Introduction à la CyberSécurité

Houssem MAHMOUDI
houssem.mahmoudi@ensicaen.fr

Plan du module

Objectifs du module

- Comprendre les concepts fondamentaux de la Cybersécurité.
- Décrire les types de menaces informatiques.
- Comprendre les techniques d'attaques utilisées par les hackers.
- Maîtriser/comprendre des techniques pour sécuriser les données et les communications.
- Comprendre les mécanismes de protection contre les Cyberattaques.
- Savoir sécuriser les réseaux Wifi.

Crénaux

- Cours : 10h
- TD : 2h
- TP : 12 h
- Notes : Examen final & Note des TPs

Chapitre 1

Notions de bases de la Cybersécurité

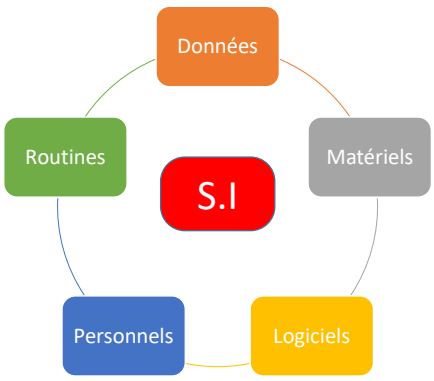
Plan

Généralités

I. Généralités

1. Système d'information

- Un système d'information (**SI**) définit un ensemble organisé des ressources qui permettent de collecter, stocker, traiter et distribuer des informations au sein d'une organisation.
- Un SI est composé de :



I. Généralités

2. La Cybersécurité

- La Cybersécurité est l'ensemble de mesures adoptées pour protéger le SI de l'entreprise contre :
  - Les Cyberattaques,
  - La fuite des données,
  - Les logiciels malveillants,
  - Les accès non autorisés.

I. Généralités

3. Objectifs de la Cybersécurité

- **Protection des données sensibles** : Protéger les données contre les abus, vol, accès non autorisé
- **Prévention des Cyberattaques** : Les attaques **Cybernétiques** peuvent entraîner des pertes financières importantes, des atteintes à la réputation et des interruptions de services.
- **Respect des réglementations** : Des lois et règlements exigent les organisations qu'elle protègent les données personnelles (**RGPD**), audit et conformité.
- **Continuité des activités** : Systèmes, réseaux et services restent opérationnel et disponible en cas d'incidents de sécurité.

I. Généralités

4. Cybercriminels

- Les Cybercriminels peuvent être :
  - Individus,
  - Groupes,
  - Etats.
- Commettent des crimes en utilisant la TIC et Internet, pour atteindre leurs objectifs illégaux.

I. Généralités

4. Cybercriminels

Les différentes catégories de Cybercriminels :

❑ **Script Kiddies :**

- Amateurs, maîtrisant des outils informatiques et souhaitant relever un défi technique en attaquant à des systèmes informatiques.
- Ils utilisent souvent des logiciels d'attaque existant ou des tutoriels trouvés sur Internet pour réaliser certaines attaques.

I. Généralités

4. Cybercriminels

❑ **Hacktivistes :**

- Pirates qui protestent contre les gouvernements et/ou les organisations.
- Exemple :
  - ✓ Anonymous.
  - ✓ LulzSec.
  - ✓ GhostShell

I. Généralités

4. Cybercriminels

❑ **Hackers :**

- **White hats** : Experts en sécurité avec grande compétence technique utilisées pour détecter et corriger les failles de sécurité d'une **manière légale**.
  - ► Améliorer la sécurité du SI et prévenir les cyberattaques.
  - ► Travaillent avec des entreprises ou les gouvernements.
  - ► Respecte la loi et l'éthique.

I. Généralités

4. Cybercriminels

❑ **Hackers :**

- **Black hats** : Cybercriminels qui piratent à des fins malveillantes. Leurs activités se déroulent principalement sur le **Dark web**.
  - ► Volent des données sensibles
  - ► Exploitent les failles de sécurité
  - ► Causer des dommages
  - ► Commettent des actes illégaux

I. Généralités

4. Cybercriminels

❑ **Hackers :**

- **Grey hats** : Pirates agissant parfois dans un bon esprit et parfois non.
  - ► Peuvent agir de manière éthique et parfois personnelle
  - ► Trouvent des failles sans autorisation
  - ► Motivations variables

I. Généralités

5. Les risques Cyber

- Tout risque de perte financière, de perturbation ou d'atteinte à la réputation d'une entreprise résultant d'une défaillance de son Systèmes Informatiques.
- Il existe 4 types de risques Cyber qui cible les particuliers et les entreprises :
  - Cybercriminalité
  - Atteinte à l'image
  - Espionnage
  - Sabotage

I. Généralités

5. Les risques Cyber

a. Cybercriminalité & Atteinte à l'image

- Les attaques de déstabilisation,
- Exfiltration d'informations (Data Breach)
- Défiguration de sites web (Defacement website).

