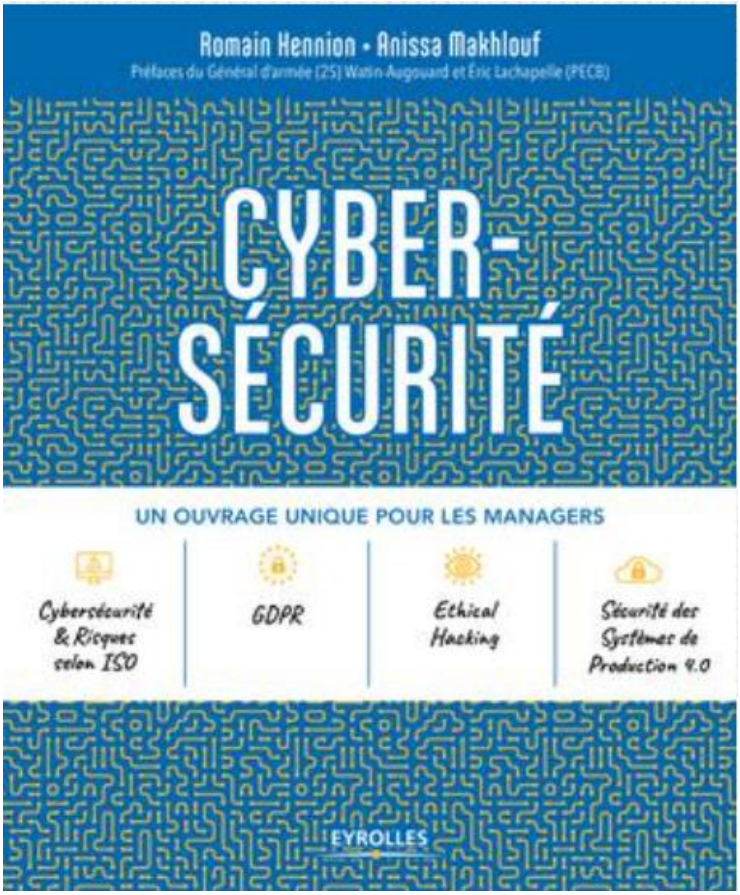


Author(s): Hennion, Romain • Makhlouf, Anissa

Publisher: Eyrolles

Pub. Date: 2018

pages: 426

Language: French

ISBN: 978-2-212-56893-6

eISBN: 978-2-212-30864-8

Edition: 1

LI : 2ème

Étudiant : Zotrim Uka

Compétence : B3

# Table des matières

# Table des illustrations

## Préambule

Ce résumé est basé sur le livre "Cybersécurité" écrit par Romain Hennion et Anissa Makhlouf. Les informations présentées dans ce document sont tirées de leur ouvrage, qui offre une exploration approfondie des principes fondamentaux et des défis contemporains liés à la cybersécurité. L'objectif de ce résumé est de fournir une vue d'ensemble condensée et accessible des sujets abordés dans le livre, en offrant aux lecteurs un aperçu des aspects essentiels de la cybersécurité.

# 1. Introduction

L'objectif central de ce livre est d'explorer les aspects fondamentaux du "comment" et du "pourquoi" de la mise en place de contrôles de sécurité dans le contexte de la cybersécurité. La dynamique de la cybersécurité s'est profondément modifiée avec l'avènement du Règlement Général sur la Protection des Données (RGPD) de l'Union Européenne, un ensemble de réglementations qui doit être respecté par toutes les organisations à partir de 2018. Ce cadre légal a fait évoluer la cybersécurité vers un domaine avec une perspective juridique plus marquée, gérable du point de vue organisationnel, notamment grâce à l'incorporation des normes ISO 27000.

La cybersécurité est un domaine extrêmement diversifié, faisant appel à un large éventail de disciplines, tant scientifiques qu'humaines. D'un côté, il sollicite des compétences scientifiques, telles que la conception d'algorithmes de chiffrement pour protéger les données sensibles. D'un autre côté, il englobe des aspects humains, comme les attaques basées sur l'ingénierie sociale, qui exploitent la crédulité des individus pour accéder à leurs informations.

Afin de concevoir et de mettre en œuvre une démarche de cybersécurité efficace, il est possible de s'appuyer sur une approche scientifique. Cette démarche scientifique repose sur cinq éléments fondamentaux : la formulation de la question appropriée, l'établissement d'hypothèses, la création de prédictions, la réalisation d'expériences pour tester ces prédictions de manière empirique, et enfin, l'analyse des résultats. C'est ce socle scientifique qui sous-tend la conception de l'ensemble des méthodes et des normes abordées dans ce livre.

Il est essentiel que les expériences menées dans le domaine de la cybersécurité répondent à des critères rigoureux tels que l'objectivité, la falsifiabilité, la reproductibilité, la prévisibilité et la vérifiabilité. Cette approche scientifique est au cœur de la gestion et de la compréhension de la cybersécurité, et elle sera explorée en profondeur tout au long de cet ouvrage.

Ainsi, ce livre offre une base solide pour la compréhension des principes fondamentaux de la cybersécurité, tout en mettant en évidence l'importance cruciale de la conformité aux réglementations légales et des normes internationales pour une protection efficace des données et des systèmes dans notre monde de plus en plus connecté.

# 2. De la sécurité à la cyber-sécurité

Le premier chapitre de l'ouvrage examine l'importance cruciale de la sécurité de l'information pour les entreprises, qu'elles soient petites ou grandes, publiques ou privées. Il introduit le concept de sécurité de l'information et évoque sa gestion dans les organisations connectées à des systèmes informatiques, préparant ainsi le terrain pour la transition vers la cybersécurité. Le chapitre définit la valeur de l'information dans les organisations modernes, met en avant les piliers fondamentaux de la cybersécurité (confidentialité, intégrité et disponibilité), et souligne les défis inhérents au partage d'informations de grande valeur. Ces concepts posent les bases essentielles pour une compréhension approfondie des enjeux liés à la sécurité de l'information et à la cybersécurité dans un monde interconnecté.

## 2.1 Le contexte

Ce chapitre met en évidence les inquiétudes majeures liées à la cybersécurité. Il souligne que, quotidiennement, des entreprises de toutes tailles et natures sont victimes de piratages, ce qui entraîne la diffusion ou la vente de données sensibles. Les statistiques mettent en lumière des coûts considérables, la création quotidienne de quantités massives de malwares, ainsi que l'ampleur des cybercriminels recherchés par le FBI. Les réseaux sociaux, en raison du partage massif de données personnelles, sont particulièrement vulnérables. Le chapitre expose également les principales méthodes d'attaque :

### *Les réseaux sociaux en ligne de mire*

- Le **like-jacking** consiste à incorporer un faux bouton "J'aime" sur une page web, déclenchant un malware ou un virus lorsqu'il est activé.
- Le **link-jacking** implique la création d'un faux lien vers une page web existante, comme Facebook, redirigeant vers un virus ou tout autre malware.
- Le **phishing** vise à obtenir d'une manière ou d'une autre des informations sensibles, telles que les mots de passe ou les numéros de cartes de crédit.
- Le **social spam** comprend la propagation sur les réseaux sociaux de discours haineux, insultants ou diffamatoires dirigés contre des individus ou des organisations.

### *Les traîtres sont parmi nous !*

Le chapitre met également en évidence les acteurs internes de l'entreprise impliqués dans les attaques. Il révèle que 45 % des attaques proviennent de concurrents, 31,5 % sont le fait d'employés malveillants à la suite d'un licenciement ou d'une démission, et 23,5 % résultent d'erreurs commises par des employés étourdis. Par conséquent, plus de la moitié des vols ou pertes d'informations confidentielles surviennent au sein de l'entreprise. Les menaces internes incluent :

- Le **Malicious insider**, un employé disposant de droits d'accès élevés, comme un administrateur système ou un directeur financier, qui vole des informations sensibles en se connectant au compte d'une tierce personne.
- L'**Exploited insider**, un employé trompé par une personne externe ayant obtenu ses identifiants pour se connecter.
- Le **Careless insider**, un employé commettant des erreurs involontaires, telles qu'une suppression ou une modification accidentelle d'informations critiques, représentant près d'un quart des pertes de données.

Malgré la multiplication des attaques, de nombreuses entreprises et PME restent mal préparées pour se défendre. En 2017, la diffusion de ransomwares a marqué les esprits. Les prochains chapitres exploreront diverses techniques de piratage, la plus courante étant le **social engineering**. Cette technique vise à extorquer des informations aux victimes sans utiliser de logiciels ou de compétences particulières. Elle repose sur quatre grandes méthodes : le téléphone, le courrier électronique, Internet et le contact direct. Par exemple, les pirates envoient des e-mails trompeurs se faisant passer pour une promotion bancaire, incitant les destinataires à cliquer sur un lien. Une fois redirigés sur un site Web imitant la banque, les victimes se connectent avec leurs identifiants, ignorant qu'il s'agit d'une arnaque. Le chapitre souligne l'importance de rester vigilant face à de telles attaques, illustrant cela avec un exemple personnel où une tentative d'arnaque par e-mail a failli réussir.

## 2.2 Qu’est-ce que la sécurité de l’information et comment l’aborder ?

La sécurité de l'information vise à protéger la confidentialité, l'intégrité et la disponibilité des données, avec d'autres aspects tels que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité qui peuvent être pertinents. Pour assurer cette protection, des compétences et

des connaissances spécifiques sont nécessaires, car notre dépendance croissante envers les systèmes d'information interconnectés accroît l'importance de la sécurité de l'information.

### *Pourquoi la sécurité dans l'information ?*

Les conséquences d'une brèche de sécurité de l'information comprennent :

- Indisponibilité du système d'information.
- Création d'une image négative et de publicités indésirables pour l'organisation.
- Risques de fraude, vol et corruption des données.
- Espionnage des individus travaillant pour l'organisation.
- Risques d'espionnage industriel et de vol de brevets.

La sécurité informatique a traditionnellement été gérée par des informaticiens et repose sur des outils et des logiciels technologiques avancés. Cependant, elle évolue désormais vers la sécurité des systèmes d'information, ce qui nécessite une approche plus holistique incluant le bon sens et la gestion. En parallèle, l'évaluation et la compréhension des risques au sein de l'organisation jouent un rôle essentiel dans l'établissement d'une gestion des risques appropriée pour assurer la sécurité de l'information.

Les trois composantes essentielles de la sécurité de l'information comprennent :

1. Une dimension humaine, visant à sensibiliser les acteurs de l'organisation aux enjeux de la confidentialité des informations.
2. Une approche organisationnelle, reconnaissant que la sécurité ne se limite pas aux outils et technologies informatiques, mais concerne l'ensemble de l'entreprise.
3. Une gestion des risques appropriée, qui est indispensable pour assurer la gestion des incidents de sécurité et garantir la continuité des opérations en cas de perturbation majeure des services et du système d'information.

### *Comment protéger l'information ?*

Pour une gestion optimale de la sécurité de l'information au sein des organisations, il est essentiel de combiner les mesures suivantes :

1. Adopter une approche pragmatique des politiques et des standards de sécurité.
2. Mettre en place un processus d'évaluation des risques qui permet de classer les risques (informatiques, humains, industriels), d'évaluer leur probabilité, leurs

conséquences et leur impact sur la confidentialité, l'intégrité et la disponibilité des informations.

3. Élaborer des politiques de sécurité qui s'appliquent à l'ensemble de l'organisation, pas seulement au domaine informatique.
4. Sensibiliser et former les acteurs et le personnel à la sécurité de l'information, établissant ainsi une culture de la vigilance pour savoir comment réagir en cas de besoin.

### *L'apport de la famille ISO 27000*

Les normes ISO 27 000 se concentrent sur la mise en place d'un système de management de la sécurité de l'information (SMSI). Ce système vise à protéger les actifs informationnels en établissant, mettant en œuvre, surveillant, évaluant, révisant et améliorant la sécurité de l'information. Il repose sur l'appréciation des risques et les niveaux d'acceptation des risques définis par l'organisation.

