Sécurité et Criminalistique des Bases de Données

Chapitre 1 : Sécurité et technologies de l'information

M. Laïdi FOUGHALI

l.foughali@univ-skikda.dz

(Site ⇒ al-moualime.com)

Université de Skikda — Département d'Informatique

1re Année Master Sécurité Informatique (SI)

Année académique 2025-2026

Version v1.0 — 2026-02-10 à 08:37:04

Plan

Vue d'ensemble

Objectif du chapitre

Maîtriser la sécurité des bases de données selon trois axes complémentaires

Axe 1 : Piliers CIA

- **Confidentialité** : accès réservé aux entités autorisées (chiffrement, authentification)
- **Intégrité** : données exactes et cohérentes, modifications contrôlées
- **Disponibilité** : accès fiable 24/7, tolérance aux pannes

Axe 2 : Menaces

- **Attaques externes** : pirates, hackers, cyberterrorisme
- **Attaques internes** : 50%
- **Malwares** : virus, ransomwares, chevaux de Troie
- **Ingénierie sociale** : 90% (phishing)

Axe 3 : Solutions de protection

- **Défense multicouche** : réseau (pare-feu, IDS/IPS Systèmes de Détection/Prévention d'Intrusion) + OS Système d'Exploitation (correctifs, antivirus) + SGBD Système de Gestion de Base de Données (contrôles d'accès, audit)
- **Cycle en 4 étapes** : *Prévention* → *Détection* → *Réaction* → *Récupération*
- **Amélioration continue** : vigilance 24/7 et adaptation aux nouvelles menaces

GDPR — General Data Protection Regulation

Définition

Le **GDPR** est un règlement européen depuis mai 2018 qui impose la protection des données personnelles de citoyens européens.

Les cinq droits fondamentaux

1. **Consentement explicite** : accord clair avant toute collecte
2. **Droit à l'oubli** : effacement sur demande
3. **Portabilité** : récupération des données (CSV Comma-Separated Values, JSON JavaScript Object Notation)
4. **Transparence** : explication de l'usage des données
5. **Notification** : 72h max pour signaler une fuite

Données protégées

Nom, email, IP Adresse Internet, cookies, GPS Géolocalisation, N° sécurité sociale

Sanctions

20M€ ou **4% CA** Chiffre d'Affaires **mondial**
Ex : Google 50M€ (2019)

HIPAA — Health Insurance Portability and Accountability Act

Définition

Le **HIPAA** (1996) oblige les acteurs médicaux à protéger les **PHI** Protected Health Information, toute information médicale identifiable d'un patient.

Les cinq exigences

1. **Confidentialité** : accès limité au personnel autorisé
2. **Intégrité** : aucune modification sans trace
3. **Disponibilité** : accès garanti aux urgences
4. **Piste d'audit** : traçabilité complète des accès
5. **Chiffrement** : données cryptées (transit et stockage)

PHI

Dossiers médicaux, analyses, ordonnances

Sanctions

Civil : **1.5M$/an**
Pénal : **250k$** + **10 ans** prison

Le paradoxe de la sécurité informatique

Progrès indéniables

Les investissements en cybersécurité ont été multipliés par trois. Les formations sont obligatoires dans les universités. Les standards (RGPD, ISO Organisation Internationale de Normalisation 27001) sont massivement adoptés.

Pourtant : la sécurité BD reste négligée

- Pénurie critique : 10 offres pour 1 expert disponible (2024)
- 80% des données sensibles concentrées dans les BD Bases de Données (IBM 2024)
- Les BD constituent la cible n°1 des hackers (Verizon 2024)

Explication du paradoxe

On investit dans la sécurité du périmètre (pare-feu, antivirus) mais on néglige le coffre-fort lui-même. Or c'est dans les BD que se trouvent les vrais trésors : CB Cartes Bancaires, dossiers médicaux, secrets industriels.

Chiffres clés de la cybersécurité

Constats alarmants (Verizon 2024)

- **55%** des violations = menace INTERNE (employés)
- **4.45 M$** ($\approx$ 4.1 M€) = coût moyen par violation (IBM 2024)
- **277 jours** = temps moyen de détection (9 mois)
- **90%** des attaques = hameçonnage
- **95%** des incidents = erreur humaine

Impact sur l'entreprise

- Amendes RGPD : jusqu'à 20M€ ou 4% CA mondial
- Perte clientèle : -30% en moyenne
- Procès collectifs possibles

À retenir

9 mois de détection = temps pour copier des millions de dossiers sans être inquiété.

Les quatre piliers d'un environnement sécurisé

Le cycle de sécurité

1. **PRÉVENTION** : bloquer les attaques avec pare-feu, mots de passe robustes, chiffrement
2. **DÉTECTION** : repérer les intrusions via alertes et journaux d'activité
3. **RÉACTION** : limiter les dégâts en isolant la BD et bloquant l'accès pirate
4. **RÉCUPÉRATION** : restaurer via sauvegardes et reconstruction

Principe fondamental

Aucun système n'est sécurisé à 100%. La sécurité est un processus continu, pas un produit qu'on achète une fois.

