

Cybercrime & security

Cybercrime is helaas een gegeven. Daarmee is informatiebeveiliging van groot belang geworden. Wij nemen u graag mee in enkele belangrijke elementen uit het palet van voorzorgsmaatregelen die RDMG Uitgevers heeft getroffen voor haar applicatie Pharius.

Het palet waar wij en onze leveranciers mee werken bestaat uit de onderwerpen: datacenter, hosting omgeving, backups, architectuur en beheer, OWASP (open web application security project), wachtwoord beveiliging, vulnerability scanning, SSL-beveiliging, veilig ontwerp en beheerderstoegang. Dit palet en haar onderlinge samenhang leiden tot een hoog niveau van beveiliging voor de data van onze gewaardeerde klanten en gebruikers.

Datacenter

De hosting en opslag is ondergebracht bij het moderne Nederlandse datacenter BIT in Ede.

Naast de ISO-certificatie is het datacenter ook NEN 7510 gecertificeerd. Dit certificaat geldt voor het toepassingsgebied ontwikkelen, leveren en ondersteunen van (cloud)diensten, connectiviteit en managed IT diensten. Er wordt voldaan aan de best practices van de ISO 27002.

Het datacenter is onderdeel van een netwerk van drie ruim van elkaar gelegen datacenters. Indien nodig is het daarmee mogelijk om uit te wijken naar een van de andere datacenters. Daarnaast zijn deze onderling verbonden met redundant uitgevoerd glasvezel verbindingen.

De provider garandeert 99.9% uptime. De webserver worden 24/7 gemonitord op storingen, dataverkeer, schijfcapaciteit, belasting en (afwijkend) gebruik. Bij afwijkingen wordt er direct gesignaleerd en actie ondernomen.

De toegangscontrole van het datacenter is georganiseerd middels een passysteem, waarbij logging extern wordt geregistreerd.

Voor wat betreft inbraak is het datacenter BORG klasse 3 beveiligd en voorzien van een uitgebreide



inbraakinstallatie met directe doormelding naar de meldkamer. Een hekwerk om het pand (met schrikdraad) en een CCTV installatie zorgen voor aanvullende veiligheid.

Voor wat betreft brand zijn alle datavloeren voorzien van een aspiratiesysteem. Dit systeem is in staat om brand in een extreem vroeg stadium te ontdekken. Via optische rookmelders (die zowel boven- als onder de datavloer zijn gemonteerd) wordt gasblussing geactiveerd indien er daadwerkelijk brand wordt gedetecteerd. De brandweer gebruikt het datacenter voor oefeningen en is dus volledig bekend met het gebouw en de aanwezige apparatuur.

Hosting omgeving

De data-opslag is gescheiden van de applicatie middels het gebruik van meerdere servers. De data-opslag is van buitenaf niet benaderbaar, maar uitsluitend benaderbaar vanuit het interne netwerk. Onze servers zijn voorzien van de laatste veiligheidsupdates en worden actief bijgehouden en gemonitord.



Update ...



Back-ups

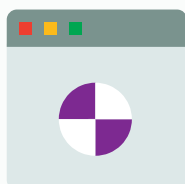
Alle data wordt dagelijks veilig gesteld aan de hand van software oplossingen voor het automatisch uitvoeren van back-ups. De back-up wordt gemaakt op een aparte server op een aparte, beveiligde locatie en is niet toegankelijk van buitenaf.

Architectuur en beheer

Pharius is gebaseerd op een OTAP structuur. Dat betekent dat er een Ontwikkel, Test (intern), Acceptatie (extern) en Productie omgeving is. De omgevingen zijn strikt gescheiden en er is een strak releasebeleid.



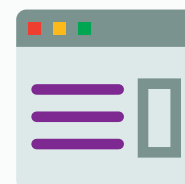
Ontwikkeling



Test



Acceptatie



Productie

OWASP

Het "Open Web Application Security Project" houdt een top 10 bij van grootste bedreigingen. RDMG Uitgevers volgt de aanbevelingen en top 10 van de OWASP nauwgezet om zo het beveiligingsniveau optimaal te houden.

Wachtwoord beveiliging

Pharius gebruikt bewezen hashing-algoritmes voor het beveiligen van gebruikerswachtwoorden.

