SÉcuritÉ des systèmes d’informatioN : eNJEUX ET CONTRAINTE DE LA CYBERSÉCURITÉ EN ENTREPRISE

Florian BESSE

[Introductions : 2](#_Toc159343379)

[Définitions : 3](#_Toc159343380)

[ Le Cyber 3](#_Toc159343381)

[ Systèmes d’informations 3](#_Toc159343382)

[ Cybersécurité 7](#_Toc159343383)

[Les enjeux de la cybersécurité : 9](#_Toc159343384)

[ Économique 9](#_Toc159343385)

[ Géopolitique 12](#_Toc159343386)

[ Vie privé 15](#_Toc159343387)

[Les contraintes de la cybersécurité 18](#_Toc159343388)

[ L’évolution 18](#_Toc159343389)

[ Financier 19](#_Toc159343390)

[ La détection d’une attaque 20](#_Toc159343391)

[Bilan 23](#_Toc159343392)

[ Bilan des enjeux 23](#_Toc159343393)

[ Bilan des contraintes 23](#_Toc159343394)

[ Bilan général 24](#_Toc159343395)

[Bibliographie 25](#_Toc159343396)

[Glossaire 28](#_Toc159343397)

[Table des illustrations 29](#_Toc159343398)

# Introductions :

Les systèmes informatiques sont omniprésents à ce jour, en effet et c’est pour cela que les entreprises doivent se prémunirent de systèmes de sécurités informatiques en effet maintenant la cybersécurité en entreprise est obligatoire pour pouvoir assurer la sécurité de leur système d’information. Ça nous amène à nous poser comme question la sécurité des systèmes d’informations : qu’elles sont les enjeux et contraintes de la cybersécurité en entreprise ? Mais avant de répondre à cette question nous allons d’abord définir ce qu’es la cybersécurité et un système d’information avant de découper le sujet en plusieurs parties pour pouvoir y répondre.

# Définitions :

## Le Cyber

Avant de rentrer dans le vif du sujet nous allons commencer par définir le mot cyber, c’est un préfixe qui sert à former des mots qui sont en rapport avec l’utilisation de tout ce qui fait partie du réseaux internet, il est donc lié à l’usage des technologies numérique.

## Systèmes d’informations

Nous allons tout d’abord commencer à définir ce qu’est un système d’information c’est un ensemble de ressources qui permet la gestion de l’information, c’est initialement associé aux technologie (le matériel, logiciel et la communication). Un SI (système d’information) possède 4 fonctions que nous allons détailler :

**-Collecter :** La sauvegarde de l’information sert à procéder à son traitement. Il peut y avoir 2 provenances de collecte :

1. **Collecte interne :** C’est le flux d’information qui est généré par les entités internes d’une entreprise/organisation (production, gestion des salariés, comptabilité, …), le fonctionnement de l’entreprise et les information informelles (climat-social, comment se sente les salariés, …).
2. **Collecte externe :** C’est le flux d’informations qui est généré par les entités externe d’un entreprise/organisation (client, fournisseur, …) ce qui est essentiel à l’adaptation du SI au sein de l’entreprise/organisation, il est important pour l’entreprise d’être particulièrement attentive aux sources d’informations externes.

-**Stocker :** Lorsque les informations sont collectées et saisie ils font donc les stocker de manière sécuriser, durable et stable pour pouvoir potentiellement être réutiliser ultérieurement ou pour des raisons légales. Ces informations sont stockées dans des bases de données ou dans un fichier :

1. **Base de données :** c’est une structure qui permet de ranger les informations un peut à la manière d’un tableau Excel



Figure : Schéma d'une base de données

1. **Un fichier :** C’est un ensemble de données qui sont réunie sous un même nom



Figure : Schéma d'un fichier

Mais une fois collecter il faut savoir où stocker ces données ? car il existe plusieurs méthodes de stocker les données :

1. **Les disques durs :** ils sont présents au sein du serveur du SI de l’organisation (ces informations est accessible que depuis ce serveurs).
2. **Les aires de stockages :** Il s’agit de gros disques durs accessible par le réseau de l’entreprise (ces informations sont accessibles par tous au sein de l’organisations où se trouvent le SI).
3. **Le cloud :** L’information est stockée dans un cloud donc accessible à tous le monde.

