North Sea Port IT infrastructuur

Architectuur visie 2019 en verder – consumer simple, enterprise secure

Auteur : Patrick Rutten

Datum : 2021-02-12

Versie : 1.2

0. Document historie

Versie	Datum	Auteur	Opmerkingen
0.1	2018-06-12	Patrick Rutten	Initiële opzet
0.2	2018-06-19	Patrick Rutten	Uitwerken thema's
0.3	2018-07-12	Patrick Rutten	Diverse updates
0.4	2018-08-08	Patrick Rutten	Diverse updates
0.5	2018-08-27	Patrick Rutten	Diverse updates
0.6	2018-09-11	Patrick Rutten	Commentaar Els verwerkt, diverse updates
0.7	2018-09-14	Patrick Rutten	2.1 uitgebreid met businessvragen cq - criteria
0.8	2018-09-21	Patrick Rutten	Thema's toegelicht
0.9	2018-10-23	Patrick Rutten	Aanpassingen na overleg binnen IT-T overleg
0.10	2019-03-05	Rick van Sluijs	Review en aanvullingen
0.11	2019-10-17	Patrick Rutten	Digital Workspace & Cloud
1.0	2019-11-08	Patrick Rutten	Definitief
1.1	2019-12-04	Patrick Rutten	Client applicatie voorkeur
1.2	2021-02-12	Patrick Rutten	Diverse updates

Inhoudsopgave

1. Inleiding

Voor u ligt een document dat richting geeft aan en duidelijkheid verschaft over de IT infrastructuur van North Sea Port. Beoogde lezers zijn naast de collegae binnen het IT cluster, ook collegae van inkoop en (beoogde) leveranciers. Zo kan het document bijvoorbeeld gebruikt worden als leidraad bij het aanschaffen van nieuwe IT systemen en het beheer van deze.

Het document beschrijft op punten de as-is situatie, en daar waar er al duidelijkheid over is, de beoogde situatie.

IT draagt bij aan het bereiken van de strategische doelstellingen door samen met de organisatie op een gestructureerde, betrouwbare en efficiënte wijze informatie/inzicht te creëren, beheren, analyseren en beschikbaar te stellen middels gepaste technologie.

Hierdoor wordt er meerwaarde gecreëerd voor de haven en de stakeholders (intern en extern) en wordt de werkvreugde van North Sea Port medewerkers verhoogd.

De (fysieke) IT-infrastructuur van North Sea Port is het fundament onder de overige IT-voorzieningen en informatiesystemen.

Dit document is een verfijning van de technische infrastructuuroverwegingen, zoals vastgesteld door het MT (IT-kaders) op 18 december 2018. De daarin genoemde uitgangspunten waren:

1. De infrastructuur moet schaalbaar (groter-kleiner) zijn;
2. Toegang tot de IT-informatievoorzieningen is anytime anyplace mogelijk, mits internet aanwezig is;
3. Flexibel zijn voor wat betreft de volgende zaken:
    a. Locatie van de voorzieningen (geografisch, in house of cloud);
    b. Uitbreidbaarheid met nieuwe functies of gebruik (bijvoorbeeld: videoconferencing vanaf werkplek, gebruik door externe partijen).

Specifieke aandacht voor security. Misbruik wordt getracht te voorkomen, de volgende uitgangspunten worden daarbij gehanteerd:

1. Medewerkers gebruiken de voorzieningen op eigen inzicht (dus: niet alles ‘dicht zetten’);
2. Externen (ook IT-leveranciers) hebben geen toegang tot productiesystemen en -data;
3. Pragmatische invulling aan GDPR-vereisten;
4. Cloud-richtlijn adviseert over in de cloud zetten van data of functionaliteit. MT beslist desgewenst daarover.

Door de strategieën en richtlijnen uit dit document te volgen en aan de eisen te voldoen wordt een goed functionerende en beheersbare IT omgeving gewaarborgd. Hierbij wordt gestreefd naar een “enterprise agility”. Hiermee wordt een robuust en veilige backend bedoeld (availibility, stability en security), waarbij zeker de aandacht voor de eindgebruiker niet vergeten mag worden: “consumer simple, enterprise secure”.

