Cybersécurité :

Plan du cours :

I. POSITION DU PROBLÈME

A. Cybermenaces

Les menaces contrées par la cybersécurité sont au nombre de **trois** :

1. **La cybercriminalité** : comprend des acteurs isolés ou des groupes qui ciblent des systèmes pour des gains financiers ou pour causer des perturbations.
2. **Les cyberattaques** : impliquent souvent la collecte d'informations pour des raisons politiques.
3. **Le cyberterrorisme** : vise à saper les systèmes électroniques pour entraîner panique ou peur.

B. Typologie des méthodes d'attaques :

De nombreuses méthodes d'attaque sont possibles, telles que :

Malware :

Les programmes malveillants, appelés « malware »

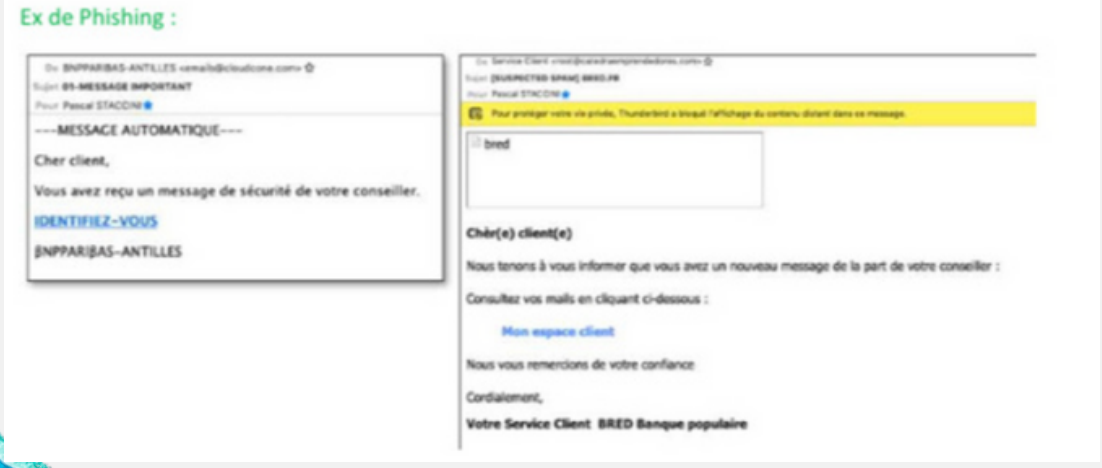
L'injection SQL :

C'est le fait d'insérer du code malveillant dans une base de données via une déclaration SQL malveillante. Ils gagnent ainsi l'accès à des informations sensibles contenues dans la base.

Attaques par phishing :

Aussi appelée tentative d'hameçonnage, le phishing consiste en l'envoi d'emails qui semblent provenir d'une entreprise légitime. Ils servent souvent à tromper les utilisateurs pour récupérer leurs coordonnées bancaires et d'autres informations personnelles.

Ex de Phishing :



Attaque dite de l'homme du milieu:

Une attaque dite de l'homme du milieu désigne un type de cybermenace consistant à intercepter la communication entre deux individus pour leur voler des données. Par exemple, sur un réseau wifi non sécurisé, un cybercriminel pourrait intercepter les données transitant entre l'appareil de la victime et le réseau.

Attaque par déni de service :

Une attaque par déni de service désigne le fait, pour les cybercriminels, d'empêcher un système informatique de répondre à des requêtes légitimes en surchargeant les réseaux et les serveurs avec du trafic. Le système devient ainsi inutilisable, empêchant une entreprise de mener à bien l'essentiel de ses tâches.

L'inside job :

Dans ce cas la fuite de données provient d'un des collaborateurs de l'entreprise

C. Nouvelles cybermenaces parmi les méthodes d'attaques :

- **Malware Dridex**

En décembre 2019, le ministère de la justice américain a inculpé le chef d'un groupe cybercriminel organisé pour son rôle dans une attaque mondiale. **Dridex est un cheval de Troie bancaire**. Arrivé en 2014, il infecte les ordinateurs via des emails de **phishing** ou des **malwares** existants. Capable de voler les mots de passe, les coordonnées bancaires et les données personnelles qui pourront être utilisés pour effectuer des transactions malhonnêtes, il a causé des pertes financières massives s'élevant à des centaines de millions. En réponse aux attaquesDridex, le National Cyber Security Centre anglais conseille au public de « s'assurer que ses appareils sont patchés, que son antivirus est activé et à jour, et que ses fichiers sont sauvegardés ».

