Université de Technologie d'Abidjan

SÉCURITÉ DES SYSTÈMES D'INFORMATION

Enseignante: Dr KIE VICTOIRE

Enseignant-chercheur à ESATIC

OBJECTIFS DU COURS

Ce cours a pour objectif de fournir aux étudiants une compréhension théorique et pratique des principes fondamentaux de la sécurité des systèmes d'information (SSI).

À l'issue du cours, les étudiants seront capables de:

•Identifier les concepts clés de la SSI, tels que la confidentialité, l'intégrité et la disponibilité

•Comprendre les différentes menaces et attaques contre les systèmes d'information

•Mettre en œuvre des mesures de sécurité pour protéger les systèmes d'information

Prérequis : Concepts de base en informatique et réseaux.

PLAN DU COURS

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

1. Définition de la SSI
2. Importance de la SSI
3. Menaces et vulnérabilités des systèmes d'information
4. Principes de base de la SSI

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

1. Définition d'un Système d'Information

Un système d'information (SI) est ensemble des ressources destinées à ***collecter***, ***classifier***, ***stocker***, ***gérer***, ***diffuser*** les informations au sein d'une organisation.
Le S.I. doit permettre et faciliter la mission de l'organisation

❑ Composants d'un Système d'Information

➢ Matériel (Hardware)

- **Ordinateurs et Serveurs** : Machines physiques qui exécutent les applications et stockent les données.

- **Périphériques** : Imprimantes, scanners, modems, routeurs, etc., qui permettent l'entrée, la sortie et la communication des informations

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

1. Définition d'un Système d'Information

❑ Composants d'un Système d'Information

➢ Logiciel (Software)

- **Systèmes d'exploitation :** Programmes qui gèrent le matériel et les ressources logicielles de l'ordinateur (Windows, Linux, macOS).
- **Applications :** Logiciels spécifiques aux besoins des utilisateurs (suites bureautiques, logiciels de gestion, ERP, etc.)

➢ Données (Data)

- **Bases de données** : Systèmes qui stockent et organisent les données.
- **Informations** : Données structurées et non structurées nécessaires aux opérations et à la prise de décisions

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

1. Définition d'un Système d'Information

❑ Composants d'un Système d'Information

➢ Personnes (People)

- **Utilisateurs :** Employés, clients, fournisseurs, partenaires qui interagissent avec le système.
- **Administrateurs :** Personnes responsables de la gestion, de la maintenance et de la sécurité du SI.

➢ Procédures (Procedures)

- **Règles et Politiques :** Directives qui régissent l'utilisation et la gestion du système d'information.
- **Processus :** Séquences d'actions nécessaires pour réaliser des tâches spécifiques (par exemple, la gestion des commandes, le traitement des factures)

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

1. Définition d'un Système d'Information

❑ Composants d'un Système d'Information

➢ Réseaux (Networks)

Réseaux (Networks)Infrastructures de communication : Internet, intranet, réseaux locaux (LAN), réseaux étendus (WAN) qui permettent l'échange de données entre les différentes composantes du système

❑ Importance des Systèmes d'Information

➢ Efficacité Opérationnelle

- **Automatisation des processus** : Réduction des tâches manuelles, amélioration de la productivité.
- **Coordination des activités :** Meilleure synchronisation entre les différentes fonctions de l'entreprise.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

1. Définition d'un Système d'Information

❑ Importance des Systèmes d'Information

➢ Prise de Décision

- **Support à la décision :** Fourniture de données précises et en temps réel pour des décisions éclairées.
- **Analyse des tendances :** Identification des tendances et des modèles à partir des données historiques..

➢ Avantage Concurrentiel

- **Innovation et Adaptabilité** : Capacité à innover et à s'adapter rapidement aux changements du marché grâce à une information fiable.
- **Service Client Amélioré** : Meilleure compréhension et réponse aux besoins des clients

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

1. Définition d’un Système d’Information

❑ Importance des Systèmes d'Information

➢ Conformité et Gestion des Risques

- **Respect des Réglementations :** Aide à la conformité avec les lois et régulations

- **Gestion des risques :** Identification et atténuation des risques grâce à une surveillance et une analyse continue.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

2. Définition de la Sécurité des Systèmes d'Information

La sécurité du système d'information (SSI), aussi appelée sécurité informatique, est l'ensemble des moyens mis en œuvre pour ***protéger*** un système d'information contre les ***menaces***.

Imaginez un système d'information comme une grande maison remplie de trésors précieux **(vos données)**. La sécurité des systèmes d'information (SSI) est comme les ***serrures***, les ***alarmes*** et les ***gardiens*** qui protègent cette maison contre les cambrioleurs (menaces).

En d'autres termes, la SSI vise à:

- **Protéger** vos données contre les fuites, les modifications ou les destructions.
- **Garder** votre système informatique en état de marche, afin que vous puissiez toujours accéder à vos données et les utiliser.
- **Assurer** la confidentialité, afin que seules les personnes autorisées puissent accéder à vos données.

