



## Beveiliging in en rond nodum

## Changelog

Datum	Versie	Door	Opmerkingen
<b>20-06-2016</b>	v0.0.1	José van Laar	Initiële versie
<b>21-06-2016</b>	v0.0.2	Kevin Koobs	Update tekstueel en visueel
<b>29-06-2016</b>	v0.0.3	Kevin Koobs	Update tekstueel
<b>30-06-2016</b>	v1.0.0	Kevin Koobs	Tekstuele revisie
<b>23-09-2016</b>	v1.0.1	José van Laar	Update tekstueel
<b>21-10-2016</b>	v.1.0.2	José van Laar	Update tekstueel

*Nodum hecht veel waarde aan de veiligheid van het platform en zijn gebruikers. In dit document staat beschreven welke maatregelen nodum neemt om een goed beveiligingsbeleid en een optimale beleving na te streven.*

## Inhoudsopgave

### **WAT IS NODUM?**

#### **INTERNE BEVEILIGINGSMAATREGELEN**

- Voor de gebruiker
- Updates
- Internet

#### **Imperva Incapsula**

- Website beveiliging
- Tegenhouden van DDoS aanvallen
- CDN optimalisatie
- Load balancer

#### **NGINX**

- Servers
- Docker
- IP-whitelisting

### **Visuele weergave beveiliging van nodum**

#### **EXTERNE BEVEILIGINGSMAATREGELEN**

- Pentesting
- Externe API's

## Wat is nodum?

In de grote wereld van online platforms is nodum het beste te betitelen als aPaaS, ofwel application Platform as a Service. Een gebruiker kan zich aanmelden op het platform en hier een project aanmaken. Nodum voorziet in (snelle) koppelingen tussen verschillende platformen waardoor programmeren voor programmeurs slechts een fractie van de tijd kost ten opzichte van eerder. Door de relatief laagdrempelige opzet van nodum is het voor consultants, front-end-developers en webdesigners ook mogelijk om webapplicaties, koppelingen en integraties te bouwen.

Het platform (en de gebruiker) werkt op basis van projecten. Per project heeft de gebruiker de beschikking over zijn eigen omgeving met projectspecifieke HTML-, CSS- en JavaScript-code. HTML-code kan worden gecombineerd met back-end logica door middel van de Twig-syntax. Hierdoor is de gebruiker helemaal vrij in wat hij doet of laat. Nodum stelt verschillende koppelingen met API's beschikbaar. Hierdoor wordt het mogelijk om externe pakketten te koppelen aan het nodum-project. Deze koppelingen worden ontwikkeld in de nodum-console, die front- en back-end-ontwikkeling bij elkaar brengt. Door de combinatie van API's, de vrijheid om eigen code te schrijven, vrij gebruik van frameworks en de mogelijkheid tot gebruik van externe bibliotheken en de verbinding met databases en automatische routing op een kant-en-klaar systeem biedt nodum gemak in het ontwikkelen van iedere gewenste koppeling.

De gebruiker van nodum kan het platform enkel benaderen via een browser (enkel Google Chrome), er is daarom geen software anders dan de browser vereist. De koppelingen, integraties en/of websites die gemaakt worden in nodum zijn op een grote hoeveelheid mobiele apparaten en desktops te openen in een keur aan verschillende browsers.

Nodum maakt dus onderdeel uit van 'de cloud' en daardoor zal de veiligheid van het platform onder een vergrootglas liggen. Er zijn verschillende beveiligingslagen ingebouwd die in dit document behandeld zullen worden. Er is nodum alles aan gelegen om een veilige omgeving te creëren voor hen die met het platform de mooiste software bouwt.

## Interne beveiligingsmaatregelen

Zoals gezegd beschikt nodum over verschillende lagen aan 'security' om te voorkomen dat (gevoelige) data beschikbaar komt voor mensen die daar geen toegang tot hebben. De eerste schil van beveiliging wordt gevormd door de gebruiker zelf. Daarna volgen er meerdere technische lagen van beveiliging die ervoor moeten zorgen dat code en data veilig zijn binnen nodum.

### Voor de gebruiker

Gebruikers kunnen nodum alleen gebruiken op basis van een combinatie van gebruikersnaam en wachtwoord. Op [nodumapp.io](https://nodumapp.io) kan worden ingelogd met deze bij de gebruiker bekende gegevens. Daarnaast biedt nodum de mogelijkheid om 2Factor Authentication toe te passen. Deze techniek maakt gebruik van een code die alleen op een bij de gebruiker bekende plaats te vinden is en iedere dertig seconden hernieuwd wordt. Deze zescijferige code kan bijvoorbeeld worden ontvangen op een smartphone of worden gekoppeld aan een app op Windows of OSX.