- **Arnaques sentimentales`**

En février 2020, le FBI mettait en garde les citoyens américains contre les escroqueries mises en place par les cybercriminels sur **les sites de rencontre**, les salons de discussion et les applications. Leurs auteurs profitent des personnes à la recherche de nouveaux partenaires en les dupant pour obtenir leurs données personnelles. Les arnaques sentimentales ont touché 114 victimes au Nouveau-Mexique en 2019, générant une perte financière de 1,6 million de dollars.

- **Malware Emotet**

Fin 2019, L'australian cyber security center mettait en garde les organisations nationales contre une cybermenace mondiale impliquant le malware Emotet. Emotet est un **cheval de Troie** sophistiqué capable de voler les données et également de **télécharger d'autres malwares**. Emotet prospère grâce à des **mots de passe peu sophistiqués** : un rappel de l'importance de créer un mot de passe sûr pour se prémunir contre les cybermenaces.

D. Programmes malveillants

Les **malwares** désignent des **logiciels malveillants** : l'une des cybermenaces les plus courantes. C'est un logiciel créé par un cybercriminel ou un hacker pour perturber ou endommager l'ordinateur d'un utilisateur.

Souvent le malware est propagé via **la pièce jointe** d'un email indésirable ou un téléchargement d'apparence sûr. Il peut être utilisé par les cybercriminels pour gagner de l'argent ou bien lors de cyberattaques sur fond de politique.
On retrouve plusieurs types de malwares :

- **Virus** : programme pouvant se dupliquer qui s'attache à un fichier sain et se propage dans tout le système en infectant les fichiers à l'aide d'un code malveillant.
- **Cheval de troie** : type de programmes malveillants se faisant passer pour des logiciels authentiques. Les cybercriminels piègent les utilisateurs en téléchargeant des chevaux de Troie dans leur ordinateur pour endommager ou collecter des données.
- **Spyware** : un programme espion qui enregistre secrètement les actions d'un utilisateur au profit des cybercriminels. *Par exemple, un spyware peut enregistrer des coordonnées bancaires.*
- **Ransomware** : un malware qui verrouille les fichiers et les données de l'utilisateur sous menace de les effacer si une rançon n'est pas payée.
- **Adware** : un logiciel publicitaire qui peut être utilisé pour propager un malware.
- **Botnets** : des réseaux d'ordinateurs infectés par des malwares que les cybercriminels peuvent utiliser pour effectuer des tâches en ligne sans l'autorisation de l'utilisateur.

E. Fuite de données

Une fuite de données est une exposition non désirée, publique ou privée, subie par une entreprise ou un particulier.

Les causes principales sont :

- les **cyberattaques** = **48%**
- **l'erreur humaine** = **27%**
- **l'erreur système** (IT et processus internes) = **25%.**

Au premier semestre 2019, il y a eu en moyenne 5,7 violations de données par jour en France contre 4,5 au deuxième semestre 2018.

- Dans 54% des cas, les fuites de données ont été d'**origine malveillante** avec 69,8% de piratage en ligne et 15% de vol physique.
- 26% des fuites de données sont accidentelles et pour le reste, les causes sont "inconnues" ou "autre".

Le premier secteur touché est celui des "**sciences et techniques**" avec 297 notifications entre juin 2018 et juin 2019. "**Le commerce**" a notifié 279 violations de données suivi par "**la finance**" (275), "**l'administration publique**" (229) et enfin "**l'hébergement et de la restauration**" avec 202 notifications.

Pour un attaquant, le vol de données permet :

- de financiariser une attaque : en vendant les données collectées ;
- de compléter une attaque : le vol de données permet d'acquérir ou d'amasser de la connaissance sur une cible précise, avant de lancer ensuite une attaque de plus grande importance.