- Conséquence désastreuse pour certaines personnes et pour les entreprises.

I. Généralités

5. Les risques Cyber

b. Espionnage

- Utilisation de techniques plus sophistiqué à des fins économique, ou scientifique.
- Fait par de pirates avancés et peuvent avoir de lourdes conséquences pour les intérêts nationaux, ou économiques pour les entreprises.
- Le but de l'attaquant est de garder son accès le plus longtemps possible afin d'exfiltrer le plus d'informations sensibles.

I. Généralités

5. Les risques Cyber

c. Sabotage

- Perturbation ou destruction de systèmes pour nuire à une entreprise, une infrastructure critique, ou un État.
- Exemple : Attaque par Ransomware, Attaque DDOS

I. Généralités

6. Cyberattaque

- Une tentative malveillante visant à compromettre, endommager ou exploiter un système informatique.
- Cible les systèmes d'informations des entreprises dépendant de la technologie et de réseaux (Internet).

I. Généralités

7. Impact d'une Cyberattaque

a. Impacts financiers :

- **Coûts directs** : Le coût d'une cyberattaque est estimé à environ 97 000 euros. Ce montant peut varier selon la nature et l'ampleur de l'attaque.
- **Coûts de réparation** : La remise en état, la récupération des données et l'achat de nouveaux équipements peuvent engendrer des dépenses importantes.
- **Pertes de revenu** : L'interruption des activités suite à une cyberattaque peut entraîner un manque des activités commerciales.

I. Généralités

7. Impact d'une Cyberattaque

b. Impacts opérationnels :

- **Perte de données :** Les informations critiques de l'entreprise peuvent être volées, corrompues ou rendues inaccessibles.
- **Paralysie des activités** : 30% des cyberattaques en 2020 ont entraîné une interruption partielle ou totale des opérations.
- **Perturbation des systèmes** : Les attaques peuvent compromettre l'intégrité et la disponibilité des systèmes d'informations.

I. Généralités

7. Impact d'une Cyberattaque

c. Impact sur la réputation :

- **Perte de confiance** : Les clients, les partenaires et les investisseurs peuvent perdre confiance en l'organisation à la suite d'une cyberattaque.
- **Dégradation de l'image de marque** : La publicité négative associée à une cyberattaque peut nuire durablement à la réputation de l'entreprise.

I. Généralités

7. Impact d'une Cyberattaque

d. Impacts juridiques et réglementaires :

- **Sanctions réglementaires :** Le non-respect des obligations en matière de protection des données peut entraîner des amendes importantes. (RGPD*)
- **Poursuites judiciaires :** Les victimes d'une fuite de données peuvent intenter des actions en justice contre l'organisation.

*RGPD : Règlement général de protection des données

I. Généralités

7. Impact d'une Cyberattaque

e. Impacts humains et psychologiques :

- **Stress et anxiété** : Les employés peuvent ressentir un sentiment d'impuissance, de vulnérabilité suite à une Cyberattaque.
- **Pression sur les équipes IT** : Les personnels informatiques peuvent être affectés, avec une remise en question de leurs compétences (investigation).
- **Climat de méfiance** : Une cyberattaque peut créer un environnement de travail tendu et stressant.

Terminologie

II. Terminologie

1. Actif

- C'est la partie d'un bien qui compose le patrimoine et présente de la valeur dans l'entreprise.
- Il peut représenter : des équipements, des matériels, des logiciels, des processus et des activités métiers.

II. Terminologie

2. Vulnérabilité

- C'est une faille dans les actifs, défaillance dans une mesure de contrôle de sécurité technique utilisées dans l'entreprise.
- Faiblesse du système qui représente une menace pouvant être exploitée par un intrus.
- Chaque vulnérabilité admet un identifiant unique dans le monde.
- **CVE** (**C**ommon **V**ulnerabilities and **E**xposures) : désigne une liste publique de failles de sécurité informatique.