Om het geautomatiseerd veelvuldig uitproberen van wachtwoordcombinaties, het zogenaamde Brute Forcing, te blokkeren wordt IP-adressen die meer dan 400 calls per minuut uitvoeren een BAN opgelegd. De openstaande verbinding wordt verbroken, waarna de BAN vanzelf weer verloopt. Naarmate de pogingen aanhouden zal de BAN ook langer worden.

Voor het beheer van alle machines behorende tot de nodum-infrastructuur wordt encrypted, 2048 bits SSH toegepast. Alleen de medewerkers van nodum kunnen bij de infrastructuur komen door middel van hardware-gebonden Private Keys.

### Updates

Het team van nodum brengt regelmatig updates uit op het platform. Wijzigingen worden uitgerold via het Git Branching Model zodat altijd herleidbaar is welke aanpassing door welke medewerker is gedaan. Ook kunnen in het verleden uitgevoerde updates die niet blijken te werken hierdoor eenvoudig worden teruggedraaid. Voordat een update beschikbaar wordt zal een nodum-medewerker nogmaals de code beoordelen.

### Internet

SSL is een van de vele technieken die bijdragen aan de veiligheid van het internet. Wanneer een website wordt bezocht via SSL is het niet mogelijk om de data die verzonden en ontvangen wordt te onderscheppen, tenzij de computer van de gebruiker is gecompromitteerd. Nodum past over het gehele platform SSL toe, te zien aan het groene slotje links van de URL in de browser. Alle communicatie loopt via HTTPS en SSL door middel van LetsEncrypt. Om bij uitrol problemen te voorkomen testen we met SkipFish (Google) om eventuele veiligheidsproblemen in de webbrowser te ondervangen.

Indien er een koppeling wordt gemaakt met een derde partij is nodum niet verantwoordelijk voor de datastroom van en naar deze partij. Koppelingen met bijvoorbeeld MailChimp, Clockwork of Slack zijn dus op eigen risico.

Ieder project wordt voorzien van SSL door middel van Lets Encrypt, nodum zelf maakt zelfs gebruik van een Comodo EV Certificaat met bedrijfsvalidatie op Synced BV.

## Imperva Incapsula

Een belangrijk beveiligingselement binnen nodum is de bescherming die [Imperva Incapsula](#) biedt. Elk klantproject dat online staat is beter beschermd door dit beveiligingsplatform. Het is hiervoor niet nodig om extra handelingen te doen zoals hardware of software te installeren, programmeercode toe te voegen of zelf integraties te maken. Ook zijn hier geen extra kosten aan verbonden voor de gebruikers van nodum. Nodum beheert en onderhoudt deze beveiliging voor het werken in [nodumapp.io](https://nodumapp.io) en alle klantprojecten op \*.nodum.io. Wanneer men een eigen domeinnaam gebruikt dient men (indien gewenst) een eigen abonnement bij Imperva, Cloudflare of een andere partij af te sluiten.

Incapsula bestaat uit een viertal onderdelen. Het biedt websitebeveiliging, het tegenhouden van DDoS aanvallen, CDN-optimalisatie en een load balancer. De beveiliging, bekend als WAF (Web Application Firewall) en daarna de DDoS mitigation zijn de belangrijkste redenen dat nodum dit beveiligingsplatform inzet. De WAF is [PCI gecertificeerd](#) door de Security Standards Council. Incapsula bezit de PCI DSS (Data security standards) 6.6, dit is de norm voor databeveiliging van webapplicaties.

### Website beveiliging

Zoals eerder in dit document beschreven staat treft nodum al diverse beveiligingsmaatregelen. Imperva Incapsula is hier als extra beveiligingslaag overheen gelegd. De software zoekt en detecteert niet wenselijke bezoekers op de website, applicatie of toepassing die op het nodumplatform zijn gebouwd. Dit kunnen bots (computerprogramma's) zijn die via contactgegevens op de website spam verzenden of hackers die het internet afgaan om zwakheden in de beveiliging te zoeken. Maar ook SQL injecties, XSS en andere aanvallen worden tegen gehouden.