2. Strategieën en richtlijnen

2.1. Context en toelichting

Dit hoofdstuk beschrijft de strategieën en richtlijnen aangaande de IT infrastructuur van North Sea Port. Dit is de huidige visie. Omdat ontwikkelingen -als fusiebedrijf- elkaar snel opvolgen, zal dit visiedocument in de tijd geactualiseerd en aangepast worden.

Een IT infrastructuur bestaat uit diverse onderdelen en worden verderop in dit document toegelicht. Zo moet(en):

- alle locaties onderling verbonden worden om een bedrijfsnetwerk te kunnen realiseren;
- er servers zijn om applicaties en diensten aan te kunnen bieden;
- de IT apparatuur op locatie ook met elkaar kunnen communiceren via een netwerk;
- medewerkers in staat worden gesteld om applicaties te kunnen gebruiken;
- beveiligde toegang tot applicaties en data goed geregeld te zijn;
- medewerkers de juiste IT middelen tot hun beschikking gesteld krijgen.

Uitgegaan wordt daarom van de volgende 6 thema's waarin North Sea Port de IT infrastructuur heeft onderverdeeld:

- WAN infrastructuur;
- Backend infrastructuur;
- LAN infrastructuur;
- Application delivery;
- Authenticatie;
- Werkplekinrichting.

Om tot een goed functionerende en beheersbare IT omgeving te komen is het belangrijk dat minimaal voldaan wordt aan de volgende businessvragen cq. -criteria:

- De omgeving dient 24u per dag beschikbaar en bereikbaar te zijn. Hiervoor geldt 99,5% uptime en maximaal 4 dagen per jaar gepland niet-beschikbaar. Dit komt neer op 43,8 uur per jaar ongepland en 96 uur per jaar gepland niet-beschikbaar zijn van de omgeving;
- In geval van een disaster wordt op dit moment gehanteerd: een RPO (= maximaal toelaatbare hoeveelheid dataverlies) van 12 uur en een RTO (hersteltijd na calamiteit) van 48 uur;
- Zorg voor een IT-beheersmatige oplossing welke financieel haalbaar is;
- Medewerkers moeten in staat worden gesteld op een eenvoudige maar veilige manier hun werkzaamheden uit te kunnen voeren met de aan hen beschikbaar gestelde IT middelen.

De kantoorautomatiseringsomgeving van North Sea Port is gebaseerd op het Microsoft platform; denk dan aan Microsoft Server, Microsoft SQL databases, Microsoft Office 365 Cloud diensten, etc..

North Sea Port geeft de voorkeur aan gestandaardiseerde aangeboden diensten / producten[1]: best-of-breed-oplossingen die voldoen aan de Microsoft standaarden. Hoe dichter op de backend van de IT-infrastructuur (bijvoorbeeld besturingssoftware servers), hoe groter de voorkeur voor

[1] Dit uitgangspunt is terug te lezen in de IT-kaders waarop het MT d.d. 18-12-2018 besloten heeft.

Microsoftproducten. Reden hiervoor is o.a. de geringe omvang van de organisatie en het IT-T-team. In plaats van een brede kennis van IT producten en diensten op te bouwen, heeft North Sea Port ervoor gekozen om de beheerders te trainen in een beperkte set van IT producten en diensten met als doel diepgaande kennis te vergaren.

De keuze voor een Microsoft platform betekent niet dat andere producten en diensten per definitie zijn uitgesloten. Indien andere producten en diensten worden aangeboden, dient er een goede onderbouwing van de keuze daarvoor meegeleverd te worden. In deze onderbouwing dient ook aangegeven te worden waarom een mogelijk alternatief in het Microsoft portfolio niet de voorkeur heeft.