La gestion des risques est un élément clé de la sécurité de l'information, impliquant l'identification, l'évaluation et le traitement des menaces potentielles. La famille de normes ISO 27000 comprend plusieurs documents, dont les principaux sont :

- ISO/CEI 27001 : Norme d'exigences des systèmes de management de la sécurité de l'information, utilisée pour la certification des organisations.
- ISO/CEI 27002 : Guide des bonnes pratiques en SMSI, fournissant des directives sur "comment faire".
- ISO/CEI 27003 : Guide d'implémentation d'un SMSI, avec des lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information.
- ISO/CEI 27004 : Norme de mesures de management de la sécurité de l'information.
- ISO/CEI 27005 : Norme de gestion des risques liés à la sécurité de l'information.

La série ISO 27000 propose également d'autres normes complémentaires pour traiter divers aspects de la sécurité de l'information, y compris la gestion de la sécurité des communications intersectorielles et interorganisationnelles (ISO/CEI 27010).

## 2.3 Les profils et les motivations des pirates

L'histoire des hackers débute avec des ingénieurs et programmeurs qui ont initialement contribué à améliorer la productivité de l'informatique. Cependant, à partir des années 1980, le piratage informatique est devenu une pratique plus répandue. De nos jours, il existe diverses catégories de pirates informatiques avec des motivations économiques ou politiques très différentes.

### *Une petite histoire du hacking*

Le hacking a une histoire de plus d'un siècle, remontant à l'époque des adolescents qui ont détourné les routeurs téléphoniques en 1876 et John Draper (Captain Crunch) qui a découvert comment faire des appels gratuits en 1971. Initialement, le terme "hacker" n'avait pas de connotations négatives, car il était associé à l'amélioration de la productivité informatique. Cependant, dans les années 1980, certains hackers ont commencé à utiliser leurs compétences à des fins criminelles pour gagner de l'argent.

### *Les motivations et compétences des hackers*

Les hackers varient dans leurs compétences techniques et motivations. Certains cherchent le gain financier en travaillant de manière indépendante, tandis que d'autres offrent leurs talents aux gouvernements ou à des associations. Il existe neuf profils de hackers différents.

1. **Wannabe (ou Lamer)** : Généralement un enfant ou un adolescent, il expérimente le piratage par curiosité, souvent sans comprendre les conséquences.
2. **Script Kiddie** : Utilise des scripts pré-écrits par d'autres car il manque de compétences techniques pour les créer lui-même.
3. **Cracker** : Désire se distinguer des hackers à connotation négative et cherche à montrer les failles de sécurité, mais n'est généralement pas motivé par le gain.
4. **Ethical Hacker** : Possède d'excellentes compétences techniques et les met au service de la communauté en découvrant et signalant les vulnérabilités.
5. **Quiet Paranoid Skilled Hacker (QPS)** : Dispose d'excellentes compétences techniques, crée ses propres systèmes de piratage, et minimise les traces laissées.
6. **Cyber-Warrior, mercenaire** : Se considère comme un héros dans un groupe extrémiste, peut avoir des compétences techniques variées et est rémunéré pour des attaques ciblées.

7. **Industrial Spy Hacker** : Pratique l'espionnage industriel en infiltrant des entreprises, recherchant des informations confidentielles.
8. **Government Agent Hacker** : Recruté par les agences gouvernementales, il participe à des enquêtes sur des attaques informatiques, récupérant des preuves pour les procédures judiciaires.
9. **Military Hacker** : Les détails sur ce profil sont rares, mais les agences militaires emploient des espions informatiques pour des activités liées à la sécurité nationale.

Les hackers se divisent en deux catégories principales :

1. **White Hat Hackers (Pirates au chapeau blanc)** : Ce sont les "gentils". Ils sont des experts en sécurité informatique spécialisés dans les tests d'entrée et autres méthodes pour garantir la protection des systèmes d'information. Ils utilisent un arsenal technologique complexe et se réunissent dans des compétitions de hackers pour améliorer leurs compétences.
2. **Black Hat Hackers (Pirates au chapeau noir)** : Ce sont les "méchants". Ils pénètrent illégalement les réseaux informatiques, créent des virus et ont des motivations variées, que ce soit pour des convictions politiques, des gains financiers en volant des informations confidentielles, ou pour attaquer les banques et effectuer des transferts de fonds frauduleux.

### *Une évolution permanente de leurs compétences*

Nous pouvons classer les pirates informatiques en cinq catégories en fonction de la sophistication de leurs attaques et des ressources à leur disposition :

- Récréatif :
  - Notoriété
  - Ressources techniques limitées
  - Exploite des failles déjà connues
- Criminel :
  - Vandalisme
  - Connaissances techniques limitées

- Hacktiviste :
    - Motivé par des convictions, souvent affilié à un groupe
    - Possède de nombreuses connaissances
    - Cible des entités en accord avec ses convictions
- Crime Organisé :
    - Profit financier
    - Maîtrise des compétences techniques avancées
    - Dispose de nombreuses ressources
- Hacking Gouvernemental :
    - Cyber-guerre, espionnage industriel, secrets d'État
    - Utilise probablement les meilleurs experts
    - Mène des attaques très sophistiquées
    - Dispose de ressources quasi illimitées

## 2.4 Le cyberspace

La cybersécurité englobe les technologies, processus et pratiques visant à protéger les réseaux, ordinateurs, logiciels et données contre les attaques et les accès non autorisés. Elle est essentielle en raison de notre dépendance croissante vis-à-vis de la technologie et des objets connectés, malgré la vulnérabilité de ces systèmes. Pour mieux comprendre la cybersécurité, explorons le monde numérique, le cyberespace.

### *Que signifie réellement « cyber » ?*

Le terme "cyber" vient du mot grec "κυβερεων" (kybereo), signifiant "contrôler". Cela a été utilisé pour décrire les systèmes contrôlés par des ordinateurs par le mathématicien Norbert Wiener dans les années 1940. La cybernétique s'applique aux machines et organismes vivants dont le fonctionnement peut être modélisé et prédit, mais elle concerne principalement des systèmes clos qui n'interagissent pas avec leur environnement.

Le préfixe "cyber" est souvent lié aux ordinateurs et aux robots. William Gibson a introduit le terme "cyberespace" dans son roman "Neuromancer", décrivant un réseau informatique mondial en 3D. Il est couramment utilisé dans la science-fiction pour décrire un espace numérique où les utilisateurs interagissent sous forme d'avatars.

De nombreux pays intègrent le cyberespace et la cybersécurité dans leurs stratégies.

Allemagne : Le cyberespace englobe tous les systèmes informatiques connectés au niveau des données à l'échelle mondiale, avec Internet comme moyen de connexion publiquement accessible, ainsi que d'autres réseaux de données. Il inclut toutes les infrastructures d'information au-delà des frontières du pays.

Australie : La sécurité nationale, la prospérité économique et le bien-être social dépendent fortement de la disponibilité, de l'intégrité et de la confidentialité des technologies de communication et d'information, y compris les ordinateurs, Internet, les appareils de communication mobiles et d'autres systèmes informatiques et réseaux.

France : La définition officielle du cyberespace par le gouvernement français n'est pas précisée, mais selon le Petit Robert, il s'agit d'un ensemble de données numérisées liées à l'interconnexion mondiale des ordinateurs, constituant un univers d'informations et un milieu de communication.

Royaume-Uni : Le cyberespace englobe les réseaux numériques utilisés pour stocker, modifier et communiquer des informations, y compris Internet et d'autres systèmes d'information qui soutiennent le commerce, les infrastructures et les services.

La cybersécurité est devenue essentielle pour tous les pays, en raison de la nécessité de protéger les secrets gouvernementaux, de défendre la nation et de sécuriser les infrastructures critiques à l'ère du 21e siècle. Les cyberattaques menacent les nations, car la société numérique présente des vulnérabilités qui génèrent des risques en termes de sécurité pour la communauté, les individus et la continuité des fonctions vitales de la société.

Un exemple marquant est survenu en mai 2017, lorsque près de cent pays, des entreprises, des gouvernements et des services publics ont été touchés par une cyberattaque internationale sans précédent. Cette attaque a affecté le service de santé britannique et le gouvernement français, notamment à travers l'entreprise automobile Renault, et leur a demandé plusieurs jours pour s'en remettre.

### *Les 5 couches du cyberspace*

Le modèle de cyberespace de Martin C. Libicki se compose de cinq couches :

- **Couche cognitive** : Cette couche englobe la perception et l'interprétation des informations par les utilisateurs en fonction de leur environnement. Les émotions et les facteurs contextuels, tels que la confiance et l'acceptation, influencent l'interprétation des données.
- **Couche de service** : Ici, se trouvent les services publics et commerciaux accessibles aux utilisateurs via Internet. Cela comprend des services opérationnels tels que les services bancaires et les médias comme YouTube.
- **Couche sémantique** : Au cœur du réseau, cette couche stocke les informations et les bases de données sur les serveurs et les ordinateurs. Elle gère également les fonctions administratives au niveau de l'utilisateur.
- **Couche syntaxique** : Cette couche englobe les programmes et les fonctions de gestion et de contrôle des systèmes, ainsi que les protocoles de réseau, la correction d'erreurs, etc.
- **Couche physique** : La couche physique comprend les éléments matériels des réseaux de communication, y compris les appareils de réseau, les routeurs, les commutateurs, et les connexions câblées ou sans fil.

Ce modèle aide à comprendre les différentes composantes du cyberespace et comment elles interagissent.

## 2.5 Les menaces de la cyberspace

Les fonctions vitales de la société sont menacées par des attaques informatiques à l'échelle internationale. Ce chapitre se penche sur les menaces physiques, économiques et virtuelles, tandis que les prochains chapitres exploreront leur gestion, de la détection à l'évaluation et au traitement.

### *Définition*

La sécurité de l'information vise à protéger les actifs de l'entreprise, qui comprennent l'information, les logiciels, les actifs physiques, les services, le personnel, ainsi que des actifs intangibles tels que la réputation et l'image de l'entreprise. Cette protection s'articule autour de plusieurs propriétés, telles que :

- **La confidentialité** : empêcher l'accès ou la divulgation non autorisés de l'information.
- **L'intégrité** : garantir l'exactitude et l'exhaustivité des actifs.
- **La disponibilité** : assurer que les actifs sont accessibles et utilisables selon les besoins des entités autorisées.
- **L'authenticité** : s'assurer que les entités sont bien ce qu'elles prétendent être.
- **L'imputabilité** : attribuer la responsabilité des actions et décisions aux entités appropriées.
- **La non-répudiation** : être capable de prouver qu'un événement ou une action s'est produite et d'identifier les entités impliquées.
- **La fiabilité** : garantir un comportement cohérent et des résultats prévisibles.

### *Vulnérabilités et menaces : quelles relations ?*

Les vulnérabilités sont des failles dans un actif ou une mesure de sécurité qui pourraient être exploitées par diverses menaces. La gestion des vulnérabilités est complexe en raison de plusieurs facteurs :

- Les erreurs de gestion : Les vulnérabilités révèlent souvent des erreurs de gestion, ce qui peut rendre difficile leur reconnaissance, car personne n'aime admettre ses erreurs.
- Impacts négatifs ignorés : Parfois, les vulnérabilités sont associées à des conséquences négatives, mais ces impacts peuvent être négligés.
- Effets secondaires indésirables : Dans d'autres cas, les vulnérabilités sont liées à des caractéristiques positives, mais elles peuvent avoir des effets secondaires indésirables. Par exemple, la mobilité des ordinateurs portables offre une grande flexibilité, mais elle augmente également le risque de vol.

Les vulnérabilités peuvent être classées en deux catégories :

- Vulnérabilités intrinsèques : Ce sont des vulnérabilités liées aux caractéristiques inhérentes des actifs. Par exemple, un serveur ayant une capacité de traitement insuffisante.

- Vulnérabilités extrinsèques : Elles sont liées à des circonstances spécifiques entourant les actifs. Par exemple, un serveur se trouvant dans une zone inondable serait vulnérable en raison de cette caractéristique extrinsèque.

