architecture** et de la conception peuvent être mis en place pour créer des barrières d'accès aux données.



Pour qu'un problème de contrôle d'accès ne se pose pas, il faut d'abord qu'il y ait un contrôle d'accès et qu'il soit bien mis en œuvre.

PARTIE 1

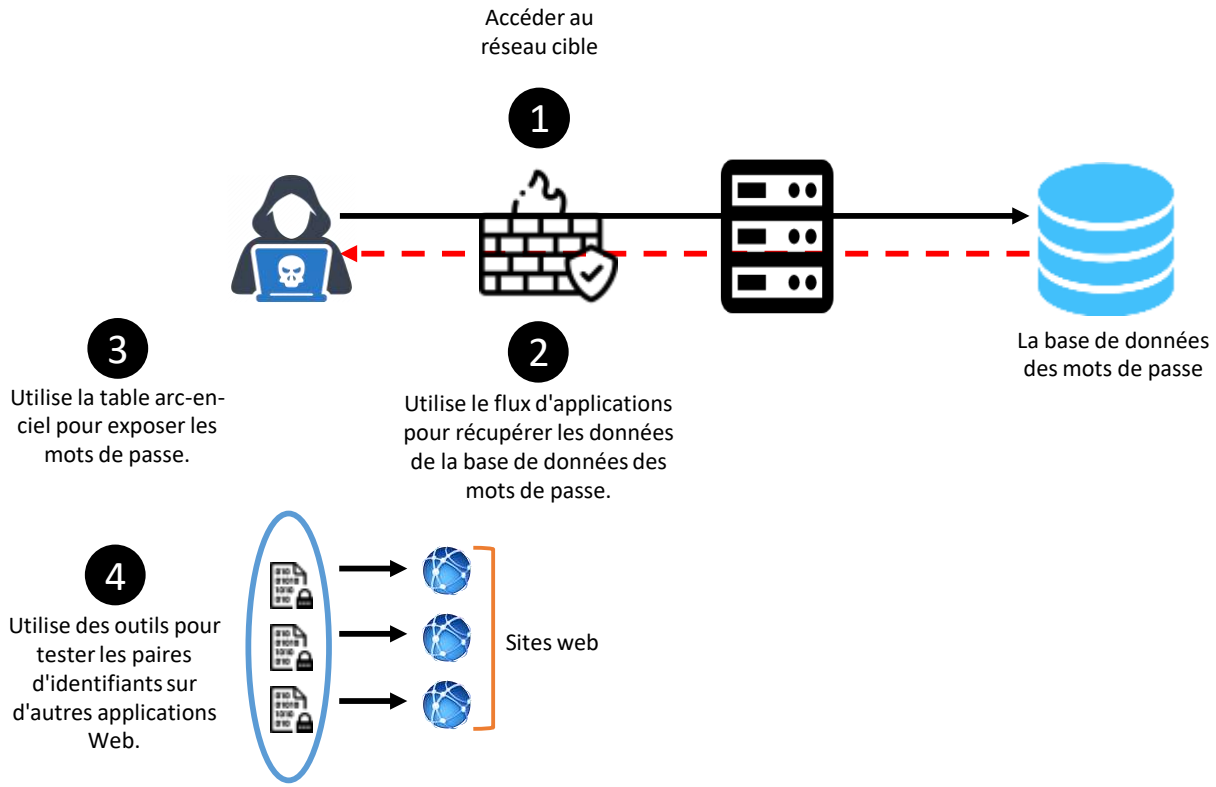
Quelles sont les dernières catégories du Top 10 OWASP ?

Défaillances cryptographiques

Les attaquants ciblent souvent les données sensibles, telles que les mots de passe, les numéros de carte de crédit et les informations personnelles, lorsque vous ne les protégez pas correctement. Les défaillances cryptographiques sont à l'origine de l'exposition des données sensibles.

Une faille cryptographique peut se produire lorsque vous faites ce qui suit :

- Stocker ou faire transiter des données en texte clair (le plus courant).
- Protéger les données avec un cryptage ancien ou faible
- Filtrer ou masquer de manière inadéquate les données en transit

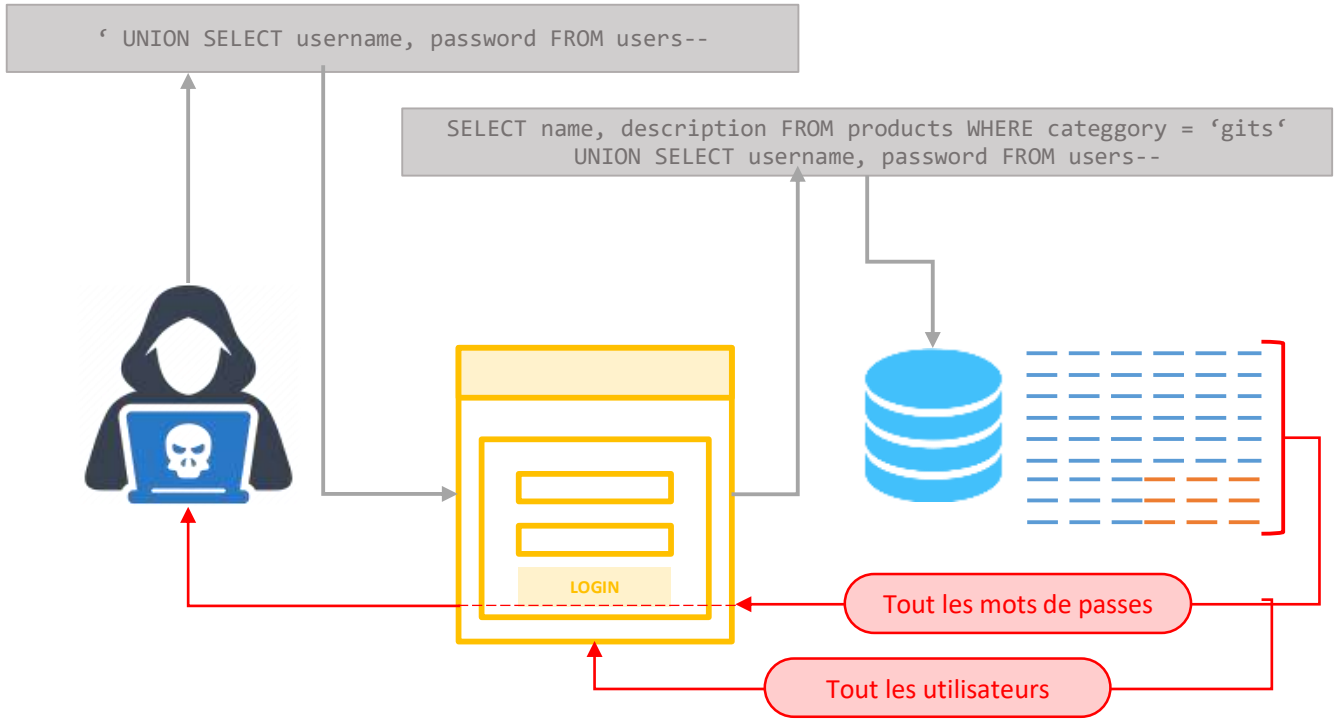


Cryptographic failures attack scenario

Quelles sont les dernières catégories du Top 10 OWASP ?

injection SQL

L'injection SQL est une vulnérabilité de sécurité web qui permet à un attaquant d'interférer avec les requêtes qu'une application effectue dans sa base de données. Elle permet généralement à un attaquant de visualiser des données qu'il n'est normalement pas en mesure de récupérer. Il peut s'agir de données appartenant à d'autres utilisateurs, ou de toute autre donnée à laquelle l'application elle-même peut accéder.



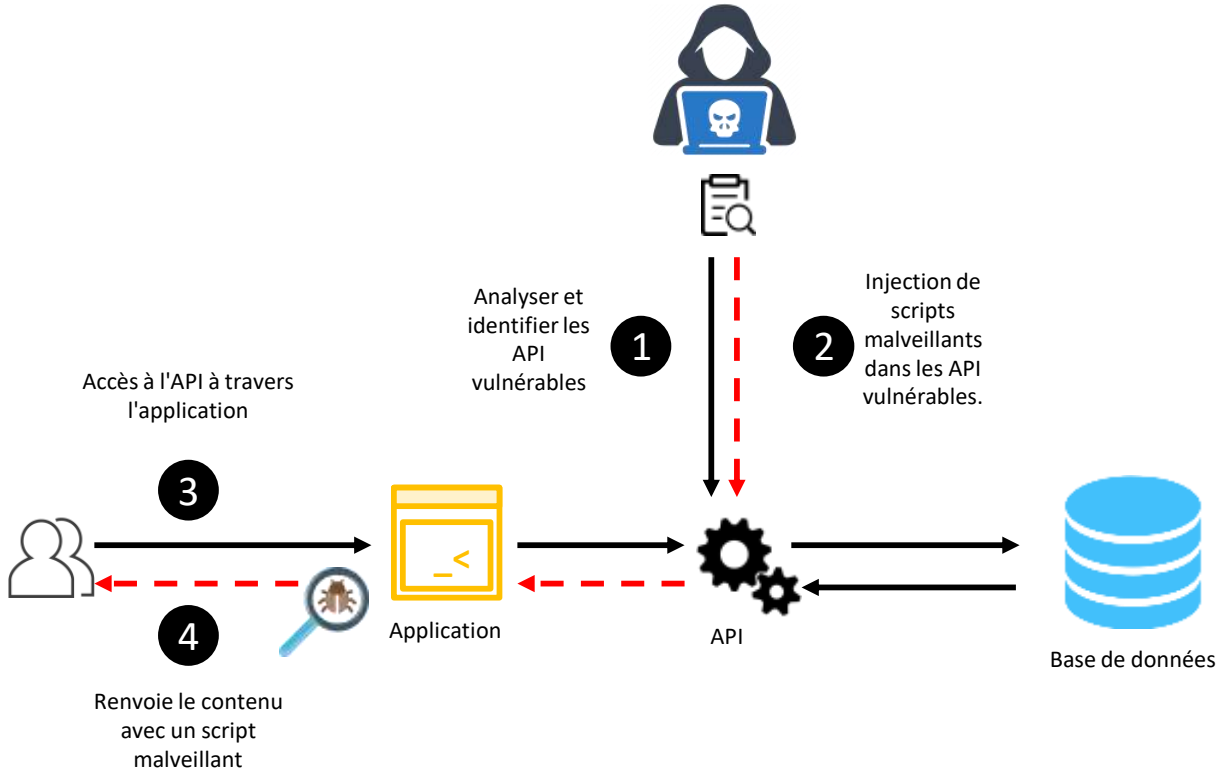
Un exemple comment un pirate peut insérer une requête SQL dans le formulaire de connexion pour récupérer tous les utilisateurs et leur mot de passe en joignant du code à la requête à travers le champ de connexion non sécurisé.

PARTIE 1

Quelles sont les dernières catégories du Top 10 OWASP ?

Conception non sécurisée

La conception non sécurisée est basée sur les risques associés aux défauts de conception et d'architecture. Elle se base sur la nécessité d'une modélisation des menaces, de modèles de conception sécurisés et de principes. Les défauts d'une conception non sécurisée ne peuvent pas être corrigés par une mise en œuvre.



Dans ce scénario d'attaque, l'attaquant exploite une API mal conçue qui ne filtre pas correctement les entrées.

PARTIE 1

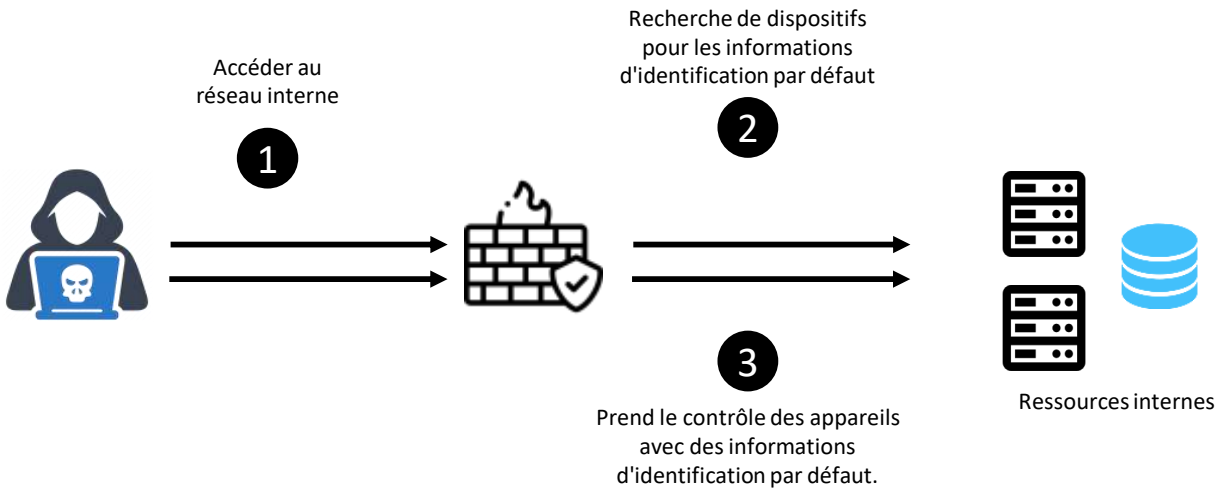
PARTIE 1

Quelles sont les dernières catégories du Top 10 OWASP ?

Conception non sécurisée

Les erreurs de configuration de sécurité se produisent lorsque des faiblesses de conception ou de configuration résultent d'une erreur ou d'un défaut de configuration.

Par exemple, si vous laissez le compte par défaut d'une application et son mot de passe d'origine activés, cela va rendre le système vulnérable à l'exploitation. Car, n'import qui peux essayer d'accéder au system en utilisant les configuration par default et notamment le nom d'utilisateur et le mot de passe par défaut.



Dans le scénario d'attaque suivant, l'attaquant exploite des périphériques réseau qui utilisent des informations d'identification par défaut.

1. *L'attaquant accède au réseau interne d'une organisation.*
2. *Il recherche les périphériques sur le réseau et effectue des vérifications par dictionnaire pour déterminer ceux qui utilisent des informations d'identification par défaut.*
3. *L'attaquant se connecte aux dispositifs vulnérables en utilisant les mots de passe par défaut et prend le contrôle.*

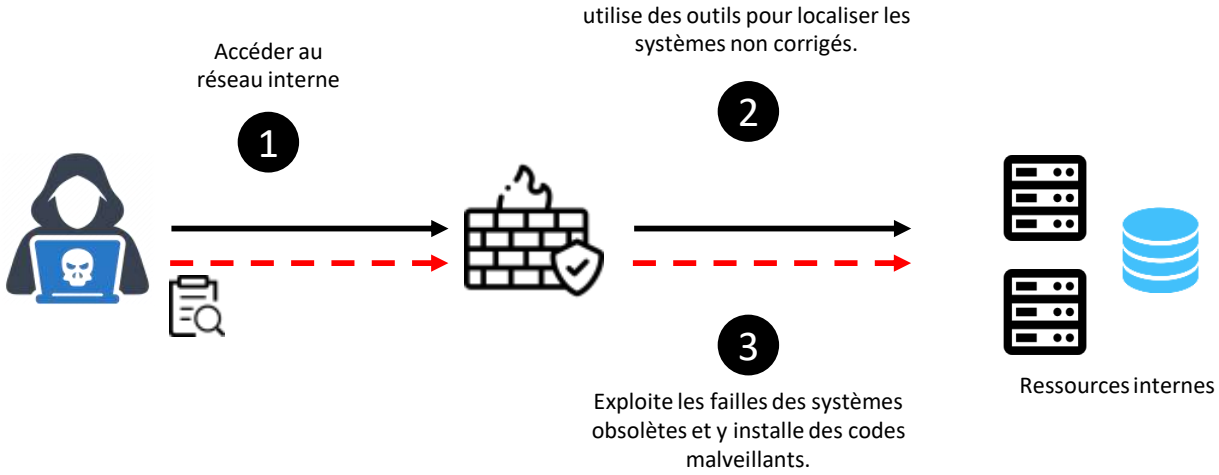
PARTIE 1

Quelles sont les dernières catégories du Top 10 OWASP ?

Composants vulnérables et obsolètes

Les vulnérabilités basées sur les composants se produisent lorsqu'un composant logiciel, comme un module ou un plugin par exemple, n'est pas pris en charge, n'est pas à jour ou est vulnérable à un exploit connu.

Vous pouvez utiliser par erreur des composants logiciels vulnérables dans des environnements de production, ce qui constitue une menace pour l'application Web.



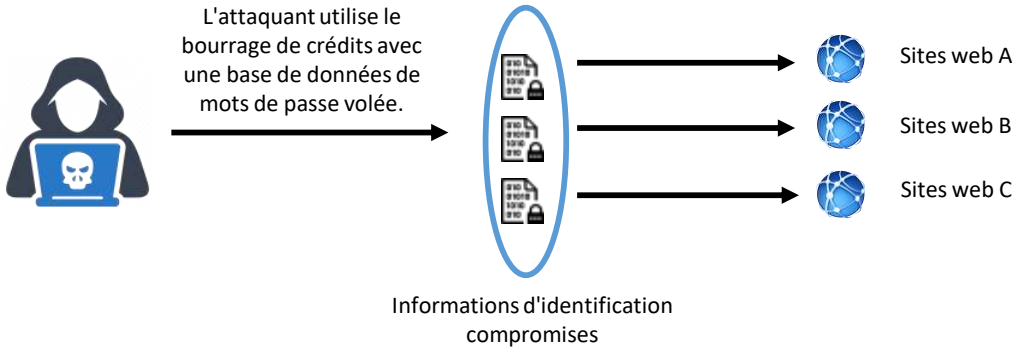
Dans le scénario suivant, l'attaquant exploite un système non corrigé pour exécuter un code malveillant sur le serveur.

1. *L'attaquant obtient l'accès au réseau interne d'une organisation.*
2. *Il utilise un outil d'analyse pour localiser les systèmes internes dont les composants ne sont pas corrigés ou sont périmés.*
3. *L'attaquant exploite une faille dans le composant obsolète qui lui permet d'installer un code malveillant sur le serveur d'applications.*

Quelles sont les dernières catégories du Top 10 OWASP ?

Échecs d'identification et d'authentification

Les échecs d'identification et d'authentification peuvent se produire lorsque les fonctions liées à l'identité d'un utilisateur, à l'authentification ou à la gestion des sessions ne sont pas mises en œuvre correctement ou ne sont pas protégées adéquatement par une application



Dans le scénario suivant, un attaquant effectue des attaques par bourrage d'identifiants contre une application qui ne met pas en œuvre de techniques de menace automatisées.

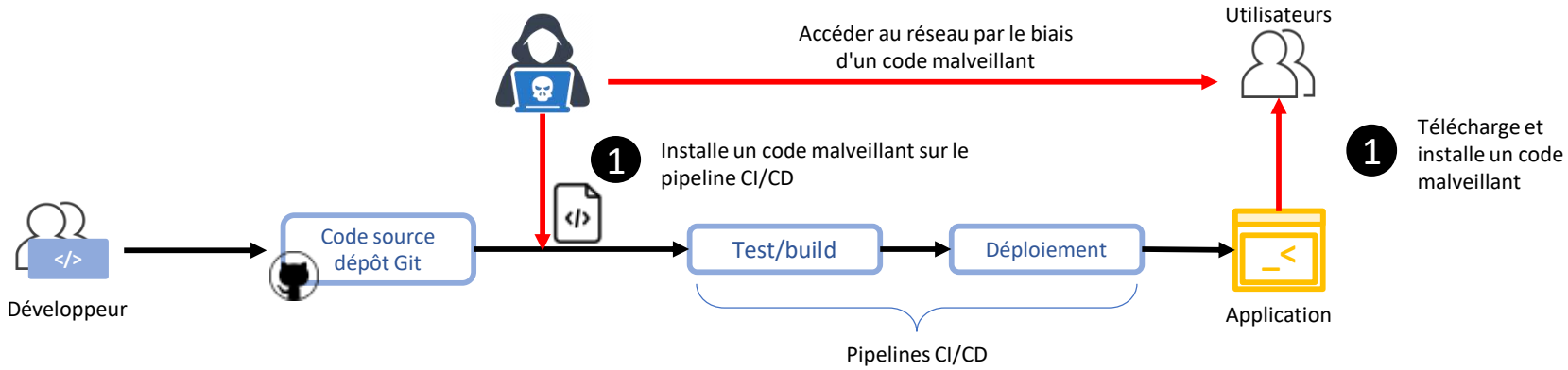
1. *L'attaquant obtient une base de données de mots de passe sur un forum de pirates.*
2. *Comme un algorithme de hachage faible a été utilisé pour chiffrer les mots de passe, l'attaquant peut exposer les informations d'identification des utilisateurs.*
3. *L'attaquant utilise des outils de bourrage d'informations d'identification pour tester les paires d'informations d'identification sur d'autres sites Web.*
4. *Si la connexion réussit, l'attaquant sait qu'il dispose d'un ensemble d'informations d'identification valides.*

PARTIE 1

Quelles sont les dernières catégories du Top 10 OWASP ?

Défaillances des logiciels et de l'intégrité des données

Les défaillances de l'intégrité des logiciels et des données concernent le code et l'infrastructure qui ne sont pas protégés contre les violations de l'intégrité. Cela peut se produire lorsque vous utilisez des logiciels provenant de sources et de dépôts non fiables ou même des logiciels qui ont été altérés à la source, en transit ou même dans le cache du point final.



Dans le scénario suivant, un attaquant exploite un pipeline CI/CD non sécurisé et installe un code malveillant qui sera distribué par le biais du processus de construction et de déploiement.

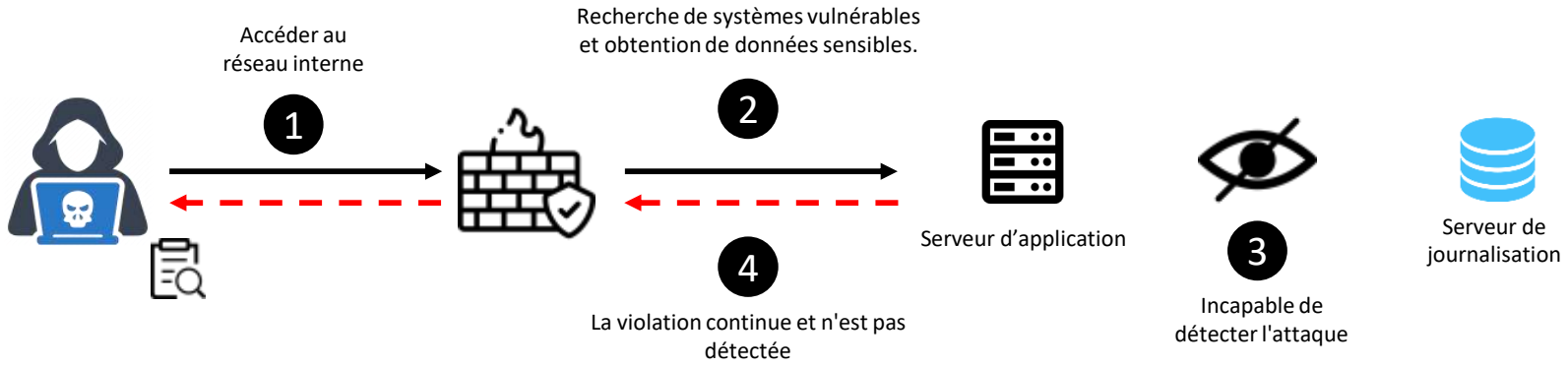
1. *L'attaquant identifie le pipeline CI/CD non sécurisé d'une organisation et installe un code malveillant qui est poussé en production.*
2. *Les clients téléchargent à leur insu le code malveillant depuis les serveurs de mise à jour de l'entreprise.*
3. *La mise à jour malveillante est installée dans l'environnement du client.*
4. *L'attaquant utilise le code malveillant pour accéder au réseau du client.*

PARTIE 1

Quelles sont les dernières catégories du Top 10 OWASP ?

Insuffisance de la journalisation et de la surveillance de la sécurité

Les Insuffisance de la journalisation et de la surveillance de la sécurité sont souvent un facteur dans les incidents de sécurité majeurs. Certains systèmes comprennent des fonctionnalités avancées de journalisation et de surveillance et offrent des fonctions de sécurité pour se protéger contre les attaques qui peuvent résulter d'une journalisation et d'une surveillance insuffisantes du système et des applications.



Dans le scénario suivant, un attaquant exploite une organisation qui n'utilise pas une journalisation et une surveillance adéquates.

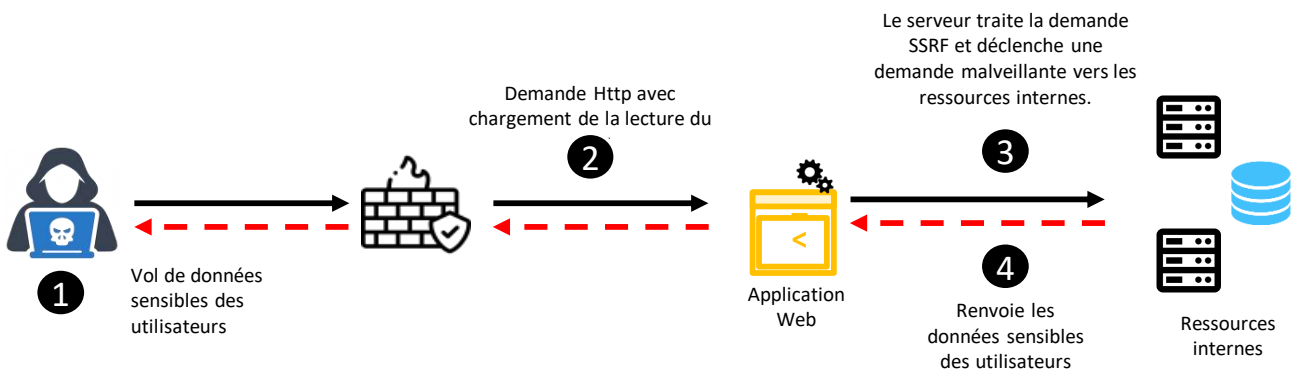
1. *Un attaquant accède au réseau interne d'une organisation.*
2. *L'attaquant exécute un outil d'analyse pour localiser les systèmes internes présentant des vulnérabilités connues et obtient des données sensibles.*
3. *Comme l'organisation ne suit pas les pratiques de journalisation et de surveillance adéquates, elle est incapable de détecter les attaques actives.*
4. *La violation des données passe inaperçue pendant des mois.*

PARTIE 1

Quelles sont les dernières catégories du Top 10 OWASP ?

Insuffisance de la journalisation et de la surveillance de la sécurité

Les Insuffisance de la journalisation et de la surveillance de la sécurité sont souvent un facteur dans les incidents de sécurité majeurs. Certains systèmes comprennent des fonctionnalités avancées de journalisation et de surveillance et offrent des fonctions de sécurité pour se protéger contre les attaques qui peuvent résulter d'une journalisation et d'une surveillance insuffisantes du système et des applications.



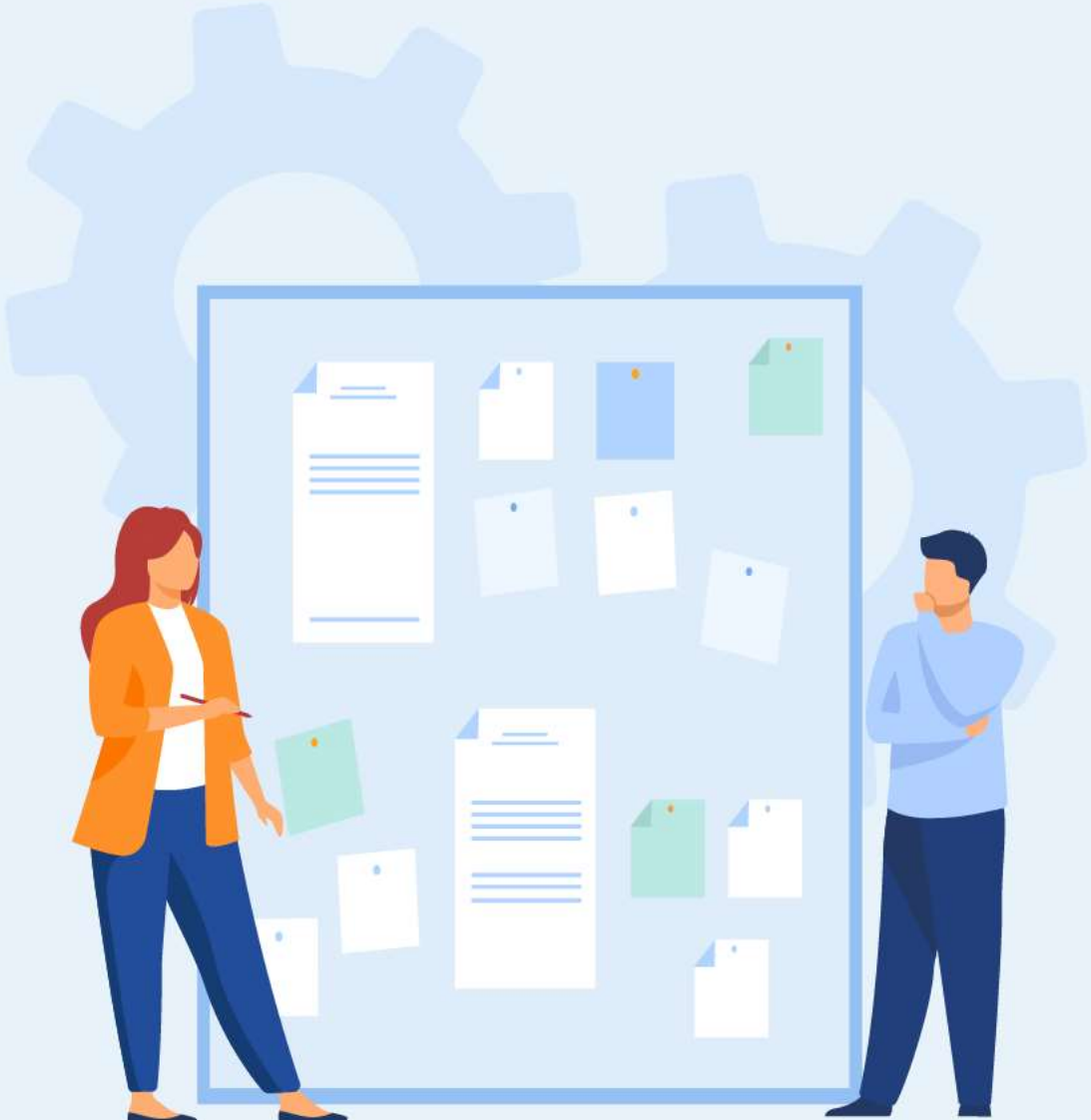
Dans le scénario suivant, un attaquant exploite une application qui effectue des appels vers une ressource interne sur le même réseau.

1. *L'attaquant identifie une application qui est vulnérable aux attaques SSRF.*
2. *L'attaquant envoie une fausse requête à l'application vulnérable et cible la ressource interne qui réside sur le même réseau.*

   Par exemple, la fausse requête suivante cible 192.0.2.100, qui réside sur le réseau interne :

   GET /index.php?url=http://192.0.2.100/admin/ HTTP/1.1

   Hôte : exemple.com
3. *L'application envoie la fausse requête à la ressource interne et reçoit une réponse contenant les données demandées.*
4. *L'application renvoie les données à l'attaquant, contournant ainsi la détection.*



CHAPITRE 2

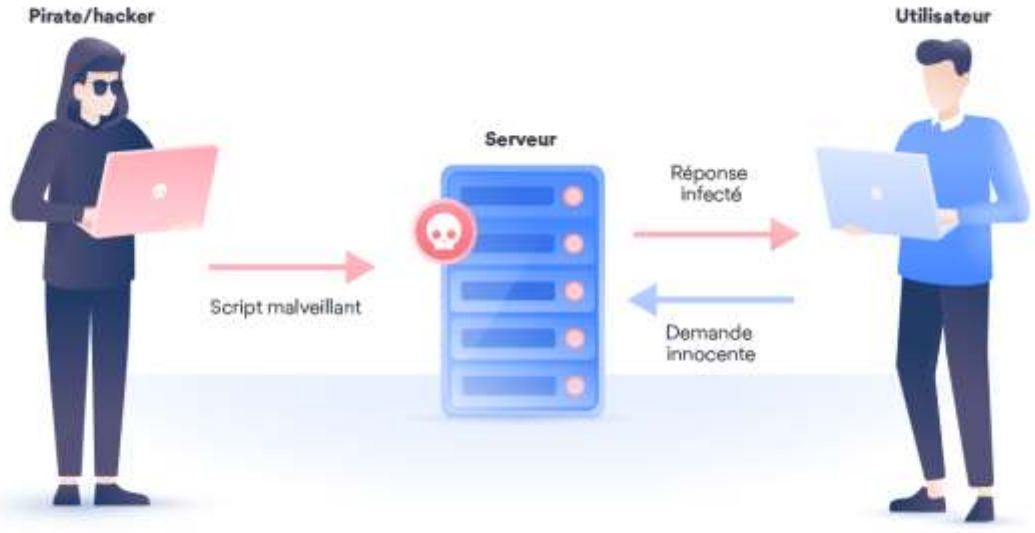
Comprendre les types d’attaques des systèmes informatiques

1. Vulnérabilités des applications Web
2. **Attaques " Cross Site Scripting " ou XSS**
3. Attaques sur les sessions (cookie poisonning, session hijacking, ...).
4. Exploitation de vulnérabilités sur le frontal HTTP (ver Nimda, faille Unicode, ...)
5. Attaques sur les configurations standards (Default Password, Directory Transversal, ...)
6. Attaques d’hameçonnage (fishing)
7. Attaques DDOS

Qu'est-ce qu'une attaque XSS ?

Le script intersites (XSS) est l'injection de scripts côté client dans les applications Web, qui est activée par un manque de validation et d'encodage correct des entrées utilisateur.

Les scripts malveillants sont exécutés dans le navigateur de l'utilisateur final et permettent diverses attaques, du vol de la session de l'utilisateur final à la surveillance et à la modification de toutes les actions effectuées par l'utilisateur final sur le site Web affecté.



Le principe d’une attaque XSS est d’utiliser un contenu malicieux, c’est-à-dire un contenu auquel l’utilisateur ne s’attend pas lorsqu’il est sur un site Internet qu’il pense sécurisé.

Cross-site Scripting (XSS) : définition et prévention | NordVPN

PARTIE 1

Types de script intersites (XSS)

Il existe différents types d'attaques XSS, qui distinguent si les scripts malveillants peuvent être injectés de manière non persistante ou persistante. De plus, il existe une différenciation entre la vulnérabilité causée par une validation d'entrée défectueuse côté client ou côté serveur.

Il existe 3 principaux types d'attaques de script intersites :

•XSS stocké

- Le script est stocké de manière persistante dans l'application Web
- Les utilisateurs visitant l'application après l'infection récupèrent le script
- Un code malveillant exploite les failles de l'application Web
- Le script et l'attaque sont visibles côté serveur (pour le propriétaire de l'application)

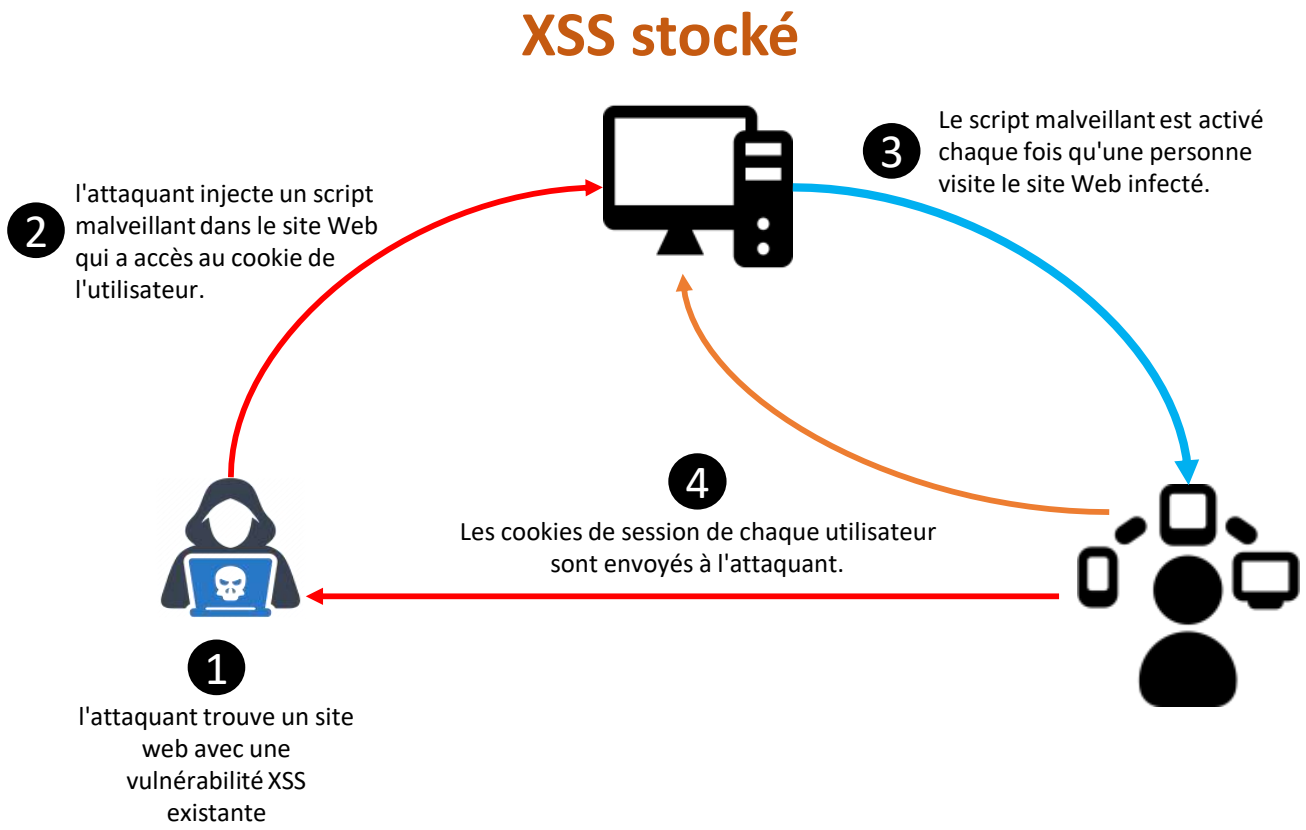
•Scripts intersites en miroir

- Le script est stocké de manière persistante dans l'application Web
- Les utilisateurs visitant l'application après l'infection récupèrent le script
- Un code malveillant exploite les failles de l'application Web
- Le script et l'attaque sont visibles côté serveur (pour le propriétaire de l'application)

•XSS basé sur Dom

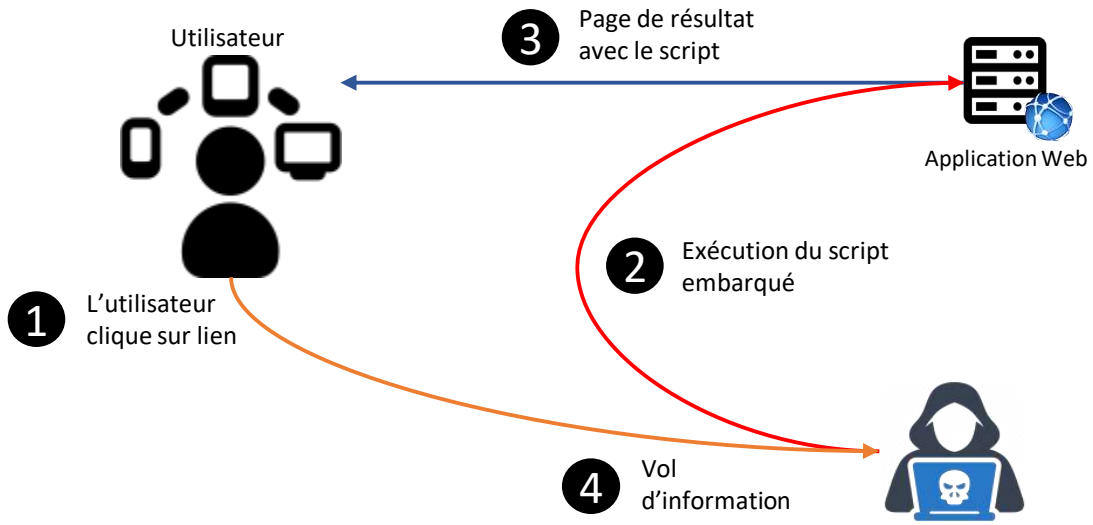
- Le script est stocké de manière persistante dans l'application Web
- Les utilisateurs visitant l'application après l'infection récupèrent le script
- Un code malveillant exploite les failles de l'application Web
- Le script et l'attaque sont visibles côté serveur (pour le propriétaire de l'application)

Types de script intersites (XSS)



Risque de vulnérabilités XSS

Scripts intersites en miroir



Dans ce cas, l'utilisateur doit d'abord envoyer la demande, puis le programme s'exécute sur le navigateur de la victime et renvoie les résultats du navigateur à l'utilisateur qui a envoyé la demande.

PARTIE 1

Types de script intersites (XSS)

XSS basé sur Dom

Supposons que le code suivant soit utilisé pour créer un formulaire permettant à l'utilisateur de choisir sa langue préférée. Une langue par défaut est également fournie dans la chaîne d'interrogation, sous la forme du paramètre "default".

1

```
…
Choisissez votre langue:
<select><script>
document.write("<OPTION
value=1>"+decodeURIComponent(document.location.href.substring(document.location
.href.indexOf("default=")+8))+"</OPTION>");
document.write("<OPTION value=2>Français</OPTION>");
</script></select>
…
```

La page est invoquée avec une URL telle que :

2

```
http://www.some.site/page.html?default=French…
```

Une attaque DOM Based XSS contre cette page peut être réalisée en envoyant l'URL suivante à une victime :

3

```
http://www.some.site/page.html?default=<script>alert(document.cookie)</
script>
```

Lorsque la victime clique sur ce lien, le serveur répond avec la page contenant le code Javascript ci-dessus. Le navigateur crée un objet DOM pour la page, dans lequel l'objet document.location contient précédente.

Le navigateur rend alors la page résultante et exécute le script de l'attaquant :

4

```
alert(document.cookie)
```

Risque de vulnérabilités XSS

Comment se protéger des attaques XSS ?

Les vulnérabilités de type **Cross-Site Scripting** sont difficiles à identifier et à corriger. Pour empêcher les attaques **XSS**, traitez toutes les entrées utilisateur comme potentiellement malveillantes et suivez certaines directives de programmation :

Éviter les entrées non fiables

Toute entrée affichée à l'intérieur d'une balise JavaScript est beaucoup plus susceptible d'être exploitée q'une entrée à l'intérieur d'un élément div ou span en HTML.

Activer la politique de sécurité du contenu (CSP)

Cela peut empêcher non seulement les attaques de type "Cross-Site Scripting", mais également les attaques par "Cross-Site Injection".

Filtrer les contrôleurs/champs de saisie de l' utilisateur

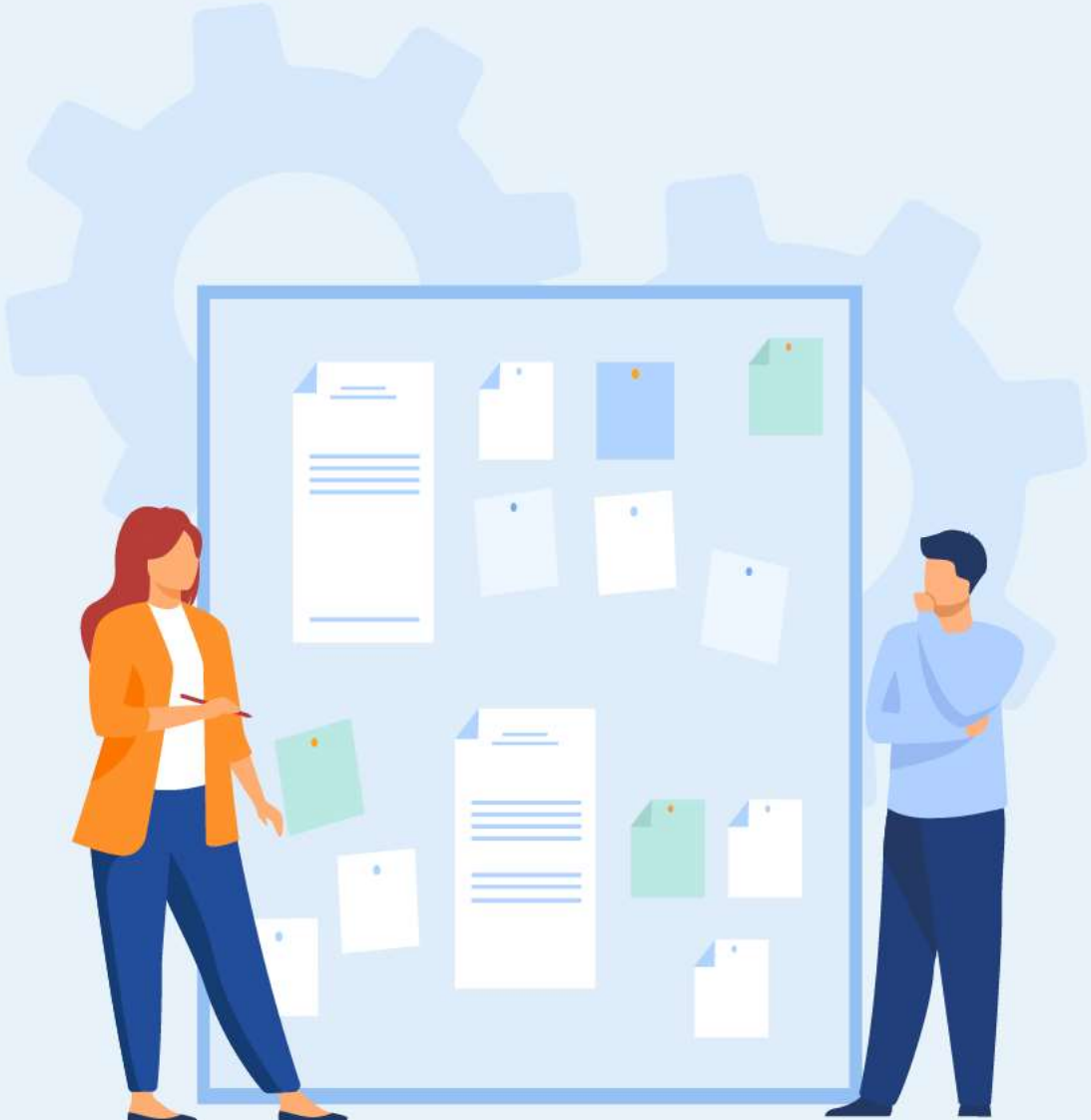
Lorsqu'une entrée non fiable s'affiche sous forme de texte normal à l'intérieur d'une balise HTML, filtrez les caractères qui permettent à un attaquant d'insérer une balise <script> dans la page

Correction du XSS basé sur DOM

Pour empêcher une attaque XSS basée sur DOM, vous pouvez utiliser une propriété JavaScript de sauvegarde telle que '`element.textContent`' pour une entrée utilisateur non fiable.

Utiliser un outil de vulnérabilité XSS

Utiliser les outils XSS comme certains scanners de vulnérabilité Web qui peuvent détecter toute vulnérabilité à laquelle vous pourriez être exposé.



