UVSQ université PARIS-SACLAY
IUT de Vélizy-Rambouillet
CAMPUS DE VÉLIZY-VILLACOUBLAY
CAMPUS DE RAMBOUILLET

Informatique 2ème année

DEGAT Teddy
CHOISY Alexis
GRONDIN David
MOUSSAMIH Elias
LEAUTHAUD Matthieu

SAé IN3SA01- Développement d'une application

Mise en oeuvre de la ressource R3.11 Droit et contrats et du numérique
Application du thème 3 : Protection des données personnelles

Nous avons pour projet de mettre en place une application web en PHP et en MySQL qui aura pour but de recueillir les demandes de dépannage des différents utilisateurs dans les salles machines. De ce fait, nous avons un rôle majeur dans la sécurité de ce système, nous ne pouvons pas y rester indifférent.

"Constitue un fichier de données à caractère personnel tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique."
"Un fichier est un traitement de données qui s'organise dans un ensemble stable et structuré de données. Les données d'un fichier sont accessibles selon des critères déterminés."
Extrait de l'article 2 de la loi informatique et libertés.

Par ces définitions, on peut en déduire que nos données traitées sont des données à caractère personnel, s'agissant du login d'utilisateurs, ainsi que leur mot de passe. Ces données servant à se connecter sur la session d'un utilisateur sont des données très sensibles, ayant un impact fort sur les utilisateurs comme sur le système si elles sont compromises. D'autres données

peuvent être liées aux utilisateurs, nous avons par exemple les demandes de dépannages qui sont liées à l'auteur de la demande ainsi qu'au technicien qui traite cette dernière. Pour des buts de statistiques et de moyennes, ces données sont conservées un an.

"Les données à caractère personnel doivent être :

Traitées de manière licite, loyale et, pour les traitements relevant du titre II, transparente au regard de la personne concernée ;
Collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des dispositions du règlement (UE) 2016/679 du 27 avril 2016 et de la présente loi, applicables à de tels traitements et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ;
Adéquates, pertinentes et, au regard des finalités pour lesquelles elles sont traitées, limitées à ce qui est nécessaire ou, pour les traitements relevant des titres III et IV, non excessives ;
Exactes et, si nécessaire, tenues à jour. Toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder ;
Conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Toutefois, les données à caractère personnel peuvent être conservées au-delà de cette durée dans la mesure où elles sont traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques. Le choix des données conservées à des fins archivistiques dans l'intérêt public est opéré dans les conditions prévues à l'article L. 212-3 du code du patrimoine ;
Traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, ou l'accès par des personnes non autorisées, à l'aide de mesures techniques ou organisationnelles appropriées."

Extrait de l’article 4 de la loi informatique et libertés.

Ainsi, selon l’article 4, nous pouvons utiliser ces données à des fins statistiques. Toutes les données personnelles récoltées seront stockées dans une base de données.

Pour un but de sécurité, nous avons limité l’accès à la base de données en fonction des rôles de chaque utilisateur, nous avons comme utilisateurs: le visiteur; l’utilisateur; le technicien; l’administrateur web; l’administrateur système.

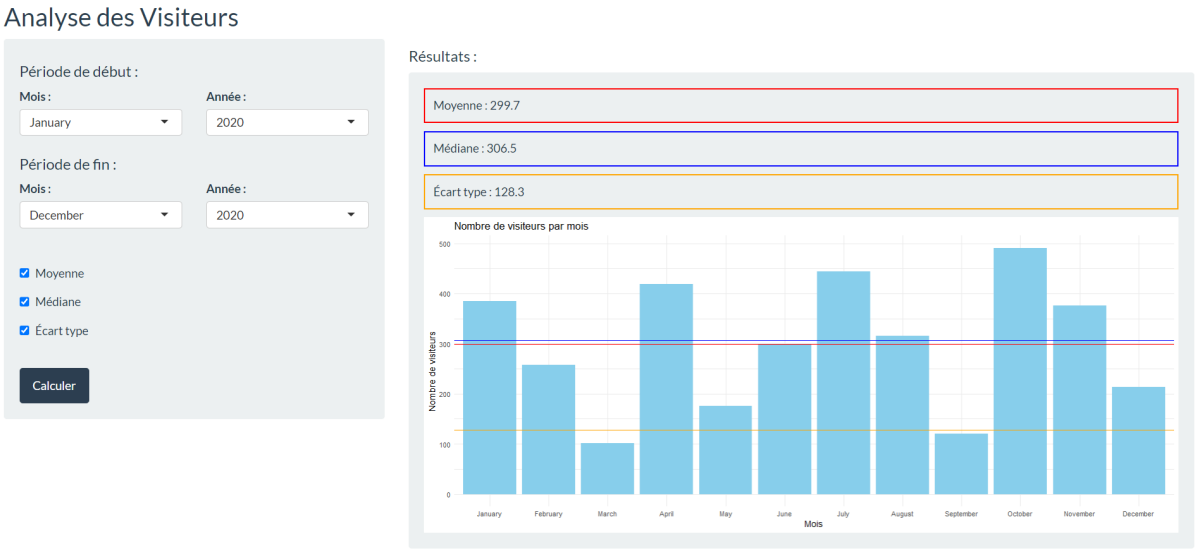
Les rôles ont été fait de sorte à ce que la base de données soit la plus sécurisée possible, pour cela, nous avons tout d’abord le visiteur. Ce rôle est attribué par défaut à tout utilisateur entrant dans le site, il s’agit de toute personne n’étant pas connectée, il ne peut seulement accéder à la page d’accueil du site web, qui explique le but de la plateforme. Nous avons ensuite l’utilisateur, connecté, il peut quant à lui ouvrir une demande, accéder à la liste de ses demandes et de voir leur état (fermé, ouvert, en cours) et enfin accéder à son profil pour le personnaliser, comme changer sa photo de profil, ajouter une description ou bien changer son mot de passe. Le rôle du technicien est de pouvoir s’attribuer lui-même des demandes, y répondre et fermer ces dernières. Le rôle de l’administrateur web est unique, il peut gérer les demandes de la même façon que le technicien, mais peut aussi attribuer des demandes aux techniciens. Il peut notamment éditer les libellés, les titres des demandes des utilisateurs. Enfin, nous avons l’administrateur système qui a accès au traitement des données des utilisateurs, de leurs demandes plus spécifiquement, afin de s’en servir uniquement à des fins statistiques.