La typologie des vulnérabilités est non exhaustive et évolutive en raison des changements technologiques constants. L'annexe D de l'ISO 27005 fournit une classification des vulnérabilités à titre indicatif. Cependant, il convient de l'utiliser avec prudence, car cette liste n'est pas exhaustive et ne peut pas l'être compte tenu des nouvelles vulnérabilités qui émergent régulièrement.

| Type de vulnérabilité | Exemples |
|---|---|
| 1 Matériel informatique | Manque d'entretien |
| | Portabilité |
| 2 Logiciel | Absence d'enregistrement des registres |
| | Interfaces de saisie compliquées |
| 3 Réseau | Absence de chiffrement des transferts |
| | Point unique d'accès |
| 4 Personnel | Formation insuffisante |
| | Manque d'encadrement |
| 5 Localisation (lieu) | Système électrique instable |
| | Site en zone inondable |
| 6 Structure organisationnelle | Absence de séparation de tâches |
| | Absence de description de tâches |

*Figure 1 : Typologie des vulnérabilités selon la norme ISO 27005*

La typologie des menaces est non exhaustive et évolutive en raison de l'évolution des technologies et des capacités des agents de menace. L'annexe C de l'ISO 27005 fournit une classification des menaces à titre indicatif. Cependant, il est important de l'utiliser avec prudence, car cette liste n'est pas exhaustive et ne peut pas prétendre à l'exhaustivité compte tenu des nouvelles menaces qui émergent régulièrement.

| Type de menace | Exemple |
|---|---|
| 1. Dommage physique | Feu |
| | Dégât des eaux |
| 2. Désastre naturel | Tremblement de terre |
| | Inondation |
| 3. Perte de service essentiel | Panne de climatisation |
| | Panne électrique |
| 4. Perturbation causée par radiations | Radiations électromagnétiques |
| | Radiations thermiques |
| 5. Information compromise | Écoute électronique |
| | Vol de documents |
| 6. Pannes techniques | Bris d'équipement |
| | Saturation de réseau |
| 7. Action non autorisée | Accès non autorisé |
| | Utilisation d'un logiciel piraté |

*Figure 2 : Typologie des menaces, selon la norme ISO 27005*

## *Les menaces spécifiques du cyberespace*

L'ENISA, l'agence européenne chargée de la sécurité des réseaux et de l'information, a proposé une taxonomie des menaces spécifiques au cyberespace. Cette taxonomie comprend divers agents de menace principaux, notamment les entreprises, les cybercriminels, les employés, les hackers activistes (hacktivists), les nations et les terroristes.

Chaque menace et chaque attaque sont classées en fonction de leur niveau de sophistication

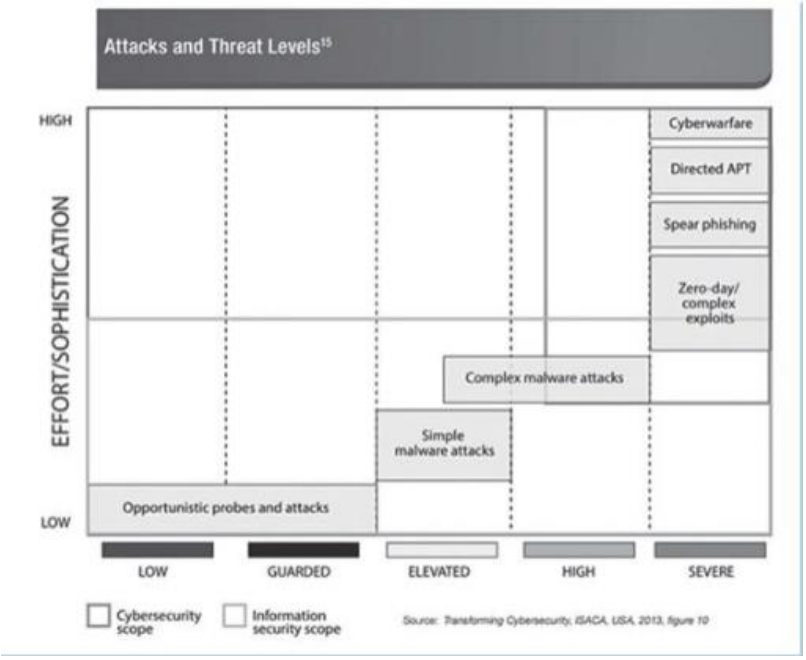


*Figure 3 : Classification des cyberattaques et menaces par leur niveau de sophistication*

## *L'approche de Cavelty*

Myriam Dunn Cavelty propose un modèle structurel en cinq couches.

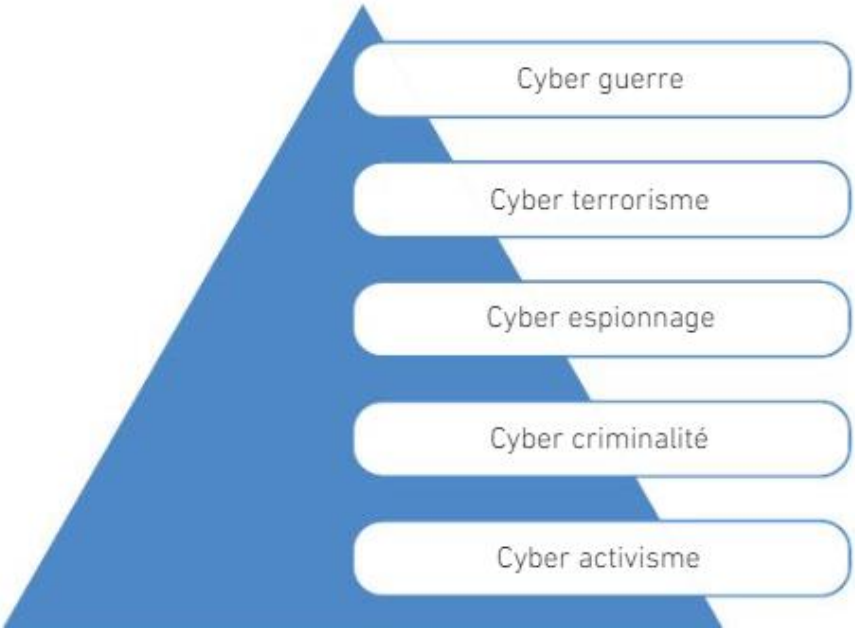


*Figure 4 : Le modèle en 5 couches de Cavelty*

Niveau 1 : Cyberactivisme - Cela englobe le cybervandalisme, le hacking, et l'hacktivisme. Ces menaces peuvent causer des dommages financiers importants aux individus ou aux entreprises.

Niveau 2 : Cybercriminalité et délits informatiques - Il s'agit d'actes criminels commis en utilisant des réseaux de communication électroniques et des systèmes d'information, ou dirigés contre ces réseaux et systèmes.

Niveau 3 : Cyberespionnage - Cette menace vise à obtenir des informations secrètes, sensibles ou privées auprès d'individus, de concurrents, de groupes, de gouvernements ou d'adversaires dans le but d'accroître le gain économique, militaire ou politique, en utilisant des moyens illicites via Internet, des réseaux, des programmes ou des ordinateurs.

Niveau 4 : Cyberterrorisme - Le cyberterrorisme utilise les réseaux de communication pour s'attaquer à des systèmes informatiques critiques, en cherchant à en prendre le contrôle. L'objectif est de causer des dommages graves, d'instaurer la peur au sein de la population et de contraindre le gouvernement à céder aux demandes des terroristes.

Niveau 5 : Cyberguerre - La cyberguerre peut être subdivisée en trois entités : la cyberguerre stratégique, la cyberguerre tactique/opérationnelle et la cyberguerre pour des conflits de faible intensité. Il n'existe pas de définition unique de la cyberguerre, mais elle implique généralement des actions menées par les gouvernements ou les nations. La cyberguerre est souvent une composante d'une guerre conventionnelle, et les menaces peuvent affecter les fonctions vitales d'une nation. Les opérations de cyberterrorisme et de cyberguerre peuvent également être menées conjointement pour causer des destructions physiques.

Chaque niveau de menace dans le cyberespace présente ses propres caractéristiques et dangers, allant des actions de protestation et de sabotage aux attaques criminelles, à l'espionnage, au terrorisme et à la guerre virtuelle.

# 3. La gestion de la sécurité et des risques au quotidien

Le terme SIM (Security Information Management) est un acronyme lié à la collecte, le suivi, et l'analyse d'incidents de sécurité liés à des informations gérées par des systèmes informatiques. Cela est automatisé par le système de management de la sécurité de l'information (SMSI), conforme aux normes ISO.

## 3.1 Les pratiques de gestion de la sécurité : cycle de vie d'un projet de sécurité, triptyque CIA

### *Projet classique ou scrum*

La principale différence entre les projets classiques (PMP ou Prince2) et les projets agiles (Scrum) réside dans leur finalité :

- Les projets classiques ont un objectif défini à l'avance, et toute la structure du projet est conçue pour l'atteindre.
- Les projets agiles n'ont pas d'objectif préétabli, car ils se concentrent sur des interactions continues entre l'équipe projet et le client. Chaque mois, l'équipe agile présente des livrables au client et des propositions à forte valeur ajoutée, qui peuvent influencer l'objectif du projet en fonction des retours du client.

Dans le contexte de la gestion de la sécurité de l'information, il est recommandé d'utiliser une structure de projet classique. La raison en est que l'objectif est clairement défini à l'avance, à savoir la mise en place d'un système de gestion de la sécurité de l'information, éventuellement en vue de l'obtention d'une certification ISO 27001 (ou autre) pour l'organisation. Une approche de projet classique offre une meilleure structuration pour atteindre cet objectif spécifique.

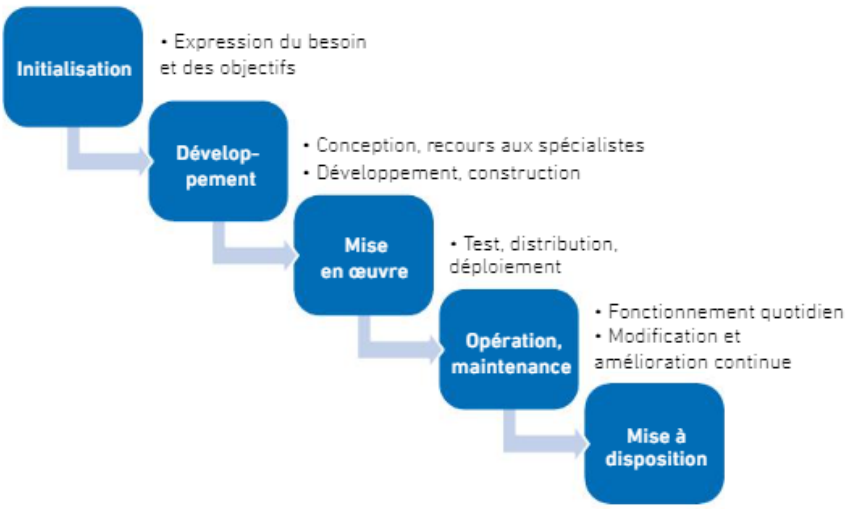


*Figure 5 : Cycle de vie d'un projet de gestion de la sécurité*

Le processus de mise en place d'un système de gestion de la sécurité de l'information peut être divisé en cinq phases clés :

1. **Phase d'initialisation** : Cette phase implique la définition des objectifs du système de gestion de la sécurité de l'information, ainsi que la documentation associée.
2. **Phase de développement/acquisition** : Au cours de cette phase, la conception du système, l'organisation des ressources, l'engagement de prestataires externes ou de spécialistes, la programmation, le développement et la construction du système sont réalisés.
3. **Phase de mise en œuvre** : Cette étape englobe les tests, l'installation et le déploiement du système de gestion de la sécurité de l'information.
4. **Phase d'opération et de maintenance** : Cette phase traite de la gestion quotidienne du système, de ses éventuelles modifications et améliorations, et de l'implémentation de matériels ou de logiciels complémentaires.
5. **Phase de mise à disposition** : Cette dernière phase concerne le transfert du système aux clients et aux parties prenantes. Elle englobe l'ensemble des processus, procédures, documentation, matériel, logiciels et bases de données associés au système.