CHAPITRE 2

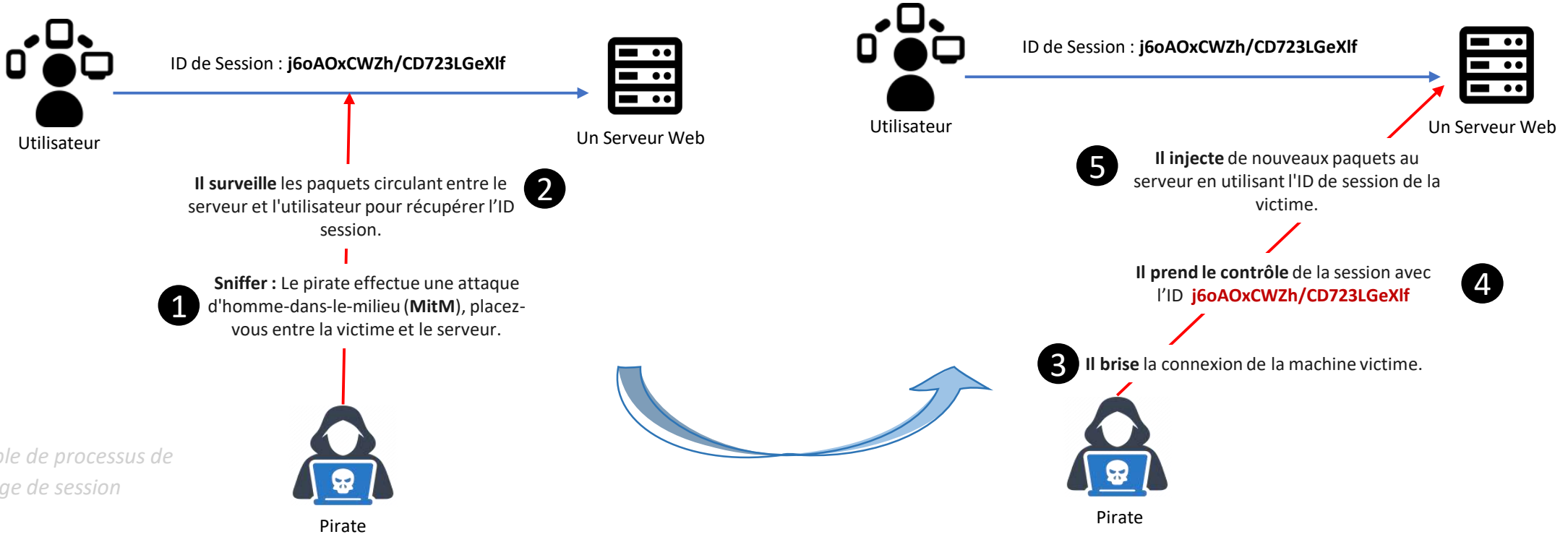
Comprendre les types d’attaques des systèmes informatiques

1. Vulnérabilités des applications Web
2. Attaques " Cross Site Scripting " ou XSS
3. **Attaques sur les sessions (cookie poisonning, session hijacking, ...).**
4. Exploitation de vulnérabilités sur le frontal HTTP (ver Nimda, faille Unicode, ...)
5. Attaques sur les configurations standards (Default Password, Directory Transversal, ...)
6. Attaques d’hameçonnage (fishing)
7. Attaques DDOS

Définition

L'attaque **Session Hijacking** consiste en l'exploitation du mécanisme de contrôle de session Web, qui est normalement géré pour un jeton de session(Session Token).

Un **jeton de session** est normalement composé **d'une chaîne de largeur variable** et il peut être utilisé de différentes manières, comme dans l'URL, dans l'en-tête de la requête http en tant que **cookie**, dans d'autres parties de l'en-tête de la requête http, ou encore dans le corps de la demande http.



Exemple de processus de piratage de session

PARTIE 1

Définition

L'attaque de détournement de session compromet le jeton de session en volant ou en prédisant un jeton de session valide pour obtenir un accès non autorisé au serveur Web. Le jeton de session peut être compromis de différentes manières et les plus courants sont :

Jeton de session prévisible

En analysant et en comprenant le processus de génération d'ID de session, un attaquant peut prédire une valeur d'ID de session valide et accéder à l'application.

Reniflage de session (Session Sniffing)

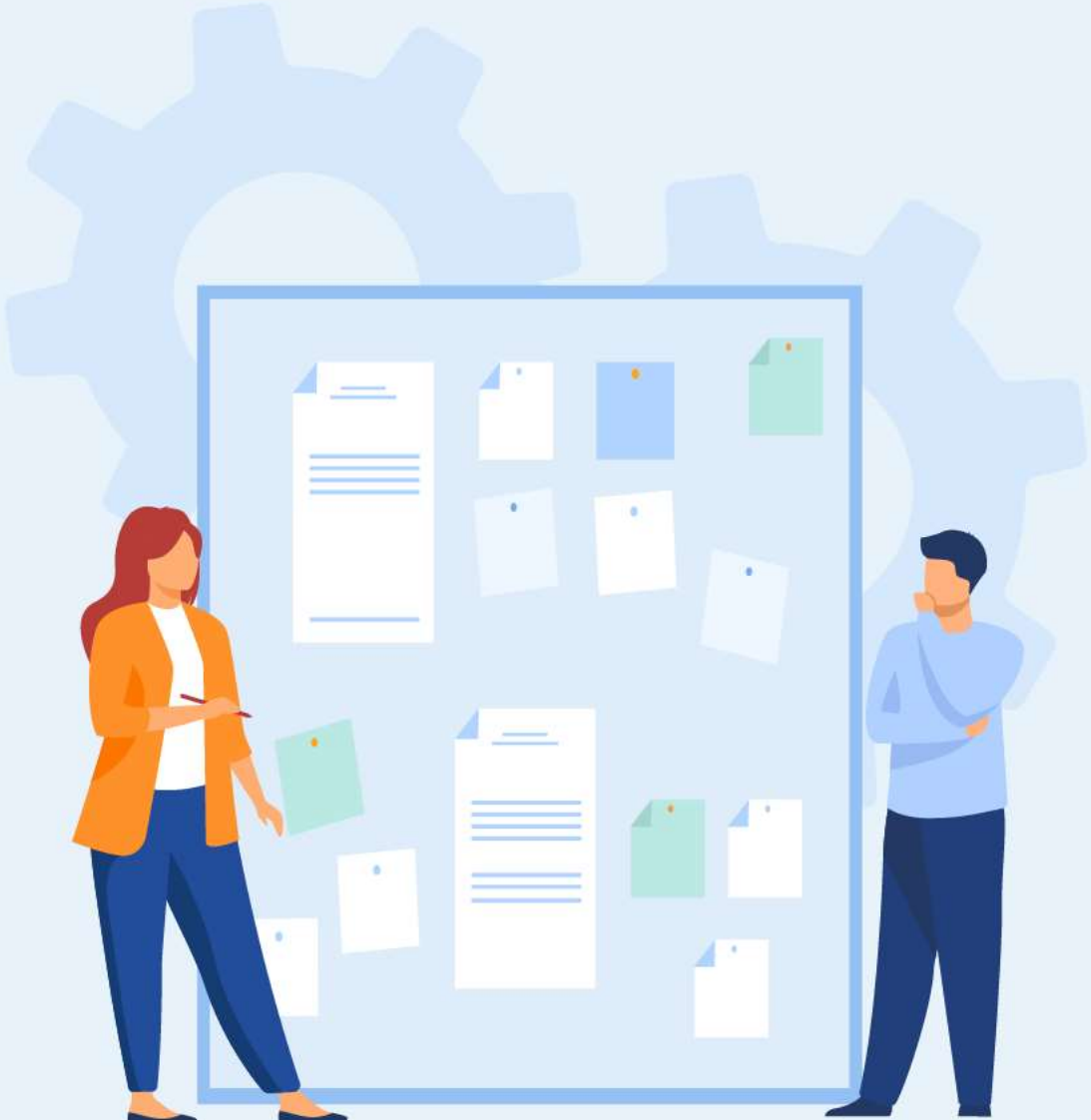
les attaquants utiliseront le **reniflage** de paquets comme **Wireshark** ou **Kismet** pour **surveiller** le trafic réseau et **voler les cookies de session après l'authentification**.

Attaque de l'homme dans le navigateur

L'attaquant infecte l'ordinateur d'un utilisateur avec un logiciel malveillant alors il peut agir comme un homme du milieu et intercepte les informations en se faisant passer pour l'utilisateur réel, le tout à l'insu de l'utilisateur.

Attaque de l'homme du milieu

Il s'agit du cas où un pirate se positionne dans le trafic entre un utilisateur et une application, soit pour écouter, soit pour se faire passer pour l'une des parties, en faisant croire qu'un échange normal d'informations est en cours.



CHAPITRE 2

Comprendre les types d’attaques des systèmes informatiques

1. Vulnérabilités des applications Web
2. Attaques " Cross Site Scripting " ou XSS
3. Attaques sur les sessions (cookie poisonning, session hijacking, ...).
4. **Exploitation de vulnérabilités sur le frontal HTTP (ver Nimda, faille Unicode, ...)**
5. Attaques sur les configurations standards (Default Password, Directory Transversal, ...)
6. Attaques d’hameçonnage (fishing)
7. Attaques DDOS

Introduction

Il devient de plus en plus susceptible d'avoir des vulnérabilités de sécurité sur le **front-end** en raison de nombreux facteurs, l'un d'eux est l'utilisation de code externe via des bibliothèques ou des **frameworks** tels que ***jQuery, ReactJS*** et ***VueJS, Lodash,*** ne configurant pas HTTPS pour crypter les données échangées entre le serveur et le client, utilisation de bibliothèques/frameworks anciens ou obsolètes.

Nous allons voir dans cette section deux exemples pour illustrer ce type de vulnérabilité:

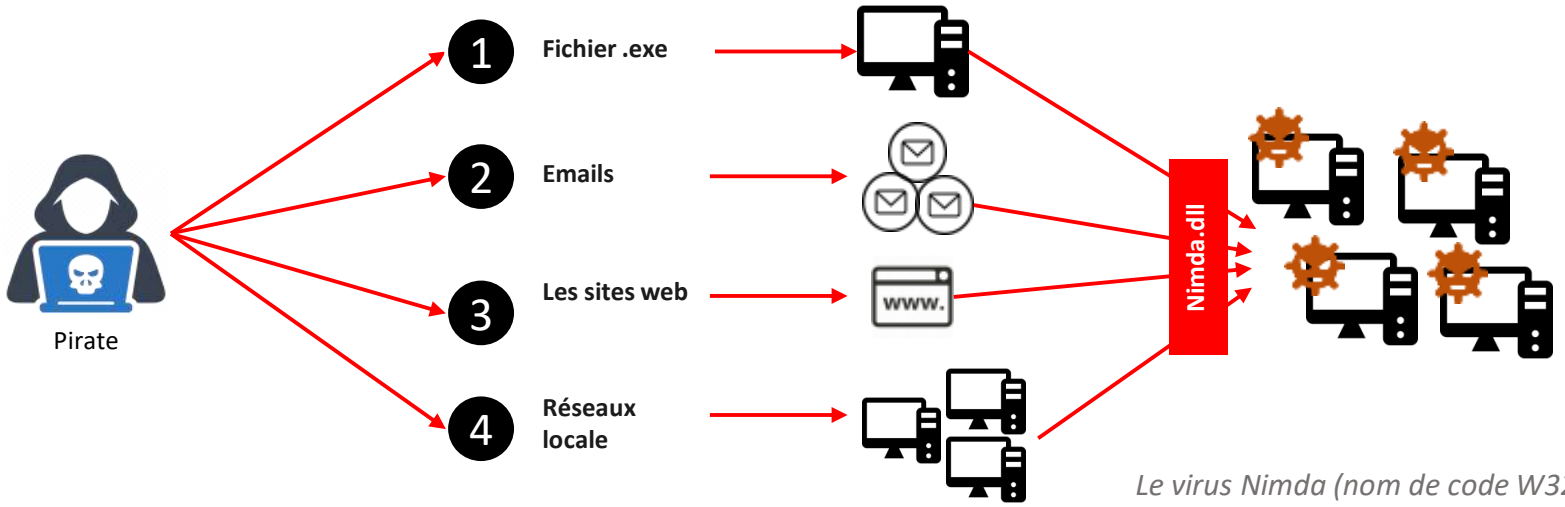
- **ver Nimda**
- **Faille Unicode**

Information

Du point de vue de la sécurité, JavaScript occupe la quatrième place sur la liste des langages les plus vulnérables, juste derrière Java, PHP et C. Pour cette raison, les développeurs doivent rester proactifs et défensifs dans la sécurisation de leurs applications JavaScript afin de préserver la sécurité du web.

Qu'est-ce que Nimda ?

Apparu pour la première fois le **18 septembre 2001**, Nimda est un virus informatique qui a provoqué des ralentissements du trafic ou le déni de service en se propageant sur Internet. Son nom de fichier, **épelé à l'envers est "admin",** fait référence au fichier minda.dll partagé via un message électronique qui, lorsqu'il est exécuté, continue de se propager, provoquant une épidémie de copies de vers.



Le virus Nimda (nom de code W32/Nimda est un ver se propageant à l'aide du courrier électronique

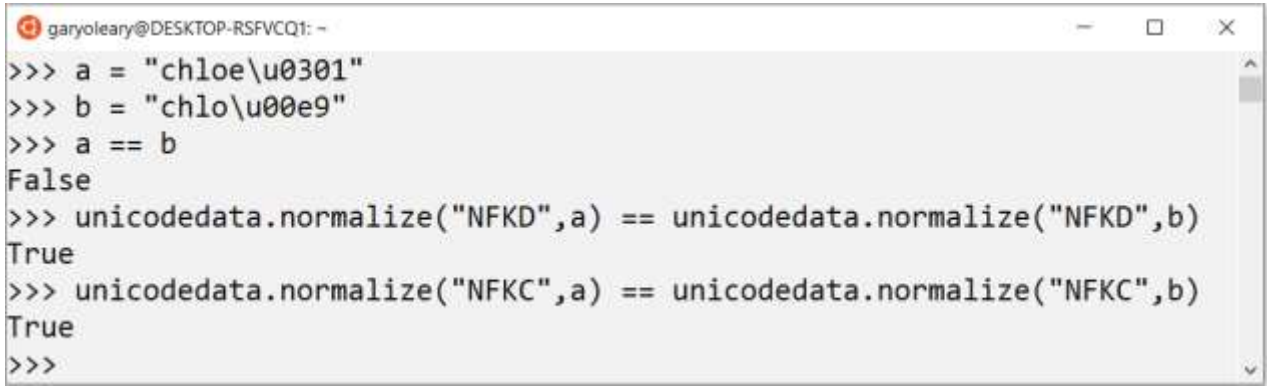
Information

Nimda a bloqué les serveurs et ralenti le trafic sur de nombreux réseaux d'entreprise, et a infecté des milliers d'ordinateurs personnels. Le ver est conçu pour se renvoyer tous les 10 jours s'il n'est pas supprimé. En outre, il peut transformer les ordinateurs en zombies qui peuvent être utilisés pour lancer de futures attaques par déni de service sur des sites Web.

PARTIE 1

La faille Unicode

L'attaque vise à explorer les failles du mécanisme de **décodage** mis en œuvre sur les applications lors du décodage du format de données **Unicode**. Un attaquant peut utiliser cette technique pour encoder certains caractères de l'URL afin de contourner les filtres de l'application, et ainsi accéder à des ressources restreintes sur le serveur Web ou forcer la navigation vers des pages protégées.



Un exemple de la façon dont Unicode normalise deux octets différents représentant le même caractère :

C'est quoi Unicode

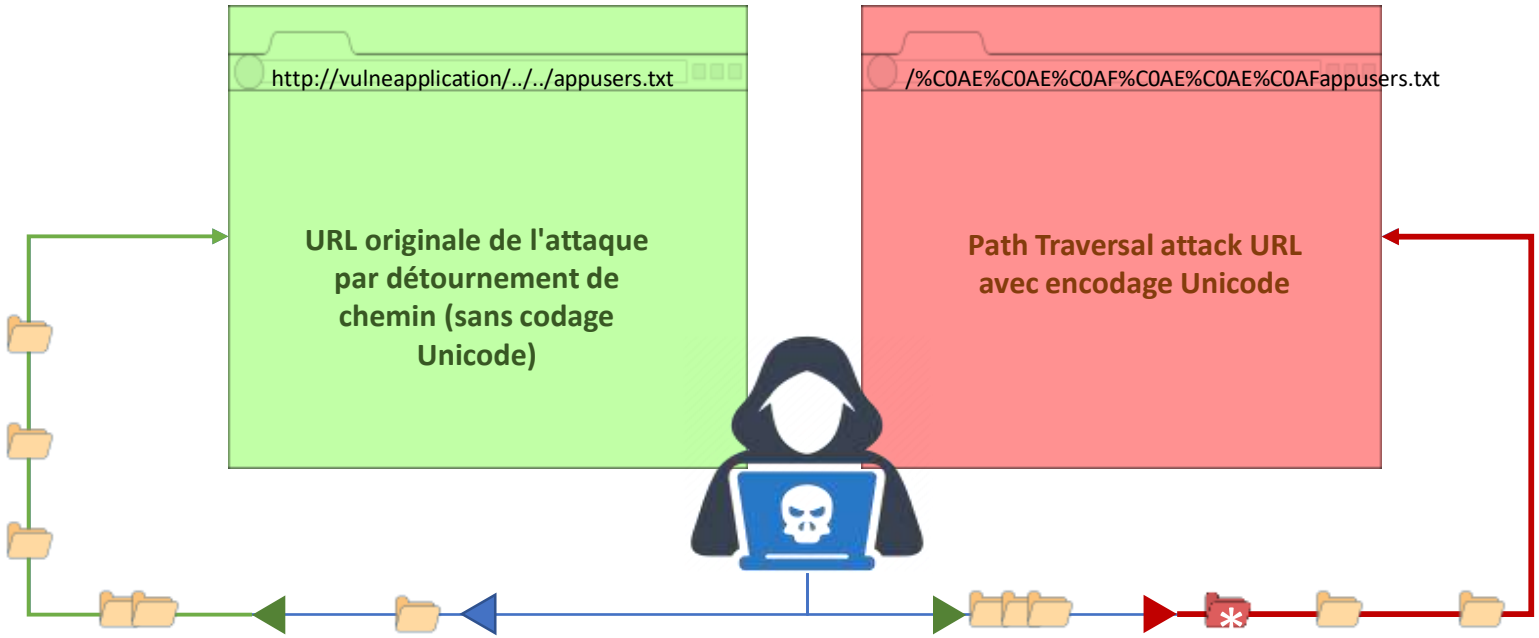
L'Unicode est une norme qui fournit **un numéro unique pour chaque caractère**, quelle que soit la plate-forme, l'appareil, l'application ou la langue. Il a été adopté par tous les fournisseurs de logiciels modernes et permet désormais de transporter des données via de nombreuses plates-formes, appareils et applications différents sans corruption.

Un exemple de la façon dont Unicode normalise deux octets différents représentant le même caractère :

La faille Unicode, exemple

Considérons une application web qui possède des répertoires ou des fichiers restreints (par exemple, un fichier contenant les noms d'utilisateur des applications : appusers.txt). Un attaquant peut coder la séquence de caractères "../" (Path Traversal Attack) en utilisant le format Unicode et tenter d'accéder à la ressource protégée, comme suit :

L'encodage Unicode de l'URL produira ici le même résultat que la première URL (Path Traversal Attack). Toutefois, si l'application dispose d'un mécanisme de filtrage de la sécurité des entrées, elle pourrait refuser toute requête contenant la séquence "../", bloquant ainsi l'attaque. Cependant, si ce mécanisme ne prend pas en compte le codage des caractères, l'attaquant peut le contourner et accéder aux ressources protégées.



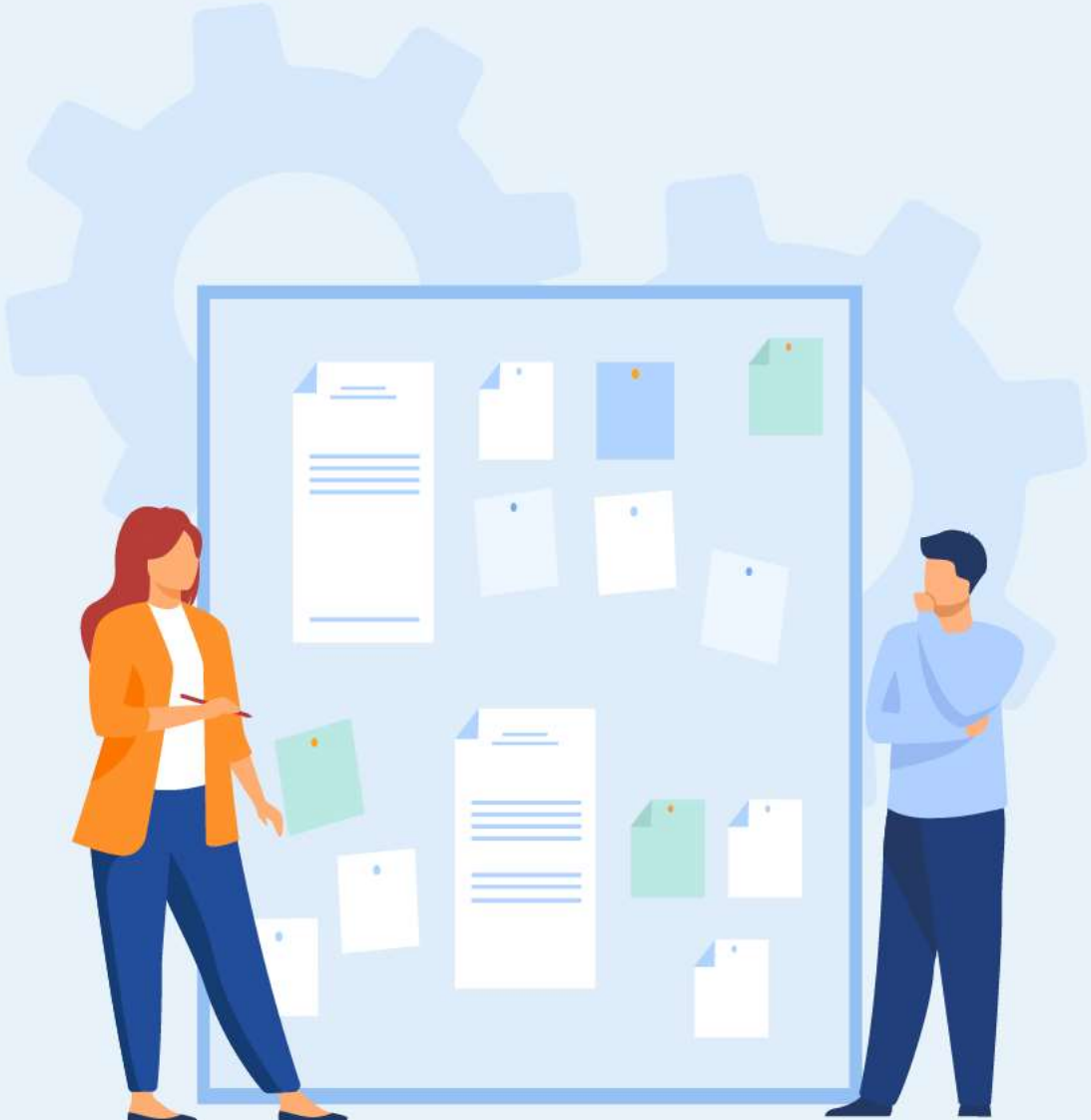
PARTIE 1

Les contre-mesures

- Utilisation des correctifs fournis par les serveurs. A titre d'exemple, Microsoft IIS a fourni un patch pour lutter contre cette vulnérabilité.

- Lorsque l'entrée du client est requise à partir de formulaires Web, évitez d'utiliser la méthode GET pour soumettre des données, car la méthode entraîne l'ajout des données du formulaire à l'URL et est facilement manipulable. Au lieu de cela, utilisez la méthode POST chaque fois que possible.

Tout contrôle de sécurité doit être effectué une fois que les données ont été décodées et validées comme contenu acceptable (par exemple, longueurs maximale et minimale, type de données correct, ne contient aucune donnée codée, les données textuelles ne contiennent que les caractères a-z et A-Z, etc.).



CHAPITRE 2

Comprendre les types d’attaques des systèmes informatiques

1. Vulnérabilités des applications Web
2. Attaques " Cross Site Scripting " ou XSS
3. Attaques sur les sessions (cookie poisonning, session hijacking, ...).
4. Exploitation de vulnérabilités sur le frontal HTTP (ver Nimda, faille Unicode, ...)
5. **Attaques sur les configurations standards (Default Password, Directory Transversal, ...)**
6. Attaques d’hameçonnage (fishing)
7. Attaques DDOS

Introduction

Les vulnérabilités de mauvaise configuration sont des faiblesses de configuration qui peuvent exister dans des sous-systèmes ou des composants logiciels. Par exemple:

- Un routeur peut être livré avec des comptes d'utilisateur par défaut qui est affiché derrière le matériel.
- Un logiciel peut avoir un ensemble connu de fichiers ou de répertoires de configuration standard que le pirate pourrait exploiter.

Le deux plus connus des attaques sont :

- Les comptes d’utilisateurs par default
- Les structures répertoires et fichiers par default

Remarques

Le terme "mauvaise configuration de sécurité" est un peu un fourre-tout qui inclut les vulnérabilités courantes introduites par les paramètres de configuration de l'application, plutôt que par un mauvais code. Les plus courantes impliquent généralement des erreurs simples qui peuvent avoir de lourdes conséquences pour les organisations qui déploient des applications présentant ces erreurs de configuration.

Les comptes d’utilisateurs par default

De nombreuses applications Web et périphériques matériels ont des mots de passe par défaut pour le compte administratif intégré. Ce qui signifie qu'ils peuvent être facilement devinés ou obtenus par un attaquant.

Lorsqu'ils tentent d'accéder à un système, les attaquants essaient d'abord les mots de passe par défaut. La plupart des ces mots de passe sont publiquement et facilement disponibles en ligne et dans la documentation du produit, l'une des premières étapes qu'un attaquant tentera est d'accéder à un appareil ou à un service à l'aide des informations d'identification par défaut du produit.

Un exemple Configuration par default d’un routeur 3G/4G avec le mot de passe et l’url d’accès

PARTIE 1

PARTIE 1

Que faire?

Modifier les mots de passe par défaut

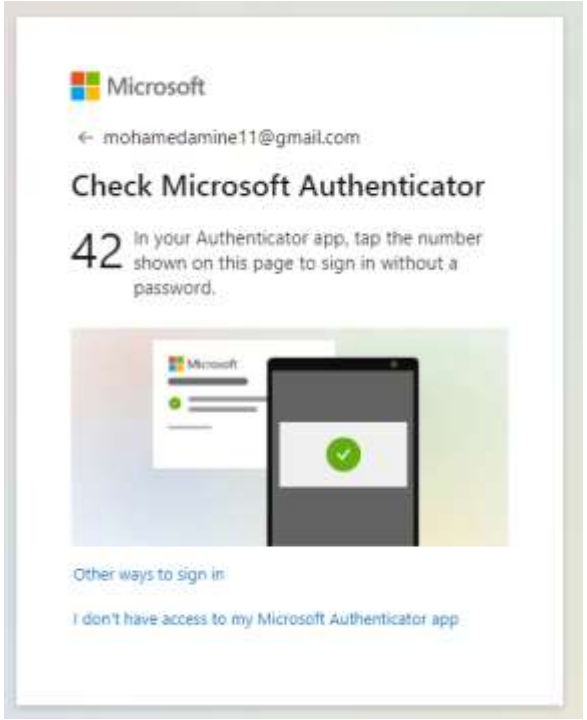
- Modifiez les mots de passe par défaut dès que possible et surtout avant de déployer le système sur Internet.
- Utilisez un mot de passe suffisamment fort et unique.
- Veillez à ne pas utiliser un mot de passe prédictible comme **password, password1, 123456, admin, azerty, etc**.

Forcer les changements de mot de passe par défaut

- Les fournisseurs peuvent concevoir des systèmes pour exiger des changements de mot de juste après la première installation.
- Lors de la création des nouveau compte sur une application obligez les utilisateur a modifier leurs MDP après leurs premiers connexion.

Utiliser des mécanismes d'authentification alternatifs

- Lorsque cela est possible, utilisez des mécanismes d'authentification alternatifs tels que
- les code OTP envoyés par sms à l'utilisateur
- l'authentification multi-facteur
- les application mobile d'authentification.



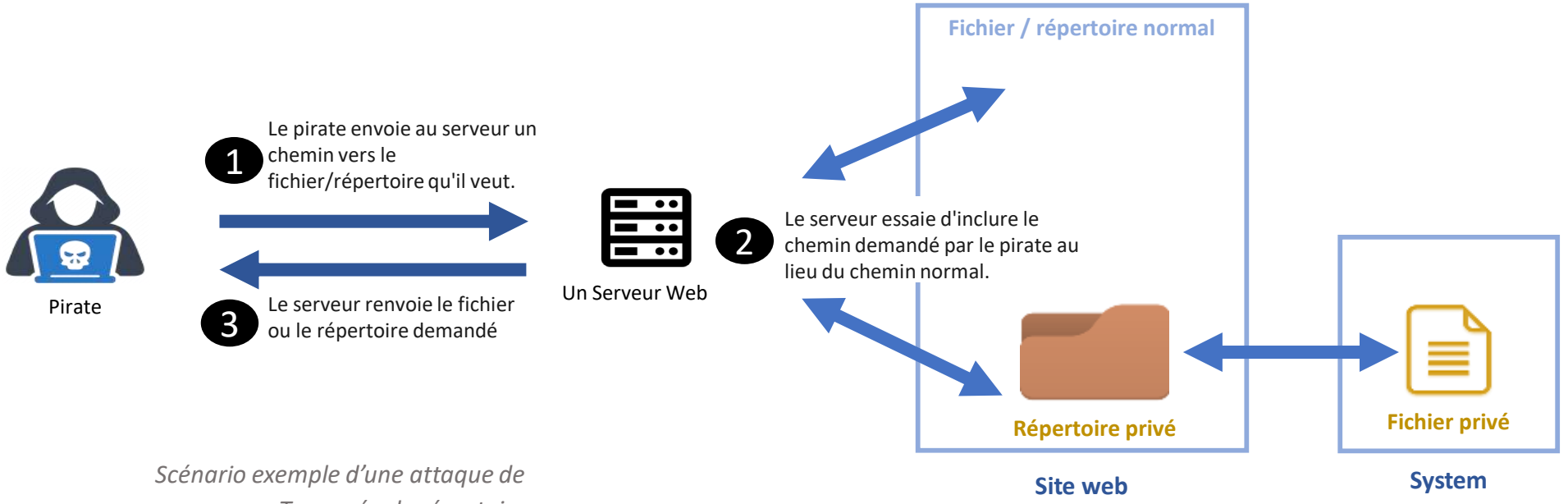
Un exemple de mécanisme d'authentification de deux facteurs de Microsoft

Traversée de répertoire (Directory traversal)

Une attaque par traversée de chemin (également connue sous le nom de traversée de répertoire) vise à accéder aux fichiers et répertoires stockés en dehors du dossier racine Web. En manipulant des variables qui référencent des fichiers avec :

- Des séquences "point-point-barre oblique (../)" et ses variantes
- En utilisant des chemins de fichier absolus

Pour lancer cette attaque, les pirates parcourent souvent une arborescence de répertoires, où ils peuvent localiser les chemins d'accès aux fichiers restreints sur les serveurs Web.



Scénario exemple d'une attaque de Traversée de répertoire

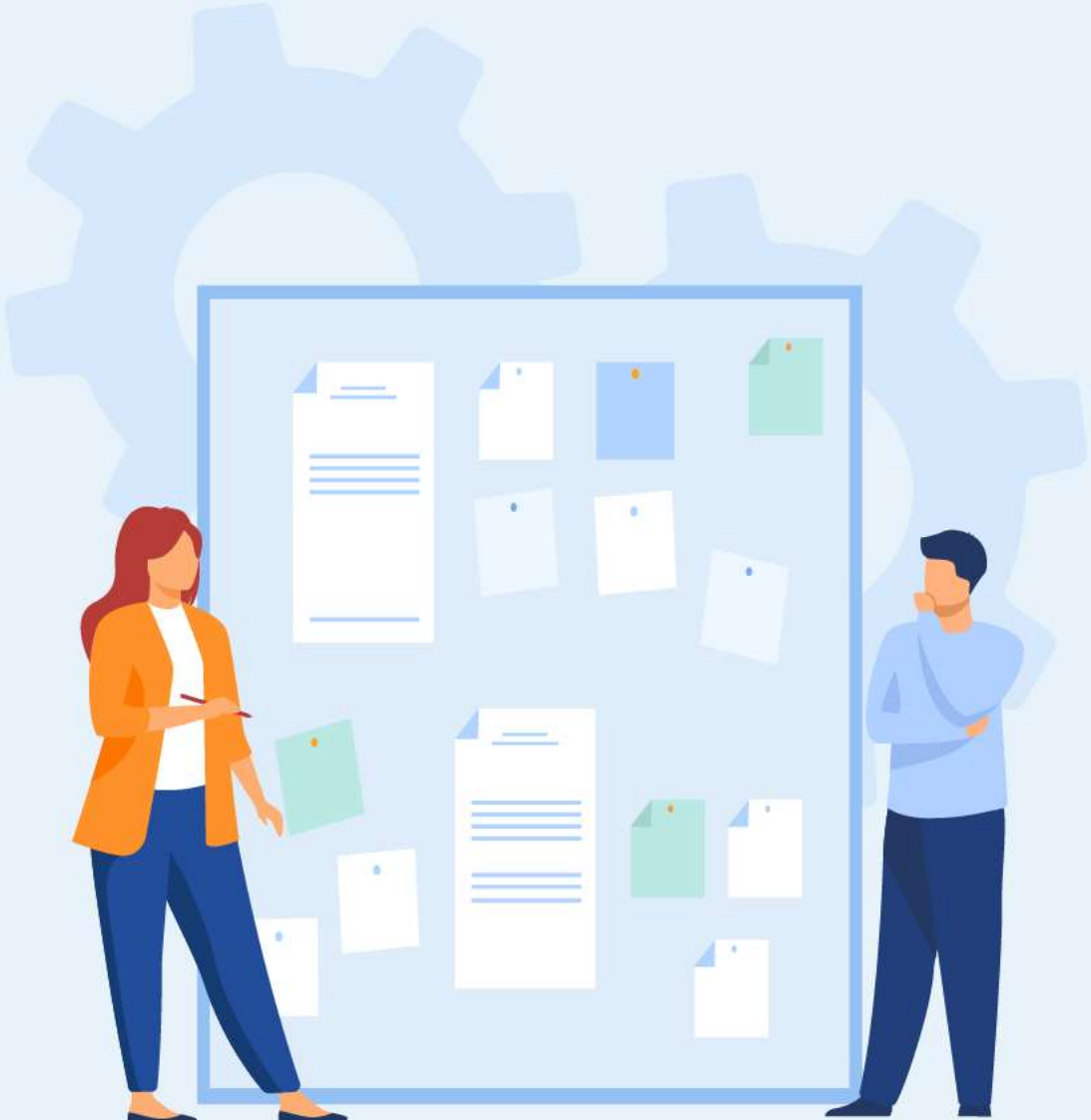
PARTIE 1

Prévention de traversée de répertoire

1. Les développeurs doivent valider les entrées utilisateur acceptées à partir des navigateurs
   - La validation des entrées peut aider à garantir que les attaquants sont empêchés d'utiliser des techniques de commande, comme l'injection SQL, qui violent les privilèges d'accès et peuvent accorder aux attaquants l'accès à un répertoire racine.
2. Les applications doivent utiliser des filtres pour bloquer les entrées suspectes des utilisateurs
   - La plupart des applications Web utilisent des filtres pour bloquer les URL contenant des commandes, ainsi que les codes d'échappement couramment utilisés par les attaquants.
3. Les administrateurs doivent tenir à jour les logiciels
   - Des logiciels comme le logiciel du serveur Web et le système d'exploitation sous-jacent, et appliquer tous les correctifs de sécurité. La pratique consistant à appliquer régulièrement des correctifs aux logiciels peut réduire considérablement les risques de sécurité et réduire les risques d'exploitation.

Remarques

Une autre mesure importante à prendre est d'utiliser judicieusement les listes de contrôle d'accès et de veiller à ce que les droits d'accès appropriés soient en place. Vous pouvez également minimiser les risques de telles attaques en filtrant les entrées fournies par l'utilisateur à partir des navigateurs.



CHAPITRE 2

Comprendre les types d’attaques des systèmes informatiques

1. Vulnérabilités des applications Web
2. Attaques " Cross Site Scripting " ou XSS
3. Attaques sur les sessions (cookie poisonning, session hijacking, ...).
4. Exploitation de vulnérabilités sur le frontal HTTP (ver Nimda, faille Unicode, ...)
5. Attaques sur les configurations standards (Default Password, Directory Transversal, ...)
6. **Attaques d’hameçonnage (fishing)**
7. Attaques DDOS

PARTIE 1

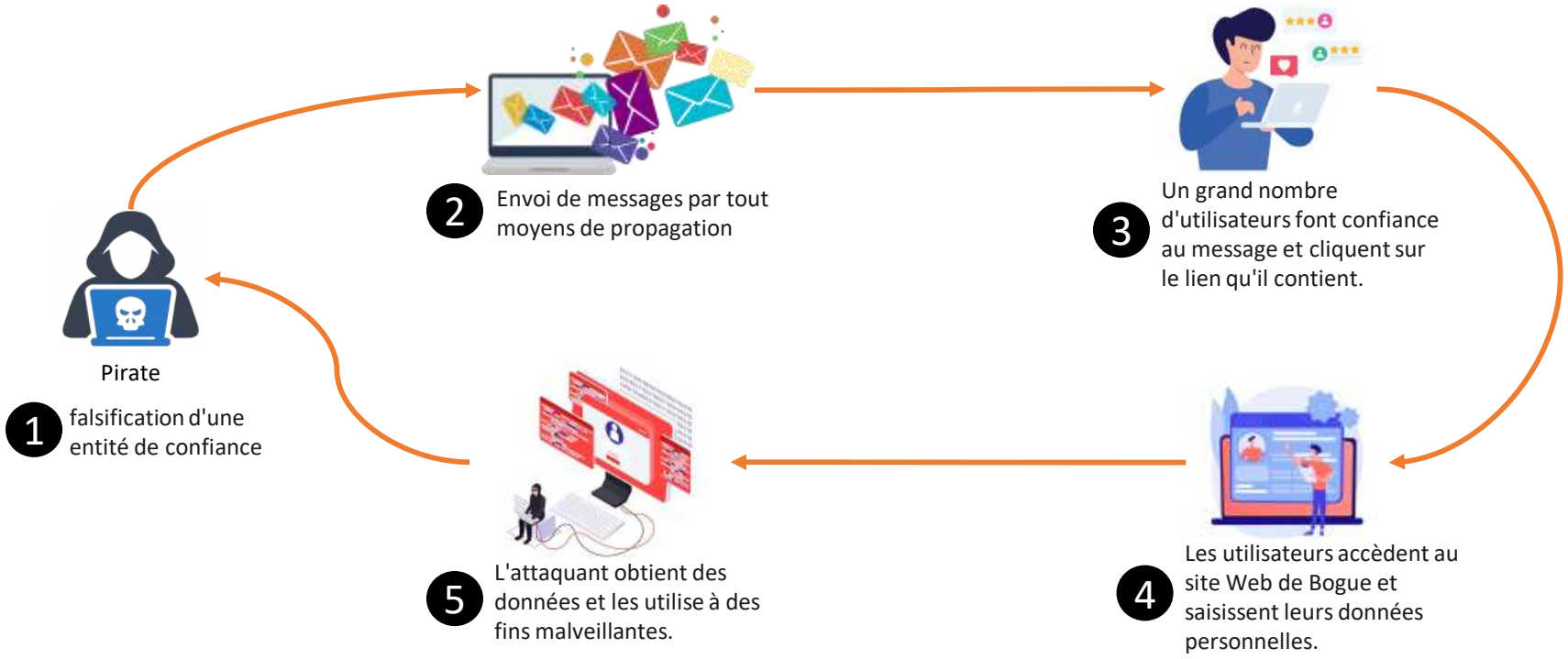
Qu'est-ce que l'hameçonnage ?

Le hameçonnage est un type d'attaque d'ingénierie sociale souvent utilisé pour voler des données d'utilisateur, notamment des identifiants de connexion et des numéros de carte de crédit. Il se produit lorsqu'un attaquant, se faisant passer pour une entité de confiance, incite une victime à ouvrir un courriel, un message instantané ou un message texte. Le destinataire est alors incité à cliquer sur un lien malveillant, ce qui peut entraîner l'installation d'un logiciel malveillant, le blocage du système dans le cadre d'une attaque par ransomware ou la révélation d'informations sensibles.

- Les hameçonneurs utilisent fréquemment des émotions comme la peur, la curiosité, l'urgence et l'avidité pour obliger les destinataires à ouvrir des pièces jointes ou à cliquer sur des liens.
- Il suffit d'une seule attaque de phishing réussie pour compromettre votre réseau et voler vos données, c'est pourquoi il est toujours important de réfléchir avant de cliquer.
- Les attaques de phishing sont conçues pour sembler provenir d'entreprises et de personnes légitimes.
- Les cybercriminels innovent en permanence et deviennent de plus en plus sophistiqués.

Comment fonctionne l'hameçonnage ?

Le hameçonnage commence par un courriel frauduleux ou un autre outil de communication conçu pour attirer une victime. Le message est présenté comme provenant d'un expéditeur de confiance. Si la victime est trompée, elle est amenée à fournir des informations confidentielles, souvent sur un site Web frauduleux. Parfois, un logiciel malveillant est également téléchargé sur l'ordinateur de la cible.



Un exemple de circuit d'attaque par hameçonnage

Types d'attaques de phishing : Spear Phishing

1 Un pirate identifie un élément de données qu'il veut et identifie l'individu qui le possède.

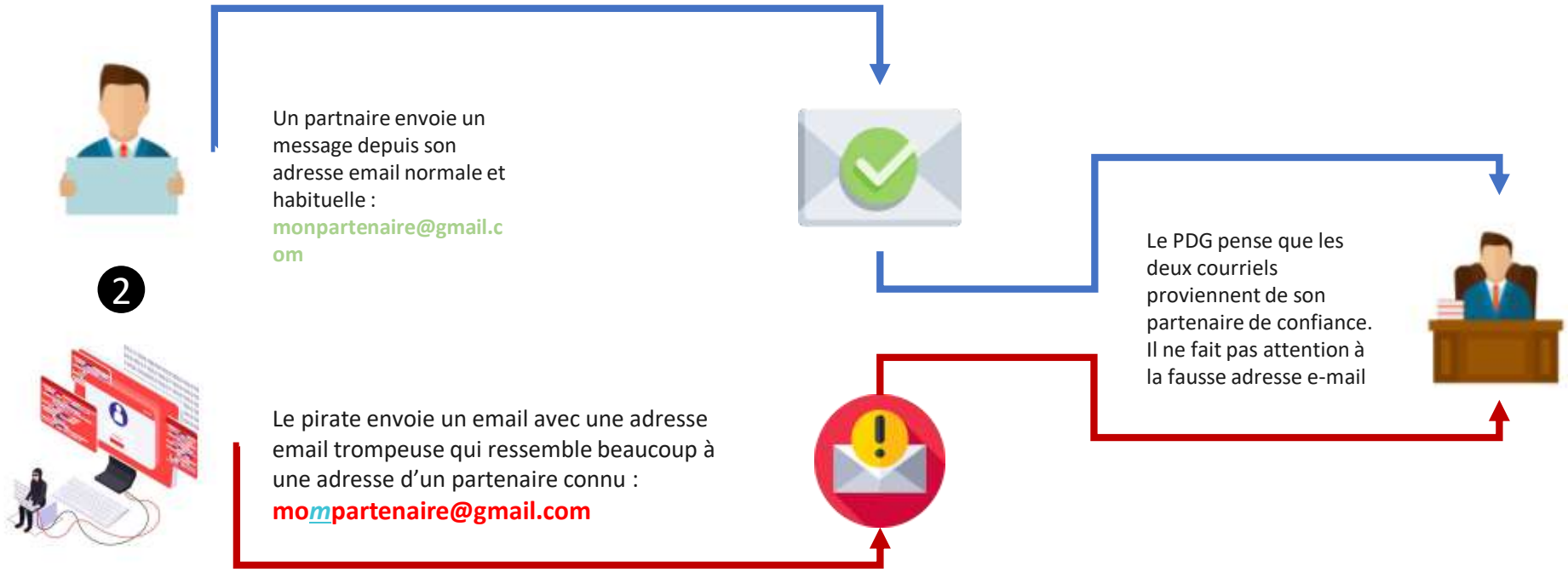
2 Un hacker retrouve l'individu et se fait passer pour l'une de ses sources de confiance.

4 Le pirate parvient à convaincre sa victime de partager ses données et les utilise pour commettre un acte malveillant.

Le Spear Phishing est une attaque ciblée contre un individu ou une organisation dans le but de récupérer des informations confidentielles à des fins frauduleuses.

PARTIE 1

Types d'attaques de phishing : Whaling



Le hameçonnage à la baleine (Whaling) est un type de hameçonnage encore plus ciblé qui s'attaque les baleines qui sont encore plus gros que les poissons. Ces attaques visent généralement un PDG, un directeur financier ou tout autre directeur d'un secteur ou d'une entreprise spécifique. Un courriel de phishing peut indiquer que l'entreprise est confrontée à des conséquences juridiques et que vous devez cliquer sur le lien pour obtenir plus d'informations.

PARTIE 1

PARTIE 1

Types d'attaques de phishing

Hameçonnage par courriel

La plupart des attaques de phishing sont envoyées par courrier électronique. Les attaquants enregistrent généralement de faux noms de domaine qui imitent des organisations réelles et envoient des milliers de requêtes communes aux victimes.

Pour les faux domaines, les attaquants peuvent ajouter ou remplacer des caractères (par exemple, my-bank.com au lieu de mybank.com), utiliser des sous-domaines (par exemple, mybank.host.com) ou utiliser le nom de l'organisation de confiance comme nom d'utilisateur de l'e-mail (par exemple, mybank@host.com).

De nombreux courriels de phishing utilisent un sentiment d'urgence ou une menace pour inciter l'utilisateur à se conformer rapidement sans vérifier la source ou l'authenticité du courriel.

Les messages de phishing par courrier électronique ont l'un des objectifs suivants :

- Amener l'utilisateur à cliquer sur un lien vers un site web malveillant, afin d'installer un logiciel malveillant sur son appareil.
- Amener l'utilisateur à télécharger un fichier infecté et l'utiliser pour déployer un logiciel malveillant.
- Amener l'utilisateur à cliquer sur un lien vers un faux site web et à soumettre des données personnelles.
- Amener l'utilisateur à répondre et à fournir des données personnelles.

From: Royal Bank of Canada [securityclient@rbc.com]
Sent: 2012, July, 20 7:33 PM
To: undisclosed-recipients
Subject: Account ALERT - Your RBC Account is at Risk!

RBC Royal Bank

Cher(e) Client. 1

Le département de vérification comptable du Groupe Financier RBC a détecté un problème de transaction dans votre compte. 2 Un montant a été déposé et retiré par notre système comptable. Nous vous avisons de cette erreur afin que vous ne soyez pas surpris quand vous verrez ces transactions sur votre relevé transactionnel. Nous avons repris le montant total sans appliquer les frais de transactions. Ne divulguez jamais vos renseignements personnels sur un site autre que le site sécurisé RBC. Si vous constatez une autre erreur, communiquez avec votre institution durant les heures de votre succursale.

Pour accéder à votre compte et **immédiatement** vérifier que tout soit normal, cliquez sur ce lien sécurisé si dessus: 3

https://www1.royalbank.com/cgi-bin/rbaccess/ 4

Soyez assuré que RBC met tout en oeuvre pour protéger les utilisateurs de ses services Internet

RBC vous remercie de votre clientèle et apprécie votre compréhension.

RBC Groupe Financier.

Svp ne répondez pas r ce courriel car c'est seulement un avis. Le courrier envoyé r cette adresse ne peut pas etre répondu.

© Banque Royale du Canada

un exemple de courriel d'hameçonnage.

Comment prévenir les attaques de phishing

Certaines des techniques les plus simples et les plus efficaces utilisées par les cybercriminels pour atteindre leurs objectifs sont ce que l'on appelle les attaques par hameçonnage. Il est souvent beaucoup plus facile d'inciter quelqu'un à cliquer sur un lien dans un courriel ou à ouvrir une pièce jointe malveillante que de contourner le pare-feu et les autres défenses d'une organisation.

Les attaques de phishing peuvent avoir plusieurs objectifs différents, notamment la diffusion de logiciels malveillants, le vol d'argent et le vol d'identifiants. Cependant, la plupart des escroqueries par hameçonnage visant à dérober vos informations personnelles peuvent être détectées si vous êtes suffisamment attentif.

Méfiez-vous toujours des e-mails de réinitialisation de mot de passe

Les courriels de réinitialisation du mot de passe sont conçus pour vous aider lorsque vous ne vous souvenez plus du mot de passe de votre compte. En cliquant sur un lien, vous pouvez réinitialiser le mot de passe de ce compte avec quelque chose de nouveau.

Ne pas connaître votre mot de passe est, bien entendu, le problème auquel les cybercriminels sont confrontés lorsqu'ils tentent d'accéder à vos comptes en ligne. En envoyant un faux courriel de réinitialisation de mot de passe qui vous dirige vers un site de phishing ressemblant à un site de phishing, ils peuvent vous convaincre de saisir les informations d'identification de votre compte et de les leur envoyer.

