Sécurité des données

Janvier 2025

Evaluer les besoins en sécurité d’un registre de traitements dans le cadre du RGPD

Pour le service RH :

Critère	Niveau	Justification
Disponibilité	Fort	Accessible en permanence pour répondre à la réglementation lié au traitement des données
Intégrité	Fort	Les informations ne doivent pas être altérées car des modifications non autorisées peuvent compromettre leur traitement
Confidentialité	Très fort	Les informations doivent être fortement protégées surtout car elles peuvent être sensibles
Preuve	Fort	Des dispositifs techniques ou réglementaires doivent être mis en place pour prouver la conformité avec le RGDP

Étude de cas : Educ & Info

1. Processus métiers

- La direction
- Le service commercial
- Le service administratif
- Le service informatique
- Le service pédagogique.

2. Actifs

- Ordinateurs
- Serveurs (radius)
- Système d'exploitation (windows 7)
- Personnels (une dizaine)
- Logiciels
- Locaux
- Base de données
- Firewall, switch, routeurs
- Réseau
- ERP

3. Vulnérabilités

Ordinateurs :

- Système d'exploitation obsolète
- Absence de contrôle d'accès pour les machines des stagiaires

Serveurs :

- Absence de PSSI pour donner les accès aux bonnes personnes
- Possible intrusion si le pare-feu ou les configurations réseau sont mal gérés

Personnel :

- Manque de sensibilisation à la sécurité
- Appareils non sécurisés connectés aux réseaux internes.

Locaux :

- Sécurité physique insuffisante (accès facile, absence de contrôle d'accès).

Base de données:

- Permissions trop larges, absence de chiffrement, sauvegardes non testées.

Équipements réseau:

- Mots de passe par défaut, firmware non mis à jour, segmentation réseau inadéquate.

Réseaux:

- Wifi public non sécurisé, Absence de segmentation, Absence de contrôle des accès, Manque de surveillance

Firewall, switch, routeurs:

- Configurations par défaut, Absence de logs, Manque de segmentation, Exploitation des failles des équipements réseau

Lien entre vulnérabilité, menaces associés et risques pour chaque actifs

Ordinateurs

Risque	Vulnérabilité	Menaces associées	Risques	Type de vulnérabilité
R1	Système d'exploitation obsolète	Exploitation de failles connues (malware, ransomware)	Compromission des systèmes, perte ou vol de données sensibles	Technique
R2	Absence de contrôle d'accès sur les machines des stagiaires	Accès non autorisé par des stagiaires ou tiers malveillants	Compromission des systèmes internes, propagation de virus/malware via le réseau	Technique

Serveurs

Risque	Vulnérabilité	Menaces associées	Risques	Type de vulnérabilité
R2	Absence de PSSI pour les accès	Accès non autorisé ou malveillant par des tiers	Vol ou modification des données sensibles, perturbation des services critiques	Organisationnelle
R2	Mauvaise gestion des configurations réseau	Intrusion via des ports mal configurés ou services exposés	Intrusion dans les réseaux internes, vol de données ou sabotage	Technique

Personnel

Risque	Vulnérabilité	Menaces associées	Risques	Type de vulnérabilité
R9	Manque de sensibilisation à la sécurité	Phishing, erreurs humaines (clic sur liens malveillants)	Introduction de malware, divulgation accidentelle de données, perte d'accès aux systèmes.	Humaine
R4	Appareils non sécurisés connectés aux réseaux	Intrusion via appareils infectés ou compromis	Propagation de malware, compromission des réseaux internes	Technique

Locaux

Risque	Vulnérabilité	Menaces associées	Risques	Type de vulnérabilité
R4/R9	Sécurité physique insuffisante	Intrusion physique (vol de matériel, sabotage)	Vol d'équipements ou de données, interruption des activités, accès non autorisés aux serveurs	Physique

Base de données

Risque	Vulnérabilité	Menaces associées	Risques	Type de vulnérabilité
R2	Permissions trop larges	Vol par des utilisateurs ayant des accès non justifiés	Divulgation de données clients, perte de propriété intellectuelle (supports pédagogiques)	Technique
R2	Absence de chiffrement	Interception des données en cas d'intrusion numérique	Exposition des données sensibles (clients, stagiaires, prestataires)	Technique
R2	Sauvegardes non testées	Défaillance du système ou cyberattaque	Perte de données critiques, incapacité à restaurer les services rapidement	Technique