**- Traiter :** le traitement de l’information permet de pouvoir produire de nouvelles informations grâce aux informations déjà existante (soit via des programmes informatiques ou via des opérations manuelles), le traitement peut avoir plusieurs formes différentes :

1. **Consulté l’information :** Cela consiste à accéder à l’informations comme elle a été enregistré à la base
2. **Organiser l’information :** elle consiste donc à organiser l’informations selon leurs critère spécifique (par client, par métier, par secteur, etc…)
3. **Mettre à jour l’information :** Ça sert à reprendre une information déjà enregistré et à l’actualiser.
4. **Produire de nouvelles informations :** Grace à des informations existante ce traitement va pouvoir crée de nouvelles informations
* **Diffusé :** C’est une diffusion de l’information (exemple une fiche de paye)

## Cybersécurité

Maintenant que nous avons défini ce qu’était un système d’informations nous allons donc définir ce qu’est la cybersécurité. La cybersécurité est une activité qui vise à protéger es systèmes informatiques, les réseaux et les programmes contre des cyberattaque, souvent des cyberattaques cherche à accéder aux informations sensibles pour soit extorquer de l’argent aux entreprises soit les détruire où alors bloquer le fonctionnement normal d’une entreprise. Pour pouvoir se prémunir contre ces attaques ils existent plusieurs types de sécurité :

1. **La sécurité du réseau :** Protections du réseaux informatiques contre des attaques ciblé ou alors des malwares.
2. **La sécurité d’application :** C’est la protection de logiciel/appareil contre des menaces puisqu’en effet une application infecté peut ouvrir l’accès aux données.

1. **La sécurité d’information :** Protection des données donc en garantir la confidentialité.
2. **La sécurité opérationnelle :** Elle consiste à gérer les autorisations des utilisateurs à l’accès du réseau car elle comprend les processus et les décisions liés au traitement et à la protection des données.

Une fois que nous avons pu définir le cyber, les systèmes d’informations et la cybersécurité nous allons maintenant pouvoir commencer à répondre à nôtre problématique.

# Les enjeux de la cybersécurité :

## Économique

La cybersécurité à des enjeux économique important sur une entreprise, si une entreprise subit une cyberattaque cela peut nuire à sa réputation.
Donc cela peut atteindre les actions d’une entreprise dont celle-ci peuvent baisser, partagé des données confidentielles qui peuvent déplaire au client d’une entreprise ou à leur partenaire professionnel ce qui dans le pire des cas peut faire tomber en faillite une entreprise, couper toute activité d’une entreprise le temps qu’elle règle le problème donc perte de temps de travail égale perte économique.

Depuis 2020 le nombre de cyberattaque attaque n’a cessé de croitre en France puisqu’elle a subi une hausse de 400%.
En effet la Covid 19 as généraliser le télétravail, ce qui veut dire que la plupart des organisations s’ouvre à plus de cyberattaque. Et donc cela en fait le risque numéro 1 pour les organisations à l’heure actuelle, en effet 69% des cyberattaques visaient des entreprises en 2023.

Le coût moyen d’une cyberattaque pour une entreprise de taille moyenne est d’environ 775 000€ mais 6% des entreprise de taille moyenne ont dû faire face à des sinistres compris entre 3 et 10 Millions €

54 % des PME Américaine qui était victime d’une cyberattaque avait une perte moyenne d’environ 500 000€

Mais il y a aussi les coûts cacher d’un cyber attaque :

 -frais de restauration

-frais de justice

-sécurisation des données après attaque

-Amélioration des dispositifs de cybersécurité

-Perte de confiance de la clientèle

-Baisse de confiance envers l’entreprise (baisse des actions, baisses des ventes)

