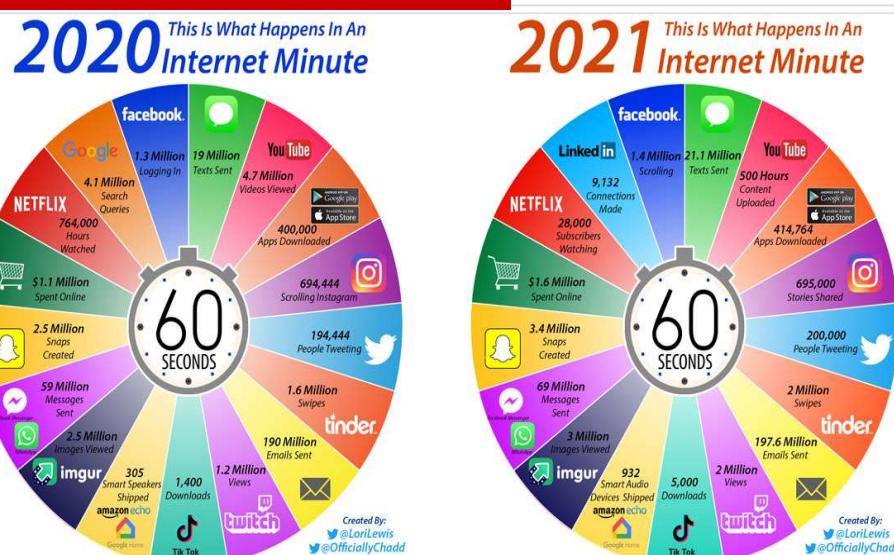
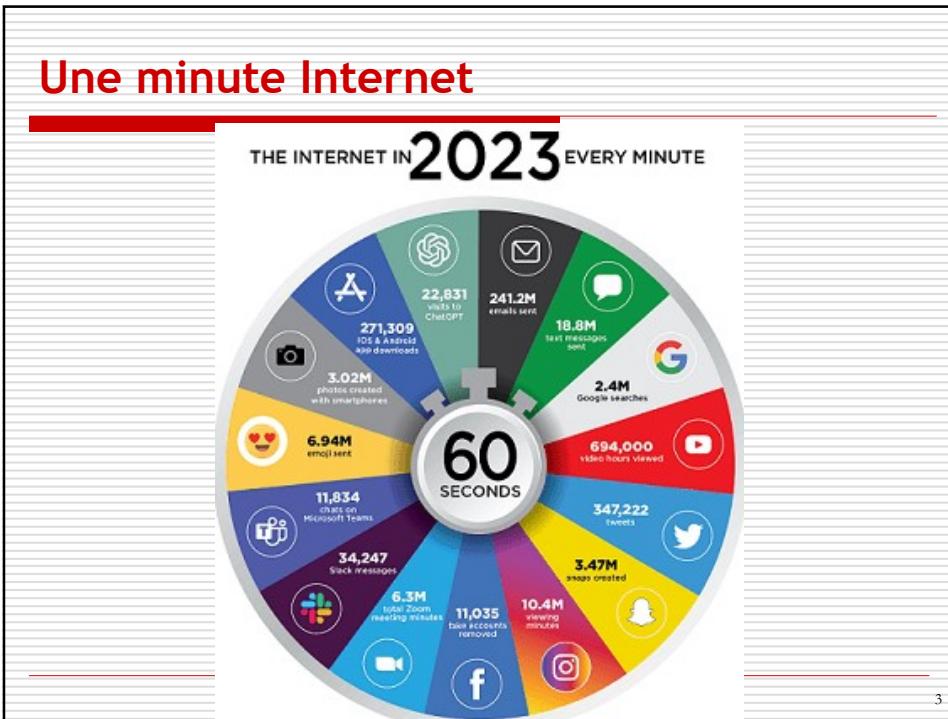