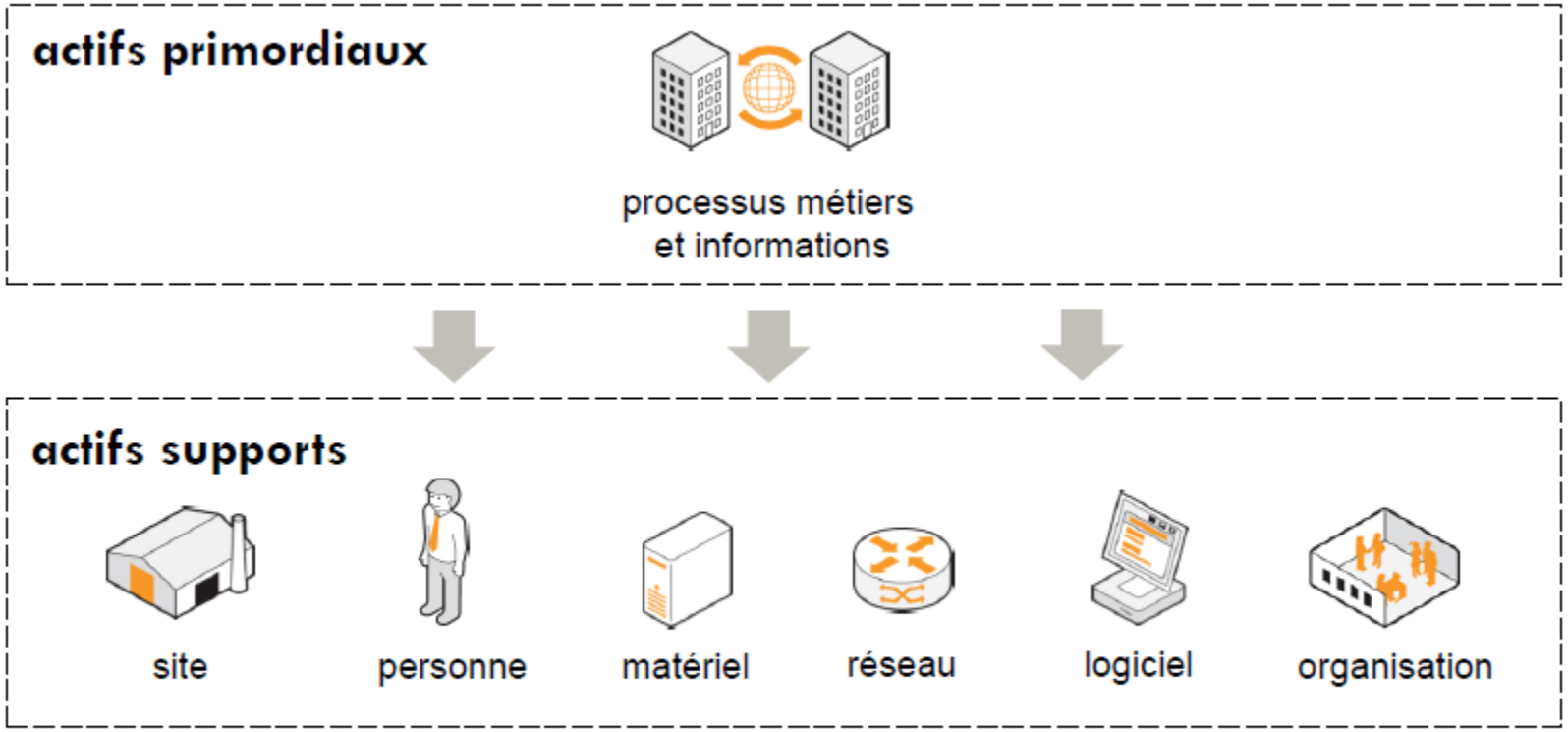
CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

2. Définition de la Sécurité des Systèmes d'Information

Les actifs primordiaux sont les éléments essentiels au bon fonctionnement de l'organisation et qui ont une valeur importante pour l'entreprise.

Les actifs supports sont les éléments qui permettent aux actifs primordiaux de fonctionner correctement.

La sécurité du S.I. consiste donc à assurer la sécurité de l'ensemble de ces biens.



Système d'information d'une organisation

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

3. Importance de la SSI

La sécurisation d'un système d'information (SSI) est d'une importance capitale pour les organisations de toutes tailles et de tous secteurs d'activité. En effet, les SI sont devenus essentiels au bon fonctionnement des entreprises, stockant des données sensibles, gérant des processus critiques et reliant les employés, clients et partenaires

Négliger la sécurité du SI peut avoir des conséquences graves, telles que :

- **Fuites de données et atteintes à la réputation :** Le vol ou la divulgation de données confidentielles, telles que des informations financières ou des données personnelles, peuvent ternir la réputation d'une organisation et entraîner une perte de confiance de la part des clients, partenaires et investisseurs.
- **Perte de productivité et interruptions d'activité** : Une cyberattaque réussie peut paralyser les opérations d'une entreprise, entraînant des pertes financières importantes et une interruption des services aux clients

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

3. Importance de la SSI

- **Atteintes à la conformité réglementaire:** De nombreuses lois et réglementations, imposent des exigences strictes en matière de protection des données et de sécurité des SI. Le non-respect de ces réglementations peut entraîner des amendes importantes, des poursuites judiciaires et d'autres sanctions.

- **Atteinte à l'innovation et à l'avantage concurrentiel**: Les entreprises qui ne protègent pas adéquatement leurs SI peuvent devenir des cibles faciles pour les cybercriminels, ce qui peut freiner l'innovation et leur donner un désavantage concurrentiel.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

3. Importance de la SSI

En revanche, investir dans la sécurisation du SI offre de nombreux avantages, tels que :

- **Protection des données critiques et des actifs :** La SSI permet de protéger les données sensibles contre les accès non autorisés, les fuites et les altérations, préservant ainsi la confidentialité, l'intégrité et la disponibilité des informations.

- **Continuité des opérations et résilience :** Un SI sécurisé est plus résistant aux cyberattaques et aux pannes système, ce qui permet aux entreprises de poursuivre leurs activités en cas d'incident.

- **Conformité réglementaire et réduction des risques juridiques** : La mise en œuvre de mesures de sécurité adéquates permet aux entreprises de se conformer aux réglementations en vigueur et de minimiser les risques de sanctions et de poursuites judiciaires.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

