Afstudeer Scriptie

Hogeschool Utrecht

Jaap Groeneveld

Colofon

Titel	Afstudeer Scriptie
Opgesteld door	Dhr J.A. Groeneveld
Datum	01-06-2007
Documentnaam	HU_Scriptie_JA_Groeneveld_v1.0
Onderwerp	Afstudeer Scriptie

Contactpersonen

Naam	**Organisatie**
Dhr. J.A. Groeneveld	Student
Dhr. B. Buitenhuis	Docentbegeleider
Dhr. P.H. Klijs	Bedrijfsbegeleider

Revisies

Versie	**Datum**	**Omschrijving**
0.1	21-02-2007	Initiële versie
0.2	02-03-2007	Aangepaste versie
0.3	14-03-2007	Aangepaste versie
0.4	22-05-2007	Aangepaste versie
1.0	01-06-2007	Aangepaste versie

1 Voorwoord

Deze scriptie is geschreven door Jaap Groeneveld, in opdracht van de Hogeschool Utrecht faculteit techniek richting informatica (Systeembeheer) te Utrecht. Deze opleiding is gevolgd in duale vorm.

Na het volgen van deze 3-jarige opleiding is de laatste fase het schrijven van een scriptie. In de hierna volgende managementsamenvatting zal het onderwerp verder worden toegelicht.

Dit werkstuk heb ik intensief en met plezier uitgewerkt. In samenspraak met mijn begeleiders is er een keuze gemaakt in het afstudeeronderwerp en uiteindelijk in de uitwerking.
Zij hebben voldoende ondersteuning gegeven op zowel inhoud als tekstuele vraagstukken.

Ondersteuning is allereerst geboden door mijn docent van de Hogeschool Utrecht,
Dhr. B. Buitenhuis. Vanaf de start van deze opleiding heb ik van dhr. Buitenhuis lessen mogen volgen. Deze lessen waren dankzij zijn praktische voorbeelden altijd goed te vertalen in bruikbare informatie.
Mijn tweede begeleider is mijn direct leidinggevende dhr. Pieter Klijs. Pieter is sinds ik ben gestart met deze opleiding mijn leidinggevende. De samenwerking met Pieter verloopt altijd zeer prettig.

Wellseind, juni 2007
Jaap Groeneveld

2 Managementsamenvatting

Het centrale vraagstuk binnen deze scriptie zal gaan over de vervanging van een ZIS infrastructuur (Ziekenhuis Informatie Systeem). De keuze voor dit onderwerp ligt gedeeltelijk voor de hand. VCD Automatisering heeft een focus op de gezondheidszorg, waar dergelijke producten uitgevoerd worden.

Als project is gekozen voor Ziekenhuis Bernhoven (ZB). Voor ZB dient een totaaloplossing te worden geboden om het totale ZIS proces op hardware matige basis te kunnen faciliteren. Om te komen tot een passende oplossing is allereerst gekeken naar de wensen/eisen van ZB. Deze hebben betrekking op de organisatie, applicatie en gebruikers. Na analyse van deze gegevens is er een passend ontwerp gemaakt. Het uiteindelijke ontwerp heet betrekking op:

- Centrale data opslag;
- High availability;
- Backup en restore;
- Ontsluiten via het internet;
- Beveiliging van patiëntgegevens.

Inhoudsopgave

3 De opdrachtgever en de klant

3.1 VCD Automatisering

VCD Automatisering heeft zich in haar bijna 30-jarig bestaan ontwikkeld tot een van de grotere zelfstandige ICT-ondernemingen in Nederland. Een innovatief bedrijf dat staat voor realisme en continuïteit. Met ruim 200 professionals is VCD landelijk actief voor klanten van formaat. VCD heeft vestigingen in Groningen (hoofdkantoor), Amsterdam en Eindhoven.