One minute Internet





Motivation pour la sécurité informatique

- Pour les entreprises, la sécurité informatique garantit la confidentialité, l'intégrité et la disponibilité des informations, assurant ainsi la continuité des opérations et la confiance des clients. Elle joue un rôle crucial contre les ransomwares, virus, et autres menaces, en protégeant les actifs numériques et en facilitant la reprise après incident
- Au niveau individuel, avec l'usage généralisé des appareils connectés (smartphones, tablettes, ordinateurs), la sécurité informatique est nécessaire pour protéger les données personnelles contre le vol et les abus. Elle assure aussi la protection des infrastructures critiques, qui sont la base de la société moderne, et contribue à la stabilité économique et politique à plus large échelle

5

Chapter 1

Notions de base sur la sécurité informatique

Progrès technologique & Sécurité requise (1)

- Début du 20ème siècle - années 1940 : Machines électromécaniques et électroniques
 - Progrès technologique : Machines de Turing, premier ordinateur électromécanique Z3 (1941), ENIAC (1946).
 - Sécurité requise : Confidentialité des données sensibles (militaires, calculs scientifiques) par contrôle d'accès physique et réglementations internes. Pas encore de menaces électroniques
- Années 1950-1970 : Premiers systèmes informatiques programmés et microprocesseurs
 - Progrès technologique : Naissance des compilateurs (Grace Hopper), apparition du terme informatique (1962), microprocesseur Intel 4004 (1971), premiers systèmes d'exploitation (UNIX 1969).
 - Sécurité requise : Contrôle d'accès par identifiants simples, premières réflexions sur la protection des données dans les entreprises, disponibilité limitée des systèmes.

7

Progrès technologique & Sécurité requise (2)

- Années 1980-1990 : Informatique personnelle et réseaux émergents
 - Progrès technologique : Premiers PC IBM (1981), développement de TCP/IP et ARPANET, invention du World Wide Web (1989).
 - Sécurité requise : Protection des accès aux ordinateurs personnels, premiers antivirus, sensibilisation aux virus informatiques, rudiments de pare-feu réseau.

8

Progrès technologique & Sécurité requise (3)

- Années 2000 à aujourd'hui : Informatique ubiquitaire et cybersécurité complexe
 - Progrès technologique : Explosion d'Internet, Cloud computing, dispositifs mobiles, intelligence artificielle, IoT
 - Risques : Attaques sophistiquées : ransomwares, phishing, attaques par déni de service distribué (DDoS), vol de données personnelles massives, failles dans les applications cloud et mobiles.
 - Sécurité requise : Politiques de cybersécurité sophistiquées, gestion des vulnérabilités logicielles, protection contre ransomwares, phishing, attaques DDoS, optimisation des pare-feu, monitoring continu des attaques, cryptographie avancée, gestion des identités et accès (IAM), sécurité des données personnelles (RGPD).

9

Principes fondamentaux de la sécurité informatique (1)

- Les principes fondamentaux de la sécurité informatique reposent principalement sur trois axes essentiels, souvent résumés par le sigle CIA :
 - Confidentialité
 - Assurer que seules les personnes autorisées puissent accéder aux ressources. Cela empêche toute divulgation non autorisée des données sensibles.
 - Intégrité
 - Garantir que les données sont exactes, complètes, et n'ont pas été altérées ou corrompues par des accès non autorisés ou des erreurs.
 - Disponibilité
 - Faire en sorte que les systèmes, services et données soient accessibles et fonctionnels lorsque les utilisateurs autorisés en ont besoin.