-Perturbation de l’activité professionnel (pire des cas l’arrêt complet)

Pour cela je vais vous parler d’un des plus gros vol de bitcoin liée à un hack mystérieux.
En 2016, Bitfinex une société d’échange de crypto monnaie a eu la bonne surprise de voir qu’un ou plusieurs(s) pirates informatique(s) s’était introduit dans leur système, et s’était fait volé 119754 bitcoins ce qui valait 72 millions $ à l’époque.
La source de se hack est encore inconnu à l’heure actuelle car Bitfiniex a cacher l’origine du hack, mais ce que l’on sait de certains rapport que [l’Organized Crime and Corruption Reporting Project](https://www.occrp.org/en) la société BitFinex n’as pas bien mis en œuvre sa sécurité numérique que Bitgo (une société partenaire en cybersécurité numérique) avait conseillé de contrôler leur finance et leur technologie.
 En 2022 quand un couple suspecter d’avoir volé ces bitcoins a été

Arrêter et prouver coupable d’un vol à 4.5 milliards $ et le FBI à saisie 3.6 milliard de $ sur un compte google drive.

Figure : image du couple qui posséder 3.6 mllrd $ de bitcoin suite au hack de bitfinex

Cet exemple n’est pas là pour montrer comment les hackeurs on fait, mais pour montrer l’importance économique que cela peut avoir.

 À l’heure actuelle il s’agit toujours du plus gros piratage de bitcoin qu’il y ai pu avoir, certes des cyberattaques au milliards $ sont rares mais les attaques peuvent couter des millions $ aussi et sont moins rares.

Cela montre l’importance économique de la cybersécurité car si BitFinex avait accordé plus d’importance à la sécurité de son réseau il n’y aurait pas eu des millions $ détourner en 2016 encore en

Circulation en 2022 qui cette fois ci se comptait en milliards $ rendez-vous compte de l’importance de l’aspect de la cybersécurité.

## Géopolitique

La cybersécurité a aussi des enjeux géopolitiques en effet une cyberattaque sur une entreprise peut se retrouver à l’échelle mondiale.

Le monde de l’informatique est très vaste et avance vite, et celui qui pense avoir le savoir absolu de l’informatique ne l’a pas, Même les grosses entreprises mondiales comme Microsoft, Alphabet, etc…

Chaque système d’information a ses failles et si un hackeur arrive à infiltrer ses failles c’est des millier/millions d’entreprises mondiales qui pourrait en être victime, puisqu’avoir un monopôle informatique c’est bien mais si celui est infiltrer alors la plupart des données des entreprises/utilisateur liées à cette grande filiale serait menacer et pourrait avoir un coût économique mondiale très Important.

Cela peut aussi avoir un impact sur un territoire/humains comme tout système informatique est faillible, alors si par exemple une Centrale nucléaire est prise pour cible l’assaillant peut couper l’électricité d’un secteur, ce qui peut avoir un très gros impact sur la population.

 On peut utiliser l’exemple des Shadow Brockers utilisant une faille de sécurité de la nsa permettant au hackeur de voler des document confidentiel dont certains parlais d’une faille informatique nommée Wannacry.
 Ce ransomware à permit d’infiltrer plusieurs centaines de milliers

D’ordinateur dans 150 pays en utilisant les versions antérieures de Windows 10 qui était obsolète, il s’agit du plus grand piratage de l’histoire.

Mais un hackeur peut hacker pour des idées politiques car oui à l’heure actuelle la politique est au cœur de notre monde, et comme tout être humain à sa propre pensée et n’est pas d’accord avec certaine politique d’entreprise/Mondiale.
 Cela peut les amener à s’introduire dans le système réseau pour faire passer ses idée ou empêcher une entreprise de travailler en faisant du chantage à cause de choix qu’elles ont fait, pour vous illustrer cela je vais vous parler d’une attaque survenu en 2014 envers Sony Universal Picture :

Un film nommée « the interview » qui racontait l’histoire de deux comédiens qui assassinait un dictateur, ce film n’a pas plus à la Corée du nord avec la forte ressemblance et voyait ça comme de la provocation de la part des Américains.

