Sécurité des réseaux

Master I I2A

2025/2026

Chapitre 1

Aspects généraux de la sécurité

1. Introduction à la sécurité des systèmes d'information

1.1 Définition et périmètre

La sécurité des systèmes d'information (SSI) est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires pour protéger les systèmes d'information contre les menaces accidentelles ou intentionnelles.

Les quatre piliers de la SSI :

- **Sécurité physique** : contrôle d'accès aux locaux, protection des serveurs, onduleurs, climatisation
- **Sécurité logique** : mots de passe, chiffrement, pare-feu, antivirus
- **Sécurité organisationnelle** : procédures, politiques, chartes, formation
- **Sécurité juridique** : conformité RGPD, lois sur la cybercriminalité, contrats

1.2 Enjeux de la sécurité

- **Enjeux économiques**
- **Coût des cyberattaques** :
  - En 2023, le coût moyen d'une violation de données était de 4,45 millions de dollars (étude IBM)
  - Perte d'exploitation, rançongiciels (ransomware), atteinte à l'image
- **Valeur de l'information** : données clients, secrets industriels, propriété intellectuelle
- **Continuité d'activité** : indisponibilité = perte de chiffre d'affaires

1.2 Enjeux de la sécurité

- **Enjeux juridiques et réglementaires**
- **RGPD (Règlement Général sur la Protection des Données)** :
  - Applicable depuis 2018
  - Obligation de notification des violations dans les 72h
  - Amendes pouvant atteindre 4% du CA mondial
- **Loi de Programmation Militaire (LPM)** :
  - Protection des OIV (Opérateurs d'Importance Vitale)
  - Certification ANSSI
- **Responsabilité** : responsabilité pénale des dirigeants en cas de négligence grave

1.2 Enjeux de la sécurité

Enjeux sociétaux et humains

- **Protection de la vie privée**
- **Confiance numérique** : e-commerce, e-administration
- **Facteur humain** : premier maillon faible (erreurs, négligence) mais aussi première ligne de défense

2. La triade CIA (ou DIC)

Fondement conceptuel de toute démarche de sécurité. Ces trois objectifs sont souvent contradictoires et nécessitent des arbitrages.

2.1 Confidentialité (Confidentiality)

Définition : Propriété selon laquelle l'information n'est pas mise à la disposition ou divulguée à des personnes, entités ou processus non autorisés.

Moyens techniques :

- **Chiffrement** : symétrique (AES) et asymétrique (RSA)
- **Contrôle d'accès** : ACL (Access Control Lists), RBAC (Role-Based Access Control)
- **Authentification forte** : 2FA, biométrie
- **Masquage** : tokenisation, anonymisation
- **Exemple concret :** Seul le destinataire légitime d'un email peut lire son contenu (chiffrement de bout en bout).

2.2 Intégrité (Integrity)

Définition : Propriété selon laquelle l'information n'a pas été altérée ou modifiée de façon non autorisée.

Moyens techniques :

- **Fonctions de hachage** : SHA-256, MD5 (obsolète)
- **Signatures numériques**
- **Checksums** (sommes de contrôle)
- **Journaux d'audit** (logs) infalsifiables
- **Contrôle de version** (ex: Git)
- **Exemple concret :** Un virement bancaire dont le montant ne peut pas être modifié entre l'émission et la réception.

2.3 Disponibilité (Availability)

Définition : Propriété selon laquelle l'information est accessible et utilisable sur demande par une entité autorisée.

Moyens techniques :

- **Redondance matérielle** : RAID, clusters
- **Sauvegardes** : règle du 3-2-1 (3 copies, 2 supports différents, 1 hors site)
- **Plan de Reprise d'Activité (PRA)** et Plan de Continuité d'Activité (PCA)
- **Protection contre les dénis de service** (anti-DDoS)
- **Bande passante dimensionnée**
- **Exemple concret :** Un site e-commerce accessible 24h/24 et 7j/7, même en cas de pic de connexions ou de panne matérielle.