II. Terminologie

2. Vulnérabilité

❖ **Codification des CVEs**

- Le numéro d'enregistrement d'un CVE suit la syntaxe suivante : **CVE-AAAA-NNNNN**
  - **AAAA** : est l'année de publication/découverte de la vulnérabilité
  - **NNNNN** : est un numéro commençant par 00001 dans l'année en cours et incrémenté par +1
- Exemples :
  - CVE-2021-26855 : Vulnérabilité dans Microsoft Exchange Server – Score 9.8
  - CVE-2019-0211 : Vulnérabilité d'escalade de privilèges dans Apache HTTP Server - Score 7.8

II. Terminologie

2. Vulnérabilité

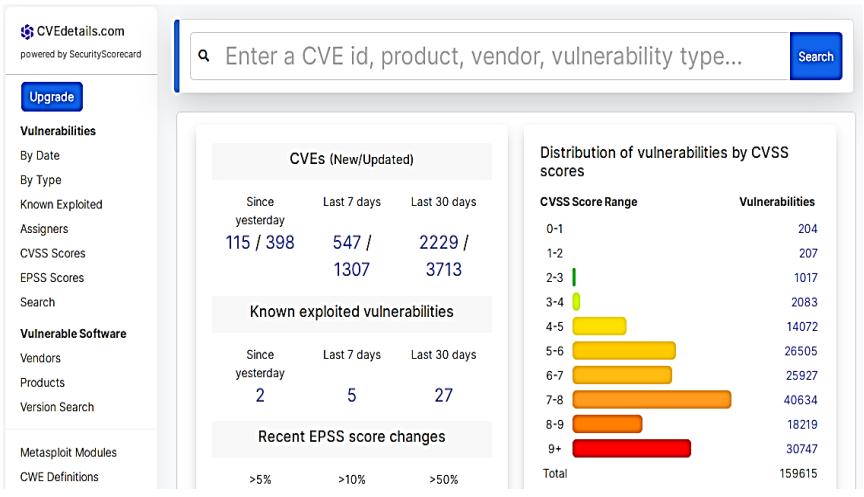
- **Scores des CVEs** :
  - **CVSS** : Common Vulnerability Scoring System
  - Système de notation de 0 à 10 : il s'agit de la criticité des failles de sécurité découvertes et annoncées.

CVSS : plages de notation (score ranges)	
Indice de sévérité	**Interprétation**
0	Aucune criticité
0.1 - 0.9	Criticité faible
1.0 - 1.9	Criticité faible
2.0 - 2.9	Criticité faible
3.0 - 3.9	Criticité moyenne
4.0 - 4.9	Criticité moyenne
5.0 - 5.9	Criticité moyenne
6.0 - 6.9	Criticité élevée
7.0 - 7.9	Criticité élevée
8.0 - 8.9	Criticité élevée
9.0 - 10	Criticité maximale

II. Terminologie

2. Vulnérabilité

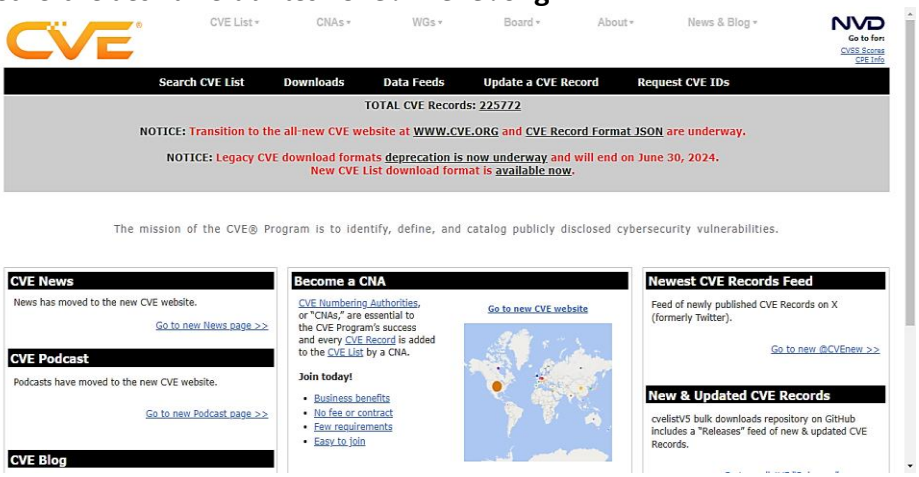
Site de recherche des vulnérabilités : **`cvedetails.com`**



