Chapitre 1

Introduction à la Sécurité des Systèmes d'Information

30 octobre 2025

Table des matières

1 Statistiques sur la Cybersécurité

1.1 Au Niveau Mondial

Chiffres Clés 2020-2023

Pertes Financières :

- **2020 :** 1000 milliards USD de pertes (plus de 1% du PIB mondial)
- **2023-2028 :** Augmentation prévue de 5,7 trillions USD (+70%)
- **2028 :** Coût estimé à 13,82 trillions USD

Entreprises Touchées :

- **61%** des grandes entreprises ciblées en 2018
- **54%** des entreprises françaises attaquées en 2021
- **56%** des organisations africaines attaquées en 2022

Coûts par Incident :

- PME : 200 000 - 1,3 million USD
- Grandes entreprises US : jusqu'à 27 millions USD

1.2 Investissements en Cybersécurité

Budgets de Sécurité

- **Moyenne 2018 :** 1,46 million USD par entreprise (+24% en 1 an)
- **2021 :** 40% des entreprises françaises ont investi
- **Problème :** 45% des entreprises ne sont pas prêtes à gérer une cyber-crise
- Seulement **17%** disposent d'un programme de cyber-résilience

1.3 Dépenses Principales

1. Temps d'arrêt du système
2. Efficacité réduite
3. Coûts de réaction aux incidents
4. Atteinte à la marque et à la réputation

1.4 Facteurs de Risque

Statistiques Importantes

- **70%** des attaques causées par l'erreur humaine
- **États-Unis :** 10% de toutes les cyberattaques mondiales
- **Turquie :** 4,7%
- **Russie :** 4,3%
- **Fréquence :** Une nouvelle attaque toutes les 39 secondes

1.5 Situation en Tunisie

Cybersécurité en Tunisie

2020 :

- Pertes estimées : **plus de 1 milliard de dinars**
- Secteur le plus touché : **Industrie** (pas le secteur financier)

Classement International :

- **45ème sur 192 pays** selon l'Indice Global de Cybersécurité (GCI 2020)
- Progression de **31 places**
- Publié par l'Union Internationale des Télécommunications (UIT)

Organisme National :

- **ANSI** devient **ANCS** (Agence Nationale de la Cybersécurité)
- Rôle : Coordinateur national
- Site : `https://www.ansi.tn/statistics`

2 Définitions Fondamentales

Sécurité des Systèmes d'Information (SSI)

La SSI est **l'ensemble des moyens** techniques, organisationnels, juridiques et humains nécessaires et mis en place pour :

- **Conserver** la sécurité de l'information
- **Rétablir** la sécurité après incident
- **Garantir** la sécurité des systèmes et ressources informatiques

Protection contre les menaces atteignant :

- La confidentialité
- L'intégrité
- La disponibilité

Importance : La sécurité est un enjeu majeur pour les entreprises et l'ensemble des acteurs.

2.1 Finalités de la SSI

1. **Court terme :** Chaque personne légitime a accès aux informations dont elle a besoin
2. **Moyen terme :** Maintenir la cohérence de l'ensemble du système d'information
3. **Long terme :** Maintenir la confiance des utilisateurs et des clients (image de marque)

2.2 Facteurs de Risques pour la Sécurité

Nouveaux Défis

- **Multiplication des terminaux** (smartphones, tablettes, IoT)
- **Hyperconnectivité** (tout est connecté)
- **Développement du travail hybride** (télétravail)
- **Nouveaux usages et services dans le Cloud**
- **Usage massif des IoT** (Internet of Things)

3 Cibles des Cyberattaques

Nul n'est à l'abri !

Les pirates peuvent cibler :

- **Individus** (citoyens, employés)
- **Entreprises** (petites et grandes)
- **Banques** (secteur financier)
- **Administrations publiques** (gouvernements)

Les dommages qui en découlent pèsent de plus en plus lourd.

4 Qui est Concerné par la SSI ?

Tous les Acteurs

La sécurité est l'affaire de tous :

- **Les informaticiens** (administrateurs, développeurs, data modelers)
- **Les dirigeants** (décisionnaires, managers)
- **Les utilisateurs** (employés, clients)
- **Tous les membres** concernés par le système d'information

4.1 Pluridisciplinarité de la Sécurité

La sécurité touche plusieurs domaines :

1. **Éthique**
2. **Législation et réglementation**
3. **Technique**
4. **Méthodologie**
5. **Normes**

5 Les Services de Sécurité

Les 5 Piliers de la Sécurité

La sécurité des systèmes d'information vise les objectifs suivants :

1. La Disponibilité

- Le système doit fonctionner sans faille durant les plages d'utilisation prévues
- Garantir l'accès aux services et ressources installées
- Assurer le temps de réponse attendu

2. L'Intégrité

- Les données doivent être celles que l'on attend
- Ne doivent pas être altérées (fortuite, illicite ou malveillante)
- Les éléments considérés doivent être exacts et complets

3. La Confidentialité

- Seules les personnes autorisées ont accès aux informations
- Tout accès indésirable doit être empêché

4. L'Authentification

- Identification des utilisateurs fondamentale
- Gérer les accès aux espaces de travail pertinents
- Valider l'authenticité de l'entité en question

5. La Non-répudiation

- Aucun utilisateur ne peut contester les opérations qu'il a réalisées
- Dans le cadre de ses actions autorisées
- Preuve de la transaction

Principe du Maillon le Plus Faible

Important : Le niveau global de sécurité des systèmes d'information est défini par le niveau de sécurité du maillon le plus faible.
Les contre-mesures doivent être envisagées en fonction des vulnérabilités.

