Fadi ALOUANI

Fadi
Alouani
BTS SIO1
groupe 1
02/01/25

B3-TD Cybersécurité question PIA

Sommaire

Introduction :

Dans ce TP, nous avons étudié la protection des données à caractère personnel et les règles imposées par le RGPD. L'objectif était de comprendre ce qu'est une donnée personnelle, comment les entreprises les utilisent, ainsi que les risques liés à leur traitement. Nous avons également appris à distinguer la sécurité de la sûreté informatique et à analyser différents scénarios pour identifier les menaces possibles.

Étape 1
Analyser un PIA

1. fait

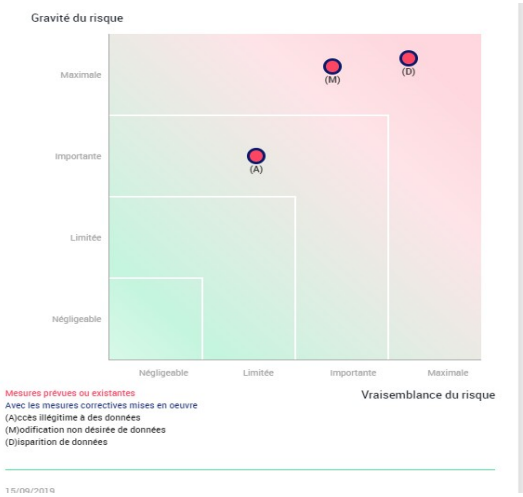
2.

1. **Accès illégitime à des données**
   gravité: Importante
   vraisemblance : limitée

2. Modification non désirées des donnés
   gravité: Maximal
   vraisemblance : importante

3. disparition de données
   gravité: Maximal
   vraisemblance : Maximal

3.



Selon la cartographie la modification de données et la disparition de données sont les cas les plus grave.Il sont également classer comme vraisemblance maximale.

4. Mesure existante ou prévues

Accès illégitime : Contrôle d'accès logique

Modification non désirée de données : Gestion des poste de travail

Disparition de données : Chiffrement

5.La cartographie montre une maturité croissante dans la gestion des risques liés aux données personnelles, mais les menaces critiques demeurent (modification et disparition de données).
Des mesures correctives supplémentaires (sauvegardes renforcées, tests de restauration, surveillance accrue des accès) sont encore nécessaires pour abaisser ces risques vers les zones de gravité et de vraisemblance plus faibles.

Étape 2 :

Cartographier le traitement des données à caractère personnel

1. La cartographie des traitements consiste à dresser une liste claire et détaillée de toutes les données personnelles que l'entreprise collecte, utilise, stocke ou partage.
Elle permet de savoir quelles données sont traitées, pourquoi, où, par qui et pendant combien de temps.

Quels sont ses enjeux ?

- **Respecter le RGPD** : c'est une obligation légale pour prouver que l'entreprise protège bien les données.
- **Identifier les risques** : repérer ce qui pourrait mettre les données en danger.
- **Améliorer l'organisation** : mieux comprendre les flux d'informations dans l'entreprise.
- **Renforcer la sécurité** : mettre en place les bonnes protections.
- **Gagner la confiance** : montrer aux clients et partenaires que leurs données sont bien traitées.

2 . Le registre des traitements est une étape préalable à la cartographie parce qu'il permet d'abord de recenser et décrire tous les traitements de données personnelles de manière générale :quelles données sont utilisées, pour quelle raison, qui y accède, combien de temps elles sont conservées, etc.
Une fois ce registre fait, on peut réaliser la cartographie, qui va plus loin : elle visualise et analyse en détail les flux de données (d'où elles viennent, où elles vont, comment elles circulent).

En résumé :

- Le registre = la liste de base des traitements.
- La cartographie = la représentation précise et complète de ces traitements et de leurs flux.

Donc, sans registre, il manque les informations nécessaires pour construire une cartographie fiable.

Étape 3 :

Repérer l'utilisation des données à caractère personnel

1.Quand une personne saisit ses données personnelles sur un formulaire Castorama.fr :

- Ses données peuvent être partagées avec d'autres entreprises du même groupe (Kingfisher : B&Q, Screwfix, etc.).
- Ses données peuvent être utilisées pour améliorer les services, les sites web, et proposer des offres adaptées.
- Ses données peuvent servir à la contacter, par exemple par email, pour lui envoyer des informations ou des offres.
- Certaines données peuvent être transmises à des partenaires techniques qui aident Castorama (ex : sociétés logistiques).