Si vous recevez un courriel non sollicité de réinitialisation de mot de passe, visitez toujours directement le site Web (ne cliquez pas sur les liens intégrés) et changez votre mot de passe pour quelque chose de différent sur ce site (et sur tout autre site ayant le même mot de passe).

Comment prévenir les attaques de phishing

si un courriel vous incite à prendre des mesures rapides ou inhabituelles, ralentissez et vérifiez qu'il est légitime avant de lui faire confiance. En outre, il est important d'examiner et faire attention aux points suivants:

•Notez toujours la langue utilisée dans l'e-mail

- Les techniques d'ingénierie sociale sont conçues pour tirer parti de la nature humaine. Cela inclut le fait que les gens sont plus susceptibles de faire des erreurs lorsqu'ils sont pressés et sont enclins à suivre les ordres des personnes en position d'autorité.

Fausse commande/livraison

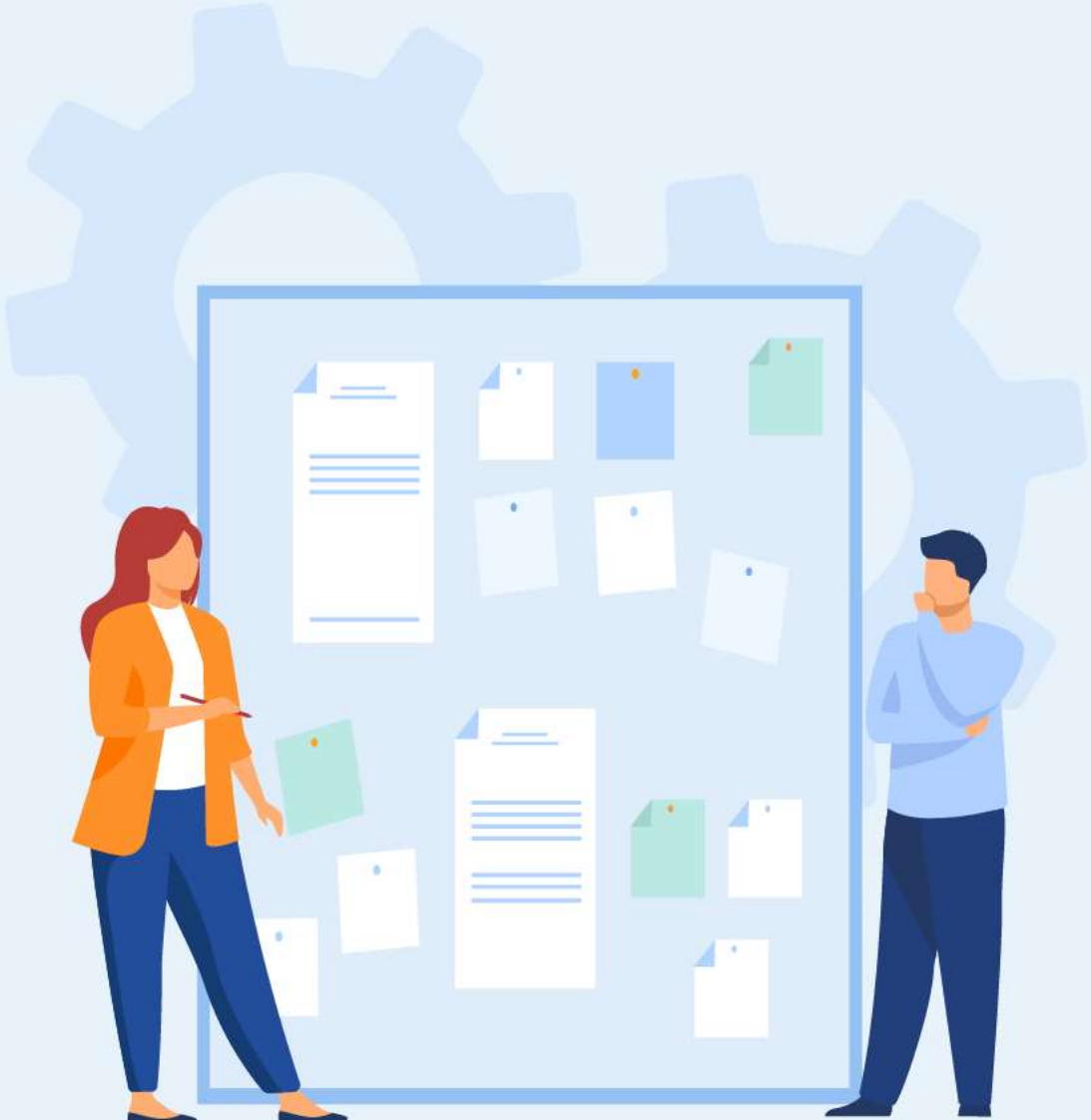
- Un courriel de phishing usurpe l'identité d'une marque de confiance (Amazon, FedEx, etc.) en affirmant que vous avez passé une commande ou que vous avez reçu une livraison. Lorsque vous cliquez pour annuler la commande ou la livraison non autorisée, le site Web (qui appartient à un cybercriminel) demande une authentification, ce qui permet à l'attaquant de voler les identifiants de connexion.

Business Email Compromise (BEC)

- Les escroqueries BEC tirent parti de la hiérarchie et de l'autorité au sein d'une entreprise. Un attaquant se fait passer pour le PDG ou un autre cadre de haut niveau et ordonne au destinataire de l'e-mail de prendre certaines mesures, comme envoyer de l'argent sur un certain compte bancaire (qui appartient à l'escroc).

Fausse facture

- Le phisher se fait passer pour un fournisseur légitime et demande le paiement d'une facture impayée. L'objectif final de cette escroquerie est de faire transférer de l'argent sur le compte de l'attaquant ou de transmettre un logiciel malveillant via un document malveillant.



CHAPITRE 2

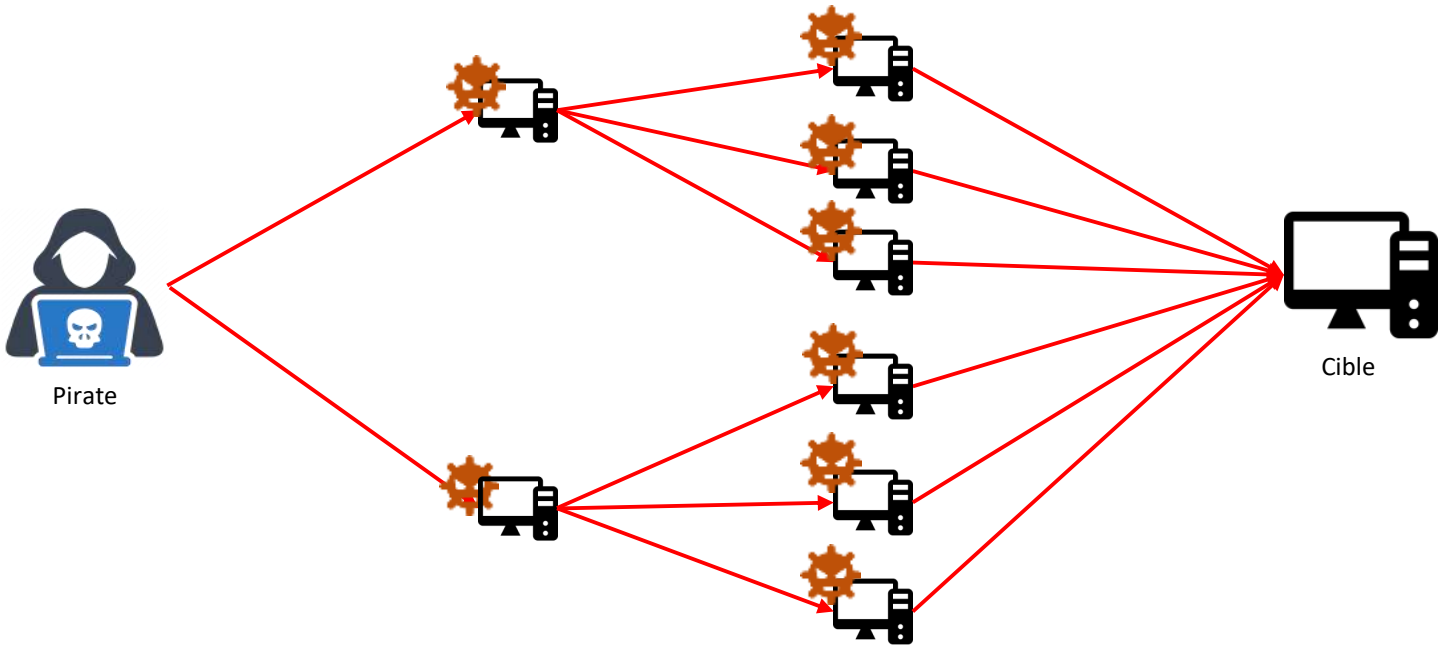
Comprendre les types d’attaques des systèmes informatiques

1. Vulnérabilités des applications Web
2. Attaques " Cross Site Scripting " ou XSS
3. Attaques sur les sessions (cookie poisonning, session hijacking, ...).
4. Exploitation de vulnérabilités sur le frontal HTTP (ver Nimda, faille Unicode, ...)
5. Attaques sur les configurations standards (Default Password, Directory Transversal, ...)
6. Attaques d’hameçonnage (fishing)
7. **Attaques DDOS**

Qu'est-ce qu'une attaque DDoS ?

Les attaques par déni de service distribué (**DDoS**) sont une sous-classe des attaques par déni de service (**DoS**). Une attaque DDoS implique de multiples dispositifs en ligne connectés, connus collectivement sous le nom de botnet, qui sont utilisés pour submerger un site web ou un serveur cible avec un faux trafic.

Une attaque DDoS vise plutôt à rendre votre site web et vos serveurs indisponibles pour les utilisateurs légitimes.

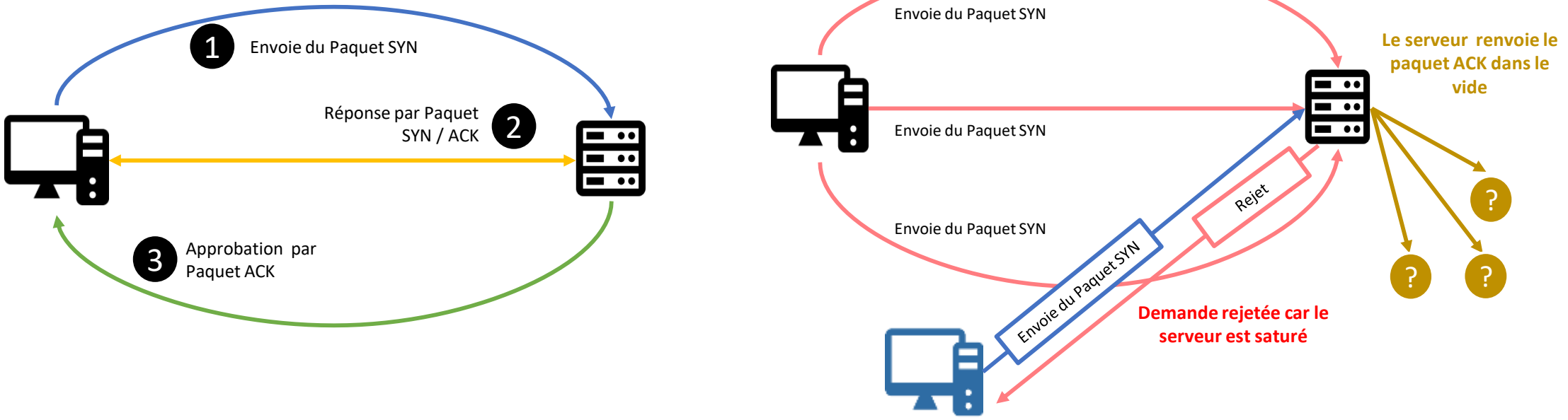


Exemple d'une attaque par déni de service (denial of service attack, d'où l'abréviation DoS)

Les attaques par dénie de service (DoS) et par déni de service distribué (DDoS):

Attaque TCP SYN flood:

Une inondation SYN (**SYN flood en Anglais**), parfois **appelée attaque semi-ouverte**, est une attaque au niveau du réseau qui bombarde un serveur avec des demandes de connexion sans répondre aux accusés de réception correspondants. Le grand nombre de connexions TCP ouvertes qui en résultent consomment les ressources du serveur pour évincer essentiellement le trafic légitime, ce qui rend impossible l'ouverture de nouvelles connexions légitimes et rend difficile, voire impossible, le fonctionnement correct du serveur pour les utilisateurs autorisés qui sont déjà connectés.



Exemple d'une attaque TCP SYN flood

PARTIE 1

Les attaques par dénie de service (DoS) et par déni de service distribué (DDoS) :

Attaque teardrop

Une attaque **teardrop** est un type d'attaque par déni de service (DoS). **C’est une attaque qui tente de rendre une ressource informatique indisponible en inondant un réseau ou un serveur de requêtes et de données.** L'attaquant envoie des paquets fragmentés au serveur cible , et dans certains cas où il existe une vulnérabilité TCP/IP, le serveur est incapable de réassembler le paquet, ce qui provoque une surcharge.

De nombreuses organisations s'appuient encore sur des systèmes d'exploitation plus anciens, obsolètes ou non corrigés pour exécuter les applications héritées dont elles ont encore besoin. Ces organisations sont vulnérables aux attaques Teardrop qui menacent de supprimer des applications critiques.

Attaque teardrop : Comment ça marche ?

Les implémentations TCP/IP diffèrent légèrement d'une plate-forme à l'autre. Certains systèmes d'exploitation, en particulier les anciennes versions de Windows et Linux, contiennent un bogue de réassemblage de fragmentation TCP/IP. Les attaques Teardrop sont conçues pour exploiter cette faiblesse. Dans une attaque Teardrop, le client envoie un paquet d'informations fragmenté intentionnellement à un appareil cible. Étant donné que les paquets se chevauchent, une erreur se produit lorsque le périphérique tente de réassembler le paquet. L'attaque profite de cette erreur pour provoquer un crash fatal du système d'exploitation ou de l'application qui gère le paquet.

Les attaques par dénie de service (DoS) et par déni de service distribué (DDoS) :

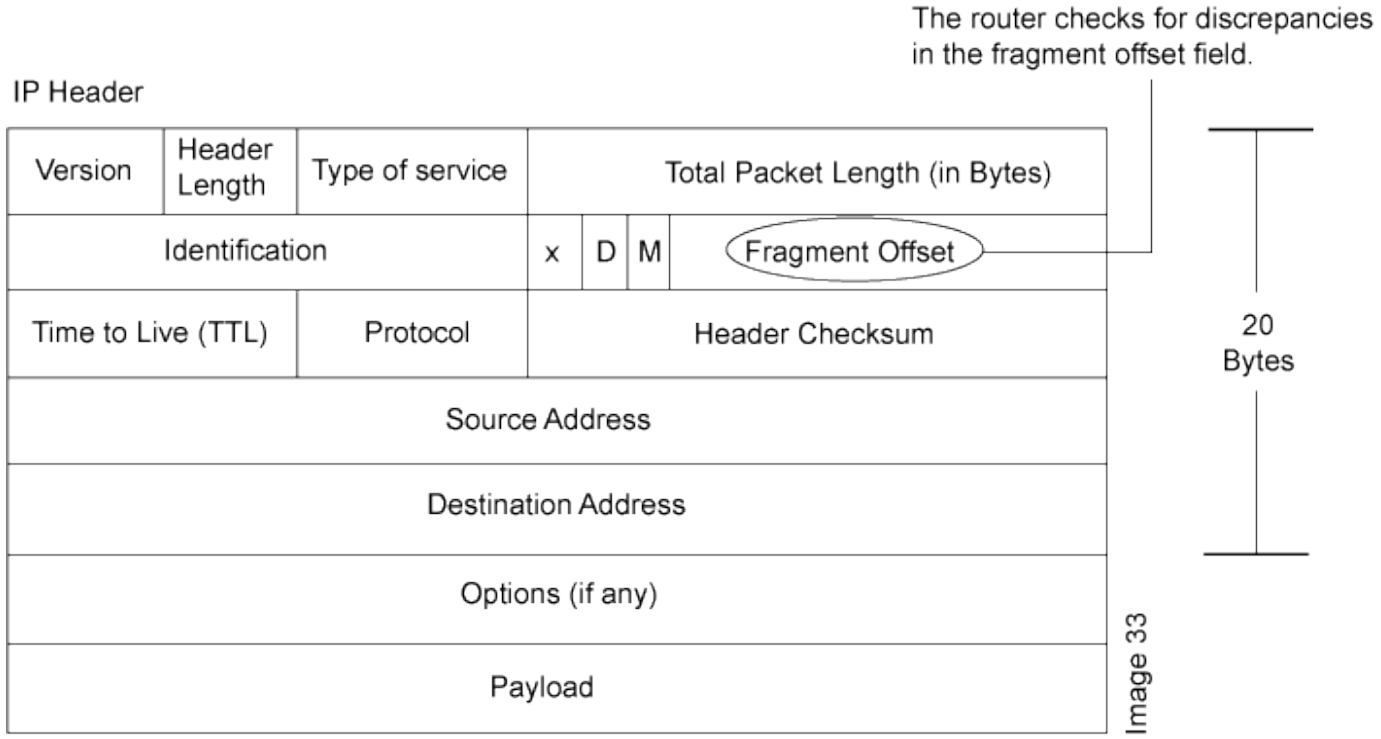


Image 33

Comme vous pouvez le voir dans la figure ci-dessus de l'en-tête IP, qui fonctionne au niveau de la couche réseau, il y a un champ appelé champ de décalage de fragment.

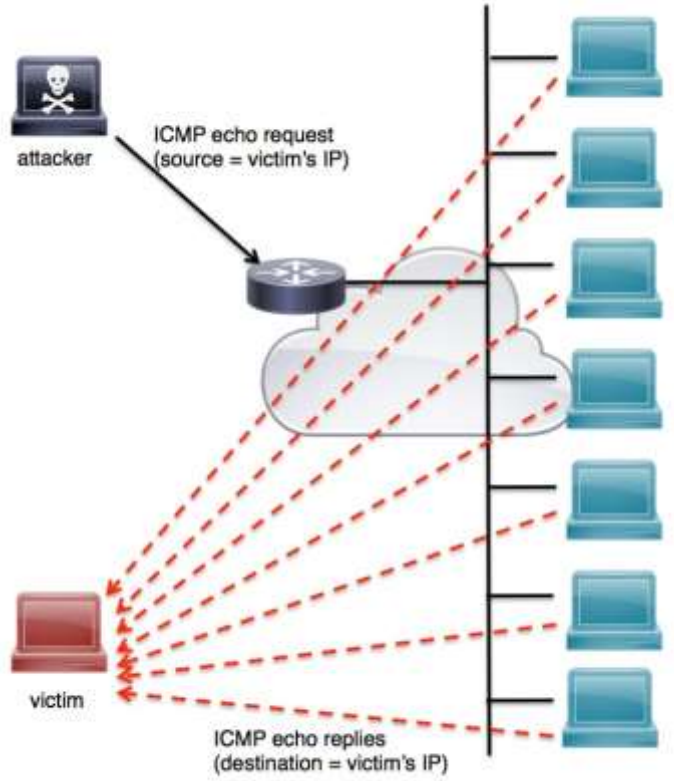
PARTIE 1

Les attaques par déni de service (DoS) et par déni de service distribué (DDoS):

- **Attaque Smurf**

Une attaque Smurf est une forme d'attaque par déni de service distribué (DDoS) qui se produit au niveau de la couche réseau. Les attaques de **Smurf** portent le nom **du malware DDoS.Smurf**, qui permet aux pirates de les exécuter. Plus largement, les attaques portent le nom des personnages de dessins animés **Les Schtroumpfs** en raison de leur capacité à éliminer des ennemis plus importants en travaillant ensemble.

Les attaques DDoS Smurf ont un style similaire aux inondations ping, qui sont une forme d'attaque par déni de service (DoS). Un pirate surcharge les ordinateurs avec des requêtes d'écho ICMP (Internet Control Message Protocol), également appelées pings. L'ICMP détermine si les données atteignent la destination prévue au bon moment et surveille la qualité de transmission des données par un réseau. Une attaque smurf envoie également des pings ICMP, mais elle est potentiellement plus dangereuse car elle peut exploiter les vulnérabilités du protocole Internet (IP) et de l'ICMP.



Si le routeur permet cela, il va transmettre le broadcast à tous les ordinateurs du réseau, qui vont répondre à l'ordinateur cible. La cible recevra donc un maximum de réponses au ping, saturant totalement sa bande passante...

PARTIE 1

PARTIE 1

Les attaques par déni de service (DoS) et par déni de service distribué (DDoS)

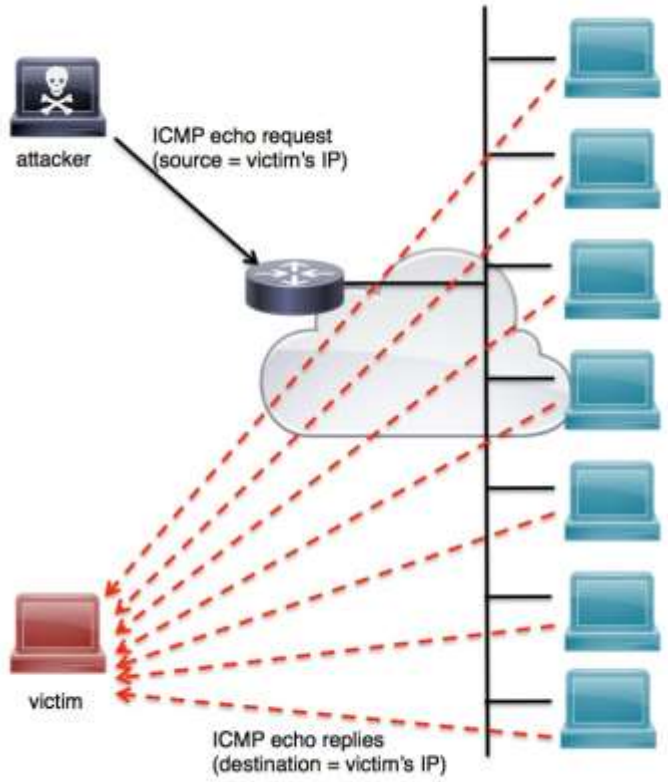
Attaque Smurf: Comment ça marche?

Une attaque ICMP pour Smurf est une forme d'attaque DDoS qui surcharge les ressources réseau en diffusant des requêtes d'écho ICMP aux appareils sur le réseau. Les appareils qui reçoivent la demande répondent par des réponses en écho, ce qui crée une situation de botnet qui génère un taux de trafic ICMP élevé.

En conséquence, le serveur est inondé de requêtes de données et de paquets ICMP, qui submergent le réseau informatique et le rendent inutilisable. Cela peut être particulièrement problématique pour les systèmes informatiques distribués, qui permettent aux appareils d'agir comme des environnements informatiques et permettent aux utilisateurs d'accéder aux ressources à distance.

Une attaque Smurf fonctionne selon le processus en trois étapes suivant :

1. Le logiciel malveillant DDoS.Smurf crée un paquet de données réseau qui s'attache à une fausse adresse IP. C'est ce qu'on appelle l'usurpation d'identité.
2. Le paquet contient un message ping ICMP, qui ordonne aux nœuds du réseau d'envoyer une réponse.
3. Ce processus, connu sous le nom d'échos ICMP, crée une boucle infinie qui submerge un réseau de demandes constantes.



Si le routeur permet cela, il va transmettre le broadcast à tous les ordinateurs du réseau, qui vont répondre à l'ordinateur cible. La cible recevra donc un maximum de réponses au ping, saturant totalement sa bande passante...

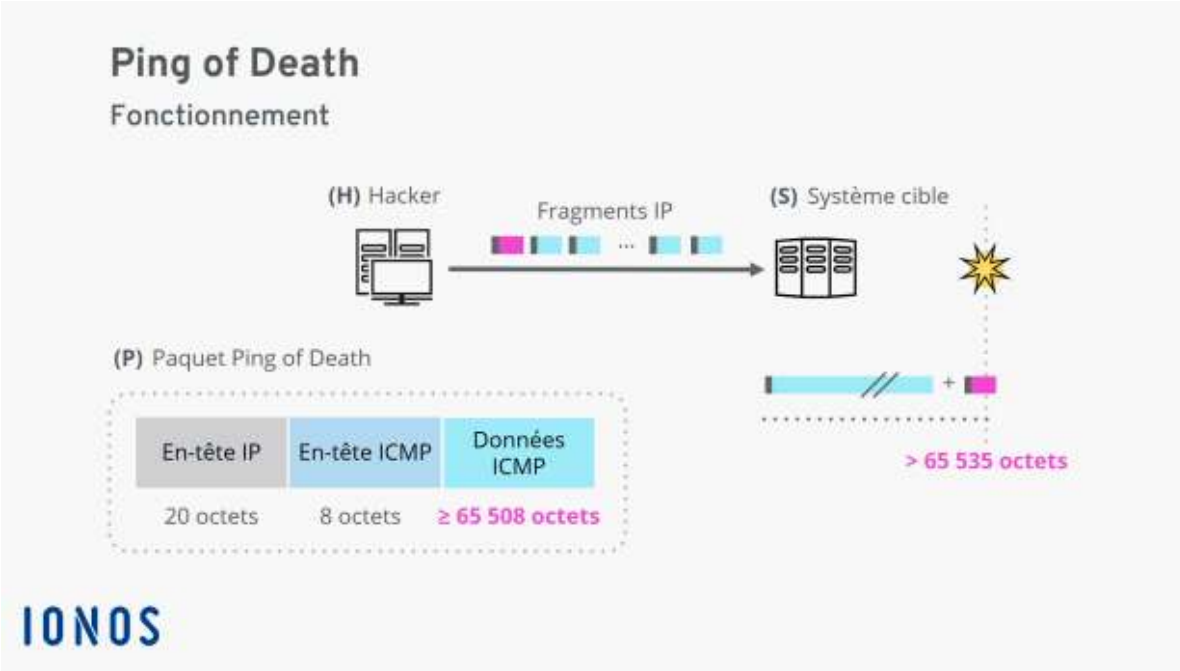
Les attaques par dénie de service (DoS) et par déni de service distribué (DDoS):

Ping de la mort

Le ping de la mort est une forme d'attaque par déni de service (DoS) qui se produit lorsqu'un attaquant plante, déstabilise ou gèle des ordinateurs ou des services en les ciblant avec des paquets de données surdimensionnés. Cette forme d'attaque DoS cible et exploite généralement les faiblesses héritées que les organisations peuvent avoir corrigées.

Les systèmes non corrigés sont également exposés aux inondations ping, qui ciblent les systèmes en les surchargeant de messages ping ICMP (Internet Control Message Protocol).

Les ordinateurs utilisent un système de message de réponse en écho ICMP, connu sous le nom de "ping", pour tester les connexions réseau. Le système agit comme un sonar entre les appareils. Il envoie une impulsion, qui émet un écho pour fournir à un opérateur des informations sur l'environnement du réseau. Lorsque la connexion fonctionne comme prévu, les machines sources reçoivent une réponse des machines cibles, ce qui est fréquemment utilisé par les ingénieurs. Les commandes Ping sont limitées à une taille maximale de 65 535 octets.



Le hacker attaque le système cible avec un paquet de données ingénieusement conçu.
Source Ping of death : un modèle d'attaque du début d'Internet - IONOS

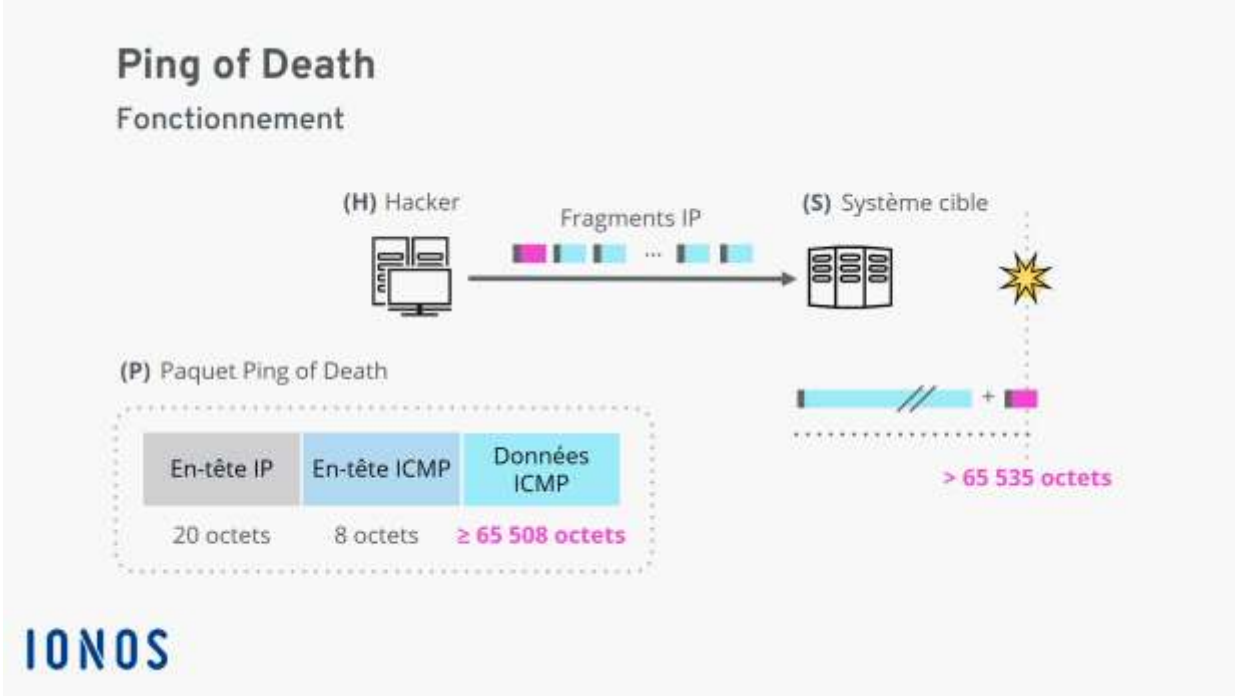
PARTIE 1

Les attaques par dénie de service (DoS) et par déni de service distribué (DDoS):

Ping de la mort : Comment ça marche ?

Un paquet IPv4 (Internet Protocol version 4) correct est composé de 65 535 octets et la plupart des ordinateurs ne peuvent pas gérer des paquets plus volumineux. Les attaquants utilisent des commandes ping pour développer une commande **Ping of Death**. Ils peuvent écrire une boucle simple qui leur permet d'exécuter la commande ping avec des tailles de paquets dépassant le niveau maximum de 65 535 octets lorsque la machine cible tente de reconstituer les fragments. Le réassemblage de ces paquets entraîne un paquet surdimensionné qui peut provoquer le plantage, le blocage ou le redémarrage du système.

La vulnérabilité peut être exploitée par toute source qui envoie des datagrammes IP, qui incluent un écho ICMP, Internetwork Packet Exchange (IPX), Transmission Control Protocol (TCP) et User Datagram Protocol (UDP).



Le hacker attaque le système cible avec un paquet de données ingénieusement conçu.
Source Ping of death : un modèle d'attaque du début d'Internet - IONOS

PARTIE 1

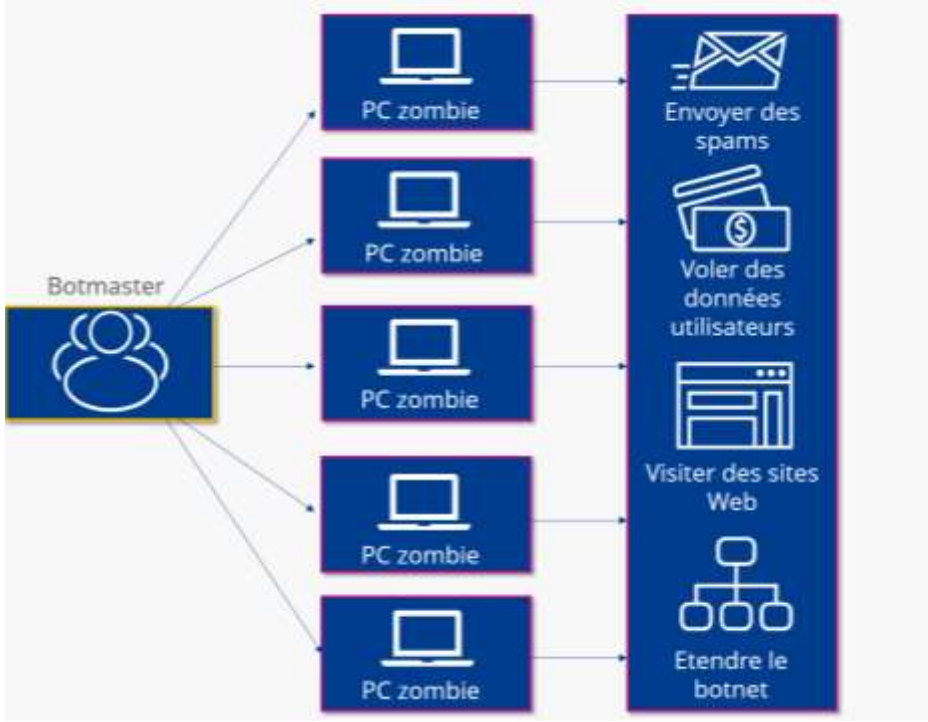
Les attaques par dénie de service (DoS) et par déni de service distribué (DDoS):

Botnets

Une attaque Botnet est une cyberattaque à grande échelle menée par des appareils infectés par des logiciels malveillants qui sont contrôlés à distance.

Il transforme les appareils compromis en « robots zombies » pour un contrôleur Botnet. Contrairement à d'autres logiciels malveillants qui se reproduisent sur une seule machine ou un seul système, les botnets constituent une menace plus importante car ils permettent à un acteur malveillant d'effectuer un grand nombre d'actions en même temps. Les attaques de botnet s'apparentent à la présence d'un acteur menaçant au sein du réseau, par opposition à un logiciel malveillant autoréplicatif.

Les attaquants utilisent les botnets pour compromettre les systèmes, distribuer des logiciels malveillants et recruter de nouveaux appareils pour le clan. Une attaque de botnet peut être principalement destinée à perturber ou à ouvrir la voie pour lancer une attaque secondaire.



Les botnets sont dirigés par un botmaster qui répartit les tâches de routine entre les PC zombies : ces tâches peuvent consister à envoyer des spams, voler des données utilisateur, visiter et analyser des sites Internet ainsi qu'à étendre le botnet.

PARTIE 1

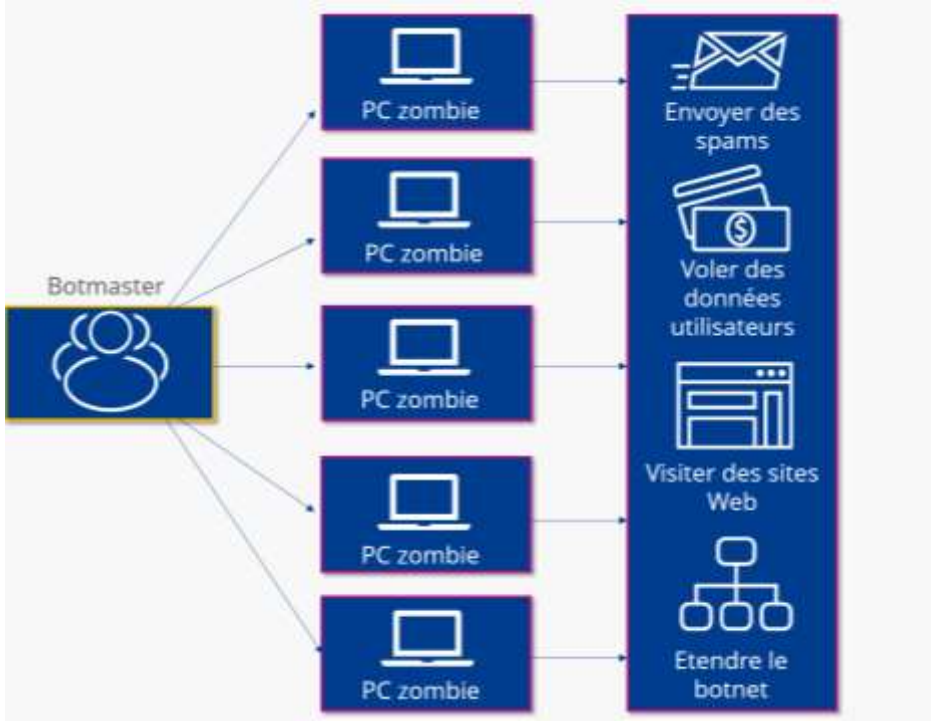
Les attaques par dénie de service (DoS) et par déni de service distribué (DDoS):

Botnets: Comment ça marche?

Les attaques de botnet commencent par les cybercriminels qui accèdent aux appareils en compromettant leur sécurité. Ils pourraient le faire via des hacks comme l'injection de **virus cheval de Troie** ou des **tactiques d'ingénierie sociale de base**.

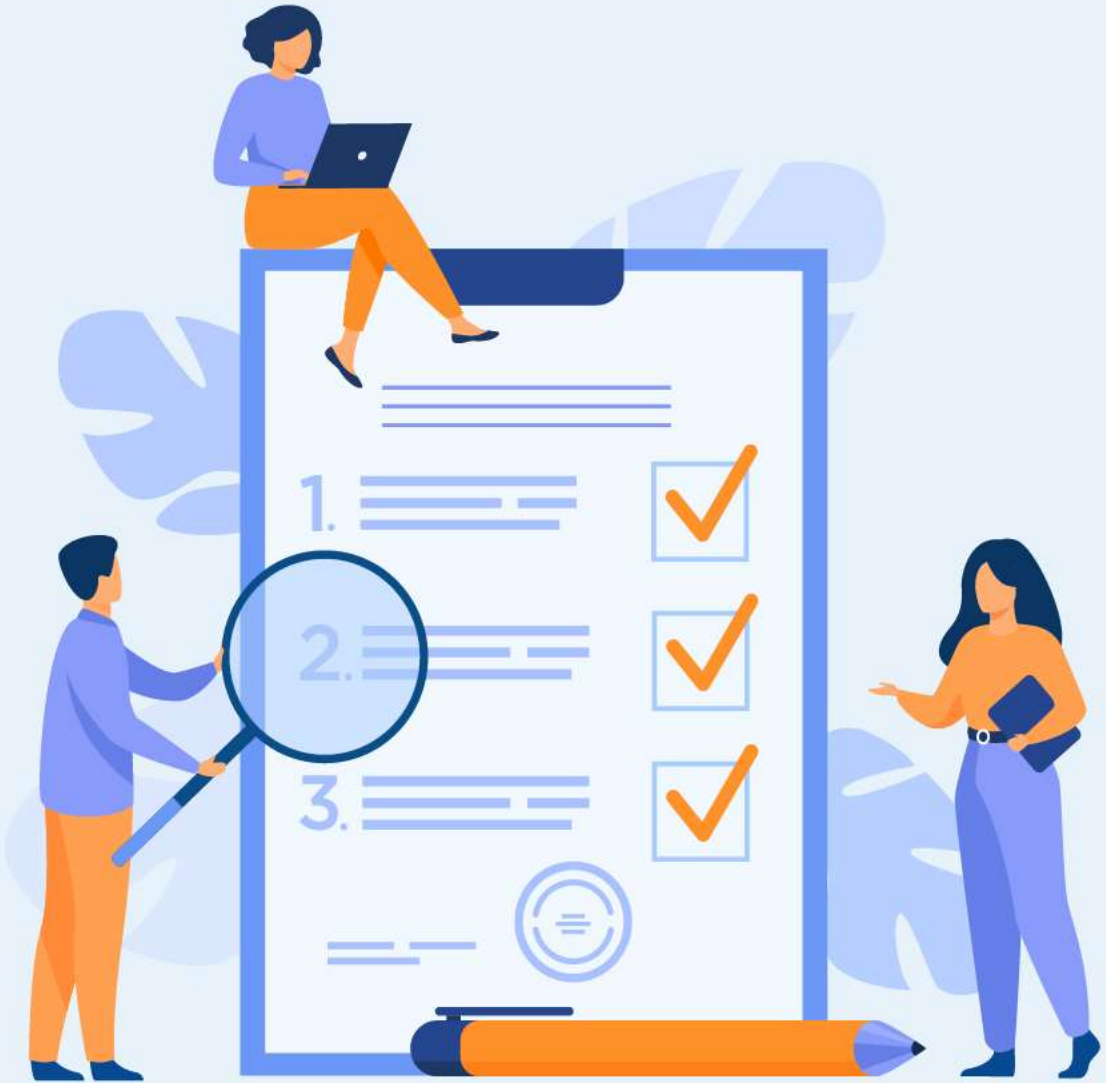
Ensuite, ces appareils sont maîtrisés à l'aide d'un logiciel qui ordonne aux appareils de mener des attaques à grande échelle.

Parfois, les attaquants eux-mêmes n'utilisent pas le botnet pour lancer des attaques, mais vendent plutôt l'accès au réseau à d'autres acteurs malveillants. Ces tiers peuvent alors utiliser le botnet comme un réseau « zombie » pour leurs propres besoins, comme diriger des campagnes de spam.



Les botnets sont dirigés par un botmaster qui répartit les tâches de routine entre les PC zombies : ces tâches peuvent consister à envoyer des spams, voler des données utilisateur, visiter et analyser des sites Internet ainsi qu'à étendre le botnet.

PARTIE 1



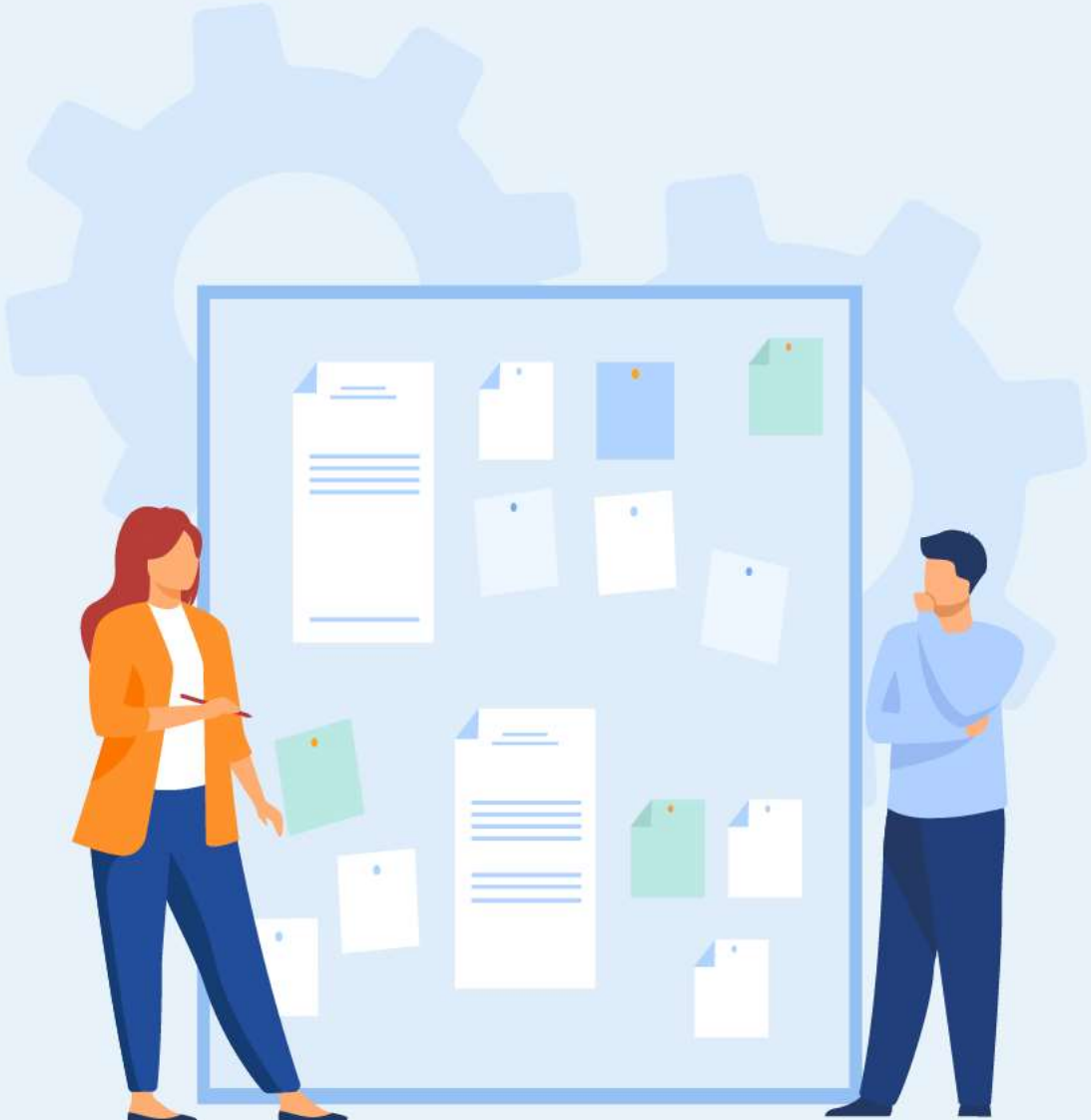
CHAPITRE 3

Se prémunir d’une quelconque tentative de piratage

Ce que vous allez apprendre dans ce chapitre :

- Techniques de protection
- Notion des Antivirus
- Notion des firewalls

02 heures



CHAPITRE 3

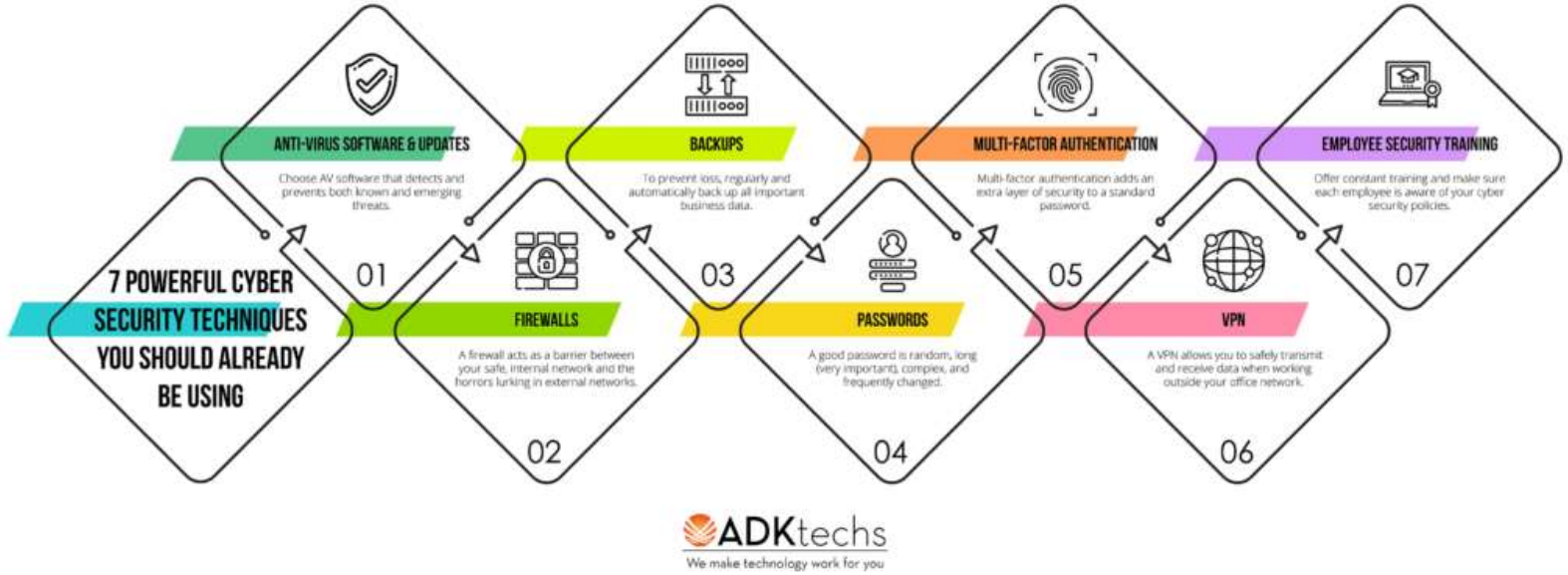
Se prémunir d’une quelconque tentative de piratage

1. **Techniques de protection**
2. Notion des Antivirus
3. Notion des firewalls

Appliquer des pratiques de sécurité solides :

La protection d'un système contre les cyberattaques peut prendre différentes formes. De la création de mots de passe forts à l'utilisation de logiciels de cybersécurité sophistiqués, la liste est longue. Nous allons donc énumérer certaines des techniques les plus efficaces pour protéger un système contre différentes cyberattaques.