Équipements réseau

Risque	Vulnérabilité	Menaces associées	Risques	Type de vulnérabilité
R2	Mots de passe par défaut	Accès non autorisé aux équipements réseau	Contrôle des réseaux internes, écoute des communications réseau	Technique
R2	Firmware non mis à jour	Exploitation de failles connues dans les équipements	Compromission des équipements réseau, accès non autorisé aux sous-réseaux ou données	Technique
R2	Segmentation réseau inadéquate	Propagation rapide des attaques dans le réseau	Dommages aux systèmes critiques	Technique
R2	Wi-Fi public non sécurisé	Attaques "man-in-the-middle", écoute des communications	Vol de données clients, stagiaires	Technique

Matrice des Risques

CONSEQUENCE	VRAISEMBLANCE					
		Négligeable	Peu probable	Possible	Probable	Très probable
	Critique		R6	R3	R2	R1
	Majeure			R5, R7	R4	R8
	Modérée				R9	
	Mineure					
	Insignifiante					

Échelle de vraisemblance	
Négligeable	Jamais rencontré
Peu probable	Vu une fois
Possible	Survenance dans l'année
Probable	Survenance dans le mois
Très probable	Survenance dans la semaine

Échelle de conséquence	
Insignifiante	Aucune perturbation : Risque sous contrôle
Mineure	Perturbation n'entraînant pas de rupture de fonctionnement : Action possible mais non prioritaire
Modérée	Perturbation limitée : Risque à surveiller, action ciblée à réaliser
Majeure	Indisponibilité temporaire : Action de prévention et protection pour réduire le risque
Critique	Indisponibilité totale : Risque à traiter en priorité

Mesures de remédiation et solutions techniques à chaque risques

R1 : Risques liés à l'exploitation de vulnérabilités et propagation de malwares

- Exploitation de failles connues (attaques par malware ou ransomware).
- Introduction et propagation de malwares, compromission des réseaux internes.

Remédiation : (Mesure 14) Mettre en place un niveau de sécurité minimal sur les postes : Installation d'antivirus, désactivation des exécutions automatiques, et mise à jour régulière des systèmes.

Solution technique :

Installation d'antivirus : Déployer un logiciel antivirus réputé sur tous les postes, avec des mises à jour automatiques pour la base de signatures.

Désactivation des exécutions automatiques : Configurer les systèmes pour désactiver l'exécution automatique des périphériques externes (clé USB, disques durs).

R2 : Risques d'accès non autorisés et intrusions

- Accès non autorisé par des stagiaires, tiers malveillants ou collaborateurs internes.
- Intrusion dans les réseaux internes, vol de données ou sabotage.

Remédiation : (Mesure 26) Contrôler l’accès physique aux salles serveurs.

Solution technique :

- Installation de lecteurs de badges ou cartes à puce
- Gestion des droits d'accès

R3 : Risques liés à la perte ou vol de données sensibles

- Divulgation ou vol de données sensibles (clients, stagiaires, prestataires).
- Vol de données ou accès non autorisé via des réseaux Wi-Fi publics.

Remédiation : (Mesures 18, 31) Chiffrer les données sensibles transmises et stockées.

(Mesure 37) Définir une politique de sauvegarde.

Solution technique : Mettre en place un chiffrement des données sensibles, aussi bien lors de leur stockage que pendant leur transmission

R4 : Risques liés à la sécurité physique et à l'accès matériel

- Vol d'équipements ou données sensibles, accès non autorisés aux serveurs.

Remédiation : (Mesure 26) Contrôler l’accès physique aux salles serveurs.

Solution technique :

- Installation de lecteurs de badges RFID **(Radio Frequency Identification)** est une technologie qui permet l'identification automatique d'objets, de personnes ou d'animaux grâce à des ondes radio.
- Audit des accès

R5 : Risques liés aux sauvegardes et à la reprise d'activité

- Incapacité à restaurer les services critiques rapidement, dommages aux systèmes critiques (ERP, serveurs, sauvegardes).

Remédiation : (Mesure 37) Politique de sauvegarde.

Solution technique : Définir une politique de sauvegarde régulière et sécurisée, incluant des sauvegardes chiffrées et stockées hors site.

R6 : Risques liés à la surveillance et à la réponse aux incidents

- Attaques prolongées sans réaction, impossibilité de détecter ou d'enquêter sur les incidents de sécurité.

Remédiation : (Mesure 38) Procéder à des audits réguliers.