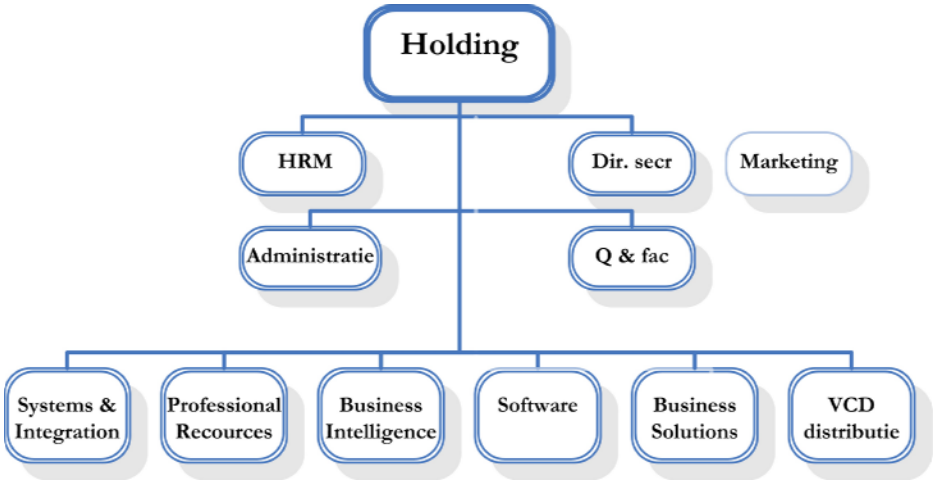
Kenmerken
VCD kan gekenmerkt worden als een no-nonsense, rationele en professionele organisatie waarbij het ondernemerschap hoog in het vaandel staat. De VCD medewerkers zijn over het algemeen ietwat bescheiden, beschikken over veel specialistische kennis en hebben een grote werkethiek. VCD is innovatief in die zin dat het continu nieuwe ontwikkelingen signaleert en niet bang is om deze op te pakken. Wel wordt er altijd gewerkt vanuit een pragmatisch oogpunt; nut en bruikbaarheid, betrouwbaarheid en stabiliteit zijn belangrijke pijlers binnen onze oplossingen. VCD streeft daarnaast voortdurend naar langdurige en intensieve samenwerking met haar klanten.

One-stop-shopping
Vanuit het one-stop-shopping concept levert VCD infrastructuur, standaard- en maatwerksoftware en business intelligence oplossingen. Ook verzorgt VCD de volledige dienstverlening (consultancy, detachering, beheer en support) omtrent bovengenoemde oplossingen. VCD focust zich op de branches groothandel en retail, gezondheidszorg, transport, zakelijke en financiële dienstverlening en non-profit instellingen.

Allianties
VCD heeft strategische allianties opgebouwd met wereldspelers in de ICT-branche als Business Objects, Citrix, Cognos, Exact Software, Hewlett Packard, McKesson, Microsoft, Progress en Royal4.
Met het oog op het one-stop-shopping concept heeft VCD in de loop der jaren diverse partnerships met externe partijen verkregen. Door deze partnerships is het mogelijk om een nog groter scala aan diensten en producten te leveren.

Financieel
De financiële positie van VCD is ronduit goed te noemen waardoor de klanten verzekerd zijn dat de continuïteit van de dienstverlening van VCD gewaarborgd is.

Organogram VCD Automatisering
In figuur 1 wordt het organogram van VCD Automatisering schematisch weergegeven.



Figuur 1 **- Organogram VCD holding**

3.2 De afdeling Systems & Integration

Tot de kerntaken van Systems & Integration behoort het correctief en preventief onderhoud van hardware, het configureren, installeren en opleveren van systemen, het systeembeheer bij klanten alsmede het verlenen van support (zowel remote als on-site) met betrekking tot systeemsoftware en het installeren en opleveren van systeemsoftware bij klanten. Het betreft over het algemeen enterprise systemen die overwegend worden ingezet ter ondersteuning van de primaire bedrijfsprocessen. Daarnaast heeft VCD S&I ook inhouse oplossingen in de vorm van housing en hosting en complete outsourcing van uw infrastructuur.

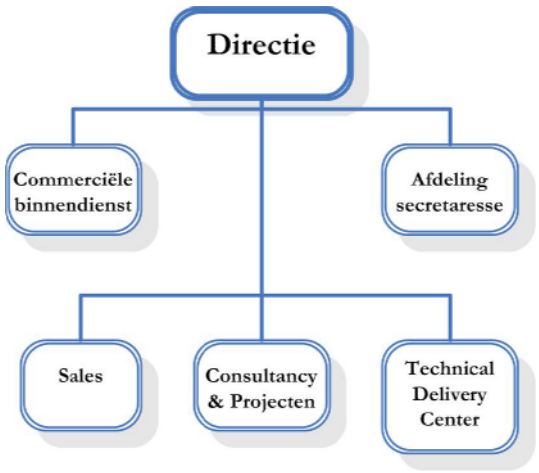
VCD Systems & Integration is HP Preferred Partner, HP Authorized Business Solutions Partner, HP Authorized Service Management Partner en HP Linux Elite Partner. Er is een ruime ervaring aanwezig in het implementeren van HP-UX oplossingen, al dan niet gecombineerd met storage en SAN omgevingen.