### *Trade off analysis (TOA)*

La Trade Off Analysis (TOA) ou analyse coût/bénéfice est une démarche visant à évaluer si un projet de sécurité de l'information est justifié. Dans le contexte de la sécurité de l'information, cette analyse est essentielle car il est impossible de sécuriser tous les actifs et informations de manière exhaustive en raison des contraintes budgétaires. Le TOA permet de définir le périmètre du projet en se concentrant sur les actifs et informations les plus importants pour l'entreprise.

Le processus du TOA comprend trois étapes clés :

1. Définir l'objectif : Identifier les exigences auxquelles la solution doit répondre, généralement exprimées en termes de Mesure Of Effectiveness (MOE) pour évaluer son efficacité.

2. Identifier les alternatives : Rechercher et répertorier toutes les solutions possibles pour résoudre le problème.

3. Comparer les alternatives : Évaluer et comparer chaque solution en se basant sur des critères tels que le MOE pour déterminer laquelle est la plus appropriée.

Cette analyse permet de prendre des décisions éclairées concernant les priorités en matière de sécurité de l'information, en maximisant les bénéfices tout en respectant les contraintes budgétaires.

### *Le triptyque CIA*

La sécurité de l'information repose sur les trois concepts fondamentaux du CIA : Confidentialité, Intégrité et Disponibilité.

- **Confidentialité** : Garantit que le contenu d'un message ne soit pas divulgué de manière non autorisée, intentionnelle ou non. La perte de confidentialité peut résulter de la mise en ligne de documents confidentiels sur des serveurs mal protégés.

- **Intégrité** : Englobe la fiabilité du contenu d'un message, assurant que seules les personnes autorisées peuvent modifier le contenu ou les données de manière autorisée, et que les données internes correspondent à la réalité des données externes.

- **Disponibilité** : S'assure que l'information est fiable et accessible quand nécessaire, garantissant que le système d'information fonctionne correctement et fournit des services conformes aux engagements de disponibilité.

Ces concepts servent de base à tous les contrôles de sécurité et à la gestion des risques dans le domaine de la sécurité de l'information.

## 3.2 la classification de l'information

La classification des actifs informationnels est une étape cruciale dans la gestion des risques de sécurité de l'information. Elle vise à déterminer la criticité des actifs en fonction des trois principaux objectifs de sécurité de l'information : disponibilité, intégrité et confidentialité. Cette classification est essentielle pour évaluer les risques et attribuer à chaque actif un niveau de protection approprié en conséquence.

### *Les objectifs de la classification*

Les informations détenues par une entreprise ne sont pas toutes d'égale importance. Certaines sont essentielles pour les décisions à long terme, d'autres pour les opérations à court terme. La perte d'informations cruciales peut avoir un impact immédiat sur le chiffre d'affaires. Les données varient en sensibilité, de secrets industriels aux informations médicales. L'objectif principal est de protéger la confidentialité, l'intégrité et la disponibilité des informations tout en minimisant les risques. Cela nécessite de mettre en place des mécanismes de protection et des contrôles pour atteindre un équilibre coût/bénéfice efficace.

### *Les concepts de la classification de l'information*

Il existe cinq niveaux de classification des données du gouvernement, allant du moins sensible au plus sensible :

- **Non classé (Unclassified)** : Les informations ne sont pas sensibles et ne sont soumises à aucune classification. Leur diffusion publique ne viole pas la confidentialité.
- **SBU (Sensitive But Unclassified)** : Ces informations incluent des secrets mineurs dont la divulgation n'entraînerait que des dommages mineurs. Par exemple, des réponses à un examen ou des informations médicales.
- **Confidentiel** : La divulgation publique de ces informations peut causer quelques dommages à la sécurité nationale.

- **Secret** : Cette classification s'applique à des informations dont la divulgation non autorisée entraînerait des dommages graves à la sécurité nationale.
- **Top secret** : Les informations classées top secret sont les plus sensibles. Leur divulgation non autorisée pourrait causer des dommages irréversibles et catastrophiques à la sécurité nationale.

Dans le secteur privé, une classification des données peut être établie comme suit, allant du moins sensible au plus sensible :

- **Public** : Ces informations sont similaires aux données non classées mentionnées précédemment. Elles peuvent être mises en libre accès sur un site Web sans aucun impact sur l'entreprise.
- **Sensible** : La perte de confidentialité ou d'intégrité de ces informations pourrait causer des dommages mineurs à l'entreprise. Par exemple, un concurrent obtient des informations au cours d'un déjeuner qui lui permettent de prendre des mesures pour éliminer un concurrent et le remplacer.
- **Privé** : La perte d'informations privées causerait des dommages importants à l'entreprise. Cela peut concerner des données telles que le fichier clients, la diffusion des salaires (surtout des dirigeants), ou la divulgation d'informations médicales sur certains patients.
- **Confidentiel** : La perte d'informations confidentielles entraînerait la fermeture de l'entreprise. Ces informations sont d'une importance stratégique extrême et concernent les partenaires, les clients, les actionnaires. Par exemple, un employé règle un différend avec son ancien employeur, une banque, en divulguant la liste de toutes les personnes ayant un compte non déclaré à l'étranger.

### *Les critères de classification de l'information*

Les critères pour déterminer la classification d'une information sont les suivants :

- **La valeur** : cette valeur est associée à un nombre ou à une quantité numérique. Par exemple, il peut s'agir du prix qu'un concurrent serait prêt à payer pour obtenir ces informations.

- **L'âge** : l'âge de l'information est lié à sa pertinence. Une information récente peut être plus intéressante pour la concurrence, tandis qu'une information plus ancienne peut avoir davantage de valeur historique que d'avantage concurrentiel.
- **La durée de vie** : chaque information suit un cycle de vie documentaire, de la conception à la mise au rebut. Ce cycle est utilisé notamment dans les normes ISO. L'utilisation d'informations obsolètes peut conduire à des erreurs dans l'environnement de production.
- **L'association personnelle** : l'information est associée à des caractéristiques personnelles et confidentielles. Par exemple, il peut s'agir d'informations nominatives qui ne doivent pas sortir du cadre de l'entreprise.


*Figure 6 : Les critères de classification de l'information*

## 3.3 La gestion des risques en cybersécurité

La gestion des risques vise à réduire le risque à un niveau acceptable pour l'organisation en identifiant, analysant, contrôlant et minimisant les pertes associées aux événements à l'origine du risque. Il est important de noter que le risque zéro n'existe pas, et il est impossible d'éliminer complètement un risque sans arrêter l'activité ou le processus associé à ce risque.

### *L'objectif de l'analyse des risques*

La gestion des risques comprend l'identification, l'évaluation et le contrôle des menaces qui pèsent sur une organisation, y compris les menaces à la sécurité des systèmes d'information et aux données. Il s'agit notamment de protéger la confidentialité, l'intégrité et la disponibilité des actifs numériques, tels que les données clients et les informations personnelles. L'analyse des risques consiste à définir et analyser les dangers liés à des causes potentielles humaines et naturelles, afin d'aligner les objectifs technologiques sur les objectifs métiers de l'entreprise. Cette analyse peut être quantitative, en utilisant des probabilités numériques pour évaluer les pertes, ou qualitative, basée sur des scénarios et des mesures pour gérer le risque.

### *Quelques définitions*

**Actif (Asset)** : Il s'agit de tout ce que l'organisation a besoin de protéger, que ce soit des ressources tangibles (capital financier, infrastructure, applications, informations) ou des compétences intangibles (processus, gestion, organisation, connaissances).

**Menace (Threat)** : Une menace est tout événement potentiel qui pourrait avoir un impact sur l'organisation, que ce soit d'origine humaine ou naturelle, avec des effets pouvant aller de négligeables à très graves pour la sécurité et la viabilité de l'entreprise.

**Vulnérabilité (Vulnerability)** : Les vulnérabilités sont des faiblesses ou des failles au niveau d'un actif, ou encore l'absence de protection de cet actif. Une vulnérabilité peut permettre à une menace mineure de devenir majeure et plus fréquente.

**Protection (Safeguard)** : La protection représente les mesures ou les contrôles mis en place pour réduire le risque associé à une menace spécifique ou à un groupe de menaces.

**Facteur d'Exposition (Exposition Factor - EF)** : Le facteur d'exposition est le pourcentage de pertes potentielles qu'une menace pourrait causer à un actif spécifique. Il influence le calcul du Single Loss Expectancy (SLE) et de l'Annual Loss Expectancy (ALE).

**Single Loss Expectancy (SLE)** : Le SLE est la perte financière attendue pour une organisation en cas de réalisation d'une menace spécifique. Il est calculé en multipliant la valeur de l'actif par le facteur d'exposition.

**Taux Annuel d'Occurrence (Annual Rate of Occurrence - ARO)** : L'ARO exprime la fréquence estimée à laquelle une menace est susceptible de se produire, allant de zéro (menace jamais réalisée) à des valeurs plus élevées, basée sur l'historique et l'expérience.

**Prévision de Perte Annuelle (Annualized Loss Expectancy - ALE)** : L'ALE est une valeur monétaire qui représente la perte financière attendue sur une année pour une organisation en raison d'une menace. Il est calculé en multipliant le SLE par l'ARO.

### *Concepts et formules associées*

EF (Facteur d'Exposition) : Pourcentage de pertes pour un actif causé par une menace.

SLE (Single Loss Expectancy) : Valeur de l'Actif (en euros ou en dollars) multipliée par le Facteur d'Exposition (EF).

ARO (Fréquence annuelle de l'occurrence d'une menace) : Il représente la fréquence estimée à laquelle une menace est susceptible de se produire au cours d'une année.

ALE (Annualized Loss Expectancy) : L'ALE est la perte financière attendue sur une année pour une organisation en raison d'une menace. Il est calculé en multipliant le SLE par l'ARO.

## 3.4 Focus sur ISO 27001

La norme ISO 27001 de la famille des normes ISO/IEC 27000 est la seule qui permet d'obtenir une certification. Les autres normes de cette série fournissent des meilleures pratiques, des recommandations et des guides pour la mise en œuvre.

### *Structure de la norme ISO 27001*

La norme ISO 27001 version 2013 est un document relativement court, avec seulement 33 pages dans sa traduction française. Cependant, chaque ligne de cette norme est hautement significative. Ses principales clauses couvrent divers aspects, notamment **la conception, la mise en œuvre, la gestion opérationnelle, le suivi, la revue, la maintenance et l'amélioration du système de management de sécurité de l'information (SMSI).** Elle traite également des exigences documentaires, **des documents de contrôle, des enregistrements de contrôle, de la responsabilité de la direction et du management, de la gestion des ressources, de la formation, de la sensibilisation, de la gestion des compétences, des audits internes, des revues des entrées et des sorties, de l'amélioration continue**, ainsi que **des actions correctives et préventives**.

### *Les exigences générales su SMSI*

La norme ISO 27001 est complétée par la norme ISO 27002. La première énonce les exigences auxquelles une organisation doit répondre pour être conforme, tandis que la seconde apporte des recommandations spécifiques.

Les aspects cruciaux de la norme ISO 27001 incluent :

- Le périmètre du SMSI, définissant l'étendue de son application.
- La politique de sécurité de l'information, qui établit la direction du SMSI dans le contexte de la gestion globale de la sécurité de l'information.
- L'adaptation du SMSI à l'ensemble de l'organisation plutôt que l'inverse.
- La gestion des actifs, couvrant les éléments nécessaires pour fournir les services de l'entreprise, qu'ils soient tangibles ou intangibles.
- L'évaluation des risques, impliquant l'identification des risques associés à chaque actif.
- Le plan de traitement des risques, définissant la manière dont les risques seront gérés, en harmonie avec la politique de sécurité et de gestion des risques de l'entreprise.
- La déclaration d'applicabilité, englobant les contrôles et objectifs de contrôle de l'annexe A de la norme ISO 27001 qui sont appliqués, généralement sélectionnés parmi les 114 objectifs de contrôle.

La norme ISO 27001 sert de cadre pour la gestion de la sécurité de l'information et doit être adaptée à chaque organisation pour garantir la conformité et l'efficacité du SMSI.

## 3.5 Les principales étapes de la gestion des risques

Calculer le risque implique d'anticiper l'impact potentiel d'un problème et de définir une réponse adéquate. De nombreuses organisations négligent cette étape, ce qui les contraint à gérer les problèmes en urgence. Le calcul des risques est une démarche recommandée par l'Open Group, propriétaire de TOGAF, un référentiel d'architecture d'entreprise. Cette approche aide les organisations à planifier et à réagir de manière plus éclairée aux menaces potentielles.