II. Terminologie

2. Vulnérabilité

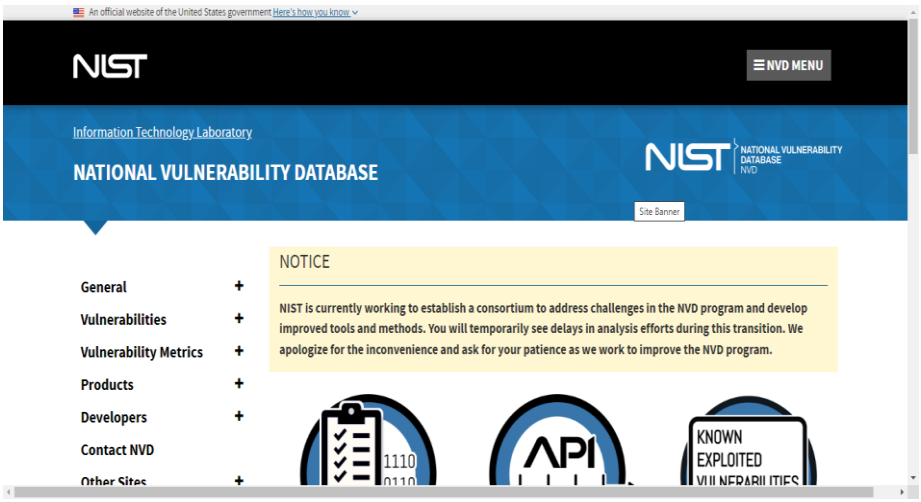
Site de recherche des vulnérabilités : **`cve.mitre.org`**



II. Terminologie

2. Vulnérabilité

Site de recherche des vulnérabilités : **`nvd.nist.gov`**



II. Terminologie

2. Vulnérabilité

Les pirates/auditeurs utilisent aussi des logiciels pour analyser et découvrir les vulnérabilités :

- **Nessus** est un outil de scanning des vulnérabilités développé par Tenable Inc largement utilisé dans l'audit de sécurité
- **OpenVAS** : (Open Vulnerability Assessment System) est un outil open-source de scanning des vulnérabilités, conçu pour détecter les failles de sécurité dans les systèmes informatiques, les réseaux, et les applications.

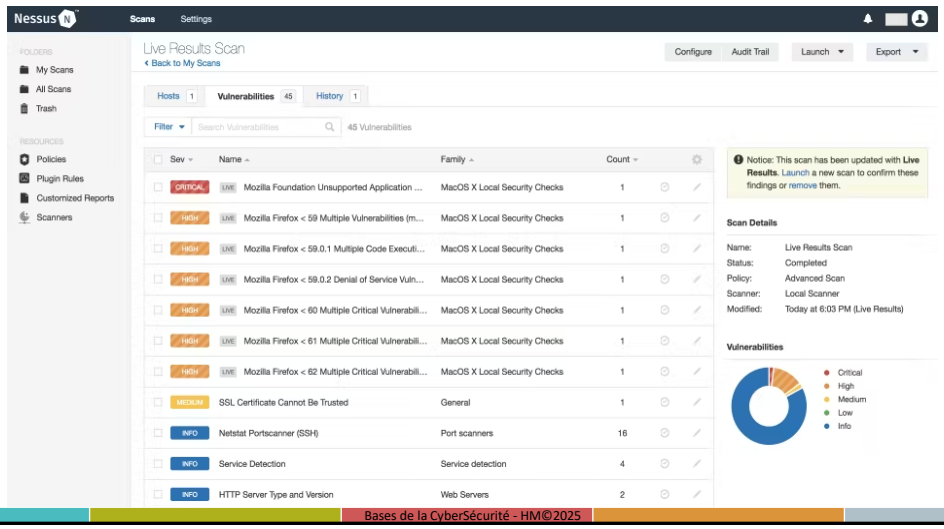
Greenbone OpenVAS
Open Vulnerability Assessment Scanner

Nessus®

II. Terminologie

2. Vulnérabilité

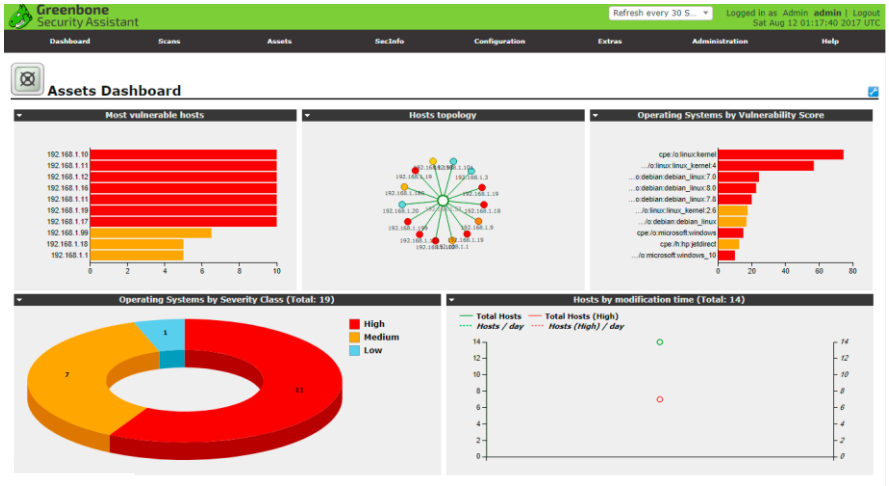
Tableau de bord : **Nessus**



II. Terminologie

2. Vulnérabilité

Tableau de bord : **OpenVAS**



II. Terminologie

3. Vulnérabilité Zero-day

Une vulnérabilité Zero-day est une faille de sécurité dans un logiciel, un système d'exploitation ou un matériel qui est inconnue du développeur et public.