Les trois règles d'or

Amélioration continue + Vigilance 24/7 + Adaptation aux nouvelles menaces

Le Triangle C.I.A. — Vue d'ensemble

Les trois objectifs fondamentaux de la sécurité

Le sigle **C.I.A.** (conservé en anglais pour sa reconnaissance internationale) représente les trois principes fondamentaux de toute stratégie de sécurité :

1. **Confidentiality** (Confidentialité) : protéger les informations sensibles
2. **Integrity** (Intégrité) : garantir l'exactitude et la cohérence des données
3. **Availability** (Disponibilité) : assurer l'accès aux ressources quand nécessaire

Le triangle équilatéral : une métaphore essentielle

Ces trois piliers doivent être équilibrés comme les côtés d'un triangle équilatéral. Un déséquilibre dans l'un des piliers compromet l'ensemble du système de sécurité. Ces trois objectifs sont interdépendants et doivent être adressés simultanément.

Principe architectural

Toute architecture de sécurité doit prendre en compte les trois piliers simultanément pour être efficace.

Confidentialité — Premier pilier du triangle CIA (1/2)

Définition et objectifs

La **confidentialité** assure que seules les personnes explicitement autorisées peuvent accéder aux informations sensibles. Les trois objectifs principaux sont :

- Limiter l'accès selon le principe du moindre privilège
- Bloquer tout accès non autorisé via une authentification robuste
- Protéger la vie privée conformément aux réglementations (HIPAA, RGPD)

Mécanismes d'authentification

L'authentification vérifie l'identité de l'utilisateur avant d'accorder l'accès :

- **Mots de passe robustes** : minimum 12 caractères, complexité élevée
- **Biométrie** : empreintes digitales, reconnaissance faciale, iris
- **2FA/MFA** Authentification à 2 / Multi-Facteurs : combinaison (mot de passe + SMS)

Autres mécanismes essentiels

Chiffrement : protection des données au repos et en transit
Audit : journalisation complète de tous les accès pour la traçabilité

Contrôle d'accès — Premier pilier du triangle CIA (2/2)

Les trois modèles de contrôle d'accès

ACL Access Control Lists : listes définissant explicitement qui accède à quelles ressources.

Exemple : "Alice peut lire le fichier X mais pas le modifier."

RBAC Role-Based Access Control : l'accès dépend du rôle dans l'organisation.

Exemple : tous les "Managers" approuvent les congés.

ABAC Attribute-Based Access Control : l'accès dépend d'attributs de l'utilisateur, de la ressource ou du contexte.

Exemple : accès si employé RH Ressources Humaines ET connexion bureau ET entre 8h-18h.

Exemple de violation de confidentialité

Cas réel : Employé d'hôpital consulte par curiosité les dossiers médicaux de patients célèbres, sans raison médicale.

Détection : Auto-Audit détecte les accès anormaux (patient non assigné).

Sanction : 50,000$ par violation + licenciement immédiat.

Solution : Principe du moindre privilège + surveillance temps réel.

Intégrité — Le pilier le plus difficile (1/3)

Définition : quatre caractéristiques essentielles

L'**intégrité** garantit que les données restent exactes (conformes à la réalité), cohérentes (sans contradictions), complètes (sans perte) et fiables (dignes de confiance) durant tout leur cycle de vie.

Pourquoi le pilier le plus difficile ?

L'intégrité exige une surveillance constante et des processus rigoureux à tous les niveaux. Les vecteurs de compromission sont nombreux : bugs logiciels, erreurs de saisie humaine, modifications non autorisées, corruption matérielle (inversion spontanée d'un bit causée par radiation cosmique ou défaillance), et attaques ciblées.

Techniques de maintien (partie 1)

1. **Contraintes de base de données** : Règles imposées au niveau du SGBD, comme DOMAIN, PRIMARY KEY, CHECK et TRIGGERS.
2. **Contrôle de version** : Permet de tracer et annuler les modifications : ROLLBACK et restauration à un point dans le temps.
3. **Sommes de contrôle** : MD5 Message Digest 5, SHA-512 Secure Hash Algorithm, etc.

Intégrité — Le pilier le plus difficile (2/3)

Techniques de maintien (partie 2)

4. Piste d'audit : Enregistrement exhaustif de toutes les opérations sur les données. Pour chaque modification : utilisateur, horodatage, opération (INSERT/UPDATE/DELETE), valeur avant et après. Ces journaux immuables garantissent la fiabilité juridique.