2.2. WAN infrastructuur

Omdat de situatie voorlopig zo zal zijn dat er meerdere hoofdlocaties (kantoren) zijn, is de visie dat:

- er 1 domein gerealiseerd wordt welke gesitueerd is op de beide hoofdlocaties;
- hoofdlocaties o.b.v. active-active ingezet worden (zie ook paragraaf 2.3.4);
- wanneer er in de toekomst gekozen wordt 1 nieuw pand te gebruiken, blijft dit principe toepasbaar en is praktisch verhuisbaar;
- de niet-benutte resources tevens toegepast kunnen worden voor test-doeleinden.

Met de WAN infrastructuur wordt de infrastructuur bedoeld die nodig is om de diverse North Sea Port locaties met elkaar te verbinden op een zodanige manier dat er een stabiel en veilig bedrijfsnetwerk gerealiseerd kan worden. Om de North Sea Port locaties onderling te verbinden wordt primair gebruik gemaakt van glasvezelverbindingen die communicatie toestaan zonder gebruik te maken van VPN verbindingen. Op dit moment wordt nog een VPN-tunnel over het publieke internet gebruikt om Terneuzen met Gent te koppelen; deze wordt in 2021 uitgefaseerd vanwege een mindere mate van controle, bandbreedte, latency etc.. Voor verbindingen naar andere locaties worden geen VPNs ingezet.

2.3. Backend infrastructuur

Met de backend infrastructuur wordt de infrastructuur bedoeld die nodig is om medewerkers van North Sea Port in staat te stellen de voor hen beschikbare ICT middelen te kunnen gebruiken. Denk dan aan bijvoorbeeld de apparatuur en systemen die in de server-ruimtes staan. Om de RTO zo kort mogelijk te laten zijn in geval van calamiteiten, is het van groot belang dat deze infrastructuur een hoge beschikbaarheid, stabiliteit en beveiliging geniet. Een uitwijkmogelijkheid in geval van calamiteit op één van de hoofdlocaties is nodig om de continuïteit van de bedrijfsvoering te kunnen waarborgen.

2.3.1. Servers

North Sea Port heeft de kantoorautomatiseringsomgeving nagenoeg volledig gevirtualiseerd; uitzonderingen zijn back-upservers en enkele Domain Controllers. Het gebruikte virtualisatie platform is gebaseerd op VMware vSphere.

Het uitdelen van resources (CPU, RAM, HDD) vindt plaats naar behoefte. De initiële basisconfiguratie is een Windows Server Standard 2016 voorzien van 2 vCPU, 8 GB RAM en 100 GB HDD. Indien meer dan de initieel toegekende resources nodig zijn, dient de noodzaak hiervan onderbouwd te worden. Zo dient de leverancier uit reproduceerbare tests aan te tonen dat structureel (over een periode van

een week) minimaal 75% van de resources belast wordt. Piekbelastingen van 100% mogen niet langer dan 15 minuten duren.

2.3.2. Storage

Het virtualisatieplatform is gekoppeld aan een centrale storage oplossing. Op dit moment wordt gebruik gemaakt van een HP 3PAR- en DELL VxRail-oplossingen.

Gekeken wordt of van de storage omgeving één platform gerealiseerd kan worden wat zich over beide hoofdlocaties heen uitstrekt. Voorwaarde voor 1 integraal platform zijn goede (glasvezel-) verbindingen tussen beide hoofdlocaties.

