

Huidige situatie beschrijving



Inleiding

SWO De Wolden Hoogeveen heeft een cruciale rol in het aanbieden van diverse maatschappelijke diensten en voorzieningen aan haar inwoners. Om deze taken effectief uit te voeren en de lokale gemeenschap te ondersteunen, is een goed functionerende technische infrastructuur van essentieel belang.

De huidige situatie beschrijving van de technische infrastructuur van SWO De Wolden Hoogeveen is een cruciaal onderwerp dat aandacht verdient in het kader van de aanbestedingsprocedure. Het begrijpen van deze huidige situatie is van groot belang voor potentiële inschrijvers, omdat het hen in staat stelt om een goed doordacht voorstel te formuleren dat voldoet aan de specifieke behoeften en uitdagingen van SWO De Wolden Hoogeveen.

Inhoudsopgave

1	Housing.....	5
1.1	<i>Datcenter.....</i>	5
1.2	<i>Kantoor.....</i>	5
1.3	<i>Stroomvoorziening.....</i>	5
1.4	<i>Koeling.....</i>	6
1.5	<i>19" kasten.....</i>	6
2	Netwerk.....	7
2.1	<i>Beschrijving huidige netwerkcomponenten.....</i>	7
2.2	<i>Raadhuis Hoogeveen.....</i>	8
2.2.1	<i>Core.....</i>	8
2.2.2	<i>Werkplek.....</i>	8
2.3	<i>Compagniehuis Hoogeveen.....</i>	9
2.3.1	<i>Core.....</i>	9
2.3.2	<i>Werkplek.....</i>	9
2.4	<i>Werkplein Hoogeveen.....</i>	9
2.4.1	<i>Core.....</i>	9
2.4.2	<i>Werkplek.....</i>	9
2.5	<i>Gemeentehuis Zuidwolde – MER.....</i>	9
2.5.1	<i>Core.....</i>	9
2.5.2	<i>Uitwijk.....</i>	9
2.5.3	<i>Werkplek.....</i>	9
2.6	<i>Gemeentehuis Zuidwolde – SER.....</i>	10
2.6.1	<i>Werkplek.....</i>	10
2.7	<i>Zwembad de Dolfijn.....</i>	10
2.8	<i>Sporthal Het Activum.....</i>	10
2.8.1	<i>MER.....</i>	10
2.8.2	<i>SER.....</i>	10
2.9	<i>Milieustraat Zuidwolde en Werf.....</i>	10
2.10	<i>Werf Hoogeveen.....</i>	10
2.11	<i>Theather De Tamboer.....</i>	10
2.12	<i>Opsomming locaties.....</i>	11
3	Virtualisatie & Opslag.....	12
4	Digitale Werkplek.....	13
4.1	<i>Fysieke werkplek.....</i>	13
4.1.1	<i>Laptops.....</i>	13
4.1.2	<i>Thinclients.....</i>	13
4.1.3	<i>Desktops.....</i>	13
4.1.4	<i>Mobiele apparaten.....</i>	13
4.1.5	<i>Thuiswerkplek.....</i>	13

4.2	<i>Virtuele werkplek</i>	13
4.2.1	Remote Desktop Services	13
4.3	<i>Het applicatielandschap</i>	14
5	Beveiliging	15
5.1	<i>Informatie Beveiligingsbeleid</i>	15
5.2	<i>Identity Access Management</i>	16
5.2.1	Identiteiten	16
5.2.2	Fysieke toegang	16
5.2.3	Multifactor Authenticatie	16
5.3	<i>Zero Trust</i>	16
5.3.1	Segmentatie	16
5.3.2	IDS/IPS	17
5.3.3	Niet actief tenzij	17
6	Beheer	18
6.1	<i>Deployment</i>	18
6.2	<i>Management</i>	18
6.3	<i>Logging</i>	18
6.4	<i>Monitoring</i>	18
6.5	<i>Updates</i>	18
6.6	<i>Backup</i>	18
6.7	<i>OTAP cyclus</i>	19
6.8	<i>Beschrijving ICT-beheerorganisatie</i>	19

1 Housing

1.1 Datacenter

De infrastructuur van de SWO De Wolden Hoozeveen (hierna SWO) is in 2 datacenters opgebouwd. De datacenters zijn gesitueerd in Hoozeveen en Zuidwolve. De afstand tussen de datacenters is +/- 8 kilometer.

Datacentra (MER)	<u>Raadhuis Hoozeveen</u> Raadhuisplein 1 7901 BP Hoozeveen
	<u>Gemeentehuis De Wolden</u> Raadhuisstraat 2 7921 GD Zuidwolve

Tabel 1

1.2 Kantoor

De medewerkers van de SWO werken verdeeld over diverse locaties, waarbij gebruik wordt gemaakt van flexwerken. De volgende locaties zijn in scope voor deze aanbesteding:

