Sécurité et gouvernance des données

PLAN

- Sécurité des données
- Gouvernance des données
- Enjeux
- Acteurs de la Sécurité et la Gouvernance des Données

SÉCURITÉ DES DONNÉES

- est un domaine clé de la gestion des systèmes d'information qui consiste à protéger les informations numériques contre:
  - les accès non autorisés,
  - la corruption,
  - le vol
  - la destruction
- **englobe l'ensemble des pratiques, technologies, et processus utilisés pour garantir la confidentialité, l'intégrité et la disponibilité des données**.

PRINCIPES FONDAMENTAUX DE LA SÉCURITÉ DES DONNÉES (CIA TRIAD)

- **Confidentialité** : Seuls les utilisateurs autorisés peuvent accéder aux données. Cela implique le chiffrement des données, la gestion des accès (via des systèmes d'identification et d'authentification), et la mise en place de politiques de confidentialité.
- **Intégrité :** Les données doivent être exactes et fiables, ce qui signifie qu'elles ne doivent pas être modifiées ou corrompues de manière non autorisée pendant le stockage ou le transfert.
- **Availability : *Disponibilité* :** Les données doivent être accessibles aux utilisateurs autorisés chaque fois que cela est nécessaire, et cela inclut la mise en place de systèmes de sauvegarde et de récupération après sinistre pour garantir un accès continu en cas de panne.

PRINCIPALES MENACES

- **Cyberattaques** : Les méthodes telles que le phishing, les attaques par ransomware, les logiciels malveillants et les attaques par déni de service sont couramment utilisées pour compromettre la sécurité des systèmes et voler ou altérer les données.
- **Accès non autorisé** : Cela inclut les intrusions dans les systèmes ou les accès non surveillés par des employés ou des parties externes. La mauvaise gestion des autorisations d'accès peut exposer les données sensibles.
- **Vulnérabilités des logiciels** : Les failles de sécurité dans les logiciels ou les systèmes d'exploitation peuvent être exploitées pour compromettre les données. Les vulnérabilités non corrigées (comme dans le cas d'Equifax en 2017) peuvent entraîner des violations massives.

TECHNIQUES ET TECHNOLOGIES DE PROTECTION DES DONNÉES

- **Chiffrement** : Le chiffrement est essentiel pour protéger les données sensibles, à la fois lorsqu'elles sont stockées et lorsqu'elles sont transmises sur des réseaux. Les algorithmes de chiffrement comme AES (Advanced Encryption Standard) et RSA (Rivest-Shamir-Adleman) sont couramment utilisés pour protéger les informations sensibles.
- **Gestion des accès** : Des outils de gestion des identités et des accès (IAM) permettent de définir et d'appliquer qui peut accéder à quelles données et à quel moment, réduisant ainsi les risques d'accès non autorisé.
- **Pare-feux et systèmes de détection des intrusions (IDS)** : Ils surveillent le trafic réseau et les comportements suspects pour bloquer ou alerter sur les tentatives d'accès ou les activités malveillantes.
- **Sauvegarde et récupération** : Des systèmes de sauvegarde réguliers sont nécessaires pour garantir que les données peuvent être restaurées en cas de perte due à une panne système ou à une cyberattaque. Les plans de reprise après sinistre (PRA) et les plans de continuité des activités (PCA) sont essentiels pour garantir la disponibilité des données.

POLITIQUES ET PROCÉDURES

- **Politiques de sécurité des données :** Les entreprises doivent élaborer et maintenir des politiques claires concernant la manière dont les données doivent être stockées, traitées, et partagées, ainsi que sur les droits d'accès et la gestion des incidents de sécurité.
- **Sensibilisation et formation :** Les employés doivent être formés pour reconnaître les menaces telles que le phishing et appliquer les bonnes pratiques de sécurité, comme l'utilisation de mots de passe forts et le respect des procédures de sécurité.
- **Audits de sécurité :** Des audits réguliers sont nécessaires pour vérifier la conformité aux politiques de sécurité, évaluer les vulnérabilités, et prendre les mesures correctives appropriées.

