SYNTHESE DROIT DU NUMERIQUE

SAE IN3SA01A

2022-2023

Quentin ROCHER, Khaoula HAJBI, Angelo LARIVIERE, Erwan BARBIER

Table des matières

Introduction

De nos jours énormément d'informations et de données circulent sur Internet. Ces données sont une mine d'or pour les pirates ou tout simplement les entreprises partenaires à qui vos données sont revendues. Pour sécuriser et éviter tout type de problèmes comme la perte de données, le vol, la revente, des règles existent, ce sont les RGPD (règlement général sur la protection des données).
Dans le cadre de nos études, nous avons à réaliser un projet qui consiste à développer une application web hébergée sur un serveur Raspberry PI4. Nous nous interrogeons alors sur l'importance et le niveau de sécurité que nous avons à mettre en place pour ce projet. D'après les 19 fiches du guide des RGPD réalisé par la CNIL, comment pouvons-nous protéger les données de nos utilisateurs et l'avons-nous bien fait ?
Nous allons dans un premier temps voir l'importance de ces règles, comment les appliquer et pourquoi. Ensuite, nous verrons ce que nous avons mis en œuvre dans notre projet, ce que nous avons réalisé jusqu'à présent et ce que nous pourrions améliorer.

Importance des RGPD

En quoi consiste les RGPD et pourquoi elles existent

Comme dit en introduction, les données nous entourent, énormément de démarches et de stockages sont réalisés numériquement et des mesures pour garantir la sécurité de ces informations sont nécessaires. L'apparition des RGPD a eu lieu en mai 2018, s'applique dans toute l'Union Européenne et n'a cessé de s'améliorer depuis. Pour faire simple, il s'agit d'un règlement qui s'applique à tout organisme qui traite des données personnelles. Ces données sont le nom, le prénom, l'adresse, date de naissance, adresse IP, numéro de téléphone, sexe, empreinte digitale, iris, et vocale, groupe sanguin, l'orientation sexuelle, … Toute information se rapportant à un individu physique identifiable est considérée comme une donnée personnelle.

Comment les appliquer dans un projet

Lorsque nous réalisons un projet, il y a la phase de réflexion sur la finalité de ce projet, vient alors le moment de se pencher sur le type des données que nous allons récolter, stocker et leur utilité. Il faut également penser au système, au lieu et à la durée de stockage de ces informations, sécuriser les serveurs, limiter les accès, penser aux méthodes de chiffrement des données et enfin la maintenance.
D'après la fiche 1 de la CNIL, nous pouvons appliquer l'anonymisation des données qui a pour objectif de ne plus rendre identifiable un individu à des données brutes. Mais une fois cela fait, il ne sera plus possible d'identifier de nouveau la personne aux données. Une des méthodes pour conserver des données sans les associer directement à un individu est la pseudonymisation. Elle consiste à demander un pseudo à l'utilisateur afin d'associer un âge, un mot de passe ou n'importe quelle information personnelle à une personne sans que l'on sache qui est cette personne. Il y a également le cryptage des informations pour qu'elles ne soient pas consultables directement.
Dans la fiche 2, la CNIL se penche sur la méthodologie, la sécurité, le choix des langages de programmation et de l'environnement de travail.
Une des parties les plus importante abordée dans ces fiches, est la sécurisation du code source, mettre en place des communications sécurisées sans faire passer les informations dans la barre URL, sécuriser les authentifications et les infrastructures.
La fiche 14 aborde la durée de conservation des données, nos données sont considérées comme actives, c'est-à-dire qu'elles sont utilisées et utilisables contrairement aux données archivées qui servent juste à de la récupération en cas de besoin. Les fichiers de log doivent être supprimés sous 1 an maximum, les données médicales doivent être conservées 20 ans.
La fiche 18 concerne surtout les phases de test, s'assurer que l'on ne peut pas atteindre des fichiers cachés directement via la barre URL, l'injection de code directement dans les champs de saisie pour s'assurer que l'on ne peut pas exécuter des commandes, se protéger des logiciels malveillants et rançongiciel et vérifier les attaques par force brute et par dictionnaire.

Les RGPD au sein de notre projet

Ce que nous avons fait ?

