Sécurité de l'information

Pharius
Conformité attestée.

Cybercriminalité et sécurité

La cybercriminalité étant malheureusement un fait, la sécurité de l'information revêt désormais une importance cruciale. Nous voudrions dès lors nous attarder sur quelques aspects clés des multiples mesures de précaution prises chez RDMG Uitgevers pour l'application Pharius.

Les mesures mises en œuvre, chez nous comme chez nos fournisseurs, reposent sur les piliers suivants : centre de données, environnement d'hébergement, back-up, architecture et gestion, OWASP (Open Web Application Security Project), sécurité des mots de passe, analyse des vulnérabilités, sécurité SSL, conception sûre et accès administrateur. Ces mesures et leurs interconnexions assurent un niveau élevé de protection des données de nos clients et des utilisateurs.

Centre de données

Les données sont hébergées et stockées dans un centre de données moderne de BIT à Ede, aux Pays-Bas.

Le centre est non seulement certifié ISO, mais aussi NEN 7510. Ce certificat s'applique au développement, à la fourniture et au support de services (cloud), de services de connectivité et de services managés IT. Les meilleures pratiques de la norme ISO 27002 sont également respectées.

Le centre de données fait partie d'un réseau de trois centres éloignés les uns des autres. Par conséquent, il est possible de transférer les données vers l'un des autres centres si cela s'avère nécessaire. Ces centres sont en outre reliés les uns aux autres par des connexions redondantes en fibre optique.

Le fournisseur garantit 99,9 % de temps exploitable (uptime). Les serveurs web font l'objet d'une surveillance ininterrompue afin de détecter les pannes et d'analyser l'échange de données, la capacité de disque, la charge et l'utilisation (non conforme). Toute anomalie est immédiatement signalée et entraîne des actions spécifiques.

Le contrôle d'accès au centre de données est organisé à l'aide d'un système de pass et les fichiers logs sont enregistrés sur un serveur extérieur.

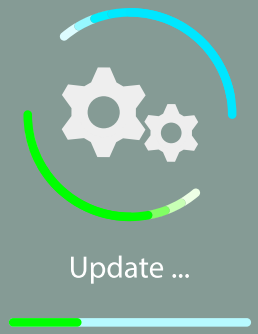
Le centre de données présente un dispositif de sécurité de

classe 3 contre l'intrusion et est doté d'un système anti-effraction sophistiqué, qui envoie instantanément une alarme à la centrale. La clôture (électrifiée) qui entoure le bâtiment et l'installation de vidéosurveillance renforcent également la sécurité.

En ce qui concerne la protection contre l'incendie, tous les centres de données sont équipés d'un système de détection par aspiration dans le faux plancher. Ce système permet de détecter un incendie à un stade extrêmement précoce. Des capteurs de fumeur optiques (montés au-dessus et en dessous du faux plancher) activent un système d'extinction par gaz si un incendie est effectivement détecté. Les pompiers utilisent le centre de données lors de leurs exercices et connaissent donc parfaitement le bâtiment, ainsi que les équipements présents.

Environnement d'hébergement

Le stockage des données est séparé de l'application grâce à l'utilisation de plusieurs serveurs. Il est impossible d'accéder au stockage de données de l'extérieur, l'accès peut uniquement se faire via le réseau interne. Les mises à jour de sécurité sont systématiquement installées sur nos serveurs, qui font l'objet d'une maintenance et d'une surveillance actives.



Back-up

AToutes les données sont protégées quotidiennement grâce à des solutions logicielles assurant des sauvegardes automatiques. Le back-up est effectué sur un autre serveur, dans un lieu distinct et sécurisé, et n'est pas accessible de l'extérieur.

Architecture et gestion

Pharius repose sur une structure DTAP, c'est-à-dire un environnement Développement, Test (interne), Acceptation (externe) et Production. Ces environnements sont parfaitement distincts et une politique très stricte de mise en production s'applique.

Développement **Test** **Acceptation** **Production**

OWASP

L'« Open Web Application Security Project » tient à jour un top 10 des principales menaces.
RDMG Uitgevers suit de près les recommandations et le top 10 de l'OWASP afin de maintenir un niveau de sécurité optimal.