### Tegenhouden van DDoS aanvallen

Bij DDoS aanvallen wordt er door veel aanvragen op hetzelfde moment af te vuren op een verbinding met de server. Zo wordt de server en zo ook de online toepassing, applicatie of website traag of zelfs onbereikbaar omdat de server zoveel verzoeken niet tegelijk kan behandelen. DDoS aanvallen zijn zonder de techniek van Incapsula moeilijk tegen te houden.

### CDN optimalisatie

De techniek van content delivery network zorgt ervoor dat de websites, toepassingen en applicaties sneller wordt geladen. Incapsula geeft hierover zelf aan: *"On average, websites using Incapsula are 50% faster and consume 60% less bandwidth"*.

### Load balancer

Deze techniek wordt ingezet om het aantal aanvragen dat wordt gedaan om een website te bekijken te verdelen over de beschikbare servers. De load balancer controleert continu de belasting van alle servers en regelt zo het aantal verzoeken per server.

Het kan ook worden gebruikt om een webservice op te schalen, hierdoor kan deze meer aanvragen behandelen. Als laatste wordt load balancing ingezet door bij een defecte server de gebruikers te verdelen over andere goed werkende servers.

## NGINX

Binnen nodum zorgt NGINX voor een buffer waar zich verschillende servers achter bevinden. De digitale aanvragen die binnenkomen in nodum worden verdeeld en gefilterd door NGINX. Het filter laat alleen gewenste aanvragen toe zodat de server minder snel overbelast raakt.

### Servers

Nodum staat continue onder monitoring. De medewerkers van nodum houden constant in de gaten wat er gebeurt en of er problemen zijn met het platform. De medewerkers hebben ook toegang tot de broncode en vallen tevens onder een geheimhoudingscontract.

Updates die via de officiële kanalen beschikbaar komen zullen in nachtelijke patches worden toegepast op het platform.

Voor nodum-gebruikers is het niet nodig om zelf hosting te regelen voor de nodum-projecten. De projecten (webapplicaties) die aangemaakt worden op het platform zullen worden gehost door nodum. Deze stelt de websites op haar beurt weer bij de Amsterdamse servers van Digital Ocean. Zij bieden een 99,99% uptime SLA-netwerk, kracht en virtuele server-beschikbaarheid. Het datacenter waar de servers staan hebben een ISO 27001 (beveiligingsmanagement), ISO 9001 (kwaliteitsmanagement), ISO 14001 (milieumanagement), OHSAS 18001 (arbomanagement) certificering en ze voldoen aan de PCI DSS normering.