Un groupe d’hacker nommée les gardiens de la paix avait hacker les studios de Sony pour pouvoir récolter le maximum d’information sur cette entreprise, pour pouvoir la faire chanter pour qu’elle ne puisse pas sortir son film.
le groupe affirme détenir des informations personnelles sur le personnel, acteur, leak les prochains films ce qu’ils ont fait ils ont fait fuité la sortie de plusieurs films des échanges de mails sur le salaire des employer. Après cela Sony a dû refaire toute son infrastructure réseau.



Figure : Conversation confidentiel de sony aillant fuité



Figure : Conversation des salaires aillant fuité

Voici 2 captures d’écran visible à la vue de tout le monde sur internet de conversation privée de Sony diffuser par le groupe d’hackeur

## Vie privé

Il y a aussi une atteinte à la vie privée lors d’une cyberattaque, c’est pourquoi la cybersécurité est aussi important.
Une entreprise subissant une attaque informatique voit ses donner privé aux mains des pirates informatiques, en effet dans n’importe qu’elle entreprise les employé/client ont leurs informations dans les systèmes informatiques dans une organisations/entreprise donc selon certaines informations renseigner (papier d’identité, coordonné bancaire, …).
Cela peut emmener les hackeurs à diffuser leurs informations privé sur le darknet à des fins monétaire, pour que des personnes puissent usurper l’identité des victimes ou même sur le web à la vue de tous, car il y a même des personnes mal intentionné sur le web.

En Europe la vie privée des utilisateurs est très importante car il y a une loi visant à protéger les protéger les données (RGPD).
 Mais ça consiste à quoi le RGPD ? C’est un texte réglementaire européen qui encadre le traitement des données, c’est-à-dire la protection des données personnels.
 Cela veut alors dire que si on intervient sur un périphérique d’un employé on n’a pas le droit d’aller regarder ses documents, car il relève du privé et cela serait contraire au RGPD.
 Donc si un Hackeur vient à voler les données personnelles des employés ou du personnel d’une entreprise en Europe il enfreint alors aussi le RGPD pour bien comprendre cela je vais vous énumérer un exemple :

Le Centre Hospitalier de Versailles a été victime d’une cyberattaque le 3 décembre 2022.
 Les Hacker ayant fait ça ont rendu indisponible les données privé du système d’information de cet hôpital à savoir ceux des patients (Données d’Etat civil, donnée du patient, document d’identité, numéro de sécurité social,  …) et aussi du personnels (Donnée d’Etat civil, donnée professionnel, donnée relative aux horaires de travail).
 Cette attaque a eu pour conséquence un ralentissement de la prise en charge des patient, une désorganisation ce qui forçais l’hôpital à dire aux habitants qui habitaient dans le coin d’appelé le 15 avant de se rendre à l’hôpital.
Cet hôpital fait partie des 11 hôpitaux français victime de ransomware en 2022 (déclaré).



Figure : Image de l'hôpital de versaille ayant subit la cyberattaque

Dans mon exemple qui a été citée on peut voir qu’un hôpital c’est fait pirater comme de nombreux en France, mais dans un hôpital il y a énormément de donnée personnelle que ça soit des patients ou du personnel.
Et ça les cyberattaquants le savent très bien et c’est pour cela qu’ils les

Attaquent car les données privées sont précieuses et ils le savent et qu’un hôpital es susceptible de payer pour pouvoir les gardés et qu’elles ne soient pas diffusés (secret médicale).
 Ce type d’attaque arrive très fréquemment donc le vol de donnée personnel donc attaquer un hôpital est vraiment immoral car cela peut couper tout un service donc mettre en danger de vie des patients mais enfreint la loi RGPD car ils ont accès aux données privé.