RÉGLEMENTATIONS ET CONFORMITÉ

- De nombreuses régulations internationales imposent des obligations en matière de sécurité des données :
- **RGPD (Règlement Général sur la Protection des Données)** : Ce règlement impose des exigences strictes sur la manière dont les données des citoyens de l'UE sont collectées, stockées et traitées, y compris en matière de sécurité et de gestion des violations de données.
- **CCPA (California Consumer Privacy Act)** : Réglementation californienne qui protège les informations personnelles des consommateurs, avec des obligations sur la transparence, le contrôle et la sécurité des données.
- **HIPAA (Health Insurance Portability and Accountability Act)** : Réglementation américaine concernant la protection des informations de santé, imposant des exigences spécifiques sur la sécurité des données médicales.

EXEMPLES DE VIOLATIONS DE DONNÉES

- Certaines des violations les plus marquantes incluent :
- **Equifax (2017)** : Une vulnérabilité non corrigée a permis le vol de données personnelles de 147 millions de personnes, causant un énorme impact financier et une perte de confiance du public.
- **Facebook/Cambridge Analytica (2018)** : L'utilisation abusive des données de millions d'utilisateurs à des fins politiques a soulevé des questions éthiques sur la gouvernance des données et la sécurité.

BONNES PRATIQUES POUR SÉCURISER LES DONNÉES

- **Mettre à jour régulièrement les logiciels et systèmes** : Assurer que toutes les vulnérabilités connues sont corrigées.
- **Utiliser le chiffrement des données sensibles** : Chiffrer les données critiques, en particulier lors de leur transfert sur des réseaux publics.
- **Mettre en place des audits réguliers** : Auditer les systèmes et processus pour garantir que toutes les mesures de sécurité sont efficaces et conformes aux réglementations.
- **Former les employés** : Éduquer les employés sur les bonnes pratiques de sécurité, la reconnaissance des menaces, et leur rôle dans la protection des données.

PLAN

- Sécurité des données
- Gouvernance des données
- Enjeux
- Acteurs de la Sécurité et la Gouvernance des Données

GOUVERNANCE DES DONNÉES

- est une discipline stratégique qui assure la gestion, la qualité, la disponibilité, la sécurité et l'utilisation correcte des données dans une organisation.
- permet aux entreprises de maximiser la valeur des données tout en minimisant les risques associés, tels que les violations de données ou les non-conformités réglementaires.
- se réfère à l'ensemble des processus, rôles, normes et politiques utilisés pour gérer les données d'une organisation de manière cohérente et fiable.
- assure que les données sont gérées comme un actif précieux, permettant une prise de décision éclairée, conforme et sécurisée.

PRINCIPAUX OBJECTIFS DE LA GOUVERNANCE DES DONNÉES

- **Qualité des données :** S'assurer que les données sont exactes, complètes, cohérentes et à jour pour répondre aux besoins de l'organisation.
- **Sécurité des données :** Garantir que les données sont protégées contre les accès non autorisés et les cyberattaques, conformément aux normes internes et réglementaires.
- **Accessibilité et disponibilité :** Les données doivent être accessibles aux bonnes personnes, au bon moment, tout en respectant les politiques d'accès sécurisées.
- **Conformité réglementaire :** Assurer que l'entreprise respecte les lois et réglementations concernant la collecte, le traitement, le stockage et la suppression des données (ex. : RGPD, CCPA, HIPAA).
- **Intégrité des données :** Assurer que les données ne sont pas corrompues ou altérées de manière non autorisée, garantissant ainsi leur fiabilité.