Avec le guide de la sécurité des données personnelles, nous avons pu faire un diagnostic complet sur notre système. Le matériel utilisé est un serveur, sur le Raspberry PI, ainsi que des ordinateurs, des téléphones, pour tous les utilisateurs du site web. Le Raspberry PI est sur le système d’exploitation Raspberry PI OS, dont les services sont accessibles par un navigateur web. Les canaux de communication du système utilisent un protocole SSH ainsi que SFTP donc, déjà crypté. L’unique support papier existant correspond aux informations données au client, c’est-à-dire le mot de passe ainsi que le login de l’administrateur du client. Le Raspberry PI est entretenu dans les locaux de l’IUT de Vélizy. Nous avons alors un risque d’accès illégitime aux données, leur modification non désirée, ainsi que leur disparition. Tandis que les menaces sont le vol, la dégradation, l’observation ou social engineering, ainsi que l’utilisation inadaptée du système.

Ci-contre se trouve un tableau représentant chacun des risques, ainsi qu'une échelle allant de faible, à modérée, à importante, puis à maximale, jaugeant l'influence des risques sur le système.

RISQUES	IMPACT SUR LES PERSONNES	PRINCIPALES SOURCES DE RISQUE	PRINCIPALES MENACES	MESURES EXISTANTES OU PRÉVUES	GRAVITÉ POUR LES PERSONNES	VRAISEMBLANCE
ACCÈS ILLÉGITIME À DES DONNÉES	Importante	Négligeable	Maximale	Modérée	Importante	Modérée
MODIFICATION NON DÉSIRÉE DES DONNÉES	Maximale	Négligeable	Maximale	Négligeable	Maximale	Négligeable
DISPARITION DES DONNÉES	Maximale	Négligeable	Maximale	Négligeable	Maximale	Négligeable

Les données utilisées sont purement à des fins statistiques accessibles seulement par l'administrateur système sur une durée d'un an.



Représentation de l'utilisation des données

Ci-dessus se trouve l'utilisation de nos données par le nombre de visiteurs en fonction d'une période, où le mois et l'année peuvent être sélectionnées. De ces données, on en tire la moyenne, l'écart type, la médiane, ainsi qu'un graphe.

Afin de réaliser le projet sans soucis internes, nous avons rédigé une charte informatique trouvable en pièce jointe à laquelle nous avons tous été d'accord selon la recommandation de la CNIL, s'y trouve également un engagement de confidentialité, avec une clause de confidentialité.

Sachant que l'erreur la plus fréquente est humaine, nous allons mettre en place, pour l'authentification des utilisateurs avec leur login et leur mot de passe, une façon sécurisée de les conserver à l'aide d'un cryptage RC4 pour que les mots de passe ne soient pas donnés directement dans notre base de données. De plus, nous utiliserons une entropie minimale de 80 bits, c'est-à-dire un mot de passe contenant au moins 12 caractères dont une majuscule, une minuscule, un chiffre et un caractère spécial.

Un système de journalisation (log) a été mis en place afin de protéger le système lors de maintenance si une faille venait de l'extérieur, le journal sera conservé pendant une année. Sont enregistrés dans ce journal les opérations de création de consultation de modification ainsi que de suppression. Ce journal n'est seulement accessible par l'utilisateur root, l'utilisateur ayant tous les droits possible sur le système. De ce fait, nous avons mis en place un système de gestion des archives où le journal, ainsi que les versions antérieures du système sont disponibles.

Les différents services et logiciels jugés inutiles sont supprimés et désinstallés du système, afin d'éviter qu'une brèche de ces derniers puisse endommager le système, ou le rendre vulnérable à une attaque.

Les ports de communication ont été limités, l'utilisateur root ne peut pas se connecter via le canal de communication SSH, il a été désactivé.

Les rôles attribués au système sont conçus de sorte à donner les permissions sensibles aux seules personnes habilitées pour éviter les failles en interne, et avoir le contrôle plus facilement sur le système.

Une sauvegarde régulière des données est faite sur un autre système à la hauteur d'une fois par semaine, en cas d'attaque ou d'accident détruisant le système, ou supprimant ses données. Le système contenant les sauvegardes est extérieur à l'IUT de Vélizy, en plus d'être une sauvegarde hors-ligne. Toutes ces données sont traitées au même niveau de sécurité, et chaque sauvegarde est protégée comme les autres.

La sécurité de nos données a été réfléchie dès les premières étapes du projet, en y comprenant les exigences de sécurité de données.

Des tests unitaires sont constamment réalisés afin de tester la sécurité du système, et d'y remédier au plus vite si nécessaire.