#

# Les contraintes de la cybersécurité

## L’évolution

L’évolution fulgurante que connaît le monde informatique ces dernières années restent une grande avancée mais c’est aussi une contrainte importante en cybersécurité.
 Plus l’informatique avance plus les techniques pour sécuriser son entreprise évolue aussi, donc cela veut dire que ceux qui s’occupe de la sécurité d’une entreprise doivent se former en permanence sur les nouvelles technologie et comment les sécuriser.
 Car avoir un système de cybersécurité obsolète laisse une grande porte d’entrée au assaillant voulant rentrer dans le réseaux, puisqu’un système non mise à jours où mal sécuriser laisse des faille informatique importante.
 Et pour des entreprises aillant des données confidentielles c’est ce mettre une balle une pied, Pour cela que les S.O.C doivent se former en permanence en passant des certification en cybersécurité, et cela peut en effet avoir un certains coût à l’entreprise (de 810 euros à 10 000euros) si c’est elle qui le finance donc il y a aussi un aspect financier avec l’évolution qui ne cesse croitre en informatique.
 Un soc est une personne qui se focalise sur la protection des données, il est là pour protéger et avertir des menaces externes qui cible le réseau il est donc un atout majeur à la protection du réseau de l’entreprises.
 On peut remarquer l’évolution informatique de ses dernière année avec les arriver technologique qui arrive par exemple l’IA il y a encore pas si longtemps cela paraissait de la science-fiction mais aujourd’hui elle est bien réel, avec l’arrivé de ChatGPT et tout autre sorte d’IA.
 En effet l’IA peut faire des choses que l’on imaginait pas par exemple faire des musiques avec la voix d’artiste différent de la musique original, créer des images et bien plus et cela peut faire peur car si une IA est aussi puissant que ça est-ce un problème pour la sécurité des entreprises
 entre les mains de personne malveillante ? Ou alors justement cela peut-il permettre d’aider une entreprise à bien sécuriser son réseau ? tant de question qui peuvent être posé avec le futur de l’évolution informatique.

## Financier

Il n’y a pas que les cyberattaques qui ont un coût financier à une entreprise mais le fait de sécurisé son entreprise a aussi un très gros coût financier.
 Puisqu’en plus des employés il faut aussi compter le coûts matériel, avoir du bon matériel informatique sert aussi à bien sécuriser son entreprise et à minimiser les failles informatiques donc retirer des portes d’entré au pirate informatique, avec du matériel informatique obsolète cela veut dire qu’il n’ont plus accès au mise à jour récente ce qui est très important car les outils informatiques mis à jours ont eu des corrections sur des failles qui ont été repéré et corriger avant que le pire arrive.
 Mais il n’y pas que le matérielle qui a un coût il y a aussi ceux qui gèrent la cybersécurité, les S.O.C (Security Operation Center) puisque bien sûr ce n’est pas gratuit d’en avoir dans son entreprise et cela rajoute un coût en plus puisque en moyenne un S.O.C en début de carrière est généralement rémunérer entre 2900 euros et 3 700 euros par mois (ce salaire peut varier selon la taille de l’entreprise, la région où il se trouve,…).
Il n’y a pas que les S.O.C il y a aussi les hackeurs étiques effectivement ils servent aussi à la cybersécurité d’une entreprise puisqu’ils servent à découvrir les failles d’un réseau une fois que le technicien réseaux à monter son infrastructure réseaux, donc cela rajoute un autre coût financier à l’entreprise.
 Tous les moyens sont bons pour protéger son entreprise, mais cela a aussi un coût donc pour sécuriser ce n’est pas gratuit comme j’ai pu le dire ;
 Monter son entreprise c’est aussi prévoir le cout budgétaire de la sécurité de l’entreprise car on pourrait penser *«  je viens de lancer mon entreprise donc personne voudra me pirater* » mais au contraire comme on a pu le voir plus tôt personne n’est à l’abris de voir son entreprise hacker.
C’est pour ça que