### *Qu'est-ce qu'un risque ?*

Un risque est un événement incertain avec des conséquences potentiellement dommageables. Il peut également être appelé "aléa" ou "imprévu". Il est essentiel de distinguer entre "risque" pour des événements futurs et "incident" ou "problème" pour des événements passés. La gestion des risques vise à réduire les dangers et à minimiser leurs impacts, en privilégiant une approche préventive plutôt que corrective, selon les normes ISO.

**Étape 1 - Identification des actifs** : Dans cette première étape, il s'agit d'identifier les actifs tels que les données, les applications et les serveurs, ainsi que de délimiter leur périmètre. Cette étape est cruciale pour le processus de gestion des risques.

Pour cette identification, il faut également identifier les menaces associées à chaque actif, caractériser les agents de menace (comme les employés, les sous-traitants, les concurrents) dans l'environnement de travail, évaluer la fréquence de leur contact avec les actifs, estimer la probabilité d'attaque par ces agents, et décrire les menaces présentes dans cet environnement.

**Étape 2 - Estimation du Loss Event Frequency (LEF)** : Cette étape implique l'estimation du LEF, un indicateur basé sur quatre paramètres clés : le Threat Event Frequency (TEF), le Threat Capability (TCap), le Control Strength (CS), et la vulnérabilité (Vuln).

- Estimation du Threat Event Frequency (TEF) : Le TEF est estimé en utilisant des indices pour classer la fréquence des menaces. Par exemple, une fréquence "Très élevée (Very High)" pourrait signifier plus de 100 incidents par an, tandis qu'une fréquence "Très faible (Very Low)" pourrait représenter moins d'une fois tous les 10 ans.

- Estimation du Threat Capability (TCap) : Le TCap évalue la capacité d'une menace à agir malveillamment contre un actif. Par exemple, un TCap "Très élevé (Very High)" signifie que la menace se classe parmi le top 2 % en termes de capacité, tandis qu'un TCap "Très faible (Very Low)" signifie que la menace est parmi le bottom 2 % en termes de capacité.

- Estimation du Control Strength (CS) : Le CS représente la probabilité que les contrôles mis en place par l'organisation résistent à une population de menaces. Par exemple, un CS "Très élevé (Very High)" signifie que les contrôles protègent contre tout, sauf les 2

% de menaces les plus élevées, tandis qu'un CS "Très faible (Very Low)" signifie que les contrôles protègent seulement contre le bottom 2 % des menaces les plus courantes.

- Description de la vulnérabilité (Vuln) : La vulnérabilité est dérivée du TCap et du CS pour évaluer la vulnérabilité d'un actif. Elle représente la possibilité qu'une menace exploite les vulnérabilités associées à un actif.

**Étape 3 - Évaluation du Probable Loss Magnitude (PLM)** : Au cours de cette étape, l'objectif est d'identifier les scénarios de pertes les plus probables, ainsi que le pire scénario possible en termes de magnitude des pertes.

Magnitude (Fourchettes) :

- Sévère (SV) : Les pertes potentielles peuvent aller jusqu'à 10 000 000 € ou plus.
- Élevé (High, H) : Les pertes potentielles peuvent varier de 1 000 000 € à 9 999 999 €.
- Significatif (Sg) : Les pertes potentielles peuvent aller de 100 000 € à 999 999 €.
- Modéré (M) : Les pertes potentielles peuvent varier de 10 000 € à 99 999 €.
- Faible (Low, L) : Les pertes potentielles peuvent varier de 1 000 € à 9 999 €.
- Très faible (Very Low, VL) : Les pertes potentielles sont comprises entre 0 € et 999 €.

Étape 4 - Dérivation et Articulation du Risque : À cette étape, nous utilisons les valeurs du Loss Event Frequency (LEF) et du Probable Loss Magnitude (PLM) pour calculer la valeur du risque. Cela se fait en utilisant une matrice de risques, comme illustré dans la figure 8.

- Risque : La magnitude du risque est dérivée du croisement entre le PLM (Probable Loss Magnitude) et le LEF (Loss Event Frequency). La matrice de risques nous aide à évaluer la magnitude du risque.

| RISQUE | | | | | | |
|---|---|---|---|---|---|---|
| *Probable Loss Magnitude PLM* | Sévère | Élevé | Élevé | Sévère | Sévère | Sévère |
| | Élevé | Modéré | Élevé | Élevé | Sévère | Sévère |
| | Significatif | Modéré | Modéré | Élevé | Élevé | Sévère |
| | Modéré | Faible | Modéré | Modéré | Élevé | Élevé |
| | Faible | Faible | Faible | Modéré | Modéré | Modéré |
| | Très faible | Faible | Faible | Faible | Modéré | Modéré |
| | | Très faible | Faible | Modéré | Significatif | Élevé |
| *Loss Event Frequency* LEF | | | | | | |

*Figure 7 : La magnitude du risque est dérivée du PLM et du LEF*

- Clés pour les valeurs de risque :
  - C (Critique) : Correspond à un niveau de risque critique.
  - H (High, Élevé) : Indique un niveau de risque élevé.
  - M (Modéré) : Indique un niveau de risque modéré.
  - L (Low, Faible) : Représente un niveau de risque faible.

L'articulation du risque doit être alignée sur le référentiel des décideurs, car c'est un défi crucial pour prendre des décisions éclairées en matière de gestion des risques.

### *Le plan de traitement des risques*

Le plan de traitement des risques propose généralement quatre options pour gérer les risques :

1. **Réduction des risques** : Cette option vise à réduire la probabilité et les conséquences négatives associées à un risque, parfois les deux à la fois.

2. **Évitement du risque** : Cela implique purement et simplement d'annuler l'activité liée au risque. Par exemple, en annulant certaines transactions financières en provenance de pays à risque.

3. **Transfert de risque** : Il s'agit de partager les risques avec une tierce partie, comme souscrire une assurance.

4. **Rétention des risques ou acceptation du risque** : Vous acceptez consciemment le risque associé, en étant conscient de la menace et de ses impacts.

Ces options ne sont pas mutuellement exclusives et peuvent être combinées. Une communication efficace entre les parties prenantes est essentielle pour prendre des décisions éclairées concernant le niveau acceptable de risque et les traitements à appliquer. La perception des risques peut varier en fonction des différentes parties prenantes, de leurs besoins, de leurs intérêts et du secteur d'activité. Il est essentiel de bien documenter et argumenter la perception des bénéfices et des pertes liés aux risques pour assurer une compréhension commune par toutes les parties impliquées.

## 3.6 Digital Forensic ou l'informatique technico- légale

### *Définition*

La "Digital Forensic" est une discipline informatique qui se concentre sur la collecte d'éléments de preuve numériques pour une utilisation en justice. Elle englobe les preuves médico-légales liées à divers éléments numériques, tels que documents informatiques, courriels, photographies, logiciels, etc., dans le cadre d'affaires judiciaires. Elle vise à acquérir, collecter, conserver et présenter des preuves légales à partir de supports numériques, notamment en cas de piratage ou de vol, afin d'identifier, préserver, récupérer, analyser et présenter des faits et des opinions dans des procédures judiciaires

### *Enjeux*

Le développement de l'informatique personnelle dans les années 1980 a donné lieu au hacking, qui consiste en partie à voler des informations confidentielles. En réponse, la Digital Forensic Science a émergé pour fournir des preuves numériques devant les tribunaux. Cette discipline est désormais reconnue par les tribunaux européens et américains, et les experts en cybersécurité sont de plus en plus sollicités pour enquêter sur des crimes liés à la cyberfraude, la pédopornographie et d'autres délits numériques. Des formations spécifiques sont disponibles, permettant d'obtenir le titre de "Lead Forensics Examiner". Ces experts travaillent sur des artefacts numériques, comme les ordinateurs et les supports de stockage, et leurs missions vont de la récupération d'informations supprimées à la compréhension des mécanismes de piratage. Il est recommandé de combiner des compétences techniques avec des compétences en gestion et en droit, en fonction des besoins spécifiques.

### *Le processus Forensic*

Le processus Forensic pour gérer des preuves numériques se divise en trois étapes essentielles : l'acquisition, l'analyse, et le reporting. L'évolution des techniques est notable, notamment grâce à l'utilisation d'outils comme Kali Linux, qui offre une gamme de logiciels permettant d'examiner divers aspects des artefacts numériques.

### *Les principales techniques de Forensic*

1. **Analyse Cross Drive :** Cette technique consiste à croiser des données de divers supports numériques pour détecter des anomalies. Par exemple, elle peut être utilisée pour identifier des personnes vulnérables, comme celles susceptibles de faire une tentative de suicide, ou pour repérer des indicateurs de préparation d'actes criminels, tels que des attentats.

2. **Analyse en temps réel :** Elle implique la collecte d'informations ou d'artefacts, tels que des disques durs, avant l'extinction de l'ordinateur. L'objectif est de préserver les preuves numériques qui pourraient être compromises ou perdues après le redémarrage de la machine. Par exemple, la création d'une image d'un disque dur en fonctionnement permet de conserver des informations cruciales, y compris les systèmes de chiffrement.

3. **File Carving pour la récupération de fichiers supprimés :** Cette technique vise à retrouver des fichiers qui ont été supprimés. Le formatage d'un disque dur ne garantit pas nécessairement la suppression définitive des fichiers, car la plupart des systèmes d'exploitation se contentent d'effacer la table d'allocation des fichiers lors du formatage. Le File Carving consiste à rechercher les en-têtes des fichiers pour les reconstruire manuellement.

4. **Pallier la volatilité des données :** Pour préserver les données volatiles, il est nécessaire de mener l'enquête avec l'ordinateur en marche, car une fois éteint, les informations peuvent être perdues. Cependant, même après l'extinction de l'ordinateur, les charges électriques stockées dans la mémoire vive (RAM) ne se dissipent pas instantanément. En refroidissant les barrettes de RAM à des températures très basses, comme -60 °C, il est possible de conserver ces données, mais cela nécessite un équipement spécialisé.

## *Les outils du Forensic*

Le Forensic dispose d'une multitude d'outils, dont beaucoup sont communs à ceux utilisés par les hackers. Ces outils couvrent divers aspects de la gestion des preuves numériques. Voici quelques catégories d'outils couramment utilisées :

1. **Gestion des images disque :** Permet de créer et de gérer des images de disques pour conserver l'intégrité des preuves numériques.
2. **Recouvrement et carving de données :** Ces outils sont utilisés pour récupérer des données effacées ou pour reconstituer des fichiers à partir de fragments.
3. **Analyse de fichiers :** Ces outils permettent d'analyser le contenu des fichiers à la recherche d'informations pertinentes.
4. **Extraction des métadonnées :** Utile pour extraire des métadonnées à partir de documents, ce qui peut fournir des informations cruciales sur leur origine et leur utilisation.
5. **Outils de gestion des images mémoire :** Pour acquérir et analyser des images de la mémoire RAM d'un ordinateur.
6. **Outils de gestion d'analyse de la mémoire :** Ces outils aident à analyser la mémoire vive pour identifier des activités suspectes ou des artefacts numériques.
7. **Outils de gestion du réseau :** Utilisés pour examiner le trafic réseau, les journaux, et détecter des activités anormales.
8. **Analyse des fichiers de log :** Permet d'analyser les journaux système et les fichiers de log pour identifier des événements pertinents.

La plupart de ces outils sont en open source et fonctionnent sous Linux. La distribution Kali Linux, par exemple, intègre un ensemble conséquent d'outils de Forensic.

En ce qui concerne le matériel, il existe des appareils capables de télécharger, copier, dupliquer et exploiter des données à partir d'appareils mobiles tels que des téléphones portables et des tablettes. Une marque reconnue dans ce domaine est Cellebrite, qui propose des appareils comme le UFED Touch 2 permettant l'extraction physique de données, de

systèmes de fichiers, et de mots de passe à partir d'appareils portables. Ces outils sont essentiels pour la collecte de preuves numériques dans le cadre d'enquêtes Forensic.