Kantoor (SER)	<u>Raadhuis Hoozeveen</u> Raadhuisplein 1 7901 BP Hoozeveen	<u>Werkplein Hoozeveen</u> Dekkerplein 1 7901 BZ Hoozeveen
	<u>Compagnieshuis</u> Raadhuisplein 24 7901 BW Hoozeveen	<u>Werf Hoozeveen</u> De Vos van Steenwijklaan 75a 7902 NP Hoozeveen
	<u>Sporthal Het Activum</u> Sportveldenweg 2, 7902 NX Hoozeveen	<u>Gemeentehuis De Wolden</u> Raadhuisstraat 2 7921 GD Zuidwolve
	<u>Zwembad de Dolfijn</u> Bentincksdijk 10 7902 NA Hoozeveen	<u>Mileustraat en Werf Zuidwolve</u> Slagendijk 11 7921 TH Zuidwolve
	<u>Theater Tamboer</u> Hoofdstraat 17 7902 EA Hoozeveen	

Tabel 2

1.3 Stroomvoorziening

Alle ICT-ruimtes zijn voorzien van een UPS met een autonomietijd van 30 minuten. Op het moment van schrijven is er een overcapaciteit.

In de locatie Raadhuis Hoozeveen en Gemeentehuis Zuidwolve is er ook een NSA aanwezig. Doorgaans neemt deze ruim binnen een minuut de stroomvoorziening over bij een stroomstoring. De ICT-ruimte van het Compagnieshuis Hoozeveen wordt ook gevoed door de NSA die geïnstalleerd is in locatie Raadhuis Hoozeveen. Op deze wijze kan er een hoge beschikbaarheid worden gerealiseerd voor de toegang tot ons netwerk.

1.4 Koeling

De ruimtes worden gekoeld door airco's specifiek voor deze ruimtes.

De airco in de MER van het Raadhuis is uitgevoerd met een dubbele unit voor hoge beschikbaarheid. Dat geldt niet voor de kast waar de switches zijn geplaatst, die wordt door een enkele airco gekoeld.

1.5 19" kasten

Binnen de datacenters zijn verschillende merken patchkasten geplaatst van onder andere Rittal en Minkels.

NB. Vrije rackspace is gedurende de transitie naar de nieuwe netwerkinfrastructuur in beide datacenters goed beschikbaar.

2 Netwerk

2.1 Beschrijving huidige netwerkcomponenten

De SWO maakt gebruik van een gesegmenteerd IP-netwerk.

Er worden switches van het merk HP gebruikt om de netwerkcomponenten aan te sluiten.

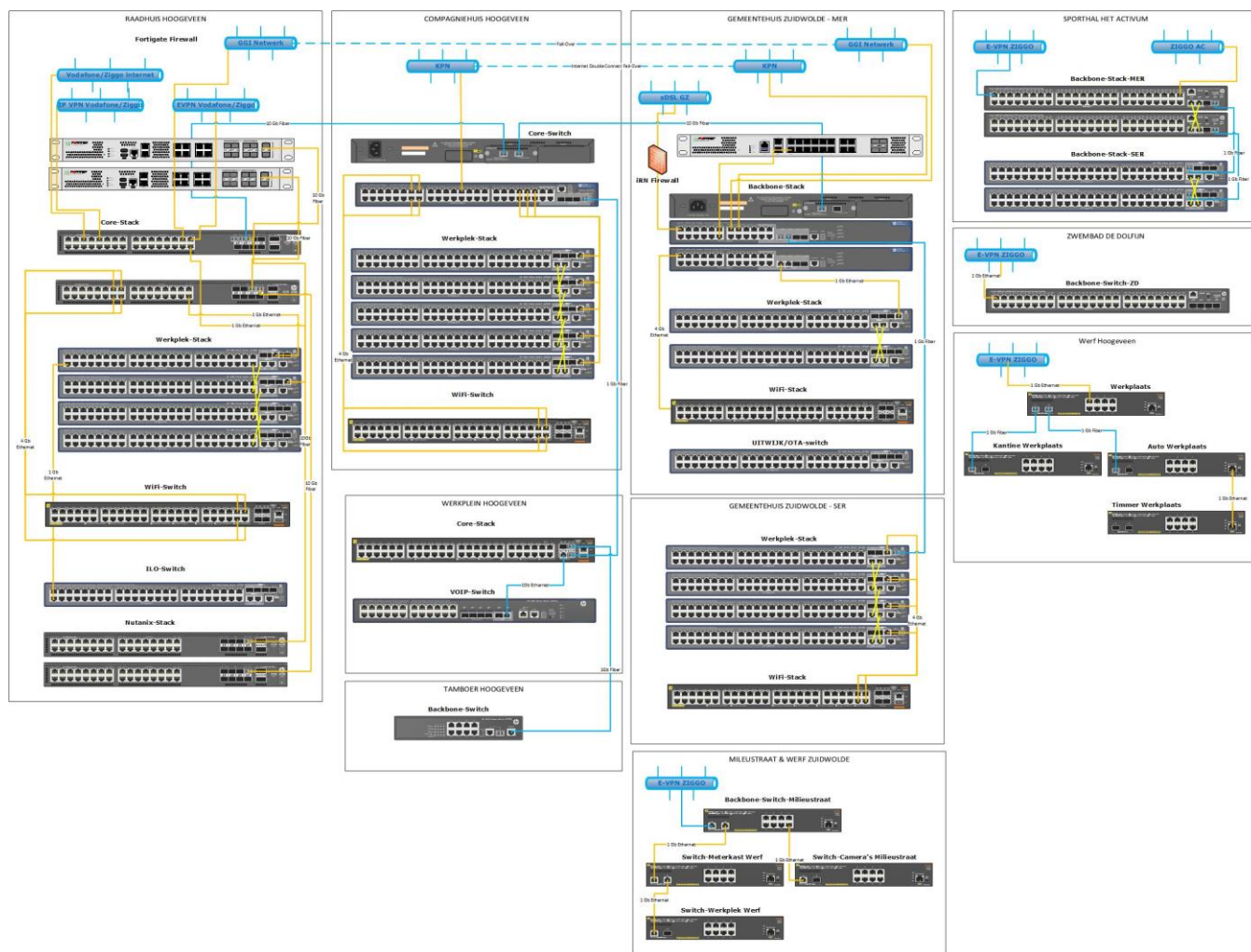
Het Raadhuis Hoogeveen is op basis van glasvezel met 10 Gb snelheid verbonden met het Compagnieshuis. Vanuit het Compagnieshuis is er een glasvezelverbinding (dark fiber) met 10 Gb snelheid naar het Gemeentehuis Zuidwolde en een glasvezelverbinding met 1 Gb snelheid naar het Werkplein. Technieken zoals CWDM en DWDM (met encryptie) worden niet toegepast.