5. Validation des entrées : Protection contre données malveillantes. Le nettoyage supprime le code dangereux saisi (ex : scripts JavaScript Langage de programmation web). Les requêtes paramétrées empêchent l'injection SQL Structured Query Language en séparant code et données, traitant les entrées utilisateur comme valeurs simples, jamais comme code exécutable.

6. Séparation des tâches : Aucune personne ne contrôle seule une opération complète. Exemple bancaire : créer un virement $\neq$ l'approuver $\neq$ l'exécuter. Cette séparation réduit fraude interne et erreurs.

Principe fondamental

L'intégrité nécessite la combinaison de ces six techniques appliquées simultanément à tous les niveaux.

Intégrité — Exemple d'une transaction bancaire (3/3)

Scénario : Transfert de 1000 euros

Un client A transfère 1000€ vers le compte d'un client B. Les exigences d'intégrité sont : montant identique des deux côtés, transaction atomique (tout ou rien), historique immuable (pas de modification post-facto), soldes cohérents (A + B = constant), horodatage précis et traçabilité complète.

Scénario de violation : bug système

Bug : Le compte B est crédité de 1000€ MAIS le compte A n'est PAS débité de 1000€.
Violation d'intégrité : 1000€ est créé de nulle part, ce qui crée une incohérence dans le système.
Impact catastrophique : Si ce bug se répète 1 million de fois, cela représente 1 million d'euros de perte pour la banque.
Détection tardive : L'audit devient extrêmement difficile après plusieurs jours ou semaines.
Solution : Implémenter des transactions ACID Atomicité, Cohérence, Isolation, Durabilité avec contraintes CHECK vérifiant systématiquement la cohérence des soldes.

Disponibilité — Troisième pilier du triangle CIA (1/10)

Définition

La **disponibilité** correspond à la capacité d'un système d'information à assurer l'accès continu à ses services et à ses données pour les utilisateurs autorisés, **lorsque ceux-ci en ont besoin**, conformément aux engagements de niveaux de service définis dans le **SLA** Service Level Agreement - Accord de Niveau de Service client/fournisseur.

Niveaux de disponibilité : interprétation des « nines »

- 99% : jusqu'à 3,65 jours d'indisponibilité par an (inacceptable)
- 99,9% (« three nines ») : 8,76 heures d'indisponibilité par an
- **99,99% (« four nines ») : 52,6 minutes par an** ← standard courant
- 99,999% (« five nines ») : 5,26 minutes par an (forte exigence technique)
- 99,9999% (« six nines ») : 31,5 secondes par an (niveau exceptionnel)

Réalité économique

L'augmentation du niveau de disponibilité est une fonction **non linéaire** des coûts liés à l'architecture, à la redondance et à l'exploitation.

Menaces sur la disponibilité (2/10)

Principales sources d'indisponibilité

1. Attaques DoS / DDoS Déni de Service / Déni de Service Distribué Objectif : rendre un service indisponible.
Techniques principales :

- Saturation réseau (volumétrique)
- Exploitation de protocoles (ex. SYN Synchronize flood - inondation)
- Surcharge applicative (ex. HTTP HyperText Transfer Protocol flood)

2. Pannes matérielles Défaillance des composants physiques : serveurs, disques, alimentation, surchauffe, catastrophes naturelles.
Exemples : HDD Hard Disk Drive plus fragiles que SSD Solid State Drive, coupures électriques. **3. Erreurs humaines** Mauvaises manipulations ou configurations : suppression accidentelle de fichiers, mise à jour défectueuse, câbles mal branchés. **Remarque :** première cause d'incidents en pratique. **4. Logiciels malveillants** Rendre un système indisponible : Ransomware (chiffre les fichiers et demande une rançon), Wiper (détruit les fichiers), Logic bomb (code dormant qui s'active à un moment précis), etc.

Menaces sur la disponibilité - Attaque SYN Flood (3/10)

SYN Flood

Le serveur est bloqué avant même que la connexion ne soit établie. Une connexion TCP Transmission Control Protocol se fait en trois étapes :

- Le client envoie **SYN** (demande de connexion)
- Le serveur répond **SYN-ACK** Synchronize-Acknowledge
- Le client confirme avec **ACK** Acknowledge

Envoi d'un grand nombre de messages **SYN**, sans finaliser la connexion.

Conséquences

- Les connexions restent en attente
- La mémoire du serveur se remplit
- Les utilisateurs légitimes ne peuvent plus se connecter

Niveau attaqué

Couche réseau / transport (TCP)

Menaces sur la disponibilité - Attaque HTTP Flood (4/10)

Idée centrale

Le serveur est submergé par de fausses requêtes HTTP légitimes.
HTTP est le protocole du Web permettant : de charger une page, de cliquer sur un lien ou d'envoyer un formulaire.
Chaque action génère une requête HTTP normale. L'attaquant envoie un grand nombre (millions) de requêtes HTTP valides : pages et API Application Programming Interface.

