Constat de l'audit de robustesse 2021

Exigences fonctionnelles

Sécurité des données à caractères personnelles

Constat

Le développeur est une petit organisation qui assure également l'exploitation. Le référent Sécurité est le développeur (également gérant de la société). Il y a eu jusqu'à trois développeurs sur le projet. Même si cette désignation n'est pas explicite, le gérant est le référent de facto donc il semble que cela soit acceptable. Point d'attention sur la continuité d'activité, le gérant étant proche d'une passation de compétences nécessaire.
Le serveur qui stocke les données appartient à la société du logiciel évalué. Montage en VM avec ProxMox et l'applicatif serveur tourne dans ProxMox.
Le support documentaire du logiciel est disponible via un wiki.
Le registre de traitement des données personnelles est établi, et le référent Sécurité est également DP. Il est connaisseur de la règlementation et a identifie la notion de criticité des données stockées, y compris celles qui ne seraient que courantes, étant donné la nature de certaines associations utilisatrices du logiciel (religion).
Ainsi, la plupart des données courantes de ce logiciel est de facto considérée comme sensible et non juste courante.
Les seules données chiffrées (hashées+salées) sont les mots de passe. Les données personnelles traitées par le logiciel ne sont pas chiffrées/anonymisées.

Actions préconisées

Actions réalisées

Procédures de sécurité pour minimiser les risques

Constat

L'organisme évalué a géré le risque sécurité sur la partie Exploitation du logiciel, ainsi que sur la gestion des credentials des utilisateurs, via un PIA. Les traitements sont étayés via des fonctions de sécurité et leur nature technique.
Le traitement des données des utilisateurs : les bases de données sont chiffrées AT REST (protection contre le scénario de vol de disque dans le centre d'hébergement mais pas de dump de BDD en live via l'interface exposée du logiciel).
Pas d'interconnexions in/out avec d'autres produits.

Actions préconisées

Préciser dans la documentation de traitement que la nature de certains de ses clients induit que les données personnelles soient courantes deviennent sensibles.

Actions réalisées

Ajout sur la page d'entrée du site de la phrase *“Logeas informatique une grande attention au données qui lui sont confiées, d'autant que plusieurs de ces clients lui confie des données considéré au sens du RGPD comme sensible. C'est pourquoi le logiciel est phase de certification NF 552 “Données personnelles”*

Authentification

Fonctionnement proposé par le logiciel

Constat

Les accès utilisateur sont protégés par mot de passe. Pas de captcha ni de nombre limité de tentatives. *Les comptes utilisateur et modérateur ne sont pas protégés par double facteur.*
Le service général (monespace.logeas.fr) est mutualisé pour tous les clients. Les interfaces du logiciel de chaque client sont ensuite dédiées à chaque client.
Les bases de chaque client sont montées sur des sous-serveurs Web.
Il y a plusieurs services par client, chacun sur un port différent de la boucle locale derrière l'interface accessible en HTTP(S).
Les mots de passe sont limités à 8 caractères minimum, renouvelés tous les 2 ans.

Actions préconisées

Mettre en place un nombre de tentatives limitées sur les comptes utilisateur et modérateur + règles de construction des mots de passe avec minuscule, majuscule, nombres, et quelques caractères spéciaux et 10 caractères mini.

Actions réalisées

A partir de la version 10.0 la politique de mot de passe est revu :

- 10 caractères minimum
- 1 majuscule, 1 minuscule, 1 chiffre
- 1 caractère spécial dans #&$;:-
- valable 2 ans
- au bout de 5 tentatives de connexion incrusteuse l'utilisateur reçoit sur son mail une demande de renouvellement de son mot de passe. Dans l'attente de son action le compte est bloqué.

Fonctionnement proposé par le logiciel

Constat

La fonction de hachage est en PKBF2 avec salage des mots de passe dans la base mais il a été vu que le sel est fixe, donc deux mots de passe identiques de deux utilisateurs différents seront similaires.
La fonction de hachage est en SHA256, via une bibliothéque propriétaire éditée par SynOps, en DELPHI (SynCrypto).