2. L'extrait montre que Castorama explique comment les données sont utilisées et avec qui elles sont partagées, mais :

- Les données ne restent pas uniquement chez Castorama, elles sont communiquées à plusieurs autres sociétés du groupe et à des partenaires.
- L'extrait ne dit pas clairement quelles mesures de sécurité sont mises en place pour garantir la confidentialité.

On ne peut pas affirmer avec certitude que la confidentialité est totalement assurée, car l'extrait ne décrit pas précisément les protections de sécurité.

Étape 4 :

Traitements et risques sur les données à caractère personnel

1) Moyens de collecte, stockage et diffusion des données à caractère personnel :

- Collecte : formulaires d'inscription, comptes clients, commande en ligne, cookies (traceurs)
- Stockage : les données sont stockées sur les serveurs du groupe Castorama (Kingfisher) et peuvent être partagées entre entités du groupe.
- Diffusion : les données peuvent être partagées avec d'autres sociétés du groupe Kingfisher.

2) **Quels sont les traitements des données personnelles :**

- Gestion des commandes (nom, adresse, paiement…)
- Gestion des comptes clients et de la fidélité.
- Utilisation des cookies / traceurs pour le marketing, l'analyse du site.
- Prévention de la fraude.
- Envoi d'offres commerciales (emails, SMS) selon le consentement.

3) **Obligations légales rappelées :**

- Castorama doit respecter le RGPD : informer les utilisateurs, obtenir des consentements quand nécessaire, garantir les droits des personnes (accès, suppression, rectification).
- Castorama doit mettre en place des mesures techniques et organisationnelles pour protéger les données.
- Castorama doit informer les utilisateurs de la durée de conservation des données.

4) **Sanctions en cas de non-respect :**

Si une entreprise comme Castorama ne respecte pas ses obligations en matière de protection des données :

- Elle peut être sanctionnée par la CNIL (amendes, injonctions).
- Elle peut subir des répercussions légales (plaintes de clients, actions en justice).
- Sa réputation peut être affectée : perte de confiance des clients, impact commercial.

Fadi ALOUANI

Étape 5 :

Dissocier les notions de sécurité et de sûreté informatique

Scénarios	Sécurité	Sûreté	Justifications
L'ensemble des serveurs est hors-service à cause d'une inondation du local technique	☐	☒	C'est un événement naturel/accidentel
Les données d'un hôpital sont illisibles à la suite d'une attaque de type *ransomware*.	☒	☐	C'est une attaque volontaire par un logiciel malveillan
L'apparence du site vitrine d'une entreprise est modifiée pendant un week-end par des personnes malveillantes.	☒	☐	Piratage volontaire
Une surcharge électrique temporaire due à des travaux réalisés dans les bâtiments de la société provoque une panne des routeurs.	☐	☒	Accident technique involontaire

Étape 6 :

Identifier les données à caractère personnel

Données	Caractère personnel	Justifications
Le nom de l'enseigne du magasin Carrefour	☐ oui ☒ non	Ce n'est pas une personne, c'est une entreprise.
L'adresse courriel professionnelle d'un directeur des services informatiques	☒ oui ☐ non	Identifie une personne dans son travail.
Une photo postée sur un réseau social	☒ oui ☐ non	Permet d'identifier une personne grâce à son image.
Une vidéo de présentation de son parcours professionnel envoyée à une entreprise dans le cadre d'un recrutement	☒ oui ☐ non	Contient l'image, la voix, le parcours = identification directe.
Les coordonnées GPS de localisation d'un smartphone	☒ oui ☐ non	Permet d'identifier indirectement un utilisateur en suivant ses déplacements
Le groupe sanguin d'un patient stocké sur le serveur de base de données de son médecin	☒ oui ☐ non	C'est une donnée de santé, donc personnelle et sensible.
Les enregistrements de vidéosurveillance d'un *datacenter*	☒ oui ☐ non	Images des personnes → identification possible.
Le numéro d'enregistrement au registre du commerce et des sociétés d'une entreprise	☐ oui ☒ non	identifie une entreprise, pas une personne physique.
Le numéro de sécurité sociale d'un salarié saisi sur sa fiche d'embauche	☒ oui ☐ non	Identifie formellement une personne → donnée personnelle sensible.

Conclusion :

Ce travail m’a permis de mieux comprendre l’importance de protéger les données personnelles et les responsabilités des entreprises en matière de confidentialité et de sécurité. J’ai aussi appris à reconnaître les différents types de données personnelles et à distinguer les risques liés aux attaques humaines ou aux incidents techniques. Ces connaissances sont essentielles pour garantir un traitement sécurisé et conforme des données dans un contexte professionnel.