La protection d'un système contre les cyberattaques peut prendre différentes formes. De la création de mots de passe forts à l'utilisation de logiciels de cybersécurité sophistiqués, la liste est longue. Nous allons donc énumérer certaines des techniques les plus efficaces pour protéger un système contre différentes cyberattaques.



7 puissantes techniques de cybersécurité qu'un système devrait déjà utiliser
Source 7 Powerful Cyber Security Techniques You Should Already Be Using - ADKtechs

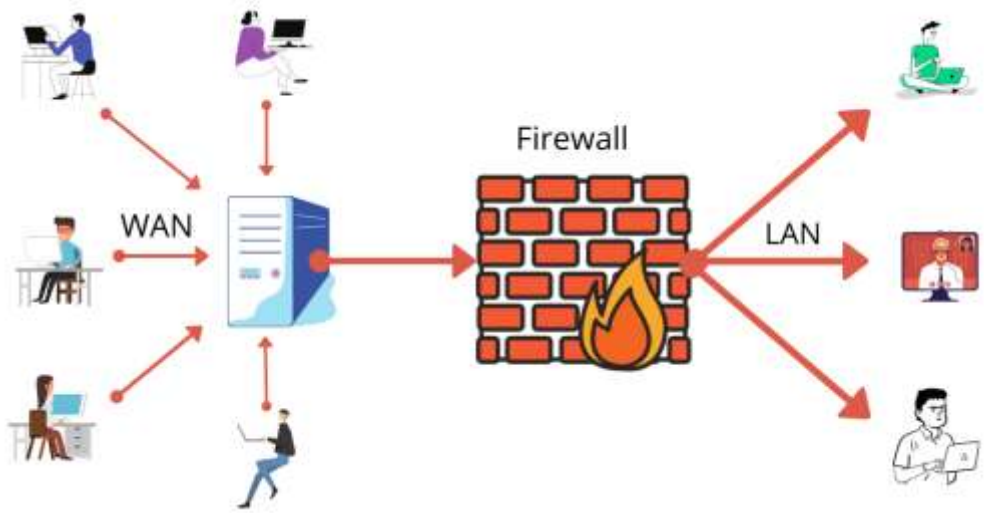
Mises à jour des logiciels anti-virus

Face à l'énorme tâche que représente la sécurisation de votre entreprise, il est facile d'oublier l'essentiel. Vous voulez un logiciel AV qui détecte et prévient les menaces connues et émergentes.

Mais ne vous contentez pas de télécharger n'importe quel logiciel AV gratuit que vous trouvez en ligne.

N'installez qu'un programme antivirus provenant d'une source fiable et légitime et maintenez-le (ainsi que votre ordinateur) toujours à jour.

Les mises à jour et les correctifs pour vos applications et appareils vous garantissent la protection la plus complète.



Un pare-feu réseau est basé sur des règles de sécurité pour accepter, rejeter ou déposer un trafic spécifique. Le but du pare-feu est d'autoriser ou de refuser la connexion ou la demande, en fonction des règles implémentées.

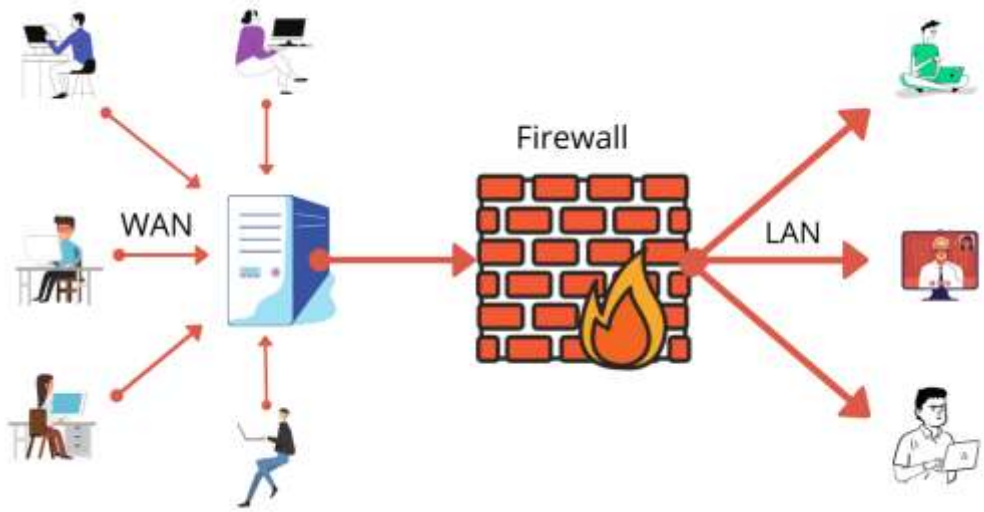
Pare-feu (Firewall)

Un pare-feu agit comme une barrière entre votre réseau interne sécurisé et les horreurs qui se cachent dans les réseaux externes.

Les pare-feu filtrent le trafic entrant et sortant en fonction d'un ensemble de règles de sécurité.

Ils constituent une protection essentielle pour les petites et grandes entreprises, ainsi que pour les réseaux domestiques.

Il est préférable d'opter pour un pare-feu de nouvelle génération qui, comme son nom l'indique, offre des fonctionnalités plus avancées qu'un pare-feu traditionnel. Vous pouvez en savoir plus dans la vidéo ci-dessus.



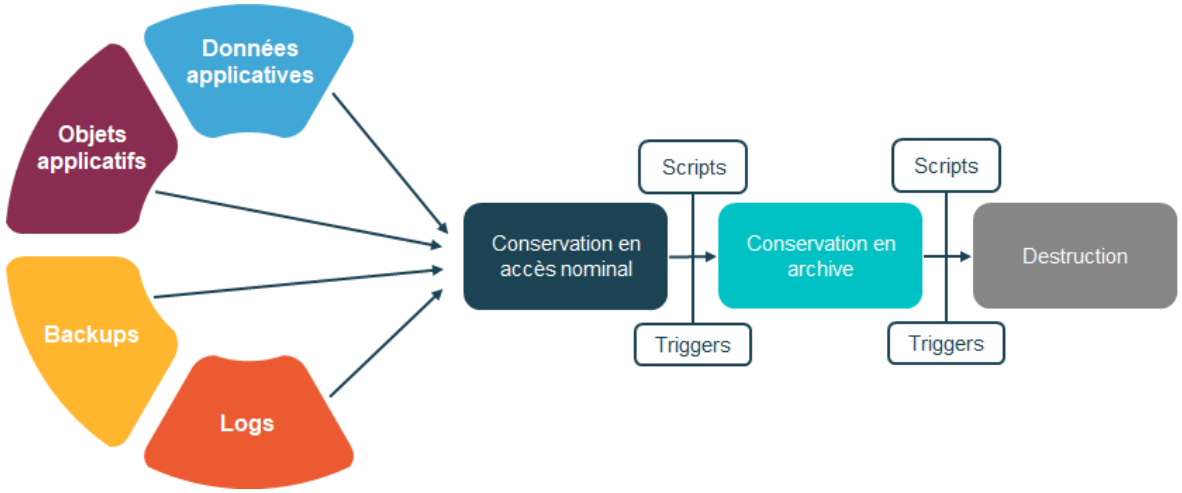
Un pare-feu réseau est basé sur des règles de sécurité pour accepter, rejeter ou déposer un trafic spécifique. Le but du pare-feu est d'autoriser ou de refuser la connexion ou la demande, en fonction des règles implémentées.

Sauvegardes

Sauvegarder régulièrement et automatiquement toutes les données importantes de l'entreprise.

Il est suggéré de sauvegarder tous les documents de traitement de texte, les feuilles de calcul électroniques, les bases de données, les fichiers financiers, les fichiers de ressources humaines et les fichiers de comptes débiteurs/payeurs.

Veillez à les stocker dans le cloud ou hors site. En cas d'attaque par ransomware, de catastrophe naturelle ou de défaillance d'un appareil, vous ne perdrez pas tout.



Processus high-level pour la politique de sauvegarde et purge des donnéesCe mécanisme global fera parti des bonnes pratiques de l'entreprise pour que chaque nouvelle solution développée intègre cette politique.

Source: [Politique de sauvegarde des données - FinOps.World]

PARTIE 1

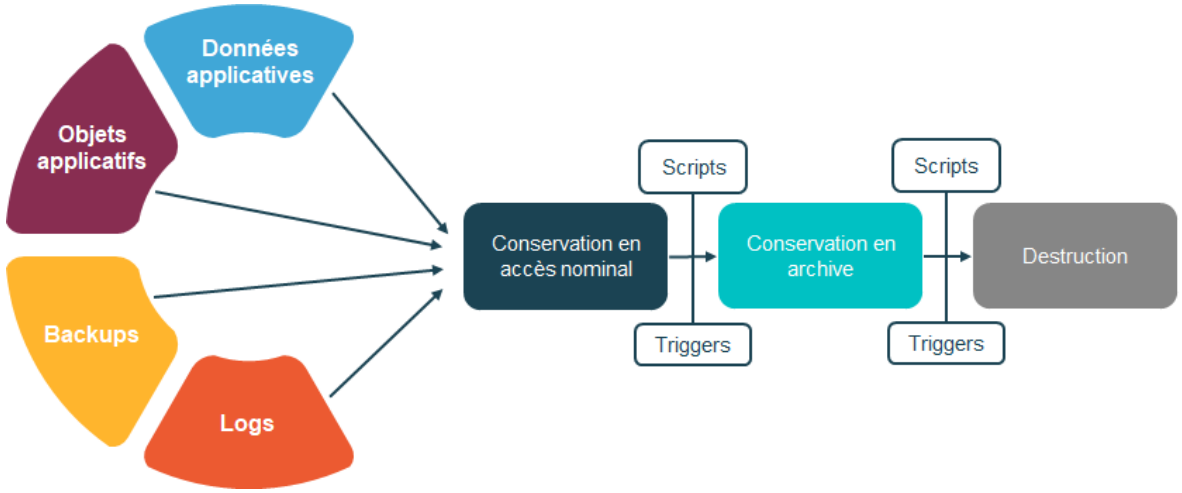
Mots de passe

Les mots de passe peuvent être un moyen simple et efficace d'éloigner les cybercriminels.

Un bon mot de passe est aléatoire, long (très important), complexe et fréquemment modifié.

Les ‘’passphrases’’ sont également utiles et parfois plus faciles à retenir qu'une chaîne aléatoire de lettres/chiffres/caractères spéciaux.

L’utilisateur peut utiliser un gestionnaire de mots de passe pour conserver la trace de tous les mots de passe.



Processus high-level pour la politique de sauvegarde et purge des donnéesCe mécanisme global fera parti des bonnes pratiques de l'entreprise pour que chaque nouvelle solution développée intègre cette politique.

Source: [Politique de sauvegarde des données - FinOps.World]

PARTIE 1

Authentification multi-facteurs

L'authentification multifactorielle (AMF), ou authentification à deux facteurs, ajoute une couche de sécurité supplémentaire à un mot de passe standard. L'AMF est une combinaison de deux ou plusieurs des éléments suivants :

- Quelque chose que vous avez (comme un code généré de manière aléatoire envoyé sur votre téléphone portable).
- Quelque chose que vous êtes (comme une empreinte digitale)
- Quelque chose que vous connaissez (comme un mot de passe)

L'AMF réduit le risque de piratage. Si un cybercriminel connaît votre mot de passe mais que la fonction AMF est activée, il est peu probable qu'il ait également accès au code que votre appareil mobile a reçu, ce qui l'empêchera d'accéder à votre compte.

Contrôler l'accès aux données et aux systèmes

Assurez-vous que les personnes ne peuvent accéder qu'aux données et services pour lesquels elles sont autorisées. Par exemple, vous pouvez

- contrôler l'accès physique aux locaux et au réseau d'ordinateurs
- restreindre l'accès aux utilisateurs non autorisés
- limiter l'accès aux données ou aux services par des contrôles d'application
- limiter ce qui peut être copié du système et enregistré sur des dispositifs de stockage
- limiter l'envoi et la réception de certains types de pièces jointes aux courriels.

Les systèmes d'exploitation et les logiciels de réseau modernes vous aideront à réaliser la plupart de ces objectifs, mais vous devrez gérer l'enregistrement des utilisateurs et les systèmes d'authentification des utilisateurs, par exemple les mots de passe. Pour plus d'informations, lisez l'introduction du NCSC sur l'identité et l'accès.

Crypter toutes les données commerciales et les informations relatives aux clients

Veillez à ce que toutes les données relatives à l'entreprise et aux clients soient fortement cryptées. Ainsi, si elles sont exposées, il y a moins de chances que les cybercriminels puissent accéder aux informations relatives aux clients ou aux secrets commerciaux dans le cadre de l'espionnage d'entreprise.

Appliquer des pratiques de sécurité solides

Veillez à ce que chaque niveau de votre organisation utilise des mots de passe forts et des gestionnaires de mots de passe afin de réduire le risque qu'un mot de passe divulgué ou craqué donne lieu à un accès non autorisé. En outre, sensibilisez vos employés aux escroqueries par hameçonnage et à la nécessité de ne pas télécharger les pièces jointes des courriels provenant d'expéditeurs inconnus.

VPN

Le WiFi public est risqué et l'utilisation d'un réseau public pour accéder à des comptes professionnels privés met toute votre organisation en danger. Lorsque vous utilisez le WiFI public, tout ce que vous faites est à la vue de tous. Un réseau privé virtuel (VPN) est un outil formidable lorsque vous travaillez en dehors du réseau sécurisé de votre bureau ; il vous permet de transmettre et de recevoir des données en toute sécurité.

Information

Le cryptage peut protéger les données des yeux indésirables. Il peut fournir une sécurité des données efficace, mais la plupart des utilisateurs n'en sont pas conscients.

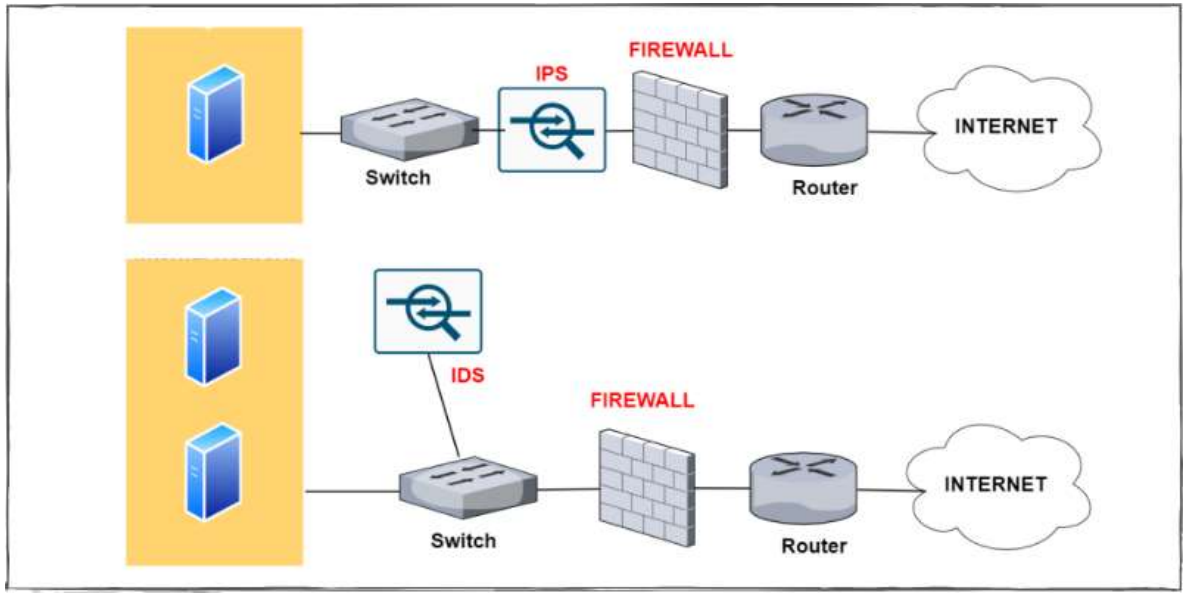
Source (Comment crypter des fichiers pour protéger les données personnelles et professionnelles? (geekflare.com)

PARTIE 1

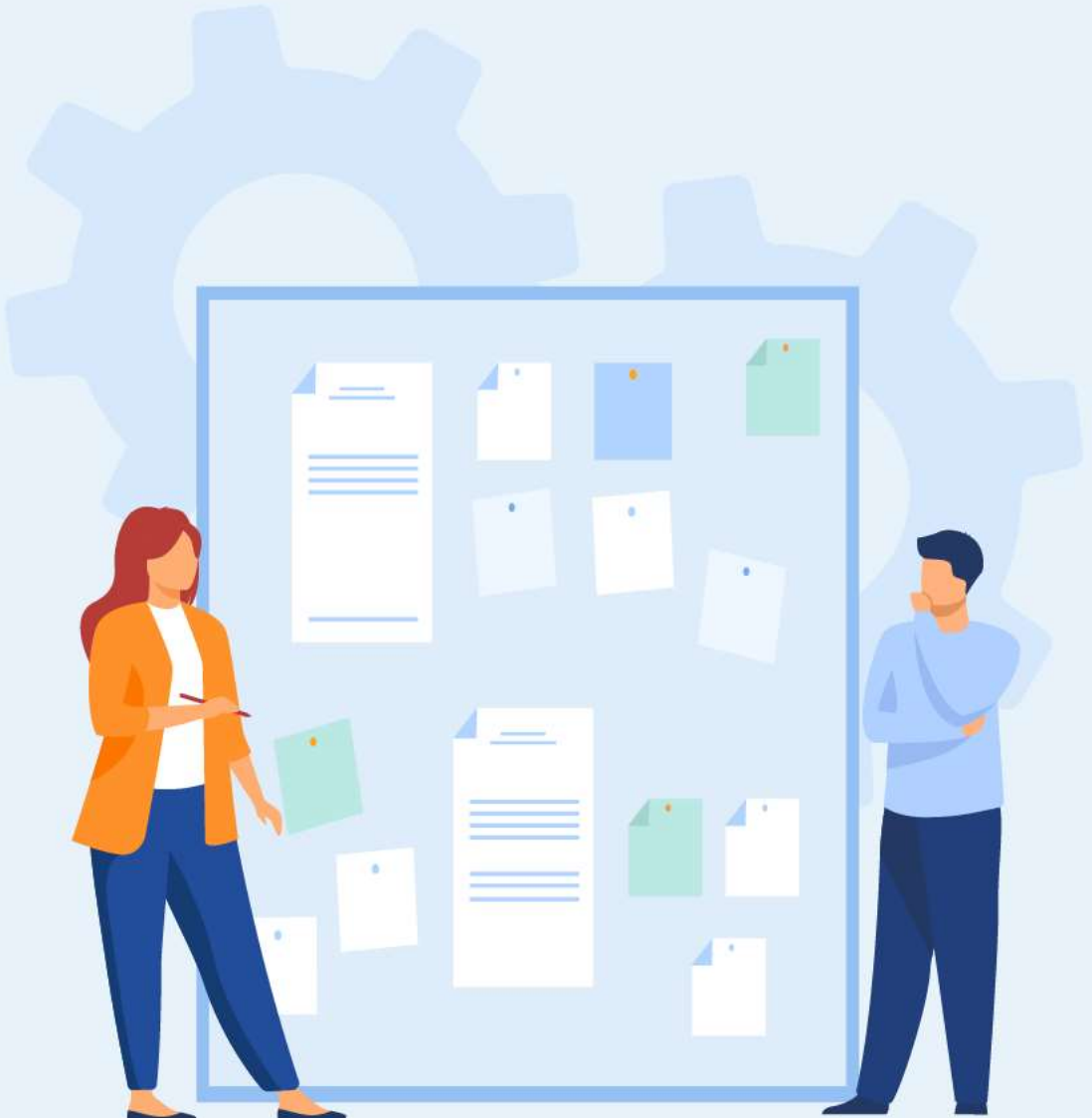
IDS et IPS

Un système de détection des intrusions (IDS) surveille le trafic sur votre réseau, analyse ce trafic à la recherche de signatures correspondant à des attaques connues, et lorsque quelque chose de suspect se produit, vous êtes alerté. Pendant ce temps, le trafic continue à circuler.

Un système de prévention des intrusions (IPS) surveille également le trafic. Mais lorsque quelque chose d'inhabituel se produit, le trafic s'arrête complètement jusqu'à ce que vous enquêtiez et décidiez de rouvrir les vannes.



l'IPS est généralement connecté derrière le pare-feu mais en ligne avec le chemin de communication qui transmet les paquets vers/depuis le réseau interne. Il est placé ici pour bloquer le trafic malveillant juste avant d'atteindre les serveurs internes.
L'IDS, par contre, il est place hors flux de trafic. Dans ce cas, le trafic passant par le commutateur est également envoyé en même temps à l'IDS pour inspection. Si une anomalie de sécurité est détectée dans le trafic réseau, l'IDS déclenchera simplement une alarme (à l'administrateur) mais il ne pourra pas bloquer le trafic.



CHAPITRE 3

Se prémunir d’une quelconque tentative de piratage

1. Techniques de protection
2. **Notion des Antivirus**
3. Notion des firewalls

03 - Se prémunir d'une quelconque tentative de piratage

Notion des Antivirus

Définition

Logiciel créé spécifiquement pour aider à détecter, prévenir et supprimer les logiciels malveillants (malware).

L'antivirus est un type de logiciel utilisé pour prévenir, analyser, détecter et supprimer les virus d'un ordinateur. Une fois installés, la plupart des logiciels antivirus s'exécutent automatiquement en arrière-plan pour fournir une protection en temps réel contre les attaques de virus.

Les programmes complets de protection contre les virus aident à protéger vos fichiers et votre matériel contre les logiciels malveillants tels que les vers ***(warms)***, les chevaux de Troie et les logiciels espions, et peuvent également offrir une protection supplémentaire telle que des pare-feu personnalisables et le blocage de sites Web.

Exemple des Antivirus les plus connus

PARTIE 1

Programmes antivirus et logiciels de protection des ordinateurs

Les programmes antivirus et les logiciels de protection de l'ordinateur sont conçus pour évaluer les données telles que les pages Web, les fichiers, les logiciels et les applications afin d'aider à trouver et à éradiquer les logiciels malveillants le plus rapidement possible.

La plupart offrent une protection en temps réel, ce qui permet de protéger vos appareils contre les menaces entrantes, d'analyser régulièrement l'ensemble de votre ordinateur à la recherche de menaces connues et de fournir des mises à jour automatiques, et d'identifier, de bloquer et de supprimer les codes et logiciels malveillants.

Exemple des Antivirus les plus connus

PARTIE 1

03 - Se prémunir d'une quelconque tentative de piratage

Notion des Antivirus

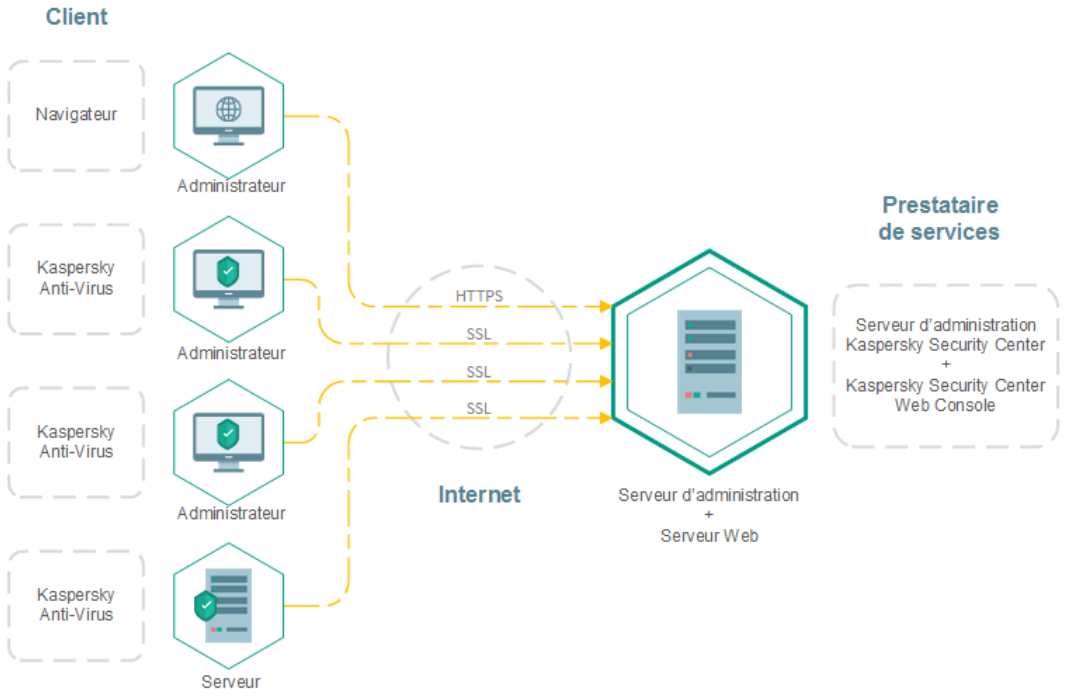
Comment fonctionne un antivirus ?

Un logiciel antivirus commence à fonctionner en vérifiant les programmes et les fichiers de votre ordinateur par rapport à une base de données de types de logiciels malveillants connus. Étant donné que de nouveaux virus sont constamment créés et distribués par les pirates, il analyse également les ordinateurs pour détecter les menaces de type nouveau ou inconnu.

La plupart des programmes utilisent trois dispositifs de détection différents :

- ***La détection spécifique, qui identifie les logiciels malveillants connus***
- ***La détection générique, qui recherche des parties ou des types de logiciels malveillants connus ou des modèles liés par une base de code commune***
- ***La détection heuristique, qui recherche les virus inconnus en identifiant les structures de fichiers suspectes connues***

Lorsque le programme trouve un fichier contenant un virus, il le met généralement en quarantaine et/ou le marque pour suppression, le rendant inaccessible et éliminant le risque pour votre appareil.



Mode de fonctionnement de Kaspersky Security Center 10 Web Console
Kaspersky Security Center 10 Web Console communique avec le Serveur d'administration de Kaspersky Security Center qui se trouve sur les serveurs du fournisseur de services de protection. Le Serveur d'administration est une application qui sert à administrer les applications de Kaspersky Lab installées sur les appareils de votre réseau. Le Serveur d'administration contacte les appareils de votre réseau via les canaux sécurisés des liaisons (SSL).

Resource: Kaspersky Security Center 10 Web Console

PARTIE 1

Types d’antivirus

Antivirus en Cloud:

Ce type d'antivirus est très puissant et analyse les données dans le nuage pour finalement envoyer la commande nécessaire à l'ordinateur. Ce logiciel antivirus est composé de deux parties : le client installé sur l'ordinateur et le service web, chacun ayant ses propres tâches.

Types d’antivirus

Logiciel autonome

Ce type d'antivirus est conçu pour combattre des virus spécifiques car il est spécialisé. L'une des caractéristiques de ce type d'antivirus est que vous pouvez l'utiliser même en cas d'urgence, car il peut également être installé sur une clé USB et utilisé pour rechercher les virus.

Cette caractéristique a incité de nombreux utilisateurs à utiliser ce type d'antivirus.

Certains logiciels antivirus de ce type n'ont pas besoin d'être installés, et il suffit de télécharger le fichier complet et de procéder à l'analyse, mais certains d'entre eux doivent être installés.

De nombreux logiciels antivirus font partie de ce type, y compris **Kaspersky Virus Removal Tool**, **Microsoft Safety Scanner**, **Avira PC Cleaner**, **Windows Defender Offline**, etc, a souligné que chacun d'entre eux a ses caractéristiques que les utilisateurs devraient le choisir en fonction de leur objectif.

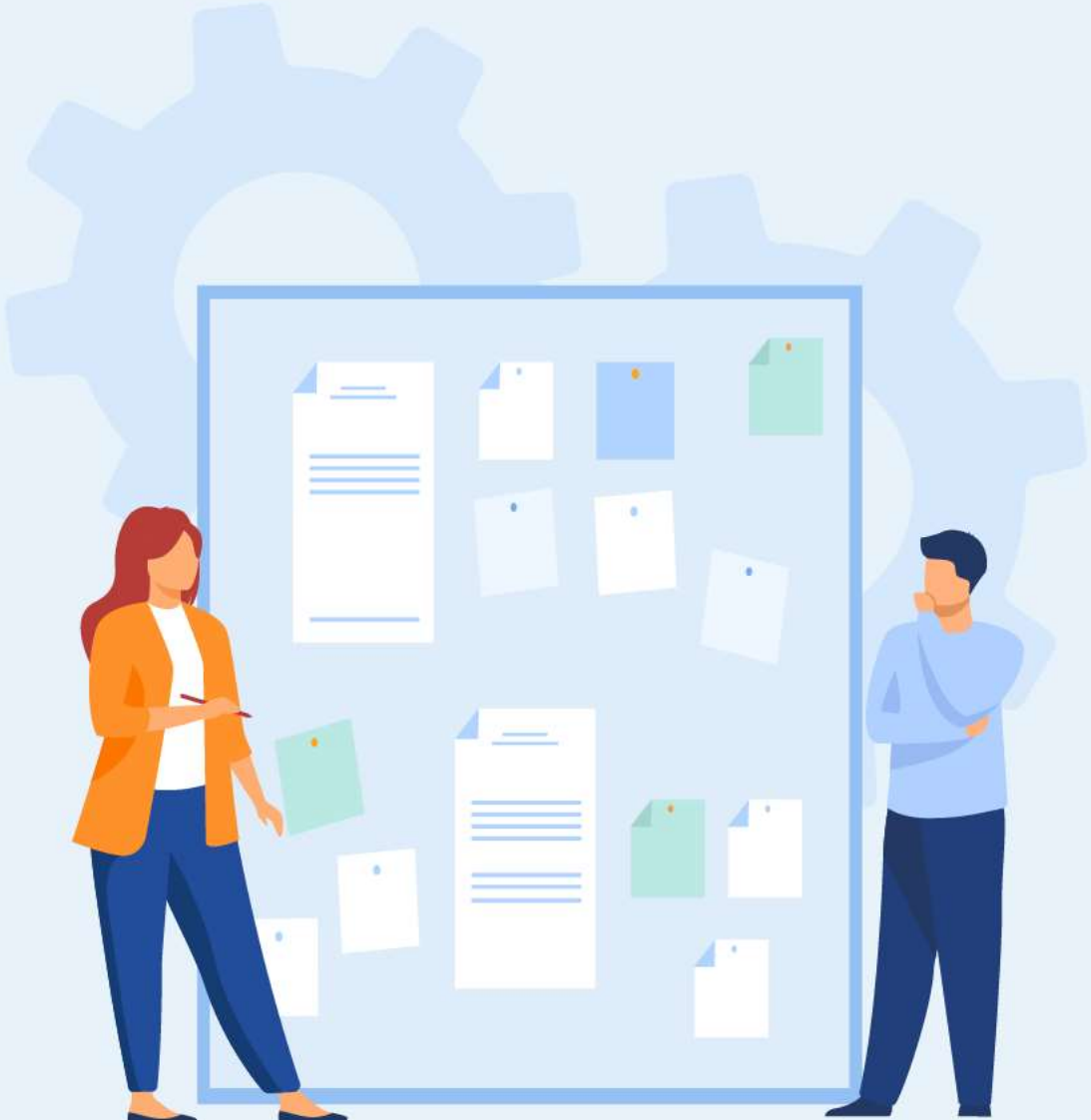
Types d’antivirus

Suites logicielles de sécurité:

Ce type peut aller bien au-delà des programmes antivirus, et en plus d'être capable d'analyser tous les virus, ils ont plus de capacités qui peuvent grandement sécuriser votre système.

L'une des caractéristiques de ce type est qu'il dispose de programmes de contrôle parental, ce qui amène de nombreux parents inquiets pour leurs enfants à se faire aider par ce type. En plus des capacités que nous avons mentionnées, ce type a d'autres capacités telles que l'authentification du site, la sauvegarde, etc.

Les meilleurs logiciels antivirus qui font partie de ce type sont Bitdefender Total Security, **Norton 360 Deluxe, Avast Ultimate, McAfee Total Protection Multi-Device, Kaspersky Total Security, etc.**



CHAPITRE 3

Se prémunir d’une quelconque tentative de piratage

1. Techniques de protection
2. Notion des Antivirus
3. **Notion des firewalls**

03 - Se prémunir d’une quelconque tentative de piratage

Notion des firewalls

Définition

Un pare-feu est un dispositif de sécurité réseau qui surveille le trafic réseau entrant et sortant et autorise ou bloque les paquets de données en fonction d'un ensemble de règles de sécurité. Son but est d'établir une barrière entre votre réseau interne et le trafic entrant provenant de sources externes (comme l'internet) afin de bloquer le trafic malveillant comme les virus et les pirates.

Que font les pare-feu ?

Un pare-feu est un élément indispensable de toute architecture de sécurité. Il élimine les incertitudes liées aux protections au niveau de l'hôte et les confie à votre dispositif de sécurité réseau. Les pare-feu, et en particulier les pare-feu de nouvelle génération, se concentrent sur le blocage des logiciels malveillants et des attaques au niveau de la couche applicative, ainsi que sur un système intégré de prévention des intrusions (IPS). Ces pare-feu de nouvelle génération peuvent réagir rapidement et de manière transparente pour détecter et réagir aux attaques extérieures sur l'ensemble du réseau. Ils peuvent définir des politiques pour mieux défendre votre réseau et effectuer des évaluations rapides pour détecter les activités invasives ou suspectes, comme les logiciels malveillants, et les arrêter.

Pourquoi avons-nous besoin de pare-feu ?

Les pare-feu, en particulier les pare-feu de nouvelle génération, se concentrent sur le blocage des logiciels malveillants et des attaques au niveau des applications. Associés à un système intégré de prévention des intrusions (IPS), ces pare-feu de nouvelle génération sont capables de réagir rapidement et de manière transparente pour détecter et combattre les attaques sur l'ensemble du réseau. Les pare-feu peuvent agir sur des politiques préalablement définies pour mieux protéger votre réseau et effectuer des évaluations rapides pour détecter les activités invasives ou suspectes, comme les logiciels malveillants, et les arrêter. En utilisant un pare-feu pour votre infrastructure de sécurité, vous configurez votre réseau avec des politiques spécifiques pour autoriser ou bloquer le trafic entrant et sortant.

Histoire du pare-feu

Les pare-feu existent depuis la fin des années 1980 et ont commencé par être des filtres de paquets, c'est-à-dire des réseaux configurés pour examiner les paquets, ou octets, transférés entre ordinateurs. Bien que les pare-feu à filtrage de paquets soient encore utilisés aujourd'hui, les pare-feu ont parcouru un long chemin au fur et à mesure que la technologie s'est développée au fil des décennies.

- **Génération 1 : Virus**
  - Génération 1, fin des années 1980, les attaques de virus sur les PC autonomes ont touché toutes les entreprises et ont donné naissance aux produits antivirus.
- **Génération 2 : Réseaux**
  - Génération 2, milieu des années 1990, les attaques de l'Internet ont affecté toutes les entreprises et ont conduit à la création du pare-feu.
- **Génération 3 : Applications**
  - Génération 3, début des années 2000, l'exploitation des vulnérabilités dans les applications a touché la plupart des entreprises et a conduit à la création des systèmes de prévention des intrusions (IPS).
- **Génération 4 : Charge utile**
  - Génération 4, vers 2010, augmentation des attaques ciblées, inconnues, évasives et polymorphes qui ont affecté la plupart des entreprises et ont conduit à la création de produits anti-bots et de sandboxing.
- **Génération 5 : Méga**
  - Génération 5, vers 2017, méga-attaques à grande échelle, multi-vecteurs, utilisant des outils d'attaque avancés, et entraînant des solutions avancées de prévention des menaces.

Types de pare-feu

Les pare-feu peuvent être logiciels ou matériels, mais il est préférable d'avoir les deux. Un pare-feu logiciel est un programme installé sur chaque ordinateur et qui régule le trafic par le biais de numéros de port et d'applications, tandis qu'un pare-feu physique est une pièce d'équipement installée entre votre réseau et la passerelle.

Les différents types de pares-feux

Types de pare-feu

Les pare-feu de filtrage de paquets, le type de pare-feu le plus courant, examinent les paquets et les empêchent de passer s'ils ne correspondent pas à un ensemble de règles de sécurité établies. Ce type de pare-feu vérifie les adresses IP source et destination des paquets.

Si les paquets correspondent à ceux d'une règle "autorisée" du pare-feu, ils sont autorisés à entrer sur le réseau.

Types de pare-feu

Les pare-feu filtrant les paquets sont divisés en deux catégories :

- Les pare-feu sans état examinent les paquets indépendamment les uns des autres et manquent de contexte, ce qui en fait des cibles faciles pour les pirates.
- Les pare-feu avec état se souviennent des informations sur les paquets passés précédemment et sont considérés comme beaucoup plus sûrs.

Si les pare-feu filtrant les paquets peuvent être efficaces, ils n'offrent en fin de compte qu'une protection de base et peuvent être très limités. Par exemple, ils ne peuvent pas déterminer si le contenu de la requête envoyée aura un effet négatif sur l'application à laquelle elle est destinée.

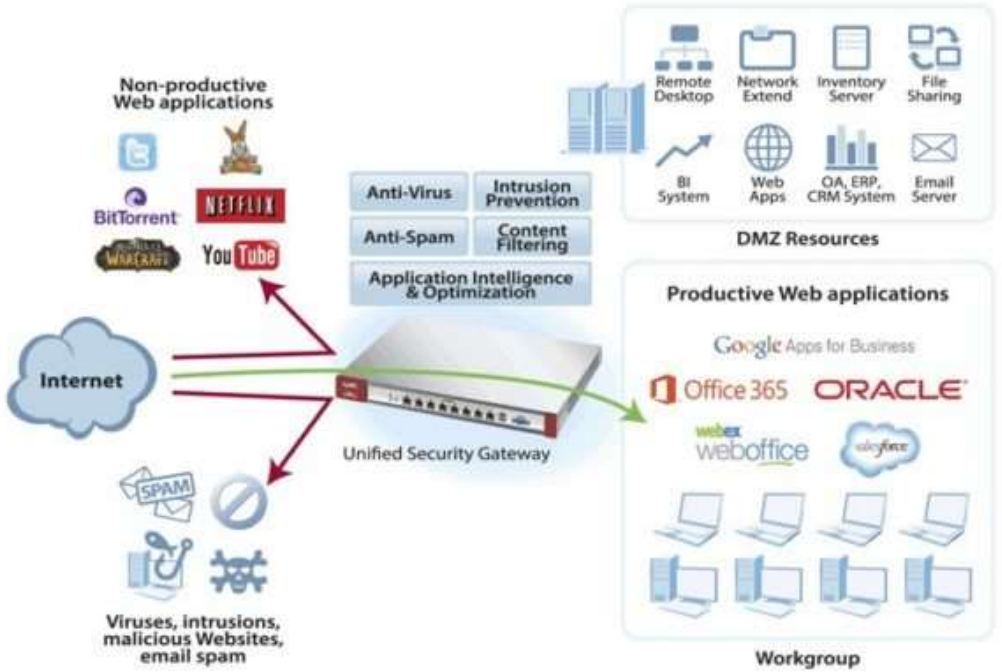
Si une requête malveillante autorisée à partir d'une adresse source de confiance entraînait, par exemple, la suppression d'une base de données, le pare-feu n'aurait aucun moyen de le savoir. Les pare-feu de nouvelle génération et les pare-feu proxy sont mieux équipés pour détecter de telles menaces.

Pare-feu de nouvelle génération (NGFW)

C’est une combinent la technologie traditionnelle du pare-feu avec des fonctionnalités supplémentaires, telles que l'inspection du trafic crypté, les systèmes de prévention des intrusions, l'antivirus, etc. Il comprend notamment l'inspection approfondie des paquets (IAP). Alors que les pare-feu de base ne regardent que les en-têtes des paquets, l'inspection approfondie des paquets examine les données contenues dans le paquet lui-même, ce qui permet aux utilisateurs d'identifier, de catégoriser ou d'arrêter plus efficacement les paquets contenant des données malveillantes.

Les pare-feu proxy

Les pare-feu proxy filtrent le trafic réseau au niveau de l'application. Contrairement aux pare-feu de base, le proxy agit comme un intermédiaire entre deux systèmes finaux. Le client doit envoyer une requête au pare-feu, où elle est ensuite évaluée par rapport à un ensemble de règles de sécurité, puis autorisée ou bloquée. Plus particulièrement, les pare-feu proxy surveillent le trafic pour les protocoles de la couche 7 tels que HTTP et FTP, et utilisent à la fois l'inspection d'état et l'inspection approfondie des paquets pour détecter le trafic malveillant.



*Les **NGFW** sont très utilisent pour analyser les usages Internet des utilisateurs de l’entreprise. Ils permettent de savoir quels utilisateurs accèdent à quels services et dans quel contexte.*

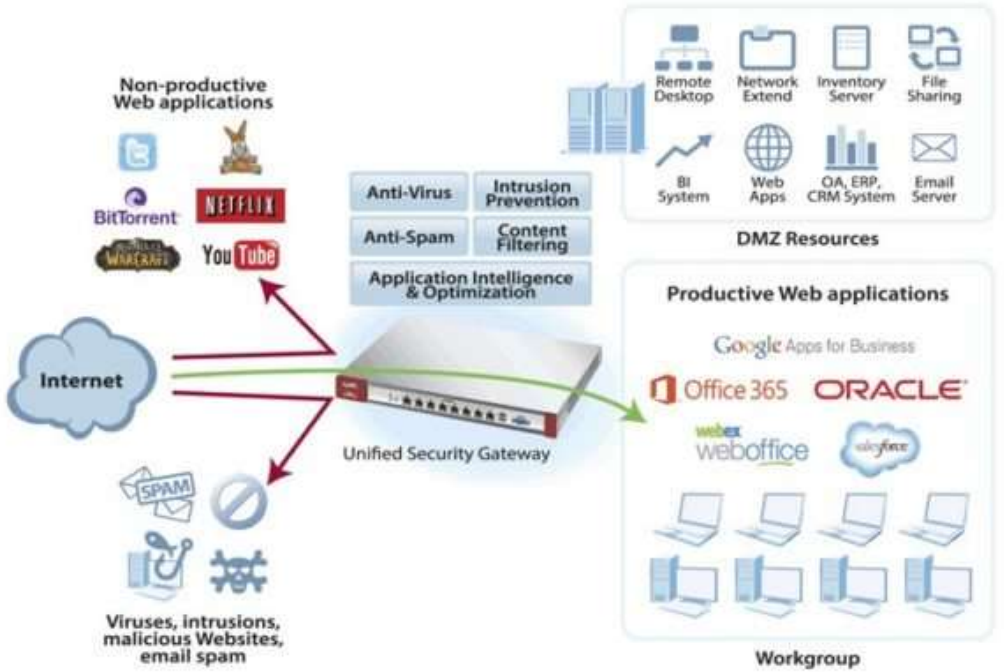
Source: [Meilleur firewall - pare-feu UTM NGFW (tomshardware.fr)]

PARTIE 1

Pare-feu de nouvelle génération (NGFW)

C'est une combinent la technologie traditionnelle du pare-feu avec des fonctionnalités supplémentaires, telles que l'inspection du trafic crypté, les systèmes de prévention des intrusions, l'antivirus, etc.

Il comprend notamment l'inspection approfondie des paquets (IAP). Alors que les pare-feu de base ne regardent que les en-têtes des paquets, l'inspection approfondie des paquets examine les données contenues dans le paquet lui-même, ce qui permet aux utilisateurs d'identifier, de catégoriser ou d'arrêter plus efficacement les paquets contenant des données malveillantes.



*Les **NGFW** sont très utilisent pour analyser les usages Internet des utilisateurs de l'entreprise. Ils permettent de savoir quels utilisateurs accèdent à quels services et dans quel contexte.*

Source: [Meilleur firewall - pare-feu UTM NGFW (tomshardware.fr)]

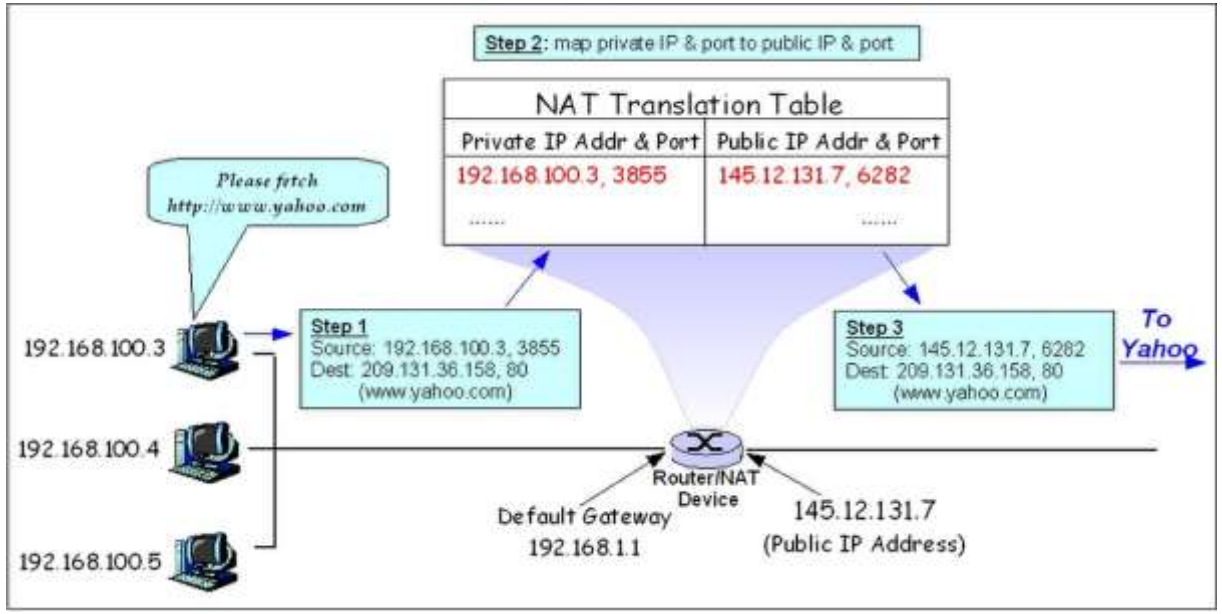
PARTIE 1

Les pare-feu SMLI (Stateful multilayer inspection)

Les pare-feu SMLI (Stateful multilayer inspection) filtrent les paquets au niveau des couches réseau, transport et application, en les comparant à des paquets de confiance connus.

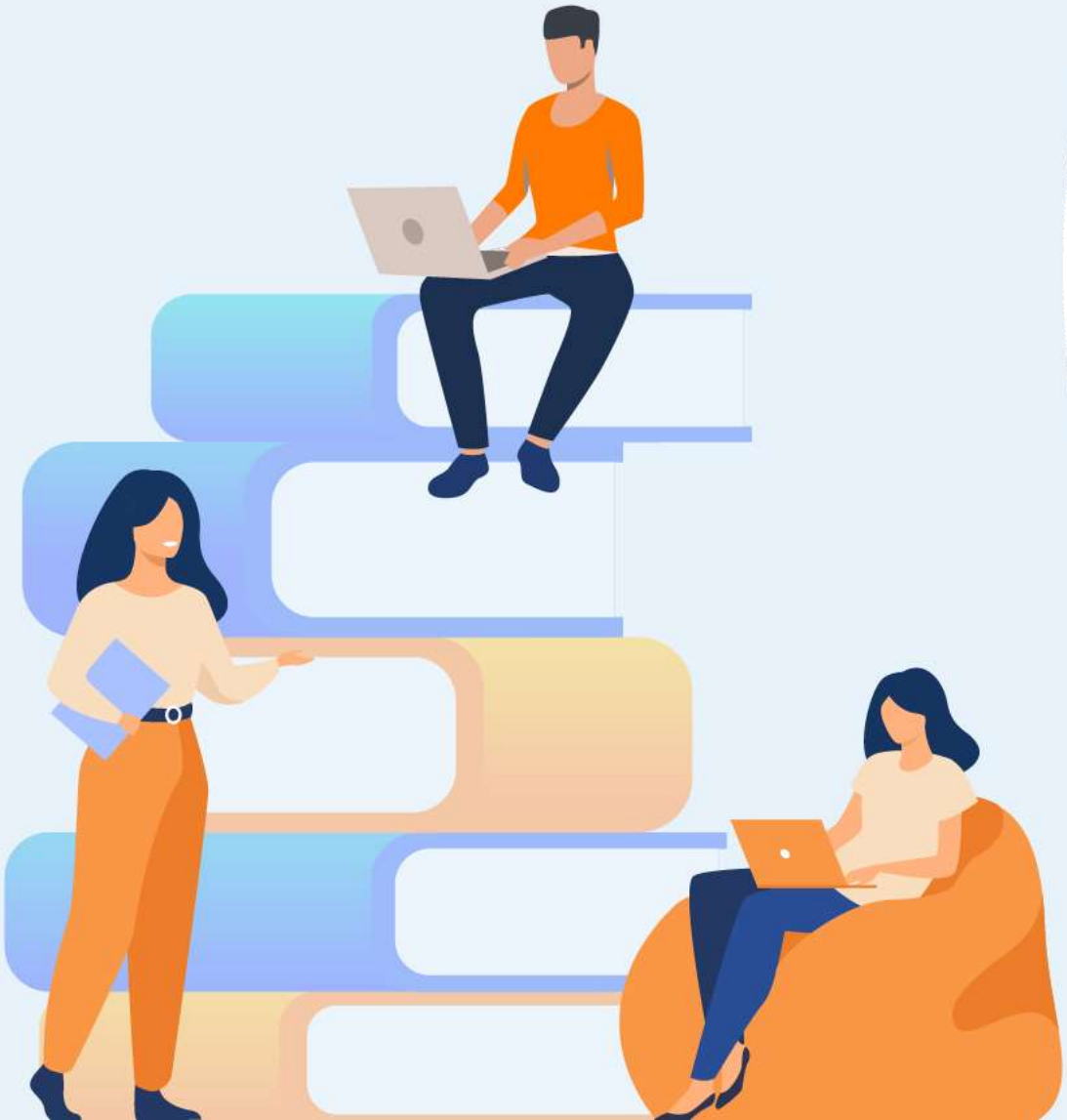
Comme les pare-feu NGFW, les SMLI examinent également l'ensemble des paquets et ne les laissent passer que s'ils passent chaque couche individuellement.