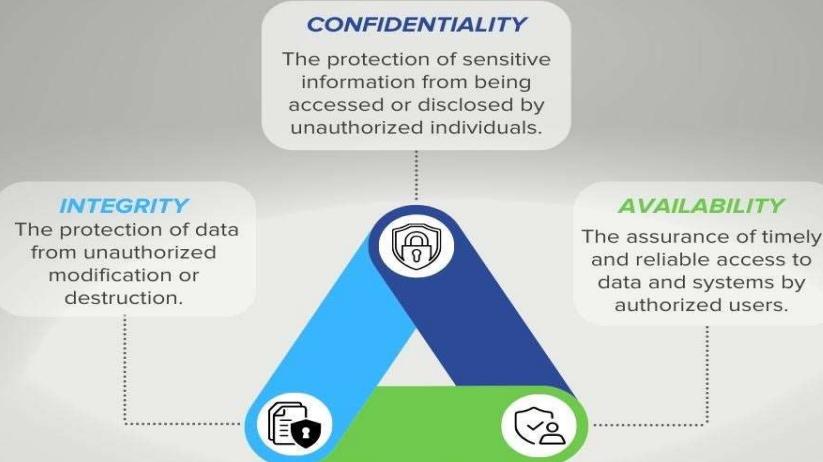
Formule : sécurité = confidentialité + intégrité + disponibilité.

10

Principes fondamentaux de la sécurité informatique (2)



What is the CIA Triad?



Principes fondamentaux de la sécurité informatique (3)

- À ces trois piliers s'ajoutent d'autres notions importantes :
 - **Authentification** : vérifier l'identité des utilisateurs ou systèmes avant d'accorder l'accès.
 - **Gestion des accès et des droits** : contrôler précisément qui peut faire quoi sur les systèmes et données.
 - **Non-répudiation** : garantir qu'une action ou communication ne puisse être niée ultérieurement par son auteur.
 - **Gestion des risques** : identifier et évaluer les menaces pour adopter des mesures adaptées.

Sécurité informatique

« La sécurité informatique consiste à garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu » JF Pillou

But

Préserver la **confidentialité**, la **disponibilité** et l'**intégrité** des ressources d'un système

Comment?

- Analyse de vulnérabilités et d'attaques
- Mise en œuvre de moyens humains, organisationnels et techniques en prévention de la menace

Pourquoi

- La valeur des biens, des données et des services informatisés
- Si ces données et services sont perdus, volés ou altérés, quelles seront les conséquences ?

Sécurité informatique & cybersécurité !

- La **cybersécurité** est un **sous-ensemble** de la sécurité informatique, qui se concentre plus précisément sur la protection contre les menaces **venant d'Internet** ou du **cyberespace**, comme les malwares, ransomwares, phishing et autres cyberattaques

Notions de base (1)

- **Vulnérabilité, brèche ou faille:** représente le niveau d'exposition face à la menace dans un contexte particulier: n'importe quel défaut matériel ou logiciel qui laisse le réseau ouvert pour une potentielle exploitation
- **Menace:** il s'agit de toute intention ou méthodes utilisées pour exploiter une vulnérabilité/faiblesse dans un système. Une menace peut être accidentelle ou intentionnelle.
- **Botnet:** groupe d'ordinateurs infectés et contrôlés par un pirate à distance
- **Malware :** désigne tout programme informatique conçu pour infecter et endommager l'ordinateur d'un utilisateur légitime de multiples façons

15

Notions de base (2)

- **Contremesures:** ensemble d'actions mises en œuvre en prévention de la menace
- **Patch**
 - Correctif de la vulnérabilité par mise à jour
- **Risque**
 - Une équation simple

$$\text{Risque} = \frac{\text{Menace} \times \text{Vulnérabilité}}{\text{Contre mesure}} \times \text{impact}$$

16

Exemple

- Dans le cas d'une authentification d'un utilisateur pour accéder à son compte mail :
 - **Vulnérabilité** : envoie de mot de passe non chiffré à travers le réseau
 - **Menace** : détournement du mot de passe
 - **Attaque** : interception du mot de passe par un pirate qui écoute la communication (man-in-the-middle)
 - **Contre-mesure** : chiffré le mot de passe avant de l'envoyer