Elle peut-être exploitée par un pirate avant qu'un correctif (*patch*) soit publié.

Exemple : Vulnérabilité publie par CERT*

VULNÉRABILITÉ DANS LES PRODUITS FORTINET

CERTFR-2025-ALE-002 • *Publié le 14 janvier 2025* • Alerte en cours

Le 14 janvier 2025, Fortinet a publié un avis de sécurité concernant la vulnérabilité critique CVE-2024-55591 affectant FortiOS et FortiProxy. Elle permet à un attaquant distant non authentifié de contourner le mécanisme d'authentification de l'interface d'administration d'un équipement FortiOS...

[MÀJ] MULTIPLES VULNÉRABILITÉS DANS FORTINET FORTIMANAGER

CERTFR-2024-ALE-014 • *Publié le 30 octobre 2024* • Alerte en cours

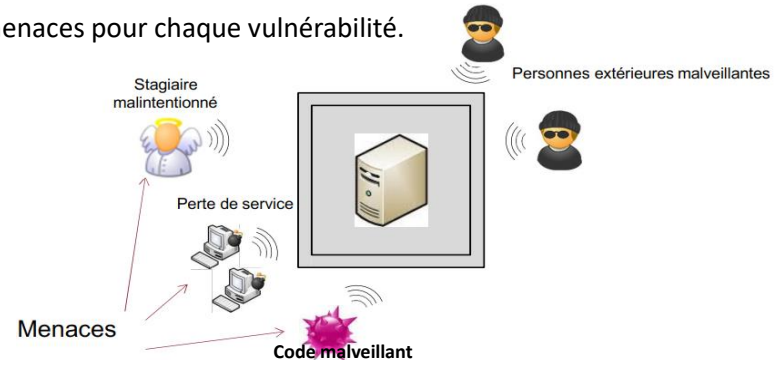
[Mise à jour du 14 janvier 2025] Publication des correctifs Le 14 janvier 2025, Fortinet a publié un avis de sécurité relatif à la vulnérabilité CVE-2024-50566 qui correspond à la vulnérabilité de type jour-zéro pour laquelle une preuve de concept a été publiée en novembre 2024. Des...

*__CERT__ : Computer Emergency Response Team

II. Terminologie

4. Menace

- Une **menace** permet d'exploiter une **vulnérabilité** pour obtenir, modifier ou empêcher l'accès à un actif ou le compromettre.
- Cause potentielle d'un incident, qui pourrait entrainer des dommages sur un **bien** de l'entreprise.
- Il peut y avoir plusieurs menaces pour chaque vulnérabilité.



II. Terminologie

5. Risque

- Le risque est la **possibilité** qu'une menace **exploite** une **vulnérabilité** pour causer des pertes des données ou des dommages au SI.
- Une méthode de gestion de risque est choisie dans une entreprise en fonction de la nature de risque, ses impacts et son coût associé.
- Exemples :
  - **EBIOS** : Expression des Besoins et Identification des Objectifs de Sécurité
  - **ISO 27005**
  - **MEHARI** : Méthode Harmonisée d'Analyse des Risques
  - **FAIR** : Factor Analysis of Information Risk

II. Terminologie

6. Impact

Il exprime les **conséquences** ou les dommages résultant de l'exploitation de la vulnérabilité par une menace.

Les impacts peuvent être évalués selon les critères suivants :

- Financiers (frais de restauration, pertes d'exploitation).
- Réputation et image de l'entreprise (par rapport à l'extérieur et au personnel).
- Expertise et savoir-faire reconnus de l'entreprise.
- Juridique.

II. Terminologie

7. Vecteur d'attaque

Un vecteur d'attaque est la **méthode** ou le **chemin** par un cybercriminel utilise pour pénétrer ou s'infiltrer dans le réseau d'une cible.

Exemple des vecteurs d'attaques :

- ✓ **Phishing** : L'attaquant envoie un e-mail frauduleux imitant une source légitime pour inciter la victime à cliquer sur un lien malveillant ou à fournir des informations sensibles.
- ✓ **Logiciels malveillants** : Un virus ou un cheval de Troie est dissimulé dans un fichier apparemment inoffensif que la victime est amenée à télécharger et exécuter.
- ✓ **Ingénierie sociale** : L'attaquant manipule psychologiquement une personne pour qu'elle divulgue des informations confidentielles ou effectue des actions compromettantes.