Ces pare-feu examinent les paquets pour déterminer l'état de la communication (d'où leur nom) afin de s'assurer que toutes les communications initiées ont lieu uniquement avec des sources fiables.



La majorité des traducteurs d'adresses réseau mappent plusieurs hôtes privés à une adresse IP publiquement exposée. Dans une configuration typique, un réseau local utilise l'un des sous-réseaux d'adresses IP privées désignés (RFC 1918).

PARTIE 1



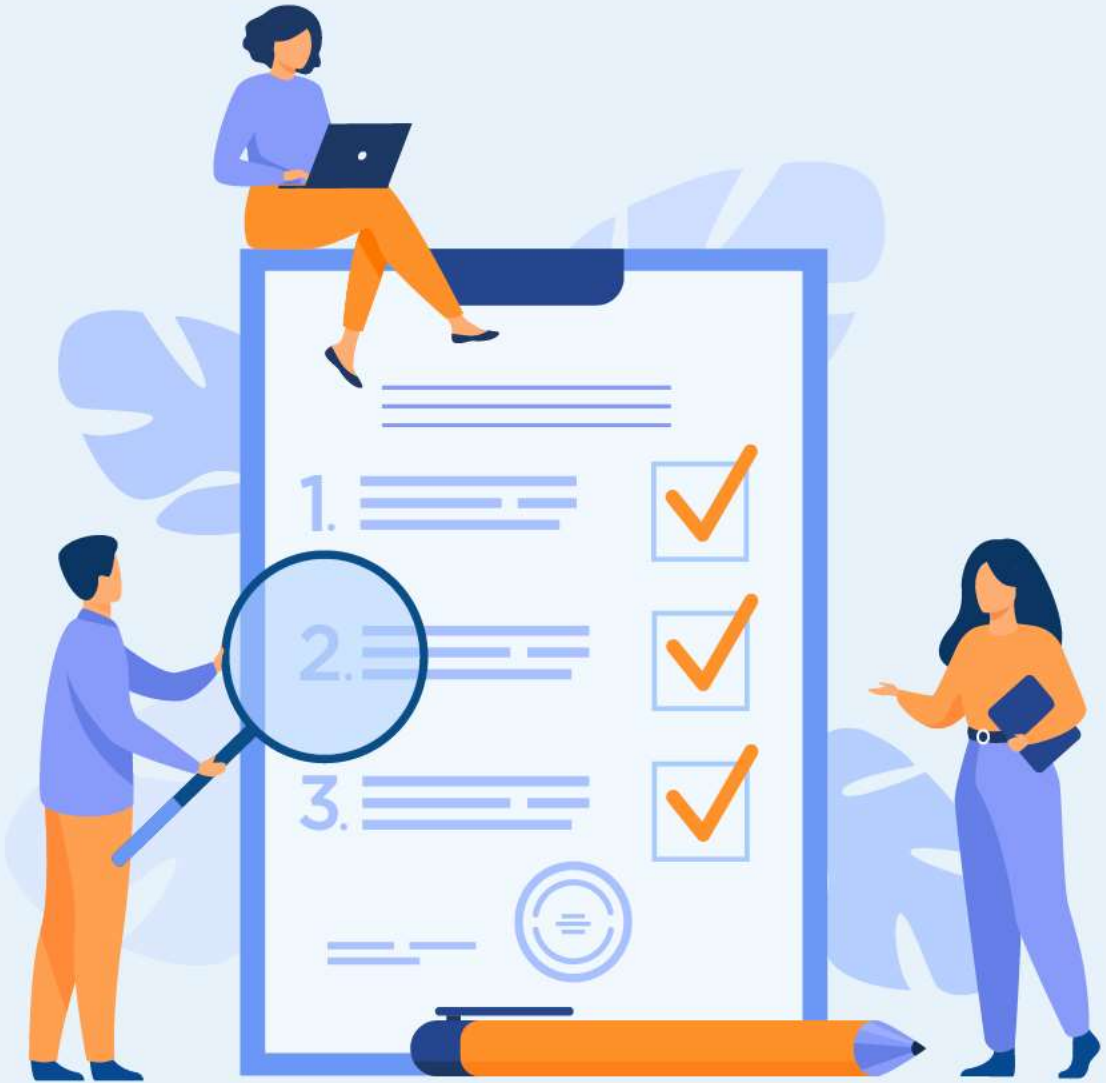
PARTIE 2

Assurer la confidentialité des données

Dans ce module, vous allez :

- Confidentialiser les données clients
- Protéger les données utilisateurs

05 heures



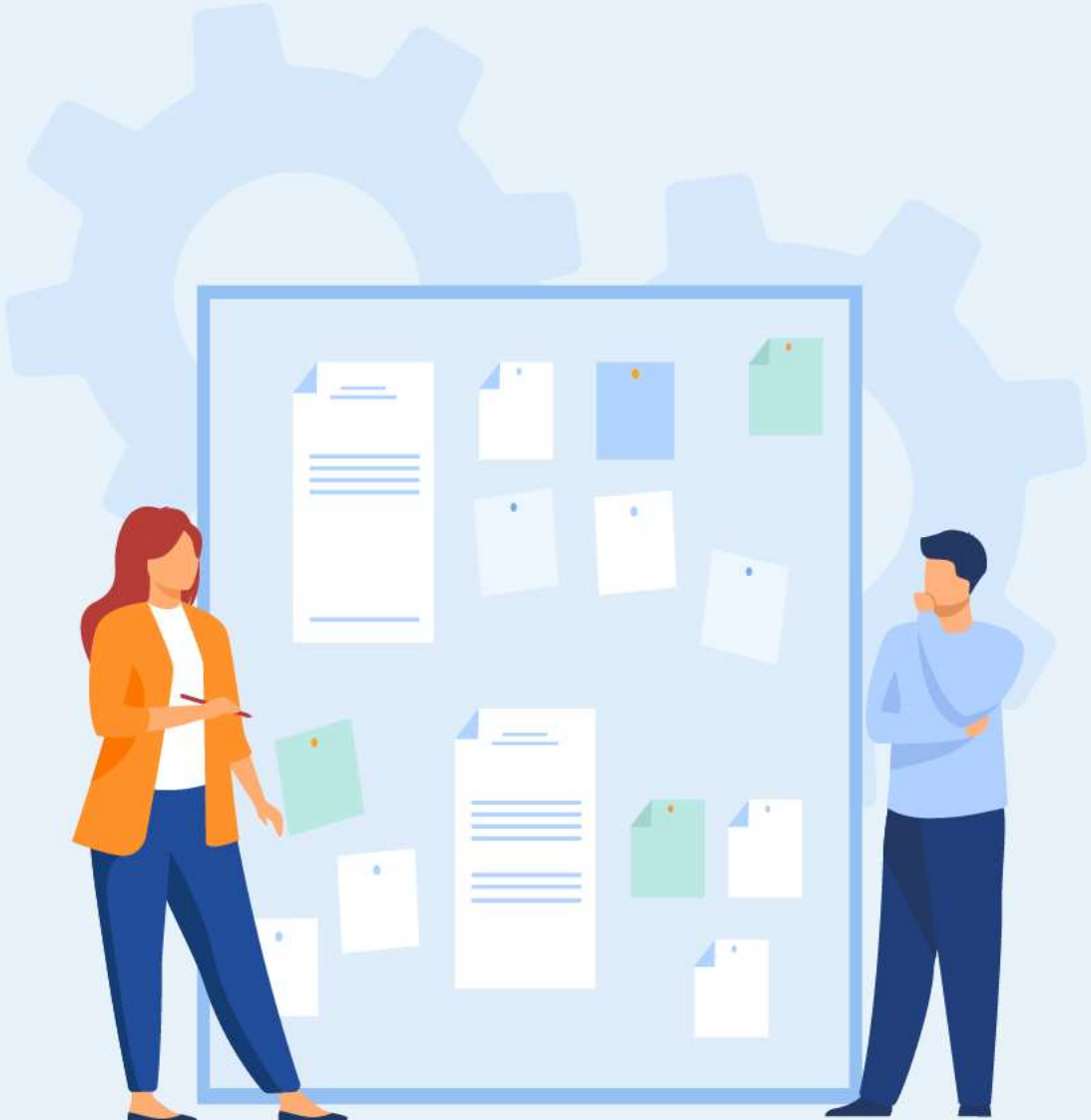
CHAPITRE 1

Confidentialiser les données clients

Ce que vous allez apprendre dans ce chapitre :

- Définition des données privées
- Initiation à la protection des données
  - Loi 09-08 (CNDP)
  - Loi 50.20 (CNDP)
  - Droits d’auteur (Copyright)
- Mécanismes de protection des données privées

02 heures



CHAPITRE 1

Confidentialiser les données clients

1. **Définition des données privées**
2. Initiation à la protection des données
   - Loi 09-08 (CNDP)
   - Loi 50.20 (CNDP)
   - Droits d’auteur (Copyright)
3. Mécanismes de protection des données privées

Définition

Toutes les données enregistrées dans les systèmes informatique et/ou le support de données sont soit privées, soit publiques. Lors de l'enregistrement des données par un utilisateur, il spécifie si les données enregistrées sont privées ou publiques.

Les données privées peuvent être lues par tous les utilisateurs qui ont accès à la bibliothèque contenant ces données, mais elles ne peuvent être modifiées que par l'utilisateur qui a écrit les données initialement.

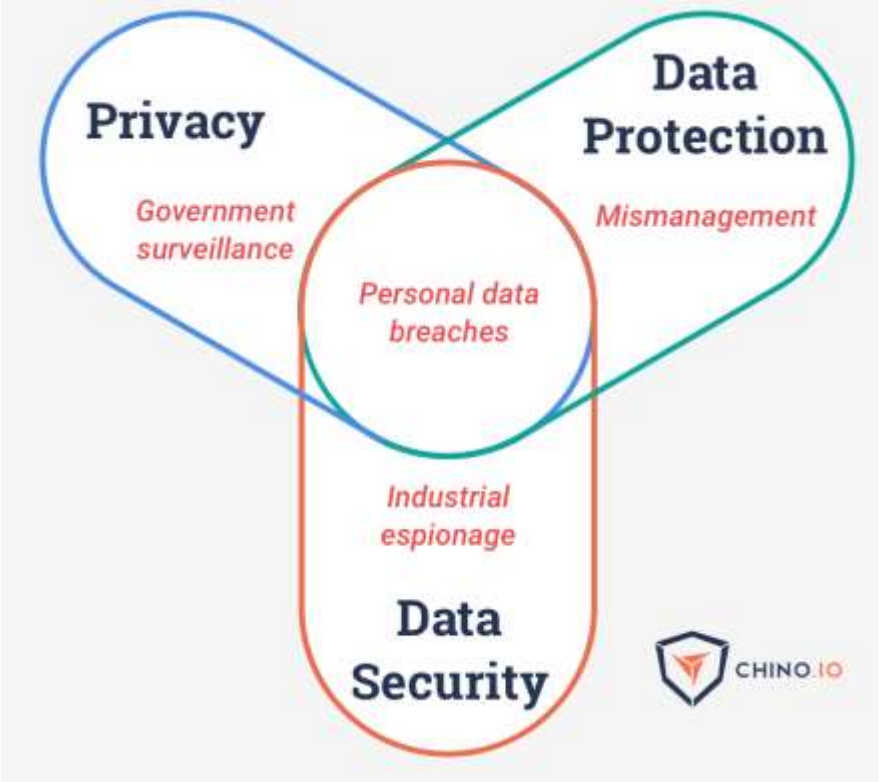
Avec une sécurité alternative, les données privées ne sont accessibles, à quelque fin que ce soit, que par leur créateur. Les données publiques, en revanche, peuvent être lues par toute personne ayant accès à la bibliothèque, mais modifiées uniquement par celui qui les a créées.

Qu'est-ce que la confidentialité des données ?

La confidentialité des données désigne généralement la capacité d'une personne à déterminer elle-même quand, comment et dans quelle mesure des informations personnelles sont partagées ou communiquées à des tiers. Ces informations personnelles peuvent être son nom, sa localisation, ses coordonnées ou son comportement en ligne ou dans le monde réel.

Par exemple, les sites web, les applications et les plateformes des réseaux sociaux doivent souvent collecter et stocker des données personnelles sur les utilisateurs afin de fournir des services.

D'autres applications et plateformes peuvent ne pas mettre en place des mesures de protection adéquates pour les données qu'elles collectent, ce qui peut entraîner une violation des données compromettant la vie privée des utilisateurs.



La relation entre la vie privée, la protection des données et la sécurité des données

01. Confidentialiser les données clients

Définition des données privées

Pourquoi la confidentialité des données est-elle importante ?

Dans de nombreuses juridictions, la vie privée est considérée comme un droit fondamental de l'Homme, et les lois sur la protection des données existent pour protéger ce droit.

La confidentialité des données est également importante car, pour que les personnes soient disposées à s'engager en ligne, elles doivent avoir la certitude que leurs données personnelles seront traitées avec soin.

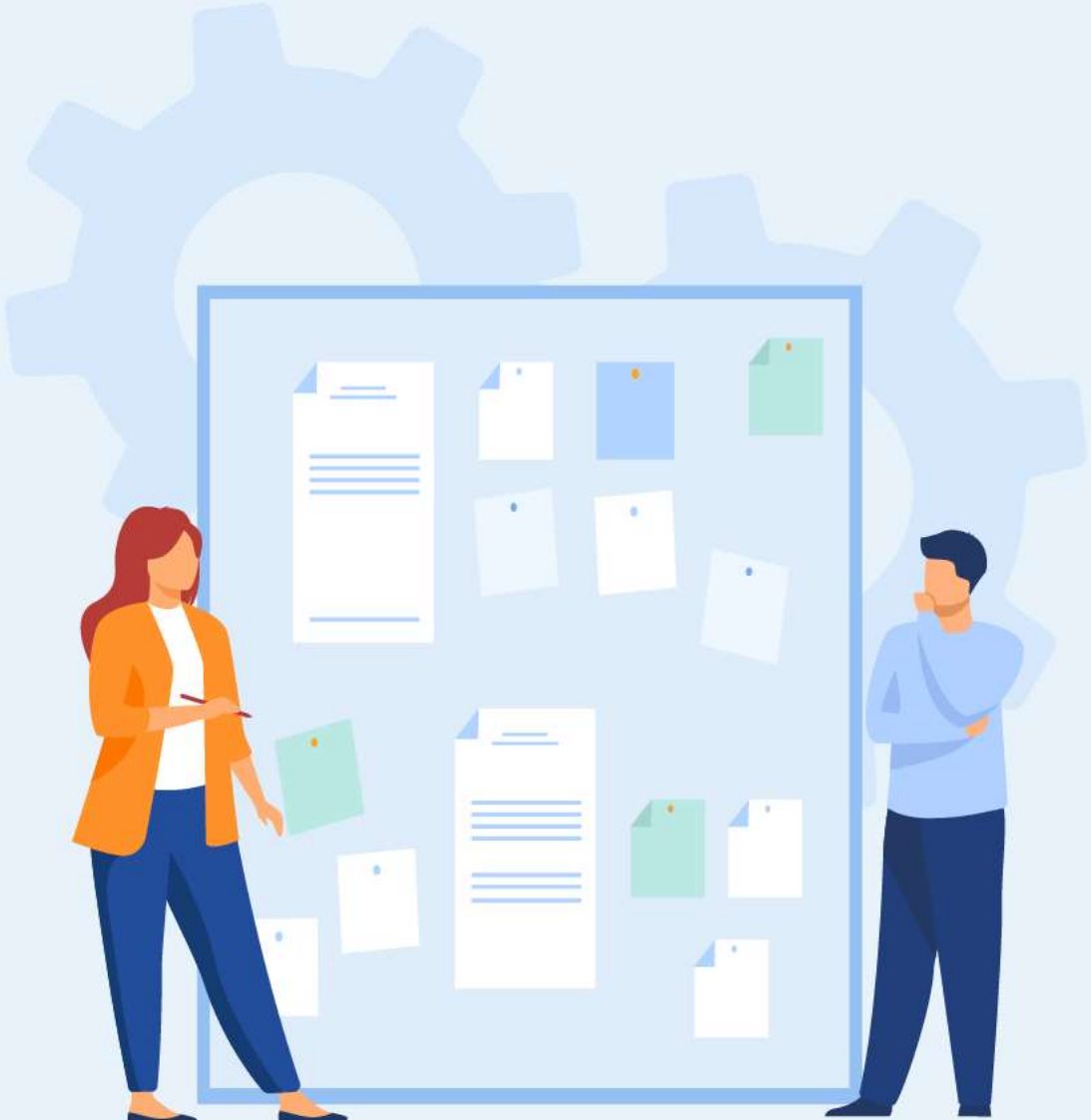
Quelles sont les lois qui régissent la confidentialité des données ?

Le règlement général sur la protection des données (**RGPD**) : **C'est une loi qui réglemente la manière dont les données personnelles des individus, peuvent être collectées, stockées et traitées, et donne aux personnes concernées le droit de contrôler leurs données personnelles (y compris un droit à l'oubli).**

La RGPD, et pour maintenir ce contrôle de protection, elle exige aux professionnels l'utilisation de différents outils et stratégies de sécurité informatique.

Au Maroc « **La Commission Nationale de contrôle de la protection des Données à Caractère Personnel (CNDP),** instituée par **la loi 09-08**, veille au respect des règles auxquelles doivent se conformer les organismes publics et privés avant et lors du traitement de vos données à caractère personnel.» site web CNDP.MA

PARTIE 2



CHAPITRE 1

Confidentialiser les données clients

1. Définition des données privées
2. **Initiation à la protection des données**
   - Loi 09-08 (CNDP)
   - Loi 50.20 (CNDP)
   - Droits d’auteur (Copyright)
3. Mécanismes de protection des données privées

PARTIE 2

Qu'est-ce que la protection des données ?

La protection des données est le processus qui consiste à protéger les informations importantes contre la corruption, la compromission ou la perte.

La protection des données est d'autant plus importante que la quantité de données créées et stockées continue de croître à un rythme sans précédent. Il y a également peu de tolérance pour les temps d'arrêt qui peuvent rendre impossible l'accès à des informations importantes.

Par conséquent, une grande partie de la stratégie de protection des données consiste à s'assurer que les données peuvent être restaurées rapidement après toute corruption ou perte.

La protection des données contre la compromission et la garantie de leur confidentialité sont d'autres éléments clés de la protection des données.

La Commission nationale de contrôle de la protection des données à caractère personnel ou CNDP est une commission marocaine, créée par la loi n°09-08 du 18 février 2009, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

Source: Commission nationale de contrôle de la protection des données à caractère personnel — Wikipédia (wikipedia.org)

Principes de la protection des données

Les principes clés de la protection des données sont la sauvegarde et la disponibilité des données en toutes circonstances.

Le terme de protection des données décrit à la fois la sauvegarde opérationnelle des données et la continuité des opérations/la reprise après sinistre. Les stratégies de protection des données évoluent selon deux axes :

- La disponibilité des données et la gestion des données.
- La disponibilité des données garantit que les utilisateurs disposent des données dont ils ont besoin pour mener leurs activités, même si ces données sont endommagées ou perdues.
- Les deux domaines clés de la gestion des données utilisés dans la protection des données sont **la gestion du cycle de vie des données** et **la gestion du cycle de vie des informations**.

Infographie sur les Principes de la Protection des Données
Resource: Introduction aux Principes de la Protection des Données | iQualit

PARTIE 2

PARTIE 2

Quel est l'objectif de la protection des données ?

Les technologies de stockage permettant de protéger les données comprennent une sauvegarde sur disque ou sur bande qui copie les informations désignées sur une matrice de stockage sur disque ou une cartouche de bande.

La sauvegarde sur bande est une option solide pour la protection des données contre les cyberattaques. Bien que l'accès aux bandes puisse être lent, elles sont portables et intrinsèquement hors ligne lorsqu'elles ne sont pas chargées dans un lecteur, et donc à l'abri des menaces sur un réseau.

Les organisations peuvent utiliser la mise en miroir pour créer une réplique exacte d'un site Web ou de fichiers afin qu'ils soient disponibles à plusieurs endroits.

Les instantanés de stockage peuvent générer automatiquement un ensemble de pointeurs vers des informations stockées sur bande ou sur disque, ce qui permet une récupération plus rapide des données, tandis que la protection continue des données (CDP) sauvegarde toutes les données d'une entreprise chaque fois qu'une modification est effectuée.

La protection des données concerne uniquement à des personnes physiques. Il encadre les conditions de collecte et d'utilisation des données dites personnelles.

Les lois sur la protection des données et la vie privée

Les lois et réglementations relatives à la protection des données et à la confidentialité varient d'un pays à l'autre, et même d'un État à l'autre -- et il y a un flux constant de nouvelles lois. La loi chinoise sur la confidentialité des données est entrée en vigueur le 1er juin 2017. Le règlement général sur la protection des données (RGPD) de l'Union européenne est entré en vigueur en 2018. Aux États-Unis, la loi californienne sur la protection de la vie privée des consommateurs soutient le droit des personnes à contrôler leurs propres informations d'identification personnelle. La conformité à un ensemble de règles, quel qu'il soit, est compliquée et difficile.

Au Maroc, **la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel** définit les obligations auxquelles sont soumis les responsables de traitements. Ces derniers doivent s'assurer que les données personnelles sont collectées et traitées d'une façon loyale, légitime et transparente. Ils doivent, en outre :

- Respecter la finalité du traitement
- Respecter le principe de proportionnalité
- S'assurer de la qualité des données
- Veiller au respect de la durée de conservation des données
- Veiller à l'exercice des droits par la personne concernée
- Assurer la sécurité et la confidentialité des traitements
- Notifier les traitements à la CNDP

D'autre part « **la loi 05-20 relative à la cybersécurité** vise notamment à mettre en place un cadre juridique préconisant un ensemble de règles et de mesures de sécurité afin d'assurer et renforcer la sécurité et la résilience des systèmes d'information des administrations de l'Etat, des collectivités territoriales, des établissements et entreprises publics et de toute autre personne morale de droit public de l'Etat ainsi que des infrastructures d'importance vitale disposant des systèmes d'information sensibles. »[1]

Cette loi « est entrée en vigueur au Maroc dès le 30 Juillet 2020 avec pour objectif de préconiser des moyens de protection assurant ainsi le développement de la confiance numérique, la digitalisation de l'économie et plus généralement l'assurance de la continuité des activités économiques et sociétales du Maroc. »[2]

1) www.dgssi.gov.ma

2) orangecyberdefense.com

Qu'est-ce que le droit d'auteur ?

Le droit d'auteur (ou copyright) est un terme juridique utilisé pour décrire les droits dont disposent les créateurs sur leurs œuvres littéraires et artistiques. Les œuvres couvertes par le droit d'auteur vont des livres, de la musique, des peintures, des sculptures et des films aux programmes informatiques, bases de données, publicités, cartes et dessins techniques.

Comment le droit d'auteur s'applique aux sites web

Un site web, en tant qu'œuvre originale, est protégé par le droit d'auteur dès sa création car un site web, par définition, satisfait à l'exigence selon laquelle le matériel est "fixé sur un support d'expression tangible". En substance, cela signifie simplement que le contenu doit être documenté ou communiqué d'une manière observable, par exemple imprimé sur du papier ou enregistré sur un disque dur.

Tout le contenu d'un **site web est protégé par le droit d'auteur**. Selon la loi sur le droit d'auteur, cela inclut tout "matériel perceptible par les utilisateurs d'un site web particulier", c'est-à-dire le texte, les images, la musique, les sons et les vidéos.

Le contenu d'un site web est protégé par le droit d'auteur dès sa publication, mais il est judicieux d'en informer explicitement les utilisateurs. C'est ce que fait l'avis de droit d'auteur figurant en bas de page, et c'est l'un des moyens de mettre la protection du droit d'auteur à votre service. Elle indique que le contenu ne peut être utilisé légalement sans l'autorisation du **propriétaire**.

Ce mot, "**propriétaire**", soulève une nouvelle question. À qui appartient le matériel protégé par le droit d'auteur ?

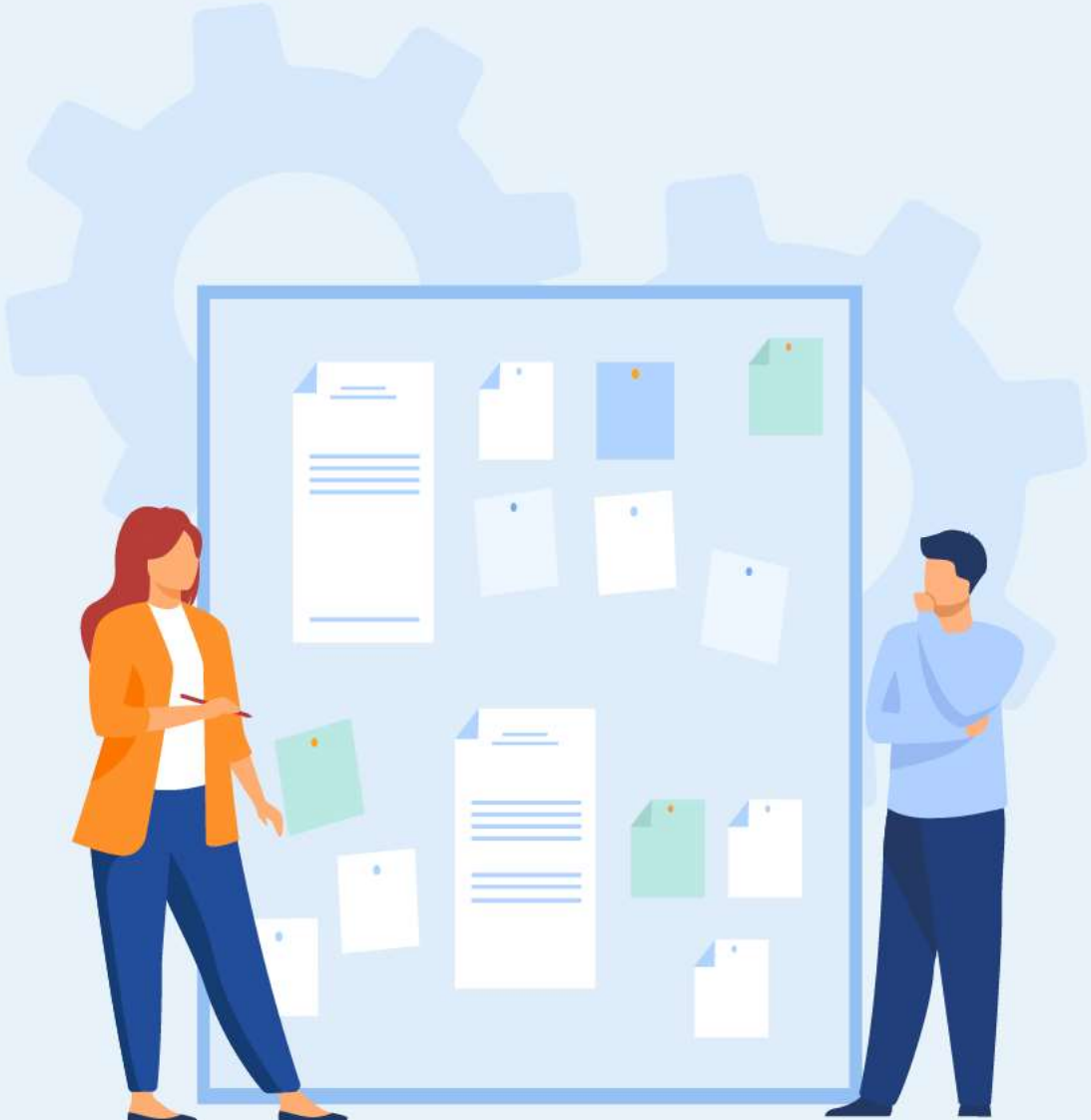
PARTIE 2

Qui est le titulaire du droit d'auteur ?

Le créateur détient les droits, mais si le travail a été réalisé dans le cadre d'un "travail à la demande", il peut y avoir un accord en place qui accorde la propriété de l'œuvre au client.

Si vous employez directement quelqu'un et que cette personne crée du contenu pour votre site, votre entreprise est propriétaire des droits d'auteur. Un entrepreneur indépendant, en revanche, est propriétaire du matériel qu'il crée, et vous devez avoir un accord pour lui réserver les droits exclusifs d'utilisation de ce matériel.

Le droit d'auteur se divise en 2 sous-catégories de droits :
Le droit moral et les droits patrimoniaux ou droits d'exploitation



CHAPITRE 1

Confidentialiser les données clients

1. Définition des données privées
2. Initiation à la protection des données
   - Loi 09-08 (CNDP)
   - Loi 50.20 (CNDP)
   - Droits d’auteur (Copyright)
3. **Mécanismes de protection des données privées**

Les technologies et pratiques pour protéger les données

Les termes "protection des données" et "confidentialité des données" sont souvent utilisés de manière ***interchangeable***, mais il existe une différence importante entre les deux. La confidentialité des données définit qui a accès aux données, tandis que la protection des données fournit **des outils et des politiques pour restreindre réellement l'accès aux données**. Les règlements de conformité permettent de s'assurer que les demandes de confidentialité des utilisateurs sont prises en compte par les entreprises, et ces dernières sont tenues de prendre des mesures pour protéger les données privées des utilisateurs.

La protection des données et la confidentialité s'appliquent généralement aux **informations de santé personnelles (PHI) et aux informations d'identification personnelle (PII).** Elles jouent un rôle essentiel dans les opérations, le développement et les finances des entreprises. En protégeant les données, les entreprises peuvent éviter les violations de données, les atteintes à la réputation et mieux répondre aux exigences réglementaires.

Les solutions de protection des données reposent sur des technologies telles que la prévention des pertes de données (DLP), le stockage avec protection des données intégrée, les pare-feu, le cryptage et la protection des points de connexion API.

PARTIE 2

Les technologies et pratiques pour protéger les données

Lorsqu'il s'agit de protéger vos données, il existe de nombreuses options de stockage et de gestion parmi lesquelles vous pouvez choisir. Les solutions peuvent vous aider à restreindre l'accès, à surveiller l'activité et à réagir aux menaces. Voici quelques-unes des pratiques et technologies les plus couramment utilisées :

- **Découverte des données:** première étape de la protection des données, il s'agit de découvrir les ensembles de données existant dans l'entreprise, ceux qui sont essentiels à l'activité et ceux qui contiennent des données sensibles susceptibles d'être soumises à des règles de conformité.
- **Prévention des pertes de données (DLP):** ensemble de stratégies et d'outils que vous pouvez utiliser pour empêcher le vol, la perte ou la suppression accidentelle de données. Les solutions de prévention des pertes de données comprennent souvent plusieurs outils permettant de se protéger contre les pertes de données et de les récupérer.
- **Stockage avec protection des données intégrée** : les équipements de stockage modernes intègrent la mise en grappe et la redondance des disques.
- **La sauvegarde:** crée des copies des données et les stocke séparément, ce qui permet de restaurer les données ultérieurement en cas de perte ou de modification. Les sauvegardes constituent une stratégie essentielle pour assurer la continuité des activités lorsque les données originales sont perdues, détruites ou endommagées, que ce soit par accident ou par malveillance.

Les outils de sauvegarde de données dans le cloud proposent de nombreux avantages, dont l'accessibilité, la capacité de gérer les documents corrompus et la récupération des fichiers.

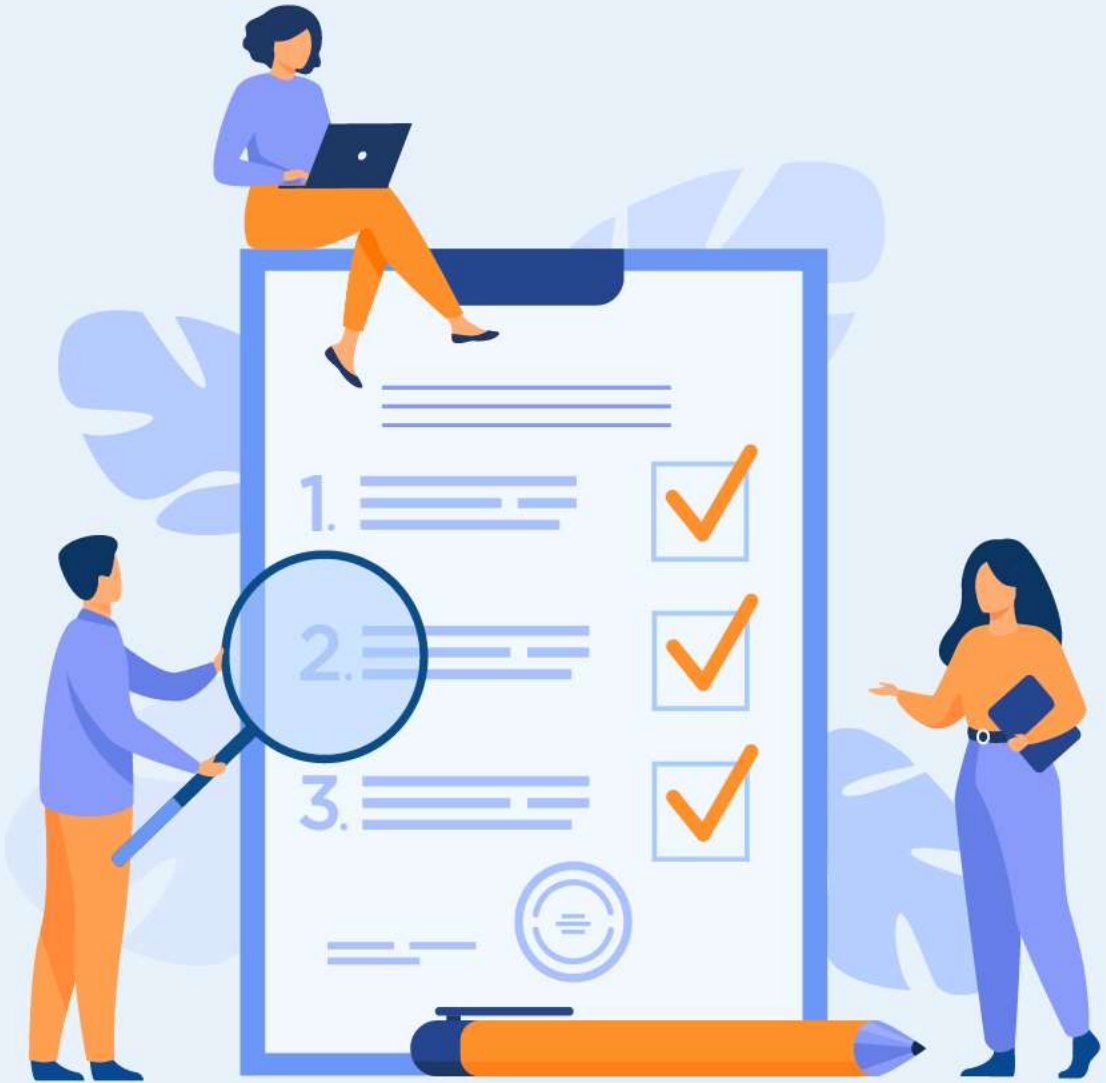
Resource: [3 technologies essentielles de protection des données - GetApp]

Les technologies et pratiques pour protéger les données

- **Snapshots:** un Snapshot est similaire à une sauvegarde, mais il s'agit d'une image complète d'un système protégé, y compris les données et les fichiers système. Un Snapshot peut être utilisé pour restaurer un système entier à un moment précis.
- **Réplication** : technique permettant de copier les données de façon continue d'un système protégé vers un autre emplacement. Cela fournit une copie vivante et à jour des données, permettant non seulement la récupération mais aussi le basculement immédiat vers la copie si le système primaire tombe en panne.
- **Pare-feu** : utilitaires qui vous permettent de surveiller et de filtrer le trafic réseau. Vous pouvez utiliser les pare-feu pour vous assurer que seuls les utilisateurs autorisés sont autorisés à accéder aux données ou à les transférer.
- **Authentification et autorisation** : contrôles qui vous permettent de vérifier les informations d'identification et de vous assurer que les privilèges des utilisateurs sont appliqués correctement.

Les technologies et pratiques pour protéger les données

- **Le chiffrement** : altère le contenu des données selon un algorithme qui ne peut être inversé qu'avec la bonne clé de chiffrement. Le chiffrement protège vos données contre tout accès non autorisé, même en cas de vol, en les rendant illisibles.
- **Protection des points d'accès:** protège les passerelles vers votre réseau, notamment les ports, les routeurs et les appareils connectés. Les logiciels de protection des points d'accès vous permettent généralement de surveiller le périmètre de votre réseau et de filtrer le trafic si nécessaire.
- **Effacement des données:** limite la responsabilité en supprimant les données qui ne sont plus nécessaires. Cette opération peut être effectuée après le traitement et l'analyse des données ou périodiquement lorsque les données ne sont plus pertinentes. L'effacement des données inutiles est une exigence de nombreuses réglementations de conformité, telles que le CNDP.
- **Reprise après sinistre:** ensemble de pratiques et de technologies qui déterminent la manière dont une organisation fait face à un sinistre, comme une cyberattaque, une catastrophe naturelle ou une panne d'équipement à grande échelle. Le processus de reprise après sinistre consiste généralement à mettre en place un site de reprise après sinistre distant avec des copies des systèmes protégés, et à basculer les opérations sur ces systèmes en cas de sinistre.



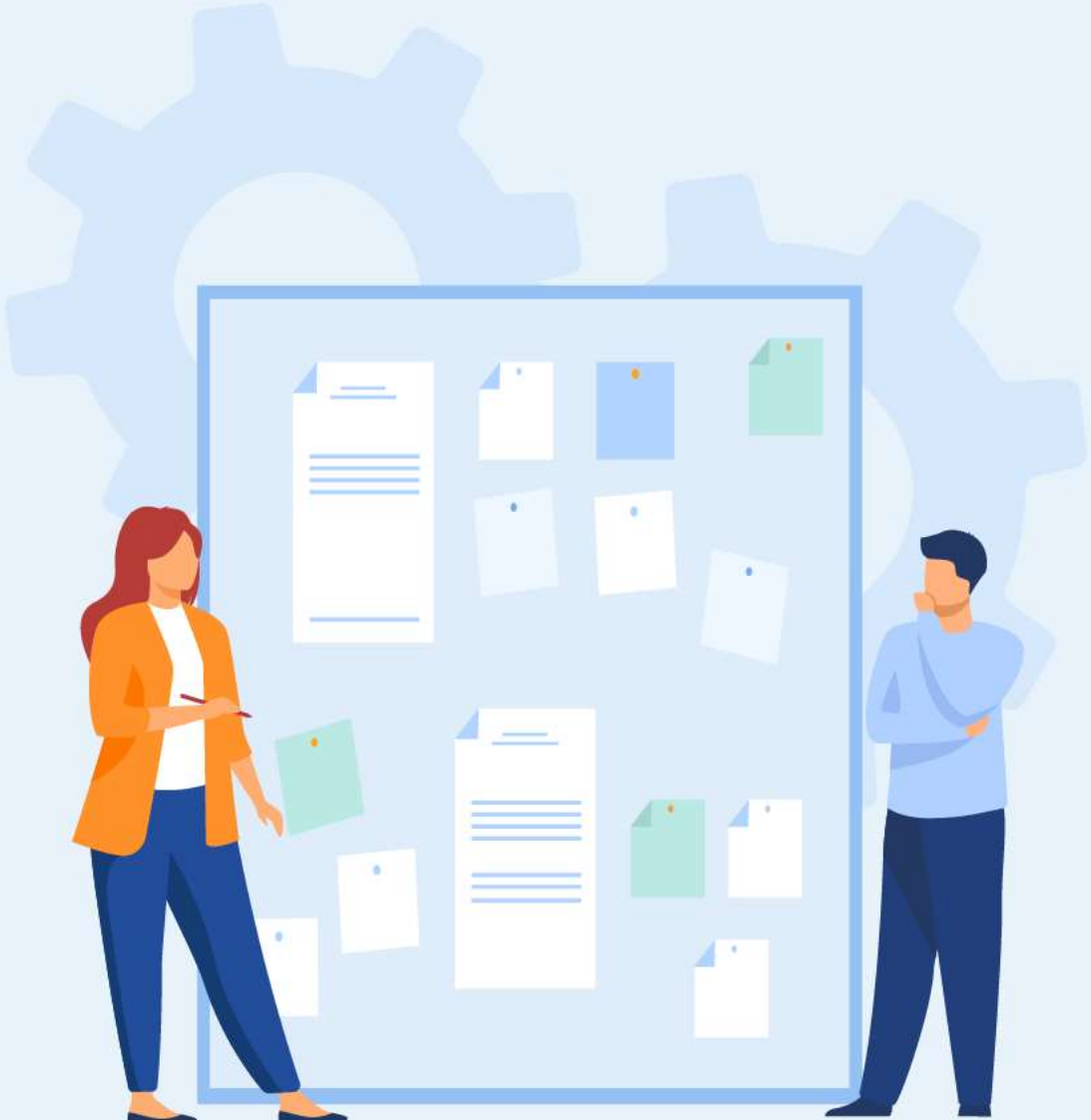
CHAPITRE 2

Protéger les données utilisateurs

Ce que vous allez apprendre dans ce chapitre :

- Obfuscation du code source
- Règles de protection des données utilisateurs
- Droits d’accès des utilisateurs d’une application
- Accès sécurisé aux données de l’application
- Cryptage des données

03



CHAPITRE 1

Protéger les données utilisateurs

1. **Obfuscation du code source**
2. Règles de protection des données utilisateurs
3. Droits d’accès des utilisateurs d’une application
4. Accès sécurisé aux données de l’application
5. Cryptage des données

Définition

L'obfuscation du code source est le processus qui consiste à compliquer délibérément le code de manière à le rendre difficile, voire impossible, à comprendre pour l'Homme, sans pour autant affecter le résultat du programme.

Les programmeurs obscurcissent le code pour empêcher qu'il ne soit volé, pour le rendre plus difficile à manipuler et pour sécuriser des informations précieuses sur la fonction du code.

Contrairement au cryptage, l'obscurcissement ne rend pas les données intelligibles que pour les humains. Comme les données restent lisibles par la machine, l'obfuscation protège le code contre les cybercriminels sans ajouter d'étapes supplémentaires, comme le décryptage, qui peuvent ralentir l'exécution du programme.

Dans le monde concurrentiel des nouvelles technologies, la propriété intellectuelle est souvent l'actif le plus précieux d'une entreprise. L'obfuscation du code source est une étape essentielle pour protéger votre propriété intellectuelle contre le vol par des concurrents.

Pourquoi le code source est-il si difficile à protéger ?

En général, les données et les informations précieuses sont protégées en limitant leur accès. Par exemple, les fichiers sensibles des clients sont conservés en sécurité dans des comptes cryptés et protégés par un mot de passe, qu'il est difficile, voire impossible, de pénétrer pour les criminels.

Cependant, le code source est visible par toute personne utilisant un programme, de sorte que les méthodes de prévention d'accès ne peuvent pas être utilisées pour sécuriser le code ou toute information stockée dans celui-ci.

Au lieu de cela, les programmeurs peuvent "déguiser" le code par le biais de l'obfuscation, de sorte qu'il devient illisible par les humains mais reste lisible par les machines. Cela empêchera les pirates de récupérer le code tout en permettant au programme de fonctionner correctement.

Un logiciel d'obfuscation peut être utilisé pour appliquer automatiquement différentes méthodes d'obfuscation à des sections du code, ou les programmeurs peuvent sélectionner des portions de données et les obfusquer à la main.

Techniques d'obfuscation

Il existe de nombreuses méthodes différentes pour obscurcir les données. Afin de renforcer les protections du code, les programmeurs peuvent combiner différentes techniques dans le code afin de le rendre encore plus difficile à lire pour les pirates.

Nous présentons ci-dessous quelques-unes des techniques les plus courantes pour obscurcir efficacement le code.

Formes alternatives du code

Traduisez de courtes sections du code en différentes formes tout au long du programme pour rendre son déchiffrage plus difficile sans affecter le temps d'exécution. Par exemple, vous pouvez traduire certaines parties de votre code en langage binaire, ou remplacer une fonction par une table de consultation de toutes les valeurs possibles que la fonction peut produire.

Changez les méthodes de stockage des données

Rendez vos données plus difficiles à lire en les "cachant" essentiellement en utilisant différents types et emplacements de stockage. Alternez le stockage des variables localement et globalement pour dissimuler la façon dont les variables fonctionnent ensemble.

Vous pouvez également randomiser les adresses auxquelles se trouvent les parties du code pour créer un niveau supplémentaire de confusion et rendre le code plus difficile à lire.

Techniques d'obfuscation

Randomisez les modèles d'agrégation

Un autre moyen de déconcerter les pirates consiste à regrouper vos données dans des tailles aléatoires. Par exemple, vous pouvez diviser les tableaux en un nombre inutilement élevé de sous-réseaux afin d'éviter toute tentative de rétroconception.

Cryptez les chaînes de caractères

Bien que le cryptage ne soit pas une méthode efficace pour protéger l'ensemble de votre code source, vous pouvez l'utiliser dans le cadre du processus d'obfuscation sans ralentir le programme. Sélectionnez des clés individuelles, des chaînes de code et d'autres éléments d'information à crypter afin de créer des ***"angles morts"*** dans le code.

Interrompre le flux de code

Ajoutez des déclarations inutiles ou du "code mort" à votre programme pour qu'il soit difficile de déterminer quelles parties du code contiennent des données réelles. Le code fictif peut également être utilisé pour dissimuler les voies par lesquelles le contrôle du programme est transmis entre les sections de la base de code.

Supprimer les données de débogage

Les informations de débogage peuvent être utilisées par les pirates pour faire de l'ingénierie inverse sur le code source d'un programme. Il est donc judicieux d'obscurcir les informations de débogage en modifiant les numéros de ligne et les noms de fichier. Vous pouvez également supprimer entièrement les informations de débogage de votre programme.