3. Importance de la SSI

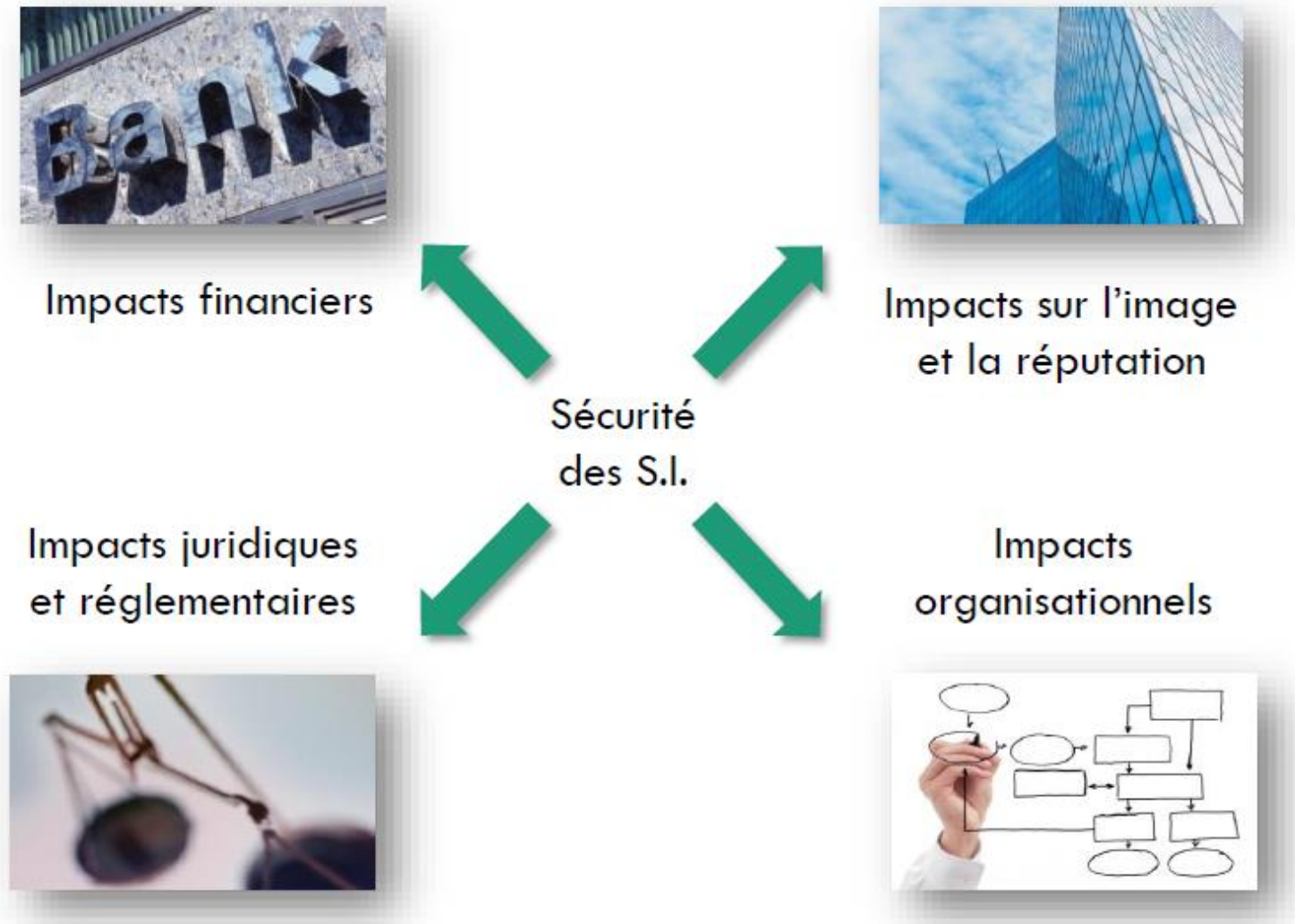
En revanche, investir dans la sécurisation du SI offre de nombreux avantages, tels que :

- **Renforcement de la confiance des clients et partenaires :** En démontrant leur engagement envers la sécurité des données, les entreprises peuvent gagner la confiance de leurs clients, partenaires et investisseurs.

- **Avantage concurrentiel et stimulation de l'innovation :** Un SI sécurisé permet aux entreprises de se concentrer sur l'innovation et la croissance, en sachant que leurs données et leurs systèmes sont protégés.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

3. Importance de la SSI



CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

4. Menaces et vulnérabilité des systèmes d’information

❑ Vulnérabilité

Faiblesse au niveau d’un bien (au niveau de la conception, de la réalisation, de l’installation, de la configuration ou de l’utilisation du bien).

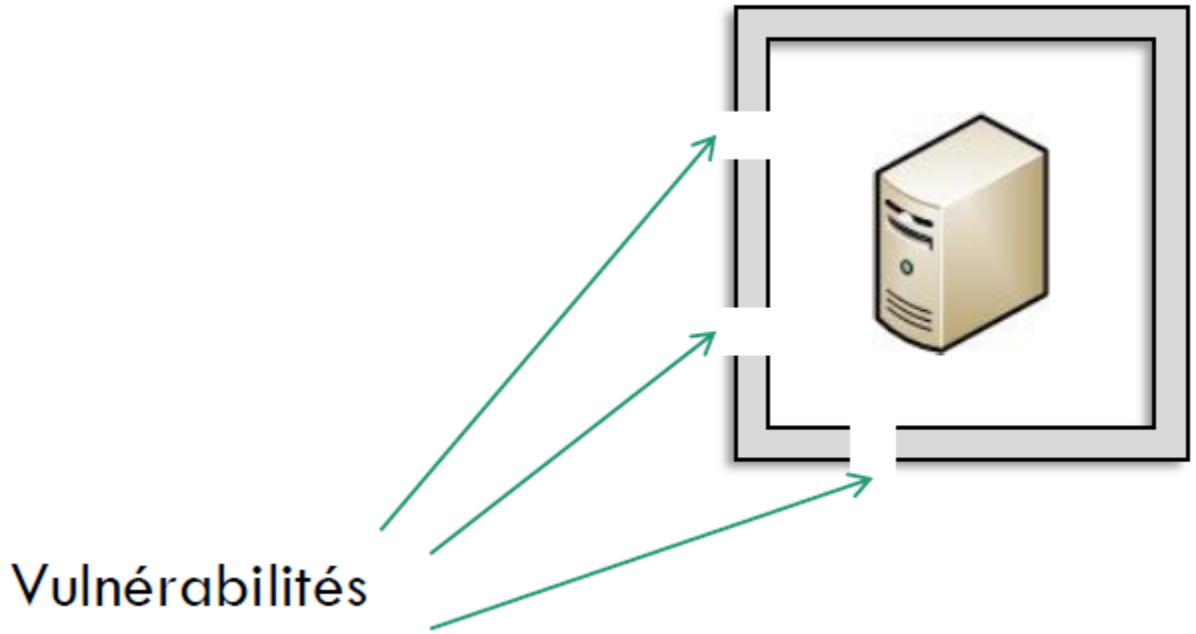
Une vulnérabilité, dans le contexte des SI, est une ***faiblesse*** ou une ***faille*** dans un système, une application, un réseau ou un processus qui peut être exploitée par une menace pour compromettre la sécurité. Cette exploitation peut conduire à des accès non autorisés, des modifications, des destructions de données, ou d'autres impacts néfastes sur la confidentialité, l'intégrité, et la disponibilité des informations et des services.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

4. Menaces et vulnérabilité des systèmes d'information

❑ Vulnérabilité

Faiblesse au niveau d'un bien (au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation du bien).