Conséquences

- Saturation du CPU Central Processing Unit - Processeur
- Surcharge de la base de données
- Application lente ou totalement indisponible

Niveau attaqué

Couche application (Web)

Haute Disponibilité : Redondance des composants (5/10)

Serveurs en cluster

- **Active-Active** : tous les serveurs sont actifs, la charge est répartie
- **Active-Passive** : un serveur de secours prend le relais en cas de panne
- **Load balancing** Répartition de charge : répartition automatique de la charge

RAID Redundant Array of Independent Disks - Ensemble Redondant de Disques Indépendants

- **RAID 1** : miroir des données
- **RAID 5** : parité simple, tolère 1 disque en panne
- **RAID 6** : double parité, tolère 2 disques en panne
- **RAID 10** : performance et sécurité

Réplication des données

- **Synchrone** : mise à jour en temps réel, cohérence garantie
- **Asynchrone** : léger décalage, meilleure performance
- Architectures : **master-slave** maître-esclave ou **multi-master** multi-maître

Haute Disponibilité : Alimentation et sauvegardes (6/10)

Alimentation électrique

- UPS Uninterruptible Power Supply - Alimentation Sans Interruption, onduleurs pour les coupures courtes
- Générateurs diesel pour l'autonomie prolongée
- **Dual power feeds** Double alimentation : deux sources électriques indépendantes (ex : réseau principal + générateur secours)

Sauvegardes

- **Complète** : sauvegarde de toutes les données
- **Incrémentale** : depuis la dernière sauvegarde
- **Différentielle** : depuis la dernière sauvegarde complète

Règle 3-2-1 et tests

3 copies des données, 2 supports différents, 1 copie hors site et des tests réguliers (au moins trimestriels)

Comprendre la fiabilité des RAID : Intuition (7/10)

Intuition de base

La **fiabilité** mesure la probabilité qu'un système fonctionne sans panne. Pour un disque seul avec fiabilité $R_d = 0{,}95$, cela signifie :

- 95% de chance de fonctionner correctement pendant 1 an
- 5% de risque de panne

Comment combiner plusieurs disques ?

RAID 0 (striping) répartition par tranches : Données réparties sur 2 disques

- Si UN SEUL disque tombe $\rightarrow$ TOUTES les données sont perdues
- Les risques se **multiplient** : $R_{\text{RAID0}} = R_d \times R_d = R_d^2$
- Moins fiable qu'un disque seul !

RAID 1 (mirroring) miroir : Données dupliquées sur 2 disques

- Il faut que LES DEUX disques tombent pour perdre les données
- Le système survit tant qu'au moins 1 disque fonctionne
- Beaucoup plus fiable qu'un disque seul !

Fiabilité extrême d'un RAID : Formules (8/10)

Définition

La **fiabilité** d'un système est la probabilité qu'il fonctionne correctement pendant un intervalle de temps donné. Pour un RAID, elle dépend de :

- fiabilité d'un disque R_d
- type de RAID
- nombre de disques

Extrêmes : RAID 0 vs RAID 1

- **RAID 0** (répartition par tranches, 2 disques) : $R_{\text{RAID0}} = R_d^2$
  $\rightarrow$ perte totale si un disque tombe
- **RAID 1** (miroir, 2 disques) : $R_{\text{RAID1}} = 1 - (1 - R_d)^2$
  $\rightarrow$ tolère 1 panne

Remarques

RAID 0 $\rightarrow$ performance maximale, fiabilité minimale
RAID 1 $\rightarrow$ sécurité maximale, coût doublé

Exercice : Fiabilité des RAID 0 et RAID 1 (9/10)

Énoncé

On dispose de deux disques durs identiques, chacun ayant une fiabilité annuelle

$$R_d = 0{,}95.$$

Calculer la fiabilité globale du système dans les cas suivants :

1. Architecture RAID 0
2. Architecture RAID 1

Formules utilisées

$$R_{\text{RAID 0}} = R_d^2 \qquad R_{\text{RAID 1}} = 1 - (1 - R_d)^2$$

Objectif pédagogique

Mettre en évidence l'opposition entre les deux architectures :

- RAID 0 : performance élevée mais faible tolérance aux pannes
- RAID 1 : redondance et forte fiabilité

Sites de secours (10/10)

Comparaison des sites de secours

Type	Activation	Données	Usage / Coût
HOT	immédiate (min)	synchro temps réel	critique, aucun temps d'arrêt toléré
WARM	quelques heures	synchro régulière	important, petit délai acceptable
COLD	48-72 h	pas pré-chargées	tolère une indisponibilité de 1 à 3 jours, économique

Choix du type de site

Dépend du :

- **RTO** Recovery Time Objective - Objectif de Temps de Récupération : délai maximal acceptable pour rétablir le service
- **RPO** Recovery Point Objective - Objectif de Point de Récupération : perte maximale de données acceptable

Équilibre et compromis du Triangle C.I.A.