Exemple : 2018, **Le scandale Facebook-Cambridge Analytica** : fuite des données personnelles de 87 millions d'utilisateurs Facebook que la société Cambridge Analytica (CA) a commencé à recueillir dès 2014. Les informations ont été obtenues par l'application « thisisyourdigitallife », un test de personnalité monté par l'universitaire Aleksandr Kogan de Cambridge, via sa société Global Science Research (GSR). Par ce biais, les internautes autorisaient à la fois la captation de certaines de leurs données (comme la ville ou les contenus aimés), mais aussi certaines infos de leurs amis, si leurs paramètres le permettaient. Ces informations ont servi à **influencer les intentions de vote** en faveur d'hommes politiques qui ont retenu les services de CA. L'affaire Cambridge Analytica a valu au réseau social **une amende record de cinq milliards de dollars**, infligée par la FCC, **la Commission fédérale des communications américaine.**

Toutes régions du monde confondues, il faut en moyenne **197 jours** à une entreprise pour **découvrir que des données ont été compromises**. Une fois identifiée, **le temps moyen de remédiation** d'une data breach s'élève à **69 jours**.

Les facteurs réduisant les impacts d'une fuite de données sont :

- **l'implication du comité de direction** sur les questions de cybersécurité
- **la sensibilisation** des employés
- la mise en place d'une **classification** des données
- l'usage d'un **logiciel de data lost protection** (DLP) (logiciel de protection desdonnées informatiques)
- la présence (en interne ou en externe) d'une **équipe de réponse aux incidents** (en cas de brèche de données)

Face à un incident, la conduite à tenir est :

- « PREVENIR » en préparant les équipes techniques et non techniques à la gestion de l'attaque
- « DETECTER » via une « équipe de cyber intelligence »,
- « ASSURER » pour couvrir les conséquences (frais de gestion, notification, préjudices financiers...)
- « REAGIR » en prévenant la Cnil dans les 72 heures suivant l'incident.

II. SÉCURITÉ INFORMATIQUE

A. Définition de la cybersécurité

La **cybersécurité** assure une **gestion de la donnée dans des conditions optimales et sécurisées**. Elle consiste à protéger les ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données contre les attaques malveillantes.

On l'appelle également **sécurité informatique** ou **sécurité des systèmes d'information**.

On la rencontre dans de nombreux contextes, de l'informatique d'entreprise aux terminaux mobiles. Le secteur de la santé n'est pas épargné !

B. Objectifs de la cybersécurité

C. Sécurité physique

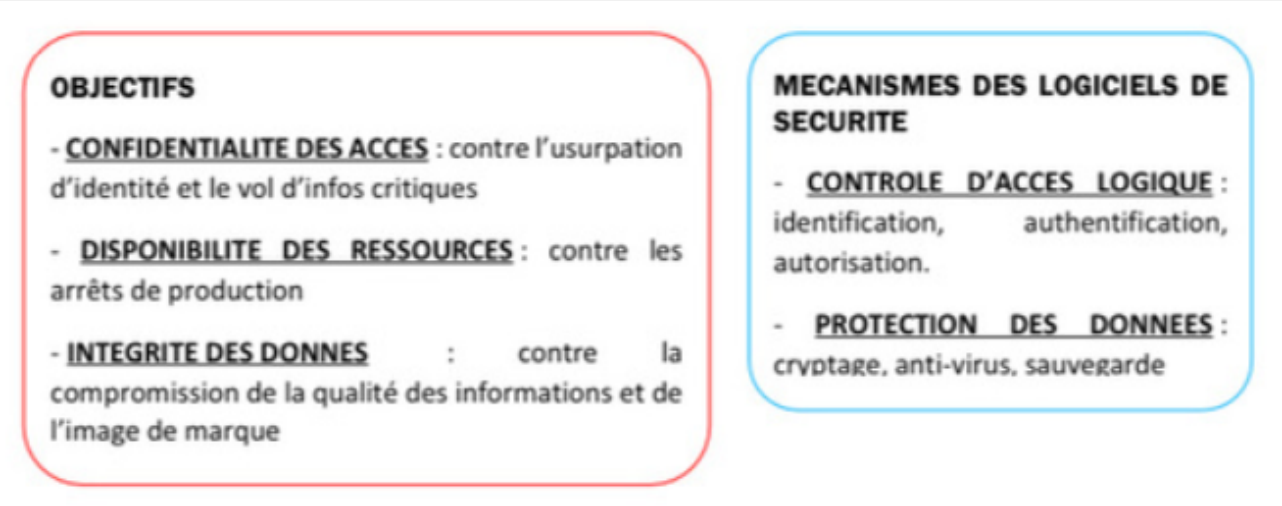
La sécurité physique consiste aussi en l'usage de **barrières, alarmes, serrures et autres contrôles physiques** permettant de conditionner l'accès physique aux locaux, aux ordinateurs et aux équipements.