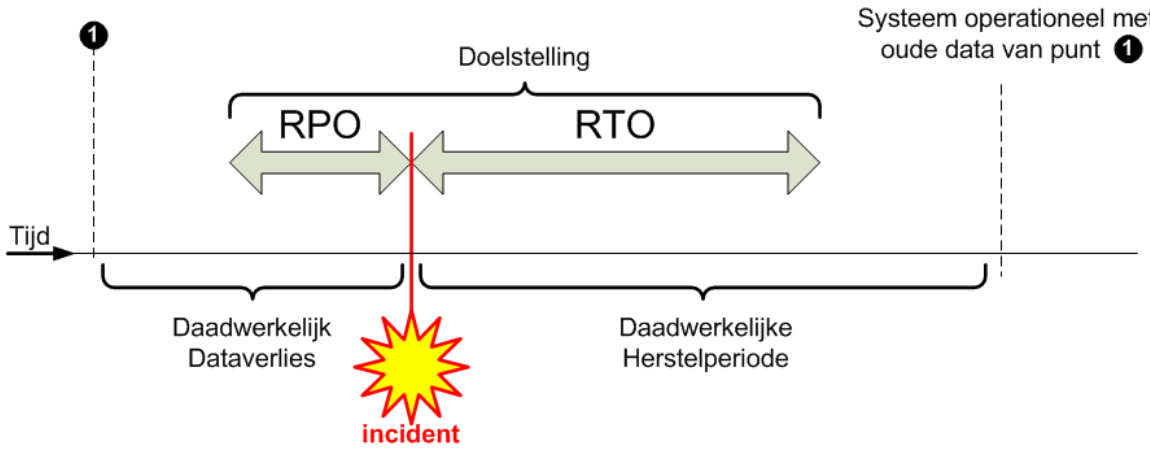
2.3.3. Back-up

Als back-up product is Veeam Backup and Replication reeds ingezet. Back-ups worden niet alleen weggeschreven naar disk (Dell Data Domain), maar ook naar tape. Structureel wordt een back-up off-site gehaald. Backups weggeschreven naar de Data Domains worden gerepliceerd naar de andere hoofdvestiging.

De Office 365 omgeving (Exchange, SharePoint) wordt eveneens met Veeam geback-upt. Hiervoor is een virtuele server ingezet op het Azure platform. Deze schrijft de back-ups weg op storage waarvan Microsoft aangeeft dat dit zich in een ander datacenter bevindt. Indien gewenst kan deze server via Azure ook nog veiliggesteld worden op een geografisch andere datacenter van Microsoft.

Op dit moment worden overige off-premises (cloud-) systemen nog niet geback-upt.

Onderstaand figuur geeft een overzicht van de Recovery Point en Recovery Time Objective. Met RPO wordt bedoeld hoeveel dataverlies er geoorloofd is. Met RTO wordt bedoeld hoelang het mag duren voordat de systemen weer beschikbaar en bereikbaar zijn. In dit voorbeeld wordt de doelstelling *niet* gehaald.



Om te kunnen voldoen aan een RPO van 12 uur en een RTO van 48 uur, worden onderstaande maatregelen getroffen.

Back-up virtuele servers

De back-up wordt binnen de kantoorautomatiseringsomgeving gedaan door Veeam. Elke dag worden er incrementele back-ups gemaakt van de complete virtuele omgeving. Elke week maakt Veeam een

Full back-up en er worden op de hoofdlocaties minimaal 1 full back-up bewaard. De back-ups worden op zondag naar tape weggeschreven.

Back-up fysieke servers

Van de fysieke servers wordt tijdens de groot-onderhouds-momenten een fysieke schijf (RAID-1) omgewisseld.

Back-up desktops en laptops

Van de desktops en laptops (zowel virtueel als fysiek) worden geen back-ups gemaakt omdat deze systemen snel opnieuw uit te rollen zijn; uitzondering hierop zijn de VM templates welke elke dag meegenomen worden tijdens de back-upcyclus.

Praktisch betekent dit dat de zakelijke systemen vlot terug te zetten zijn; maar alle data op een laptop is verloren. Het is verantwoordelijkheid van de gebruiker om zelf zorg te dragen voor haar persoonlijke data en bestanden. Zakelijke data en bestanden dienen de gebruikers altijd (ook) centraal op het netwerk opgeslagen worden. Bij implementatie van informatievoorzieningen (zoals het DMS) wordt zoveel als mogelijk er voor gezorgd dat deze synchronisatie automatisch verloopt.