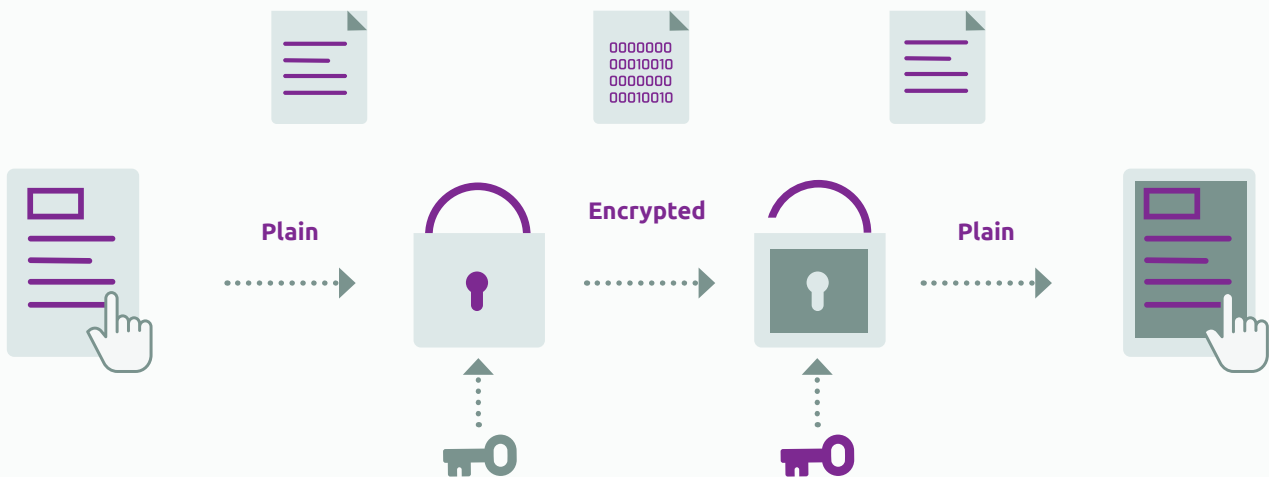
Vulnerability scanning

RDMG Uitgevers beschikt over high-end software om op automatische wijze de beveiliging van Pharius te scannen en rapporteren.

SSL-beveiliging

De gegevensoverdracht tussen de browser van de eindgebruiker en de webserver is beveiligd met een SSL-certificaat.

Hierdoor is alle verzonden en ontvangen data versleuteld waardoor gegevens niet onderschept kunnen worden door een kwaadwillende.



Veilig ontwerp

Elke wijziging en nieuwe functionaliteit is onderworpen aan een beleid voor wijzigingsbeheer om ervoor te zorgen dat alle wijzigingen in de applicatie zijn geautoriseerd voordat deze in productie worden genomen.

Ons robuuste beveiligingsframework op basis van OWASP-standaarden, dat is geïmplementeerd in het applicatieniveau, biedt functies om bedreigingen zoals SQL-injectie, cross-site scripting en DOS-aanvallen op applicatieniveau te beperken.

Borging leverancier

Onze leverancier inzake webdevelopment is een ervaren ontwikkelaar van webbased-software zoals Pharius. Het bedrijf is ISO-9001 gecertificeerd. RDMG Uitgevers heeft met hen een Service Level Agreement (SLA) afgesloten en een Verwerkersovereenkomst in het kader van de AVG. De medewerkers zijn contractueel gebonden aan geheimhouding en beschikken over expertise inzake informatiebeveiliging.

Borging personeel

Medewerkers van RDMG Uitgevers zijn middels hun arbeidscontract gehouden aan strikte geheimhouding aangaande klantgegevens. In geval van uitdiensttreding worden toegangsgegevens tot onze applicatie per direct geblokkeerd.

Beheerderstoegang

We gebruiken technische toegangscontroles en intern beleid (ISO-gecertificeerd) om te voorkomen dat medewerkers op een willekeurige manier toegang hebben tot gebruikersgegevens. We houden ons aan de principes van rechten met minimale bevoegdheden en rolgebaseerde machtigingen om het risico op blootstelling van gegevens te minimaliseren.

Toegang tot productieomgevingen wordt onderhouden door een centraal systeem, geverifieerd met een combinatie van sterke wachtwoorden, twee-factor-authenticatie en SSH-sleutels. Bovendien maken we dergelijke toegang mogelijk via een afzonderlijk netwerk met strenge regels en beveiligde apparaten. We registreren alle activiteiten en controleren deze regelmatig.