Tensions naturelles entre les piliers

Confidentialité vs Disponibilité : renforcer la sécurité peut ralentir l'accès.

- MFA Authentification Multi-Facteurs allonge le temps de connexion
- Chiffrement CPU-intensif peut retarder le traitement des données

Intégrité vs Performance : plus de contrôles et contraintes ralentissent le système.

- Contraintes de base de données sur INSERT/UPDATE
- Transactions ACID ajoutent un overhead surcharge notable

Disponibilité vs Coût : améliorer la disponibilité nécessite plus de ressources.

- La redondance double au minimum le matériel
- Passer de 99,9% à 99,99% de disponibilité peut coûter 10 fois plus cher

Trouver le juste équilibre

L'équilibre optimal dépend des besoins métier, du niveau de risque acceptable et des contraintes budgétaires.

Vue d'ensemble des menaces

Qui nous attaque et pourquoi ?

Deux grandes catégories de menaces pèsent sur les bases de données :

1. **Menaces externes** (45%) : attaquants extérieurs à l'organisation
2. **Menaces internes** (55%) : employés, administrateurs, ex-employés

Le paradoxe de la sécurité

55% des violations viennent de l'intérieur

Pourtant, 80% des budgets sécurité sont dépensés contre les menaces externes !

Les quatre vecteurs d'attaque

1. Ingénierie sociale (90% des attaques) : tromper l'humain
2. Vulnérabilités Web : failles dans les sites/applications
3. Malware : virus, vers, chevaux de Troie, rançongiciels
4. Applications trompeuses : faux sites qui imitent les vrais

Menaces EXTERNES — Qui sont-ils ?

Les quatre profils d'attaquants externes

1. **Hackers éthiques** (chapeaux blancs) : professionnels légaux qui cherchent les failles pour les corriger
   - Rémunération : 500-2000€/jour
   - Travaillent avec autorisation écrite
2. **Script Kiddies** (pirates amateurs) : adolescents (13-19 ans) utilisant des outils gratuits
   - Dangereux par leur nombre : 100× plus nombreux que les pros
   - Ne comprennent pas ce qu'ils font
3. **Cybercriminels** (chapeaux noirs) : motivés par l'argent
   - Rançongiciels, vol de données, extorsion
   - Impact 2023 : 6000 milliards USD
4. **Espionnage d'État** : groupes soutenus par des gouvernements
   - Budgets illimités
   - Ciblent secrets d'État et propriété intellectuelle

Cas Mafiaboy (2000) — Quand un ado paralyse Internet

Le Script Kiddie qui a marqué l'histoire

L'attaquant : Michael Calce, Canadien de **15 ans**
Pseudonyme : "Mafiaboy" (son surnom utilisé en ligne)
L'attaque :

- Paralyse Yahoo, Amazon, CNN, eBay avec des outils gratuits téléchargés
- Attaque par saturation DDoS (*Distributed Denial of Service*)
- Impact : 1,7 milliard USD de pertes en quelques heures

Les conséquences :

- Peine : 8 mois de détention pour mineur
- Aujourd'hui : consultant en cybersécurité reconnu

La leçon à retenir

Un adolescent avec des outils simples peut paralyser
les plus grands sites d'Internet en quelques heures

Cas WannaCry (2017) — La pandémie numérique

Le malware

Nom : WannaCry (de l'anglais "Want to Cry" = "envie de pleurer")
Type : Ver + Rançongiciel combinés
Faille : SMB v1 (*Server Message Block version 1*)

La propagation

- 230 000 PC, 150 pays
- En 4 jours seulement
- Exploit "EternalBlue" volé à la NSA (*National Security Agency*)
- Automatique (sans clic)

Les victimes

- NHS (*National Health Service*) UK : opérations chirurgicales annulées
- Renault : usines arrêtées
- FedEx, Telefónica
- Ambulances détournées

L'arrêt miraculeux

Un chercheur découvre par hasard un "bouton d'arrêt" dans le code
Solution : Enregistrer un nom de domaine pour 10$ → Propagation stoppée !

La leçon

Faire les MAJ à temps — Microsoft publia 2 mois avant le correctif !

Menaces INTERNES — Le danger méconnu

Le chiffre qui fait peur

55% des violations proviennent de **L'INTÉRIEUR** de l'organisation

Pourquoi sont-elles si dangereuses ?

Les employés ont trois avantages sur les pirates externes :

1. **Accès légitime** : ils possèdent déjà identifiants, mots de passe et permissions. Pas besoin de pirater pour entrer.
2. **Connaissance interne** : ils savent exactement où sont stockées les données sensibles (serveurs, bases de données, dossiers)
3. **Confiance implicite** : les systèmes de sécurité sont configurés pour les faire confiance. On surveille les étrangers, pas ses collègues.