De overige kleine(re) locaties zijn op diverse manieren op ons netwerk aangesloten via (e)VPN verbindingen en maken op die manier onderdeel uit van het netwerk. Enkele buitenlocaties hebben alleen een internetverbinding.

Met betrekking tot WiFi wordt er gebruik gemaakt van Aerohive Access Points. Hierop worden verschillende netwerken aangeboden voor verschillende doelgroepen:

- Medewerkers
- Gasten
- Gasten – sporthal Het Activum

Nb: Op de tekening (zie figuur 1) is te zien dat op sommige locaties aparte WiFi switches waarop de access points zijn aangesloten. Op andere locaties waar nog niet is voorzien van aparte WiFi switches zijn de access points op de werkplekswitches aangesloten. Op het moment van spreken vindt er een actie plaats waarbij op alle locaties voorzien worden van separate WiFi switches.



Figuur 1

2.2 Raadhuis Hoogeveen

2.2.1 Core

In het Raadhuis Hoogeveen bevindt zich het primaire datacenter. In het datacenter bevindt zich een Nutanix cluster met een daar bijhorende cluster van 2 HPE FlexFabric 5700 switches. Deze switches worden niet meegenomen in deze aanbesteding, omdat deze gemanaged worden door de leverancier van de dataopslag.

In de MER bevinden zich de switches waarbij er een stack van 2 HPE FlexFabric 5700 switches zijn. Er worden nu circa 50 10 Gb poorten gebruikt voor het koppelen van de servers en netwerkapparatuur.

Er loopt vanaf de core een 10 Gb fiber verbinding naar de Core in het Compagniehuus.

De IP VPN en EVPN verbindingen worden vanaf deze locatie opgebouwd naar alle sublocaties die op basis van deze techniek zijn aangesloten. En daarnaast de verbinding richting de Gemeentelijke Gemeenschappelijke Infrastructuur (het GGI Network).

2.2.2 Werkplek

Daarnaast hebben we een werkplek cluster van 4 HP A3600 switches waarop diverse apparatuur op ontsloten wordt. Dat zijn onder andere werkplekken, printer, AudioVisuele apparaten, telefoons, etc.

De 33 Access Points in dit gebouw zijn aangesloten op één switch van het type HPE Aruba 6200F.

In het datacenter staat nog één switch voor het aansluiten van managementpoorten van de daar aanwezige hardware.

Het totaal aantal benodigde poorten op het moment van schrijven is 190 poorten.

2.3 Compagniehuis Hoogeveen

2.3.1 Core

Op deze locatie bevindt zich een core switch welke deze locatie koppelt met verschillende locaties (Raadhuis Hoogeveen, Gemeentehuis Zuidwolde, Werkplein Hoogeveen). Het gaat hier om een HP A5120 switch. Op deze switch zijn op het moment van schrijven 28 poorten in gebruik

2.3.2 Werkplek

Daarnaast is er een stack van 5 HP A3600 switches waarop diverse apparatuur op ontsloten wordt. Dat zijn onder andere werkplekken, printer, AudioVisuele apparaten, telefoons, Access Points, etc.

Er zijn in deze locatie 37 Access Points in gebruik die op een HPE Aruba 6200F zijn aangesloten.

Het totaal aantal benodigde poorten op het moment van schrijven is 160 poorten.

2.4 Werkplein Hoogeveen

2.4.1 Core

Op deze locatie bevindt zich een core switch welke deze locatie koppelt met verschillende locaties. Het gaat hier om een HPE Aruba 6200F switch. Op deze switch zijn op het moment van schrijven 23 poorten in gebruik.

2.4.2 Werkplek

De 13 Access Points in dit gebouw zijn aangesloten op de core switch aangesloten.