Solution technique :

- Implémentation d'un SIEM (Security Information and Event Management) collecte des journaux et des événements provenant de divers systèmes (serveurs, équipements réseau, systèmes de contrôle d'accès, systèmes de vidéosurveillance, etc.). Il analyse ces données pour identifier des comportements suspects ou des incidents de sécurité et génère des alertes ou des rapports d'audit
- Audit des événements d'accès

R7 : Risques liés aux équipements réseau

- Compromission des équipements réseau (pare-feu, routeurs, switch), accès non autorisé aux sous-réseaux ou données internes.

Remédiation : (Mesure 19) Mise en place de VLAN et pare-feu interne.

Solution technique : Mise en place de VLAN pour séparer les sous-réseaux et installation de pare-feu internes pour contrôler et limiter l'accès aux équipements réseau et aux données sensibles.

R8 : Risques liés à l'accès au réseau sans contrôle (Wi-Fi public)

- Accès non autorisé aux systèmes via le Wi-Fi public ou absence de contrôle d'accès sur les réseaux.

Remédiation : (Mesure 20) Sécuriser les réseaux Wi-Fi.

Solution technique :

- **Utilisation du chiffrement WPA 3** : Chiffrer les communications Wi-Fi pour garantir que les données échangées ne peuvent pas être interceptées par des personnes non autorisées
- **Segmentation des réseaux Wi-Fi (Réseau invité vs Réseau interne) :** Séparer le trafic des utilisateurs internes et des visiteurs pour limiter les risques d'accès non autorisé.

R9 : Risques liés aux erreurs humaines et à la gestion des accès

- Contournement des mécanismes de protection, erreurs humaines dans la gestion des accès.

Remédiation : (Mesure 2) Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique.

Solution technique : Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique, telles que la gestion des mots de passe et la prévention du phishing, pour éviter les erreurs humaines et le contournement des protections.

R10 : Risques d'impact global sur les opérations

- Compromission de plusieurs services critiques, perturbation complète du fonctionnement de la société.

Remédiation : Superviser et auditer

Solution technique :

- **Mise en place d'un Système de Gestion des Informations et des Événements de Sécurité (SIEM)** Collecter, analyser et surveiller les événements de sécurité afin de détecter des incidents en temps réel et d'améliorer la réponse aux menaces.
- **Systèmes de Détection et de Prévention d'Intrusion (IDS/IPS)** : Identifier et prévenir les intrusions ou attaques sur le réseau en temps réel.

TOP 10 de l'OWASP

1. Injection

Risque : Un attaquant injecte du code malveillant (SQL, commandes système, scripts) dans des champs de saisie ou des requêtes pour altérer le comportement de l'application.

Dangers :

- Accès non autorisé aux bases de données
- Modification ou suppression de données
- Prise de contrôle du serveur

Comment éviter :

- Utiliser des requêtes paramétrées
- Valider et échapper toutes les entrées utilisateur
- Limiter les privilèges des comptes d'accès aux bases de données

Exemple d'attaque :

SQL Injection (SQLi) : Un attaquant manipule une requête pour accéder à des données confidentielles dans une base via une entrée utilisateur.

2. Identification et Authentification de Mauvaise Qualité

Risque : Les mécanismes d’authentification et de gestion des sessions sont mal configurés ou peu sécurisés, facilitant le contournement des contrôles d’accès.

Dangers :

- Usurpation d’identité
- Accès non autorisé aux comptes utilisateurs ou administrateurs
- Compromission des données sensibles.

Comment éviter :

- Implémenter des mots de passe forts
- Activer l’authentification multifactorielle (MFA)
- Protéger les tokens de session et limiter les tentatives de connexion

Exemple d'attaque :

Credential Stuffing : Un attaquant teste des combinaisons nom d'utilisateur/mot de passe volées sur une autre application pour accéder au système.

3. Composants Vulnérables et Obsolètes

Risque : L'application utilise des bibliothèques, frameworks ou logiciels contenant des vulnérabilités connues ou non maintenues.

Dangers :

- Exploitation de failles connues pour accéder au système
- Exécution de code malveillant
- Perturbation de l'application

Comment éviter :

- Maintenir une veille de sécurité
- Appliquer régulièrement les mises à jour et correctifs
- Utiliser uniquement des composants maintenus par des développeurs fiables

Exemple d'attaque :

Equifax (2017) : Exploitation d'une faille dans le framework Apache Struts, utilisé dans l'application, entraînant le vol de millions de données d'utilisateurs.

4. Carence des Systèmes de Contrôle et Journalisation

Risque : Absence ou mauvaise gestion des logs et de la journalisation des activités utilisateurs.