Les quatre profils de menaces internes

44% Négligents : clic sur email piégé, mot de passe "123456", clé USB perdue
23% Malveillants : vol de données, sabotage, espionnage pour concurrent
20% Administrateurs piratés : pirate obtient accès admin via phishing
13% Ex-employés : employé parti il y a 6 mois a toujours son compte actif

Capital One (2019) — Quand la négligence coûte cher

Le contexte

Profil : Ingénieur cloud, négligent (pas malveillant)
L'entreprise : Capital One, grande banque américaine

L'erreur fatale

Configure mal un pare-feu sur serveur cloud Amazon AWS (*Amazon Web Services*)

- Serveur censé être privé → accidentellement exposé sur Internet public
- Une pirate externe (Paige Thompson) découvre la faille
- Elle aspire 100 millions de dossiers clients en quelques heures

Les conséquences

- **Données volées** : noms, adresses, revenus, scores de crédit, numéros de sécurité sociale
- **Amende** : 190 millions USD par le gouvernement américain
- **Réputation** : confiance des clients détruite pendant des années
- **Procès** : centaines de plaintes collectives

Tesla (2020) — Le vol de propriété intellectuelle

Le contexte

Profil : Ingénieur logiciel, action malveillante
L'entreprise : Tesla, constructeur automobile électrique

L'action criminelle

Objectif : Voler secrets du pilote automatique (Autopilot)
Actions :

- Télécharge massivement le code source confidentiel
- Transfert 300 000 fichiers vers compte personnel iCloud
- Prévoit partir chez concurrent chinois XPeng avec les secrets

La détection

Signal d'alarme : Système d'audit (logs & caméra) détecte activité anormale

- Téléchargement 100× supérieur à la normale
- Alerte automatique déclenchée
- Investigation lancée → vol découvert avant départ de l'ingénieur

Menaces INTERNES — Comment se protéger ?

Cinq protections essentielles contre les menaces internes

1. Former les utilisateurs — Expliquer régulièrement les erreurs fréquentes (emails frauduleux, partage de mots de passe) pour réduire les risques humains.
2. Appliquer le moindre privilège — Donner uniquement les droits nécessaires au travail afin de limiter les dégâts en cas d'erreur ou d'abus.
3. Surveiller les activités — Analyser les connexions et accès aux données pour détecter rapidement un comportement anormal.
4. Gérer automatiquement les accès — Activer et désactiver les comptes sans intervention manuelle pour éviter les oublis dangereux.
5. Séparer les responsabilités — Répartir les actions sensibles entre plusieurs personnes pour empêcher une manipulation seule.

Idée clé

La majorité des incidents viennent d'actions humaines : la prévention repose sur les procédures autant que sur la technologie.

Vecteur d'attaque — Ingénierie sociale : Phishing

Définition

L'ingénierie sociale consiste à manipuler la psychologie humaine pour obtenir des informations ou provoquer une action risquée. Le phishing (hameçonnage) imite une entité de confiance afin de tromper l'utilisateur.

Analogie

Un faux facteur demande vos clés pour "vérifier" votre boîte aux lettres.

Leviers

Urgence : compte bloqué rapidement
Curiosité : contenu surprenant
Peur : sanction ou problème administratif

Risque

Vol d'identifiants, données personnelles ou installation de malware.

Vecteur d'attaque — SQL Injection (SQLi)

Définition

SQLi (*SQL Injection*) : insertion de code SQL dans une entrée utilisateur. Si l'application mélange données et requêtes, la base exécute une commande non prévue.

Mécanisme

Entrée malveillante '' OR 1=1 –'
Une requête mal sécurisée peut alors contourner un contrôle d'accès.

Risque

Accès non autorisé, extraction ou modification des données.

Vecteur d'attaque — Cross-Site Scripting (XSS)

Définition

XSS (*Cross-Site Scripting*) : injection de script dans une page web. Le navigateur des utilisateurs exécute ce code en pensant qu'il provient du site légitime.

Types

Stocké : script enregistré sur le serveur
Réfléchi : script transmis via un lien piégé

Risque

Vol de session, usurpation de compte ou redirection malveillante.

Vecteur d'attaque — Cross-Site Request Forgery (CSRF)

Définition

CSRF (*Cross-Site Request Forgery*) : une requête est envoyée à un site où la victime est connectée, sans qu'elle le sache, en utilisant sa session authentifiée.

Mécanisme

Le navigateur envoie automatiquement les cookies d'authentification avec la requête.

Risque

Actions non voulues : modification de paramètres, transactions ou suppression de données.

Vecteur d'attaque — Path Traversal

Définition

Path Traversal : manipulation de chemins de fichiers pour accéder à des ressources hors du dossier autorisé.