6 Risques, Menaces, Vulnérabilités

6.1 Définitions

Concepts Clés

Menace

- Attaque possible d'un individu ou d'un élément naturel sur des biens
- Entraîne des conséquences potentielles négatives
- Violation potentielle d'une propriété de sécurité
- *Exemple :* Développeur modifiant le code pour détournement de fonds, vol d'ordinateur portable

Vulnérabilité

- Caractéristique d'une entité constituant une faiblesse ou faille
- Peut être organisationnelle, humaine, logicielle ou matérielle
- *Exemple :* Pas de politique de sécurité, pas de formation, produits non testés, fichiers non protégés

Impact

- Conséquence sur l'organisme de la réalisation d'une menace
- Peut être exprimé financièrement ou par échelle contextuelle

Risque

- Combinaison d'une menace et des pertes qu'elle peut engendrer
- Potentialité de l'exploitation de vulnérabilité par un élément menaçant
- Impact sur l'organisme

Remarque Importante

La notion de risque dépend de l'impact : une menace ayant une grande probabilité de se concrétiser, mais ayant un impact nul constitue un risque presque nul.

6.2 Estimation des Risques

Pour évaluer les risques, il faut estimer :

1. **La gravité des impacts** si les risques se réalisent
2. **La vraisemblance des risques** (potentialité ou probabilité d'occurrence)

7 Cycle de Sécurité

Les 3 Phases du Cycle

1. **Prévention**
   - Ensemble de mesures pour réduire la fréquence des incidents
   - Optique de protection
   - Empêcher de violer la politique de sécurité
2. **Détection**
   - Mesures pour détecter et diminuer l'effet d'une attaque
   - Suivi attentif et constant de l'état des systèmes
   - Monitoring et alertes
3. **Réaction**
   - Restaurer les biens et les actifs après un incident de sécurité
   - Réagir vite et de manière ordonnée
   - Plan de réponse aux incidents

8 Démarche Générale de Sécurisation

4 Étapes Principales

Pour sécuriser les systèmes d'information, la démarche consiste à :

1. **Évaluer les risques et leur criticité**
   - Quels risques et quelles menaces ?
   - Sur quelles données et quelles activités ?
   - Avec quelles conséquences ?
2. **Rechercher et sélectionner les parades**
   - Que va-t-on sécuriser ?
   - Quand et comment ?
   - *Étape difficile :* Choix dans un contexte de ressources limitées (temps, compétences, argent)
3. **Mettre en œuvre les protections**
   - Implémenter les solutions choisies
   - Vérifier leur efficacité (évaluation)
4. **Mettre à jour**
   - Au regard de l'évolution des risques
   - Amélioration continue

9 Approche Globale de la Sécurité

4 Aspects Complémentaires

La sécurité doit être abordée dans un contexte global :

1. Sensibilisation des Utilisateurs

- Formation aux problèmes de sécurité
- Bonnes pratiques
- Culture de la sécurité

2. Sécurité Logique

- Sécurité au niveau des données de l'entreprise
- Applications
- Systèmes d'exploitation

3. Sécurité des Télécommunications

- Technologies réseau
- Serveurs de l'entreprise
- Réseaux d'accès

4. Sécurité Physique

- Infrastructures matérielles
- Salles sécurisées
- Lieux ouverts au public
- Espaces communs de l'entreprise
- Postes de travail des personnels

10 Politique de Sécurité

PSSI - Politique de Sécurité des Systèmes d'Information

Définition :
La PSSI est un **plan d'actions** définies pour maintenir un certain niveau de sécurité. Elle reflète la vision stratégique de la direction de l'organisme en matière de sécurité des systèmes d'information.