Dangers :

- Impossibilité de surveiller les actions des utilisateurs
- Échec de la détection des accès non autorisés ou des comportements suspects

Vulnérabilités associées :

- Manque de mécanismes d'alerte
- Logs insuffisants ou incohérents pour permettre une enquête efficace

Comment éviter :

- Implémenter une journalisation systématique des événements critiques (connexions, modifications, erreurs)
- Surveiller et analyser les journaux régulièrement.

5. Défaillance Cryptographique

Risque : Utilisation d'algorithmes cryptographiques obsolètes (par exemple, MD5 ou SHA-1) pour chiffrer des données sensibles.

Dangers :

- Exposition des données sensibles
- Facilité de déchiffrement pour les attaquants

Vulnérabilités associées :

- Algorithmes obsolètes comme MD5
- Vulnérables aux collisions ou attaques par force brute

Comment éviter :

- Utiliser des algorithmes modernes comme SHA-256 ou bcrypt pour le stockage des mots de passe

6. Falsification de Requête Côté Serveur

Risque : Un attaquant manipule des requêtes envoyées par l'application pour accéder à des systèmes internes ou externes.

Dangers :

- Exfiltration de données
- Propagation d'attaques
- Accès aux ressources internes sensibles

Comment éviter :

- Valider et filtrer les entrées utilisateur
- Restreindre l'accès aux ressources internes
- Désactiver les redirections inutiles

Exemple d'attaque :

Capital One (2019) : Une SSRF a permis à un attaquant d'exfiltrer des données sensibles via un service interne.

7. Conception Non Sécurisée

Risque : L'application est vulnérable dès sa conception en raison de l'absence de principes de sécurité.

Dangers :

- Failles structurelles difficiles à corriger
- Vulnérabilités exploitables tout au long du cycle de vie

Comment éviter :

- Appliquer des principes de sécurité dès la conception
- Analyser les menaces et gérer les permissions
- Effectuer des tests réguliers

Exemple d'attaque :

Equifax (2017) : La conception non sécurisée a permis l'exploitation de failles connues dans le framework utilisé.

8. Contrôle d'Accès Défaillant

Risque : Une mauvaise implémentation des contrôles d'accès permet à des attaquants de contourner les restrictions.

Dangers :

- Accès non autorisé à des données sensibles
- Modification ou suppression de ressources
- Escalade de privilèges

Comment éviter :

- Implémenter un contrôle d'accès basé sur des rôles RBAC un mécanisme de contrôle d'accès qui définit les rôles et les autorisations de chaque utilisateur) ou attributs (ABAC: détermine l'accès en fonction de caractéristiques propres à l'utilisateur, de caractéristiques d'objet, de types d'action, etc.)
- Ne pas se fier aux contrôles côté client
- Effectuer des audits réguliers

Exemple d'attaque :

Une faille dans l'application Instagram (2019) permettait à un attaquant d'accéder aux informations personnelles des utilisateurs sans authentification.

9. Mauvaise Configuration de Sécurité

Risque : Une configuration inadéquate ou par défaut rend le0s systèmes vulnérables.

Dangers :

- Exposition de données sensibles
- Compromission des serveurs
- Élargissement de la surface d'attaque

Comment éviter :

- Utiliser des configurations sécurisées par défaut
- Effectuer des revues et audits réguliers
- Restreindre l'accès aux interfaces d'administration

Exemple d'attaque :

En 2020, une mauvaise configuration d'un serveur Elasticsearch a exposé des données d'utilisateurs sans authentification.

10. Absence d'Intégrité des Données et Logiciels

Risque : Absence de mécanismes pour vérifier l'intégrité des données ou logiciels, permettant à des attaquants de manipuler les fichiers.

Dangers :

- Introduction de malwares
- Manipulation de données sensibles
- Perte de confiance des utilisateurs

Comment éviter :

- Utiliser des signatures numériques et des hash
- Mettre en place des contrôles de version

Exemple d'attaque :

L'attaque SolarWinds (2020) a exploité une chaîne d'approvisionnement logicielle, compromettant une mise à jour.

Différents protocoles de chiffrement

Actif	Protocole	Avantages	Inconvénients
Wi-Fi	WPA3	Sécurité renforcée, anti-dictionnaire.	Pas compatible avec les anciens appareils.

Définition :

- **WPA 3** (Wi-Fi Protected Access 3) est la troisième version du protocole de sécurité Wi-Fi, conçu pour protéger les réseaux sans fil contre les cyberattaques.

Exemple WPA 3 :

- Une entreprise déploie WPA 3 sur son réseau Wi-Fi pour protéger les communications internes et empêcher les accès non autorisés.
  WPA3 sécurise votre Wi-Fi en chiffrant les connexions et en protégeant chaque appareil individuellement contre les attaques.