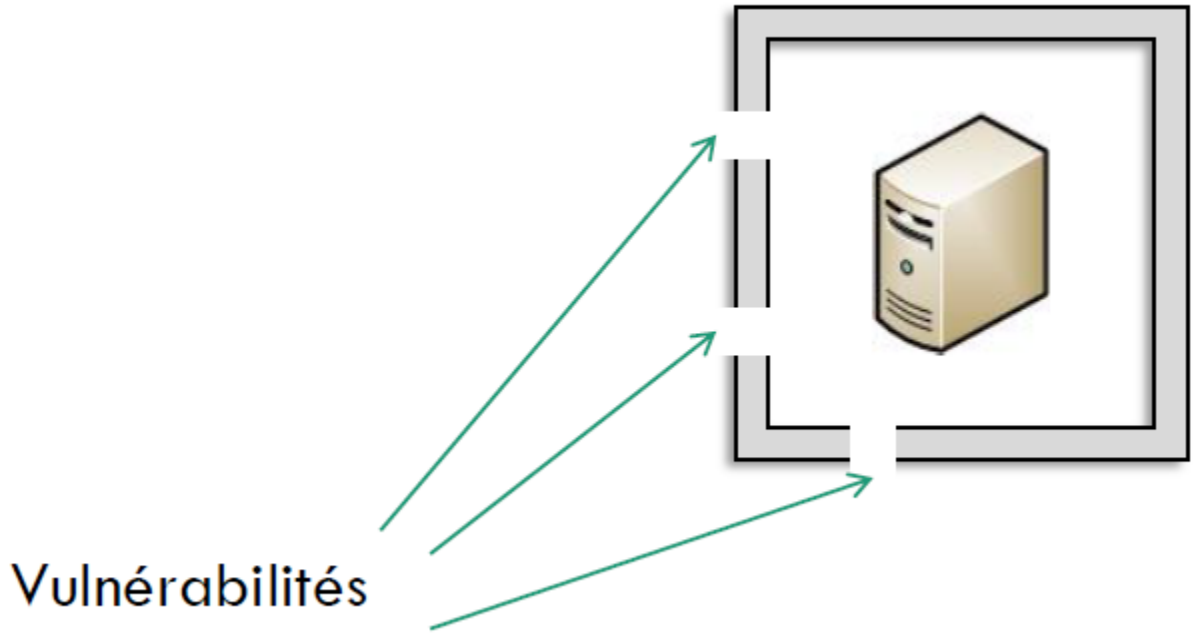


CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

4. Menaces et vulnérabilité des systèmes d'information

❑ Vulnérabilité

Faiblesse au niveau d'un bien (au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation du bien).



CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

4. Menaces et vulnérabilité des systèmes d'information

❑ Types de vulnérabilités

- **Vulnérabilités logicielles** : Failles ou erreurs dans le code d'un logiciel ou d'une application qui peuvent être exploitées pour exécuter des actions non autorisées. Par exemple, des bugs, des erreurs de configuration, ou des omissions de sécurité dans le code.

- **Vulnérabilités matérielles** : Faiblesses dans les composants physiques d'un système informatique. Cela peut inclure des défauts de fabrication, des conceptions obsolètes ou des pannes matérielles.

- **Vulnérabilités réseau** : Failles dans les protocoles de communication ou les configurations de réseau qui permettent à des attaquants d'intercepter, modifier ou bloquer les données en transit.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

4. Menaces et vulnérabilité des systèmes d’information

❑ Types de vulnérabilités

- **Vulnérabilités humaines :** Comportements ou erreurs des utilisateurs qui peuvent compromettre la sécurité. Cela inclut des pratiques de mot de passe faibles, le manque de sensibilisation à la sécurité ou des erreurs de configuration.

- **Vulnérabilités procédurales** : Failles dans les processus ou les procédures de gestion de la sécurité. Cela peut inclure des politiques de sécurité insuffisantes, des procédures de mise à jour de sécurité inadéquates ou des audits de sécurité peu fréquents.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

4. Menaces et vulnérabilité des systèmes d'information

❑ Exemples de vulnérabilités

- **Logiciel non mis à jour :** Ne pas appliquer les mises à jour ou les correctifs de sécurité disponibles pour les logiciels et systèmes d'exploitation.
- **Mots de passe faibles :** Utilisation de mots de passe simples ou facilement devinables, comme "123456" ou "password".
- **Absence de chiffrement** : Transmettre des données sensibles en clair sans chiffrement.
- **Permissions excessives** : Attribuer des droits d'accès trop élevés à des utilisateurs qui n'en ont pas besoin.
- **Phishing** : Exploitation de la confiance des utilisateurs pour obtenir des informations sensibles via des courriels ou des sites web frauduleux.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

4. Menaces et vulnérabilité des systèmes d'information

❑ Gestion des vulnérabilités

- **Identification :** Utilisation d'outils de scan et d'audits de sécurité pour détecter les vulnérabilités.
- **Évaluation :** Analyse des vulnérabilités identifiées pour déterminer leur gravité et l'impact potentiel.
- **Remédiation :** Application de correctifs, mises à jour ou autres mesures pour corriger les vulnérabilités.
- **Surveillance :** Mise en place de systèmes de surveillance pour détecter et réagir rapidement aux tentatives d'exploitation des vulnérabilités**.**
- **Sensibilisation :** Formation continue des utilisateurs et des administrateurs sur les meilleures pratiques de sécurité et les menaces émergentes.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