Actions préconisées

Paramétrer un sel spécifique à chaque compte utilisateur (minimum), il ne doit pas être prédictible et accessible par les utilisateurs. Idéalement : une chaine aléatoire par compte utilisateur. Utiliser une méthode de génération aléatoire telle que celles dans les bibliothèques cryptographiques.
La gateway d'authentification met en œuvre un paramétrage de déconnexion après une durée d'utilisation (Peut-être 1h? à confirmer par l'organisme, à confirmer par l'organisme, voir à implémenter dans le code si besoin pour disposer de cette fonctionnalité de limitation du temps des sessions)

Actions réalisées

A partir de la version 10.0 :

- une base de données complémentaire est mise en place afin de stocké les mots de passe des base de donnée, ainsi que le salage des mots de passe utilisateur. A phase d'exploitation cette base de donnée sera stocké sur un serveur différent du serveur d'exploitation. Ce serveur n'étant pas accessible directement depuis Internet (pour plus d'information on se reportera Partie cryptologie de LoGeAs (chaine aléatoire, cryptage, signature...))
- les chaines aléatoire sont déformée générée à partir de la fonction d'OpenSSL (Voir ici
- une fonction de timeout est implémenté dans le client lourd et l'interface “MonEspace”, en plus d'une fonction interne au serveur, réglé à 30mn

Stockage des mots de passe

Constat

Stockage des clés de chiffrement des bases : actuellement une clé est utilisée de manière unique pour toutes les bases.

Actions préconisées

Spécifier une clé unique (à partir d'un générateur aléatoire) à chaque client pour le chiffrement des bases. Séparer la clé du code source, avec a minima un fichier différent à

chaque client, pour le stockage de sa clé, droits d'accès restreints en lecture seule à ce fichier et seulement pour le compte ayant besoin d'accéder à cette clé pour déchiffrer la base. Voir (sur proposition de l'organisme) créer un serveur dédié pour les clés avec accès seulement interne par les autres serveurs.

Actions réalisées

A partir de la version 10.0 :

- une base de données complémentaire est mise en place afin de stocké les mots de passe des base de donnée, ainsi que le salage des mots de passe utilisateur. A phase d'exploitation cette base de donnée sera stocké sur un serveur différent du serveur d'exploitation. Ce serveur n'étant pas accessible directement depuis Internet (pour plus d'information on se reportera Partie cryptologie de LoGeAs (chaine aléatoire, cryptage, signature...))
- les chaines aléatoire sont déformée générée à partir de la fonction d'OpenSSL (Voir ici

Dimensionnement des clefs

Constat

Le choix des algorithmes constatés (SHA256) est en ligne avec le RGS de l'ANSSI.
En revanche le mécanisme de génération des clés (pour le moment une seule clé stockée en dur dans le code source pour déchiffrer tous les bases) doit être amélioré.
La fonction de chiffrement est AES-OFB avec une clé de 128 bits, ce qui est acceptable vis à vis des recommandations de l'ANSSI.

Actions préconisées

Actions réalisées

Suite au changement de bibliothèque de chiffrement les choix technologique ont évolué voir Partie cryptologie de LoGeAs (chaine aléatoire, cryptage, signature...)

Contrôle d'accès

Fonctions de gestion de droit

Constat

Le logiciel permet de gérer une hiérarchies de structures auxquelles sont associées des groupes dans lesquels on assigne des utilisateurs.
Le droit d'import de données permet d'ajouter des listes de membres (données de la base de chaque

organisme/association qui est client du logiciel.
Les droits possibles sont la consultation (authentifiée) des journaux, l'import de lignées pour la base des membres, la gestion des champs personnalisés
Le compte “par défaut” de chaque base est initialisé manuellement par l'organisme, (le login est donc unique par base puisqu'il correspond au mail paramétré par l'organisme et communiqué à l'établissement du contrat par le client).
La création de compte se fait via un lien envoyé à l'adresse mail du compte en cours de création, avec une clé d'activation acceptable. En revanche la durée de vie minimale du lien d'activation n'est pas spécifiée.
Il n'y a par conséquent pas de mots de passe par défaut. Il n'y a pas non plus de compte par défaut dans la mesure où l'assistance de l'organisme paramètre des comptes spécifiques nominatifs via la même procédure que celle permettant aux utilisateurs de créer leurs comptes.
Bon niveau de maturité organisationnel : l'organisme possède une charte informatique qu'elle a fait signer à ses membres, et qui spécifie les règles de gestion des mots de passe.
La gestion de suppression des comptes et données personnelles se fait via une intervention manuelle de l'assistance (contrairement aux bases de membres où dans ce cas les administrateurs peuvent facilement supprimer les données nécessaires)

Actions préconisées

Ajouter un timeout de durée de vie des liens d'activation, et dans le cas d'une sauvegarde de mot de passe précédent, une durée de vie minimale de mot de passe (par exemple 1 journée)