Techniques d'obfuscation

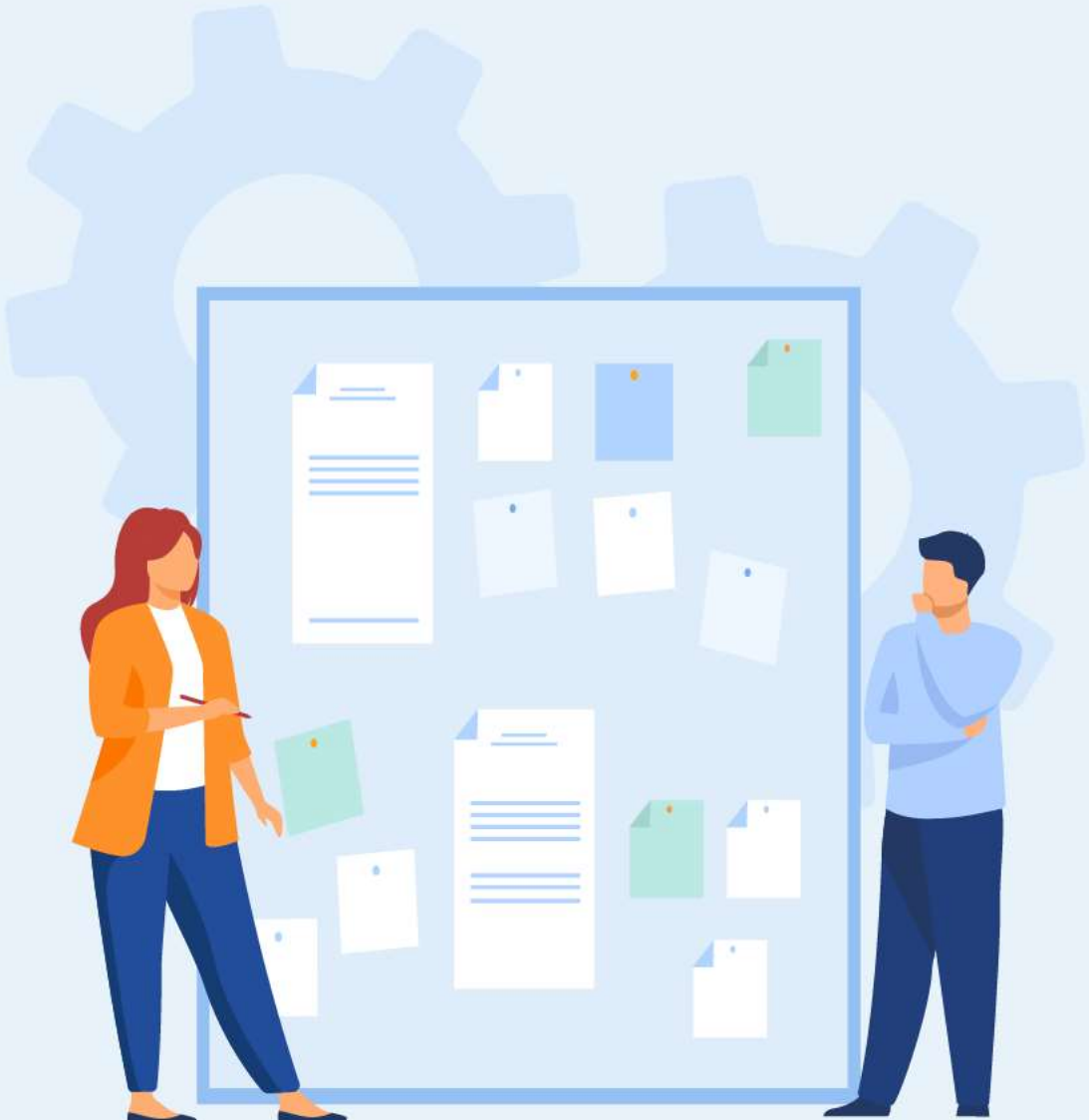
Obfusquer le code d'assemblage

Concentrez vos efforts d'obfuscation sur le assembleur afin de le rendre particulièrement difficile à désassembler. De nombreux programmeurs aiment cacher le assembleur à l'intérieur d'un autre code dans une sorte de modèle de poupée russe appelée la technique du "jump-in-the-middle", qui empêchera un désassembleur de produire les sorties correctes.

Renouveler régulièrement les tactiques d'obfuscation

Utilisez un calendrier de renouvellement des tactiques d'obscurcissement et rafraîchissez les techniques que vous avez utilisées dans le code. Variez les éléments d'information que vous avez cachés et cryptés, et alternez les tactiques dans différentes parties du code.

L'utilisation de plusieurs tactiques pour obscurcir le code source et la mise à jour régulière de l'obscurcissement protégeront la propriété intellectuelle de la société contre la majorité des piratages potentiels. Cependant, aucune mesure de sécurité ne peut garantir une sécurité irréprochable à 100%.



CHAPITRE 1

Protéger les données utilisateurs

1. Obfuscation du code source
2. **Règles de protection des données utilisateurs**
3. Droits d’accès des utilisateurs d’une application
4. Accès sécurisé aux données de l’application
5. Cryptage des données

Introduction

Le Règlement général sur la protection des données (RGPD) a réécrit les règles relatives à la vie privée, obligeant les entreprises à mettre à jour leurs opérations et même à reconcevoir la conception de leurs produits, leurs services et leur image de marque.

Ainsi, bien que le GDPR ait été adopté en 2016, ses principes fondamentaux sont aussi pertinents aujourd'hui que lorsque les législateurs les ont émis pour la première fois. Les principes clés au cœur de la loi devraient informer chaque étape d'un programme moderne de gestion de la vie privée.

Nous listons ci-après les principes clés du GDPR :

- Légalité, équité et transparence
- Limitation de la finalité
- Minimisation des données
- Exactitude
- Limitation du stockage
- Intégrité et confidentialité (sécurité)
- Responsabilité

Légalité, équité et transparence

Chaque fois que vous traitez des données personnelles, vous devez avoir une bonne raison de le faire. Le GDPR appelle ce principe la licéité. Les raisons de traiter des données peuvent inclure :

- L'utilisateur vous a donné son **consentement** pour le faire.
- Vous devez le faire pour exécuter un **contrat**.
- C'est nécessaire pour remplir une **obligation légale**.
- Pour la **protection des intérêts vitaux d'une personne physique**.
- Il s'agit d'une **tâche publique** effectuée dans l'intérêt public.
- Vous pouvez prouver que vous avez **un intérêt légitime** et qu'il n'est pas supplanté par les droits et intérêts de la personne concernée.

Le concept de loyauté énoncé dans le GDPR va de pair avec la légalité. Il signifie que vous ne devez pas dissimuler délibérément des informations sur la nature ou la raison de votre collecte de données. En d'autres termes, les utilisateurs ne seraient pas surpris s'ils savaient comment vous utilisez leurs données. L'équité signifie que vous ne malmènerez pas ou n'utiliserez pas à mauvais escient les données que vous collectez.

La transparence est intrinsèquement liée à la loyauté : La transparence est intrinsèquement liée à l'équité : être clair, ouvert et honnête avec les personnes concernées sur qui vous êtes, et pourquoi et comment vous traitez leurs données personnelles est la définition de la transparence. **En la respectant, vous agissez de manière équitable envers vos personnes concernées.**

Limitation de la finalité

Le deuxième principe du GDPR définit les limites de l'utilisation des données uniquement pour des activités spécifiques. Cette limitation de la finalité signifie que les données sont "collectées uniquement pour des finalités déterminées, explicites et légitimes", comme l'indique le GDPR.

Vos objectifs de traitement des données doivent être clairement établis. Et elles doivent également être clairement communiquées aux individus par le biais d'un avis de confidentialité. Enfin, vous devez les suivre de près, en **limitant le traitement des données aux seules fins que vous avez indiquées**.

Si, à un moment donné, vous souhaitez utiliser les données que vous avez collectées pour une nouvelle finalité incompatible avec la finalité initiale, **vous devez redemander** spécifiquement le consentement de la personne concernée pour le faire - à moins que vous n'ayez une obligation ou une fonction clairement établie par la loi.

Exactitude

C'est à vous de garantir l'exactitude des données que vous collectez et stockez. Mettez en place des contrôles et des vérifications pour corriger, mettre à jour ou effacer les données incorrectes ou incomplètes qui vous parviennent. Prévoyez également des audits réguliers pour vérifier la propreté des données stockées.

Responsabilité

Les régulateurs du GDPR savent qu'une organisation peut dire qu'elle respecte toutes les règles sans pour autant les appliquer. C'est pourquoi ils exigent un certain niveau de responsabilité : Vous devez mettre en place des mesures et des enregistrements appropriés comme preuve de votre conformité aux principes de traitement des données. Les autorités de contrôle peuvent demander ces preuves à tout moment. La documentation est essentielle à cet égard. Elle crée une piste d'audit que vous - et les autorités - pouvez suivre si vous devez prouver votre responsabilité.

Minimisation des données

Ne collectez que la plus petite quantité de données dont vous aurez besoin pour mener à bien vos objectifs. C'est le principe de minimisation des données du GDPR.

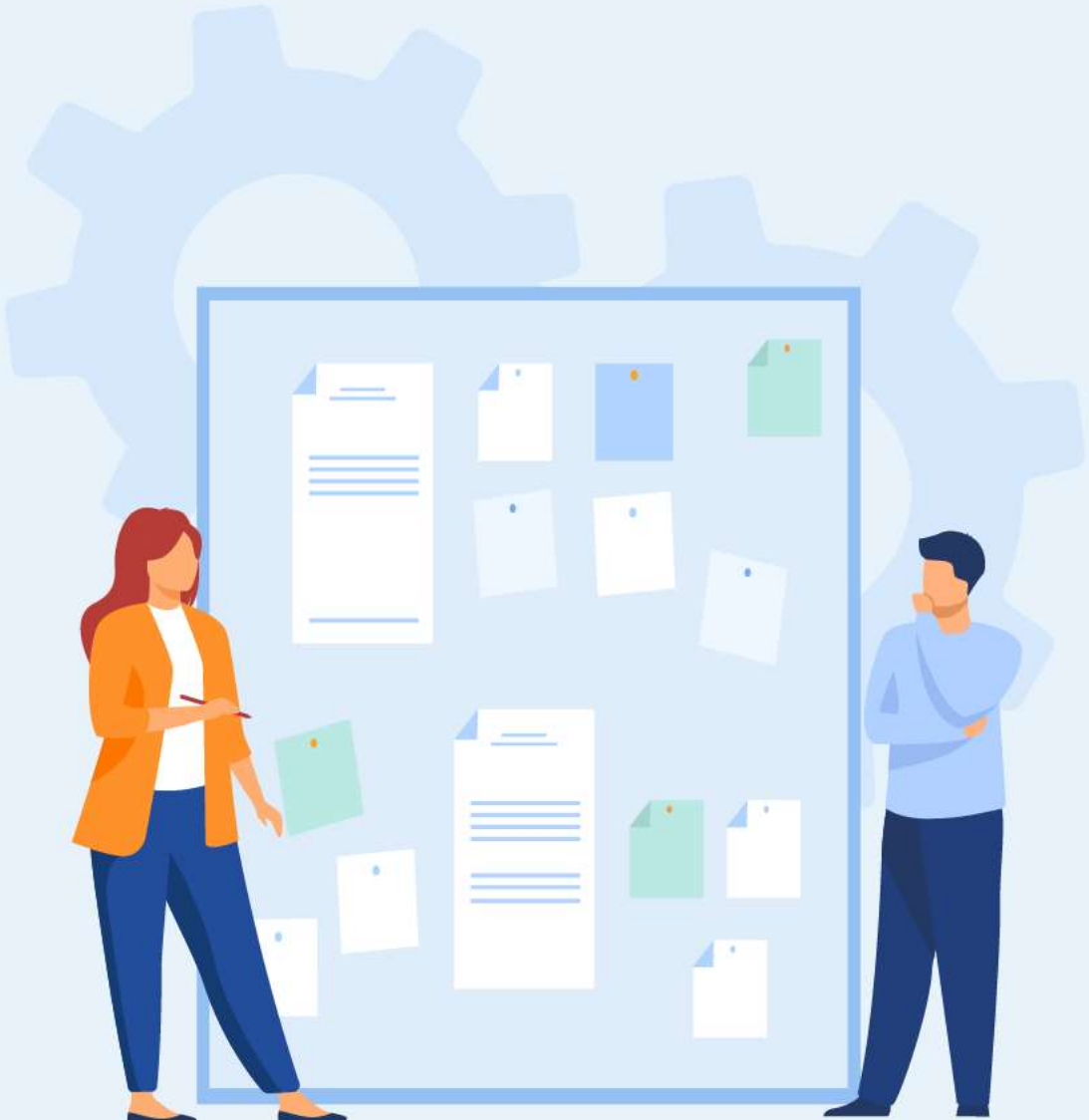
Par exemple, si vous voulez rassembler des abonnés pour votre lettre d'information électronique, vous ne devez demander que les informations nécessaires à l'envoi des lettres d'information. Évitez de recueillir des données personnelles telles que des numéros de téléphone ou des adresses personnelles, qui ne sont pas directement liées à votre objectif.

Limitation du stockage

Selon le GDPR, vous devez justifier la durée de conservation de chaque donnée que vous stockez. Les périodes de conservation des données sont une bonne chose à établir pour répondre à cette politique de limitation du stockage. Créez une période standard après laquelle vous anonymiserez toutes les données que vous n'utilisez pas activement.

Intégrité et confidentialité

Le GDPR exige que vous mainteniez l'intégrité et la confidentialité des données que vous collectez, essentiellement en les préservant des menaces internes ou externes. Cela nécessite une planification et une diligence proactive. Vous devez protéger les données contre tout traitement non autorisé ou illégal et contre toute perte, destruction ou dommage accidentel.



CHAPITRE 1

Protéger les données utilisateurs

1. Obfuscation du code source
2. Règles de protection des données utilisateurs
3. **Droits d’accès des utilisateurs d’une application**
4. Accès sécurisé aux données de l’application
5. Cryptage des données

Définition

Les droits d'accès sont les autorisations dont dispose un utilisateur individuel ou une application informatique pour lire, écrire, modifier, supprimer ou accéder d'une autre manière à un fichier informatique ; modifier les configurations ou les paramètres, ou ajouter ou supprimer des applications.

L'administrateur réseau ou informatique d'une entreprise peut définir des autorisations pour des fichiers, des serveurs, des dossiers ou des applications spécifiques sur l'ordinateur.

Dans une application CRM (Client Relationship Manager), la création de droits d'accès pour les utilisateurs permet aux employés de différents services d'examiner les informations sur le client et - en particulier dans le cas des appels au service clientèle - l'historique des appels et des services.

Par exemple, ceux qui aident un client à résoudre un problème technique lié à l'Internet ou au câble peuvent voir quand le client a appelé, avec qui il a parlé, les conversations ou les solutions précédentes et le résultat.

Comment l'accès des utilisateurs est-il mis en œuvre ?

Le contrôle d'accès basé sur les rôles permet aux organisations d'améliorer leur posture de sécurité et de se conformer aux réglementations en la matière. Cependant, la mise en œuvre du contrôle d'accès basé sur les rôles dans l'ensemble d'une organisation peut s'avérer complexe et susciter des réticences de la part des parties prenantes.

Pour réussir le passage au RBAC, le processus de mise en œuvre doit être traité comme une série d'étapes :

- **Comprendre les besoins de votre entreprise** - Avant d'adopter le système RBAC, l'administrateur doit effectuer une analyse complète des besoins afin d'examiner les fonctions, les processus opérationnels et les technologies. Il doit également tenir compte des exigences réglementaires ou d'audit et évaluer la situation actuelle de l'organisation en matière de sécurité. Il peut également bénéficier d'autres types de contrôle d'accès.
- **Planification de la portée de la mise en œuvre** - L'administrateur identifie la portée des exigences RBAC et planifie la mise en œuvre pour s'aligner sur les besoins de l'organisation. Réduisez son champ d'application pour vous concentrer sur les systèmes ou les applications qui stockent des données sensibles. Cela aidera également l'organisation à gérer la transition.
- **Définir les rôles** - il sera plus facile de définir les rôles une fois qu'il aura effectué l'analyse des besoins et compris comment les individus exécutent leurs tâches. Il faut faire attention aux pièges courants de la conception des rôles, comme la granularité excessive ou insuffisante, le chevauchement des rôles et l'octroi de trop d'exceptions pour les autorisations RBAC.
- **Mise en œuvre** - la dernière phase consiste à déployer le RBAC. Elle peut se faire par étapes, afin d'éviter une charge de travail trop importante et de réduire les perturbations pour l'entreprise;
    - S'adresser à un groupe central d'utilisateurs.
    - Commencer par un contrôle d'accès à gros grain avant d'augmenter la granularité.
    - Recueillir les réactions des utilisateurs et surveiller l'environnement pour planifier les étapes suivantes de la mise en œuvre.

Comment l'accès des utilisateurs est-il mis en œuvre ?

Pour la plupart des dirigeants d'entreprise, l'idée de mettre en œuvre une politique d'accès sécurisé des utilisateurs vous semble fastidieuse et contre-productive.

Votre politique d'accès des utilisateurs bien organisée garantira que chaque utilisateur dispose de ce dont il a besoin pour faire son travail. Ce à quoi il n'a pas accès n'affectera pas ses activités, car il n'en a pas besoin.

La création d'une première politique prend certes du temps, mais ces avantages sont considérables. Une fois la politique créée, un examen périodique régulier garantira que les actifs sensibles restent protégés.

Le contrôle d'accès basé sur les rôles (RBAC)

Le contrôle d'accès basé sur les rôles est une technique qui consiste à attribuer des autorisations d'accès aux utilisateurs de votre organisation en fonction de leurs rôles et des tâches qu'ils effectuent.

La sécurité du contrôle d'accès basé sur les rôles garantit que les utilisateurs n'ont accès qu'aux informations ou aux fichiers qui sont pertinents pour leur poste ou leur projet actuel.

Dans les organisations qui comptent de grandes divisions, la mise en place d'un système de contrôle d'accès basé sur les rôles est essentielle pour limiter les pertes de données.

Mise en œuvre du contrôle d'accès basé sur les rôles

Le contrôle d'accès basé sur les rôles permet aux organisations d'améliorer leur posture de sécurité et de se conformer aux réglementations en la matière. Cependant, la mise en œuvre du contrôle d'accès basé sur les rôles dans l'ensemble d'une organisation peut s'avérer complexe et susciter des réticences de la part des parties prenantes.

Pour réussir le passage au RBAC, le processus de mise en œuvre doit être traité comme une série d'étapes :

- **Comprendre les besoins de votre entreprise** - Avant d'adopter le système RBAC, l'administrateur doit effectuer une analyse complète des besoins afin d'examiner les fonctions, les processus opérationnels et les technologies. Il doit également tenir compte des exigences réglementaires ou d'audit et évaluer la situation actuelle de l'organisation en matière de sécurité. Il peut également bénéficier d'autres types de contrôle d'accès.
- **Planification de la portée de la mise en œuvre** - L'administrateur identifie la portée des exigences RBAC et planifie la mise en œuvre pour s'aligner sur les besoins de l'organisation. Réduisez son champ d'application pour vous concentrer sur les systèmes ou les applications qui stockent des données sensibles. Cela aidera également l'organisation à gérer la transition.
- **Définir les rôles** - il sera plus facile de définir les rôles une fois qu'il aura effectué l'analyse des besoins et compris comment les individus exécutent leurs tâches. Il faut faire attention aux pièges courants de la conception des rôles, comme la granularité excessive ou insuffisante, le chevauchement des rôles et l'octroi de trop d'exceptions pour les autorisations RBAC.
- **Mise en œuvre** - la dernière phase consiste à déployer le RBAC. Elle peut se faire par étapes, afin d'éviter une charge de travail trop importante et de réduire les perturbations pour l'entreprise;
    - S'adresser à un groupe central d'utilisateurs.
    - Commencer par un contrôle d'accès à gros grain avant d'augmenter la granularité.
    - Recueillir les réactions des utilisateurs et surveiller l'environnement pour planifier les étapes suivantes de la mise en œuvre.

Types de contrôle d'accès

Les mesures de contrôle d'accès déterminent qui peut consulter ou utiliser les ressources d'un système informatique, en s'appuyant souvent sur une authentification ou une autorisation basée sur les identifiants de connexion. Elles sont essentielles pour minimiser les risques opérationnels. Les systèmes de contrôle d'accès peuvent être physiques, limitant l'accès aux bâtiments, aux salles ou aux serveurs, ou logiques, contrôlant l'accès numérique aux données, aux fichiers ou aux réseaux.

Voici quelques exemples de ces types de contrôle d'accès :

Contrôle d'accès discrétionnaire (CAD)

Le propriétaire d'un système ou d'une ressource protégée établit des politiques définissant qui peut y accéder. Le CDA peut impliquer des mesures physiques ou numériques.

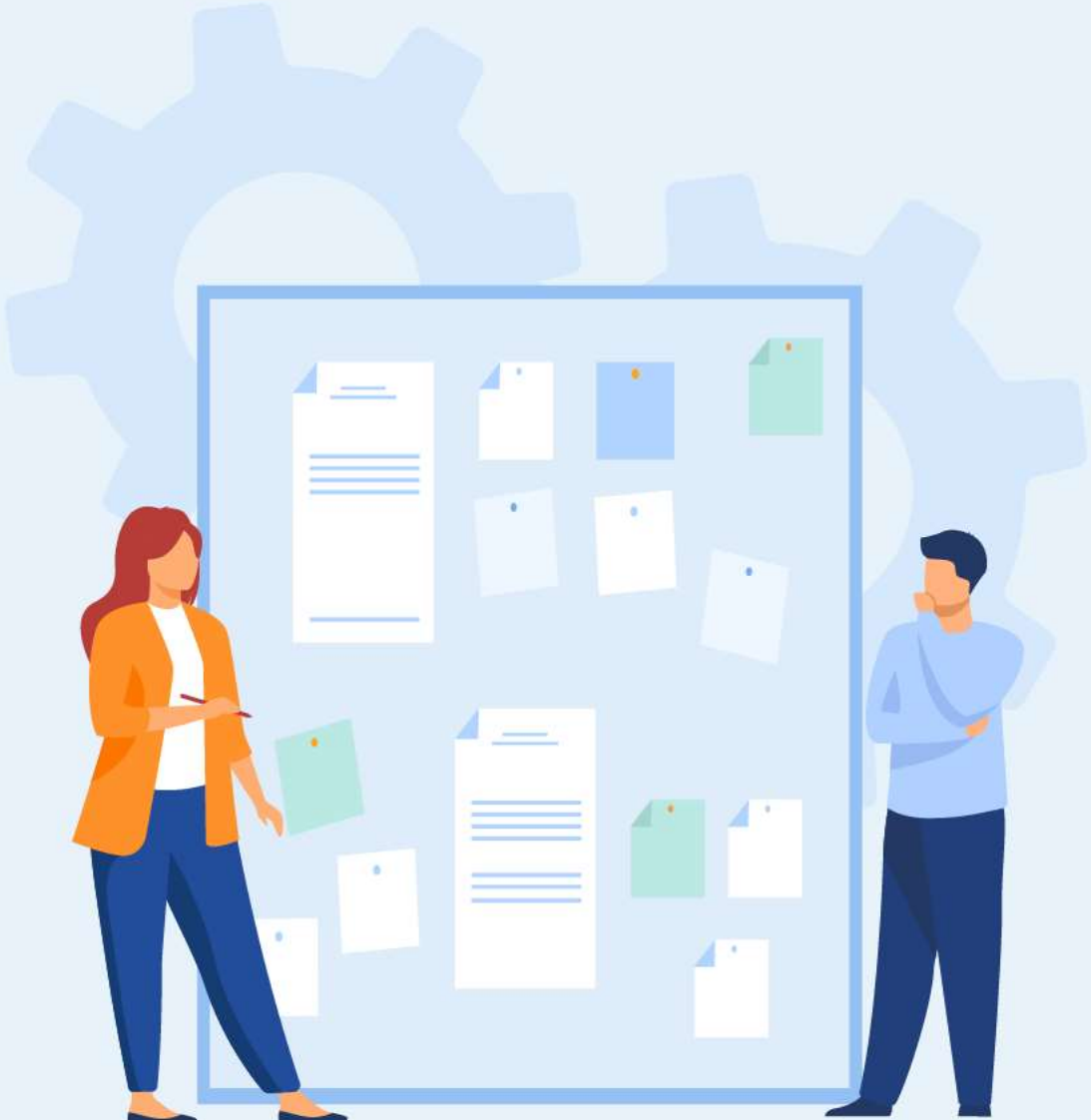
Il est moins restrictif que les autres systèmes de contrôle d'accès, car il offre aux individus un contrôle total sur les ressources qu'ils possèdent. Cependant, il est également moins sûr, car les programmes associés héritent des paramètres de sécurité et permettent aux logiciels malveillants de les exploiter à l'insu de l'utilisateur final.

Contrôle d'accès obligatoire (MAC)

Une autorité centrale réglemente les droits d'accès en fonction de plusieurs niveaux de sécurité.

Le MAC consiste à attribuer des classifications aux ressources du système et au noyau de sécurité ou au système d'exploitation.

Seuls les utilisateurs ou les appareils possédant l'habilitation requise en matière de sécurité des informations peuvent accéder aux ressources protégées. Les organisations ayant différents niveaux de classification des données, comme les institutions gouvernementales et militaires, utilisent généralement le MAC pour classifier tous les utilisateurs finaux.



CHAPITRE 1

Protéger les données utilisateurs

1. Obfuscation du code source
2. Règles de protection des données utilisateurs
3. Droits d’accès des utilisateurs d’une application
4. **Accès sécurisé aux données de l’application**
5. Cryptage des données

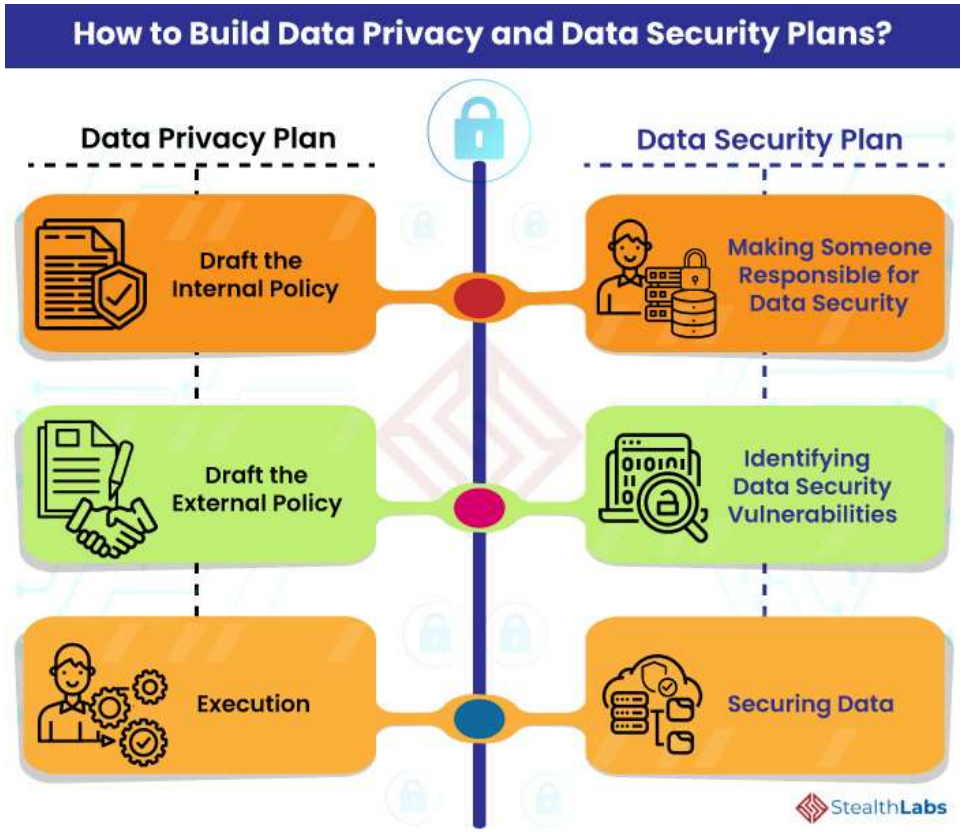
Pourquoi la sécurité des données est-elle importante ?

La sécurité des données consiste à protéger les informations numériques contre les accès non autorisés, la corruption ou le vol tout au long de leur cycle de vie.

Il s'agit d'un concept qui englobe tous les aspects de la sécurité de l'information, de la sécurité physique du matériel et des dispositifs de stockage aux contrôles administratifs et d'accès, en passant par la sécurité logique des applications logicielles.

Il inclut également les politiques et procédures organisationnelles.

La sécurité des données implique le déploiement d'outils et de technologies qui améliorent la visibilité de l'organisation sur l'endroit où résident ses données critiques et sur la manière dont elles sont utilisées. Idéalement, ces outils devraient être en mesure d'appliquer des protections telles que le **cryptage**, le **masquage des données** et la **rédaction de fichiers sensibles**, et devraient automatiser la création de rapports afin de simplifier les audits et le respect des exigences réglementaires.



les principaux points pour élaborer un solide plan de confidentialité des données

PARTIE 2

Types de sécurité des données

Cryptage

En utilisant un algorithme pour transformer des caractères de texte normaux en un format illisible, les clés de cryptage brouillent les données afin que seuls les utilisateurs autorisés puissent les lire. Les solutions de cryptage de fichiers et de bases de données constituent une dernière ligne de défense pour les volumes sensibles en masquant leur contenu par le biais du cryptage ou de la tokenisation (*système de jetons*). La plupart des solutions comprennent également des fonctions de gestion des clés de sécurité.

Effacement des données

Plus sûr que l'effacement standard des données, l'effacement des données utilise un logiciel pour écraser complètement les données sur tout dispositif de stockage. Il vérifie que les données sont irrécupérables.

Masquage des données

En masquant les données, les organisations peuvent permettre aux équipes de développer des applications ou de former des personnes en utilisant des données réelles. Il masque les informations personnelles identifiables (PII) lorsque cela est nécessaire pour que le développement puisse se faire dans des environnements conformes.

Résilience des données

La résilience est déterminée par la capacité d'une organisation à supporter ou à se remettre de tout type de défaillance, qu'il s'agisse de problèmes matériels, de coupures de courant ou d'autres événements qui affectent la disponibilité des données. La rapidité de la récupération est essentielle pour minimiser l'impact.

PARTIE 2

Qu'est-ce que la gestion de l'accès aux données ?

La gestion de l'accès aux données est un ensemble de processus et de technologies utilisés pour contrôler l'accès aux applications ou aux données. Elle implique la création de groupes ou de rôles avec des privilèges d'accès définis, puis le contrôle de l'accès en définissant les appartenances aux groupes.

Ces processus s'appuient sur le principe de sécurité de l'information du "moindre privilège" (ou "moindre autorité"), selon lequel chaque utilisateur ne doit pouvoir accéder qu'aux informations ou ressources nécessaires à son travail.

La gestion de l'accès aux données permet à l'organisation de maintenir un environnement sécurisé qui non seulement empêche toute utilisation non autorisée, mais évite également les violations de données susceptibles de briser la confiance des clients et d'entraîner des pénalités financières.

Pour éviter des détournements de comptes d'utilisateurs, il est recommandé d'utiliser le système de double authentification (2 factor authentification abrégé 2FA) le plus sécurisé.

Les bonnes pratiques en gestion de l'accès aux données

Implémenter une sécurité à confiance zéro

La meilleure stratégie dans le contexte dynamique des réseaux d'entreprise modernes consiste à supposer que personne n'est digne de confiance, sauf preuve du contraire.

Le modèle de confiance zéro est axé sur l'authentification continue des consommateurs : les activités sont suivies et les niveaux de risque sont évalués au cours de chaque session. La confiance zéro équipe un dispositif pour identifier les comportements anormaux qui suggèrent une violation ou une infraction à la loi.

Utilisation de l'authentification multifactorielle

L'authentification multifactorielle ou AMF est la première étape de la création de couches de confiance pour les comptes de vos consommateurs. Outre le mot de passe, elle offre deux couches supplémentaires d'authentification.

- Quelque chose que vos consommateurs possèdent.
- Quelque chose dont vos consommateurs ont hérité.

Le premier élément peut être une clé ou un laissez-passer de sécurité. La seconde est constituée d'éléments biométriques, par exemple des scanners rétiniens, des empreintes digitales ou une reconnaissance vocale que vos clients ont configurés.

L'AMF garantit que le pirate doit toujours franchir une autre couche de sécurité pour accéder à votre système.

Les bonnes pratiques en gestion de l'accès aux données

Il faut éviter les comptes privilégiés

Le principe du moindre privilège (également connu sous le nom de principe de moindre autorité) s'applique à la pratique consistant à attribuer à un consommateur des niveaux d'accès - ou des autorisations - minimaux, essentiels à l'accomplissement de son rôle et des tâches correspondantes.

Bien que les comptes privilégiés soient nécessaires pour certaines tâches, ils ne devraient pas être utilisés comme une pratique quotidienne. Car si une violation de données survient sur de tels comptes, le résultat peut être catastrophique.

Un moyen efficace de réduire la possibilité de violations de données internes et externes est le contrôle d'accès basé sur les rôles (RBAC) ou la restriction de l'accès non essentiel aux informations sensibles.

Vous pouvez appliquer cette meilleure pratique de gestion des identités et des accès en offrant l'accès à un consommateur pour une durée déterminée (par exemple, 30 minutes), puis en le révoquant automatiquement. Cette micro-gestion de l'accès peut améliorer le quotient global de cybersécurité.

Les bonnes pratiques en gestion de l'accès aux données

Appliquer une politique de mots de passe forts

Les mots de passe forts ont toujours été l'un des piliers d'une stratégie IAM efficace. Les meilleurs doivent être faciles à retenir et difficiles à deviner. Voici quelques bonnes pratiques pour la création de mots de passe recommandées.

- La longueur idéale doit être comprise entre huit et au moins 64 caractères.
- Utilisez des caractères spéciaux.
- Évitez les caractères séquentiels et répétitifs comme (par exemple, 12345 ou abcde).
- Mettez en place une politique d'expiration des mots de passe.
- Limitez l'utilisation de mots du dictionnaire comme mots de passe.

L'adoption d'une politique de mot de passe bien pensée présente quatre avantages principaux.

Procédures d'embarquement en libre-service

L'intégration en libre-service permet aux consommateurs de s'intégrer eux-mêmes. Le parcours **d'onboarding** commence souvent par une page d'inscription. La tâche consiste à faire passer les consommateurs de la page d'inscription à l'activation. En fin de compte, cela aide aussi à les retenir.

PARTIE 2

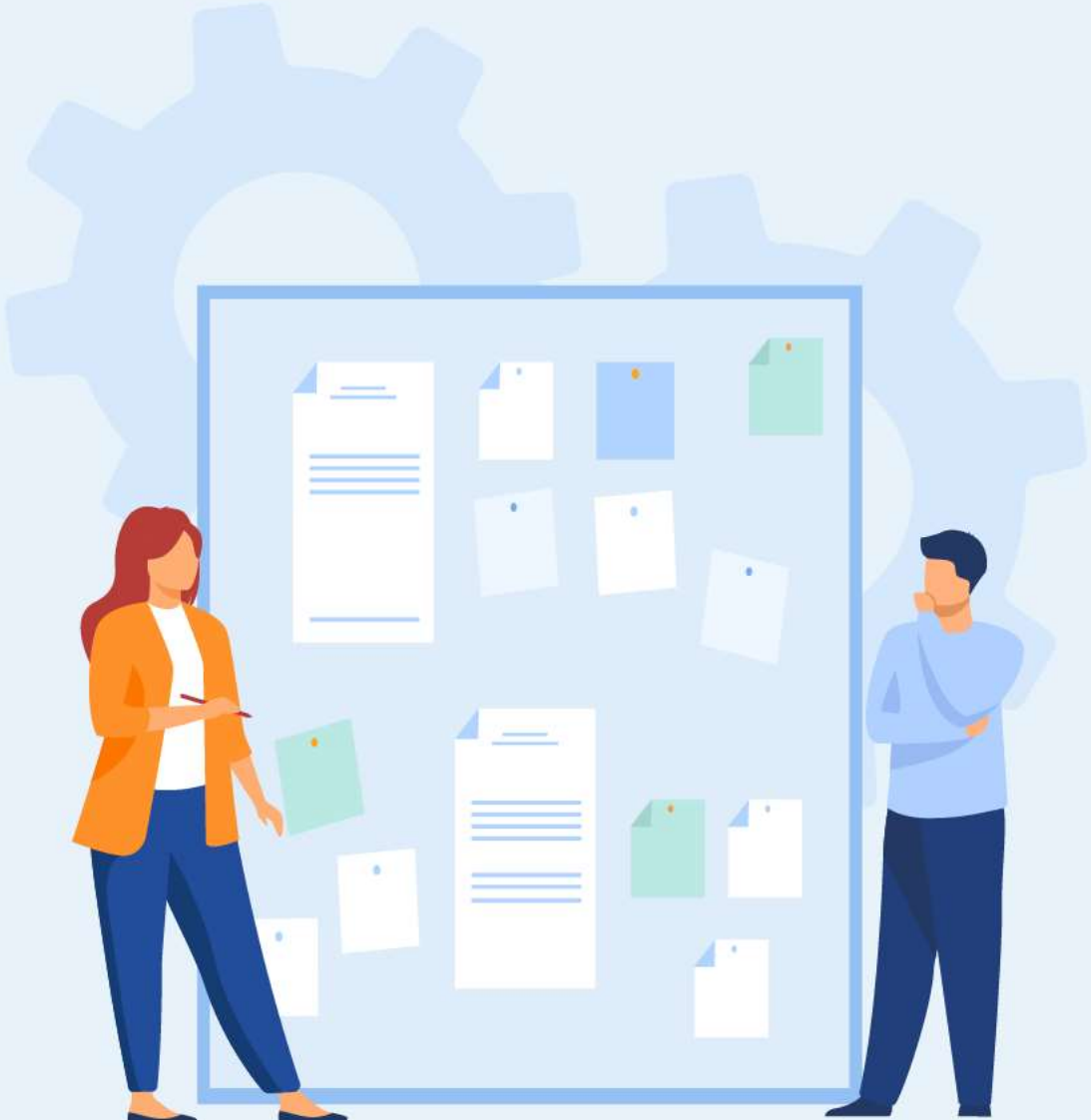
Les bonnes pratiques en gestion de l'accès aux données

Sans mot de passe

Comme son nom l'indique, la connexion sans mot de passe est la méthode d'authentification des consommateurs sans qu'ils aient besoin de saisir un mot de passe. Les avantages d'une connexion sans mot de passe sont nombreux : amélioration de l'expérience globale du consommateur, qui n'a plus besoin de mémoriser d'informations d'identification, gain de temps et de productivité, sécurité plus solide contre les attaques telles que le phishing, le bourrage d'informations d'identification et la force brute, et plus grande facilité d'accès.

La connexion sans mot de passe peut être mise en œuvre par différentes approches. Voici les approches les plus courantes :

- **La connexion par courrier électronique** : Les consommateurs peuvent se connecter au moyen d'un code unique envoyé à l'identifiant de messagerie associé.
- **Connexion par SMS** : Les consommateurs peuvent se connecter grâce à un code unique envoyé au numéro de téléphone associé.
- **Connexion par biométrie** : Les consommateurs peuvent se connecter grâce à des technologies biométriques telles que les empreintes digitales, le visage ou l'iris.
- **Connexion sociale** : Les consommateurs peuvent se connecter via leurs comptes de médias sociaux existants tels que Facebook, Twitter ou Google.



CHAPITRE 1

Protéger les données utilisateurs

1. Obfuscation du code source
2. Règles de protection des données utilisateurs
3. Droits d'accès des utilisateurs d'une application
4. Accès sécurisé aux données de l'application
5. **Cryptage des données**

Définition

Le cryptage des données est une méthode de sécurité dans laquelle les informations sont codées et ne peuvent être consultées ou décryptées que par un utilisateur disposant de la bonne clé de cryptage.

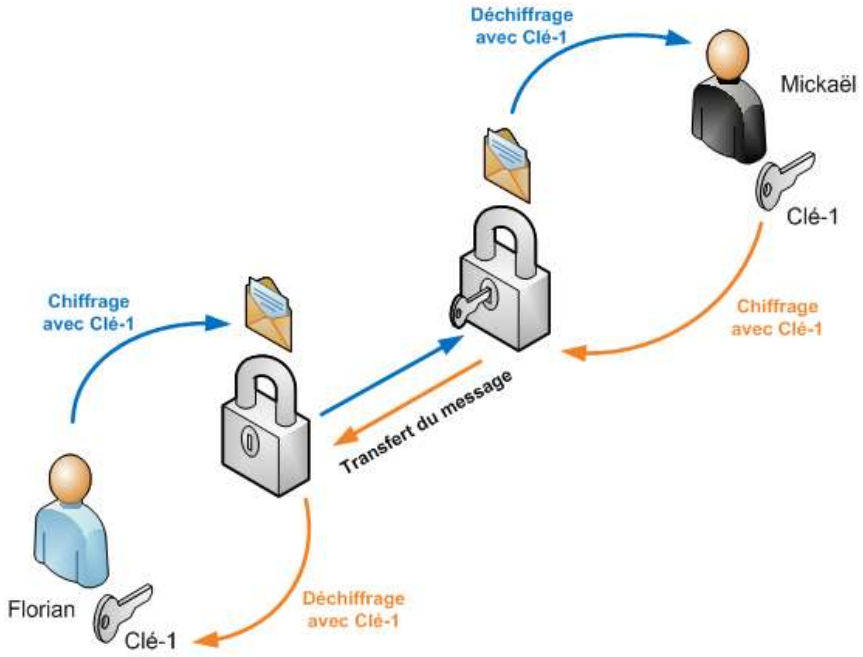
Les données cryptées, également appelées texte chiffré, apparaissent brouillées ou illisibles pour une personne ou une entité qui y accède sans autorisation.

Comment le cryptage des données est-il utilisé ?

Le cryptage des données est utilisé pour dissuader les parties malveillantes ou négligentes d'accéder à des données sensibles. Ligne de défense importante dans une architecture de cybersécurité, le cryptage rend l'utilisation des données interceptées aussi difficile que possible.

Il peut être appliqué à toutes sortes de besoins en matière de protection des données, qu'il s'agisse d'informations gouvernementales confidentielles ou de transactions personnelles par carte de crédit.

Le logiciel de cryptage des données, également connu sous le nom d'algorithme de cryptage ou de chiffre, est utilisé pour développer un schéma de cryptage qui, en théorie, ne peut être cassé qu'avec une grande puissance de calcul.



Le chiffrement symétrique est un chiffrement dans lequel la clé de chiffrement sert également à déchiffrer. On parle alors de clé secrète.

PARTIE 2

Comment fonctionne le cryptage ?

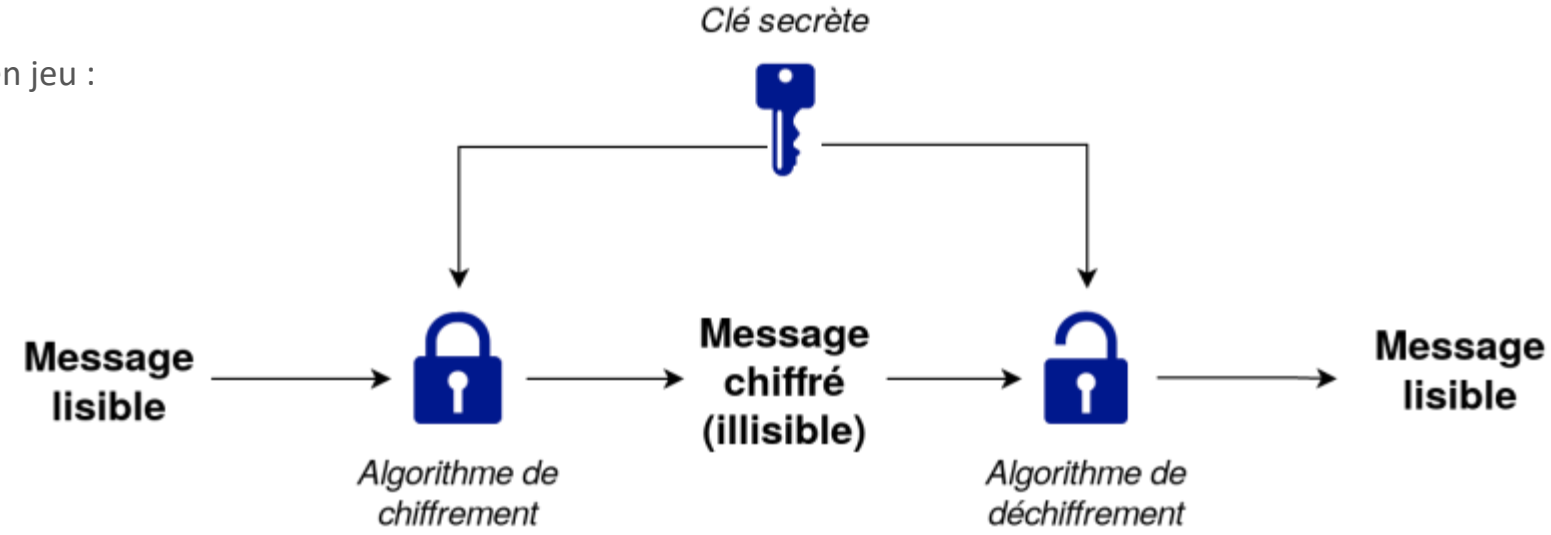
Maintenant que nous avons bien compris le concept de cryptage, voyons comment il fonctionne exactement.

En termes simples, le cryptage utilise des algorithmes pour mélanger les données que vous souhaitez crypter. Avant d'envoyer le message ou les données à la personne qui les reçoit, vous devez disposer d'une clé générée de manière aléatoire, grâce à laquelle elle pourra les décrypter.

Imaginez que vous ayez mis un verrou sur la boîte contenant des documents importants à l'aide d'une clé. Vous envoyez cette boîte à votre amie. Elle possède la même clé que vous, ce qui lui permet de la déverrouiller et d'accéder à ces documents importants. Mais dans le monde numérique, tout cela se fait électroniquement !

Il y a donc trois niveaux de cryptage qui sont en jeu :

- Texte en clair
- Texte chiffré
- Texte décrypté (identique au texte initial).



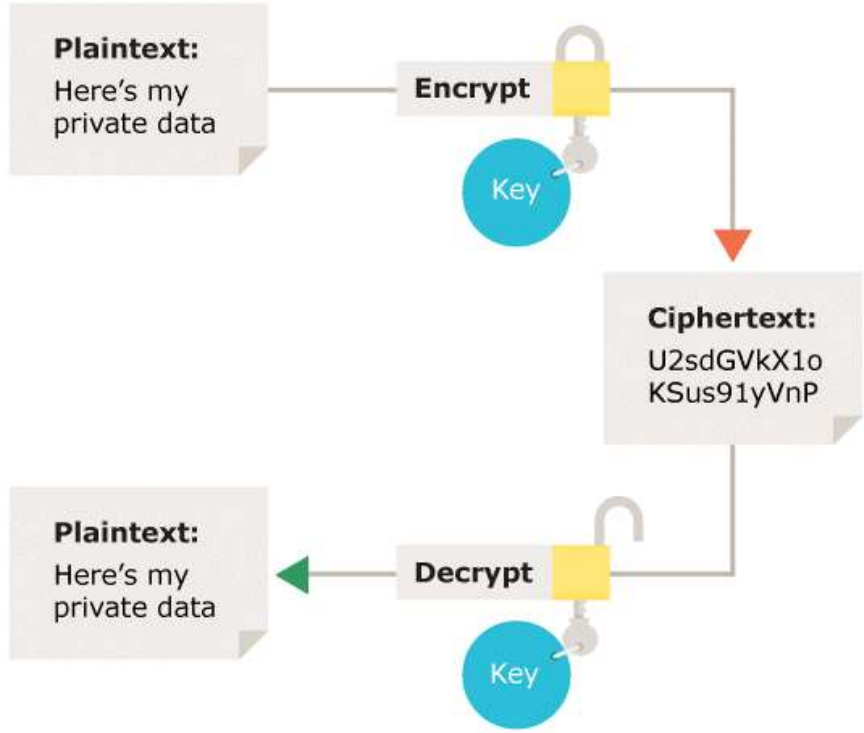
PARTIE 2

Les méthodes de cryptage des données

Il existe deux méthodes de cryptage largement utilisés aujourd'hui **: le cryptage symétrique et le cryptage asymétrique**. Le nom provient du fait que la même clé est utilisée ou non pour le cryptage et le décryptage.

Le cryptage symétrique

Dans le cryptage symétrique, la même clé est utilisée pour le cryptage et le décryptage. Il est donc essentiel d'envisager une méthode sécurisée pour transférer la clé entre l'expéditeur et le destinataire.



Cryptage symétrique - Utilisation de la même clé pour le cryptage et le décryptage.

PARTIE 2

Les méthodes de cryptage des données

Le cryptage asymétrique

Le cryptage asymétrique utilise la notion de paire de clés : une clé différente est utilisée pour le processus de cryptage et de décryptage. L'une des clés est généralement appelée clé privée et l'autre clé est appelée clé publique.