PROCESSUS DE GOUVERNANCE DES DONNÉES

- **Collecte des données**
  - Définir comment les données doivent être collectées, les sources et selon quels critères de qualité.
  - S'assurer que les données sont collectées de manière éthique et conforme à la loi.
- **Traitement et stockage des données**
  - Créer des politiques qui définissent où et comment les données doivent être stockées (DB locales, cloud, etc.).
  - S'assurer que les données sont stockées de manière sécurisée, avec des systèmes de sauvegarde adéquats.
- **Accès et partage des données**
  - Établir des contrôles d'accès rigoureux pour s'assurer que seules les personnes autorisées y ont accès.
  - Développer des politiques claires sur le partage des données, tant en interne qu'avec des tiers, afin de protéger la confidentialité et la sécurité.
- **Utilisation des données**
  - Assurer que les données sont utilisées conformément aux finalités pour lesquelles elles ont été collectées.
  - Mettre en place des procédures pour l'audit des activités liées aux données et identifier les mauvaises utilisations.
- **Archivage et suppression**
  - Gérer les données obsolètes ou non pertinentes en les archivant ou en les supprimant conformément aux politiques de conservation et aux lois sur la protection des données (ex. : droit à l'oubli dans le RGPD).

PLAN

- Sécurité des données
- Gouvernance des données
- Enjeux
- Acteurs de la Sécurité et la Gouvernance des Données

ENJEUX ACTUELS DE LA GOUVERNANCE ET DE LA SÉCURITÉ DES DONNÉES

- **Le Big Data**
- **Les Cybermenaces et Cyberattaques**
- **Conformité à des Réglementations Strictes**
- **Multiplication des Sources de Données**
- **Menaces internes**

BIG DATA : LES 6V

Big Data

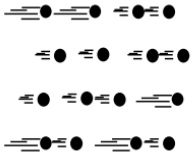
Open Data

Volume

Data at Rest

Terabytes to exabytes of existing data to process

Velocity



Data in Motion

Streaming data, milliseconds to seconds to respond

Variety

Data in Many Forms

Structured, unstructured, text, multimedia

Veracity

Data in Doubt

Uncertainty due to data inconsistency & incompleteness, ambiguities, latency, deception, model approximations

Visibility

Data in the Open

Open data is generally open to anyone. Which raises issues of privacy. Security and provenance

Value

Data of Many Values

Large range of data values from free (data philanthropy to high value monetization)

CYBERMENACES ET CYBERATTAQUES

- sont des actions malveillantes visant à compromettre la confidentialité, l'intégrité ou la disponibilité des systèmes informatiques, des réseaux et des données.
- **Types de Cybermenaces et Cyberattaques**
  - Ransomware (Logiciels de rançon)
  - Phishing et Spear Phishing
  - Attaques par Déni de Service
  - Malware (Logiciels malveillants)
- **Impacts**
  - -- Pertes financières
  - -- Sanctions Légales et Amendes
  - -- Dommages à la Réputation
  - -- Interruption des Opérations

