B3 - Module D5

Introduction à la cybersécurité des SI

Prof. M. LAROUSSI

Définition de la cybersécurité

- Le terme cybersécurité est construit à partir du préfixe « cyber », d'origine grecque, concernant l'étude des processus de contrôle et de communication chez l'être vivant et la machine. *Le préfixe "cyber" est lié à tout ce qui a trait à l'Internet et web.*

- La cybersécurité assure une gestion de la data dans **des conditions optimales et sécurisées**.

- Elle permet **la protection des systèmes d'informations et des données** qui circulent contre ceux que l'on appelle les **cybercriminels**.

- La cybersécurité traite des menaces qui peuvent exister ou non dans le cyberespace.

- Outre les cyberattaques, la cybersécurité permet la mise en place de processus auprès des collaborateurs pour **l'instauration de bonnes pratiques**.

Cybersécurité vs Sécurité informatique

- **La sécurité informatique** protège l'intégrité des technologies de l'information comme les systèmes, les réseaux et les données informatiques contre les attaques, les dommages ou les accès non autorisés.

- La cybersécurité se concentre **plus étroitement sur la protection des systèmes informatiques à toutes les échelles (Etats, organisations, …)**, des dispositifs numériques et des données contre les accès non autorisés.

- La cybersécurité traite des menaces qui peuvent ou non exister dans le cyberespace, telles que la protection des comptes de médias sociaux, les informations personnelles, etc ; tandis **que la sécurité de l'information traite principalement des actifs d'information, de leur intégrité, de leur confidentialité et de leur disponibilité.**

Cibles de la cybersécurité

- La cybersécurité est née de l'interconnexion des réseaux.
- Elle consiste à protéger les ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux, les applications et les données contre les attaques malveillantes.

La sécurité réseaux

- Protéger les infrastructures contre tout intrus, qu'il s'agisse d'attaques ciblées ou de malwares opportunistes (Antivirus, firewall, proxy, …)
- Fiabilité du fonctionnement (câblage, équipements interconnexion, …)
- Confidentialité des accès et gestion des habilitations
- Complexité des mots de passe
- Segmentation en VLAN
- Utilisation des annuaires (Active Directory)
- Utilisation des protocole d'authentification (Radius)

Cibles de la cybersécurité

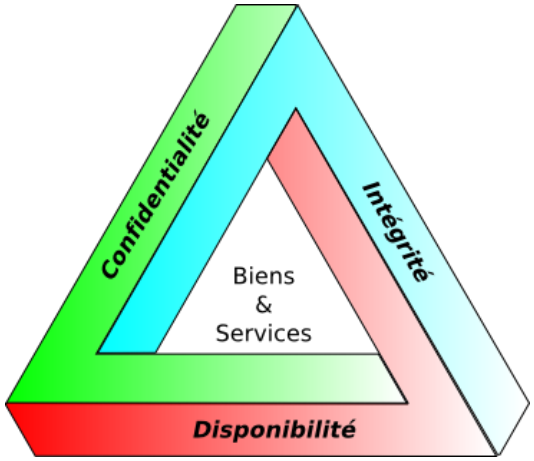
La sécurité des applications

- Protéger les logiciels et les appareils contre les menaces.
- Une application corrompue pourrait ouvrir l'accès aux données qu'elle est censée protéger.
- Un système de sécurité fiable se définit dès l'étape de conception, bien avant le déploiement d'un programme ou d'un appareil.
- Applications en cloud

La sécurité des informations

La SSI (Sécurité des Systèmes d'Information) doit garantir :

- La confidentialité des données
- La disponibilité des data
- Intégrité des données (cryptographie, chiffrement, VPN, …)



Cibles de la cybersécurité

La sécurité opérationnelle

- Les processus et les décisions liés au traitement et à la protection des données.
- Les autorisations et les habilitations accordées aux utilisateurs pour l'accès aux infrastructures
- Les procédures qui définissent le stockage et l'emplacement des données relèvent de ce type de sécurité.