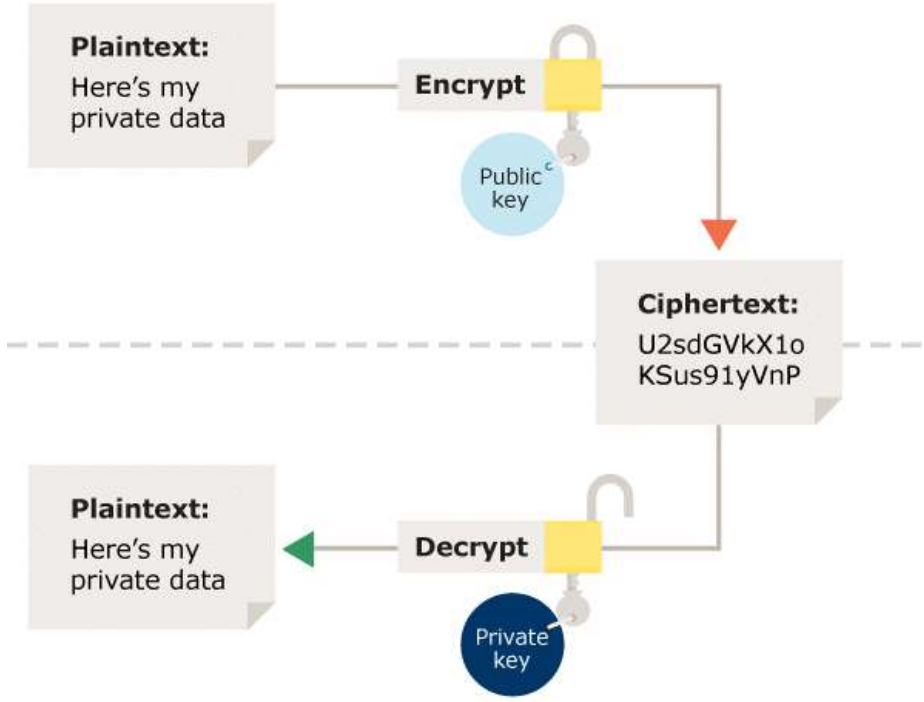
La clé privée est gardée secrète par le propriétaire et la clé publique est soit partagée entre les destinataires autorisés, soit mise à la disposition du grand public.

Les données cryptées avec la clé publique du destinataire ne peuvent être décryptées qu'avec la clé privée correspondante. Les données peuvent donc être transférées sans risque d'accès non autorisé ou illégal aux données.

Le hachage

Le hachage est une technique qui génère une valeur de longueur fixe résumant le contenu d'un fichier ou d'un message. Elle est souvent considérée, à tort, comme une méthode de cryptage.

Les fonctions de hachage sont utilisées avec la cryptographie pour fournir des signatures numériques et des contrôles d'intégrité, mais comme aucune clé secrète n'est utilisée, le message n'est pas privé car le hachage peut être recréé.



Cryptage asymétrique - Utilisation d'une clé différente pour le processus de cryptage et de décryptage.

PARTIE 2

Les types de cryptage des données

Au fur et à mesure que la technologie progresse, les techniques de cryptage modernes ont remplacé les techniques dépassées. Par conséquent, il existe plusieurs types de logiciels de cryptage qui nous ont facilité la tâche.

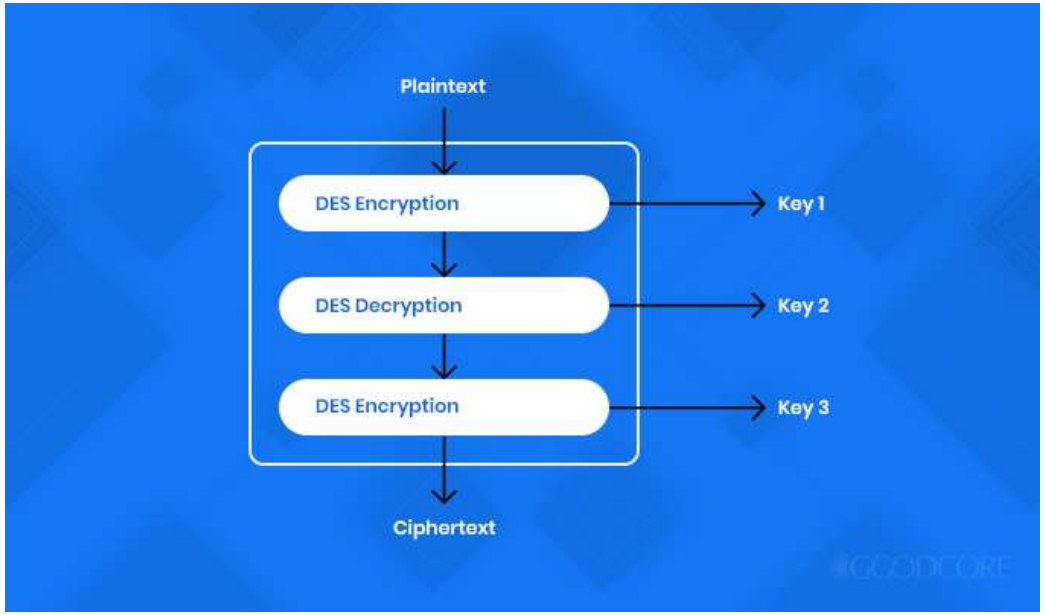
Triple DES

L'algorithme de chiffrement triple des données ou Triple-DES utilise le chiffrement symétrique. Il s'agit d'une version avancée du chiffrement par blocs DES, dont la clé était auparavant de 56 bits. Toutefois, et comme son nom l'indique, TDES chiffre les données en utilisant trois fois une clé de 56 bits, ce qui en fait une clé de 168 bits. Il fonctionne en trois phases lors du cryptage des données :

1. crypter
2. décryptage
3. re-cryptage

De même, les phases de décryptage sont les suivantes :

1. décrypter
2. crypter
3. décrypter à nouveau



Cryptage asymétrique - Utilisation d'une clé différente pour le processus de cryptage et de décryptage.

PARTIE 2

Les types de cryptage des données

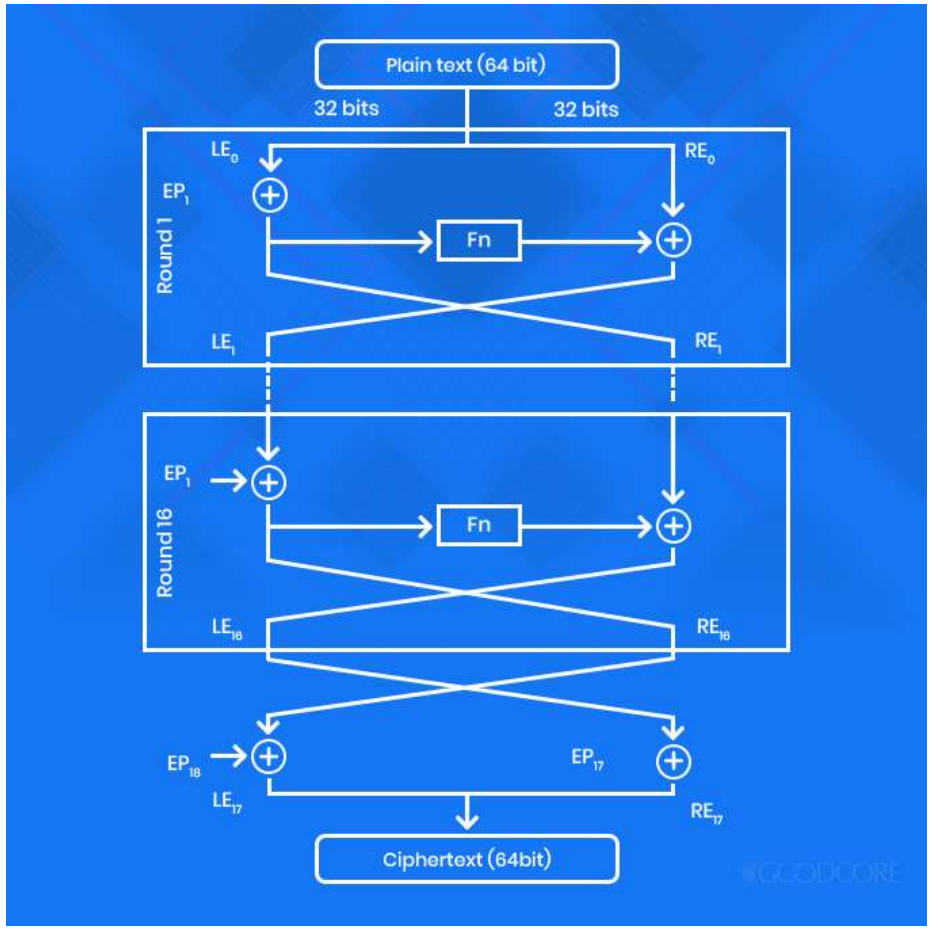
AES

L'Advanced Encryption Standard (AES) utilise le chiffrement par blocs et crypte un bloc de taille fixe à la fois. Il fonctionne en 128 ou 192 bits mais peut être étendu jusqu'à une longueur de clé de 256 bits. Pour crypter chaque bit, il y a différents tours. Par exemple, la clé 128 bits comporte 10 tours, la clé 192 bits en comporte 12, etc.

Il est considéré comme l'un des meilleurs algorithmes de cryptage et également l'un des types de cryptage les plus sûrs, car il fonctionne avec une seule clé privée.

Blowfish

Autre algorithme de chiffrement conçu pour remplacer DES, **Blowfish** est un chiffrement par blocs symétrique, qui fonctionne avec une longueur de clé variable de 32 à 448 bits. Comme il s'agit d'un chiffrement par blocs, il divise les données ou un message en blocs fixes de 64 bits lors du cryptage et du décryptage.



Modèle de cryptage Blowfish

PARTIE 2

Les types de cryptage des données

Twofish

Également un chiffrement par blocs symétrique, **Twofish** est une version avancée du chiffrement **Blowfish**. Il possède une taille de bloc de 128 bits et peut s'étendre à une longueur de clé de 256 bits. Comme les autres chiffrements symétriques, il décompose également les données en blocs de longueur fixe.

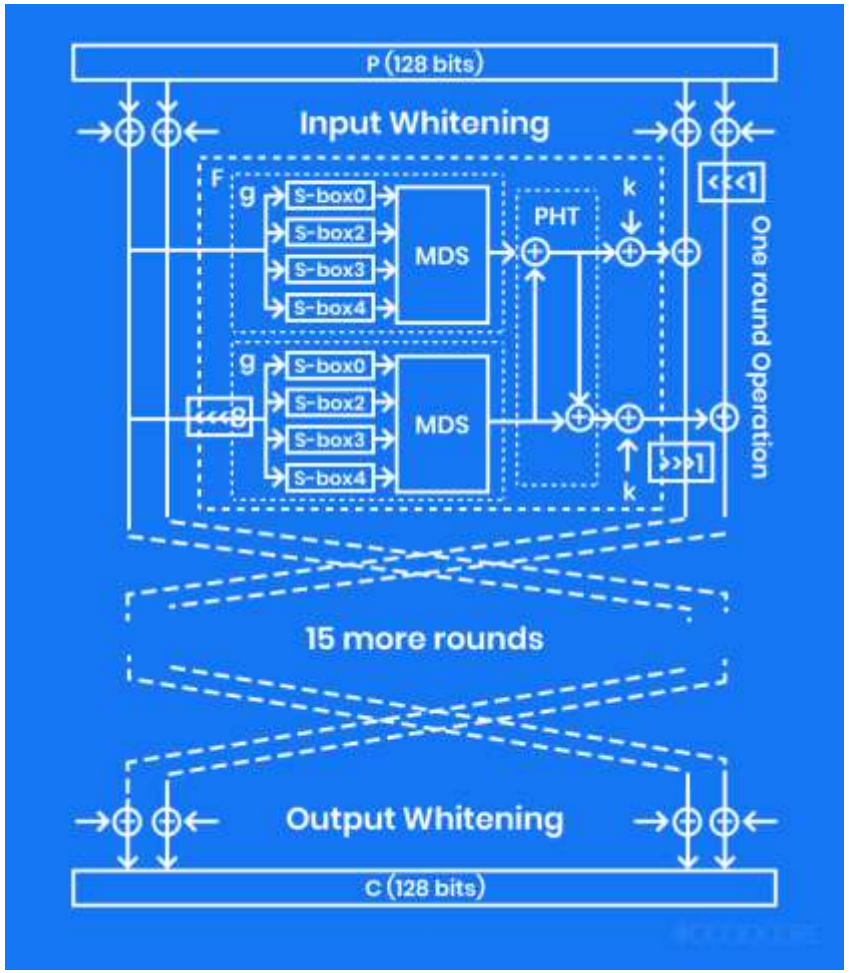
Cependant, il fonctionne en 16 cycles, quelle que soit la taille des données. Parmi les différents types de cryptage, celui-ci est flexible. Il vous permet de choisir un processus de cryptage rapide et une configuration de clé lente, et vice versa.

FPE

Le cryptage avec préservation du format (FPE) est l'une des méthodes de cryptage les plus récentes. Elle crypte vos données dans un format similaire. Par exemple, si vous avez crypté votre mot de passe en utilisant 6 lettres, 5 chiffres et 4 lettres spéciales, votre résultat sera une combinaison différente d'un format similaire.

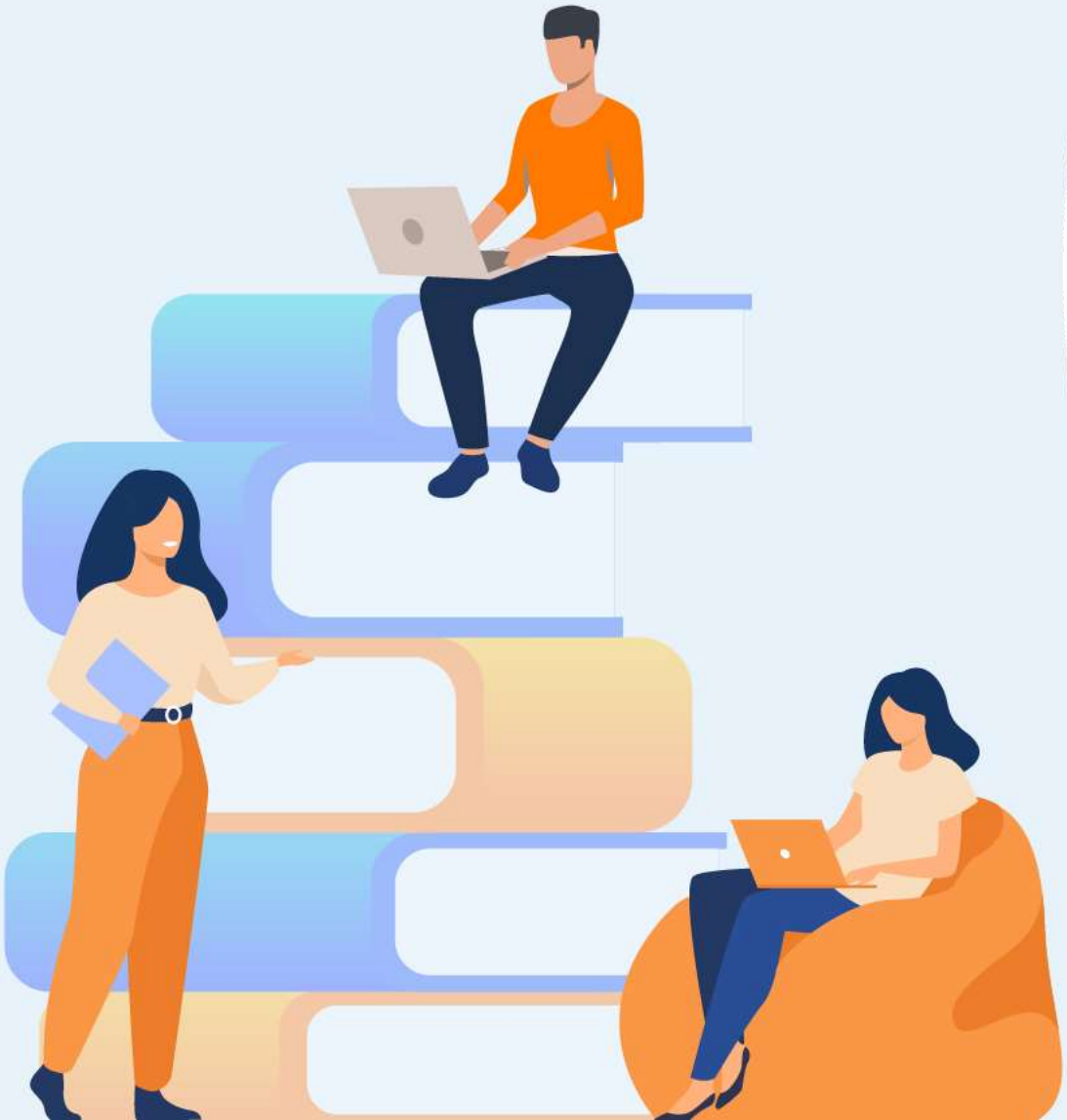
En d'autres termes, si vous utilisez cette technique de cryptage, elle préservera le format de votre texte en clair, c'est-à-dire qu'après le cryptage, la structure de vos données restera la même.

Elle est largement utilisée dans les systèmes de bases de données financières, les systèmes bancaires, la revente au détail, etc.



Modèle de cryptage Twofish

PARTIE 2



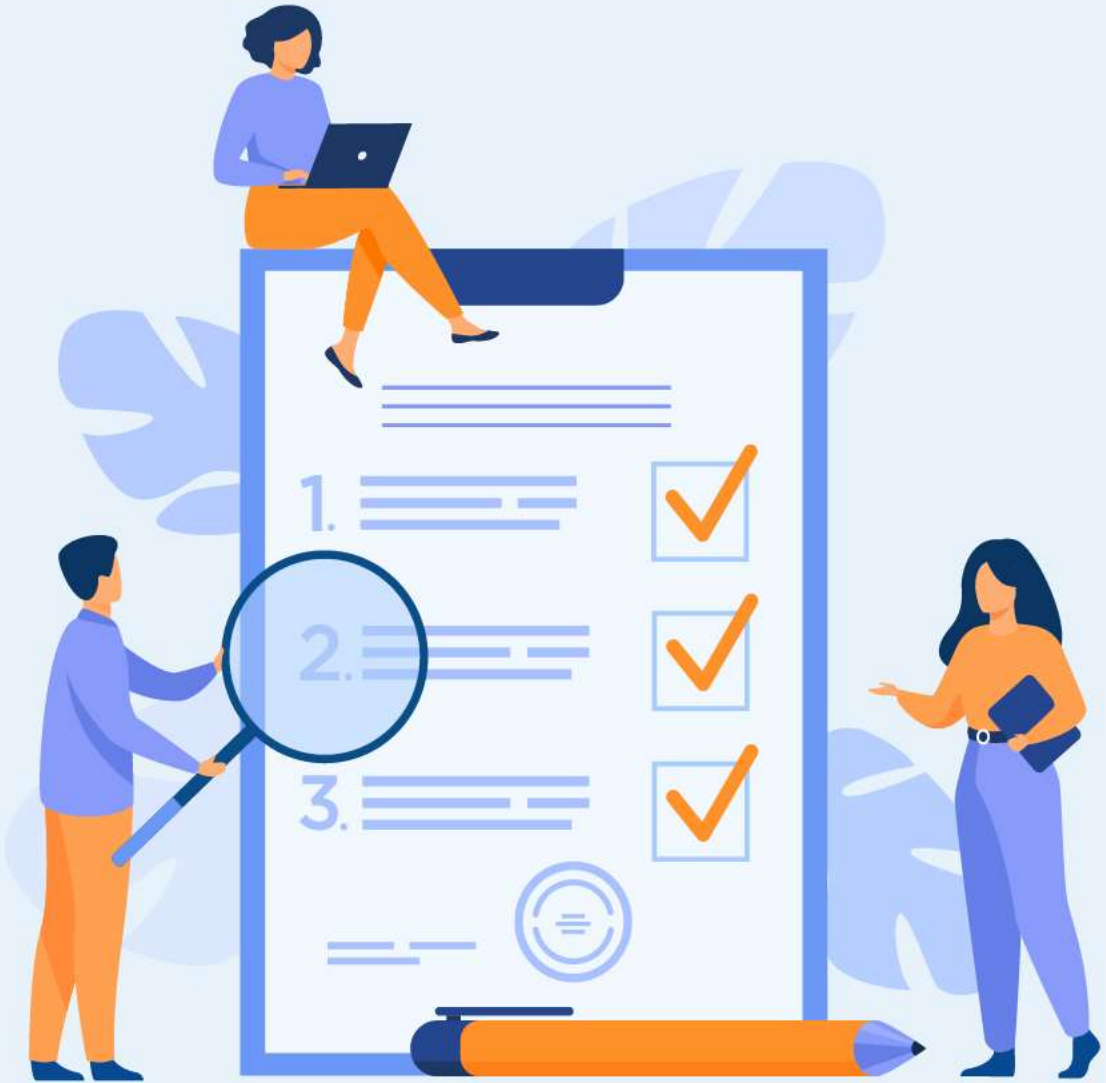
PARTIE 3

Protéger les applications Web

Dans ce module, vous allez :

- Sécuriser un service
- Utiliser les firewalls

05 heures

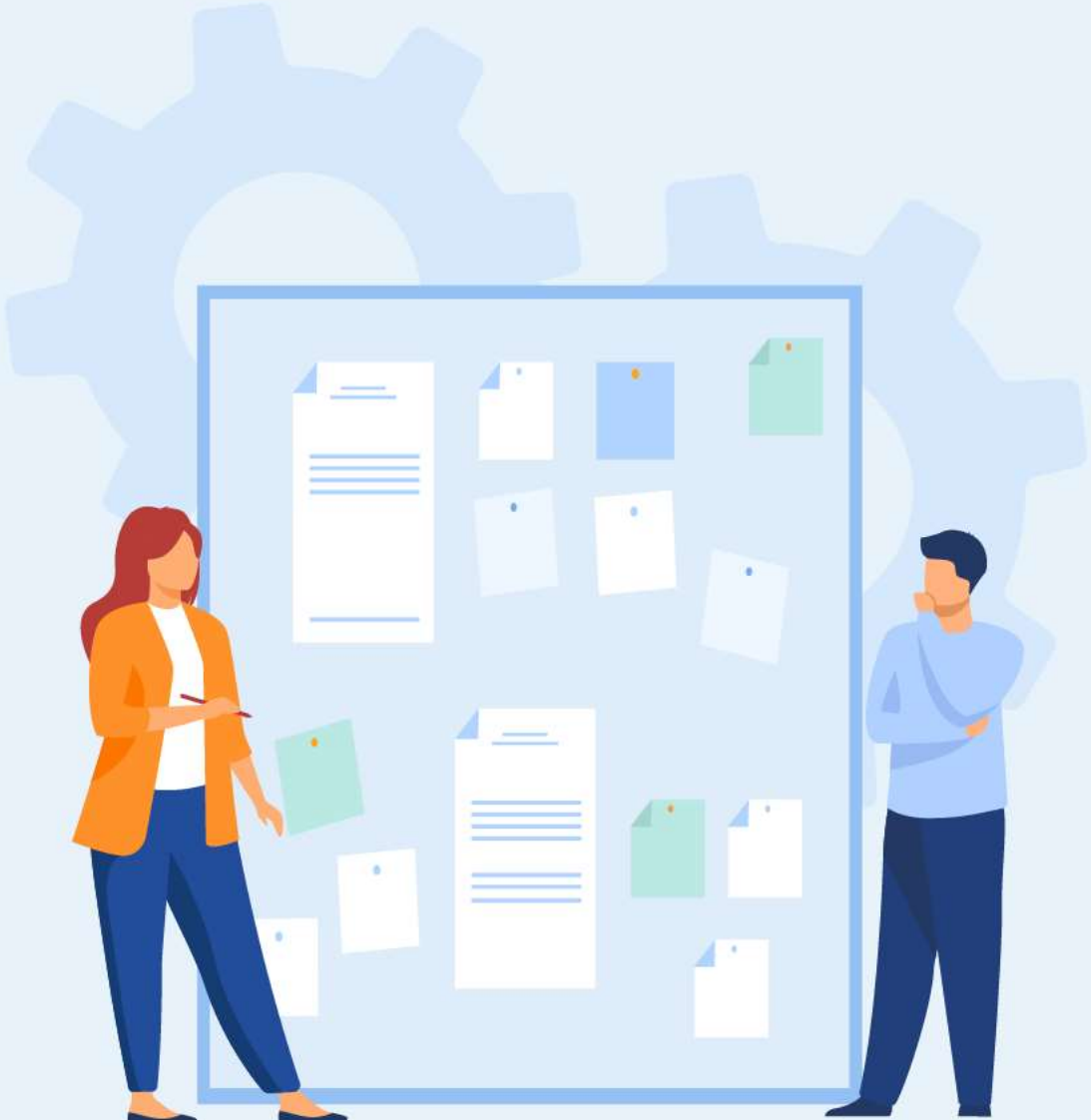


Sécuriser un service

Ce que vous allez apprendre dans ce chapitre :

- Gestion de la politique d’utilisation des mots de passe
- Gestion des rôles d’utilisateurs
- Chiffrements symétriques et asymétrique
- Notion de private/public Key

03 heures



Sécuriser un service

1. **Gestion de la politique d’utilisation des mots de passe**
2. Gestion des rôles d’utilisateurs
3. Chiffrements symétriques et asymétrique
4. Notion de private/public Key

Introduction

Une politique de mot de passe est un ensemble de règles destinées à renforcer la sécurité informatique en encourageant les utilisateurs à employer des mots de passe forts et à les utiliser correctement.

Une politique de mot de passe fait souvent partie du règlement officiel d'une organisation et peut être enseignée dans le cadre d'une formation de sensibilisation à la sécurité.

Soit la politique de mot de passe est simplement consultative, soit les systèmes informatiques obligent les utilisateurs à s'y conformer. 1

1) Password policy - Wikipedia

les meilleures clés pour une politique de sécurité des mots de passe

Utilisez des mots de passe complexes : Cela peut sembler élémentaire. Mais les mots de passe simples sont facilement compromis. L'application d'exigences en matière de complexité est une bonne première étape pour mettre fin aux tentatives de piratage par force brute. Vous pouvez exiger que tous les utilisateurs créent des mots de passe qui ne font pas référence au nom légal ou au nom d'utilisateur de l'utilisateur. Les mots de passe robustes utilisent également des combinaisons de caractères, de chiffres, ainsi que des lettres majuscules et minuscules.

Définissez la longueur minimale des mots de passe : Vous pouvez renforcer la robustesse des mots de passe au sein de votre organisation en fixant une longueur minimale de caractères. Une pratique courante est un minimum de huit caractères. Une longueur minimale de 14 caractères est la meilleure norme.

Utilisez des phrases de passe : Les comptes des administrateurs de domaine nécessitent une plus grande protection. Dans ce cas, les phrases de passe (d'une longueur minimale de 15 caractères) sont plus faciles à mémoriser et à saisir, mais plus difficiles à atteindre.

Réinitialisation obligatoire du mot de passe : Pour une meilleure protection, il est courant de fixer des périodes minimales de réinitialisation. Cette durée peut également être modifiée pour les fonctions plus critiques de l'organisation.

1) Password policy - Wikipedia

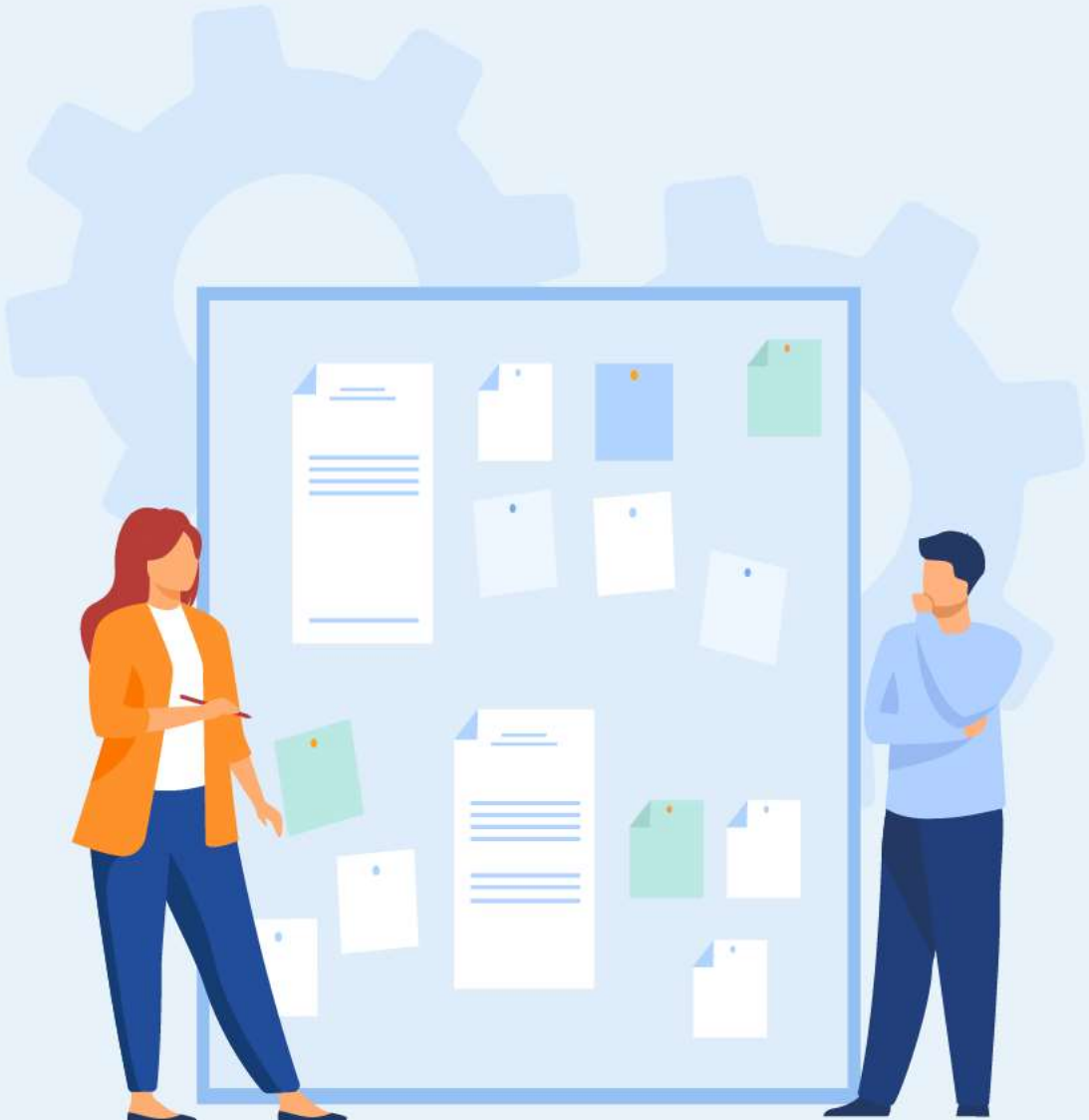
les meilleures clés pour une politique de sécurité des mots de passe

Limitez la réutilisation des mots de passe : Le recyclage est bon pour l'environnement, mais pas pour la gestion des mots de passe de votre entreprise ! En choisissant d'appliquer l'exigence de l'historique des mots de passe, vous limiterez le nombre de fois où un ancien mot de passe peut être utilisé. La fixation de seuils minimums, comme l'interdiction des cinq derniers mots de passe, peut contribuer à éviter la surutilisation des mots de passe "favoris".

Fixez des limites d'âge minimum et maximum pour les mots de passe : Il arrive que les employés changent temporairement de mot de passe et reviennent ensuite à un mot de passe familier. Le fait d'exiger que chaque mot de passe soit conservé pendant trois à sept jours élimine ce problème. Cependant, votre support informatique doit être disponible pour changer les mots de passe compromis lorsque la limite d'âge minimale n'est pas respectée. La fixation d'une limite d'âge maximale pour les mots de passe contribue également à la sécurité du réseau. En général, cette limite est fixée entre 90 jours pour les mots de passe et 180 jours pour les phrases de passe.

Envoyez des rappels : les équipe est susceptible d'oublier d'elle-même de se conformer à la politique de l'entreprise en matière de mots de passe. Des notifications sont envoyée par email pour leur rappeler de changer leurs mots de passe avant qu'ils n'expirent.

Fixez des limites de validité minimales et maximales pour les mots de passe : Il arrive que les employés changent temporairement de mot de passe et reviennent ensuite à un mot de passe familier. Le fait d'exiger que chaque mot de passe soit conservé pendant trois à sept jours élimine ce problème. Cependant, votre support informatique doit être disponible pour changer les mots de passe compromis lorsque la limite d'âge minimale n'est pas respectée. La fixation d'une limite d'âge maximale pour les mots de passe contribue également à la sécurité du réseau. En général, cette limite est fixée entre 90 jours pour les mots de passe et 180 jours pour les phrases de passe.

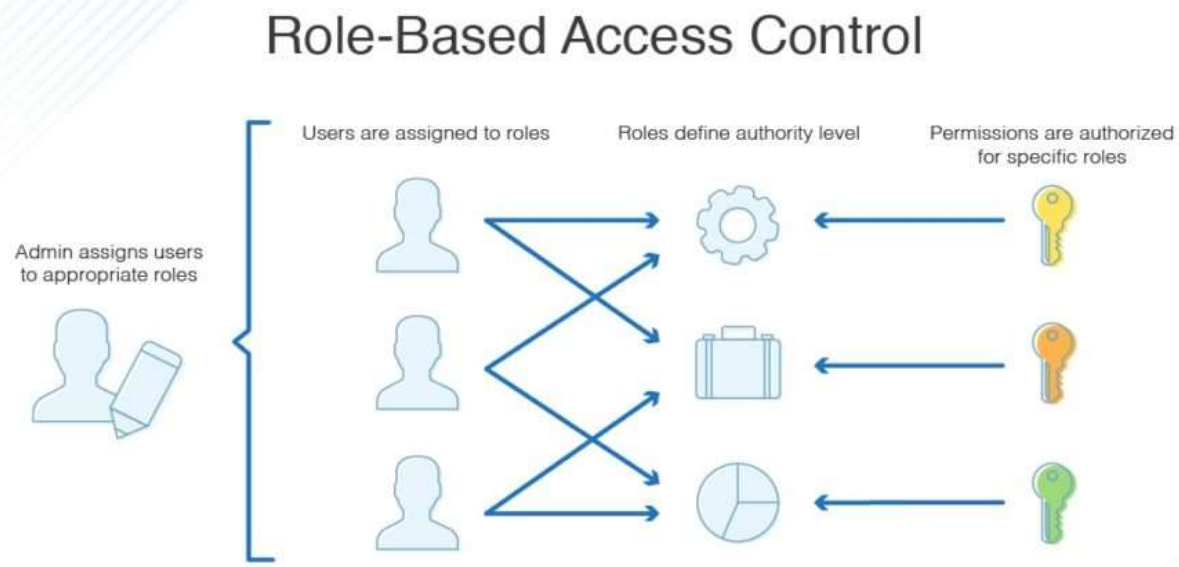


Sécuriser un service

1. Gestion de la politique d’utilisation des mots de passe
2. **Gestion des rôles d’utilisateurs**
3. Chiffrements symétriques et asymétrique
4. Notion de private/public Key

Le contrôle d'accès basé sur les rôles (RBAC)

Le contrôle d'accès basé sur les rôles est une technique qui consiste à attribuer des autorisations d'accès aux utilisateurs de votre organisation en fonction de leurs rôles et des tâches qu'ils effectuent. La sécurité du contrôle d'accès basé sur les rôles garantit que les utilisateurs n'ont accès qu'aux informations ou aux fichiers qui sont pertinents pour leur poste ou leur projet actuel. Dans les organisations qui comptent de grandes divisions, la mise en place d'un système de contrôle d'accès basé sur les rôles est essentielle pour limiter les pertes de données.



Comment fonctionne le système RBAC ?

Un système de droits d'accès utilisant RBAC fonctionne selon le principe du moindre privilège pour aider à garantir la sécurité des données sensibles. L'utilisation de RBAC peut être extrêmement utile pour les grandes entreprises comptant un grand nombre d'employés, où les administrateurs ont du mal à attribuer des identifiants uniques à chaque employé. Avec le contrôle d'accès automatisé basé sur les rôles, les administrateurs peuvent créer des groupes d'utilisateurs ayant des autorisations et des droits similaires, attribuer des rôles et des responsabilités et autoriser l'accès à un ensemble défini de ressources.

Avantages de RBAC

Limiter l'accès inutile des employés aux informations critiques pour l'entreprise peut contribuer à garantir la sécurité et la conformité en

Améliorant l'efficacité opérationnelle : Le contrôle d'accès basé sur les rôles peut contribuer à réduire les tâches manuelles et la paperasserie en rationalisant l'automatisation des droits d'accès. Avec une solution logicielle RBAC, les entreprises peuvent plus facilement attribuer, modifier, ajouter et supprimer des rôles et des responsabilités pour améliorer l'efficacité opérationnelle.

Démonstration de la conformité : La mise en œuvre de RBAC aidera les organisations à démontrer leur conformité aux réglementations locales, fédérales et étatiques. Les équipes informatiques et les administrateurs peuvent ainsi gérer plus efficacement l'accès aux données confidentielles. Les sites web financiers et de santé peuvent utiliser RBAC pour gérer l'accès aux données critiques.

Principes de base du contrôle d'accès basé sur les rôles

Les trois principes communs du contrôle d'accès basé sur les rôles sont les suivants :

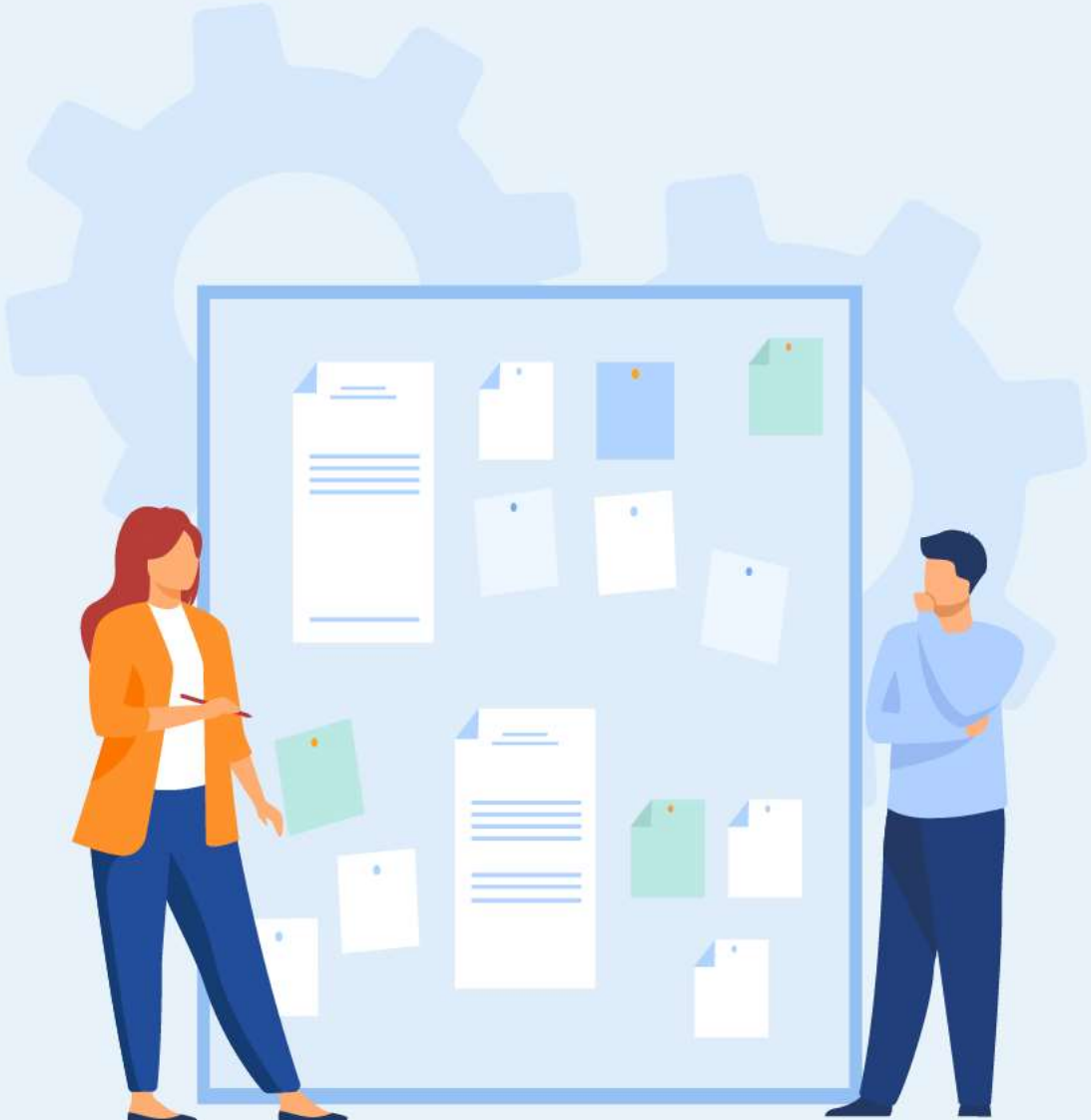
- L'attribution d'un rôle à l'utilisateur : L'autorisation ou les droits d'accès ne sont accordés que si l'individu se voit attribuer un rôle ou une tâche.
- Autorisation du rôle de l'utilisateur : Le rôle actif de l'utilisateur dans la tâche doit être autorisé.
- L'autorisation et les droits d'accès du rôle de l'utilisateur : L'individu ne peut utiliser ses droits d'autorisation que s'il a reçu l'autorisation d'exécuter son rôle actif.

Un RBAC efficace peut aider à accorder des permissions et des accès systématiques aux informations critiques pour l'entreprise afin d'améliorer la cybersécurité et de maintenir la conformité aux réglementations telles que HIPAA, GDPR, et plus encore. L'utilisation d'une solution logicielle RBAC automatisée peut également fournir des modèles structurés pour surveiller les niveaux d'accès des utilisateurs et simplifier le processus d'audit.

Bonnes pratiques pour la mise en œuvre de RBAC?

En suivant quelques bonnes pratiques, la mise en œuvre du contrôle d'accès basé sur les rôles peut être un processus simple. Voici quelques bonnes pratiques pour faciliter la mise en œuvre de RBAC :

- **Notez les permissions actuelles des utilisateurs attribuées aux ressources**. Il est important de disposer d'informations détaillées et de pouvoir visualiser facilement l'accès des utilisateurs aux applications et aux ressources, comme les logiciels et le matériel.
- **Utilisez des modèles spécifiques aux rôles pour attribuer des droits d'accès aux seuls utilisateurs** qui en ont besoin en fonction des responsabilités professionnelles et standardisez les informations d'identification des utilisateurs.
- **Suivez toutes les modifications ou changements apportés aux rôles, droits d'accès et autorisations** des utilisateurs afin d'identifier et d'enquêter sur les abus de privilèges, les activités de compte suspectes et autres vulnérabilités.



Sécuriser un service

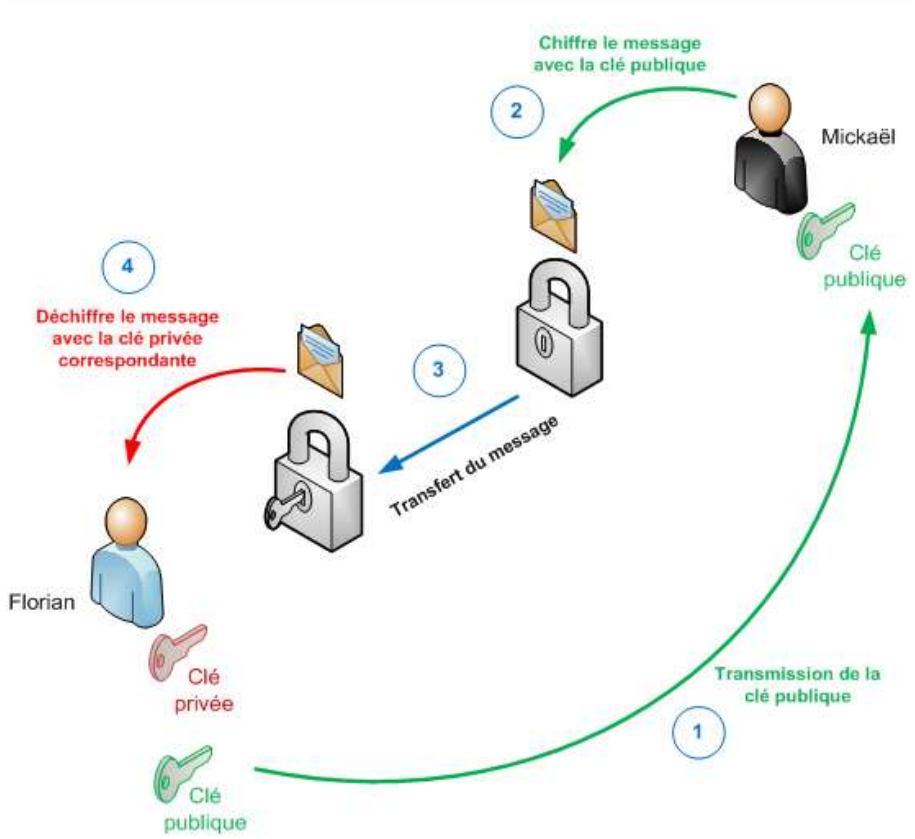
1. Gestion de la politique d’utilisation des mots de passe
2. Gestion des rôles d’utilisateurs
3. **Chiffrements symétriques et asymétrique**
4. Notion de private/public Key

Qu'est-ce que le cryptage asymétrique ?

Une communication chiffrée comporte deux parties : l'expéditeur, qui **chiffre** les données, et le destinataire, qui les **déchiffre**. Comme son nom l'indique, le cryptage asymétrique est différent de chaque côté ; l'expéditeur et le destinataire utilisent deux clés différentes.

Le cryptage asymétrique, également connu sous le nom de **cryptage à clé publique**, utilise une paire de **clé publique-clé privée** : les données cryptées avec la clé privée ne peuvent être décryptées qu'avec la clé publique, et vice versa.

Par exemple le TLS (ou SSL), le protocole qui rend le HTTPS possible, repose sur le cryptage asymétrique. Un client obtient la clé publique d'un site Web à partir du certificat TLS (ou SSL) de ce site et l'utilise pour lancer une communication sécurisée. Le site web garde la clé privée secrète.



Qu'est-ce que le cryptage symétrique ?

Dans le cryptage symétrique, la même **clé permet de crypter et de décrypter les données**. Pour que le cryptage symétrique fonctionne, les deux ou plusieurs parties qui communiquent doivent connaître la clé.

PARTIE 3

PARTIE 3

Qu'est-ce qu'un certificat SSL ?

SSL est l'abréviation de Secure Sockets Layer (couche de sockets sécurisés). En bref, il s'agit de la technologie standard permettant de sécuriser une connexion internet et de protéger les données sensibles envoyées entre deux systèmes, empêchant ainsi les criminels de lire et de modifier les informations transférées, y compris les données personnelles potentielles. Les deux systèmes peuvent être un serveur et un client (par exemple, un site web d'achat et un navigateur) ou un serveur à un serveur (par exemple, une application avec des informations personnelles identifiables ou avec des informations de paie).

Pour ce faire, il s'assure que toutes les données transférées entre les utilisateurs et les sites, ou entre deux systèmes, restent impossibles à lire. Il utilise des algorithmes de cryptage pour brouiller les données en transit, empêchant les pirates de les lire lorsqu'elles sont envoyées par la connexion. Ces informations peuvent être sensibles ou personnelles, notamment les numéros de carte de crédit et autres informations financières, les noms et les adresses.

Qu'est-ce qu'un certificat TLS ?

TLS (Transport Layer Security) est simplement une version actualisée et plus sécurisée de SSL. Nous faisons toujours référence à nos certificats de sécurité sous le nom de SSL, car il s'agit d'un terme plus communément utilisé.

Qu'est-ce qu'un certificat HTTPS ?

HTTPS (Hyper Text Transfer Protocol Secure) apparaît dans l'URL lorsqu'un site web est sécurisé par un certificat SSL. Les détails du certificat, y compris l'autorité émettrice et la raison sociale du propriétaire du site, peuvent être consultés en cliquant sur le symbole du cadenas dans la barre du navigateur.