Daarnaast is er een H3C S5500 switch waarop diverse apparatuur op ontsloten wordt. Dat zijn onder andere werkplekken, printer, AudioVisuele apparaten, telefoons, Access Points, etc.

Het totaal aantal benodigde poorten op het moment van schrijven is 10 poorten.

2.5 Gemeentehuis Zuidwolde – MER

2.5.1 Core

Op deze locatie bevindt zich een stack van 2 HP A5120 switches. Op deze stack zijn op het moment van schrijven 30 poorten in gebruik.

Daarnaast bevindt zich in deze locatie de secundaire datacenter. In geval van een calamiteit, moet er uitgeweken kunnen worden naar deze locatie. Hier staat dan ook een Nutanix cluster met een stack van 2 HPE FlexFabric 5700 switches die worden beheerd door de leverancier van de dataopslag.

2.5.2 Uitwijk

Voor het ontsluiten en koppelen van de Uitwijk omgeving staat er één HP A5120 switch die zorgt voor de interne koppelingen van de uitwijk componenten. Deze switch heeft geen directe koppeling met ons netwerk, maar is voorbereid om tijdens een calamiteit ingezet te worden.

Tijdens de OTA cycli wordt de switch wel actief ingezet, maar niet voor productie doeleinden.

Het totaal aantal benodigde poorten voor deze switch zijn 30 poorten.

2.5.3 Werkplek

Daarnaast is er een stack van 2 HP A3600 switches waarop diverse apparatuur op ontsloten wordt. Dat zijn onder andere werkplekken, printer, AudioVisuele apparaten, telefoons, etc.

De 20 Access Points in dit gebouw zijn aangesloten op één switch van het type HPE Aruba 6200F.

Het totaal aantal benodigde poorten op het moment van schrijven is 60 poorten

2.6 Gemeentehuis Zuidwolde – SER

2.6.1 Werkplek

In de SER is een stack van 4 HP A3600 switches waarop diverse apparatuur op ontsloten wordt. Dat zijn onder andere werkplekken, printer, AudioVisuele apparaten, telefoons, Access Points, etc.

Er zijn in deze locatie 16 Access Points in gebruik welke op een HPE Aruba 6200F zijn aangesloten.

Het totaal aantal benodigde poorten op het moment van schrijven is 95 poorten

2.7 Zwembad de Dolfijn

Deze locatie is met E-VPN aangesloten op ons netwerk. Er staat één switch van het type HP A5130.

Er zijn in deze locatie 5 Access Points in gebruik.

Het totaal aantal benodigde poorten op het moment van schrijven is 38 poorten.

2.8 Sporthal Het Activum

2.8.1 MER

Deze locatie is met E-VPN aangesloten op ons netwerk.

In de MER staat een stack van 2 switches van het type HP A5130. In de MER zijn 9 Access Points aangesloten en een totaal van 48 poorten in gebruik.

2.8.2 SER

In de SER staat een stack van 2 switches van het type HP A3600. In de SER zijn 7 Access Points aangesloten en een totaal van 30 poorten in gebruik.

2.9 Milieustraat Zuidwolde en Werf Zuidwolde

Deze locatie is met E-VPN aangesloten op ons netwerk. Er staan 2 switches van het type Aruba 1930, waarvop één 6 camera's is aangesloten.

Het totaal aantal benodigde poorten op het moment van schrijven is 14 poorten

De werf (staat op hetzelfde perceel) is via de locatie de milieustraat verbonden met ons netwerk. Op deze locatie staan ook twee Aruba 1930 switches met een totaal aantal poorten van 16.

Daarvan zijn er in de Werf 4 Access Points

2.10 Werf Hoogeveen

Deze locatie is met E-VPN aangesloten op ons netwerk. De verschillende gebouwen zijn met switches van het type Aruba 1930 met elkaar verbonden. Deze locatie wordt op het moment van schrijven ingericht en zal ongeveer 32 poorten in totaal in gebruik nemen, waarvan 5 Access Points.

2.11 Theater De Tamboer

Deze locatie is gekoppeld aan de switch van het Werkplein. Er zijn 8 poorten in gebruik. Er staat een H3C S3100 switch.

2.12 Opsomming locaties

In de onderstaande tabel staan de actuele aantallen van aangesloten poorten per type switch in een totaaloverzicht opgesomd.

Locatie	Poorten Core	Poorten werkplek	Access Points	Verwachte groei
Raadhuis Hoogeveen	50	190	33	Geen
Compagniehuis Hoogeveen	28	160	37	Ja, beperkt op de werkplek
Werkplein Hoogeveen	23	10	-	Geen
Gemeentehuis Zuidwolde - MER	30	60	20	Ja, beperkt op de werkplek
Gemeentehuis Zuidwolde - MER - Uitwijk	30	-	-	Geen
Gemeentehuis Zuidwolde - SER	-	95	16	Geen
Zwembad de Dolfijn	10	24	5	Geen
Sporthal Het Activum - MER	24	48	9	Geen
Sporthal Het Activum - SER	-	30	7	Geen
Milieustraat Zuidwolde	8	6	-	Geen
Werf Zuidwolde	4	8	4	Geen
Werf Hoogeveen	4	24	4	Geen
Theater De Tamboer	4	4	-	Geen
Totalen	221	671	149	

Tabel 3

3 Virtualisatie & Opslag

De SWO maakt gebruik van een Hyperconverged Nutanix cluster waarop virtuele servers gehost worden met behulp van de Nutanix Acropolis Hypervisor.