2.3.4. Uitwijk

Om de omgevingen te kunnen uitwijken, zijn er op beide locaties voldoende resources beschikbaar om de totale omgeving op 1 locatie te kunnen draaien. In de praktijk worden beide locatiers actief ingezet. Deze configuratie brengt met zich mee dat de hele omgeving zo veel als mogelijk software-gedefinieerd is om eenvoudig te kunnen uitwijken mocht dat nodig zijn.

2.4. LAN infrastructuur

Met de LAN infrastructuur wordt de (netwerk-) apparatuur en systemen bedoeld die de werkplekken van de medewerkers koppelt aan de backend infrastructuur.

Zoveel als mogelijk zullen de werkplekken draadloos verbinding maken met het netwerk. Dit om de flexibiliteit te vergroten. Gasten kunnen via het wifi netwerk gebruik maken van de ter beschikking gestelde internetvoorzieningen.

Binnen de kantoorautomatiseringsomgeving wordt gebruik gemaakt van VLANs op een gerouteerd netwerk. Zoveel als mogelijk wordt aan servers, netwerkcomponenten etc. een vast IP-adres uitgedeeld.

2.5. Application delivery

Applicaties worden zoveel als mogelijk centraal aangeboden en beheerd, mits de applicatie hierop niet inboet aan functionaliteit én performance. De keuze hiervoor is eenvoud in beheer en een lagere total cost of ownership. Uitzondering hierop is het standaard Office (365) pakket dat lokaal op de laptops via Microsoft Intune wordt geïnstalleerd, zodat ook bij afwezigheid van een (internet-) verbinding nog bepaalde basisfunctionaliteit geboden wordt.

Centraal aangeboden en beheerde applicaties kunnen bijvoorbeeld worden aangeboden via een Virtual Desktop, Remote Desktop, Remote Application of Cloud Application. Hiertoe is een Digital Workspace opgezet.

De Digital Workspace is gebaseerd op een Horizon View Enterprise on-premises oplossing gecombineerd met diverse Workspace One Saas diensten. Het design voorziet in een zgn. Cloud Pod Architecture waarbij beide locaties actief worden ingezet. Voorzieningen om een calamiteit op te kunnen vangen zijn eveneens meegenomen in het design.

North Sea Port geeft de voorkeur aan web- of cloud-based applicaties. Traditionele client-applicaties (Windows 10) worden bij hoge uitzondering geaccepteerd, mits de nood ervan voldoende onderbouwd is en er geen alternatieven voorhanden zijn.

2.6. Authenticatie

North Sea Port synchroniseert haar Active Directory naar Microsoft Azure Active Directory. Zoveel als mogelijk dient authenticatie op basis van Single Sign On te gebeuren om het gebruikersgemak te verhogen. Aanmelden met aparte credentials dient voorkomen te worden.

Zodra een gebruiker toegang wil hebben tot onze systemen vanaf niet-vertrouwde locaties (off-premises), zal multi-factor authenticatie toegepast moeten worden.

2.7. Werkplekinrichting

De meeste medewerkers hebben een laptop en een mobiele telefoon tot zijn / haar beschikking gekregen. De laptops worden beheerd via het Microsoft Intune platform, gekoppeld aan de Azure Active Directory. Op de kantoorlocaties worden de bureaus voorzien van twee monitoren met een dockingstation om de laptop op aan te sluiten.

De medewerkers worden in staat gesteld ongeacht tijd, plaats en apparaat zijn / haar werkzaamheden te kunnen doen (Digital Workspace). Een internet verbinding dient dan wel voorhanden te zijn.

3. Aanvullingen

3.1. OTAP-procedure (on-premises)

Voordat producten of diensten in gebruik worden, dienen deze getest te worden. Van de OTAP-procedure (on-premises) worden de laatste twee stappen uitgevoerd op de kantoorautomatiseringsomgeving van North Sea Port. Hiertoe kan er (grotendeels) gebruik gemaakt worden van een Lab omgeving, welke een kopie-in-tijd is van de Productie omgeving. Nieuwe producten en diensten ondergaan dan ook de volgende stappen:

- Leverancier ontwikkelt op eigen omgeving;
- Leverancier vraagt de functioneel applicatiebeheerder toestemming om het op de Lab omgeving te zetten;
- De functioneel applicatiebeheerder vraagt om een LabSync of ServerSync (komt neer op een back-up/restore van de Prod omgeving naar de Lab omgeving);
- IT voert LabSync of ServerSync uit (doorlooptijd 2 dagen);
- Leverancier installeert op de Lab omgeving en maakt meteen een installatiehandleiding (alle handelingen tbv installatie en configuratie moeten hier in beschreven zijn);
- De functioneel applicatiebeheerder test;
- Leverancier lost problemen op en past indien nodig de installatiehandleiding aan;
- De functioneel applicatiebeheerder geeft akkoord voor “go-live”;
- IT voert wederom een LabSync of ServerSync uit (optioneel kan dit een revert-snapshot zijn);
- IT installeert op de Lab omgeving volgens installatiehandleiding, indien nodig wordt de handleiding aangepast door leverancier;
- De functioneel applicatiebeheerder voert een snelle controle uit;
- Indien zowel leverancier als functioneel applicatiebeheerder als ICT akkoord zijn, dan installeert IT op de Prod omgeving.

Mocht de Lab omgeving niet ingezet worden om de OTAP procedure geheel te doorlopen, dan dient vooraf een test-scenario uitgewerkt worden. Dit scenario dient de Prod omgeving niet te verstoren.

3.2. OTAP-procedure (cloud)

Om dingen te testen in de cloud dient de leverancier met een vergelijkbare oplossing te komen. Voor ontwikkelingen op Office 365 heeft North Sea Port een aparte 365 tenant ingericht (testnorthseaport.com). Deze test-omgeving wordt niet geback-upt en ook niet synchroon gehouden d.m.v. een back-up/restore procedure.

3.3. Onderhoudsmomenten

North Sea Port houdt primair 4 onderhoudsmomenten per jaar. Het gaat dan in principe om de 1^{e} weekenden van maart, juni, september en december. Op deze dagen is de kantoorautomatiseringsomgeving van North Sea Port niet beschikbaar. Op die dagen vinden o.a. de volgende werkzaamheden plaats:

- Firmware updates van servers, clients, netwerkcomponenten etc.;
- Microsoft updates;
- Back-ups fysieke servers;
- Restore naar Lab omgeving;

- Changes die bedrijfsbrede impact hebben;
- Etc..

Mocht er een zwaarwegende reden zijn om van deze momenten af te wijken, dan dient er een akkoord te zijn van het MT-lid welke verantwoordelijk is voor de betreffende change. De wijzigingen worden dan tijdens kantooruren doorgevoerd en dienen vooraf (indien mogelijk) de OTAP procedure doorlopen te hebben. In dit geval heeft het niet bereikbaar en beschikbaar zijn van de omgeving geen invloed op de uptime-berekening van de omgeving.

3.4. Remote toegangsprocedure

Leveranciers hebben normaliter geen toegang tot Productieomgevingen. Uitzondering hierop zijn productie verstorende issues welke de bedrijfsvoering zodanig hinderen dat het werken onmogelijk wordt gemaakt. In deze gevallen krijgt een leverancier toegang tot Productie via Teamviewer onder toezicht:

- Leverancier vraagt (via Jira) om toegang om een (in Jira) vastgelegd issue op te lossen;
- Joris, Peter, Patrick verifiëren bij de business of dit issue de bedrijfsvoering verstoort;
- Er wordt gezamenlijk een moment gepland om de werkzaamheden uit te voeren;
- IT logt in op betreffende server (of desktop) en start daar een Teamviewer QuickSupport sessie;
- Leverancier vult ID en password in op eigen PC om de server via Teamviewer over te nemen;
- Leverancier fixt het issue onder toezicht van IT;
- Sessie wordt verbroken;
- Leverancier beschrijft de fix (in Jira) zodat deze indien nodig ook uitgevoerd kan worden op Lab;
- Leverancier meldt business en IT dat issue opgelost is.