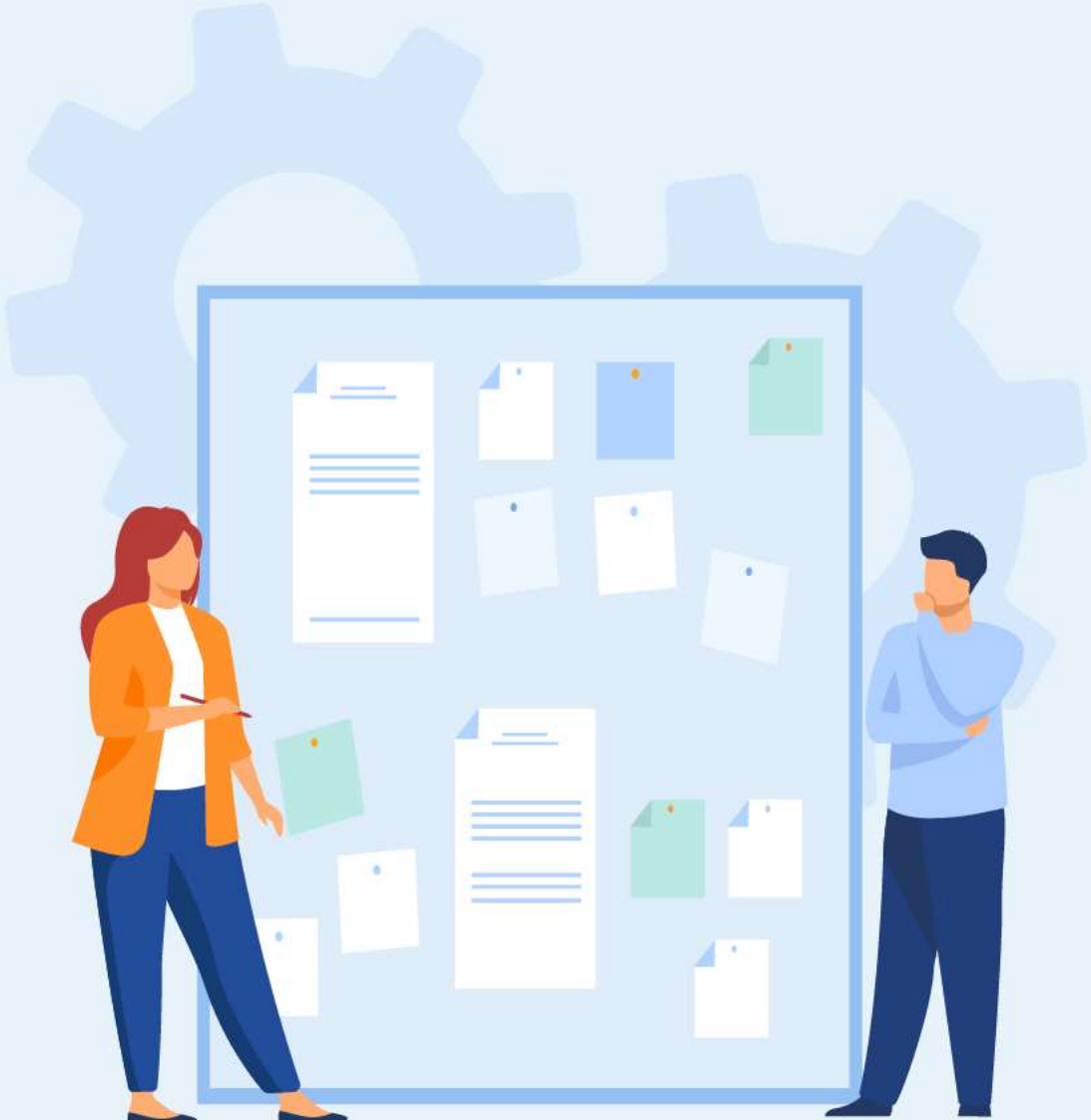
Ce message indique que la connexion n'est pas sécurisée (pas de SSL valide) et que sans antivirus ou chiffrement, vous serez facilement piraté.

Outils de chiffrements?

GnuPG permet de crypter et de signer vos données et vos communications, dispose d'un système de gestion des clés polyvalent ainsi que de modules d'accès à toutes sortes de répertoires de clés publiques. GnuPG, également connu sous le nom de GPG, est un outil en ligne de commande doté de fonctionnalités permettant une intégration facile avec d'autres applications.

AES Crypt est un utilitaire de cryptage de fichiers avancé qui s'intègre avec le Shell de Windows ou s'exécute à partir de l'invite de commande Linux pour fournir un outil simple et puissant de cryptage de fichiers à l'aide de l'Advanced Encryption Standard (AES).

Encrypto vous permet de chiffrer des fichiers avant de les envoyer à des amis ou à des collègues. Il suffit de déposer un fichier dans Encrypto, de définir un mot de passe, puis de l'envoyer comme vous le feriez normalement, mais cette fois avec une sécurité accrue. Ce logiciel est gratuit pour Mac et Windows.

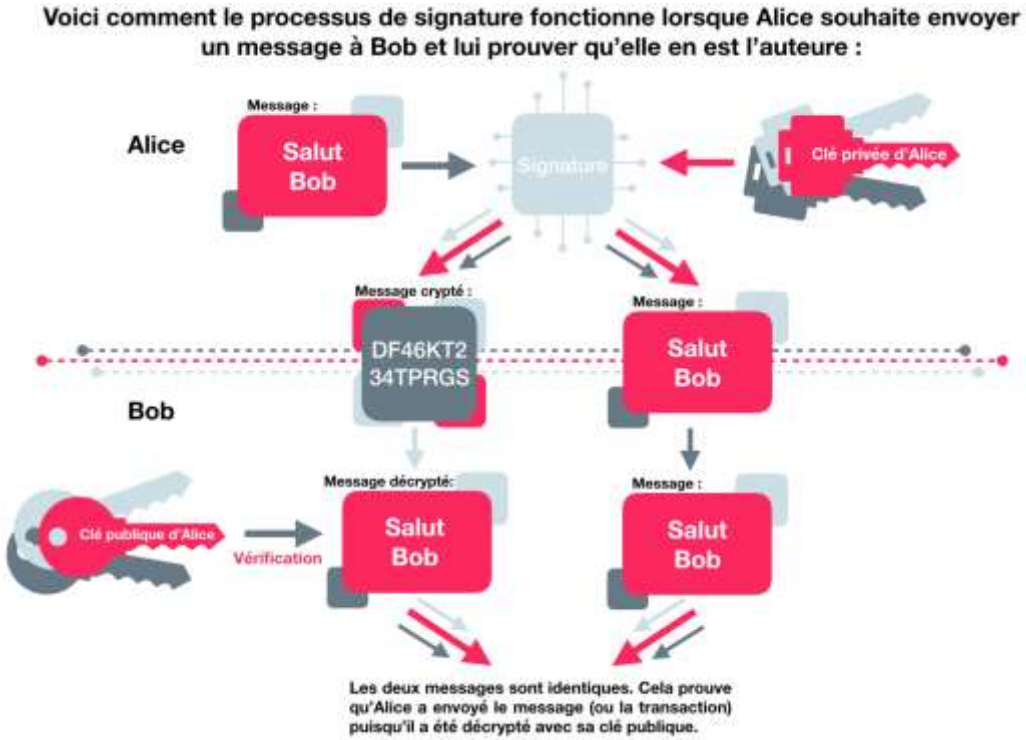


Sécuriser un service

1. Gestion de la politique d’utilisation des mots de passe
2. Gestion des rôles d’utilisateurs
3. Chiffrements symétriques et asymétrique
4. **Notion de private/public Key**

Comment fonctionne une clé cryptographique ?

Une clé est une chaîne de données qui, utilisée en conjonction avec un algorithme cryptographique, permet de chiffrer ou de déchiffrer des messages. Les données cryptées à l'aide de la clé ressembleront à une série de caractères aléatoires, mais toute personne disposant de la bonne clé (soit la même clé, soit une des paires de clés publiques/privées) peut les remettre sous forme de texte en clair.



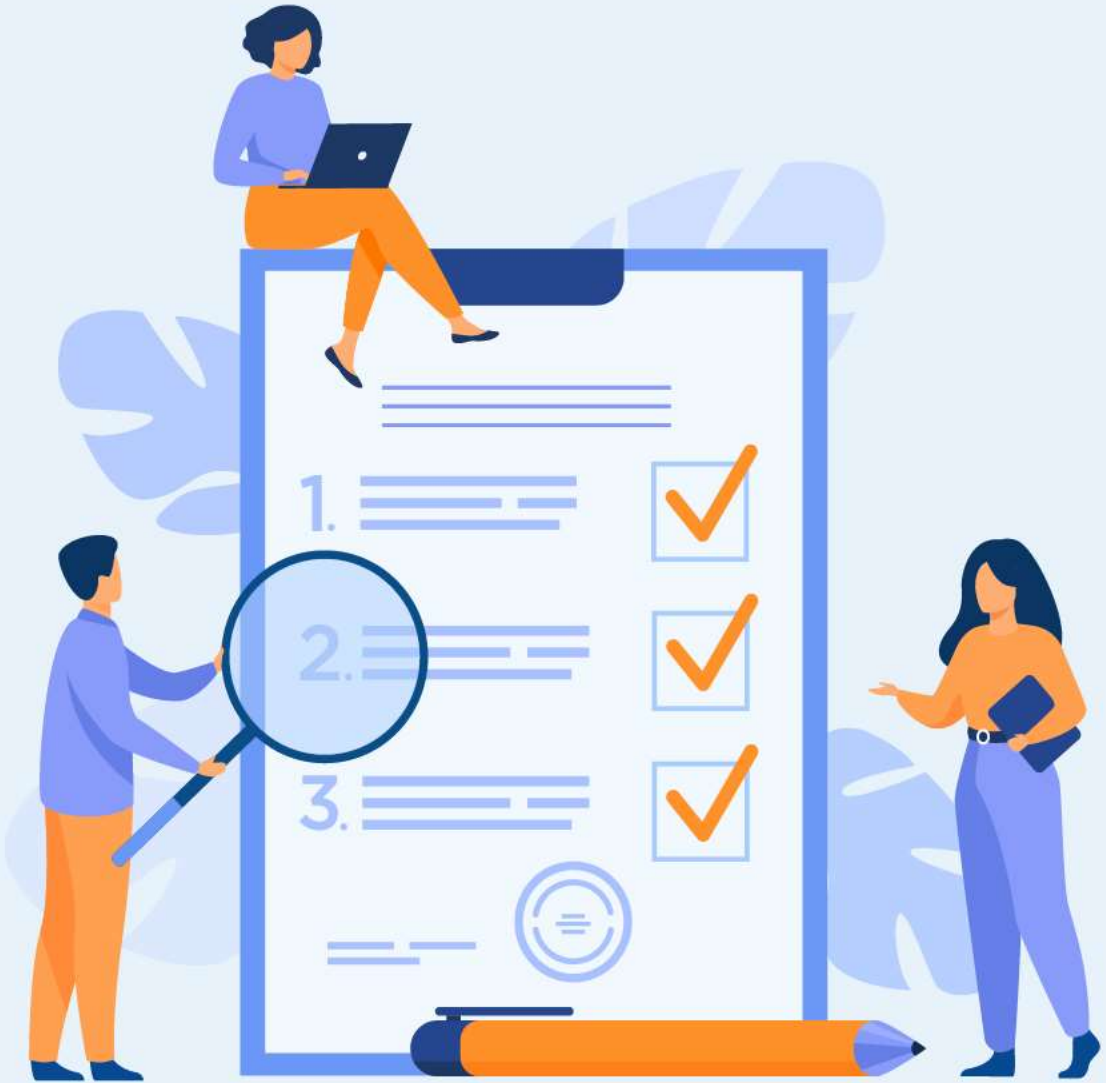
Clé privée

Dans la clé privée, la même clé (clé secrète) est utilisée pour le cryptage et le décryptage. Dans ce cas, la clé est symétrique car la seule clé qui peut être copiée ou partagée par une autre partie pour décrypter le texte chiffré. Elle est plus rapide que la cryptographie à clé publique.

Clé publique

Dans le cas d'une clé publique, deux clés sont utilisées : une clé est utilisée pour le cryptage et une autre pour le décryptage. Une clé (clé publique) est utilisée pour crypter le texte en clair afin de le convertir en texte chiffré et une autre clé (clé privée) est utilisée par le destinataire pour décrypter le texte chiffré et lire le message.

Clé privée	Clé publique
Dans ce cas, la même clé (clé secrète) et le même algorithme sont utilisés pour crypter et décrypter le message.	Dans la cryptographie à clé publique, deux clés sont utilisées, l'une pour le cryptage et l'autre pour le décryptage.
Dans la cryptographie à clé privée, la clé est gardée secrète.	Dans la cryptographie à clé publique, l'une des deux clés est gardée secrète.
La clé privée est symétrique car il n'y a qu'une seule clé, appelée clé secrète.	La clé publique est asymétrique car il existe deux types de clés : la clé privée et la clé publique.
Dans cette cryptographie, l'expéditeur et le destinataire doivent partager la même clé.	Dans cette cryptographie, l'expéditeur et le destinataire n'ont pas besoin de partager la même clé.
Dans cette cryptographie, la clé est privée.	Dans cette cryptographie, la clé publique peut être publique et la clé privée est privée.

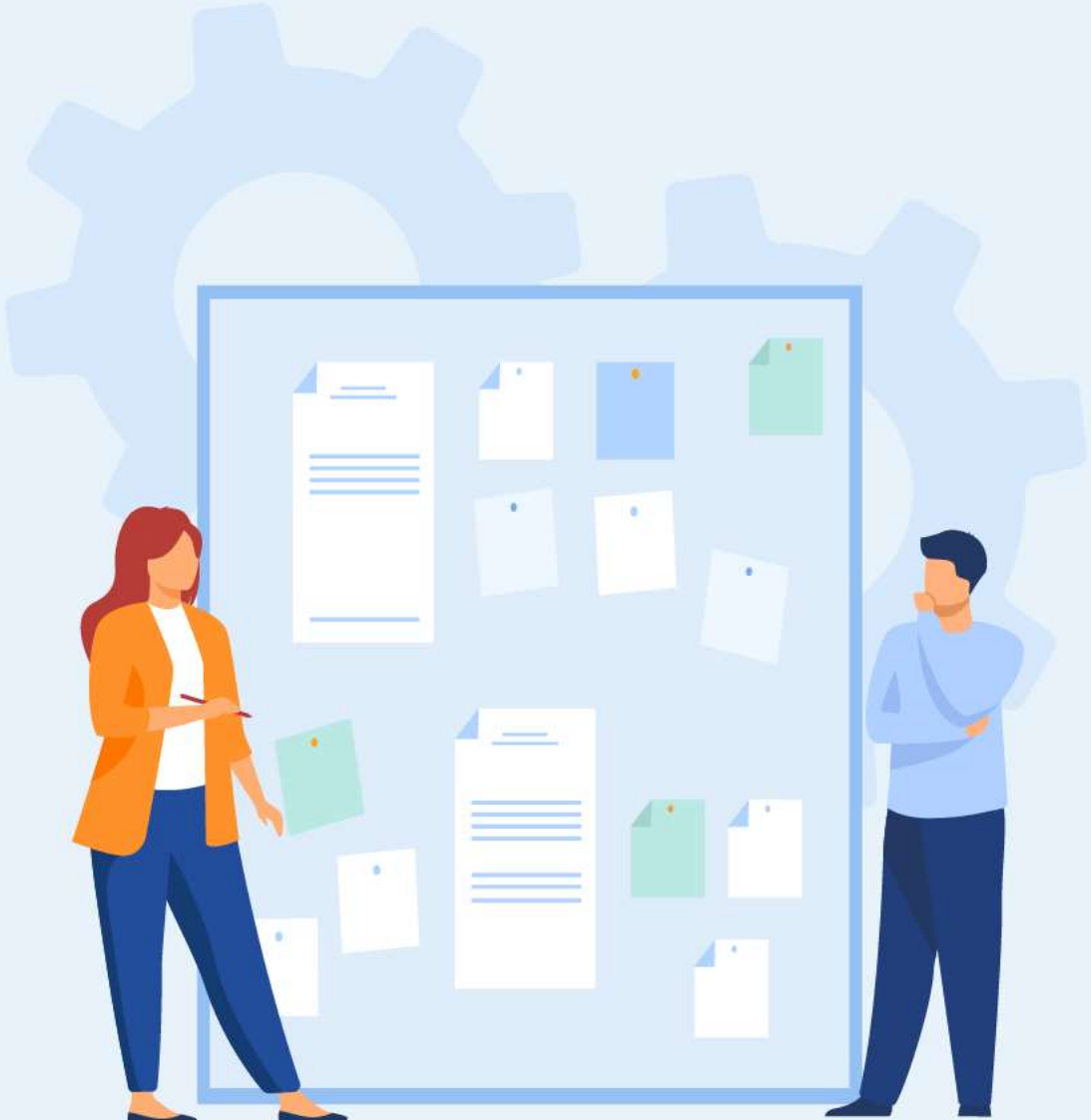


Utiliser les firewalls

Ce que vous allez apprendre dans ce chapitre :

- Fonctionnement d’un firewall réseau dans la protection d'application HTTP
- Principe du développement sécurisé
- Firewall "applicatif "

02



Utiliser les firewalls

1. **Fonctionnement d’un firewall réseau dans la protection d'application HTTP**
2. Principe du développement sécurisé
3. Firewall "applicatif "

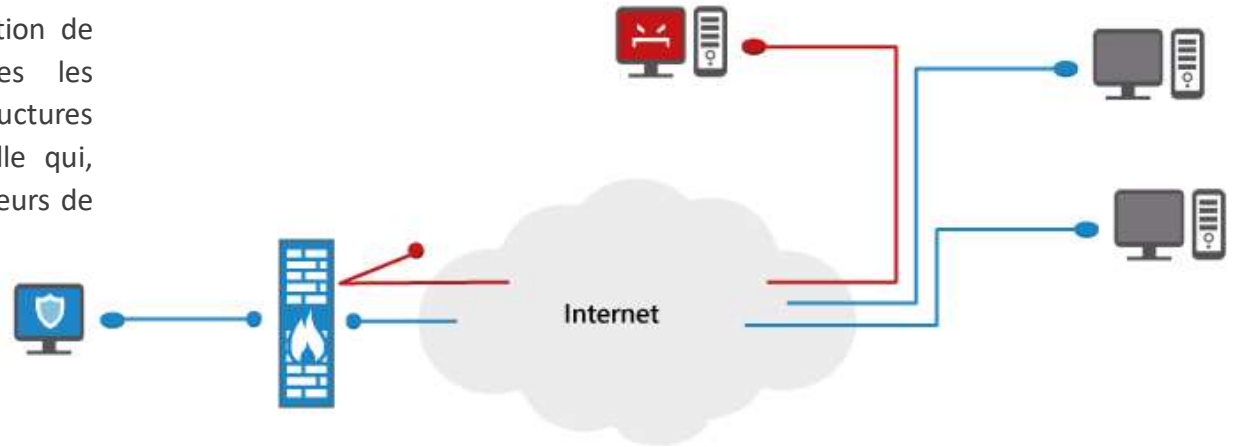
Qu'est-ce qu'un pare-feu de réseau ?

Un pare-feu réseau est un système capable de contrôler l'accès au réseau local et donc de protéger ce réseau. Il agit comme un filtre pour bloquer le trafic entrant non légitime avant qu'il ne puisse pénétrer dans le réseau local pour y causer des dommages.

Son objectif principal est d'assurer la protection d'un réseau interne en le séparant du réseau externe. Il contrôle également les communications entre les deux réseaux.

En général, l'objectif d'un pare-feu est de réduire ou d'éliminer l'apparition de communications réseau indésirables tout en permettant à toutes les communications légitimes de circuler librement. Dans la plupart des infrastructures de serveurs, les pare-feu constituent une couche de sécurité essentielle qui, associée à d'autres mesures, empêche les attaquants d'accéder à vos serveurs de manière malveillante.

Lors du passage des données, le pare-feu matériel analyse le contenu en profondeur afin de décider si elles peuvent passer ou non. Il y a des pare-feu ne faisant rien d'autre que de suivre des règles établies par l'utilisateur.



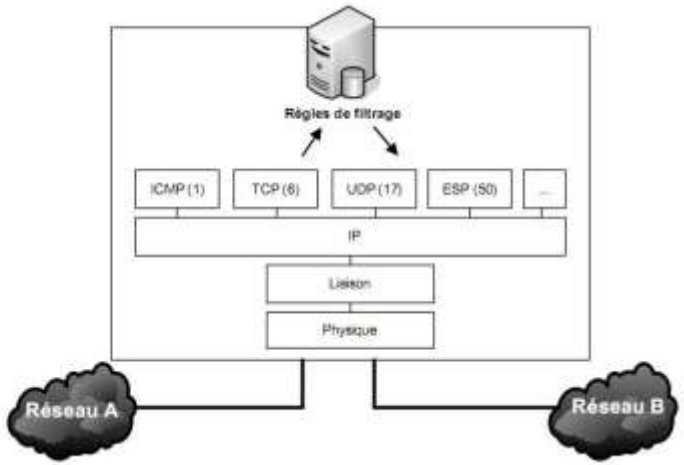
Comment le pare-feu contrôle et surveille le trafic sur le réseau ?

Le filtrage des paquets: Les paquets sont de petites quantités de données. Lorsqu'un pare-feu utilise le filtrage de paquets, les paquets qui tentent d'entrer sur le réseau sont soumis à un groupe de filtres. Ces filtres suppriment les paquets qui correspondent à certaines menaces identifiées et laissent passer les autres vers leur destination prévue.

Service proxy Ces pare-feu sont incroyablement sûrs, mais ils ont leurs propres inconvénients. Ils fonctionnent plus lentement que les autres types de pare-feu et sont souvent limités en ce qui concerne les types d'applications qu'ils peuvent prendre en charge. Au lieu de servir de système de filtrage à travers lequel les données passent, les serveurs proxy fonctionnent comme des intermédiaires. En créant essentiellement un miroir de l'ordinateur situé derrière le pare-feu, ils empêchent les connexions directes entre l'appareil du client et les paquets entrants, protégeant ainsi l'emplacement de votre réseau d'éventuels mauvais acteurs.

Inspection dynamique: Alors que le filtrage statique examine les en-têtes des paquets, les pare-feu à inspection dynamique examinent une variété d'éléments de chaque paquet de données et les comparent à une base de données d'informations fiables. Ces éléments comprennent les adresses IP source et destination, les ports et les applications. Les paquets de données entrants doivent correspondre suffisamment aux informations de confiance pour être autorisés à passer par le pare-feu. L'inspection dynamique est une méthode plus récente de filtrage des pare-feu.

Pare-feu avec filtrage de paquets



C'est la méthode de filtrage la plus simple, elle opère au niveau de la couche réseau et transport du modèle OSI. La plupart des routeurs d'aujourd'hui permettent d'effectuer du filtrage simple de paquet. Cela consiste à accorder ou refuser le passage de paquet d'un réseau à un autre

Types de pare-feu

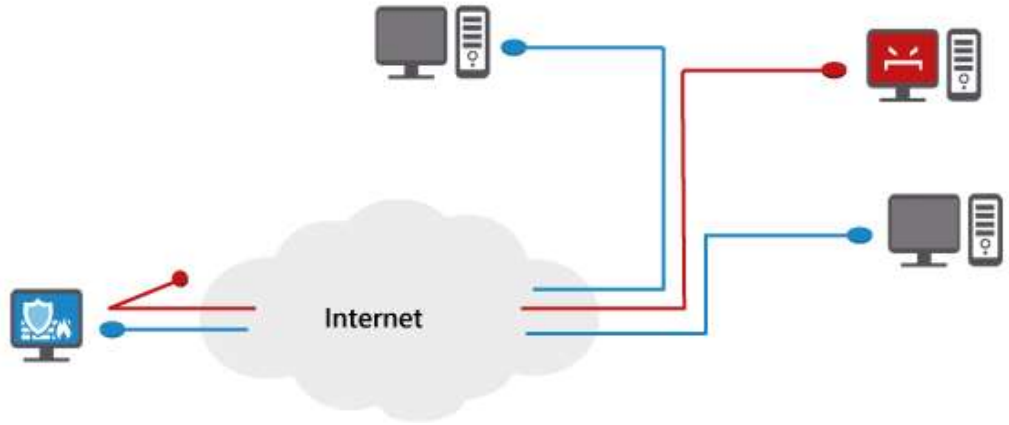
Généralement, il y a trois types fondamentaux de pare-feu réseau : **le filtrage de paquets (sans état), le filtrage avec état et la couche application.**

Les pare-feu à filtrage de paquets, ou sans état, fonctionnent en inspectant les paquets individuels de manière isolée. Ils ne sont donc pas conscients de l'état de la connexion et ne peuvent autoriser ou refuser des paquets que sur la base de leurs en-têtes.

Les pare-feu dynamiques sont capables de déterminer l'état de connexion des paquets, ce qui les rend beaucoup plus flexibles que les pare-feu sans état. Ils collectent les paquets connexes jusqu'à ce que l'état de la connexion puisse être déterminé, avant que les règles du pare-feu ne soient appliquées au trafic.

Les pare-feu applicatifs vont plus loin en analysant les données transmises, ce qui permet de comparer le trafic réseau à des règles de pare-feu spécifiques à certains services ou applications. Ces pare-feu sont également connus sous le nom de **pare-feu à base de proxy**.

Outre le logiciel de pare-feu, qui est disponible sur tous les systèmes d'exploitation modernes, la fonctionnalité de pare-feu peut également être fournie par des dispositifs matériels, **tels que des routeurs ou des appareils de pare-feu**.



Un des plus grands avantages d'un pare-feu logiciel est celui de son prix d'habitude moins élevé si on le compare avec un pare-feu matériel autonome.

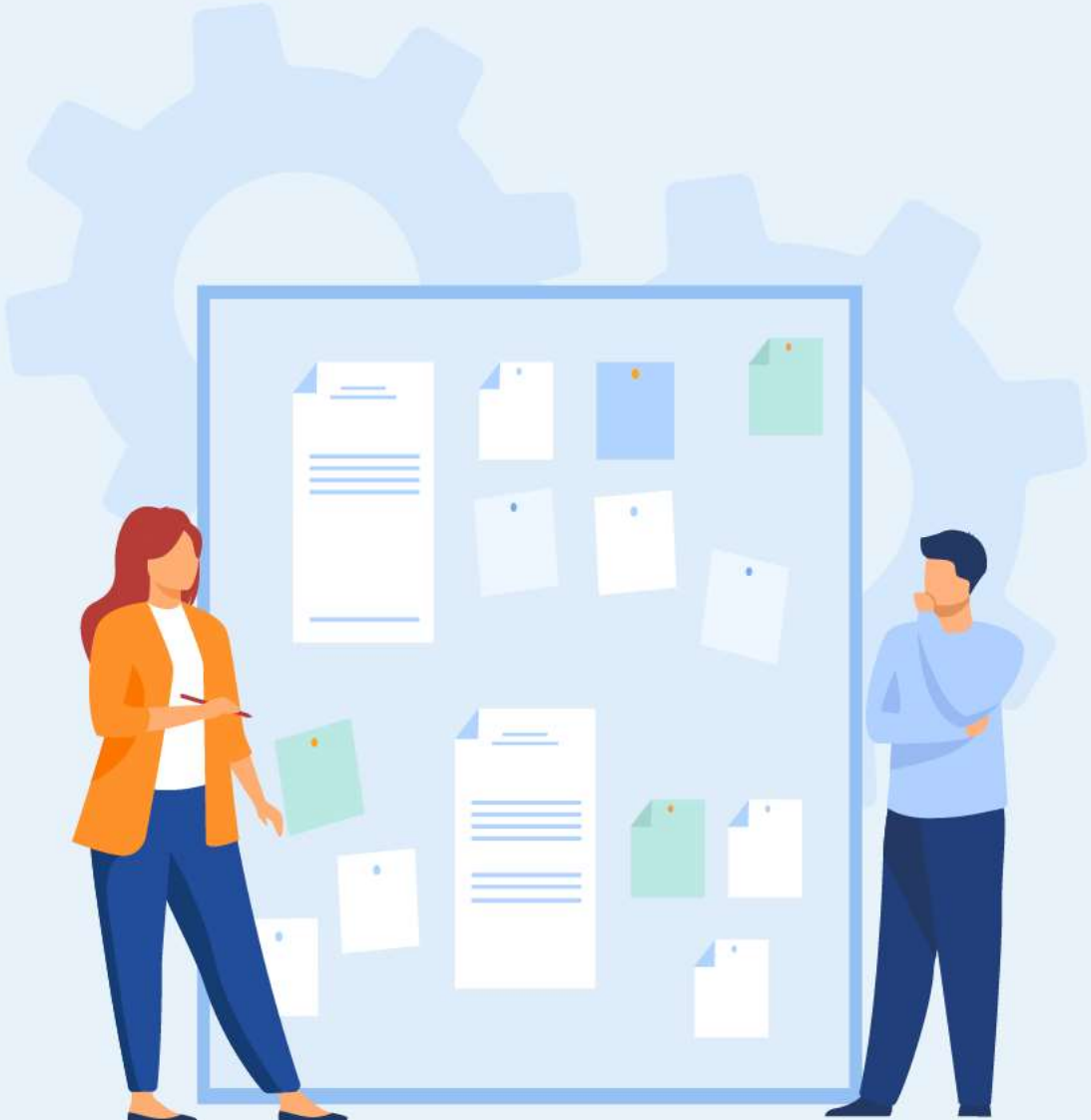
Règles de pare-feu

Comme le trafic réseau qui traverse un pare-feu est comparé à des règles afin de déterminer s'il doit être autorisé ou non. Une façon simple d'expliquer ce que sont les règles de pare-feu est de montrer quelques exemples, ce que nous allons faire maintenant.

Supposons que vous ayez un serveur avec cette liste de règles de pare-feu qui s'appliquent au trafic entrant :

- **Accept** le trafic entrant nouveau et établi vers l'interface du réseau public sur les ports 80 et 443 (trafic Web HTTP et HTTPS).
- **Reject** le trafic entrant provenant des adresses IP des employés non techniques de votre bureau sur le port 22 (SSH)
- **Drop** le trafic entrant, nouveau et établi, de la plage d'adresses IP de votre bureau vers l'interface du réseau privé sur le port 22 (SSH).

Notez que le premier mot dans chacun de ces exemples est soit « **Accept** », « **Reject** » ou « **Drop** ». Ce mot spécifie l'action que le pare-feu doit entreprendre dans le cas où un élément du trafic réseau correspond à une règle. **Accept** signifie autoriser le trafic, **Reject** signifie bloquer le trafic mais répondre par une erreur "inaccessible", et **Drop** signifie bloquer le trafic et ne pas envoyer de réponse. Le reste de chaque règle consiste en la condition à laquelle chaque paquet est comparé.



Utiliser les firewalls

1. Fonctionnement d’un firewall réseau dans la protection d'application HTTP
2. **Principe du développement sécurisé**
3. Firewall "applicatif "

Introduction

L'explosion des frameworks de développement d'applications de haute qualité a été une formidable réussite pour les logiciels du monde entier. Il est plus facile que jamais de créer une application et de commencer à offrir de la valeur aux clients, qui peuvent venir de n'importe où dans le monde.

Malheureusement, il en va de même pour les pirates informatiques qui viennent attaquer une application. Les logiciels du monde entier étant de plus en plus connectés et contenant des données de plus en plus précieuses, les pirates informatiques sont devenus plus sophistiqués. La sécurité des applications en réseau doit être capable de résister à des centaines d'heures de temps CPU et à des adversaires engagés.

Malheureusement, il est impossible d'écrire des applications parfaitement sécurisées. Des bogues vont se glisser, et s'ils le font, les attaquants les trouveront. La bonne nouvelle est que vous pouvez concevoir vos applications de manière à minimiser les dommages causés par ces bogues. La meilleure nouvelle encore est que la conception d'applications sécurisées n'est ni compliquée ni mystérieuse.

La solution est de suivre les principes clés pendant la phase de conception et de développement de l'application. Ainsi, même lorsque des bugs se manifestent, les dommages qu'ils causent permettent pas aux attaquants de s'emparer de toutes les données sensibles, ni à l'ensemble du service de tomber en panne.

Les 10 principes de sécurité en développement

Le respect de ces principes est essentiel pour garantir que les logiciels que vous expédiez sont sûrs et sécurisés pour vos clients.

1. Minimiser la surface d'attaque

Chaque fois qu'un programmeur ajoute une fonctionnalité à son application, il augmente le risque d'une vulnérabilité de sécurité.

Le principe de minimisation de la surface d'attaque consiste à restreindre les fonctions auxquelles les utilisateurs sont autorisés à accéder, afin de réduire les vulnérabilités potentielles.

Par exemple, vous pouvez coder une fonction de recherche dans une application. Cette fonction de recherche est potentiellement vulnérable aux attaques par inclusion de fichier et aux attaques par injection SQL.

Le développeur pourrait limiter l'accès à la fonction de recherche, afin que seuls les utilisateurs enregistrés puissent l'utiliser, ce qui réduirait la surface d'attaque et le risque de réussite de l'attaque.

Les 10 principes de sécurité en développement

2. Établir des valeurs par défaut sécurisées

Ce principe stipule que l'application doit être sécurisée par défaut. Cela signifie qu'un nouvel utilisateur doit prendre des mesures pour obtenir des privilèges plus élevés et supprimer les mesures de sécurité supplémentaires (si elles sont autorisées).

Établir des valeurs par défaut sûres signifie qu'il doit y avoir des règles de sécurité solides concernant la manière dont les enregistrements des utilisateurs sont traités, la fréquence à laquelle les mots de passe doivent être mis à jour, la complexité des mots de passe, etc.

Les utilisateurs d'applications peuvent être en mesure de désactiver certaines de ces fonctions, mais elles doivent être définies par défaut à un niveau de sécurité élevé.

3. Le principe du moindre privilège

Le principe du moindre privilège (POLP) stipule qu'un utilisateur doit disposer de l'ensemble minimal de privilèges requis pour effectuer une tâche spécifique.

Le POLP peut être appliqué à tous les aspects d'une application web, y compris les droits des utilisateurs et l'accès aux ressources. Par exemple, un utilisateur inscrit à une application de blog en tant qu'"auteur" ne devrait pas disposer de privilèges administratifs lui permettant d'ajouter ou de supprimer des utilisateurs. Il ne doit être autorisé qu'à publier des articles dans l'application.

Les 10 principes de sécurité en développement

4. Le principe de défense en profondeur

Le principe de défense en profondeur stipule que de multiples contrôles de sécurité qui abordent les risques de différentes manières constituent la meilleure option pour sécuriser une application.

Ainsi, au lieu d'avoir un seul contrôle de sécurité pour l'accès des utilisateurs, vous aurez plusieurs couches de validation, des outils d'audit de sécurité supplémentaires et des outils de journalisation.

Par exemple, au lieu de laisser un utilisateur se connecter avec un simple nom d'utilisateur et un mot de passe, vous pouvez utiliser une vérification de l'adresse IP, un système Captcha, l'enregistrement de ses tentatives de connexion, la détection de la force brute, etc.

5. Échouer en toute sécurité

Il existe de nombreuses raisons pour lesquelles une application web peut échouer dans le traitement d'une transaction. Il peut s'agir de l'échec d'une connexion à une base de données ou d'une erreur dans les données saisies par l'utilisateur.

Ce principe stipule que les applications doivent échouer de manière sécurisée. L'échec ne doit pas donner à l'utilisateur des privilèges supplémentaires et ne doit pas lui montrer des informations sensibles comme les requêtes ou les journaux de la base de données.

Les 10 principes de sécurité en développement

6. Ne pas faire confiance aux services

De nombreuses applications web utilisent des services tiers pour accéder à des fonctionnalités supplémentaires ou obtenir des données supplémentaires. Ce principe stipule que vous ne devez jamais faire confiance à ces services du point de vue de la sécurité.

Cela signifie que l'application doit toujours vérifier la validité des données envoyées par les services tiers et ne pas donner à ces services des autorisations de haut niveau dans l'application.

7. La séparation des fonctions

La séparation des fonctions peut être utilisée pour empêcher les individus d'agir frauduleusement. Par exemple, un utilisateur d'un site de commerce électronique ne devrait pas avoir le droit d'être également administrateur, car il pourra modifier les commandes et s'attribuer des produits.

L'inverse est également vrai : un administrateur ne doit pas avoir la possibilité de faire ce que font les clients, comme commander des articles depuis la page d'accueil du site web.

8. Éviter la sécurité par l'obscurité

Ce principe de l'OWASP stipule qu'il ne faut jamais se fier à la sécurité par l'obscurité. Si votre application nécessite que son URL d'administration soit cachée pour rester sécurisée, alors elle n'est pas sécurisée du tout.

Des contrôles de sécurité suffisants doivent être mis en place pour assurer la sécurité de votre application sans cacher la fonctionnalité de base ou le code source.

Les 10 principes de sécurité en développement

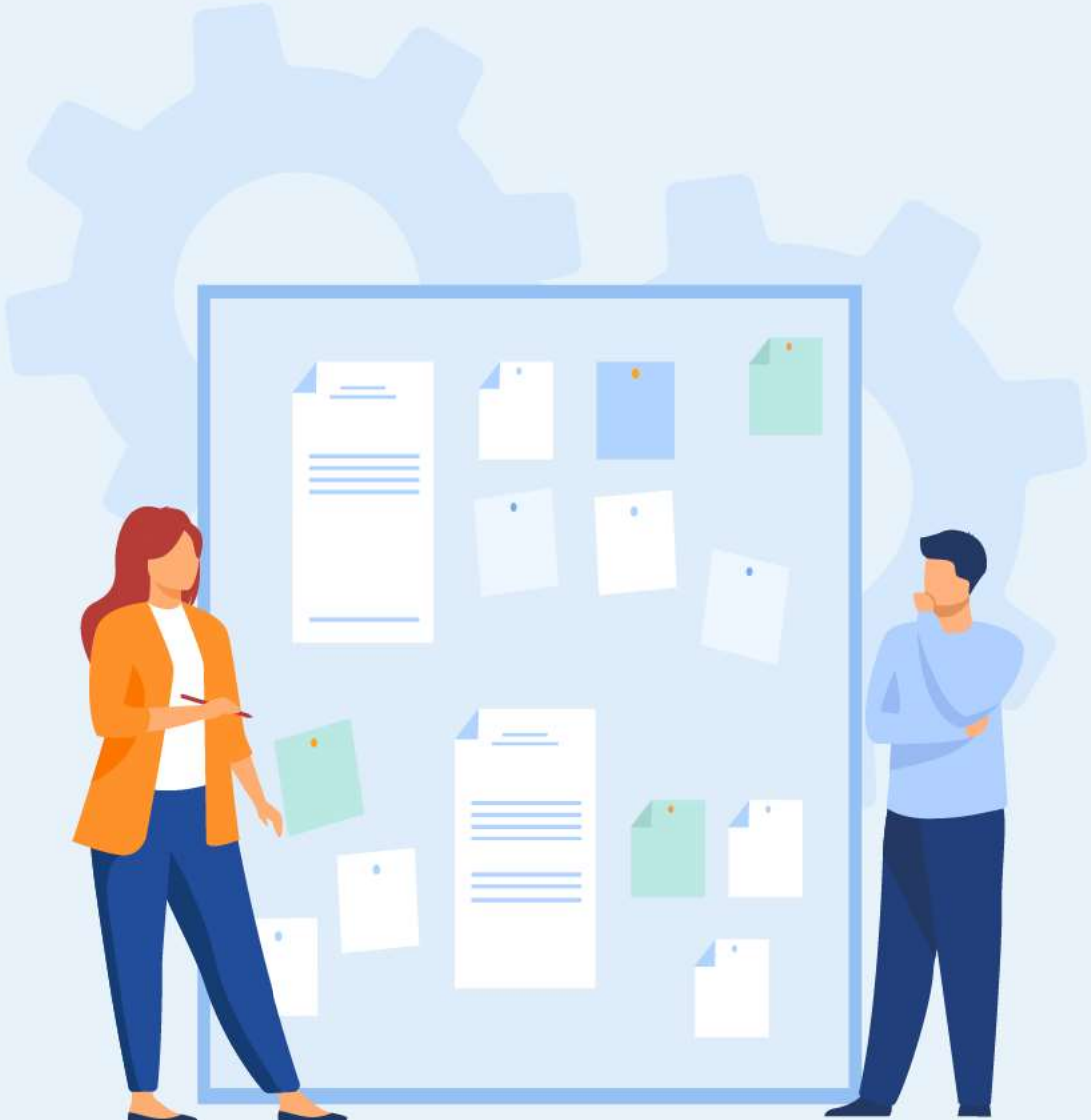
9. Garder la sécurité simple

Les développeurs doivent éviter d'utiliser une architecture très sophistiquée lorsqu'ils développent des contrôles de sécurité pour leurs applications. Des mécanismes très complexes peuvent augmenter le risque d'erreurs.

10. Corriger correctement les problèmes de sécurité

Si un problème de sécurité a été identifié dans une application, les développeurs doivent déterminer la cause profonde du problème.

Ils doivent ensuite le réparer et tester les réparations de manière approfondie. Si l'application utilise des modèles de conception, il est probable que l'erreur soit présente dans plusieurs systèmes. Les programmeurs doivent prendre soin d'identifier tous les systèmes affectés.



Utiliser les firewalls

1. Fonctionnement d’un firewall réseau dans la protection d'application HTTP
2. Principe du développement sécurisé
3. **Firewall "applicatif "**

Définition

Un pare-feu applicatif est un type de pare-feu qui analyse, surveille et contrôle l'accès et les opérations du réseau, d'Internet et du système local vers et depuis une application ou un service. Ce type de pare-feu permet de contrôler et de gérer les opérations d'une application ou d'un service externe à l'environnement informatique.

Un pare-feu d'application est principalement utilisé comme une amélioration du programme de pare-feu standard en fournissant des services de pare-feu jusqu'à la couche application.

Pare-feu applicatif basé sur le réseau : Analyser et surveiller le trafic réseau destiné à la couche application ou à une application spécifique. L'Iptables**, par exemple,** est un pare-feu en mode ligne de commande qui filtre les paquets en fonction des règles prédéfinies. Avec Iptables, les utilisateurs peuvent accepter, refuser ou transférer les connexions ; il est incroyablement polyvalent et largement utilisé.

Pare-feu applicatif basé sur l'hôte : Ils surveillent tout le trafic entrant et sortant initié par une application ou un service sur un ordinateur, un système ou un hôte local.

Actuellement, les pare-feu d'applications Web (WAF) sont les plus utilisés pour filtrer, surveiller et bloquer le trafic HTTP/S en provenance et à destination d'une application et de services Web.

Qu'est-ce qu'un pare-feu d'application Web (WAF) ?

Un WAF ou pare-feu d'application Web aide à protéger les applications Web en filtrant et en surveillant le trafic HTTP entre une application Web et Internet. Il protège généralement les applications Web contre les attaques telles que la falsification intersites, le cross-site-scripting (XSS), l'inclusion de fichiers et l'injection SQL, entre autres.

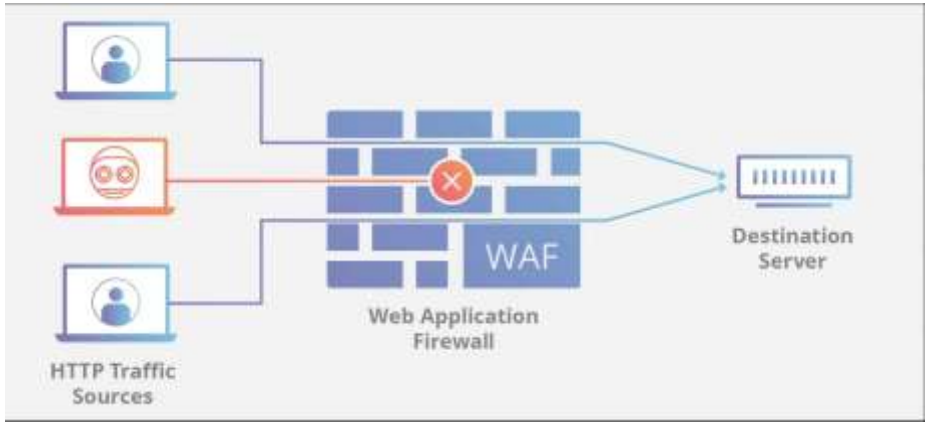
Un WAF est une défense de **la couche 7 du protocole (dans le modèle OSI),** et n'est pas conçu pour se défendre contre tous les types d'attaques. Cette méthode d'atténuation des attaques fait généralement partie d'une suite d'outils qui, ensemble, créent une défense globale contre une série de vecteurs d'attaque.

Pourquoi la sécurité des WAF est-elle importante ?

Les WAF sont importants pour un nombre croissant d'organisations qui proposent des produits ou des services en ligne, notamment les développeurs d'applications mobiles, les fournisseurs de médias sociaux et les banquiers numériques. Un WAF peut vous aider à protéger les données sensibles, telles que les dossiers des clients et les données des cartes de paiement, et à prévenir les fuites.

Les organisations stockent généralement une grande partie de leurs données sensibles dans une base de données dorsale à laquelle on peut accéder via des applications Web. Les entreprises emploient de plus en plus d'applications mobiles et de dispositifs IoT pour faciliter les interactions commerciales, de nombreuses transactions en ligne se produisant au niveau de la couche applicative. Les attaquants ciblent souvent les applications pour atteindre ces données.

Il est important de disposer d'un WAF, mais il est recommandé de le combiner avec d'autres mesures de sécurité, telles que les systèmes de détection d'intrusion **(IDS),** les systèmes de prévention d'intrusion **(IPS)** et les pare-feu traditionnels, pour obtenir un modèle de sécurité de défense en profondeur.



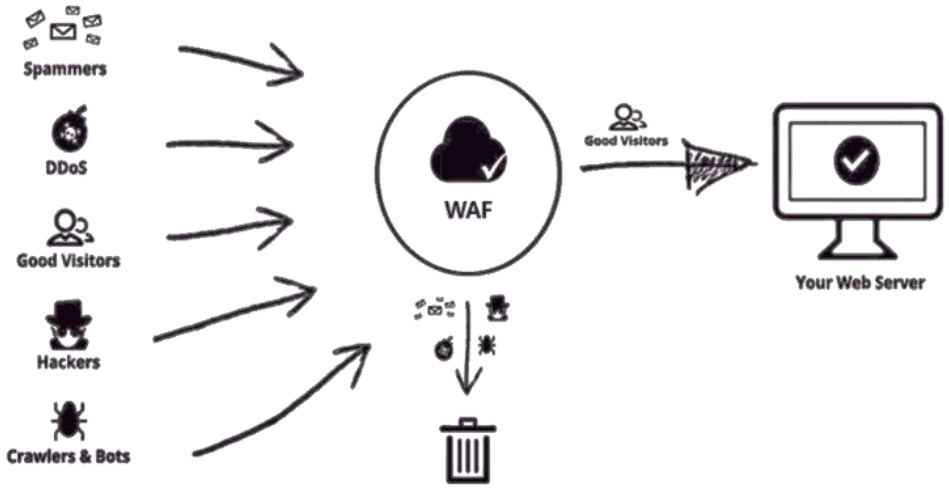
Le rôle du WAF est d'analyser les flux HTTP et HTTPs pour bloquer les tentatives d'attaques sur les applications. Dans l'architecture réseau, le WAF est positionné entre les utilisateurs et les serveurs hébergeant les applications

PARTIE 3

Types de pare-feu d'applications Web

Il existe trois principales façons de mettre en œuvre un WAF :

- **WAF basé sur le réseau** : généralement basé sur du matériel, il est installé localement pour minimiser la latence. Cependant, il s'agit du type de WAF le plus coûteux et il nécessite le stockage et la maintenance d'équipements physiques.
- **WAF basé sur l'hôte** : peut être entièrement intégré dans le logiciel d'une application. Cette option est moins chère que les WAF basés sur le réseau et est plus personnalisable, mais elle consomme beaucoup de ressources de serveur local, est complexe à mettre en œuvre et peut être coûteuse à entretenir. La machine utilisée pour exécuter un WAF basé sur l'hôte doit souvent être renforcée et personnalisée, ce qui peut prendre du temps et être coûteux.
- **WAF basé sur le cloud** : une solution abordable et facile à mettre en œuvre, qui ne nécessite généralement pas d'investissement initial, les utilisateurs payant un abonnement mensuel ou annuel à un service de sécurité. Un WAF basé sur le cloud peut être régulièrement mis à jour sans coût supplémentaire et sans aucun effort de la part de l'utilisateur. Toutefois, étant donné que vous faites appel à un tiers pour gérer votre WAF, il est important de s'assurer que les WAF basés sur le cloud disposent d'options de personnalisation suffisantes pour répondre aux règles commerciales de votre organisation.



Le WAF analyse les requêtes HTTP (Hypertext Transfer Protocol) et applique un ensemble de règles pour séparer les codes bénins des codes malveillants.

PARTIE 3