Naast de primaire cluster in het Raadhuis in Hoogeveen is er ook een secundaire cluster in het gemeentehuis Zuidwolde. Alle servers worden eens in de 90 dagen naar deze locatie gerepliceerd. Dat wil zeggen dat de VMs worden verwijderd en via de reguliere backup (Commvault) worden de productie VM's teruggezet.

Voor de database platformen zijn er twee VMware ESXi servers waarop Oracle en MS SQL Server databases worden aangeboden. Voor productie wordt hiervoor een Dell PowerEdge R640 met local storage gebruikt, welke is aangesloten op de coreswitch in het Raadhuis. Voor uitwijk betreft dit een Dell PowerEdge R740 met local storage, welke is aangesloten op de coreswitch in het gemeentehuis.

Door middel van VLAN-tagging worden de virtuele servers in verschillende netwerksegmenten geplaatst, waarbij de communicatie naar andere servers moet worden geconfigureerd in de lokale firewall én de centrale Fortigate Cluster.

4 Digitale Werkplek

4.1 Fysieke werkplek

De werkzaamheden worden op laptops (standaard werkplek) en op enkele zware (grafische) desktop pc's van de medewerkers uitgevoerd. Alle clients zijn gebaseerd op Windows 10.

Het grootste deel van medewerkers heeft een laptop en smartphone tot zijn of haar beschikking. Er zijn buiten de laptops ook nog een aantal desktops en thinclients in omloop.

4.1.1 Laptops

Er zijn ongeveer 900 laptops in gebruik binnen de organisatie. Deze medewerkers kunnen de standaard kantoorautomatiseringssoftware gebruiken op deze laptops. Deze laptops werken allemaal via Wifi en hebben toegang tot het netwerk.

De SWO is bezig met het zoveel mogelijk standaardiseren op laptopgebruik. Hierdoor zal het aantal zware werkplekken af gaan nemen en het aantal mobiele apparaten (laptops) zal hierdoor verder gaan stijgen. Minimale bandbreedte voor WiFi voor een laptop is gesteld op 1Gbit.

4.1.2 Thinclients

Er zijn een 60-tal thinclients/minidesktops in gebruik. Deze worden alleen gebruikt voor de Citrix VDI oplossing. Minimale bandbreedte bekabeld voor een thinclient is gesteld op 1Gbit

4.1.3 Desktops

Er wordt gebruik gemaakt van ongeveer 25 zware werkplekken die veelal ingezet worden bij applicatiebeheerders en bij medewerkers die gebruik maken van applicaties die hoge eisen stellen aan lokale resources. Minimale bandbreedte bekabeld voor een desktop is gesteld op 1Gbit

4.1.4 Mobiele apparaten

Er zijn meer dan 1000 mobiele telefoons in gebruik binnen de organisatie. Medewerkers maken hoofdzakelijk gebruik van Samsung of Apple toestellen. Medewerkers mogen zelf bepalen welk type zij willen gebruiken. Leidinggevend en raadsleden hebben nog de mogelijkheid om een iPad te gebruiken. Het beheer en onderhoud van deze apparaten vindt met behulp van MS Intune plaats.

4.1.5 Thuiswerkplek

De medewerkers werken ook veelal vanuit huis. Alle medewerkers hebben de beschikking over een laptop die wordt uitgegeven en beheerd door de SWO. De medewerker kan gebruik maken van zijn internetverbinding thuis en dan middels een VPN-verbinding toegang verkrijgen tot het netwerk van de SWO.

4.2 Virtuele werkplek

Medewerkers kunnen kiezen om lokaal op de laptop of desktop te werken of een verbinding te maken met de Citrix VDI omgeving. In de praktijk wordt Citrix VDI omgeving vooral voor Taak Specifieke Applicaties (TSA) gebruikt. Voor de standaard kantoorautomatisering applicaties (MS office enz.) vindt er steeds meer een verschuiving naar het lokaal werken op de laptop of desktop plaats.

4.2.1 Remote Desktop Services

De SWO maakt gebruik van een Citrix Virtual Desktop omgeving waar ongeveer 75 procent van de medewerkers op werkt. De Citrix Virtual Desktop omgeving bestaat uit 10 Dell PowerEdge R740 servers met Citrix Hypervisor. De Citrix VDI omgeving wordt mede vorm gegeven met behulp van Citrix Provisioning Server. In totaal zijn 10 Citrix Hypervisors in de infrastructuur gepositioneerd die elk 60 virtual desktops hosten.

4.3 Het applicatielandschap

Op de werkplekken van de SWO staat Office 365, exclusief Onedrive en Sharepoint geïnstalleerd. In de toekomst wordt gekeken of Onedrive en Sharepoint binnen het applicatielandschap kan worden opgenomen.