2.4 Autres critères complémentaires

- **Non-répudiation** : impossibilité de nier avoir effectué une action (signature numérique)
- **Authenticité** : garantir que l'information provient bien de la source déclarée
- **Traçabilité** : capacité à reconstituer l'historique des actions

3. Principes fondamentaux de la sécurité

3.1 Défense en profondeur (Layered security)

Concept : Multiplier les barrières de sécurité pour qu'un attaquant doive franchir plusieurs obstacles avant d'atteindre sa cible.

Les 7 couches de la défense en profondeur :

- **Politique de sécurité** : règles, procédures, formation
- **Sécurité physique** : badges, gardiens, serrures
- **Périmètre réseau** : pare-feu, IDS/IPS
- **Réseau interne** : VLANs, segmentation, NAC
- **Hôtes** : antivirus, HIDS, durcissement (hardening)
- **Applications** : code sécurisé, WAF
- **Données** : chiffrement, sauvegardes
- **Analogie :** Un château fort avec douves, remparts, fossés, pont-levis, herses, et gardes.

.2 Principe du moindre privilège (Least Privilege)

Concept : Un utilisateur, un programme ou un processus ne doit disposer que des droits strictement nécessaires pour accomplir sa tâche, et pour une durée limitée.

Applications :

- **Utilisateurs** : pas de droits administrateur en permanence
- **Comptes de service** : droits minimaux sur la base de données
- **Règle du "need-to-know"** : accès à l'information uniquement si nécessaire
- **Segmentation des tâches** (Separation of Duties)
- **Exemple concret :** Un stagiaire a accès en lecture seule aux dossiers partagés, pas en écriture.

3.3 Principe du maillon faible

Concept : La sécurité d'un système est aussi forte que son élément le plus vulnérable.

Points faibles typiques :

- **Facteur humain** : phishing, mots de passe faibles, clés USB trouvées
- **Composants non patchés** : vulnérabilités non corrigées
- **Configuration par défaut** : mots de passe par défaut non modifiés
- **Sous-traitants** : accès non contrôlés des prestataires
- **Exemple concret :** Un réseau ultra-sécurisé compromis parce qu'un employé a branché une clé USB trouvée dans le parking contenant un malware.

3.4 Principe de la simplicité

Concept : Plus un système est complexe, plus il est difficile à sécuriser.

Implications :

- Complexité = plus de bugs et de failles potentielles
- Complexité = difficulté d'audit et de maintenance
- Préférer des solutions éprouvées et standardisées (KISS principle)
  "Keep It Simple, Stupid" or "Keep It Short and Simple"

4. Gestion des risques

4.1 Définitions fondamentales

Terme	Définition	Exemple
Actif	Tout ce qui a de la valeur pour l'organisation	Serveur de base de données clients
Menace	Cause potentielle d'un incident non désiré	Pirate informatique, inondation
Vulnérabilité	Faiblesse pouvant être exploitée par une menace	Logiciel non patché, mot de passe faible
Risque	Combinaison de la probabilité et de l'impact d'un événement	Probabilité de piratage × impact financier
Impact	Conséquence de la réalisation d'une menace	Perte de 1M€, fermeture administrative

4.2 Processus d'analyse des risques

Étape 1 : Identification des actifs

- Inventaire matériel (serveurs, postes, équipements réseau)
- Inventaire logiciel (applications, bases de données)
- Données (clients, financières, RH)
- Ressources humaines

4.2 Processus d'analyse des risques

Étape 2 : Identification des menaces

- **Menaces naturelles** : incendie, inondation, séisme
- **Menaces accidentelles** : erreur humaine, panne
- **Menaces intentionnelles** : hacking, malveillance interne, espionnage
- **Menaces technologiques** : obsolescence, bug

4.2 Processus d'analyse des risques

Étape 3 : Évaluation des vulnérabilités

- Audits techniques (tests d'intrusion)
- Analyse de configuration
- Revue de code
- Enquêtes sociales (ingénierie sociale)