Mécanisme

Séquences comme '../' pour remonter l'arborescence et atteindre des fichiers sensibles.

Risque

Lecture de fichiers confidentiels ou de configuration système.

Malware — Vue d'ensemble

Définition

Malware = MALicious softWARE (logiciel malveillant)
Code informatique conçu pour nuire : voler, détruire, espionner, bloquer

L'ampleur du problème

600 000 nouveaux malwares créés **CHAQUE JOUR**
= 219 millions par an

Les cinq grandes familles

1. **Virus** : S'attache à fichiers, besoin action humaine (clic)
2. **Vers** (Worms) : Se propage SEUL via réseau, sans intervention
3. **Chevaux de Troie** : Se déguise en logiciel légitime
4. **Rançongiciels** : Chiffre vos fichiers + demande rançon
5. **Réseaux de zombies** : Millions d'ordinateurs contrôlés à distance

1. Les Virus informatiques

Comment fonctionne un virus ?

Un virus est un programme malveillant qui :

1. S'attache à un fichier légitime (Word, Excel, .exe)
2. Se cache en attendant que vous ouvriez le fichier
3. S'active quand vous cliquez : infection !
4. Cherche d'autres fichiers à infecter (réplication)
5. Exécute sa mission : destruction, espionnage, porte dérobée

Analogie avec virus biologique

Comme un virus biologique (grippe, COVID) :

- Besoin d'un hôte pour survivre (cellule / fichier)
- Se réplique en infectant d'autres hôtes
- Peut muter pour éviter détection (polymorphisme)

2. Les Vers (Worms) — Propagation automatique

Différence clé avec les virus

Virus : Besoin d'un fichier hôte + action humaine (clic)
Ver : Programme AUTONOME, se propage SEUL via Internet

Comment un ver se propage

1. Scanne Internet pour trouver ordinateurs vulnérables
2. Exploite faille de sécurité pour entrer sans permission
3. S'installe sur nouvelle machine
4. Recommence depuis la nouvelle machine → progression exponentielle

Vitesse : Peut infecter 90% d'Internet vulnérable en 10 minutes !

Exemples historiques

ILOVEYOU (2000) : 45 millions PC, email "lettre d'amour"
Conficker (2008) : 9-15 millions PC, encore actif en 2024 !

3. Les Chevaux de Troie — Le déguisement

Origine du nom

Dans la mythologie grecque : les Grecs offrent un cheval de bois géant en "cadeau" aux Troyens. La nuit, soldats cachés à l'intérieur sortent et ouvrent les portes de la ville.
Principe identique : Malware déguisé en logiciel utile ou attractif

Déguisements courants

Logiciels "gratuits" : Photoshop crack, Office gratuit, générateur de clés
Médias : Film.exe, série, jeu vidéo piraté
Optimiseurs PC : "Accélérez votre ordinateur gratuitement !"
Apps mobiles : Fausses applications ou clones d'apps populaires

Les sept types de Trojans

Porte dérobée | Banking (vol bancaire) | Keylogger (enregistre frappes) | Destructif | Spam | Proxy | DDoS

4. Les Rançongiciels — L'extorsion numérique (1/2)

Le modèle criminel

1. Malware entre dans votre ordinateur (email, site piraté)
2. Cherche TOUS vos fichiers importants (documents, photos, bases de données)
3. Les **chiffre** avec algorithme incassable
4. Affiche message : "Payez 500€ en Bitcoin pour récupérer vos fichiers"
5. Deadline : 24-72h sinon prix double ou fichiers détruits

L'ampleur du fléau

2023 : 1,1 milliard USD payés en rançons
Coûts totaux (arrêt activité, restauration) : 20 milliards USD
71% des organisations ont été touchées

4. Les Rançongiciels — Évolution et défense (2/2)

L'évolution des tactiques

Version simple : Juste chiffrement
Double extorsion (2019+) : Chiffrement + Vol de données AVANT - Menace : "Payez ou on publie vos données confidentielles"
Triple extorsion (2020+) : + Contact de VOS clients - "Votre fournisseur a été piraté, vos données sont compromises"

Faut-il payer la rançon ?

FBI et Europol disent NON car :
1. Finance le crime organisé
2. Aucune garantie de récupérer les fichiers (30% n'y arrivent pas)
3. Vous devenez cible répétée (80% sont réattaqués)

La meilleure défense

Sauvegardes régulières + hors ligne + testées régulièrement

5. Les Réseaux de zombies (Botnets)

Comment ça marche ?

1. Pirate infecte des milliers/millions d'ordinateurs avec malware discret
2. Ces ordinateurs deviennent des "zombies" : contrôlés à distance
3. Pirate envoie commandes simultanées à toute son "armée"
4. Zombies obéissent : attaque coordonnée massive

Utilisations criminelles

DDoS : Saturer un site web (millions de requêtes simultanées)
Spam : Envoyer des milliards d'emails publicitaires/phishing
Minage crypto : Utiliser votre électricité pour créer Bitcoin
Vol identifiants : Tester millions de mots de passe simultanément

Vous êtes peut-être zombie !