Verder zijn er ongeveer 150 applicaties binnen de organisatie in gebruik, waaronder de volgende grote/organisatie breed toegepaste applicaties:

- Decos Join (Zaaksysteem)
- SAP (leverancier PinkRoccade t.b.v. Financiën & Belastingen) welke gaat bewegen richting een cloudoplossing.
- Afas (HRM cloud)
- iBurgerzaken (Cloud)
- Civision Samenlevingszaken (Sociaal Domein) welke gaat bewegen richting een cloudoplossing.
- Squit 20/20 (Vergunningverlening cloud toepassing)
- Neuron (BAG/BGT)

5 Beveiliging

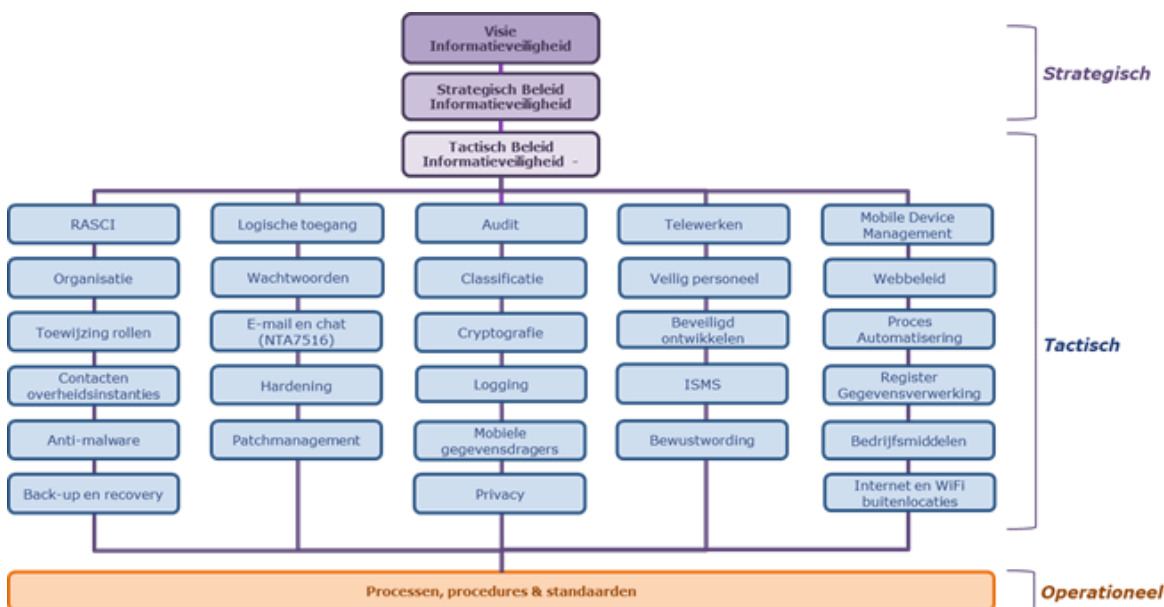
5.1 Informatie Beveiligingsbeleid

Ten aanzien van Informatieveiligheid geldt dat het Colleges van B&W van de gemeenten Hoogeveen en De Wolden (politiek) eindverantwoordelijk is voor een juiste omgang met gegevens door de organisatie. Vanuit die verantwoordelijkheid heeft het College van B&W het Strategisch Beleid Informatieveiligheid vastgesteld. Het Strategisch Beleid Informatieveiligheid beschrijft met name welke wet- en regelgeving van toepassing is, hoe de verantwoordelijkheden zijn belegd, welke processen er zijn voor de borging en hoe de organisatie rondom informatieveiligheid en privacy geregeld is.

De implementatie en borging van informatieveiligheid en de Baseline Informatiebeveiliging Overheid (hierna: BIO) is belegd bij de directie van de SWO. De directie is (ambtelijk) verantwoordelijk voor de correcte implementatie en uitvoering van informatieveiligheid en de BIO. Door middel van het Tactische Beleid Informatieveiligheid geeft de directie de kaders aan die binnen de gemeentelijke organisatie gelden ten aanzien van informatieveiligheid.

Samen met het Strategisch Beleid Informatieveiligheid vormen het Tactische Beleid Informatieveiligheid het fundament voor de informatiebeveiliging van de organisatie. De BIO staat centraal in het beleid. Gemeenten baseren hun beleid op informatieveiligheid en hun verantwoording aan de gemeenteraad en de toezichthouders vanuit het Rijk (met de zelfevaluatie Eenduidige Normatiek Single Information Audit (ENSIA)) op de BIO.

Een overzicht van de beleidsstukken op het gebied van informatieveiligheid & privacy:



Figuur 2

5.2 Identity Access Management

Onderstaand wordt een invulling gegeven hoe binnen SWO wordt omgegaan met gebruikersidentiteiten, hun authenticatie (verificatie van identiteit), autorisatie (toegangsrechten en bevoegdheden) en het beheer van deze rechten gedurende de hele levenscyclus van een gebruiker binnen een organisatie.

Dit helpt bij het waarborgen van beveiliging, het minimaliseren van risico's en het naleven van regelgeving, aangezien het zorgt voor een gecontroleerde en veilige toegang tot gevoelige informatie en systemen.