Sécurité des mots de passe

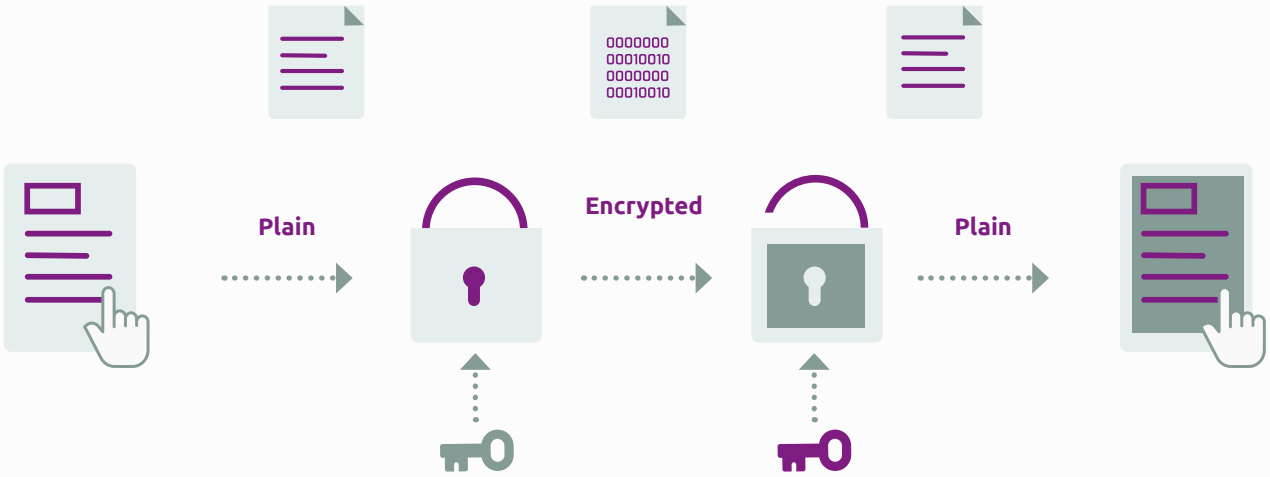
Pharius utilise des algorithmes de hachage dont l'efficacité a été démontrée pour protéger les mots de passe des utilisateurs.

Analyse des vulnérabilités

RDMG Uitgevers dispose de logiciels sophistiqués d'analyse et de reporting qui assurent une surveillance automatique du système de protection de Pharius.

Sécurité SSL

Le transfert de données entre le navigateur de l'utilisateur final et les serveurs web est protégé par un certificat SSL.
Toutes les données envoyées et reçues sont donc cryptées et ne peuvent être interceptées par une personne malveillante.



Conception sûre

Chaque modification ou fonctionnalité nouvelle est soumise à une politique de gestion des modifications afin de garantir que toutes les modifications apportées à l'application ont été autorisées avant d'être intégrées dans la production. La solide infrastructure de sécurité basée sur les normes OWASP implémentée au niveau de l'application comprend des fonctionnalités destinées à limiter les menaces telles que l'injection SQL, l'injection de code indirecte (*cross-site scripting*) et les attaques par déni de service (DoS - *denial of service*) au niveau de l'application.

Garantie liée au fournisseur

Notre fournisseur en matière de développement web possède une expérience démontrée dans le secteur des logiciels basés sur le web comme Pharius. Cette entreprise est certifiée ISO 9001. RDMG Uitgevers a signé avec elle un Service Level Agreement (SLA) et un accord relatif aux sous-traitants dans le cadre du Règlement général sur la protection des données (RGPD). Les collaborateurs sont contractuellement tenus de respecter le secret professionnel et disposent de l'expertise requise en matière de sécurité de l'information.

Garantie relative au personnel

Les collaborateurs de RDMG Uitgevers sont tenus, en vertu de leur contrat de travail, de respecter strictement le secret professionnel concernant les données des clients. Lorsqu'un contrat de travail prend fin, les données d'accès à notre application sont immédiatement bloquées.

Accès administrateur

Nous utilisons des contrôles d'accès techniques et mettons en œuvre une politique interne (certifiée ISO) pour éviter que des collaborateurs n'accèdent de façon arbitraire aux données des utilisateurs. Nous nous en tenons aux principes des droits assortis de compétences minimales et des autorisations basées sur les rôles afin de minimiser le risque de divulgation de données.

Un système central contrôle l'accès aux environnements de production. La vérification repose sur une combinaison de mots de passe forts, l'authentification à deux facteurs et des clés SSH. Nous autorisons en outre cet accès via un réseau séparé basé sur des règles strictes et des appareils sécurisés. Nous enregistrons toutes les activités et les contrôlons régulièrement.

Pharius
Conformité attestée.