faire de la prévention aux entreprise sur cet aspect est très important, beaucoup de grosse cyberattaque sont liée à une mauvaise prévention et prise en charge de la sécurité du réseaux d’une entreprise.
 On peut réutiliser l’exemple de wannacry qui aurait pu être évité si les entreprises avait mis à jour leur périphérique (système d’exploitation de leurs ordinateurs), mais aussi avec BitFinex qui n’avait pas pris au sérieux leur sécurité ce qui a valu au plus gros vol de bitcoin qui a été fait.
 Donc même si l’aspect financier peut paraitre une corvée il permet d’éviter de perdre encore plus d’argent voire même la faillite de l’entreprise. Donc posez-vous la question : « *Je préfère monter un réseau bien sécuriser quitte à payer cher ou faire le minimum mais perdre plus que si je subit une cyber attaque ?* »

## La détection d’une attaque

On pourrait penser qu’une cyberattaque est facilement détectable alors que non, avant qu’une attaque soit détecté les cybers attaquants sont déjà sur le réseau et depuis plus longtemps que l’on ne le pense.
 Et c’est pour cela que nous allons voir ce qui précède la découverte d’une attaque.



Voici les 7 étapes d’une cyberattaque que nous allons détailler :

* **Enquêter**: cette étape consiste aux attaquants d’obtenir un maximum d’information sur leur cible car toute informations est bonne à prendre pour pouvoir s’infiltrer dans le réseau de leurs victimes
* **Outiller :** S’outiller est l’étape où les attaquants recherchent la meilleure manière de pouvoir s’introduire dans le réseau et là conçoivent alors
* **Déployer :**  Une fois que la manière dont l’attaque aura lieu il faut maintenant la déployer et attendre que la/les victime(s) mord(ent) à l’hameçon.
* **Exploiter :**  Une fois l’attaque déployée, à cette étape le cyber attaquant exploite les failles dans le réseau et essaye d’arriver aux postes les plus importants (admin réseaux)
* **Contrôler :**  Une fois le logiciel malveillant bien implanter dans le réseau les hackeurs prennent le contrôle d’un périphérique
* **Exécuter :** L’hackeur exécute alors son plan initial pour récupérer les données qui l’intéresse
* **Maintenir :** L’hackeur essaye de rester dans le réseau malgré la découverte des intru et continuer à exécuter leur plan

On a pu voir les différentes phases d’une cyberattaque mais on peut se demander quand est-ce que l’attaque est donc détecter ?
 Au risque de vous surprendre une attaque est souvent détecter à la 6èmes phases (exécuter), cela veut dire les cyber assaillant ont eu le temps de récupérer des données et infiltrer le réseau sans que personnes n’est pu s’en rendre compte, cela peut faire peur.
 car ce dire que pendant que l’on est entrain de travaillé peut-être il y a des hackeurs sur le réseau qui voit ce que l’on fait qui ont pris nos données les plus importante sans rien voir et sans rien pouvoir faire.
 Cela est un vrai inconvénient car ça pourrait nous amenez à nous demander à quoi ça sert d’avoir quelqu’un qui surveille nôtre réseau sans qu’il puisse remarqué les pirates plus tôt.
Il y a une méthode qui peut servir à savoir si quelqu’un de malveillant est en train de nous pirater c’est en regardant les logs mais ont se situe quand même à la 4ème phases donc il peut se passer quand même des choses c’est pour cela qu’avoir un bon système informatique mis à jour et de la prévention est très important.

On peut réutiliser l’exemple du hack de Sony car comme c’est une grosse entreprise elle peut parler à beaucoup de personne avant que le hack soit Découvert.
 Les hackeurs étaient dans le réseau pendant plusieurs mois avant de passer à l’action, et pourtant on ne parle pas d’une petite entreprise mais d’une très grosse avec du matériel sécuriser donc qu’on le veuille ou non une attaque est très difficile à détecter avant que les hackeur exécutent leurs plan.