5.2.1 Identiteiten

De SWO maakt gebruik van een tool om geautomatiseerd gebruikersbeheer uit te voeren. Indien een medewerker in- of uitdienst wordt geregistreerd in de personeelsadministratie, dan wordt (geautomatiseerd) een gebruikersaccount voor deze medewerker aangemaakt of verwijderd. Het betreft het volgende:

- Gebruikersaccount
- Standaard autorisaties
- Toegangsdruppel voor toegang tot de gebouwen, het gebruik van afdrukapparatuur en poolauto's
- Telefoonnummer
- Email postbus
- Taak specifieke autorisaties

5.2.2 Fysieke toegang

Via een fysiek gescheiden netwerkinfrastructuur maakt de SWO gebruik van toegangsdruppels om de toegang tot de gebouwen te verlenen. Deze druppels worden echter voor meerdere doeleinden gebruikt. De toegangsdruppels worden onder andere ook gebruikt voor het kunnen starten van de poolauto's en het kunnen vrijgeven van de printfunctionaliteit in de gemeentelijke hoofdgebouwen.

5.2.3 Multifactor Authenticatie

De smartphones maken met behulp van de app Microsoft Authenticator een essentieel onderdeel uit van onze aanmelding. Tijdens aanmelden op zowel laptop als zware werkplek wordt er een VPN opgebouwd naar de Fortigate cluster, waarbij er een MFA challenge wordt gevraagd.

5.3 Zero Trust

Zero Trust is een beveiligingsconcept gebaseerd op het principe dat organisaties niet automatisch vertrouwen moeten verlenen, ongeacht of de toegangspoging intern of extern is. In plaats daarvan moet elke poging tot toegang tot het systeem geverifieerd, geautoriseerd en continu gemonitord worden op integriteit en veiligheid. De SWO werkt toe naar een ICT-landschap waarin het zero trust principe volledig wordt toegepast. Dit betekent voor nieuwe toepassingen of vervanging van huidige systemen dat dit principe wordt gehanteerd.

5.3.1 Segmentatie

Onder Zero Trust verstaat de SWO het volgende: Met behulp van VLANs vindt netwerksegmentatie plaats ten behoeve van de verschillende systemen. Denk hierbij aan fysieke en virtuele servers, printers, workstations, thin clients, ed. Microsegmentatie wordt nog niet toegepast, maar zal mogelijk in de toekomst een rol spelen.

De medewerkers hebben een eigen segment, waar er alleen toegang is tot het internet. De medewerkers moeten vanuit dit segment vanaf hun mobiele apparaat toegang tot het netwerk verschaffen via een VPN.

Het netwerk voor gasten is een openbaar netwerk. Dit netwerk heeft ook zijn eigen internet breakout en is dus daarin ook volledig gescheiden van het netwerk van de medewerkers. De gasten moeten wel akkoord gaan met

voorwaarden voordat er toegang verleend wordt tot het internet en het verkeer wordt via de Fortgate firewall gefilterd.

5.3.2 IDS/IPS

Tussen de verschillende segmenten wordt het verkeer met behulp van de Fortigate cluster gescand middels Intrusion Prevention en Application Control.

Daarnaast wordt al het verkeer via een Port Mirror Group verstuurd naar de Intrusion Detection System “Cyberalarm” van SecureMe2 voor analyse op verdacht verkeer.

5.3.3 Niet actief tenzij

Toegang tussen de verschillende systemen en netwerken worden specifiek in de Fortigate geconfigureerd. De minimaal benodigde poorten worden opengezet voor communicatie.

6 Beheer

6.1 Deployment

De switches worden handmatig voorzien van de juiste firmware-versie. De access points daarentegen worden centraal voorzien. Zie ook hoofdstuk 6.5.

6.2 Management

Er wordt geen centrale management tool gebruikt voor het beheer van de switches. Voor configuratiewijzigingen wordt rechtstreeks op de betreffende switch ingelogd via SSH of HTTP(S). Lukt dit niet dan wordt een laptop via de console-poort gekoppeld.

Er is binnen de SWO infrastructuur geen out-of-band netwerk geïmplementeerd. Bij onbeschikbaarheid van het netwerk wordt een laptop fysiek via de console-poort gekoppeld.

De Access Points worden daarentegen allemaal centraal beheerd vanuit een appliance die het datacenter staat. Inmiddels vindt er een beweging richting een beheeroplossing in de cloud.

6.3 Logging

Er is geen centraal log-platform waarop de logdata van de infrastructuur en applicaties worden bewaard. Als er logging plaatsvindt, dan wordt dit op de device/VM zelf bewaard.

6.4 Monitoring

Zabbix wordt gebruikt voor monitoring en alerting van de operationele kant van de ICT infrastructuur.

MyCyberAlarm van SecureMe2 wordt gebruikt om security issues te detecteren in de ICT infrastructuur.

6.5 Updates

Handmatig worden de upgrades/updates op de switches uitgevoerd. De access points worden daarentegen via centraal beheeroplossing voorzien van de benodigde updates.