Ces mesures sont nécessaires pour protéger les ordinateurs, leur contenu et les autres ressources matérielles contre l'espionnage, le vol et la destruction accidentelle ou intentionnelle :

- Sécurité dégâts des eaux
- Sécurité de l'électricité
- Sécurité de la climatisation
- Sécurité dégâts du feu
- Dégâts liés à l'électrostatique
- Dégâts liés à une intervention physique
- Dégâts liés aux communications
- Sécurité de l'accès à la salle informatique

D. Sécurité logique

La sécurité logique repose sur la mise en œuvre d'un système de contrôle d'accès logique s'appuyant sur un service d'authentification, d'identification et d'autorisation, et elle repose également sur les dispositifs mis en place pour garantir la confidentialité, dont la cryptographie, une gestion efficace des mots de passe et des procédures d'authentification, des mesures antivirus et de sauvegarde des informations sensibles.



E. Typologie des sécurités

La sécurité des réseaux consiste à protéger le réseau informatique contre les intrus, qu'il s'agisse d'attaques ciblées ou de malwares opportunistes.

La sécurité opérationnelle comprend les processus et les décisions liés au traitement et à la protection des données. Les autorisations des utilisateurs pour l'accès au réseau et les procédures qui définissent le stockage et l'emplacement des données relèvent de ce type de sécurité.

La sécurité des informations veille à garantir l'intégrité et la confidentialité des données, qu'elles soient stockées ou en transit.

La sécurité des applications : vise à 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 reconnaît dès l'étape de conception, bien avant le déploiement d'un programme ou d'un appareil.

La reprise après sinistre et la continuité des opérations spécifient 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 après sinistre régissent la manière dont une entreprise recouvre ses opérations et ses informations pour retrouver la même capacité de fonctionnement qu'avant l'événement. La continuité des opérations se réfère au plan sur lequel s'appuie une entreprise tout en essayant de fonctionner sans certaines ressources.

La formation des utilisateurs finaux porte sur le facteur le plus imprévisible : les personnes. 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.

F. Classes des cybersécurités

Classe 1 :

Il s'agit des systèmes industriels pour lesquels le risque ou l'impact d'une attaque est faible. L'ensemble des mesures préconisées pour cette classe doivent pouvoir être appliquées en complète autonomie. Ce niveau correspond principalement aux règles d'hygiène informatique énoncées dans le guide de l'ANSSI.

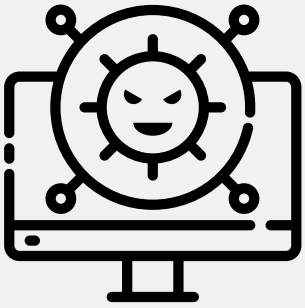
Classe 2 :

Il s'agit des systèmes industriels pour lesquels le risque ou l'impact d'une attaque est significatif. Il n'y a pas de contrôle étatique pour cette classe de système industriel mais l'entité responsable doit pouvoir apporter la preuve de la mise en place des mesures adéquates en cas de contrôle ou d'incident.

Classe 3 :

Il s'agit des systèmes industriels pour lesquels le risque ou l'impact d'une attaque est critique. Dans cette classe, les obligations sont plus fortes et la conformité de ces systèmes industriels est vérifiée par l'autorité étatique ou un organisme accrédité

Les deux premières parties de ce cours c'est PAR COEUR surtout les exemples des méthodes d'attaque ainsi que les types de programmes malveillants ! Le professeur aime beaucoup les faire tomber en examen ! De même que la typologie des sécurités et les classes des cybersécurité !



III. COMPLÉMENTS

A. Cybersurveillance :

La « cybersurveillance » est un mécanisme de surveillance de personnes (physiques ou morales), de locaux, d'objets physiques ou de processus de travail. Elle s'exerce au niveau des systèmes d'information, en particulier via les réseaux de communication numériques.

Tout comme la surveillance, mais avec des capacités adaptées au traitement de données volumineuses, variées et véloces, elle renvoie à des activités de collecte et d'analyse d'informations poursuivant diverses finalités :

Prévenir certains risques,
Orienter les investigations,
Identifier les protagonistes susceptibles d'avoir causé ou facilité un acte de malveillance délictueux ou criminel.