Matérialisation :

- Ensemble de documents
- Présente les règles de sécurité à appliquer et à respecter
- Organisation permettant sa mise en place

Contenu :

- Document de référence
- Définit les objectifs poursuivis en matière de sécurité
- Définit les moyens mis en œuvre
- Règles, procédures et bonnes pratiques
- Niveau de sécurité conforme aux besoins

10.1 Mise en Place de la PSSI

Conditions de Réussite

Approche :

- Conduit comme un véritable **projet**
- Associant des représentants des utilisateurs
- Conduit au **plus haut niveau de la hiérarchie**
- Pour être accepté par tous

Communication :

- Une fois rédigée, communiquer les clauses au personnel
- Donner le maximum d'impact à la politique

Nécessité :

- Les cyberattaques augmentent en fréquence, complexité et gravité
- Mettre en place une bonne gestion de la sécurité des informations

11 Modèles de Sécurité

11.1 McCumber Cube

Le Cube de McCumber (1991)

Créé par John McCumber : modèle de sécurité complet appelé **CyberSecurity Cube**.
Dimension 1 : Principes Fondamentaux (Triade CID)

- **Confidentialité**
- **Intégrité**
- **Disponibilité**

Dimension 2 : États des Données

- En **stockage**
- En **transmission**
- En **traitement**

Dimension 3 : Types de Contre-mesures

- **Technologies** (firewalls, antivirus, chiffrement)
- **Politiques et pratiques** (règles, procédures)
- **Formation et sensibilisation** (humain)

11.2 Modèle ISO

Cadre ISO/IEC

L'ISO (International Organization for Standardization) et l'IEC (International Electrotechnical Commission) ont développé un cadre complet pour guider la gestion de la sécurité de l'information.
Objectif : Comprendre et aborder des tâches complexes liées à la sécurité de bout en bout.

12 Normes et Standards

12.1 Famille ISO/IEC 27000

ISO/IEC 27000 : SGSI/ISMS

Normes pour la mise en place, l'utilisation, la tenue à jour et la gestion d'une politique de sécurité informatique : **SGSI (Système de Gestion de la Sécurité de l'Information)**.
Principales Normes :
ISO/IEC 27000 :2009 - Aperçu général et vocabulaire
ISO/IEC 27001 :2022 - Norme principale

- Exigences pour mettre en place et certifier un SMSI
- Caractère **certifiable**
- Définit les exigences obligatoires
- Établir, mettre en œuvre, maintenir et améliorer un SMSI

ISO/IEC 27002 :2022 - Code de bonnes pratiques

- Référentiel de mesures de sécurité
- **Non certifiable** (guide)
- 93 mesures de sécurité (contrôles)
- 4 thèmes : Organisationnels, Personnes, Physiques, Techniques

ISO/IEC 27003 :2010 - Lignes directrices pour la mise en œuvre
ISO/IEC 27004 :2009 - Mesurage
ISO/IEC 27005 :2011 - Gestion des risques de sécurité
ISO/IEC 27006 :2007 - Exigences pour les organismes d'audit et certification
ISO/IEC 27007 :2011 - Lignes directrices pour l'audit
ISO/IEC 27017 et 27018 - Sécurité et protection des données dans le cloud

12.2 ISO 27002 : Évolution

ISO 27002 :2013

Approche processus pour la mise en place d'un SMSI
Contenu :

- 114 mesures de bonnes pratiques
- 11 articles ou thèmes
- Aspects : techniques, organisationnels, sociaux et juridiques

ISO 27002 :2022

Référentiel de mesures adaptables selon les risques
Contenu :

- 93 mesures de sécurité (contrôles)
- 4 thèmes principaux :
  1. Contrôles organisationnels
  2. Contrôles liés aux personnes
  3. Contrôles physiques
  4. Contrôles techniques

Complémentarité : Accompagne ISO 27001 qui fixe les exigences du SMSI.

13 Mise en Place d'un SMSI (ISO 27001)

Roue de Deming (PDCA)

Un projet de mise en place de la sécurité suit la logique de la roue de Deming :
Phase PLAN (Planifier)

1. Définition du périmètre et de la politique
2. Appréciation des risques
3. Traitement du risque
4. Sélection des mesures de sécurité

Phase DO (Faire)

1. Planification du traitement des risques
2. Génération d'indicateurs significatifs
3. Formation et sensibilisation du personnel
4. Gestion quotidienne du SMSI
5. Détection et réaction aux incidents

Phase CHECK (Vérifier)

- Moyens de contrôle
- Audits
- Contrôles
- Revues

Phase ACT (Agir)

- Actions correctives si écarts constatés
- Actions préventives
- Amélioration continue

14 Résumé et Points Clés

À Retenir

Sécurité = Affaire de Tous
- 70% des attaques dues à l'erreur humaine
- Formation et sensibilisation essentielles

Approche Globale
- Technique + Organisationnel + Humain + Juridique
- Le maillon le plus faible détermine le niveau de sécurité

5 Services Fondamentaux
- Disponibilité, Intégrité, Confidentialité
- Authentification, Non-répudiation

Gestion des Risques
- Risque = Menace × Vulnérabilité × Impact
- Cycle : Prévention → Détection → Réaction

Normes ISO 27000
- 27001 : Certifiable (exigences)
- 27002 : Guide de bonnes pratiques
- PDCA : Amélioration continue

La sécurité est un processus continu, pas un état !

Ressources :
- Quiz : `https://apcpedagogie.com/qcm-la-securite-informatique/`
- ANCS Tunisie : `https://www.ansi.tn/statistics`