Actions réalisées

A METTRE EN PLACE

Journalisation des tentatives d'accès

Constat

Le logiciel possède une fonctionnalité de journalisation de l'activité, qui est protégée en intégrité et authenticité via un chainage des signatures de chaque ligne du journal.
Mécanisme de signature des journaux : la fonction passe par une signature RSA sans padding acceptable (PKCS#1 2.1 OAEP ou PSS)
L'accès aux journaux est seulement permis en lecture et via un droit paramétrable par un administrateur. Pas d'accès en lecture possible sur les journaux depuis les interfaces utilisateur/administrateur

Actions préconisées

Mettre à jour la fonction de signature soit en ajoutant un padding acceptable à RSA, soit en utilisant un autre mécanisme permettant d'assurer authenticité/intégrité (ECDSA / empreinte à clé HMAC-SHA256, ...). NB : attention si HMAC SHA256, le même secret est utilisé pour signer et vérifier

l'authenticité donc attention à ne pas compromettre le secret dans ce cas-là (aucun problème si biclé RSA/ECDSA puisque seule la partie publique est publiée).
Action de l'organisme : Journalisation des tentatives de connexion (via l'interface de connexion classique ou via le lien envoyé par mail → à mettre dans la piste d'audit)

Actions réalisées

Les fonction de cryptage ont été entièrement revu voir Partie cryptologie de LoGeAs (chaine aléatoire, cryptage, signature...) Les accès à l'interface qui n'aboutisse pas ne peuvent être pisté au niveau de piste d'audit de Logeas Web, car on se connecte en deux étapes : d'abord auprés de mom espace puis par la suite la liste des bases accésible et renvoyé et l'accés est choisi par l'utilisateur. On ne peut donc savoir à l'avance la base cible. **Faut-il envisagé de de le pister dans la piste d'audit de MonEspace ?**

Conservation numérique

Conservation des données à caractères personnelles

Constat

Les sauvegardes sont signées d'une façon similaire à la fonction utilisée par les journaux. Il y a au moins un champ (Intitulé) qui contient de la donnée perso dans les logs et qui n'est pas signé → La NF203 fait réduire les champs signés dans les logs, à arbitrer par INFOCERT
Il semble que le mécanisme de signature constaté, à base de RSA, implémente également un padding PKCS#1 1.5 via la bibliothèque TPBL3 qui n'apparait pas maintenue (dernières versions datant du début des années 2010).
Les sauvegardes sont effectuées automatiquement tous les jours, via un zip de toutes les bases (chiffrées) qui est transféré via FTPS sur un autre serveur de LOGEAS, localisé dans un autre datacenter.

Actions préconisées

Action de l'organisme : même chose que pour la signature des journaux, passer à une signature acceptable vis à vis du RGS de l'ANSSI.

Actions réalisées

Traitement via une connexion sécurisées

Constat

La configuration TLS du serveur NGINX assurant la négociation des sessions TLS doit être améliorée

(actuellement toutes les versions de TLS sont permises depuis SSLv3, bien qu'une politique “HIGH” soit configurée et que le hash MD5 soit bloqué, il reste d'autres suites de chiffrement et versions de protocoles de TLS qui ne sont pas satisfaisantes)

Actions préconisées

Action de l'organisme : améliorer la configuration de TLS côté serveur en spécifiant TLS1.3, voir également 1.2 mais en supprimant toutes les suites de chiffrement dépréciées (avec MD5/SHA-1/DH pour certains groupes).

Actions réalisées

Sera mis en place lors de la mise en ligne de la version 10.0

Intégrité

Sécurisation des données

Constat

Les bases de données (fichiers SQLite) sont chiffrées unitairement par le système de gestion des bases SQLite. A noter que bien que ce mécanisme ne prémunisse que des extractions de données AT REST (suite au vol du disque sur lequel reposent ces données), cette fonctionnalité répond quand même à cette exigence.
NB : le scénario contre lequel l'organisme ne pourrait pas se prémunir entièrement est celui d'une extraction en “live” des données de la bases via une injection de requêtes SQL au travers d'une interface non protégée. Point jugé non rédhibitoire bien qu'il pourrait être amélioré.
Le chiffrement constaté est en revanche conforme au RGS de l'ANSSI (cf. constats plus haut). par ailleurs le chiffrement de la base permet de couvrir le spectre de toutes les données qui y sont stockées.

Actions préconisées

Actions réalisées

Contrôle de l'intégrité des données personnel

Constat

Globalement conforme en dehors des données des journaux qui sont sujettes à d'autres référentiels (cf. NF203).