17

Types de vulnérabilités des systèmes

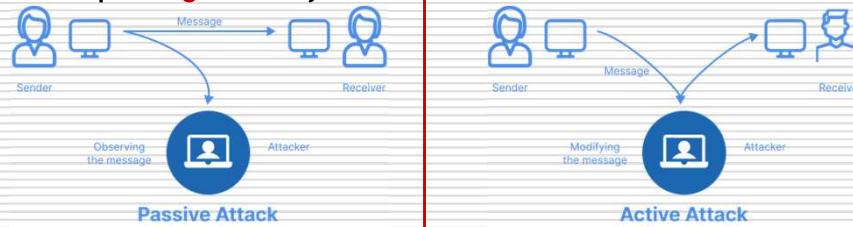
- **Vulnérabilités technologiques**
 - Hardware, logiciel et réseau
 - Mauvaise conception
 - Erreur d'implémentation (Bugs)
 - Exemple :
 - Erreur de dépassement de tampon
 - injection SQL
 - cross site scripting

- **Vulnérabilités organisationnelles**
 - Manque de documents formels, de procédures, de manuels de travail de validation et de maintenance suffisamment détaillés pour faire face aux problèmes de sécurité
 - Manque de procédures en cas d'anomalies, de pannes, etc.

18

Attaques informatique (1)

- L'attaque informatique peut viser un **système**, un **réseau** ou un **appareil informatique** pour en compromettre la **confidentialité/ou l'intégrité et/ou la disponibilité**
- On distingue deux grands types d'attaques selon la manière dont l'attaquant **agit** sur le système :



- Ces deux types d'attaques sont complémentaires et souvent combinés dans des attaques complexes : d'abord une attaque passive pour recueillir des informations, puis une attaque active pour exploiter les vulnérabilités découvertes.

19

Attaques informatique (2)

□ Attaque passive

- L'attaquant intercepte, observe ou collecte des informations sans modifier ou perturber le système ciblé.
- **Objectif** : espionnage, vol de données, écoute clandestine.
- **Exemple** : interception de communications (sniffing), espionnage de mots de passe Wi-Fi, écoute sur le réseau.
- **Caractéristique** : difficile à détecter car elle ne laisse pas de trace ni dégradation visible.
- **Impact prioritaire** : menace sur la **confidentialité**.

20

Attaques informatique (3)

- Quelles sont les étapes pour détecter une attaque passive?**
- Voici les étapes principales pour détecter une attaque passive en sécurité informatique :
 - Surveiller constamment le trafic réseau à la recherche d'anomalies inhabituelles. Un flux excessif ou un comportement suspect peut indiquer une interception ou une écoute clandestine des données.
 - Analyser les journaux et logs système afin d'identifier des accès ou requêtes inhabituelles. Les attaques passives **ne modifiant pas** les données, la détection repose souvent sur la **corrélation d'activités inhabituelles**.

21

Attaques informatique (4)

- Attaque active**
 - L'attaquant intervient directement en modifiant, perturbant ou détruisant les ressources, les données ou fonctions du système.
 - **Objectif** : sabotage, déni de service, injection de code malveillant.
 - **Exemple** : ransomware (chiffrement des données), attaques par déni de service (DoS), modification de bases de données.
 - **Caractéristique** : souvent détectable car cause un impact visible ou interruption.
 - **Impact prioritaire** : menace sur la disponibilité et l'intégrité.

22

Attaques informatique (5)

- Une attaque peut être perpétrée par l'intérieur ou de l'extérieur de l'organisation.
 - Une «**attaque interne**» est une attaque initiée par une entité dans le périmètre de sécurité, c'est-à-dire une entité autorisée à accéder aux ressources du système mais qui les utilise d'une manière non approuvée par ceux qui ont accordé l'autorisation.
 - Une «**attaque extérieure**» est initiée depuis l'extérieur du périmètre, par un utilisateur non autorisé ou illégitime du système

23

Principaux types d'attaquants (Hacker) (1)

- **Hackers à chapeau noir (Black Hat)** : ce sont des individus malveillants qui exploitent les failles pour voler, détruire ou compromettre les systèmes à des fins financières ou de sabotage.
- **Hackers à chapeau gris (Gray Hat)** : ils naviguent entre le légal et l'illégal, révélant parfois des failles pour obtenir une récompense ou démontrer leurs compétences, sans intention purement malveillante.
- **Hacktivistes** : attaquent les systèmes pour soutenir des causes idéologiques, politiques ou sociales, avec pour but de diffuser un message ou dénoncer une injustice.