# Bilan

## Bilan des enjeux

On a pu qu’il y a 3 grand enjeux majeurs à la cybersécurité :
 Economique, géopolitique et sur la vie privée.
 Il ne faut pas négliger ses enjeux car ils sont très importants au niveau d’une entreprise, mais aussi au niveau d’un pays car comme on a pu le voir une mauvaise faille informatique peut impacter Plusieurs entreprises dans plusieurs pays différent (Wannacry) et bloqué plusieurs entreprises ce qui touche aussi à l’économie.
 L’économie est le nerf de la guerre d’une entreprise car une perte d’argent peut faire couler une entreprise, devoir licencier du personnel dans les petites PME/TPE pour pouvoir essayer de garder son entreprise en vie ou alors cela peut aussi faire baisser les actions d’une entreprise.
 Mais la vie privée est toute aussi importante que le reste car des informations privées devenu publique peut amener à beaucoup plus de problème que l’on peut penser c’est-à-dire usurpation d’identité, vol de coordonnée bancaire, etc.
Une atteinte à la vie privée sur internet est une violation de la RGPD comme nous avons pu le voir

## Bilan des contraintes

Malgré l’utilité de la cybersécurité en entreprise il y a des contraintes.
 Comme la détection tardive d’une attaque sur un réseau comme on a pu le voir le temps que l’attaque soit détectée un hackeur a déjà pris beaucoup d’information, et est déjà bien implanté dans le réseau mais il n’y pas que

Ça.
 il y a aussi la question financière, en effet avoir un système d’information sécuriser a un coût que ça soit matériel que humain, car il faut des personnes expérimenter pour pouvoir sécuriser un système dans son ensemble et cela a un prix.
 Il y a aussi l’évolution technologique qui est une contrainte car avec l’évolution certes les systèmes sont de plus en plus expérimentés mais comme on a pu le voir tout système est faillible et à chaque avancé une faille peut être découverte par des personnes malveillante avant même qu’elle puisse être mise à jour.

## Bilan général

L’importance de la sécurité des systèmes d’informations est de plus en plus importante à l’heure actuelle, car énormément d’hackeur prennent pour cible les entreprises comme tout maintenant se fait en ligne et tout est stocker dans des serveurs.
 Et ils savent que tout système est faillible soit une erreur humaine (phishing) ou alors une faille informatique qui permet de rentrer dans le réseau donc pour eux c’est un vrai bisness de les prendre pour cible car ils savent qu’ils peuvent toucher bien plus qu’en travaillant ou alors pour des idéologie politique ils peuvent pirater donc personnes n’en n’est à l’abris.

# Bibliographie

<https://openclassrooms.com/fr/courses/2100086-decouvrez-le-monde-des-systemes-dinformation/5195891-identifiez-les-4-fonctions-du-systeme-d-information>

<https://itsocial.fr/enjeux-it/enjeux-infrastructure/datacenter/quest-systeme-dinformation-5-meilleurs-articles-systeme-dinformation/>

<https://rendre-notre-monde-plus-sur.goron.fr/zoom-sur-5-types-de-cyberattaques/>

<https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/cyberattaques-des-donnees-relatives-a-thales-publiees-sur-le-dark-web_5470773.html>

<https://www.francebleu.fr/infos/faits-divers-justice/cybersecurite-vise-par-un-groupe-de-hackers-thales-ouvre-une-enquete-interne-sur-le-vol-de-donnees-1667306863>

<https://www.netexplorer.fr/blog/les-10-cyberattaques-qui-ont-marque-la-france-en-2022/>

<https://www.20minutes.fr/by-the-web/4013317-20221205-yvelines-sait-cyberattaque-contre-hopital-versailles>

<https://www.ch-versailles.fr/0/1/34/49>

<https://www.sfrbusiness.fr/room/securite/cybersecurite-5-plus-grandes-cyberattaques.html>

<https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/cybersecurite-l-agence-nationale-de-la-securite-des-systemes-d-information-a-compte-a-peu-pres-2-000-cyberattaques-en-2022-en-france_5943899.html>