CYBERATTAQUE

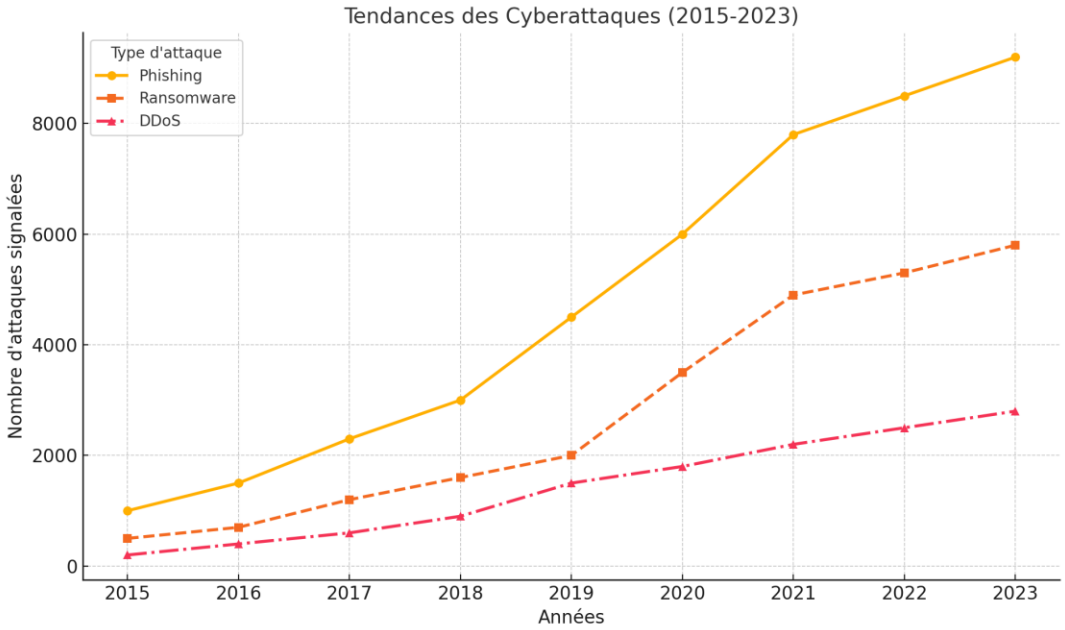
- Selon le FBI, les USA ont perdu plus de 10,2 milliards de dollars à cause de la cybercriminalité en 2022, soit une augmentation de près de 35 % par rapport à l'année précédente.

En France de 2022 à 2023

- 53% des entreprises ont subi une attaque, 48% en 2022
- Coût moyen de de 15 640€ vs 14 720€ en 2023
- une entreprise sur huit rapporte plus les 230 000€
- Piratage de messagerie professionnelle est le vecteur d'attaque le plus fréquent

- **Facteurs de vulnérabilité les plus courants**
  Absence de formation régulière
- Mise à jour et maintenance déficientes:
- Manque de plans de réponse aux incidents

cybermenaces et cyberattaques dans le monde



PLAN

- Sécurité des données
- Gouvernance des données
- Enjeux
- Acteurs de la Sécurité et la Gouvernance des Données

ACTEURS CLÉS DANS LA SÉCURITÉ ET LA GOUVERNANCE DES DONNÉES

- **Délégué à la Protection des Données (DPO - Data Protection Officer)**
- **Responsable de la Sécurité des Systèmes d'Information (RSSI - Chief Information Security Officer, CISO)**
- **Propriétaire des Données (Data Owner)**
- **Administrateur des Données (Data Custodian)**
- **Utilisateur des Données (Data User)**

DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPO - DATA PROTECTION OFFICER)

- est responsable de la supervision de la stratégie de protection des données dans l'organisation et du respect des obligations légales.
- **Principales responsabilités du DPO :**
- **Conformité**: Il s'assure que l'organisation respecte les lois sur la protection des données, telles que le RGPD, et autres réglementations pertinentes. Il surveille l'application des pratiques de protection des données dans tous les processus de l'entreprise.
- **Audit et surveillance** : Il effectue des audits réguliers pour vérifier la conformité de l'entreprise avec les réglementations en vigueur. Le DPO doit identifier les risques potentiels liés aux données personnelles et recommander des actions pour les atténuer.
- **Formation et sensibilisation** : Le DPO est chargé de former les employés aux bonnes pratiques de gestion des données personnelles et d'assurer qu'ils comprennent les exigences légales liées à la protection des données.
- **Point de contact avec les autorités de régulation** : Le DPO agit comme l'interlocuteur principal entre l'entreprise et les autorités de protection des données (comme la CNIL en France). En cas de violation de données, le DPO coordonne la notification aux autorités compétentes dans les délais prescrits.

DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPO - DATA PROTECTION OFFICER)

- **Compétences requises :**
- Connaissance approfondie des réglementations en matière de protection des données (RGPD, CCPA, etc.).
- Expertise en matière de gestion des risques liés aux données personnelles.
- Capacité à communiquer efficacement avec les équipes internes et les autorités externes.
- **Exemple de responsabilité :**
- Lors d’une violation de données, le DPO est responsable d’évaluer l’incident, d’informer les autorités dans les 72 heures (comme stipulé par le RGPD), et de s'assurer que les mesures correctives appropriées sont prises.

RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (RSSI - CHIEF INFORMATION SECURITY OFFICER, CISO)

- est chargé de la gestion et de la protection des infrastructures informatiques et des données d'une organisation. Responsable de la sécurité technique des systèmes d'information, assurant que les données sont protégées contre les cyberattaques, les fuites et les accès non autorisés.
- **Principales responsabilités du RSSI :**
- **Définition de la stratégie de cybersécurité** : Le RSSI établit une stratégie de sécurité des systèmes d'information qui inclut la mise en œuvre des politiques, des procédures et des technologies pour protéger l'organisation contre les cybermenaces.
- **Gestion des incidents de sécurité** : En cas de cyberattaque ou de violation de données, le RSSI est responsable de coordonner la réponse à l'incident. Il supervise la gestion des crises, la résolution des problèmes, et la restauration des systèmes après un incident.
- **Surveillance et évaluation des risques** : Le RSSI doit identifier les vulnérabilités dans les systèmes informatiques de l'entreprise et mettre en place des mesures de prévention pour réduire les risques, comme l'application des mises à jour de sécurité, la gestion des accès, et la surveillance des systèmes.
- **Mise en œuvre des technologies de sécurité** : Le RSSI supervise l'implémentation des solutions de sécurité telles que les pare-feux, les systèmes de détection d'intrusion (IDS), les outils de gestion des accès (IAM), et les systèmes de chiffrement.

RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (RSSI - CHIEF INFORMATION SECURITY OFFICER, CISO)

- **Compétences requises :**
- Expertise en sécurité des systèmes d’information, cybersécurité, et gestion des risques.
- Connaissances techniques approfondies des réseaux, des systèmes, et des applications de sécurité.
- Leadership pour gérer des équipes de sécurité informatique et communiquer avec la direction sur les enjeux de sécurité.
- **Exemple de responsabilité :**
- Le RSSI met en place un plan de réponse aux incidents pour faire face à une attaque par ransomware. Ce plan comprend des sauvegardes régulières, des solutions de chiffrement, et une stratégie de récupération après sinistre pour garantir que les données peuvent être restaurées sans payer la rançon.

PROPRIÉTAIRE DES DONNÉES (DATA OWNER)

- Le **Data Owner** est le responsable métier ou fonctionnel d'une certaine catégorie de données dans l'organisation. Il ne gère pas techniquement les données, mais il est responsable de la qualité, de la sécurité et de l'utilisation des données à travers leur cycle de vie. Le Data Owner prend des décisions sur la manière dont les données sont utilisées et partagées dans l'organisation.
- **Principales responsabilités du Data Owner :**
- **Gestion des droits d'accès** : Le Data Owner définit qui peut accéder aux données et quel niveau d'accès leur est accordé, en collaboration avec l'équipe de sécurité (CISO ou DPO).
- **Assurance de la qualité des données** : Il est responsable de la qualité et de l'intégrité des données. Cela inclut la correction des erreurs, l'harmonisation des données, et la gestion des doublons.
- **Conformité et gouvernance** : Le Data Owner s'assure que les données qu'il gère sont traitées conformément aux politiques de gouvernance des données et aux réglementations applicables.

PROPRIÉTAIRE DES DONNÉES (DATA OWNER)

- **Compétences requises :**
- Compréhension approfondie des processus métiers associés aux données qu'il gère.
- Capacité à collaborer avec les équipes techniques pour assurer que les exigences de sécurité et de gouvernance sont respectées.
- Sens des responsabilités en ce qui concerne la protection des données critiques de l'entreprise.
- **Exemple de responsabilité :**
- Un Data Owner dans une banque est responsable de l'ensemble des données clients. Il veille à ce que les informations soient exactes et mises à jour, et à ce que seules les personnes autorisées (comme les gestionnaires de comptes) puissent y accéder.