24

Principaux types d'attaquants (Hacker) (2)

- **Cybercriminels organisés** : groupes structurés, souvent motivés par le profit, menant des campagnes de phishing, d'extorsion ou des attaques par ransomware.
- **États-nations (cyberespions)** : organisations gouvernementales qui ciblent des infrastructures critiques ou des bases de données sensibles pour l'espionnage ou la déstabilisation.

25

Principaux types d'attaquants (Hacker) (3)

- Le **white hacker** n'a pas été listé précédemment car on parle souvent des types d'attaquants en référence aux acteurs malveillants ou ambivalents. Le white hacker, ou hacker éthique, diffère fondamentalement des autres types d'attaquants :
 - Il agit avec l'autorisation des propriétaires des systèmes qu'il teste.
 - Son but est de découvrir les vulnérabilités de façon légale pour aider à renforcer la sécurité.
 - Il utilise les mêmes techniques que les hackers malveillants mais dans un cadre légal et éthique.
 - Il travaille pour prévenir les attaques, souvent dans des programmes de "bug bounty" où il est récompensé pour ses découvertes.

26

Données, ressources matérielles et logicielles et sécurité

27

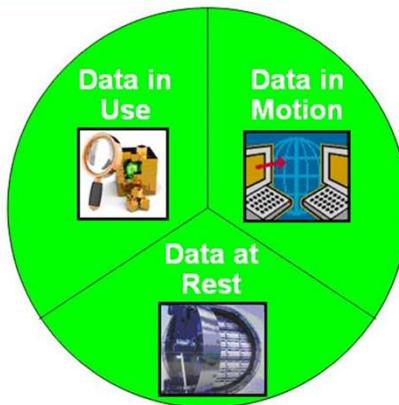
Types de données à protéger



28

Les états de la data

Data in Use:
Active data under constant change stored physically in databases, data warehouses, spreadsheets etc.



Data in Motion:
Data that is traversing a network or temporarily residing in computer memory to be read or updated.

Data at Rest:
Inactive data stored physically in databases, data warehouses, spreadsheets, archives, tapes, off-site backups etc.

29

Ressources et violation de la sécurité

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.		
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

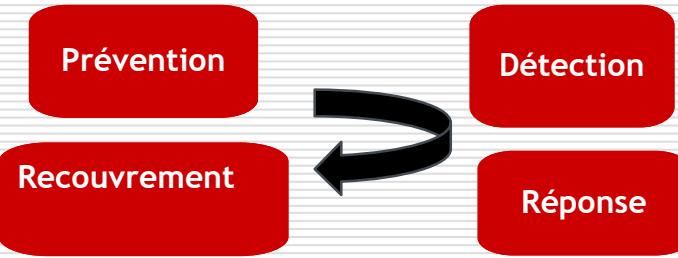
30

Implémentation de la sécurité

31

Gestion des menaces et incidents de la sécurité informatique (1)

- L'implémentation de la sécurité informatique s'articule autour de quatre phases clés : **prévention, détection, réponse et récupération**. Ces phases permettent de couvrir le cycle complet de gestion des menaces et incidents de la sécurité informatique



32

Gestion des menaces et incidents de la sécurité informatique (2)

