Continuïteit Nedap Ons

Document

Last review date	13 Mar 2022
Classification	PUBLIC

Inleiding

Nedap Healthcare levert software-as-a-service (SaaS) oplossingen voor klanten in de zorgsector. Voor ons en onze klanten is het essentieel dat onze software 24 uur per dag, 7 dagen per week beschikbaar is. Om te kunnen voldoen aan deze beschikbaarheidseisen zijn er vele maatregelen en technieken ingezet. Dit document van Nedap Healthcare is een samenvatting waarin de belangrijkste elementen van onze interne documentatie en processen op het gebied van (bedrijfs)continuïteit beschreven staan.

Het is goed om te realiseren dat Nedap Healthcare niet de volledige infrastructuur van Ons tot aan de eindgebruiker onder controle heeft en/of er invloed op kan uitoefenen. De dienstverlening is een software-as-a-service (SaaS) model, en dat betekent dat de eindgebruikers en klanten zelf moeten zorgen voor een goede, stabiele, redundante internetverbinding en eventuele interne infrastructuur. De invloedssfeer van Nedap Healthcare is beperkt tot het moment dat de data onze datacenters verlaat, en via het internet beschikbaar komt.

Redundantie

Uitgangspunt voor de volledige dienstverlening van Nedap Healthcare is dat deze zo is opgebouwd dat er zowel technisch als juridisch-organisatorisch geen single-point-of-failure (SPOF) bestaat.

Redundante housing in meerdere datacenters in Nederland

Tijdens risicoanalyses en kwetsbaarheidsanalyses die door Nedap Healthcare zijn uitgevoerd, zijn een verscheidenheid aan risico's geïdentificeerd. De belangrijkste preventie-maatregel die wij hebben genomen om bedrijfscontinuïteit te kunnen garanderen, is redundantie. Om alle mogelijke verstoringen die vallen in de categorie "Natuurlijke rampen" (storm, overstroming, stroomuitval, brand, ...) te kunnen opvangen, is onze dienstverlening redundant ondergebracht in 4 verschillende datacenters van twee juridisch volledig gescheiden organisaties in Nederland met een grote geografische spreiding:

- Amsterdam (datacenter van Equinix Netherlands B.V.)
- Enschede (datacenter van Equinix Netherlands B.V.)
- Hengelo, Overijssel (datacenter van Previder B.V.)
- Zwolle (datacenter van Equinix Netherlands B.V.)

Tussen de verschillende datacenters is een volledig redundante, fysiek volledig gescheiden glasvezelring aangelegd. Al deze inter-datacenter links zijn bovendien volledig versleuteld door middel van de industry-standard technologie IEEE 802.1AE. Dit betekent dat iemand die toegang krijgt tot één van de glasvezelverbindingen tussen onze datacenters daarmee nog steeds geen toegang kan krijgen tot informatie die tussen de datacenters wordt getransporteerd.

Voor alle datacenters geldt dat er strikte eisen zijn gesteld aan de (fysieke) toegang tot de datacenters en dat alleen personeel van Nedap Healthcare bepaalt wie er toegang heeft tot de servers. Ook voldoen alle datacenters aan de strengste eisen op het gebied van toegangsbeveiliging, klimaatbeheersing, brandpreventie en stroom-redundantie (UPS, generatoren). De datacenters waar Nedap Healthcare gebruik van maakt zijn in ieder geval ISO 27001 en NEN 7510 gecertificeerd. Daarnaast bezitten de datacenters over een SOC en/of ISAE verklaring voor Data Center Hosting Services (of vergelijkbaar).

Uitval van IT componenten kan altijd voorkomen. Om hierop voorbereid te zijn, hebben we verschillende vormen van redundancy toegepast op verschillende niveau's in onze infrastructuur en applicatie-ontwerp. De verschillende vormen worden gebruikt in verschillende situaties, waardoor beschikbaarheid maar ook (bijvoorbeeld) data-integriteit passend wordt beschermd in de specifieke situatie.

Juridische redundantie

Zoals eerder benoemd onder "Redundante hosting in meerdere datacenters in Nederland" is onze dienstverlening redundant ondergebracht in 4 verschillende datacenters van twee juridisch volledig gescheiden organisaties in Nederland. De scheiding van de dienstverlening loopt ook grofweg over dezelfde lijn: ongeveer de helft van de dienstverlening wordt aangeboden vanuit het datacenter van de ene leverancier en de helft van de dienstverlening wordt aangeboden vanuit datacenters van de andere. Doel van deze scheiding is dat het (mogelijke) uitvallen van 1 van deze leveranciers geen gevolgen heeft voor de dienstverlening van Nedap Healthcare. Hiertoe wordt bijvoorbeeld ook alle data in databases van alle klanten in meerdere datacenters opgeslagen, waarvan altijd minimaal één kopie in een datacenter van de ene leverancier en minimaal één kopie in een datacenter van een andere leverancier.

Ook de bedrijfscontinuïteit van de dienstverlening van Nedap Healthcare bij een mogelijk ernstig gevolg voor Nedap zelf (bijvoorbeeld faillissement) is geborgd. Daarvoor zijn we met één van de twee leveranciers een continuïteitsovereenkomst overeen gekomen. Naast afspraken over het continueren van de dienstverlening is er ook door middel van een bankgarantie geborgd dat de dienstverlening van Nedap Healthcare in ieder geval voor een halfjaar gecontinueerd zal worden. Met de andere leverancier is een dergelijke afspraak niet gemaakt, omdat dit door de al aanwezige datacenter-redundantie (zie hiervoor) geen toegevoegde waarde heeft.