La reprise après sinistre et la continuité des opérations (PRA, PCA)

- La manière dont une entreprise répond à un incident de cybersécurité ou tout autre événement causant une perte des opérations ou de données.
- Les politiques de reprise (PRA) après sinistre régissent la manière dont une entreprise recouvre ses opérations et ses informations pour retrouver la même capacité de fonctionnement qu'avant l'incident.

Cibles de la cybersécurité

Information et formation des utilisateurs

- Facteur le plus imprévisible : les personnes.
- Insister sur l'application des bonnes pratiques
- Tout le monde peut accidentellement introduire un virus dans un système habituellement sécurisé en ne respectant pas les bonnes pratiques de sécurité.
- Apprendre aux utilisateurs à supprimer les pièces jointes suspectes et à ne pas brancher de clés USB non identifiées est essentiel pour la sécurité d'une entreprise.

Cyberattaques

Une **cyberattaque** est un acte de piratage qui cible des Systèmes d'Information (SI) ou des entreprises dépendant de moyens numériques, dans le but de voler, modifier ou détruire un système sensible et capital.

Le gouvernement a classé les **cyberattaques** en 4 catégories :

- Cybercriminalité
  il s'agit d'un délit qui est commis en utilisant un réseau informatique ou l'Internet.
- Atteinte à l'image
  Altération des pages d'un site pour modifier et déformer les contenus
- Espionnage
  Cible beaucoup plus les gouvernements et les structures politiques
- Sabotage.

Mécanismes de la cybersécurité

Parmi les mécanismes de cybersécurité, on pourra citer :

- Les processus d'identification,
- Le chiffrement des données et des connexions,
- Les processus pour le contrôle et la mesure des mécanismes mis en place
- La mise à jour permanentes des logiciels
- La sécurisation des codes
- La sauvegarde et la restauration des données
- L'audit et la traçabilité
- la mise en place de dispositifs permettant la récupération rapide des données sensibles en cas de problèmes techniques

Types de cyberattaques

Les principales cyberattaques qui ciblent les organisations sont :

- Attaques par déni de service (DoS) et par déni de service distribué (DDoS)
- Attaque de l'homme au milieu (MitM)
- Hameçonnage (phishing) et harponnage (spear phishing)
- Cassage de mot de passe
- Injection SQL
- Cross-site scripting (XSS)
- Écoute clandestine
- Vol d'information
- Logiciel malveillant (malware, ransomware)
- Brute force attaque

Déni de service (DoS) par déni de service distribué (DDoS)

- Une attaque par déni de service **submerge les ressources d'un système** afin que ce dernier ne puisse pas répondre aux demandes de service.

- Une attaque DDoS vise elle aussi les ressources d'un système, mais elle est lancée à partir d'un grand nombre d'autres machines hôtes infectées par un logiciel malveillant contrôlé par l'attaquant.

- À la différence des attaques conçues pour permettre à un attaquant d'obtenir ou de faciliter des accès, le déni de service ne procure pas d'avantage direct aux attaquants.

- Une attaque DoS peut aussi avoir pour but de mettre un système hors ligne afin de pouvoir lancer un autre type d'attaque. Un exemple courant de cette technique est le détournement de session (qui sera présenté par la suite).

- Il existe différents 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*.

Outils d'attaques par DOS/DDOS

Low Orbit Ion Cannon (LOIC)

High Orbit Ion Cannon (HOIC)

Slowloris

R.U.D.Y (R-U-Dead-Yet)

https://www.cloudflare.com/fr-fr/learning/ddos/ddos-attack-tools/how-to-ddos/

Attaque de l'homme au milieu (MitM)

L'**attaque de l'homme du milieu** (HDM) ou man-in-the-middle attack (MITM), parfois appelée attaque de l'intercepteur, est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis.

Usurpation d'identité

- Un pirate peut utiliser l'usurpation d'adresse IP pour convaincre un système qu'il communique avec une entité connue et fiable afin de lui donner accès au système.
- Le pirate envoie à un hôte cible un paquet contenant l'adresse IP source d'un hôte connu et fiable au lieu de sa propre adresse IP source.