4. Menaces et vulnérabilité des systèmes d’information

❑ Les menaces

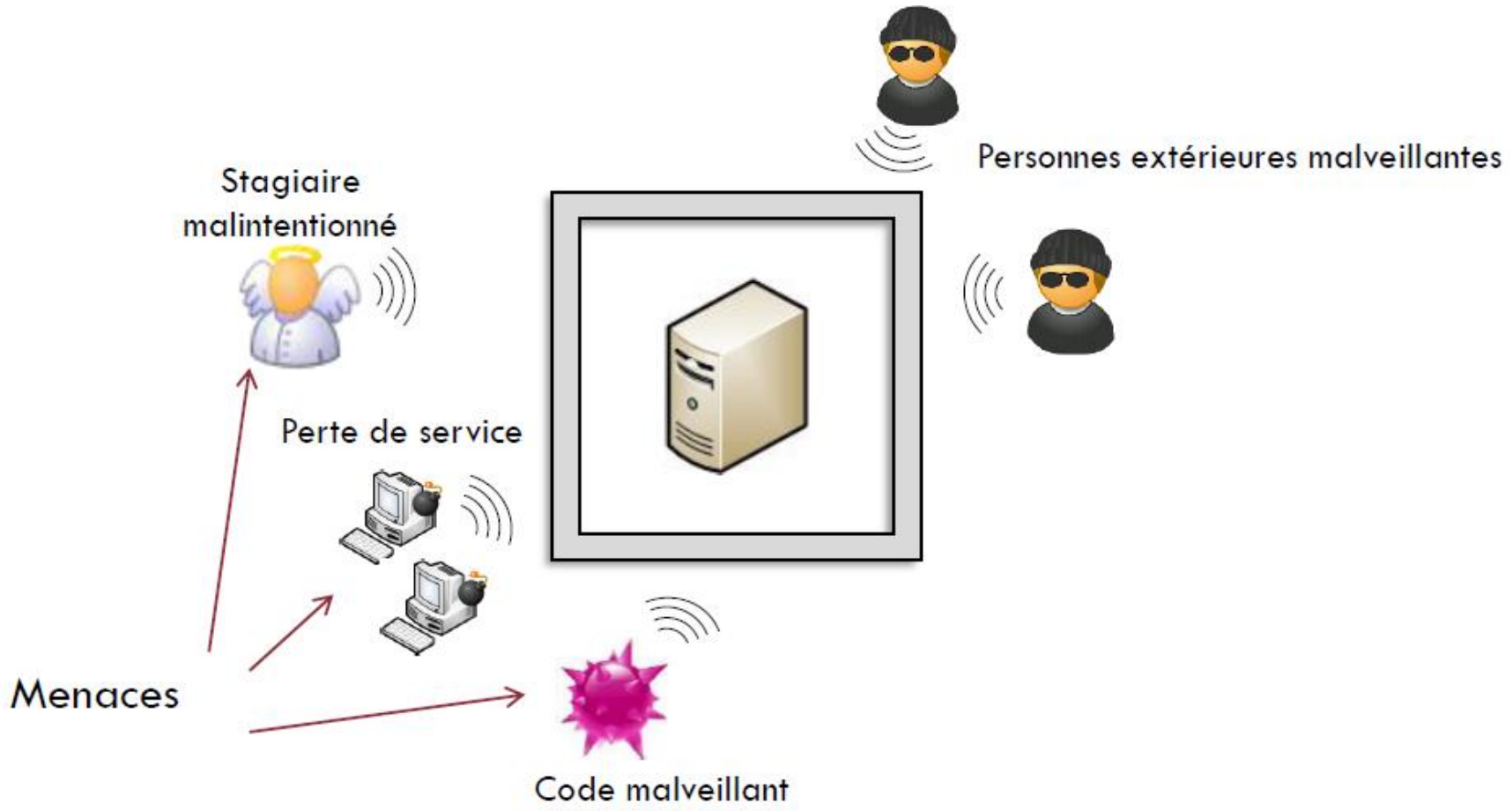
Cause potentielle d’un incident, qui pourrait entrainer des dommages sur un bien si cette menace se concrétisait.

Les menaces sont des ***agents***, des ***conditions*** ou des ***événements*** susceptibles de causer des dommages à un système d'information. Elles peuvent être intentionnelles ou accidentelles, et proviennent de sources variées, y compris des individus malveillants, des erreurs humaines, des défaillances techniques et des catastrophes naturelles.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

4. Menaces et vulnérabilité des systèmes d'information

❑ Les menaces



CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

4. Menaces et vulnérabilité des systèmes d’information

❑ Types de Menaces

➢ Menaces Humaines Intentionnelles

- **Hackers** : Individus ou groupes cherchant à exploiter les vulnérabilités des systèmes pour un gain personnel ou pour causer des perturbations.

- **Espionnage** : Actes de surveillance illégale visant à obtenir des informations confidentielles.

- **Malveillants internes** : Employés ou collaborateurs ayant accès aux systèmes et qui utilisent ces privilèges pour nuire intentionnellement.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

4. Menaces et vulnérabilité des systèmes d'information

❑ Types de Menaces

➢ **Menaces Humaines Accidentelles**

- **Erreurs de configuration :** Mauvaise configuration des systèmes par les administrateurs qui peut ouvrir des portes aux attaques**.**
- **Fautes humaines :** Actions involontaires comme l'envoi d'informations sensibles à la mauvaise personne ou l'oubli de mettre à jour un système.

➢ **Menaces Logicielles**

- **Malwares** : Logiciels malveillants conçus pour causer des dommages, voler des données ou prendre le contrôle des systèmes (ex. : virus, ransomwares).
- **Vulnérabilités logicielles** : Failles dans les programmes qui peuvent être exploitées pour pénétrer les systèmes

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

4. Menaces et vulnérabilité des systèmes d'information

❑ Types de Menaces

➢ **Menaces Matérielles**

- **Défaillances matérielles :** Pannes de composants critiques du système comme les disques durs, les serveurs ou les réseaux.
- **Vol ou perte de matériel :** Dispositifs contenant des informations sensibles qui sont perdus ou volés.

➢ **Menaces Environnementales**

- **Catastrophes naturelles :** Événements tels que les inondations, les incendies, les tremblements de terre, qui peuvent détruire les infrastructures physiques.

- **Pannes de courant :** Interruption de l'alimentation électrique entraînant des interruptions de service.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

4. Menaces et vulnérabilité des systèmes d’information

❑ Types de Menaces

➢ **Menaces Sociales**

- **Ingénierie sociale :** Tactiques de manipulation psychologique visant à tromper les individus pour qu'ils divulguent des informations sensibles.