Prévention

- La prévention vise à réduire les vulnérabilités en mettant en place des mesures de protection telles que les pare-feux, le chiffrement, les mises à jour régulières, les contrôles d'accès stricts, ainsi que la sensibilisation et la formation des utilisateurs. L'objectif est de minimiser la surface d'attaque et d'éviter que les incidents ne surviennent

Détection

- La détection consiste à identifier rapidement les incidents de sécurité grâce à des outils de surveillance continue comme les systèmes de détection d'intrusions (IDS), les journaux d'événements, les solutions SIEM (Security Information and Event Management) ou les services de détection et réponse gérées (MDR). Cette phase est cruciale pour reconnaître et analyser une violation avant qu'elle ne se propage

33

Gestion des menaces et incidents de la sécurité informatique (3)

Réponse

- Une fois un incident détecté, la réponse vise à contenir et neutraliser la menace. Cela inclut l'isolement des systèmes affectés, la suppression des codes malveillants, la correction des vulnérabilités exploitées. La réponse doit être rapide et coordonnée pour limiter l'impact opérationnel et financier, en suivant un plan de réponse aux incidents bien défini

Récupération

- Enfin, la récupération se concentre sur la restauration des systèmes et des services affectés pour reprendre normalement les activités. Elle implique souvent la restauration des données à partir de sauvegardes et la vérification de l'intégrité post-incident. Des tests réguliers du plan de reprise après sinistre (DRP) garantissent une capacité efficace de récupération

34

Gestion des menaces et incidents de la sécurité informatique (4)

Phase	Objectif principal	Moyens typiques
Prévention	Éviter les incidents	Pare-feux, chiffrement, mises à jour, formations
Détection	Identifier rapidement les incidents	IDS, SIEM, journaux, surveillance continue
Réponse	Confinement et neutralisation de la menace	Isolation, suppression d'attaques, plan de réponse
Récupération	Restaurer les systèmes et activités normales	Sauvegardes, tests DRP, contrôle d'intégrité

35

Security Policy

- formal statement of rules and practices that specify or regulate security services
- factors to consider:
 - value of the protected assets
 - vulnerabilities of the system
 - potential threats and the likelihood of attacks
- trade-offs to consider:
 - ease of use versus security
 - cost of security versus cost of failure and recovery

36

36

Security Policy types

Security Policy types

- 1. Identification and Authentication Policies
- 2. Password Policies
- 3. Acceptable Use Policies
- 4. Remote Access Policies
- 5. Network Maintenance Policies
- 6. Incident Handling Policies

37

37

**Comment appliquer la confidentialité,
intégrité et disponibilité en entreprise?**

38

Confidentialité

- Pour appliquer les principes de confidentialité, intégrité et disponibilité (CIA) en entreprise, voici des pratiques clés associées à chaque principe :
 - Confidentialité
 - Mettre en place des mécanismes d'authentification forte (mots de passe robustes, authentification multifactorielle).
 - Chiffrer les données sensibles, en transit (SSL/TLS) et au repos (cryptage des bases de données).
 - Définir des politiques d'accès basées sur les rôles (RBAC), limitant l'accès aux informations selon les responsabilités.
 - Former les employés sur la confidentialité des données (sensibilisation aux risques de phishing, protection des accès).

39

Intégrité & Disponibilité

- Intégrité
 - Utiliser des contrôles d'intégrité comme les sommes de contrôle (hash) pour détecter toute altération des fichiers ou données.
 - Mettre en place des systèmes de journalisation et audit pour retracer les modifications et actions réalisées.
 - Déployer des mécanismes de sauvegarde régulière et testée des données pour pouvoir restaurer les états intacts
- Disponibilité
 - Assurer une redondance des infrastructures (serveurs, réseaux) pour éviter les interruptions.
 - Installer des solutions de protection contre les attaques par déni de service (DDoS).
 - Organiser des procédures de continuité d'activité (PCA) et de reprise après sinistre (PRA).
 - Monitorer en temps réel la performance et la santé des systèmes pour anticiper les pannes.

40