<https://3dvf.com/actualite-11671-sony-pictures-pirates-annoncent-attentats.html/>

<https://www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/cybersecurite/autopsie-dune-cyberattaque-par>

<https://fr.linkedin.com/pulse/cybercriminalit%C3%A9-chiffres-cl%C3%A9s-%C3%A0-connaitre-en-2023-cyber-cover-fr>

[Internal Report Suggests Security Lapses at Hacked Crypto Exchange Bitfinex | WIRED](https://www.wired.com/story/security-lapses-at-hacked-crypto-exchange-bitfinex/#:~:text=The%20Ledger%20Lab%20investigation%20found,to%20manipulate%20Bitfinex%27s%20operating%20system.)

[Ponemon Library | Ponemon Institute](https://www.ponemon.org/research/ponemon-library/ponemon-library.html?keywords=cyber+attack)

[Cisco | LinkedIn](https://fr.linkedin.com/company/cisco)

[Plongez au cœur d’une cyberattaque - Découvrez l'univers de la cybersécurité - OpenClassrooms](https://openclassrooms.com/fr/courses/8028761-decouvrez-lunivers-de-la-cybersecurite/8187986-plongez-au-coeur-d-une-cyberattaque)

[Utilisez la matrice ATT&CK pour définir des scénarios d'attaque - Optimisez la sécurité informatique grâce au monitoring - OpenClassrooms](https://openclassrooms.com/fr/courses/1750566-optimisez-la-securite-informatique-grace-au-monitoring/7145826-utilisez-la-matrice-att-ck-pour-definir-des-scenarios-dattaque)

[LE COUPLE MILLIARDAIRE DU CYBERCRIME (youtube.com)](https://www.youtube.com/watch?v=IqiNyBgVZ6o)

[SHADOWBROKERS : HACKER LA NSA (youtube.com)](https://www.youtube.com/watch?v=tYi972SBFgw)

[LAZARUS : LES HACKERS DE LA CORÉE DU NORD (youtube.com)](https://www.youtube.com/watch?v=XYgM9jSkYAM)

# Glossaire

Flux : Grande abondance de choses

Leak : Fuite de donnée

Faillible : être sujet à se tromper

Faille : Point faible

Pirate/hackeur : personne s’infiltrant sur le réseau qu’ils soient bien ou mal intentionné

Cyberattaque : attaque se produisant sur le réseau informatique

Bitcoin : monnaie virtuelle

RGPD : Règlement général sur la protection des données

Données : Élément qui sert de base à un raisonnement

PME : entreprise de moins de 500 employés

TPE : entreprise de moins de 20 employés

# Table des illustrations

[Figure 1 : Schéma d'une base de données 5](file:///E%3A%5Cveille%20th%C3%A9matique%5CVeille%20th%C3%A9matique%20%201%201.docx#_Toc159342573)

[Figure 2 : Schéma d'un fichier 5](file:///E%3A%5Cveille%20th%C3%A9matique%5CVeille%20th%C3%A9matique%20%201%201.docx#_Toc159342574)

[Figure 3: image du couple qui posséder 3.6 mllrd $ de bitcoin suite au hack de bitfinex 11](file:///E%3A%5Cveille%20th%C3%A9matique%5CVeille%20th%C3%A9matique%20%201%201.docx#_Toc159342575)

[Figure 4: Conversation confidentiel de sony aillant fuité 14](file:///E%3A%5Cveille%20th%C3%A9matique%5CVeille%20th%C3%A9matique%20%201%201.docx#_Toc159342576)

[Figure 5 : Conversation des salaires aillant fuité 14](file:///E%3A%5Cveille%20th%C3%A9matique%5CVeille%20th%C3%A9matique%20%201%201.docx#_Toc159342577)

[Figure 6 : Image de l'hôpital de versaille ayant subit la cyberattaque 16](file:///E%3A%5Cveille%20th%C3%A9matique%5CVeille%20th%C3%A9matique%20%201%201.docx#_Toc159342578)