Relectrure

- Une attaque par rejeu se produit lorsqu'un attaquant intercepte et enregistre d'anciens messages, puis essaie plus tard de les envoyer, se faisant passer pour l'un des participants.
- Ce type d'attaque peut facilement être contré avec un horodatage des sessions ou un *nonce* (nombre ou chaîne aléatoire variant avec le temps).

Attaque de l'homme au milieu (MitM)

Détournement de session

Dans ce type d'attaque MitM, un attaquant détourne une session entre un client de confiance et un serveur réseau.

L'ordinateur attaquant substitue son adresse IP au client de confiance pendant que le serveur poursuit la session, croyant qu'il communique avec le client.

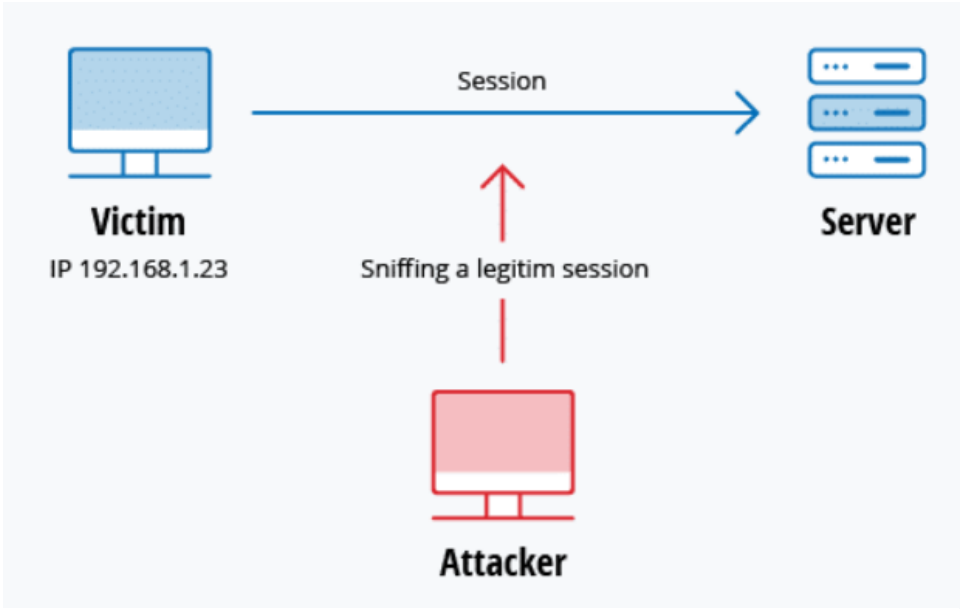
Par exemple, l'attaque pourrait se dérouler ainsi :

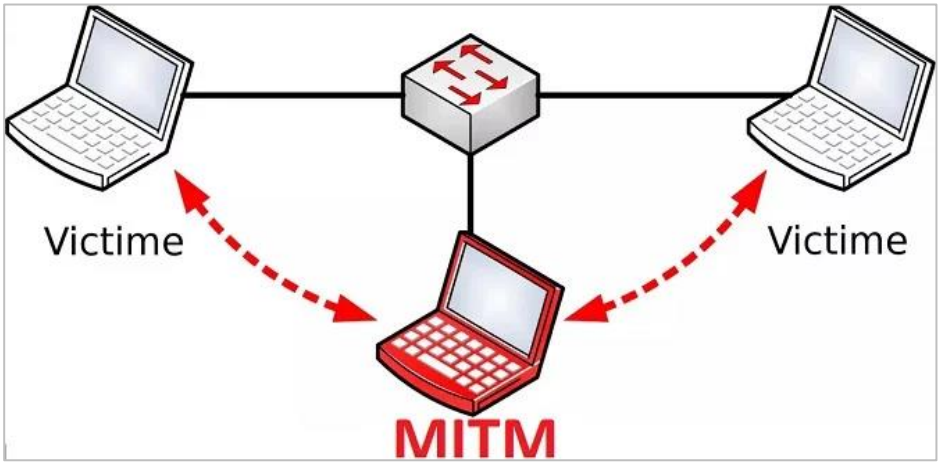
1. Un client se connecte à un serveur.
2. L'ordinateur de l'attaquant prend le contrôle du client.
3. L'ordinateur de l'attaquant déconnecte le client du serveur.
4. L'ordinateur de l'attaquant remplace l'adresse IP du client par sa propre adresse IP et son propre nom de domaine et usurpe les numéros de séquence du client.
5. L'ordinateur de l'attaquant poursuit le dialogue avec le serveur, le serveur croit qu'il communique toujours avec le client.