Lifecycle management

- Upgrades worden eerst getest in een Testomgeving
- Security fixes worden op basis van de CVSS score geprioriteerd. Waarbij een score van 9 of hoger dezelfde dag nog geïmplementeerd dient te worden
- Regulier onderhoud dient minimaal eens per half jaar uitgevoerd te worden, of eerder indien er sprake is van een security fix (CVE)

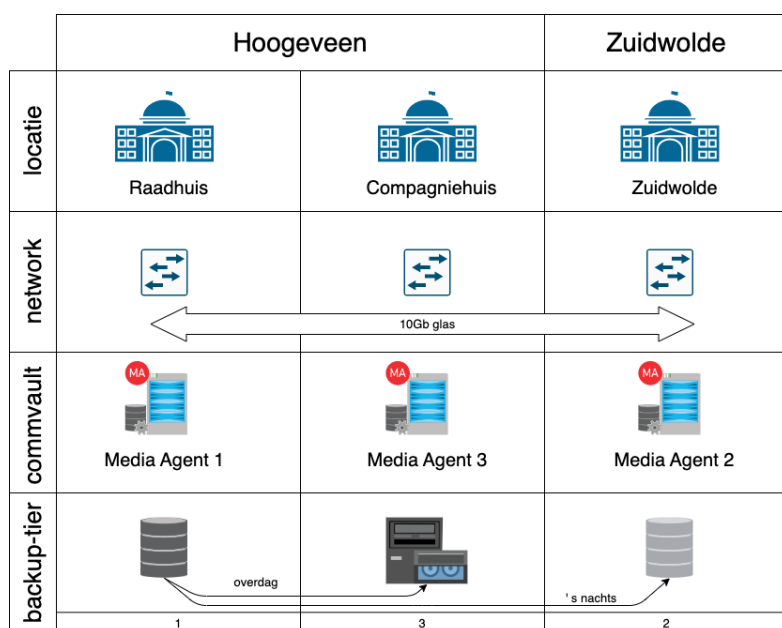
Bovenstaand releasebeleid geldt voor alle apparatuur en programmatuur dat door de SWO in gebruik is.

6.6 Backup

De SWO maakt gebruik van de backupoplossing van Commvault. Er worden minimaal 3 exemplaren van een backup opgeslagen. Eén on-site (tier 1), één off-site (tier 2) en een offline backup (tier 3). De backups worden via VSA (Virtual Server Agent) gemaakt (= hypervisor mediated, lees image backups).

De configuraties van de netwerkinfrastructuur geëxporteerd naar een tekstbestand, welke op de fileservers worden bewaard. Deze fileservers worden vervolgens in de reguliere backup meegenomen.

Bijgevoegd een schema van de backup architectuur. De Media Agents zijn op de coreswitches van de betreffende locaties aangesloten.



Figuur 3

6.7 OTAP cyclus

De SWO maakt gebruik van een 9-wekelijkse OTAP-cyclus waarin updates, ontwikkelingen en projecten volledig getest kunnen worden alvorens deze binnen het productienetwerk geïmplementeerd worden.

In deze omgeving zijn alle virtuele servers beschikbaar voor het testen van de applicaties. De omgeving is een vrijwel 100% identieke afspiegeling van de on-premise productie-omgeving.

De OTAP-omgeving wordt gehost in de uitwijklocatie in het gemeentehuis Zuidwolde en kan met behulp van een portaal door de gebruikers benaderd worden.

Doordat de SWO gebruik maakt van een volledig gevirtualiseerde omgeving, biedt dit de mogelijkheid om snel en eenvoudig een OTAP-omgeving op te bouwen.

Het opbouwen van een OTAP-omgeving wordt in deze uitwijklocatie gerealiseerd door de virtuele servers te starten op de uitwijk hardware zoals deze geplaatst is in de uitwijk omgeving. Middels een portaal wordt een Citrix VDI desktop aangeboden waarmee de eindgebruiker zich kan aanmelden op de OTAP-omgeving. Dit resulteert in een OTAP-omgeving waarbij alle servernamen en ip-reeksen en dus ook de servers identiek blijven aan de productie-omgeving. Op deze manier kan realistisch getest worden.

Een uitzondering hierop is de netwerkinfrastructuur. Hiervoor is geen OTAP cyclus ingericht. Vooraf dient te worden verklaard met welke reden en hoe de upgrades worden toegepast. Daarnaast dient een fallback procedure te worden overlegd mocht een upgrade/update niet succesvol zijn.

6.8 Beschrijving ICT-beheerorganisatie

Afdeling automatisering bestaat uit ongeveer 18 FTE. Binnen de afdeling zijn de volgende functies werkzaam:

- Teamleider
- Medewerker servicedesk
- Medewerker ICT tweede lijn
- Medewerker ICT derde lijn

Meldingen worden aangenomen door onze Servicedesk. Indien meldingen niet direct opgelost kunnen worden door onze Servicedesk, worden deze in behandeling genomen door medewerkers tweede of derde lijn. Onze IT Proces specialist beschrijft, verbetert en controleert proces afspraken die wij binnen het team automatisering hebben gemaakt.

De applicatiebeheerders, Coördinator Informatieveiligheid en onze CIO/CISO maken geen deel uit van de afdeling automatisering. Wel is er regelmatig contact met deze specialismen waaronder ook bij implementatie van nieuwe producten/diensten of bij de vervanging hiervan.