II. Terminologie

8. Surface d'attaque

Une surface d'attaque désigne l'ensemble des **points d'accès vulnérables** d'un système d'information qu'un pirate pourrait exploiter pour le compromettre.

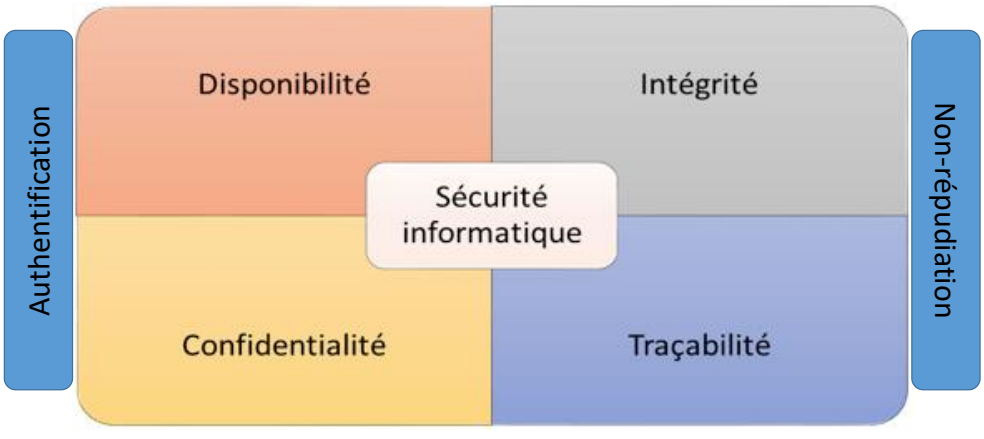
On distingue généralement trois types principaux de surfaces d'attaque :

- ✓ **Surface d'attaque numérique** : Elle comprend l'intégralité de l'environnement réseau, données et logiciels d'une entreprise.
- ✓ **Surface d'attaque physique** : Elle couvre tous les éléments matériels de l'entreprise.
- ✓ **Surface d'attaque humaine** : Elle concerne les vulnérabilités liées au comportement humain.

Quelles sont les principales propriétés assurées par la sécurité informatique ?

Objectifs de la sécurité informatique

III. Objectifs de la sécurité informatique



III. Objectifs de la sécurité informatique

1. Disponibilité

- C'est une propriété d'un système d'information qui **garantit l'accès aux ressources** sans interruption, sans délai et sans dégradation ou moment voulu aux personnes autorisées.
- Pour assurer la disponibilité dans un SI, il est recommandé d'appliquer :
  - Des mesures de sauvegarde (Data on-promises et on Cloud).
  - Redondance dans le système et réseau (Redondance des serveurs, l'alimentation, disques,…)
  - Des plans de continuité des activités (PCA).

III. Objectifs de la sécurité informatique

2. Intégrité

- L'intégrité assure que les données et les systèmes sont exacts, complets et n'ont pas été modifiés de manière non autorisée.
- Pour vérifier l'intégrité des données dans un SI, il est conseillé d'appliquer :
  - Les signatures numériques,
  - Mécanismes de contrôle d'accès des personnes autorisées IAM,
  - Fonctions de hachage.

III. Objectifs de la sécurité informatique

3. Confidentialité

- La confidentialité vise à garantir que les informations ne sont **accessibles qu'aux personnes autorisées**.
- Pour garantir la confidentialité des données dans un SI, il est conseillé de pratiquer :
  - Chiffrement des données.
  - Mécanisme de contrôle d'accès (Forte authentification).
  - Gestion des identités & permissions (Principe de moindre privilège).
  - Formation et sensibilisation.

III. Objectifs de la sécurité informatique

4. Traçabilité

- Garder un **historique sur toutes les actions** et évènements qui se produisent dans un système informatique.
- Aussi sauvegarder des **tentatives d'accès** et conserver les **traces** comme une preuve exploitable.
- Pour garantir la traçabilité des actions, il est conseillé d'implémenter :
  - Journalisation des évènements (Logging).
  - Bonne gestion de logs (Serveur log distant, chiffrement de logs).
  - Suivi des modifications.

III. Objectifs de la sécurité informatique

5. Non répudiation

- La non-répudiation est la capacité de prouver qu'un **événement** ou une **transaction** a eu lieu ainsi que d'identifier les entités à l'origine. (empêcher le démenti).
- Pour garantir la non-répudiation des transactions , il est conseillé d'utiliser :
  - La signature numérique.
  - Les certificats numérique.
  - Journalisation et enregistrement des transactions.
  - Authentification forte (2FA, MFA).