# 4. Introduction au pen testing et au hacking

## 4.1 Introduction au hacking et aux tests d'intrusion

### *Les étapes d'un test d'intrusion*

Le test d'intrusion (penetration testing ou pen test) comprend les étapes suivantes :

5. Identification de la cible : reconnaissance passive
6. Reconnaissance active et exploration des vulnérabilités
7. Exploitation
8. Post-exploitation : actions sur le système cible
9. Post-exploitation : persistance

**La démarche de reconnaissance**

La reconnaissance est la première étape technique d'un test d'intrusion, où un pirate ou un auditeur en sécurité consacre une grande partie de ses efforts. Son objectif est de collecter des informations sur le système cible pour identifier les failles potentielles à exploiter (comme le déni de service, le vol de données, la modification des données, etc.). La reconnaissance se divise en deux types : passive et active.

Reconnaissance passive :

9. Aucune interaction directe avec le système cible.
10. Collecte d'informations publiques à partir de sources telles que Google, WHOIS, etc.
11. L'interaction avec le système cible est normale, ce qui la rend difficile à repérer comme une attaque.

Reconnaissance active :

1. Interaction directe avec le système cible, permettant de détecter une attaque (système de détection d'intrusion).
2. Collecte d'informations à l'aide d'un scan du système cible.

3. Utilisation de techniques de dissimulation telles que des signatures, des proxies, etc.

**Identification de la cible : reconnaissance passive**

La reconnaissance passive dans le cadre d'un test d'intrusion implique l'analyse des informations disponibles publiquement, en particulier sur Internet grâce à des moteurs de recherche. Par exemple, le pirate ou l'auditeur en sécurité consulte la base Whois pour identifier le propriétaire du site Web et son hébergeur. Les actions du pirate sur le site Web de l'entreprise sont considérées comme normales, telles que la consultation de pages et le téléchargement de documents publics. Il est essentiel de noter que ces interactions ne sont jamais identifiées comme le prélude à une attaque.

Les principales étapes de la reconnaissance passive comprennent :

- Open Source Intelligence Target (OSINT) : collecte d'informations sur l'entreprise cible à partir de sources publiques telles qu'Internet et Google.
- Reconnaissance des Domain Name Systems (DNS) et du routage : utilisation de whois, IP V4, IP V6 et routage pour obtenir des informations sur la cible.
- Obtention d'informations sur les utilisateurs : récupération des noms des employés et de leurs adresses e-mail.
- Profil des utilisateurs et listes de mots de passe.

**Reconnaissance active et scan des vulnérabilités**

La reconnaissance active et le scan des vulnérabilités sont des étapes essentielles d'un test d'intrusion. L'objectif de ces phases est de collecter un maximum d'informations sur la cible pour faciliter la phase suivante d'exploitation. Contrairement à la reconnaissance passive, la reconnaissance active implique une interaction directe avec le système ciblé, et elle peut être détectée.

Les principales techniques de reconnaissance active incluent l'application de stratégies de camouflage pour masquer l'adresse IP du pirate, l'identification de l'infrastructure réseau, la découverte des ports, des systèmes d'exploitation et des services hébergés, ainsi que le scan des vulnérabilités. Les pirates utilisent des outils spécifiques tels que Nmap, Recon-ng, et Maltego pour effectuer ces activités.

Il est important de noter que, en France, le scan de ports est interdit. Les bons pirates utilisent des techniques de camouflage pour masquer leurs attaques, rendant ainsi difficile leur détection. Ils veillent également à utiliser un chiffrement et un type de trafic non standard pour éviter d'être tracés.

**Exploitation**

La phase d'exploitation est le moment où le pirate ou l'auditeur sécurité passe à l'attaque en tentant d'ouvrir un accès au système d'information cible ou en perturbant son accès aux utilisateurs. L'objectif peut être d'obtenir un accès permanent au système. Pour mener à bien cette phase, le pirate doit se poser plusieurs questions, notamment sur la définition du système cible, la clarté de l'exploitation prévue, la possibilité d'une exploitation à distance ou en local, et les activités de post-exploitation potentielles.

Les étapes de la phase d'exploitation comprennent la modélisation des menaces pour préparer une stratégie d'attaque, l'utilisation des ressources associées aux vulnérabilités en ligne et en local, l'exploitation de cibles multiples avec des outils comme Metasploit framework et Armitage, ainsi que le contournement des outils de détection tels que les antivirus.

**Post- exploitation : actions sur le système cible**

La phase de post-exploitation intervient une fois que le système d'information cible a été compromis. Le pirate ou l'auditeur sécurité a plusieurs objectifs à ce stade, notamment :

- Évaluer rapidement l'environnement local, y compris l'infrastructure, les connexions, les comptes, les fichiers cibles, et les applications vulnérables.
- Localiser, copier ou modifier les fichiers cibles, comme les bases de données contenant des informations sensibles.
- Créer des comptes utilisateurs supplémentaires et apporter des modifications au système pour un accès ultérieur.
- Rechercher des moyens d'escalader les privilèges vers les comptes d'administrateur système.
- Tenter d'étendre l'attaque à d'autres systèmes connectés.

- Installer des portes dérobées et des canaux protégés pour un accès ultérieur (persistance de post-exploitation).
- Effacer les traces de l'attaque pour éviter la détection.

**Post- exploitation : persistance**

La phase de persistance de la post-exploitation a pour but de maintenir un accès direct au système cible de manière à pouvoir y revenir ultérieurement. Elle implique une communication bidirectionnelle avec le système d'information cible qui doit rester ouverte sans être détectée.

Les objectifs du pirate ou de l'auditeur sécurité durant cette phase sont les suivants :

- Ajouter des outils complémentaires pour effectuer d'autres attaques, notamment contre les systèmes locaux connectés au système compromis.
- Faciliter l'exfiltration de données depuis le système compromis.
- Installer des outils anti-forensic (pour éviter la détection lors d'une enquête), y compris des systèmes d'effacement de mémoire et de traçage des modifications des fichiers système. Cette approche est basée sur l'authentification forte et le chiffrement.

Les activités courantes de persistance durant la phase de post-exploitation incluent :

- La compromission du système existant, des applications et des données pour permettre un accès distant ultérieur via des services tels que Telnet, Windows Terminal Services ou Virtual Network Computing.
- L'utilisation d'agents persistants avec des outils comme Netcat.
- Le maintien de la persistance en utilisant le Framework Metasploit, par le biais de scripts tels que Metsvc et des scripts de persistance.
- La création d'un agent de persistance autonome avec Metasploit.
- La redirection des ports pour contourner les contrôles réseau, incluant la redirection de port simple et bidirectionnelle.

## 4.2 Test d'intrusion (pen test) : types, méthode, étapes

Ce chapitre introduit le test d'intrusion, un processus d'évaluation de la sécurité des systèmes d'information. Il explore les caractéristiques des tests de sécurité, les différences entre les approches Black Box et White Box, les distinctions entre les tests d'intrusion et les tests de vulnérabilité, ainsi que les méthodes couramment utilisées par les organisations pour renforcer leur sécurité.

### *Le pen test : un test de sécurité à la forme très agressive*

Les tests d'intrusion peuvent être effectués en interne ou par des partenaires externes, et chaque test doit être accompagné d'un contrat légalement contraignant. Ils sont une composante essentielle de la gestion des risques en sécurité informatique, intégrant des pratiques de sécurité spécifiques. Les tests d'intrusion, réalisés par des professionnels qualifiés, évaluent tous les composants de l'infrastructure informatique, y compris les applications, le réseau, les systèmes d'exploitation, etc. Ils génèrent des rapports identifiant les vulnérabilités du système cible et proposent des mesures correctives. Ces tests suivent des méthodologies établies pour garantir un contrôle efficace et des améliorations pour l'organisation cliente.

### *Les deux types de pen test*

Il existe deux principales catégories de tests d'intrusion : les tests Black Box et les tests White Box.

**Black Box Test** : Dans ce type de test, le testeur évalue l'infrastructure réseau sans connaissance préalable des technologies internes de l'organisation ciblée. Ils utilisent diverses techniques de hacking pour identifier et potentiellement exploiter des vulnérabilités. Les résultats sont présentés dans un rapport qui classe et hiérarchise les vulnérabilités en fonction de leur niveau de risque.

**White Box Test** : Les testeurs White Box ont une connaissance approfondie des technologies internes de l'organisation. Ils concentrent leurs attaques en utilisant des approches spécifiques aux environnements cibles.

Ces deux types de tests sont complémentaires. Le White Box est utile pour identifier et éliminer les failles internes, tandis que le Black Box teste la sécurité réelle du système depuis l'extérieur. Ils partagent une méthodologie similaire, mais le Black Box tester se focalise sur

des vecteurs d'attaque réalistes, ce qui le rend plus efficace pour identifier les vulnérabilités. Il est souvent plus coûteux, mais donne une perspective réaliste de la posture de sécurité de l'organisation. En général, il est recommandé d'associer les deux types de tests pour une évaluation plus complète.

### *Approche méthodologique d'un pen test*

La réussite d'un test d'intrusion dépend non seulement des outils, mais aussi d'une méthodologie bien définie. Cette méthodologie consiste en des règles, des pratiques et des procédures qui guident l'évaluation de la sécurité d'un réseau, d'une application ou d'un système. Elle est essentielle pour obtenir des résultats significatifs. Le framework présenté dans ce chapitre est une synthèse de référentiels existants et peut s'appliquer aux tests Black Box et White Box. Il offre une approche éprouvée et adaptable en fonction de la cible.

1. **Périmètre de la cible (Target scoping):** Définir ce qui doit être testé, comment, les conditions et les limites. Identifier les objectifs métiers et le temps nécessaire.

2. **Collecte d'informations (Information gathering):** Rassembler des données sur la cible à partir de sources publiques et outils pour obtenir un maximum d'informations.

3. **Découverte de la cible (Target discovery):** Identifier le réseau cible, ses systèmes d'exploitation et l'architecture, en utilisant des outils comme Kali Linux.

4. **Dénombrement (Enumerating target):** Identifier les ports ouverts du système cible en utilisant différentes techniques de scan.

5. **Cartographie des vulnérabilités (Vulnerability mapping):** Analyser les vulnérabilités liées aux ports et services ouverts en utilisant des outils automatisés.

6. **Ingénierie sociale (Social engineering):** Utiliser des tactiques humaines, telles que le phishing, pour accéder au système cible.

7. **Exploitation de la cible (Target exploitation):** Pénétrer le système en exploitant les vulnérabilités identifiées, combinant souvent des attaques techniques et de l'ingénierie sociale.

8. **Escalade des privilèges (Privilege escalation):** Augmenter les privilèges pour obtenir un accès étendu au système, en utilisant des exploitations locales.

9. **Maintien de l’accès (Maintaining access):** Conserver l'accès pour démontrer les accès illégitimes, en utilisant des méthodes de tunnels secrets.

10. **Documentation et rapports:** Présenter les vulnérabilités, les exploitations et les recommandations dans un rapport pour aider à remédier aux failles de sécurité identifiées.

# 5. La sécurité des systèmes de production 4.0

La digitalisation croissante des processus de production vise à améliorer l'efficacité et réduire les coûts, notamment dans l'industrie 4.0. Cependant, cette transformation expose davantage les systèmes informatiques industriels à des menaces de cybersécurité complexes. Cette transition examine la nature technologique de l'industrie 4.0, les risques de cybersécurité, les spécificités des systèmes industriels, les opportunités et risques des nouvelles technologies, les coûts associés, et donne des exemples de cibles potentielles.

## 5.1 Industrie 4.0 et cybersécurité

### *L'industrie 4.0, c'est quoi ?*

Le terme "industrie 4.0" fait référence à la transformation numérique des systèmes de production et des modèles commerciaux. Il a été introduit en 2011 à la Foire de Hanovre. Cette évolution implique l'utilisation du numérique pour réorganiser le travail et moderniser les moyens de production. Les usines 4.0 sont interconnectées et intelligentes, permettant l'interaction entre produits, processus et machines via un réseau externe. Ce concept est considéré comme la quatrième révolution industrielle, succédant à la mécanisation, à la production de masse et à l'automatisation de la production au cours des siècles précédents

### *Pourquoi une industrie 4.0*

L'industrie 4.0 vise principalement à résoudre les défis contemporains tels que la personnalisation à grande échelle des produits, l'optimisation de la productivité et de l'efficacité des ressources sur l'ensemble de la chaîne de valeur. Les avantages se répartissent entre les clients, les entreprises et les employés, engendrant des produits plus attractifs et abordables pour les clients, une meilleure communication et coordination entre les métiers pour les entreprises, et l'amélioration des conditions de travail et de l'ergonomie pour les employés.