4.2 Processus d'analyse des risques

Étape 4 : Estimation des risques

Formule simplifiée : Risque = Probabilité × Impact

Matrice des risques (exemple) :

Impact ↓ / Probabilité →	Faible	Moyen	Élevé
Faible	Acceptable	Surveiller	Traiter
Moyen	Surveiller	Traiter	Prioritaire
Élevé	Traiter	Prioritaire	Critique

4.3 Stratégies de traitement des risques

Stratégie	Description	Exemple
Réduire	Mettre en place des mesures pour diminuer la probabilité ou l'impact	Installer un pare-feu, former les utilisateurs
Transférer	Faire porter le risque par un tiers	Assurance cyber, externalisation
Éviter	Supprimer l'activité qui génère le risque	Arrêter un service trop vulnérable
Accepter	Conserver le risque en connaissance de cause	Risque résiduel après mesures

4.4 Risque résiduel

- Le risque qui subsiste après la mise en œuvre des mesures de sécurité. Il doit être :
- Explicitement identifié
- Documenté
- Accepté par la direction

5. Politique de sécurité (PSSI)

5.1 Définition

La Politique de Sécurité du Système d'Information (PSSI) est un document cadre qui formalise la vision, les orientations stratégiques, les règles et les responsabilités en matière de sécurité.

5.2 Structure typique d'une PSSI

1. Préambule et contexte

- Objectifs du document
- Périmètre d'application (toute l'organisation, filiales, sous-traitants)
- Références légales et réglementaires

2. Engagements de la direction

- Déclaration d'importance de la sécurité
- Allocation des ressources

5.2 Structure typique d'une PSSI

3. Rôles et responsabilités

- **RSSI** (Responsable de la Sécurité des Systèmes d'Information) : pilotage
- **Correspondants sécurité** : relais dans les directions
- **Utilisateurs** : respect des règles
- **DPO** (Délégué à la Protection des Données) : conformité RGPD

4. Règles générales

- Gestion des identités et des accès
- Classification des informations (confidentiel, interne, public)
- Utilisation des équipements (ordinateurs, smartphones)
- Télétravail et mobilité

5.2 Structure typique d'une PSSI

5. Règles spécifiques

- Sécurité physique
- Sécurité des réseaux
- Sécurité des applications
- Sauvegardes
- Gestion des incidents

6. Sanctions et contrôles

- Disciplinaires
- Techniques (audits)

5.3 Charte informatique (déclinaison pour les utilisateurs)

- Document simplifié, signé par chaque utilisateur, contenant :
- Règles de mots de passe
- Usage acceptable d'Internet et de la messagerie
- Interdiction des logiciels non autorisés
- Procédure en cas d'incident

6. Menaces et acteurs

6.1 Typologie des attaquants

Type d'acteur	Motivation	Compétences	Exemples
Hacktivistes	Politique, idéologique	Moyennes	Anonymous
Cybercriminels	Financière	Élevées	Rançongiciels (ransomware)
États-nations	Espionnage, sabotage	Très élevées	APT (Advanced Persistent Threat)
Initiateurs internes	Négligence ou malveillance	Faibles à moyennes	Employé mécontent
Script kiddies	Notoriété, amusement	Faibles	Utilisation d'outils existants

6.2 Classification des attaques

Selon la source :

- **Internes** : initiées depuis l'intérieur de l'organisation
- **Externes** : initiées depuis l'extérieur

Selon la cible :

- Matérielle, logicielle, humaine, réseau

Selon l'impact :

- Passive (écoute) vs Active (modification)

7. Évolution et tendances

7.1 Nouvelles menaces liées à l'IA

- **Attaques adversariales** : tromper les modèles d'IA
- **Deepfakes** : usurpation d'identité vidéo/audio
- **Phishing augmenté** : emails plus convaincants générés par IA

7.2 Évolution des défenses

- **IA pour la détection** : analyse comportementale, anomalies
- **SOAR** (Security Orchestration Automation and Response) : automatisation des réponses
- **Zero Trust** : "Ne jamais faire confiance, toujours vérifier"