- **Cybersurveillance ANS :**

Depuis le 1er octobre 2017, les structures de santé sont tenues de relayer aux agences régionales de santé (ARS) les incidents de sécurité informatique jugés "graves" et "significatifs", et l'Agence du Numérique en Santé (ANS) est chargée d'apporter un appui au traitement des incidents.

Le service cybersurveillance de l'ANS réalise des **audits externes de cybersécurité** des établissements de santé à distance et à leur demande : L'analyse se concentre sur les applications médicales, et/ou elle utilise les signalements d'incidents à la cellule d'accompagnement cybersécurité des structures de santé (ACSS) de l'ANS.

- **Cybersurveillance ANS, résultats :**

Le constat est alarmant :

50% des structures auditées n'avaient **jamais réalisé d'audit de sécurité**
40% n'avaient **aucun mécanisme de protection en place**
Dans 40% des établissements, des **serveurs à l'abandon ou non répertoriés** ont été découverts

Outre le risque de divulgation d'informations, les autres vulnérabilités les plus répandues concernent :

l'implémentation de la **cryptographie** (23%)
la gestion des **correctifs** (18%)
la gestion de la **configuration logicielle** (11%)
le défaut de **contrôle d'accès** (10%)

Les vulnérabilités les plus graves détectées sont :

un **système d'exploitation qui n'est pas à jour** (37% des cas) + la possibilité d'**attaque par force brute ou dictionnaire sur les mots de passe** (37%)

la présence d'un **composant obsolète** (37%), des injections possibles de code au sein d'une application (21%) des **serveurs de développement accessibles** (21%)

B. Guide d'hygiène informatique :

Le guide d'hygiène informatique est édité par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). 42 mesures d'hygiène informatique constituent le socle minimum pour protéger les informations de l'organisation.

Ces mesures sont classées en 9 chapitres :

- **Sensibiliser et former**
- **Connaître le système d'information Authentifier et contrôler les accès**
- **Sécuriser les postes**
- **Sécuriser le réseau**
- **Sécuriser l'administration**
- **Gérer le nomadisme**
- **Maintenir le système d'information à jour**
- **Superviser, Auditer, Réagir**

C. Sécurité et RGPD :

L'obligation de sécurité des données personnelles est prévue à l'article 32 du RGPD. Les sanctions peuvent atteindre jusqu'à 10 M€ ou 2% du chiffre d'affaires annuel mondial.

La sécurité doit être proportionnée aux risques : le fichier des membres d'une association sportive demande certainement moins de sécurité que des bases de données médicales.

Les risques concernent :

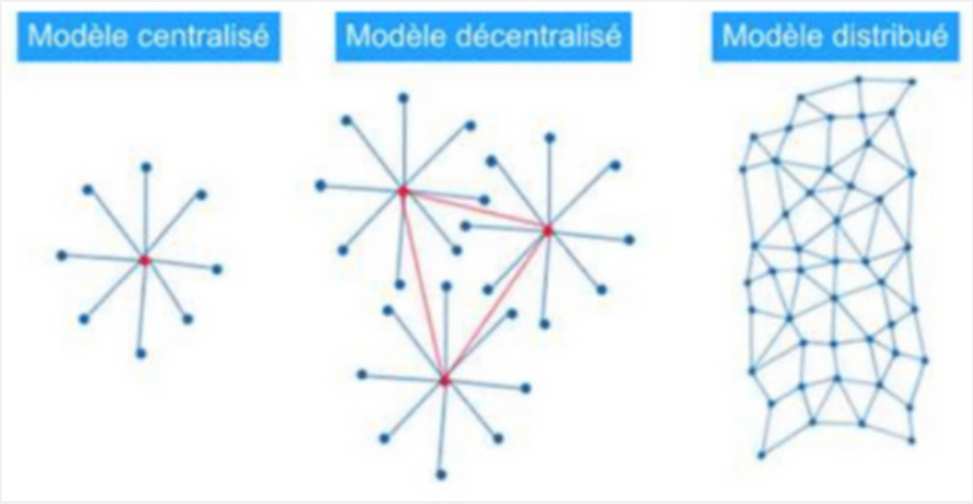
- **les accès non autorisés** (confidentialité),
- **les modifications non désirées** (intégrité)
- **les disparitions de données** (disponibilité) ;

La source de ces risques peut être interne ou externe, et accidentelle ou délibérée : il peut s'agir d'employés ou visiteurs, mais aussi de concurrents, d'attaquants malveillants, voire du crime organisé. Il faut également tenir compte des pannes (serveurs, climatisation, etc.), des sinistres (inondation, incendie, etc.) et **autres incidents** (casse, mauvaise manipulation, etc.), comme des **actions volontaires** (vol d'ordinateur, attaque informatique, etc.).