III. Objectifs de la sécurité informatique

6. Authentification

- L'authentification est le processus de **vérification de l'identité d'un utilisateur**, d'un appareil ou d'une entité qui tente d'accéder à des ressources protégées.
- Plusieurs façons d'implémenter les techniques d'authentification :
  - Authentification par mot de passe
  - Authentification à deux facteurs (2FA)
  - Authentification biométrique
  - Authentification par carte à puce
  - Authentification par certificat électronique

Comment je dois appliquer la sécurité informatique à mon SI pour garantir ses objectifs principaux ?

Frameworks de sécurité informatique

IV. Frameworks de sécurité informatique

1. Définition

- Un Framework de sécurité est un ensemble structuré de **bonnes pratiques** (recommandations) et de principes visant à protéger le SI contre les Cybermenaces.
- Fournir une approche systématique et cohérente pour :
  - Gérer les risques de sécurité de l'organisation.
  - Amélioration continue du processus de Cybersécurité.
  - Réduire les coûts liés aux incidents de sécurité.

IV. Frameworks de sécurité informatique

2. Principaux Framework de sécurité

a. NIST

- National Institute of Standards and Technology.
- Agence américaine créer en 1901
- Définir des normes qui assurent la qualité, la sécurité et l'efficacité des produits et des technologies.
- Offre une approche évolutive pour gérer les risques de Cybersécurité.
- Couvre les domaines de l'identification, la protection, la détection, la réponse et du rétablissement.

IV. Frameworks de sécurité informatique

3. Principaux Framework de sécurité

b. ISO/IEC 27001

- Norme internationale pour la gestion de la sécurité de l'information.
- Fournit les exigences pour mettre en place et gérer le Système de Management de la Sécurité de l'Information (SMSI).
- Largement adoptée dans de nombreux secteurs.

IV. Frameworks de sécurité informatique

3. Principaux Framework de sécurité

c. PCI DSS

- Payment Card Industry Data Security Standard.
- Standard de sécurité pour les organisations traitant les paiements par carte bancaire.
- Vise à protéger les données des titulaires de carte de paiement.
- Obligatoire pour toute entreprise acceptant les paiements par carte.

IV. Frameworks de sécurité informatique

3. Principaux Framework de sécurité

d. ITIL

- Information Technology Infrastructure Library
- Framework de bonnes pratiques pour la gestion des services informatiques.
- Couvre la conception, la mise en œuvre et l'amélioration continue des services TI.
- Intègre des aspects de sécurité.

IV. Frameworks de sécurité informatique

3. Principaux Framework de sécurité

e. COBIT

- Control OBjectives for Information and related Technologies,
- Développé par *ISACA* (Information Systems Audit and Control Association) en 1996.
- Framework de gouvernance et de management des technologies de l'information.
- Met l'accent sur l'alignement des TI avec les objectifs stratégique de l'entreprise.
- Couvre la définition, la mise en œuvre et le contrôle des processus de gestion des TI

Politique de sécurité informatique

V. Politique de sécurité informatique

1. Définition

- Une politique de sécurité (PS) est un **document** établi par une organisation pour protéger son système d'information contre les menaces internes et externes.
- Elle représente une implémentation concrète d'un Framework de sécurité, définissant les **règles**, les **procédures** et les **bonnes pratiques** pour protéger le **SI** contre les **menaces internes et externes**.
- **Exemple** : Une PS peut contenir :
  - Les comportements attendus des utilisateurs,
  - Les mesures de protection à mettre en place,
  - Les mécanismes d'authentification,
  - Les protocoles à suivre en cas d'incident de sécurité.

V. Politique de sécurité informatique

2. Acteurs de la politique de sécurité

- La politique de sécurité informatique dans une entreprise est définie par plusieurs acteurs qui sont :
  - **Direction générale** : Garantir une vision stratégique de la sécurité
  - **Responsable de la Sécurité des Systèmes d'Information** (**RSSI**) : Architecte principal de la PS, définit les risques potentiels et propose des bonnes pratiques pour protéger les actifs de l'entreprise.
  - **Equipe IT** : en collaboration avec le RSSI
  - **Département juridique** : S'assure que la PS respecte les lois en vigueur

VI. Evaluation de connaissances

1. Tommy évalue la sécurité de plusieurs serveurs de base de données dans le Datacenter et se rend compte qu'il manque à l'un d'entre eux un correctif de sécurité Oracle critique. Quel type de situation Tommy a détecté ?

A. Risque

B. Vulnérabilité

C. Piratage

D. Menace

VI. Evaluation de connaissances

2. Parmi les affirmations suivantes, laquelle décrit correctement la différence entre un White Hat et un Script Kiddie ?

A. Un White Hat utilise des outils prédéfinis sans comprendre leur fonctionnement ; Script Kiddie est un expert en Cybersécurité.