- **Phishing :** Techniques de fraude par courriel ou sites web falsifiés pour obtenir des informations personnelles.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

4. Menaces et vulnérabilité des systèmes d’information

❑ Attaques

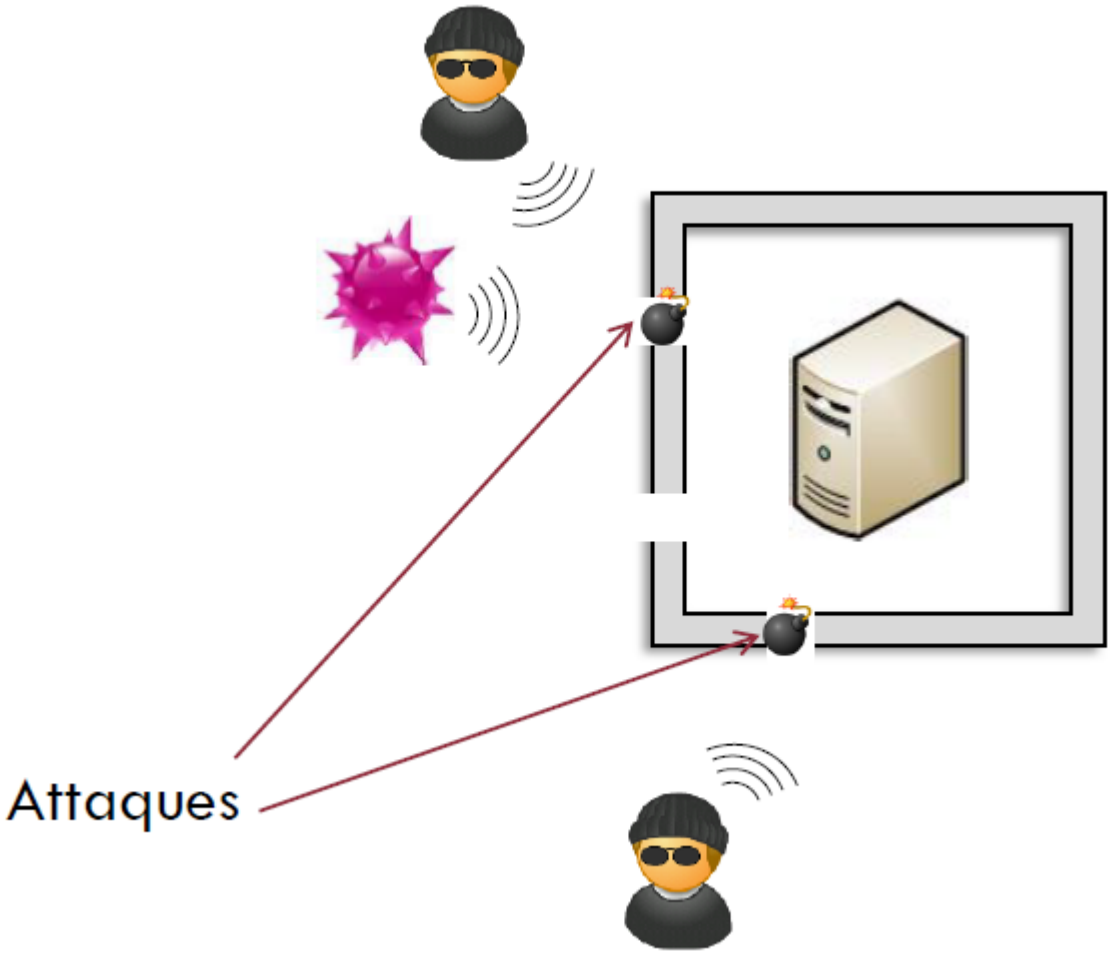
Action malveillante destinée à porter atteinte à la sécurité d’un bien. Une attaque représente la concrétisation d’une menace, et nécessite l’exploitation d’une vulnérabilité.

dans le contexte des systèmes d'information, se réfèrent à toute action délibérée visant à ***perturber***, ***endommager***, ou accéder de manière ***non autorisée*** à un système informatique, à ses données ou à ses services. Les attaques peuvent être menées par des individus ou des groupes avec des motivations variées, telles que le vol d'informations, l'extorsion, le sabotage ou la démonstration de compétences techniques.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

4. Menaces et vulnérabilité des systèmes d'information

- ❑ **Attaques**



CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

4. Menaces et vulnérabilité des systèmes d’information

❑ Types d'Attaques

➢ Attaques Logicielles

- **Malwares** : Logiciels malveillants comme les virus, les vers, les chevaux de Troie, et les ransomwares qui infectent les systèmes pour les endommager ou en prendre le contrôle.
- **Spywares** : Logiciels espions conçus pour surveiller les activités des utilisateurs et voler des informations sensibles.

➢ Attaques par Ingénierie Sociale

- **Phishing** : Tentatives de tromper les utilisateurs pour qu'ils divulguent des informations personnelles en se faisant passer pour des entités de confiance.
- **Spear Phishing** : Version plus ciblée du phishing, visant des individus spécifiques avec des messages personnalisés.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

4. Menaces et vulnérabilité des systèmes d’information

❑ Types d'Attaques

➢ **Attaques de Réseau**

- **Man-in-the-Middle (MitM) :** Interception et altération des communications entre deux parties sans leur consentement.
- **Attaques par déni de service (DoS/DDoS) :** Surcharge des serveurs ou des réseaux pour les rendre indisponibles aux utilisateurs légitimes**.**

➢ **Attaques par Force Brute:** Tentatives répétées de deviner des mots de passe ou des clés de chiffrement en essayant toutes les combinaisons possibles jusqu'à ce que la bonne soit trouvée

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

4. Menaces et vulnérabilité des systèmes d'information

❑ Types d'Attaques

➢ **Attaques Exploitant les Vulnérabilités**

- **Exploits :** Utilisation de failles logicielles connues pour accéder de manière non autorisée à un système ou exécuter du code malveillant**.**
- **Zero-Day Attacks** : Attaques exploitant des vulnérabilités pour lesquelles aucun correctif n'est encore disponible**.**

➢ **Attaques Physiques**

- **Vol ou destruction de matériel :** Accès non autorisé aux équipements informatiques pour voler ou détruire des données.