### *Comment fonctionne une industrie 4.0 ?*

Selon le cabinet Kurt Salmon (2015), l'industrie 4.0 repose sur six principes clés :

1. **Interopérabilité des systèmes :** Capacité des systèmes à communiquer et interagir, exemplifié par la collaboration entre Mercedes-Benz et KUKA Roboter GmbH pour la construction simultanée de différents modèles de voiture.

2. **Virtualisation de l'usine :** Simulation en 3D des produits, des processus et de l'environnement de production.

3. **Décentralisation des décisions :** Capacité des systèmes cyber-physiques à prendre des décisions de manière autonome.

4. **Orientation service :** Amélioration de la maintenance et renforcement de l'offre de services.

5. **Modularité des lignes de production :** Adaptation rapide à une demande changeante en permettant la production de petites séries et en transformant l'usine en un mécano composé de pièces de Lego.

6. **Analyse et prise de décision en temps réel :** Communication permanente et instantanée permettant une analyse et une prise de décision en temps réel.

### *Les 9 piliers de l'industrie 4.0*

Selon le Boston Consulting Group, l'industrie 4.0 repose sur neuf piliers fondamentaux. Bien que ces piliers soient déjà utilisés de manière isolée dans la production industrielle, l'avènement de l'"usine intelligente" permet de les réunir en un flux de production entièrement intégré, automatisé et optimisé.

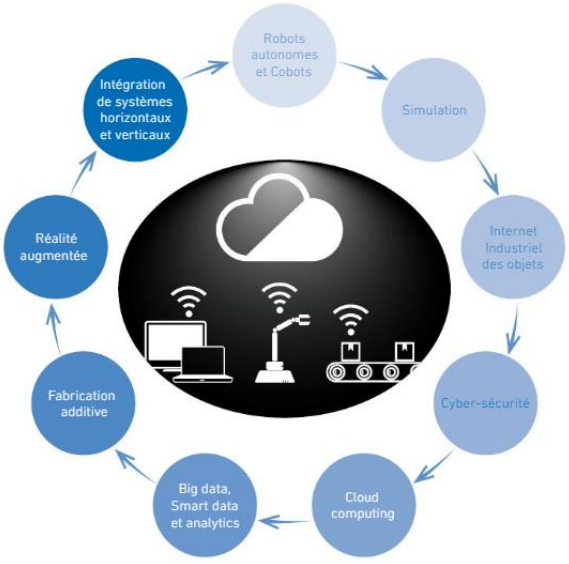


*Figure 8 : Les 9 piliers technologiques de l'industrie 4.0*

### *Comment mettre en place l'industrie 4.0*

L'Industrie 4.0 favorise une communication instantanée entre machines, capteurs et postes de travail, améliorant la flexibilité et l'adaptabilité aux demandes clients en temps réel. Cependant, cette révolution des données soulève des préoccupations majeures en matière de cybersécurité. Les piliers technologiques incluent des applications telles que le cloud computing, le big data, la réalité augmentée, l'intégration de systèmes, les robots autonomes, la simulation, l'Internet Industriel des Objets (IIoT), et la cybersécurité, chacun apportant des avantages spécifiques à la production industrielle. Ces avancées technologiques exigent une vigilance accrue contre les cybermenaces, soulignant ainsi l'importance de la cybersécurité dans le contexte de l'Industrie 4.0.

## 5.2 La cybersécurité industrielle

### *Objectifs et spécificités de la cybersécurité industrielle*

Les objectifs principaux de la cybersécurité industrielle, classés par ordre de priorité, sont les suivants :

1. **Disponibilité de l'outil de production :** Assurer le fonctionnement ininterrompu des systèmes industriels.
2. **Confidentialité des informations et du savoir-faire :** Protéger les données sensibles et les connaissances spécifiques liées à la production.
3. **Intégrité des données échangées :** Garantir l'exactitude et l'authenticité des informations circulant au sein des systèmes industriels.

### *Vulnérabilités des systèmes d'information industriels*

Les systèmes d'information industriels présentent plusieurs vulnérabilités, souvent non médiatisées pour protéger la réputation des entreprises. Le secteur manufacturier est particulièrement visé en raison de la perception de faiblesse de la sécurité de ces systèmes. Parmi les vulnérabilités identifiées par l'Anssi :

1. Sécurité négligée lors des phases de conception, installation, exploitation et maintenance.
2. Absence d'inventaire des équipements et de vision des générations technologiques et de leurs vulnérabilités.

3. Manque d'analyse des risques, de plan de continuité et de plan de reprise d'activités.
4. Utilisation de mots de passe par défaut et stockage en clair dans les codes sources.
5. Manque d'expérience et de culture cybersécurité des opérationnels.
6. Gestion faible des accès utilisateurs, comptes restant actifs après le départ des intervenants.
7. Emploi de comptes avec des profils administrateur plutôt que des droits utilisateur.
8. Partage de fichiers en accès complet plutôt qu'en lecture seule sur le réseau.
9. Accès à des fichiers de configuration via des protocoles non sécurisés tels que FTP.
10. Utilisation d'outils de prise de main à distance non sécurisés (VNC, Dameware).
11. Emploi de services/protocoles non sécurisés tels que HTTP, Telnet, SNMP v1 ou v2.
12. Modification en ligne des programmes automates autorisée sans contrôle.
13. Rechargement de la configuration au redémarrage via une clé USB

### *Mesures de protection et de prévention*

Pour faire face aux défis de cybersécurité, la métropole de Lyon a créé en 2017 un collectif européen dédié à la cybersécurité des systèmes industriels et urbains, en partenariat avec les acteurs du territoire. Les objectifs du collectif incluent la fédération des parties prenantes, le partage d'informations sur les solutions et les bonnes pratiques, la valorisation des savoir-faire, et l'amélioration des compétences des acteurs impliqués. Ce collectif réunit divers acteurs tels que des fabricants d'équipements, des éditeurs de solutions, des intégrateurs, des experts en cybersécurité, un centre de recherche (CEA Leti), et des opérateurs de systèmes industriels et urbains. Lors du Salon industrie Lyon en avril 2017, le collectif a présenté le premier démonstrateur de cybersécurité des systèmes industriels, illustrant les impacts de scénarios d'attaque sur des équipements industriels réels et fournissant des enseignements sur la protection des systèmes.

## 5.3 Internet des Objets et cybersécurité

### *Objets connectés et risque de vol de données et piratage*

En matière de cybersécurité des objets connectés (Internet des Objets - IoT), des vulnérabilités importantes ont été exposées lors de la DEF CON, mettant en évidence des faiblesses dans des dispositifs tels qu'un fauteuil roulant, un thermostat, et des serrures connectées. Ces failles permettent des attaques malveillantes, illustrant le potentiel de piratage des objets IoT, qui font référence à une interconnexion d'appareils physiques via Internet, permettant la collecte et l'échange de données. Des exemples notoires incluent le piratage d'une Jeep Cherokee en 2015, où des chercheurs ont pris le contrôle à distance via le bus CAN du véhicule, et l'attaque du Mirai Botnet en 2016, qui a paralysé une partie de l'Internet américain en ciblant des caméras connectées. De plus, des failles dans des stimulateurs cardiaques ont été signalées en 2017, soulignant les risques pour la santé liés aux vulnérabilités de l'IoT. Ces exemples mettent en évidence l'importance croissante de sécuriser les objets connectés pour prévenir des conséquences graves.

### *Quelles sont les sources majeures de vulnérabilités de l'Internet des Objets ?*

La cybersécurité des objets connectés (IoT) est confrontée à plusieurs points de vulnérabilité, dont :

- **L'objet connecté lui-même :** L'analyse approfondie des composants tels que la carte SD, les mémoires, et les processeurs peut révéler des failles de sécurité, permettant à un hacker d'exploiter une vulnérabilité commune à tous les objets de même conception. Une telle faille peut conduire à des rappels massifs de produits par les fabricants.

- **La transmission des données :** Constituant l'une des vulnérabilités les plus critiques, la transmission des données offre la possibilité d'accéder à distance à un grand nombre d'objets connectés sans que les utilisateurs en soient conscients. Des bases de données en ligne, comme Shodan, répertorient de nombreux objets connectés non sécurisés auxquels on peut se connecter directement via le Web.

- **La plateforme Internet :** C'est le point central où toutes les données des objets connectés sont remontées. La sécurité de cette plateforme est cruciale pour prévenir tout accès non autorisé.

- **L'application sur smartphone :** Souvent utilisée comme interface de paramétrage et de contrôle des objets connectés, cette application peut être une cible pour les attaques si elle n'est pas correctement sécurisée.

- **L'utilisateur :** Un maillon important de la chaîne de sécurité, l'utilisateur peut négliger des pratiques sécuritaires essentielles, telles que la modification du mot de passe initial ou la mise en place de mesures de protection adéquates pour ses objets connectés.

### *Comment protéger ses données personnelles dans cet Internet des Objets ?*

La prolifération des objets connectés dans notre quotidien ne doit pas masquer la sensibilité des données qu'ils traitent. Voici quelques recommandations de la CNIL pour assurer une utilisation sécurisée des objets connectés :

1. **Vérifier les paramètres d'accès :** S'assurer que l'objet ne permet pas une connexion non autorisée, en vérifiant notamment que l'appairage avec un smartphone ou depuis Internet nécessite un bouton d'accès physique ou l'utilisation d'un mot de passe.

2. **Modifier les paramètres par défaut :** Changer les paramètres par défaut de l'objet, tels que le mot de passe, le code PIN, etc.

3. **Sécuriser l'accès au smartphone et au réseau Wi-Fi :** Protéger l'accès à l'écran de déverrouillage du smartphone et sécuriser le réseau Wi-Fi utilisé avec l'objet connecté par un mot de passe fort.

4. **Vigilance accrue pour les données sensibles :** Être particulièrement vigilant en matière de sécurité lorsque les objets produisent des données sensibles, notamment liées à la santé ou aux enfants.

5. **Préserver la vie privée :** Être attentif à la vie privée en cas d'association de l'objet à des réseaux sociaux, en désactivant le partage automatique des données.

6. **Garantir l'accès et la suppression des données :** S'assurer de la possibilité d'accéder aux données générées par l'objet et de les supprimer selon les besoins.

7. **Éteindre l'objet inutilisé :** Éteindre l'objet lorsqu'il n'est pas utilisé, notamment pour éviter la collecte non autorisée de données sensibles.

Pour les objets connectés nécessitant un compte en ligne :

- **Utiliser des pseudonymes :** Maximiser l'utilisation de pseudonymes au lieu de noms réels.
- **Minimiser les informations fournies :** Ne communiquer que les informations strictement nécessaires au service.
- **Créer des adresses de messagerie distinctes :** Utiliser des adresses de messagerie différentes pour chaque objet ou service en ligne.
- **Sécuriser l'accès au compte en ligne :** Protéger l'accès au compte en ligne avec un mot de passe fort et différent des autres comptes.

En cas de mise au rebut ou de changement d'utilisateur :

- **Supprimer l'association avec les comptes en ligne :** Avant la mise au rebut ou le changement d'utilisateur, supprimer l'association de l'objet avec ses différents comptes, notamment sur les réseaux sociaux.
- **Effacer les données et supprimer le compte :** Effacer les données stockées sur l'objet et supprimer le compte en ligne s'il n'est plus utilisé.
- **Réinitialiser les paramètres d'usine :** Utiliser la fonction "réinitialiser les paramètres d'usine" de l'objet si elle est disponible.