La pseudonymisation et le chiffrement ne sont que des exemples : il s'agit de bonnes pratiques qui peuvent être pertinentes dans les systèmes, mais il ne s'agit pas des seules mesures à envisage

D. Gouvernance des systèmes distribués :

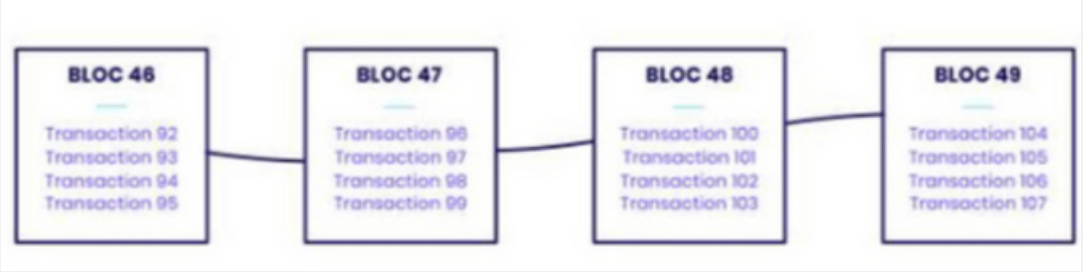
Traditionnellement, les réseaux informatiques adoptent **un modèle de gouvernance centralisé** autour d'une **base de données unique et centrale**. Les modèles **décentralisés** permettent de gérer des **réseaux plus étendus**, mais conservent **des points de contrôle « centralisés »**. Dans les réseaux **distribués**, chaque nœud du réseau doit avoir accès à la même information.



E. Blockchain : sécurité distribuée

Une **blockchain** (ou chaîne de blocs) est une technologie de **stockage** et de **transmission** d'informations, **transparente**, **sécurisée** et fonctionnant **sans organe central de contrôle**. C'est une base de données **distribuée**, **infalsifiable**, sur laquelle les informations enregistrées sont soumises au **contrôle des acteurs** du réseau.

Une blockchain constitue une base de données qui contient **l'historique** de tous les échanges effectués entre ses utilisateurs depuis sa création. Cette base de données est **sécurisée** et **distribuée** : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne.