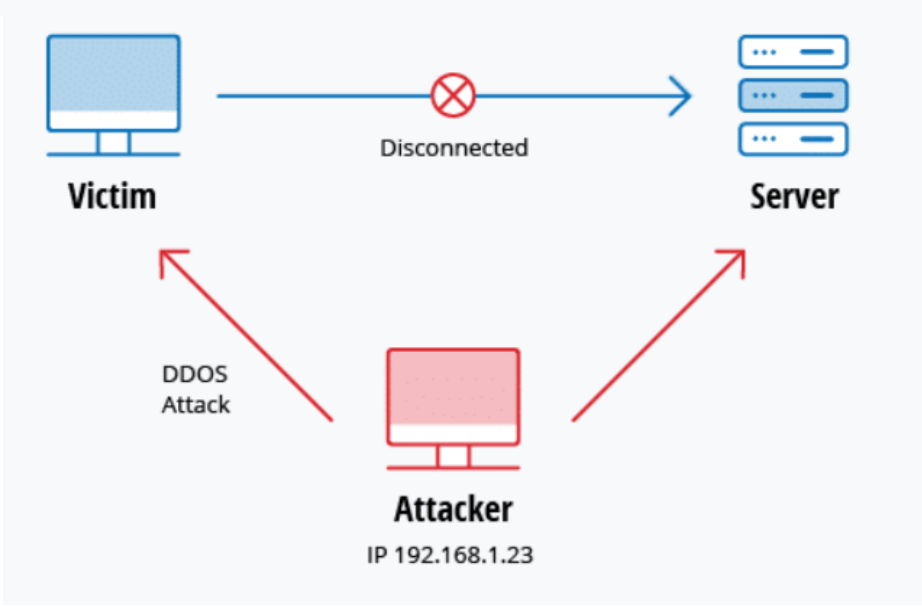
Renniflage des paquets (Packet sniffing)

Injection des paquets

Attaque de l'homme au milieu (MitM)







Attaques phishing et spear phishing

- L'hameçonnage **consiste à envoyer des e-mails qui semblent provenir de sources fiables** dans le but d'obtenir des informations personnelles ou d'inciter les utilisateurs à faire quelque chose.

  En 2013, 110 millions de dossiers clients et enregistrements de cartes de crédit ont été volés auprès de clients de la chaîne de magasins Target.

- Peut impliquer une pièce jointe à un e-mail, qui charge un logiciel malveillant sur votre ordinateur.

- Utilise aussi un lien pointant vers un site Web illégitime qui vous incite à télécharger des logiciels malveillants ou à transmettre vos renseignements personnels.

- **Le harponnage (spear phishing) est un hameçonnage très ciblé**. Les attaquants prennent le temps de mener des recherches sur leurs cibles et de créer des messages personnels et pertinents

- L'un des moyens les plus simples pour un pirate **de mener une attaque de harponnage est d'usurper une adresse électronique**, c'est-à-dire de falsifier la section « De » d'un e-mail, pour vous donner l'impression que le message a été envoyé par une personne de confiance.

Attaque par injection SQL

- L'injection SQL est devenue un problème courant qui affecte les sites Web exploitant des bases de données.