ADMINISTRATEUR DES DONNÉES (DATA CUSTODIAN)

- Le **Data Custodian** est souvent un membre de l'équipe technique qui assure la gestion technique des données. Ce rôle est axé sur l'infrastructure informatique et le stockage des données, garantissant que les systèmes de gestion des données fonctionnent correctement et sont sécurisés.
- **Principales responsabilités du Data Custodian :**
- **Stockage et sécurité des données** : Il veille à ce que les données soient stockées de manière sécurisée et que les systèmes de sauvegarde et de récupération après sinistre soient en place.
- **Mise en œuvre des politiques de sécurité** : Le Data Custodian s'assure que les politiques de sécurité définies par le RSSI et les propriétaires de données sont appliquées au niveau technique (ex : chiffrement, gestion des accès, audit).
- **Surveillance des systèmes de données** : Il surveille les systèmes de données pour s'assurer qu'ils fonctionnent correctement, qu'il n'y a pas de pannes et que les performances sont optimisées.

ADMINISTRATEUR DES DONNÉES (DATA CUSTODIAN)

- **Compétences requises :**
- Expertise technique en gestion des bases de données, en sécurité informatique et en administration des systèmes.
- Capacité à travailler en étroite collaboration avec le CISO pour assurer la sécurité des données.
- Compétences en gestion des infrastructures cloud, des solutions de stockage et de la continuité des activités.
- **Exemple de responsabilité :**
- Le Data Custodian est responsable de la configuration des bases de données et de leur sécurité, en veillant à ce que les sauvegardes automatiques soient effectuées régulièrement et que l'accès à la base de données soit limité aux utilisateurs autorisés.

UTILISATEUR DES DONNÉES (DATA USER)

- L'**Utilisateur des Données** est une personne au sein de l'organisation qui accède, utilise ou manipule les données pour réaliser ses tâches professionnelles. Bien que ce ne soit pas un rôle de gouvernance, l'utilisateur des données est essentiel à la sécurité globale des données.
- **Responsabilités de l'Utilisateur des Données :**
- **Respect des politiques de sécurité** : L'utilisateur doit respecter les règles et les bonnes pratiques définies par les autres acteurs (DPO, RSSI), comme la protection des informations sensibles ou l'utilisation correcte des systèmes.
- **Signalement des incidents** : Si l'utilisateur constate des anomalies, des accès non autorisés ou des erreurs dans les données, il est tenu de les signaler immédiatement.
- **Exemple de responsabilité :**
- Un employé dans un service client doit utiliser les données des clients en respectant les politiques internes de protection des données, en s'assurant que les informations ne sont pas partagées de manière non sécurisée.

ÉTUDES DE CAS

CAS DE ÉQUIFAX EN 2017

- En 2017, **Equifax**, l'une des plus grandes agences de crédit des États-Unis, a subi une violation de données majeure qui a exposé les informations personnelles sensibles de **147 millions de personnes**. Les données compromises comprenaient des **noms**, **numéros de sécurité sociale (SSN)**, **dates de naissance**, **adresses**, **numéros de permis de conduire**, et dans certains cas, des **numéros de cartes de crédit**.
- La violation a été causée par l'exploitation d'une vulnérabilité non corrigée dans une application web utilisant le framework **Apache Struts**, bien que la faille ait été signalée plusieurs mois avant l'attaque. Les attaquants ont pu accéder aux serveurs d'Equifax et exfiltrer les données sur plusieurs mois, sans être détectés. L'entreprise a découvert l'attaque en juillet 2017, mais celle-ci a commencé en mai 2017. Equifax a officiellement révélé la violation en septembre 2017.
- Cette violation a affecté principalement des citoyens américains, ainsi que certains résidents du Royaume-Uni et du Canada.

ACTIVITÉ EN GROUPE

- Identifier les menaces potentielles dans un cabinet de dentiste déterminer qui devrait être responsable de la gouvernance des données.