Actif	Protocole	Avantages	Inconvénients
Serveurs	TLS	Chiffrement standardisé et sûr.	Impact sur les performances CPU.
Base de données	TLS	Sécurise les connexions client-serveur.	Performance réduite sous forte charge.
Serveur RADIUS	TLS	Confidentialité et authenticité.	Gestion complexe des certificats.

Définition :

- **TLS** (Transport Layer Security) est un protocole cryptographique utilisé pour sécuriser les communications sur Internet

Exemple Serveurs:

- Lorsqu'un utilisateur envoie un e-mail via un serveur de messagerie utilisant TLS, le protocole chiffre le contenu du message pendant le transit entre le client de messagerie et le serveur de messagerie, garantissant la confidentialité de l'e-mail.

Exemple Base de données :

- Dans le cas d'une **base de données** utilisant **TLS** (Transport Layer Security), un exemple parfait serait la connexion sécurisée d'une application web à une base de données **MySQL**.

Exemple Serveurs Radius :

- Le serveur RADIUS est configuré pour utiliser **EAP-TLS** comme méthode d'authentification. Cela signifie qu'il va utiliser TLS pour sécuriser la communication entre le client (l'appareil de l'utilisateur) et le serveur d'authentification.

Actif	Protocole	Avantages	Inconvénients
Site web	HTTPS	Confidentialité, inspire confiance.	Certificats payants ou mal configurés.

Définition :
- **HTTPS** (HyperText Transfer Protocol Secure) est un protocole de communication sécurisé utilisé pour échanger des informations sur Internet

Exemple HTTPS :
- Un utilisateur visite le site web de sa banque en ligne via HTTPS, garantissant que ses informations de connexion restent privées et sécurisées.

Actif	Protocole	Avantages	Inconvénients
Ordinateurs	BitLocker/LUKS	Protection des données en cas de vol.	Impact possible sur les performances. Accessible uniquement sur les éditions professionnelles et entreprises (Pro, Enterprise, Ultimate).

Définition :
- **BitLocker** est un **outil de cryptage** intégré à certaines versions de **Windows**. Il permet de chiffrer l'intégralité d'un **disque dur**, rendant les données inaccessibles sans une clé de décryptage spécifique. Concrètement, cela signifie que si votre appareil est volé, les données qu'il contient seront protégées et illisibles pour toute personne non autorisée.

Exemple Bitlocker :

- Un utilisateur active BitLocker sur son disque dur externe pour protéger ses fichiers sensibles en cas de perte ou de vol.

Actif	Protocole	Avantages	Inconvénients
Ordinateurs commerciaux	VPN	Sécurise les connexions publiques	Dépend de la configuration et du protocole.

Définition :

- Un **VPN** (Réseau Privé Virtuel) est une technologie qui permet de créer une connexion sécurisée entre l'utilisateur et un réseau distant via Internet.

Exemple VPN :

- Un employé de **Société** travaille à distance depuis chez lui et doit accéder à des fichiers internes stockés sur le serveur de l'entreprise. Il se connecte à un VPN de l'entreprise, qui chiffre sa connexion et lui permet d'accéder à ces fichiers comme s'il était dans les bureaux de l'entreprise, tout en gardant la confidentialité des données.

Actif	Protocole	Avantages	Inconvénients
Switch/ Routeur	SNMPv3	Messages sécurisés et authentifiés. Support des Traps pour envoyer des alertes en temps réel en cas de panne ou de surcharge.	Compatibilité réduite avec l'ancien matériel. Complexité de configuration

Définition :

- **SNMPv3** est un protocole utilisé pour la gestion et la surveillance des équipements réseau, tels que les routeurs, commutateurs, serveurs

Exemple SNMPv3 :

- Un administrateur réseau souhaite savoir si l'un des **commutateurs** (switch) utilise trop de bande passante, ce qui pourrait ralentir le réseau.du coup il utilise le protocole.

Actif	Protocole	Avantages	Inconvénients
Messagerie	PGP/MIME	Chiffrement bout en bout.	Complexité pour les utilisateurs.

Définition :

- **PGP/MIME** est une norme qui permet de sécuriser les emails en chiffrant leur contenu et leurs pièces jointes.

Exemple PGP/MIME :

- Une entreprise envoie des contrats sensibles à un partenaire via email en utilisant PGP/MIME pour chiffrer les pièces jointes et protéger les données.

https://www.cnil.fr/sites/cnil/files/atoms/files/guide_referentiel_-_recrutement.pdf