- Elle se produit lorsqu'un malfaiteur exécute une requête SQL sur la base de données via les données entrantes du client au serveur.

- Des commandes SQL sont insérées dans la saisie du plan de données (par exemple, à la place du nom d'utilisateur ou du mot de passe) afin d'exécuter des commandes SQL prédéfinies.

- Un exploit d'injection SQL réussi peut lire les données sensibles de la base de données, modifier (insérer, mettre à jour ou supprimer) les données de la base de données, exécuter des opérations d'administration de la base de données (par exemple la fermer), récupérer le contenu d'un fichier spécifique, et, dans certains cas, envoyer des commandes au système d'exploitation.

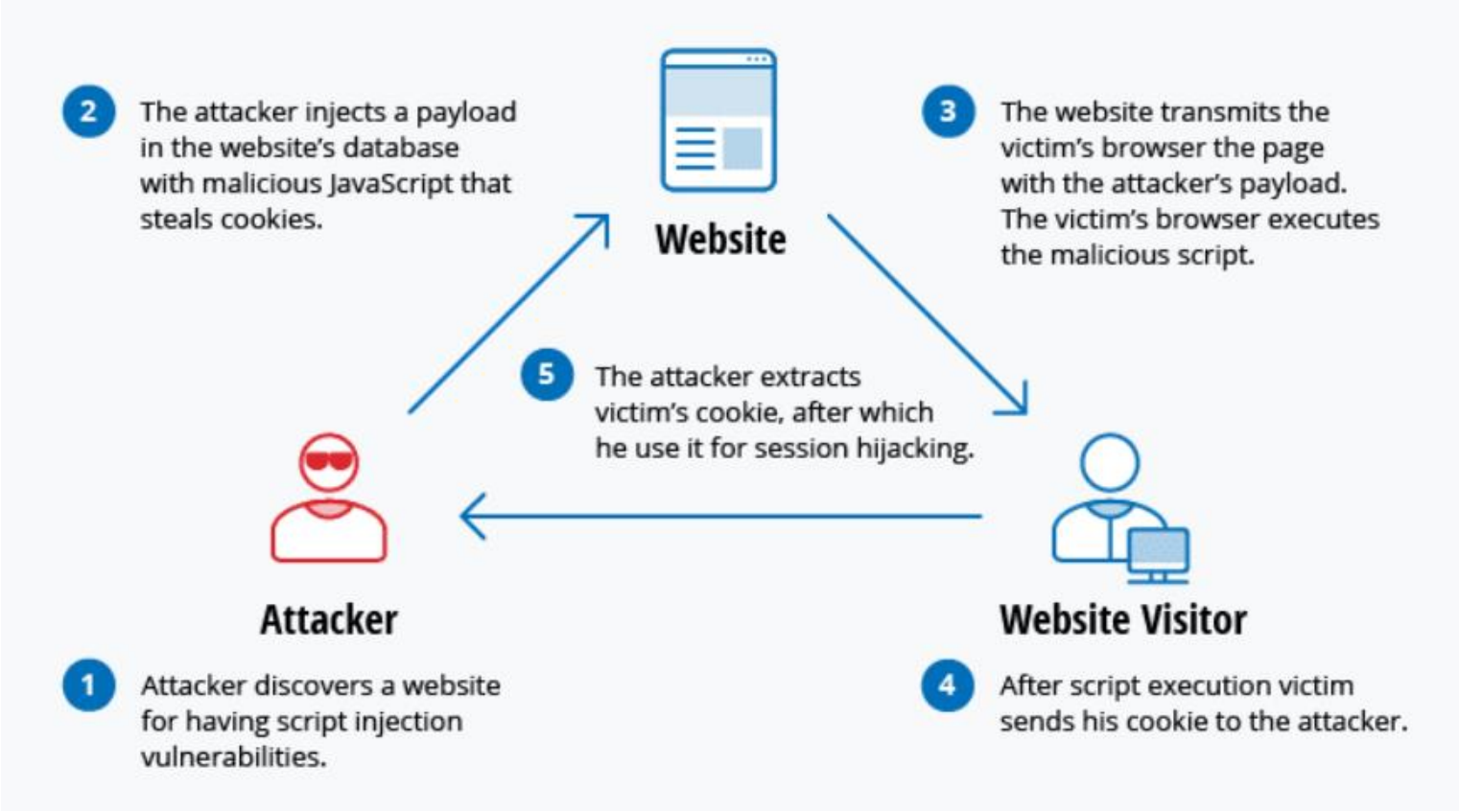
- Par exemple, le formulaire Web d'un site Web peut demander le nom de compte d'un utilisateur, puis l'envoyer à la base de données afin d'extraire les informations de compte associées à l'aide de SQL dynamique, comme ceci :

```
"SELECT * FROM users WHERE account = '" + userProvidedAccountNumber +"';"
```