Actions préconisées

Actions réalisées

détection des violations d'intégrités

Constat

Il a pu être constaté que plusieurs évènements pertinents et constitutifs potentiellement de violation de données sont journalisés correctement. Le mécanisme permettant de vérifier l'intégrité a été vérifié et jugé conforme durant l'audit.
Bien que la procédure de gestion des incidents ne soit pas formalisée, une clause de gestion d'incidents sur les données personnelles est incluse dans les contrats avec les clients (non vérifié durant l'audit), et le référent sécurité étant également DPO, le circuit entre le constat d'un incident et la notification à la CNIL se fait par une seule et même personne, ce qui semble acceptable.

Actions préconisées

Actions réalisées

Sauvegarde et Restauration

Sauvegarde des données personnelles

Constat

Fonctionnalité de sauvegarde présente et fonctionnelle. Plan de sauvegarde existant et cohérent. Sécurisation des sauvegardes OK (en dehors du point sur le padding de la signature, déjà remonté ci-dessus)

Actions préconisées

Actions réalisées

restauration des données personnelles

Constat

Le test de restauration a été effectué dans cet audit et le résultat est satisfaisant.
Par ailleurs, le test de restauration fait partie des cas du plan de test qui est déroulé à chaque

déploiement de version majeure (une fois par an minimum)

Actions préconisées

Actions réalisées

Privacy by Design

Limitation des saisies au minimum

Constat

Les formulaires de saisie sont en partie limitatifs (dans la mesure où certaines données sont obligatoires, d'autres ne peuvent être sélectionnés qu'à partir de listes bien qu'il soit possible de saisir autre chose qu'un item de la liste en question, etc.)
La présence de tels mécanismes est suffisant d'un point de vue robustesse dans la mesure où les données restent protégées vis à vis de la criticité maximale de données possible.

Actions préconisées

Actions réalisées

Gestion des données statiques

Constat

D'un point de vue de robustesse le paramétrage proposé est jugé acceptable (probablement améliorable néanmoins).
Etant donné que la plupart des champs sont paramétrables, cette fonctionnalité est couverte par la fonction d'extraction des différents champs de données.
Amélioration possible (mais pas jugée indispensable) : extraction ciblée des mémos parmi les données saisies.

Actions préconisées

Actions réalisées

Privacy by Default

Limitation de la durée de conservation

Constat

Le logiciel dispose à la fois d'un mécanisme d'archivage des données des membres (saisies par les associations), ainsi que d'une fonction d'archivage au niveau des clients du logiciel (pour les comptes des administrateurs de chaque organisation). Ceci est satisfaisant au titre du premier de l'exigence en case F26.
Le logiciel dispose d'une fonctionnalité de droit à l'oubli mise à la disposition des utilisateurs pour gérer les données de leurs membres. Un bug empêchant la suppression de la date de naissance a été constaté, mais en dehors de cela le mécanisme de suppression semble acceptable.
Droit à l'oubli au niveau des comptes administrateur : suppression manuelle des données en base par le support LOGEAS. Les journaux ne peuvent en revanche pas être altérés étant donné le mécanisme de protection nécessaire au titre de la NF203. Au niveau des sauvegardes, pas de suppression des les sauvegardes antérieures.
La suppression est paramétrable au niveau des comptes membres gérés par les administrateurs de chaque organisme (y compris la durée de consentement, paramétrée par défaut à 3 ans). Celle-ci est réalisée automatiquement au déclenchement de la fonctionnalité de droit à l'oubli dans le logiciel par un administrateur en sélectionnant la personne concernée.
A noter que les suppressions de données sur les membres sont journalisées correctement par le logiciel, comme constaté durant cet audit.

Actions préconisées

Action de l'organisme : corriger le bug de suppression de la date de naissance des personnes supprimées.

Actions réalisées

Gestion des accès

Constat

Il a été constaté que la visualisation des ressources et des comptes utilisateurs au format de matrice est possible, et que celle-ci permet d'établir quelle ressource est accessible depuis quel utilisateur, et quelles ressources sont accessibles à un utilisateur, ce qui est satisfaisant.
La procédure de contrôle des ressources n'est pas formalisée, en revanche il est constaté que ce contrôle peut être fait efficacement en cas de besoin et que l'équipe de développement est restreinte, ce qui semble suffisant pour la maitrise de cette fonctionnalité en cas de besoin.

Actions préconisées

Actions réalisées