- **Interférences physiques :** Actions comme la coupure de l'alimentation ou le sabotage de l'infrastructure matérielle.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

4. Menaces et vulnérabilité des systèmes d’information

❑ Types d'Attaques

➢ **Attaques sur les Applications Web**

- **Injection SQL :** Insertion de code malveillant dans les requêtes SQL pour manipuler les bases de données.
- **Cross-Site Scripting (XSS) :** Insertion de scripts malveillants dans des pages web vues par d'autres utilisateurs.

➢ **Attaques de l'Internet des Objets (IoT)**

- **Botnets IoT :** Réseaux d'appareils IoT compromis utilisés pour lancer des attaques à grande échelle comme les DDoS.

- **Accès non autorisé :** Exploitation des vulnérabilités des appareils IoT pour accéder à des réseaux plus larges

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

4. Menaces et vulnérabilité des systèmes d'information

❑ Objectifs des Attaques

Les attaques peuvent avoir divers objectifs, parmi lesquels **:**

- **Vol de données :** Accéder à des informations sensibles comme des données personnelles, financières ou commerciales.

- **Extorsion :** Demander une rançon en échange de la restitution de l'accès ou de la suppression de logiciels malveillants.

- **Sabotage :** Perturber les opérations d'une organisation pour nuire à sa réputation ou à sa productivité.

- **Espionnage :** Obtenir des informations confidentielles pour un avantage stratégique ou concurrentiel

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

5. Principe de base de la SSI

Les principes de base de la sécurité des systèmes d'information visent à protéger les données, les processus et les infrastructures contre diverses menaces

❑ Confidentialité

La confidentialité consiste à garantir que les informations sont accessibles uniquement aux personnes autorisées et à protéger les données sensibles contre l'accès non autorisé.

➢ Mesures de Protection

- **Chiffrement** : Utilisation d'algorithmes pour rendre les données illisibles à quiconque ne possédant pas la clé de déchiffrement.
- **Contrôle d'accès** : Mise en place de politiques et de systèmes de gestion des droits d'accès pour s'assurer que seules les personnes autorisées peuvent accéder aux informations.
- **Authentification** : Vérification de l'identité des utilisateurs via des mots de passe, des cartes à puce, des biométries ou des tokens d'authentification

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

5. Principe de base de la SSI

❑ Intégrité

L'intégrité vise à s'assurer que les données ne sont pas altérées de manière non autorisée et qu'elles demeurent exactes et fiables.

➢ Mesures de Protection

- **Contrôles de version :** Systèmes permettant de suivre et de gérer les modifications apportées aux données.

- **Hachage :** Utilisation de fonctions de hachage pour vérifier que les données n'ont pas été modifiées.

- **Signatures numériques :** Utilisation de signatures cryptographiques pour garantir que les données proviennent d'une source authentique et n'ont pas été altérées.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

5. Principe de base de la SSI

❑ Disponibilité

La disponibilité garantit que les informations et les ressources sont accessibles aux utilisateurs autorisés lorsqu'ils en ont besoin.

➢ Mesures de Protection

- **Redondance :** Implémentation de composants redondants pour éviter les points de défaillance uniques.

- **Sauvegardes :** Réalisation régulière de copies de sauvegarde des données pour prévenir la perte de données.

- **Plans de reprise après sinistre :** Développement de plans pour restaurer les systèmes et les données en cas d'incident majeur.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

5. Principe de base de la SSI

❑ Authenticité

L'authenticité assure que les informations proviennent bien de la source prétendue et que les utilisateurs sont ceux qu'ils prétendent être.

➢ Mesures de Protection

- **Certificats numériques :** Utilisation de certificats délivrés par des autorités de certification pour vérifier l'identité des entités.

- **Protocoles d'authentification :** Utilisation de protocoles sécurisés pour vérifier l'identité des utilisateurs et des systèmes.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

5. Principe de base de la SSI

❑ Non-répudiation

La non-répudiation garantit qu'une partie ne peut nier avoir effectué une action ou envoyé une communication.

➢ Mesures de Protection

- **Journalisation et audit :** Enregistrement des actions et des transactions pour créer des traces d'audit.

- **Signatures numériques :** Utilisation de signatures numériques pour garantir que les messages ou les transactions ne peuvent être contestés

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

5. Principe de base de la SSI

❑ Contrôle d'accès

Le contrôle d'accès régit qui peut accéder aux informations et aux ressources du système d'information.

➢ Mesures de Protection

- **Modèles de contrôle d'accès :** Implémentation de modèles comme le contrôle d'accès basé sur les rôles ou le contrôle d'accès basé sur les attributs s.

- **Politiques de sécurité :** Définition et application de politiques de sécurité strictes pour contrôler l'accès.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

5. Principe de base de la SSI

❑ Sécurité physique

La sécurité physique concerne la protection des infrastructures matérielles et des locaux contre les menaces physiques.

➢ Mesures de Protection

- **Contrôles d'accès physiques :** Utilisation de badges, de cartes d'accès et de contrôles biométriques pour limiter l'accès aux installations.

- **Surveillance et alarmes :** Mise en place de systèmes de surveillance, de détecteurs d'intrusion et d'alarmes pour prévenir et détecter les intrusions.

- **Protection contre les catastrophes :** Conception des installations pour résister aux catastrophes naturelles et aux incidents physiques.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

5. Principe de base de la SSI

- **Sécurité des communications**

La sécurité des communications vise à protéger les données en transit contre les interceptions et les altérations.

- **Mesures de Protection**
- **Chiffrement des communications :** Utilisation de protocoles de chiffrement comme TLS/SSL pour sécuriser les données en transit.

- **VPNs (Virtual Private Networks) :** Création de tunnels sécurisés pour protéger les communications sur des réseaux non sécurisés.

- **Protocoles sécurisés :** Adoption de protocoles sécurisés pour les échanges de données, tels que HTTPS, SFTP, et SSH.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

5. Principe de base de la SSI

❑ Gestion des incidents

La gestion des incidents consiste à détecter, répondre à et récupérer après des incidents de sécurité.

❑ Mesures de Protection

- **Plans de réponse aux incidents :** Développement de plans détaillés pour répondre rapidement et efficacement aux incidents de sécurité.

- **Équipes de réponse aux incidents :** Mise en place d'équipes spécialisées dans la gestion et la résolution des incidents.