Dans notre cas, dès le début de notre projet, nous savions qu'il faudrait protéger les données de nos utilisateurs. Pour ce faire nous avons déjà commencé à réfléchir sur le type de données que nous allions récolter. Les seules données que nous récoltons de nos utilisateurs sont le nom, le prénom, un pseudo et leur mot de passe. Nous n'avons pas l'utilité de récupérer l'âge, l'adresse ou encore le numéro de téléphone de nos utilisateurs. Pour sécuriser leur compte, le mot de passe est chiffré, stocké dans la base de données et est seulement traité par notre code afin de garder le mot de passe chiffré, de cette manière nous ne récupérons jamais leur mot de passe. Pour se connecter, nous faisons le rapprochement entre le mot de passe et le pseudo, si les deux correspondent, l'utilisateur peut alors se connecter. Nous n'utilisons plus le nom et prénom de l'utilisateur. Pour chaque utilisateur, nous avons un historique des simulations qu'il a exécutées, il s'agit d'une variable qui compte le nombre d'exécutions. Nous avons également un fichier de log qui recense toutes les tentatives de connexion échouées avec l'heure, la date et le login tenté. Selon la conservation des données, ce fichier doit être supprimé tous les 6 mois et 1 an maximum.
Pour le serveur, nous avons totalement la main dessus, nous savons où il est et nous ne passons pas par un tiers, ce qui limite également les risques car lorsqu'une entreprise fait de la

sous-traitance, ils n'ont pas la main sur la sécurité des données.
Pour ce qui est du langage utilisé, nous avons choisi le SQL pour la base de données et le PHP pour faire la liaison entre les pages web et la base de données. L'une des erreurs les plus fréquente avec l'utilisation de ce langage est de ne pas faire attention à l'injection SQL, ce que nous avons empêché dès le début de notre développement.
Lors de notre évaluation des risques, ce qui posait le plus problème était le serveur Raspberry. Celui-ci devait être suffisamment sécurisé pour que personne ne puisse s'y connecter. Pour ce faire, nous avons limité les tentatives de connexion à 3, après ces tentatives, le serveur ne peut plus être accessible.

Qu'aurions-nous pu améliorer ou changer ?

Pour ce qui est de la récolte des données, nous aurions pu nous contenter de récupérer seulement un pseudo et un mot de passe, sans le nom et prénom de la personne. Pour une meilleure fiabilité dans la connexion, nous aurions pu mettre en place une double authentification mais cela impliquerait de récupérer une adresse mail ou un numéro de téléphone, ce que nous ne voulons pas.
Ce qui pourrait être utile de réaliser serait de faire une autre sauvegarde du serveur sur un autre serveur, un backup, toutes les 24h le serveur pourrait se copier sur un autre serveur pour éviter de perdre des données. Dans le cadre de la SAE cela n'est pas possible et nous n'avons pas de données très importantes mais sur de plus lourds projets, avoir des backups est recommandé.
On pourrait mettre en place des critères spécifiques pour le mot de passe comme 12 caractères minimum, l'utilisation d'une majuscule, minuscule d'un chiffre, … Afin d'améliorer le niveau de sécurité.
Le fait de ne pas avoir l'adresse mail de l'utilisateur ou aucun moyen de communiquer, nous ne pouvons pas les informer en cas de vol ou fuite de données.
En ce qui concerne le fichier de log, nous n'avons pas mis en place de suppression tous les ans.

Conclusion

Les RGPD sont essentiels pour garantir la sécurité et la protection des données personnelles. Il est important de prendre en compte ces règles lorsque nous développons un projet qui nécessite la collecte de données personnelles. Nous avons déjà mis en œuvre certaines mesures pour protéger les données de nos utilisateurs, mais il y a toujours de la place pour l'amélioration comme la double authentification. On peut donc dire que nous avons une assez bonne sécurité, nous n'avons pas de gros conflits avec les RGPD, étant donné qu'il s'agit d'un petit projet limité dans le temps, nous n'avons pas la possibilité de mettre en place énormément de pratique de RGPD, seulement ce qui est nécessaire. Il est donc important de continuer à s'informer sur les RGPD et de mettre en place les meilleures pratiques pour garantir la sécurité de nos utilisateurs. Respecter ces règles est important du côté légal comme du côté de la confiance, une entreprise qui respecte les données de ses utilisateurs, qui les sécurisent du mieux possible aura une meilleure image et moins de problèmes.

Sources :

Guide RGPD du développeur

RGPD de quoi parle-t-on ?

RGPD quand pourquoi