Attaque XSS (Croiss-site scripting)

- Les attaques XSS utilisent des ressources Web tierces pour exécuter des scripts dans le navigateur Web de la victime ou dans une application pouvant être scriptée.

- L'attaquant injecte un JavaScript malveillant dans la base de données d'un site Web. Lorsque la victime demande une page du site Web, le site Web transmet la page à son navigateur avec le script malveillant intégré au corps HTML



Attaque par des logiciels malveillants

Un logiciel malveillant peut être décrit comme un logiciel indésirable installé dans votre système à votre insu.

Il peut s'attacher à un code légitime et se propager, se cacher dans des applications utiles ou se reproduire sur Internet.

Quelques types de logiciels malveillants les plus courants :

- Macro-virus –
- Infecteurs de fichiers
- Infecteurs de système ou de secteur d'amorçage
- Virus furtifs (rootkit)
- Chevaux de Troie
- Bombe logique
- Vers et virus
- Injecteurs
- Rançongiciels (ransomware)
- Logiciels publicitaires (adware)
- Logiciels espions (spyware)

Attaque par des logiciels malveillants

- Le **ransomware** (aussi appelé rançongiciel ou cryptolocker) est une variante de malware (cheval de troie) particulièrement populaire depuis 2010.

- Le principe est d'utiliser un virus qui va chiffrer les fichiers de l'utilisateur contre son gré, puis d'exiger le paiement d'une rançon contre la clé de chiffrement utilisée par le ransomware

- Les différentes familles de ransomwares telles que Teslacrypt et autres Locky présentent des caractéristiques différentes et ont parfois recours à des outils de chiffrement différent. (*https://fr.wikipedia.org/wiki/TeslaCrypt*)

Attaque par des logiciels malveillants

Dans la liste présentée précédemment, chaque groupe choisit 3 types de logiciels malveillants et réalise une présentation qui permettra de décrire les aspects suivants :

- Nom du malware
- Date de création
- Auteurs
- Faille d'exploitation
- Effets réalisés sur un système
- Outils utilisés pour lancer le type d'attaques
- Données statistiques si possible

Qu'est-ce que l'OWASP ?

- L'Open Web Application Security Project, ou OWASP, est une organisation internationale à but non lucratif qui se consacre à la sécurité des applications web.
- L'un des principes fondamentaux de l'OWASP est que tous ses documents soient disponibles gratuitement et facilement accessibles sur son site web, ce qui permet à chacun d'améliorer la sécurité de ses propres applications web.
- Le matériel qu'ils proposent comprend de la documentation, des outils, des vidéos et des forums.
- Leur projet le plus connu est peut-être le Top 10 de l'OWASP.

OWASP (L'Open Web Application Security Project

- Attaques par Injection SQL
- Authentification frauduleuse
- Exposition aux données sensibles
- Entités externes XML (XEE)
- Contrôle d'accès interrompu
- Mauvaise configuration de la sécurité
- Scénario de site croisé
- Désérialisation incertaine
- Utilisation de composants présentant des vulnérabilités connues
- Insuffisance de l'enregistrement et de la surveillance