- **Analyse post-incident :** Conduite d'analyses pour identifier les causes des incidents et mettre en place des mesures correctives**.**

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

5. Principe de base de la SSI

❑ Conformité

La conformité assure que les systèmes d'information respectent les lois, les réglementations et les normes de l'industrie.

➢ Mesures de Protection

- **Audits réguliers :** Réalisation d'audits internes et externes pour vérifier la conformité**.**

- **Politiques et procédures :** Définition de politiques et de procédures pour garantir le respect des exigences réglementaires.

- **Formation et sensibilisation :** Formation continue du personnel sur les obligations réglementaires et les bonnes pratiques de sécurité.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

5. Principe de base de la SSI

❑ Conformité

La conformité assure que les systèmes d'information respectent les lois, les réglementations et les normes de l'industrie.

➢ Mesures de Protection

- **Audits réguliers :** Réalisation d'audits internes et externes pour vérifier la conformité**.**

- **Politiques et procédures :** Définition de politiques et de procédures pour garantir le respect des exigences réglementaires.

- **Formation et sensibilisation :** Formation continue du personnel sur les obligations réglementaires et les bonnes pratiques de sécurité.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

6. TD1

❑ Exercice 1 : Définitions Clés

Définissez les termes suivants :

- Sécurité des systèmes d'information
- Confidentialité
- Intégrité
- Disponibilité
- Authentification
- Non-répudiation

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

6. TD1

❑ Exercice 1 : Solutions

- **Sécurité des systèmes d'information** : Protection des informations et des systèmes d'information contre les accès non autorisés, les perturbations, les modifications ou les destructions.
- **Confidentialité** : Garantie que les informations ne sont accessibles qu'aux personnes autorisées.
- **Intégrité** : Assurance que les données ne sont pas altérées de manière non autorisée.
- **Disponibilité** : Assurance que les informations et les ressources sont accessibles aux utilisateurs autorisés lorsqu'ils en ont besoin.
- **Authentification** : Vérification de l'identité d'un utilisateur, d'un appareil ou d'une entité.
- **Non-répudiation** : Assurance qu'une partie ne peut nier une action ou une communication qu'elle a effectuée.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

6. TD1

❑ Exercice 2 : Identification des Menaces

Pour chaque scénario suivant, identifiez la menace et expliquez en quoi elle consiste.

- Un employé télécharge un fichier malveillant en cliquant sur un lien dans un courriel de phishing.
- Un hacker utilise une vulnérabilité dans un logiciel pour accéder aux bases de données d'une entreprise.
- Une panne de courant entraîne l'arrêt des serveurs d'une entreprise pendant plusieurs heures

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

6. TD1

❑ Exercice 2 : Solutions

- **Phishing** : Technique de manipulation pour obtenir des informations sensibles en se faisant passer pour une entité de confiance.

- **Exploitation de vulnérabilité** : Utilisation de failles logicielles pour accéder illégalement à des systèmes ou des données.

- **Panne de courant** : Menace environnementale qui peut interrompre la disponibilité des systèmes et des services.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

6. TD1

❑ Exercice 3 : Identification des Vulnérabilités

Identifiez et expliquez les vulnérabilités potentielles dans les situations suivantes :

- Utilisation de mots de passe simples comme "123456" ou "password".
- Ne pas appliquer les mises à jour de sécurité sur un logiciel critique.
- Stocker des informations sensibles sur un serveur non sécurisé.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

6. TD1

❑ Exercice 4 : Application des Principes de Base

Pour chaque principe de sécurité, proposez une mesure de protection correspondante.

- Confidentialité
- Intégrité
- Disponibilité
- Authenticité
- Non-répudiation

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

6. TD1

❑ Exercice 4 : Solutions

Pour chaque principe de sécurité, proposez une mesure de protection correspondante.

- **Confidentialité** : Utilisation du chiffrement pour protéger les données sensibles.
- **Intégrité** : Mise en œuvre de contrôles de version et de hachage pour vérifier l'intégrité des données.
- **Disponibilité** : Utilisation de systèmes redondants et de sauvegardes régulières
- **Authenticité** : Déploiement de certificats numériques et de protocoles d'authentification.
- **Non-répudiation** : Utilisation de signatures numériques et de journaux d'audit.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

6. TD1

❑ Exercice 5 : Analyse de Sécurité d'une Entreprise

Étudiez le cas suivant et répondez aux questions.

Scénario :Une entreprise IVOIRE stocke des données clients sensibles sur ses serveurs. Récemment, ils ont remarqué une augmentation des tentatives de connexion non autorisées. Les employés utilisent souvent des mots de passe faibles et les mises à jour de sécurité ne sont pas appliquées régulièrement. L'entreprise n'a pas de plan de réponse aux incidents.

1. Identifiez les principales menaces auxquelles l'entreprise IVOIRE est confrontée.
2. Quelles sont les vulnérabilités présentes dans le système d'information de l'entreprise IVOIRE ?
3. Proposez un plan d'action pour améliorer la sécurité des systèmes d'information de l'entreprise IVOIRE.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

6. TD1

❑ Exercice 5 : Solutions

1. Principales menaces : Tentatives de connexion non autorisées (brute force, exploitation de vulnérabilités), potentiel d'attaques par phishing, menaces internes (erreurs humaines, employés malveillants).

2. Vulnérabilités : Utilisation de mots de passe faibles, absence de mises à jour de sécurité, absence de plan de réponse aux incidents.

CHAPITRE I: Introduction à la Sécurité des Systèmes d'Information

6. TD1

❑ Exercice 5 : Solutions

3. Plan d'action :

a. **Améliorer** la gestion des mots de passe : Imposer des mots de passe forts et mettre en œuvre l'authentification multi-facteur.
b. **Appliquer** régulièrement les mises à jour de sécurité : Mettre en place un processus de gestion des correctifs.
c. **Développer** et tester un plan de réponse aux incidents : Inclure des procédures pour détecter, répondre et récupérer après des incidents.
d. **Former** les employés : Sensibilisation à la sécurité et aux bonnes pratiques pour éviter les erreurs humaines et les attaques de phishing.
e. **Renforcer** la surveillance et les contrôles d'accès : Utiliser des systèmes de détection des intrusions et des contrôles d'accès rigoureux.