Informatiebeveiliging bij Van der Let & Partners

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 Van der Let & Partners heeft getroffen die voor LetsManage10 applicaties gelden.

Het palet waar wij en onze leveranciers mee werken bestaat uit de onderwerpen Algemeen (bijvoorbeeld geheimhoudingsverklaringen), Informatiebeveiligingsbeleid, Eisen aan personeel, Beheer, Logische toegangsbeveiliging, Change Management, Continuïteit Management, Incident Management, Naleving privacy, Contract Management en het SLA (Service Level Agreement). 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.**

BIT is ISO/IEC 27001 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 3 datacenters. Indien nodig is het daarmee mogelijk om uit te wijken naar een van de andere datacenters.

De provider garandeert 99.9% uptime. De web servers 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 pas-systeem, 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 van het datacenter.

Hosting omgeving

Het is mogelijk de data-opslag te scheiden 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.

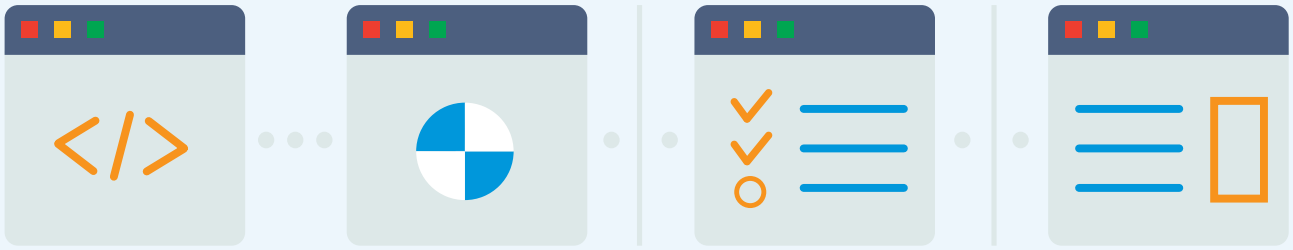
Backups

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

In overleg is het backupschema uit te breiden van dagelijks naar per uur of zelfs 'real-time'.

Architectuur en Beheer

De applicaties die gemaakt worden middels LetsManage10 zijn 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. Van der Let & Partners volgt de aanbevelingen en top 10 van de OWASP nauwgezet om zo het beveiligingsniveau optimaal te houden.

Wachtwoord beveiliging

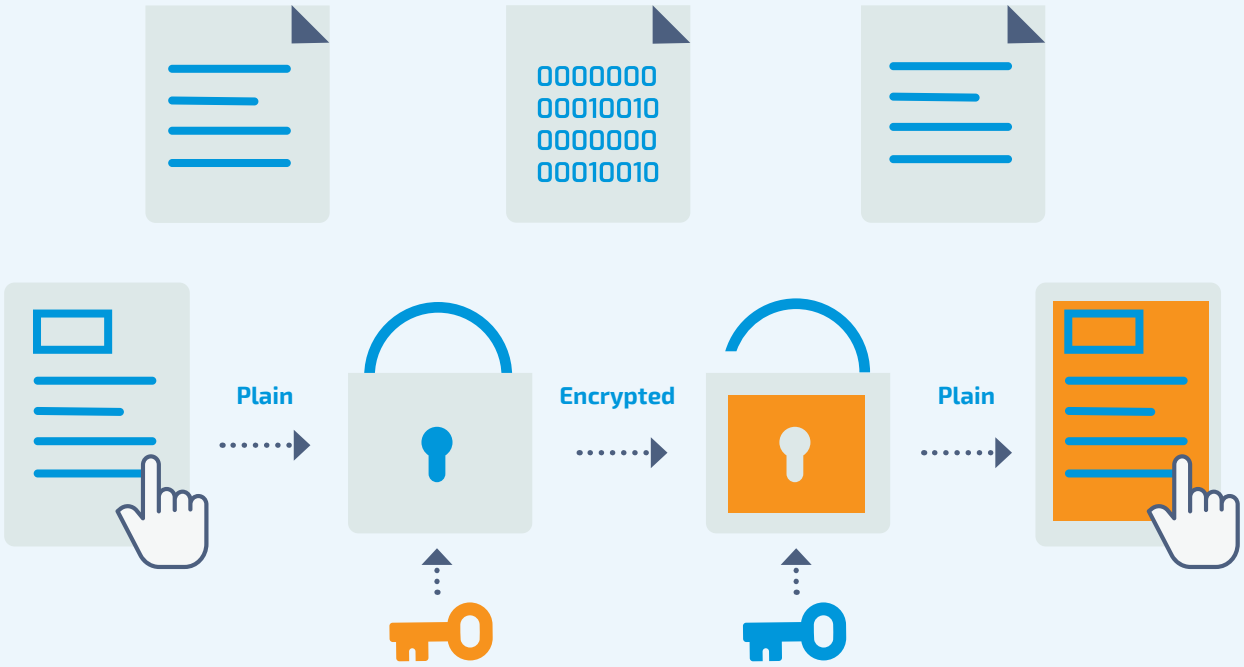
LetsManage10 gebruikt bewezen hashing-algoritmes voor het beveiligen van gebruikerswachtwoorden.

Vulnerability scanning

Van der Let & Partners beschikt over high-end software om op automatische wijze de beveiliging van webapplicaties te scannen en rapporteren.

SSL-beveiliging

De gegevensoverdracht tussen de browser van de eindgebruiker en de webservers is beveiligd met een SSL-certificaat.
Hierdoor is alle verstuurde 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 beveiligings framework 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.

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 strengere regels en beveiligde apparaten. We registreren alle activiteiten en controleren deze regelmatig.