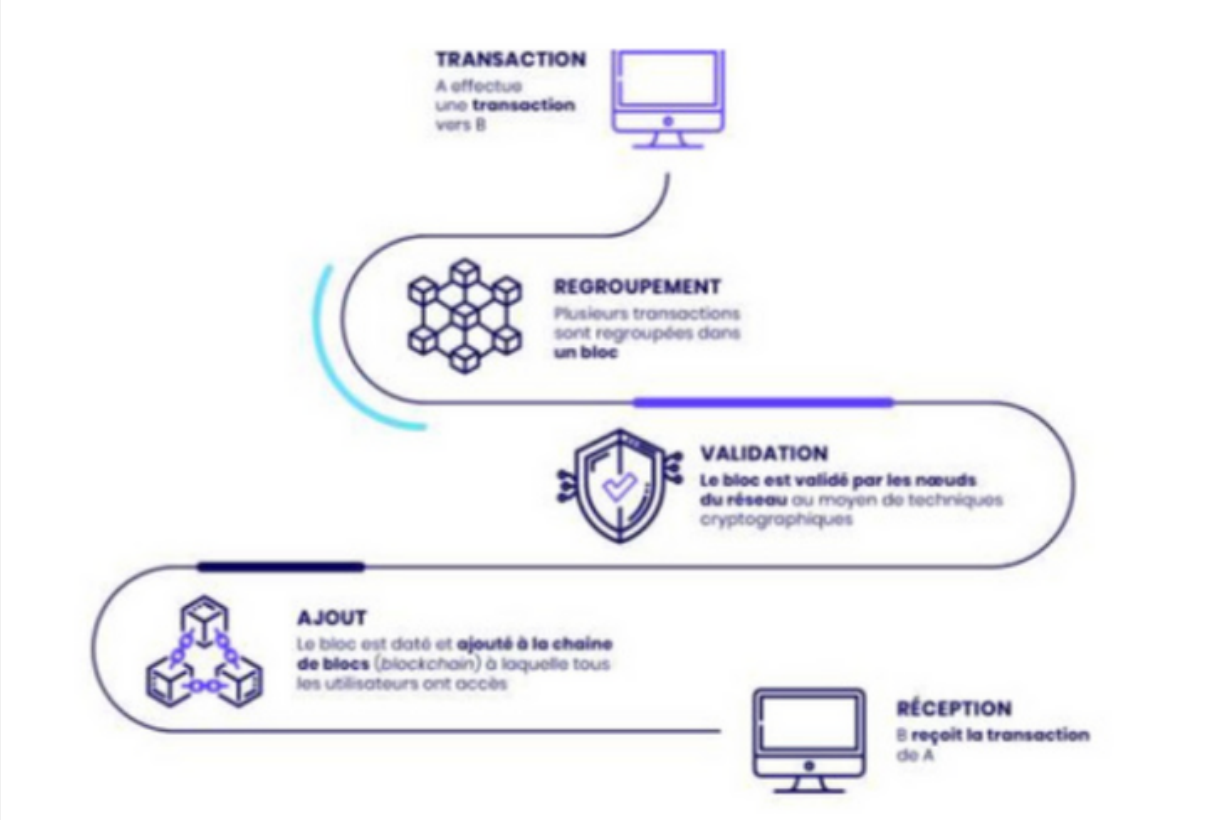


On retrouve plusieurs types de blockchains :

Les blockchains dites **publiques**, où n'importe qui peut rejoindre le réseau et l'utiliser pour échanger avec d'autres participants,

Les blockchains dites **privées**, où seuls certains participants sont autorisés à rejoindre et utiliser le réseau. Le rôle des participants est rigoureusement défini et contrôlé.

Les **consortiums** qui peuvent être considérés comme des blockchains **privées** avec cependant des **réseaux plus conséquents**. Ce sont souvent des blockchains créées par des groupes d'entreprises, généralement du même secteur d'activité.



F. Lexique :

- **Profil d'habilitation** : un profil d'habilitation définit, pour un groupe d'utilisateurs, leurs droits sur un ensemble de données et/ou d'applications.

- **Routeur filtrant et ACL** : un routeur est un équipement qui permet l'aiguillage de l'information entre deux réseaux. Certains routeurs intègrent une fonction de filtrage du trafic, telle que celle des pares-feux, qui met en œuvre une liste des adresses et ports autorisés ou interdits d'accès (Access Control List).

- **Pare-feu (ou « firewall »)** : équipement logiciel et/ou matériel permettant de cloisonner des réseaux. Il met en œuvre des règles de filtrage du trafic entrant et sortant et doit interdire l'utilisation de protocoles de communication non sécurisés (Telnet par exemple).

- **« tunneling » ou VPN (réseau privé virtuel)** : un VPN permet de sécuriser les échanges de données de type "extranet". Pour cela, il met en œuvre un mécanisme d'authentification et de chiffrement des données. On parle alors d'encapsulation des données grâce à un protocole de « tunneling ».

- **Chiffrement** : méthode de codage/décodage des données mettant généralement en œuvre un mécanisme de clé(s) logique(s) afin de rendre impossible la lecture d'un fichier à des tiers qui ne possèdent pas la ou les clé(s).

- **IPsec, SSL/TLS, HTTPS** : protocoles réseaux permettant de sécuriser les accès distants par chiffrement des données transmises.

- **Tolérance de panne** : dispositif de sécurité mis en œuvre notamment au niveau des disques durs qui permet de se prémunir de la panne d'un disque en évitant l'arrêt des applications ou l'endommagement des données stockées.

- **BIOS** : système exécutant, à la mise sous tension d'un ordinateur, des opérations élémentaires telles que le contrôle des éléments matériels, l'ordonnancement de démarrage des périphériques, la lecture d'un secteur sur un disque.

C'est finit ! Le cours est long c'est vrai mais largement faisable en plusieurs fois ! Je le mettrais à jour dés que le cours sera fait. Je vous sortirais surement une fiche récapitulative du cours pour vous permettre de vous concentrer sur les notions importantes.

Le cours est déjà assez long je m'arrête là ! Bonne chance dans vos révisions !