Redundantie van (internet)connectiviteit

Gezien de aard van de dienstverlening - een software-as-a-service (SaaS) model - is connectiviteit met het internet en klanten van groot belang. Nedap Healthcare is daarvoor zelf direct en redundant aangesloten op twee van de grootste internet-knooppunten van Europa: de Amsterdam Internet Exchange (AMS-IX) en de Neutral Internet Exchange (NL-ix). Daarnaast heeft Nedap Healthcare private verbindingen met zorgspecifieke of andere relevante netwerken, zoals bijvoorbeeld E-Zorg. E-Zorg is een besloten (zorg)netwerk, volledig gescheiden van het openbare internet.

Overige maatregelen

Bescherming van connectiviteit

De capaciteit van alle internetverbindingen is ruim voldoende voor de dienstverlening van Nedap Healthcare. Deze capaciteit wordt voortdurend gemonitord en wordt ook regelmatig uitgebreid.

Desondanks kan het voorkomen dat de capaciteit onvoldoende is voor de meest extreme situaties - meestal gaat het dan om (Distributed) Denial of Service aanvallen, afgekort (D)DoS-aanvallen. Om te voorkomen dat de dienstverlening van Nedap Healthcare getroffen wordt door dit soort aanvallen, wordt er op meerdere plaatsen in de dienstverlening gebruik gemaakt van anti-DDoS oplossingen.

Monitoring en informatievoorziening

Er vindt alle dagen van het jaar - 24x7 - monitoring plaats op de dienstverlening van Nedap Healthcare. Dit beperkt zich niet alleen tot het monitoren van beschikbaarheid, maar ook zaken als performance wordt gemonitord. De monitoring van de dienstverlening leidt in het geval van verstoringen ook - geautomatiseerd - tot het inschakelen van personeel van Nedap Healthcare. Natuurlijk is ook de supportafdeling van Nedap Healthcare 24x7 te bereiken. Buiten kantoortijden is support enkel te bereiken voor het melden van kritieke incidenten of andere ernstige problemen. Zie voor meer informatie over de ondersteuning en support van Nedap Healthcare de SLA.

Naast de supportafdeling zijn ook ontwikkelaars 24x7 beschikbaar in zogenaamde on-call shifts om incidenten op te kunnen lossen. Ook zijn er afspraken met de belangrijkste leveranciers om op (zeer) korte termijn ondersteuning te bieden, mocht dat nodig zijn. Bij een grote(re) verstoring waarbij een meerdere klanten getroffen worden, wordt er pro-actief gecommuniceerd via het Supportportaal en de statuspagina van Nedap Healthcare.

Maatregelen bij klantorganisaties

Dit document van Nedap Healthcare beschrijft de belangrijkste maatregelen die Nedap Healthcare heeft genomen om de continuïteit van de dienstverlening van Nedap Healthcare te borgen. Er zijn echter ook een aantal maatregelen die de klantorganisatie kan nemen om de beschikbaarheid van Nedap Healthcare voor haar gebruikers verder te borgen, of alternatieven in te richten zodat de belangrijkste informatie beschikbaar is en er in veel gevallen doorgewerkt kan worden.

Internetverbinding

De gebruikers van Nedap Healthcare zijn (ook) afhankelijk van partijen als telecomproviders en internet service providers (ISP) voor de dienstverlening. De dienstverlening van Ons is Software-as-a-Service dienstverlening, en is daarmee afhankelijk is van een werkende internetverbinding van zowel de aanbieder als de gebruiker. Het verdient de aanbeveling om als klant te inventariseren welke leveranciers onderdeel uitmaken van deze keten en na te gaan welke maatregelen de provider heeft genomen om toegang tot Nedap Healthcare te kunnen blijven leveren. Eventueel kan een klant ook aanvullende maatregelen treffen; denk hierbij bijvoorbeeld ook aan het redundant uitvoeren van eigen internetverbindingen (bekabeld, of SIM-kaarten van meerdere telecomproviders).

Offline werken

De mobiele apps van Nedap Healthcare (voor Android en iOS) zijn voor belangrijke delen ook offline te gebruiken. Deze functionaliteit is ontworpen om te kunnen werken op plaatsen waar geen mobiel bereik of WiFi beschikbaar is, maar werkt ook in gevallen dat Nedap Ons niet bereikbaar is via de betreffende telecomprovider of internet service provider.

In de Nedap Ons app zijn planning, team- en cliëntgegevens offline beschikbaar. Deze informatie wordt periodiek bijgewerkt. De gebruiker kan bijvoorbeeld dus altijd offline de planning inzien of het telefoonnummer van een cliënt kan opzoeken.

Ook is de Ons Dossier app offline te gebruiken: het is mogelijk om dossiers in te zien en rapportages te schrijven, óók op het moment dat er geen internetverbinding is of Ons niet beschikbaar is. Standaard

probeert deze app elke zes uur de informatie te verversen. Rapportages en metingen kunnen ook gemaakt worden terwijl je offline bent; deze worden in het dossier opgeslagen zodra er weer verbinding is.

Andere alternatieve oplossingen

Afhankelijk van de behoeften van een klant zijn er ook andere processen in te richten om op alternatieve manier door te kunnen werken. Zo is het bijvoorbeeld mogelijk om elke nacht een PDF-export van de planning uit Ons Planning naar een e-mailadres van de klant te mailen als mogelijke backup-oplossing. Het spreekt voor zich dat als gebruik wordt gemaakt van dergelijke backup-scenarios er ook processen aan de zijde van de klant moeten zijn ingericht om het gebruik van deze scenarios mogelijk te maken. Vergelijkbare afwegingen gelden bijvoorbeeld voor scenarios waarbij (papieren) nooddossiers worden ingericht.