### *Comment sécuriser l'Interne des Objets ?*

Pratiques clés pour minimiser les attaques via l'IoT :

**Pour les concepteurs :**

1. **Privacy by Design :** Appliquer la protection de la vie privée dès la conception, comme illustré par la caméra de surveillance Myfox qui ajuste automatiquement son fonctionnement en fonction de la présence.
2. **Mots de passe uniques :** Choisir des mots de passe uniques pour chaque appareil.
3. **Modification des identifiants par défaut :** Rendre obligatoire la modification du nom d'utilisateur et du mot de passe par défaut lors de l'installation de tout périphérique sur Internet.

4. **Capacité d'action locale :** Assurer que l'objet connecté peut agir localement sans connexion Internet et rejeter des ordres incohérents.

**Choix stratégique pour les fabricants :**

1. **Audit de sécurité :** Mettre en place un audit de sécurité complet de la chaîne de données pour identifier les vulnérabilités et comprendre les risques et les solutions.

2. **Analyse des modes de défaillance :** Utiliser l'AMDEC comme outil pour évaluer les modes de défaillance, leurs effets, et leur criticité. Faire des choix stratégiques en fonction du coût, du risque de piratage, et de l'impact sur l'utilisateur et l'entreprise.

**Pour les utilisateurs :**

1. **Éviter les périphériques non mis à jour :** Éviter l'utilisation de périphériques qui ne peuvent pas avoir leur logiciel, mot de passe, ou firmware mis à jour.

2. **Mises à jour obligatoires :** Effectuer obligatoirement les dernières mises à jour de logiciels et de micrologiciels pour atténuer les vulnérabilités des périphériques IoT.

3. **Décomposition de l'information :** Décomposer l'information en locale et à distance, en privilégiant la collecte et le traitement local des informations vitales au lieu de les transmettre sur Internet.

### *Sécuriser l'Internet des Objets avec la blockchain*

Blockchain : Une blockchain est une base de données distribuée et sécurisée qui enregistre des transactions de manière transparente et immuable. Chaque bloc de données est lié cryptographiquement au précédent, formant une chaîne, d'où le nom "blockchain". Cette technologie offre une transparence, une sécurité et une décentralisation accrues.

**Utilisation de la Blockchain pour Sécuriser l'Internet des Objets (IoT) :**

La blockchain, une technologie sous-tendant les cryptomonnaies comme le Bitcoin, offre des solutions cruciales pour la sécurité de l'Internet des Objets (IoT). Voici comment elle peut être exploitée :

1. **Plateformes Décentralisées et Collaboratives :** La blockchain permet de créer des plateformes décentralisées et collaboratives pour le partage d'objets connectés, éliminant les intermédiaires et réduisant les coûts de transaction.

2. **Réseaux IoT Peer-to-Peer (P2P) :** En favorisant les réseaux IoT peer-to-peer, la blockchain élimine le besoin de confiance entre les périphériques, évitant les points de défaillance centralisés.

3. **Sécurité des Transactions :** En tant que registre universellement distribué, la blockchain assure la sécurité des transactions. Les nœuds, participants au réseau, valident les transactions via des processus cryptographiques, renforçant la confiance sans autorité centrale.

4. **Protection des Identités :** La décentralisation des données de l'Infrastructure à Clé Publique (PKI) protège les identités, éliminant le besoin d'une autorité centrale pour authentifier les périphériques et les utilisateurs.

5. **Intégrité des Données :** Les mécanismes des nœuds garantissent mutuellement la validité des modifications de données, assurant l'intégrité des informations échangées.

6. **Protection de l'Infrastructure :** La gestion distribuée des entrées DNS par la blockchain contribue à diminuer les impacts des attaques par déni de service distribué (DDoS).

## 5.4 Cloud computing et cybersécurité

### *Qu'est- ce que le cloud ?*

Le Cloud Computing, défini par le NIST, est l'accès à la demande à des ressources informatiques partagées via un réseau. Il externalise l'infrastructure informatique, utilisant la puissance de serveurs distants. Trois principaux modèles de services incluent l'Infrastructure en tant que Service (IaaS), la Plateforme en tant que Service (PaaS), et le Logiciel en tant que Service (SaaS). Cette approche offre une flexibilité majeure, mais nécessite une considération particulière en matière de sécurité lors de son adoption.

### *Quels sont les différents types de cloud ?*

Le Cloud Computing se décline en différentes structures répondant à des besoins spécifiques. Le cloud public offre des ressources partagées gérées par un tiers, tandis que le cloud privé, exploité par une seule entreprise, garantit une sécurité renforcée. Le cloud hybride permet de combiner des ressources internes et externes pour une flexibilité optimale en fonction des besoins d'activité.

- **Cloud Public :** Géré par un tiers, accessible via Internet, partage de ressources entre plusieurs entités.
- **Cloud Privé :** Exploité par une seule entreprise, offre une sécurité renforcée, peut être virtuellement hébergé sur le cloud public.
- **Cloud Hybride :** Combinaison de ressources internes privées avec des ressources externes publiques, offrant une flexibilité optimale pour répondre aux variations d'activité.

### *Le cloud en chiffres*

Un sondage de Vanson Bourne en 2017 a révélé que la migration vers le cloud progresse lentement, avec seulement 37 % des organisations ayant déplacé la majorité de leurs workloads vers un environnement de cloud privé ou public. Actuellement, 54 % des workloads reposent sur des data centers on-premise, mais cette part devrait chuter à 11 % d'ici 2020, tandis que le cloud privé devrait représenter 50 % et le cloud public 23 %. La migration concerne de plus en plus les données stratégiques, avec 56 % des entreprises ayant migré des informations corporate et 47 % des informations personnelles identifiables. Seulement 5 % des entreprises refusent actuellement de migrer des données sur le cloud, soulevant des préoccupations de sécurité et de conformité au RGPD.

## 5.5 Coût de la cybersécurité

### *Évolution du coût moyen annuel de cybercriminalité*

Selon l'étude "Cost of Cyber Crime" d'Accenture et Ponemon Institute, le coût moyen de la cybercriminalité a atteint 11,7 millions de dollars par entreprise à l'échelle mondiale en 2017, avec une augmentation de 62 % au cours des cinq dernières années. Cette hausse significative est attribuée à des attaques majeures telles que WannaCry et Petya, qui ont causé des préjudices financiers importants à plusieurs grandes entreprises mondiales.

### *Répartition des coûts de cybercriminalité par pays*

D'après l'étude "Cost of Cyber Crime" d'Accenture et Ponemon Institute, le coût moyen de la cybercriminalité en 2017 varie selon les pays, allant de 5,4 millions de dollars en Australie à 21,1 millions de dollars aux États-Unis. En France, les principales sources de coûts liés à la cybercriminalité sont les logiciels malveillants (22%), suivis du Web (20%), du déni de service (12%), des attaques internes (12%), du phishing et du code malicieux (10% respectivement), des terminaux volés (9%), des ransomwares (5%), et des botnets (2%). Les malwares représentent 98% des incidents, suivis du phishing et de l'ingénierie sociale, des attaques Web et des botnets, touchant les deux tiers des entreprises interrogées. En moyenne, une entreprise subit 130 violations de sécurité par an, avec une augmentation de 27,4% par rapport à 2016. La durée pour corriger les problèmes a augmenté de 50 jours en moyenne pour les incidents internes par rapport à 2016, atteignant 23 jours pour les attaques par ransomware. Les attaques par malware et par le Web sont les plus coûteuses, avec une dépense moyenne de 2,4 et 2 millions de dollars par entreprise, respectivement.

### *Cyberattaque : 14 impacts de coûts selon Deloitte*

L'étude de Deloitte identifie 14 impacts financiers d'une cyberattaque, divisés en coûts visibles et cachés. Les coûts visibles incluent les honoraires d'avocats, la mise en conformité réglementaire, les enquêtes techniques, la sécurité des données client post-incident, les relations publiques, et l'amélioration des dispositifs de cybersécurité.

Les coûts cachés comprennent l'augmentation des primes d'assurance, l'augmentation du coût de la dette, les impacts liés à la perturbation des activités, l'érosion du chiffre d'affaires due à la perte de contrats client, la dépréciation de la valeur de la marque, la perte de propriété intellectuelle, et la perte de la confiance du client. Ces coûts peuvent s'étaler sur cinq ans,

soulignant la durée des effets d'une cyberattaque. La perte d'informations est considérée comme l'effet le plus préjudiciable pour les organisations.

## 5.6 Exemple de cybercibles

### *Équipements Médicaux et Cyberattaques*

Dans la quête d'amélioration des soins et de la performance économique, le secteur de la santé adopte de plus en plus les nouvelles technologies, notamment l'Internet des Objets (IoT). Les établissements de santé sont en première ligne de cette révolution technologique, intégrant l'IoT dans les soins pour bénéficier de nouvelles données au service des patients.

*Adoption de l'IoT dans le Secteur de la Santé :*

- Le secteur de la santé se classe troisième dans l'adoption de l'IoT, avec plus de 60 % des acteurs de la santé ayant introduit des appareils IoT dans leurs organisations.
- En 2019, on prévoit que 87 % des acteurs de la santé auront adopté l'IoT.

*Cybersécurité des Équipements Médicaux :*

- L'augmentation de l'utilisation de l'IoT dans le secteur médical soulève des préoccupations en matière de cybersécurité.
- Certains équipements médicaux connectés, tels que les pacemakers et les pompes à insuline, présentent des vulnérabilités qui pourraient compromettre leur fonctionnement.

*Exemples de Vulnérabilités :*

- En décembre 2016, Johnson & Johnson a contacté 114 000 patients pour corriger une faille dans le boîtier de contrôle d'une pompe à insuline, susceptible d'être exploitée malicieusement pour injecter une dose potentiellement mortelle.
- Des chercheurs en sécurité ont démontré des vulnérabilités, comme le défaut de chiffrement du flux de connexion d'une pompe à insuline, pouvant être intercepté pour injecter des données erronées.

*Actions et Recommandations :*

- Aux États-Unis, la Food and Drug Administration (FDA) a pris des mesures dès 2015, retirant du marché des dispositifs médicaux connectés présentant des risques.

- La FDA recommande aux fabricants de dispositifs médicaux de mettre en œuvre des programmes complets pour gérer les risques de cybersécurité, comprenant l'évaluation des vulnérabilités, la collaboration avec les chercheurs en cybersécurité, la surveillance continue des vulnérabilités, et le déploiement de correctifs.

*En France, Recommandations de la Haute Autorité de Santé (HAS) :*

- La HAS a publié un référentiel de 101 bonnes pratiques pour concevoir des objets connectés médicaux plus sûrs.
- Des exigences strictes sont imposées aux applications et aux processus de transfert et de stockage de données personnelles ou de santé.

### *Principaux critères à respecter pour les applications et objets connectés en santé*

*Qualité et Fiabilité des Informations :*

- Les données récupérées doivent être pertinentes et strictement liées à la fonction de l'application.
- La pseudonymisation doit être appliquée dès la collecte sur le terminal pour rendre les données confidentielles.
- Le chiffrement robuste des données, utilisant des suites cryptographiques, doit être assuré du recueil jusqu'à la transmission à l'hébergeur.
- L'hébergeur agréé doit vérifier l'intégrité et l'authenticité des données transférées.

*Garantie de la Confidentialité et Sécurité des Données Personnelles :*

- Les délais de conservation des données sur le serveur doivent être annoncés à l'utilisateur, avec la possibilité de demander l'arrêt de la collecte et la suppression à tout moment.
- La sécurité du serveur doit être évaluée et adaptée régulièrement.
- En cas de violation de données ou d'incident de sécurité, les autorités compétentes (Anssi, Cnil, autorités judiciaires) doivent être informées.

*Cas des Équipements Hospitaliers :*

- Les équipements hospitaliers, tels que les scanners et les IRM connectés au Web, sont également soumis aux mêmes critères de sécurité.
- Les autorités et les fabricants prennent désormais au sérieux la menace, notamment les infections potentielles par des codes malveillants via Internet ou des clés USB.
- Toutefois, des défis subsistent, notamment la perte d'agrément de santé en cas de modification du système, ce qui peut décourager les clients d'appliquer des correctifs.

## 6. Référence

1. Hennion, R., & Makhlouf, A. (2018, May 17). Cybersécurité. Editions Eyrolles.