Signes : Ordinateur lent, ventilateur bruyant, activité réseau étrange

Le cycle de sécurité — Processus continu

Principe fondamental

La sécurité n'est PAS un produit qu'on achète une fois.
C'est un **PROCESSUS CONTINU** qui ne s'arrête jamais.
Métaphore : Comme l'entretien d'une voiture (vidange, révision, pneus)

Les quatre phases du cycle

Phase 1 — ÉVALUATION : Où sont nos failles ? (audit, pentest)
Phase 2 — CONCEPTION : Comment se protéger ? (architecture, outils)
Phase 3 — DÉPLOIEMENT : Mise en place (installation, formation)
Phase 4 — GESTION : Surveillance 24/7, corrections, mises à jour
$\rightarrow$ Retour Phase 1 après 6-24 mois (nouvelles menaces apparaissent)

Erreur fréquente

Faire 1-2-3 puis s'arrêter = Obsolescence rapide et failles non détectées

Défense en profondeur — Les trois couches (1/2)

Principe de base

Ne jamais dépendre d'UNE SEULE protection.
Superposer plusieurs couches de défense indépendantes.
Analogie château médiéval : Douves + murailles + portes + gardes + donjon

Couche 1 — RÉSEAU (périmètre)

- Pare-feu (*firewall*) : Filtre le trafic entrant/sortant
- IDS/IPS (*Intrusion Detection/Prevention Systems*) : Détecte et bloque attaques
- Segmentation : Séparer production, développement, invités

Couche 2 — SYSTÈME (serveurs, ordinateurs)

- Mises à jour sécurité régulières (patchs)
- Antivirus nouvelle génération
- Désactivation services inutiles

Défense en profondeur — Les trois couches (2/2)

Couche 3 — BASE DE DONNÉES (les données elles-mêmes)

- Contrôle d'accès strict (qui peut voir quoi)
- Chiffrement des données sensibles
- Audit complet (journalisation de toutes les actions)

Principe clé : défense multicouche

Si une couche échoue, les autres continuent à protéger.
Exemple : Même si un pirate franchit le pare-feu (couche 1), il doit encore contourner les protections système (couche 2) et base de données (couche 3).

Métaphore

Un château fort ne dépend pas d'une seule muraille —
chaque obstacle ralentit et décourage l'attaquant.

Exemple défense — Attaque SQL Injection

Scénario : Pirate tente SQL Injection

Couche 1 — Réseau : WAF (*Web Application Firewall*) détecte pattern suspect → Bloque 70% des tentatives basiques
Couche 2 — Système : Serveur web valide les entrées utilisateur → Bloque encore 20% des tentatives qui ont passé couche 1
Couche 3 — Base de données : Requêtes paramétrées empêchent injection → Traite tout comme DONNÉES, jamais comme CODE
Couche 3 bis : Même si injection réussit, RBAC (*Role-Based Access Control*) limite dommages → Compte web ne peut QUE lire, pas modifier ni supprimer
Couche 3 ter : Audit enregistre TOUT → Alerte déclenchée, analyse forensique possible
Couche 3 quater : Données chiffrées → Même si vol, illisibles sans clé

Résultat

Attaquant doit franchir 6 barrières → Probabilité succès très faible

Messages essentiels du chapitre

Les trois chiffres à retenir

55% des violations = INTERNES (employés)
90% des attaques = PHISHING (manipulation humaine)
600 000 nouveaux malwares créés CHAQUE JOUR

Les cinq familles de malware

Virus : S'attache à fichiers, besoin clic
Vers : Se propage seul via réseau
Chevaux de Troie : Déguisement en logiciel légitime
Rançongiciels : Chiffre fichiers + demande paiement
Botnets : Réseaux d'ordinateurs zombies contrôlés

Les deux principes de défense

1. Cycle continu : Évaluation → Conception → Déploiement → Gestion → Recommencer
2. Défense multicouche : Réseau + Système + Base de données

Le message final — L'humain au centre

La vérité inconfortable

95% des incidents de sécurité
impliquent une ERREUR HUMAINE
à un moment de la chaîne d'attaque

La sécurité est un processus humain

La technologie seule ne suffit pas. Il faut :

- **Former** régulièrement tous les employés
- **Sensibiliser** aux dangers du phishing et mots de passe
- **Créer une culture** de la sécurité dans l'organisation
- **Comprendre** que chacun est responsable de la sécurité

Rappel priorités

Les bases de données contiennent les actifs les plus précieux :
Données clients | Secrets industriels | Informations médicales | Données financières
Leur protection doit être la PRIORITÉ ABSOLUE