### Docker

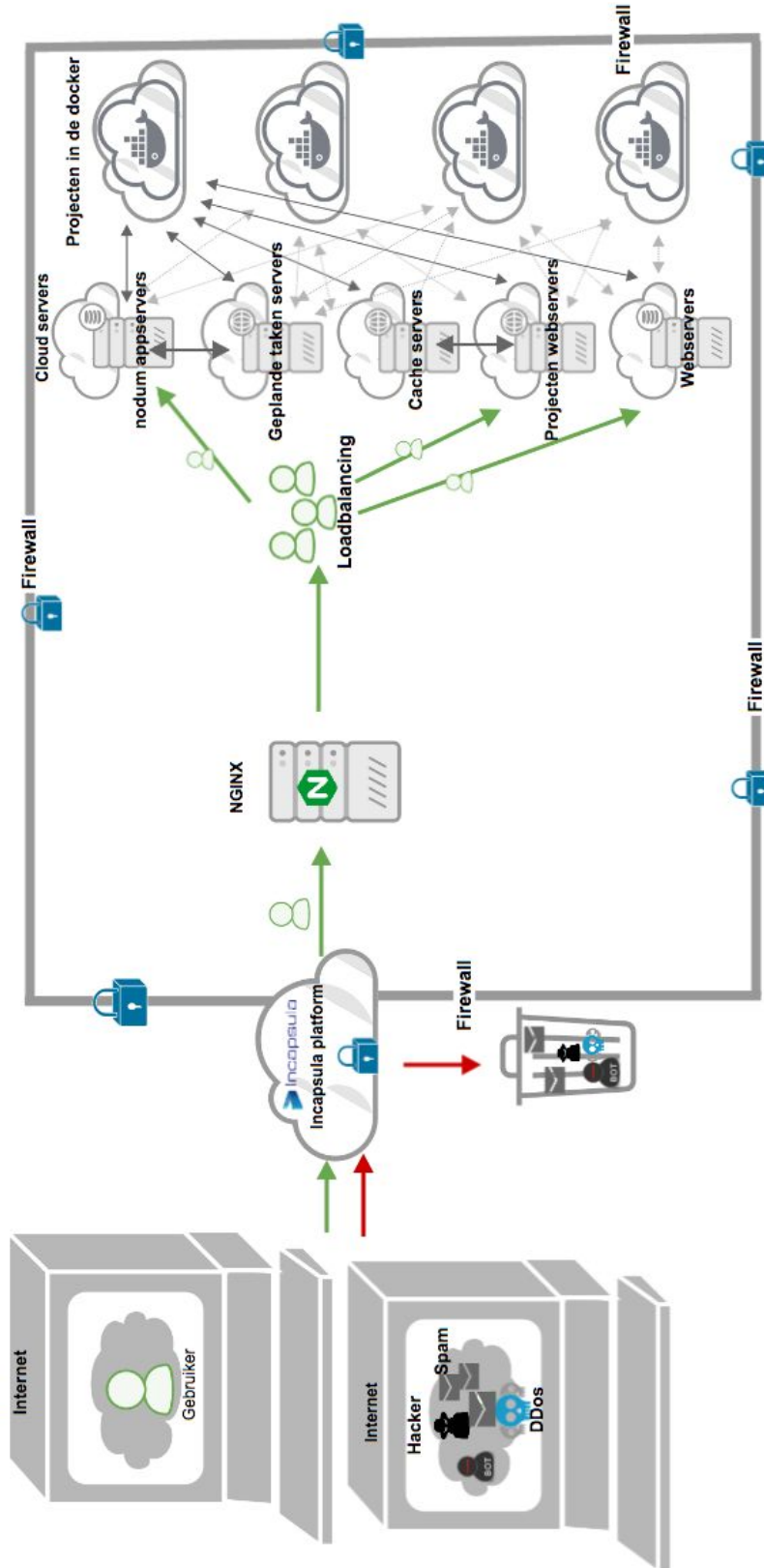
Achter NGINX en de Web Application Firewall (WAF) worden de projecten in containers op de servers opgeslagen. Deze containers maken gebruik van de technieken van Docker waardoor het niet mogelijk is om vanuit een project naar de brondata van een ander project te gaan. Door het gebruik van Docker worden de projecten geheel van elkaar gescheiden, het zogenaamde Sandboxing. Docker biedt een van de meest vooraanstaande methodes hiervoor, waarbij er minimale extra overhead ontstaat.

## IP-whitelisting

De communicatie tussen een externe gebruiker en nodum is afkomstig vanaf een eigen IP-adres. Het is in nodum mogelijk om bepaalde IP-adressen te whitelisten voor een project, waardoor alleen die betreffende adressen toegang krijgen tot het platform. Hierdoor wordt het mogelijk om een bedrijfsnetwerk toegang te geven tot het nodum-project zodat het project enkel intern benaderd kan worden. De instellingen hiervoor kunnen worden aangepast in de algemene configuratie van een project.



## Visuele weergave beveiliging van nodum



## Externe beveiligingsmaatregelen

Iedere klant heeft de software in een eigen zogenaamde sandbox draaien. Toegang tot de infrastructuur van het platform is enkel mogelijk voor medewerkers van nodum vanaf het IP-adres van het kantoor in Amersfoort. Een 2048 bits SSL VPN-verbinding en hardware-gebonden Private Key zijn eveneens nodig om bij de sandboxes te kunnen komen. Al onze servers worden tevens nachtelijk gepatcht door middel van Landscape.

Nodum moedigt haar gebruikers aan om zelf ook pentests te laten doen. Dit echter wel in overleg met het nodumteam zodat er een sandbox geregeld kan worden voor de test die extreme load of schade aan het systeem kan voorkomen.

### Pentesting

Nodum laat haar software zowel op infra-niveau als op web-applicatie-niveau pentesten door Acunetix. Er zijn nog nooit kritische zaken in het platform aangetroffen. Tevens heeft nodum recent meerdere pentests door grote afnemers met verve doorstaan. Voor meer informatie kan contact worden opgenomen met nodum.

### Externe API's

Het platform dient enkel als doorgeefluik waar de gebruiker data uit externe bronnen op kan opslaan. Nodum zal nooit ongevraagd data opslaan uit externe bronnen tenzij de projecteigenaar dit als zodanig heeft ontwikkeld. Nodum doet er alles aan om deze informatie zo veilig mogelijk te houden.