B. Un White Hat est un pirate malveillant qui exploite des vulnérabilités pour son profit ; Script Kiddie est un professionnel de la sécurité qui protège les systèmes.

C. Un White Hat est un expert en Cybersécurité qui travaille de manière éthique pour identifier et corriger les vulnérabilités ; Script Kiddie utilise des outils/scripts existants sans compréhension approfondie, souvent à des fins malveillantes.

D. Un White Hat et un Script Kiddie sont deux termes désignant la même chose : des pirates informatiques malveillants.

VI. Evaluation de connaissances

3. L'entreprise rédige un document intitulé « Utilisation acceptable » qui définit ce que l'entreprise autorise les utilisateurs à faire et à ne pas faire sur leurs systèmes de travail. L'entreprise demande aux nouveaux employés de lire et de signer ce document. Comment s'appelle ce type de document ?

A. Standard

B. Politique

C. Procédure

D. Contrat

VI. Evaluation de connaissances

4. Lequel des objectifs suivants n'est pas l'un des trois principaux objectifs que les professionnels de la sécurité de l'information doivent atteindre pour protéger leur organisation contre les menaces de Cybersécurité ?

A. Intégrité
B. Non-répudiation
C. Disponibilité
D. Confidentialité

VI. Evaluation de connaissances

5. Une entreprise subit une attaque par Ransomware, paralysant ses opérations pendant trois jours. Quel est l'impact immédiat et quelle serait la meilleure approche pour gérer cette situation ?

A. L'impact est mineur ; il suffit d'attendre que l'attaque cesse.
B. Payer la rançon et espérer la récupération des données.
C. L'impact est l'arrêt des opérations ; il faut restaurer les données à partir de sauvegardes et améliorer la sécurité pour éviter de futures attaques.
D. Aucune action n'est nécessaire si aucune donnée sensible n'a été affectée.

VI. Evaluation de connaissances

6. Comment une vulnérabilité peut-elle être réduite efficacement ?

A. Par l'ignorance des risques
B. Par la mise à jour régulière des systèmes
C. En augmentant la surface d'attaque
D. En réduisant les actifs

VI. Evaluation de connaissances

7. Un attaquant exploite une faille non documentée dans une application. Comment cette faille est-elle qualifiée ?

A. Menace connue
B. Risque
C. Vulnérabilité Zero-day
D. Actif critique

VI. Evaluation de connaissances

8. Quelle est la relation entre une menace et une vulnérabilité ?

A. Une vulnérabilité exploite une menace

B. Une menace exploite une vulnérabilité

C. Elles sont indépendantes

D. Les deux désignent la même chose

VI. Evaluation de connaissances

9. Quelle mesure peut garantir la disponibilité d'un système ?

A. L'implémentation de sauvegardes régulières

B. L'activation de journaux d'accès

C. La cryptographie asymétrique

D. L'utilisation d'une authentification forte

VI. Evaluation de connaissances

10. Le vecteur d'attaque désigne :

A. Les données chiffrées pendant une attaque
B. Le chemin emprunté par l'attaquant pour accéder au système
C. Le niveau de risque de l'organisation
D. Une vulnérabilité corrigée

VI. Evaluation de connaissances

11. Une entreprise découvre qu'un logiciel interne a été compromis par une vulnérabilité non reconnue et exploitée par des pirates avant que le fournisseur ne publie un correctif. Quel est le terme approprié pour désigner cette situation ?

A. Vecteur d'attaque
B. Risque
C. Menace
D. Zero-day

https://secnumacademie.gouv.fr

UNITÉ 3

Les acteurs de la cybersécurité

Temps passé : 00:00:00 Score : 0%

Commencer S'évaluer

UNITÉ 4

Protéger le cyberespace

Temps passé : 00:00:00 Score : 0%

Commencer S'évaluer

UNITÉ 1

Un monde numérique hyper-connecté

Temps passé : 00:00:00 Score : 0%

Commencer S'évaluer

UNITÉ 2

Un monde à hauts risques

Temps passé : 00:00:29 Score : 0%

Commencer S'évaluer

UNITÉ 1

Principes de l'authentification

Temps passé : 00:00:00 Score : 0%

Commencer S'évaluer

UNITÉ 2

Attaques sur les mots de passe

Temps passé : 00:00:00 Score : 0%

Commencer S'évaluer

UNITÉ 3

La navigation web

Temps passé : 00:00:00 Score : 0%

Commencer S'évaluer

UNITÉ 4

La messagerie électronique

Temps passé : 00:00:00 Score : 0%

Commencer S'évaluer