VCD Systems & Integration heeft ruime ervaring met onder andere:

- Het implementeren en beheren van complexe netwerken;
- Het implementeren en beheren van storage oplossingen;
- Het implementeren en beheren van Thin Cliënt concepten (Citrix).

Een goede infrastructurele oplossing is aanmerkelijk meer dan een verzameling technische componenten. Het is het fundament van uw geautomatiseerde processen, de basis voor optimaal rendement. Daarom zorgt VCD voor een infrastructuur die uw processen perfect ondersteunt en uw automatiseringssysteem beheersbaar en flexibel maakt.

Figuur 2 geeft het organogram van de business unit schematisch weer:



Figuur 2 - Organogram VCD S&I

HP levert niet rechtstreeks aan eindgebruikers, maar doet dit via partners. Door certificering zijn partners van HP in staat om te beschikken over de juiste kennis om de HP producten op de juiste wijze te implementeren. McKesson leverde in het verleden ook de benodigde infrastructuur voor haar oplossingen. De hardware leverancier vereiste certificering, waarnaar McKesson heeft besloten deze activiteiten niet zelf uit te voeren maar over te dragen aan VCD. Hierdoor is er een samenwerking ontstaan tussen McKesson en VCD. VCD levert, installeert en onderhoudt in veel gevallen de benodigde infrastructuur bij de eigen en McKesson klanten.

3.3 Ziekenhuis Bernhoven

Ziekenhuis Bernhoven is een regionaal ziekenhuis. En beslaat 2 locatie, de hoofdlocatie is gevestigd in Oss. Als tweede locatie is er een vestiging in Veghel. Ziekenhuis Bernhoven kan worden aangemerkt als een volwaardig ziekenhuis.

Doordat de verschillende medische afdelingen zijn verdeeld over de twee locaties zijn beide ziekenhuizen middels een infrastructurele oplossing aan elkaar verbonden. Deze locaties connectie met elkaar verbonden middels een glasvezel. Vanuit beheer en financieel oogpunt is er in het verleden gekozen voor een centrale ICT omgeving.

3.4 De rol van de afstudeerder

Binnen VCD ben ik aangesteld als 'Systems Engineer' voor regio Zuid Nederland op de vestiging in Eindhoven. Samengevat beslaat deze functie: de technische infrastructuur bij klanten zodanig installeren en beheren dat deze conform de gestelde prestatiekenmerken functioneert.

Binnen deze functie valt dit onder te verdelen in een aantal kerntaken te weten:

- Ontwerpen van netwerken configuraties van computersystemen en servers;
- Selecteren van hardware en systeemsoftware;
- Installeren van netwerkcomponenten, servers, en programmatuur;
- Maken en uitvoeren van testplan (actielijst/ functioneel ontwerp / documentatie);
- Opstellen wijzigingsvoorstel;
- Ondersteunen gebruiker(s) bij nieuwe omgeving;
- Opstellen gebruiksinstructies en gebruikershandleidingen.

4 Probleemstelling en opdrachtomschrijving

4.1 Globale probleemstelling

Centaal voor dit project staat de gestelde vraag van Ziekenhuis Bernhoven (ZB) voor het aandragen van één oplossing voor de vervanging van de huidige ZIS infrastructuur (Ziekenhuis Informatie Systeem).

ZB maakt gebruikt van het door McKesson ontwikkelde ZIS. Er dient in samenspraak met McKesson te komen tot een gewenste/passende oplossing (performance / ondersteunende hardware / back-up & recovery).

De huidige infrastructuur voor de ZIS applicatie is reeds vijf jaar oud. ZB heeft aangegeven deze oplossing te willen vervangen door een nieuwe infrastructuur voor hun ZIS applicatie. Hoge onderhoudskosten en niet flexibele uitbreidingsmogelijkheden zijn mede oorzaak om te komen tot een nieuwe oplossing.

4.2 Opdrachtomschrijving

De opdrachtomschrijving is een verlengde van de globale probleemstelling en heeft als hoofdthema: vervanging van de huidige ZIS-infrastructuur (vooral gericht op de hardware).

Tevens dient dit nieuwe platform middels een koppeling met het internet te worden ontsloten. Dit om derden toegang te bieden tot de patiënt informatie. Gezien de patiënt gevoelige informatie, welke buiten het ziekenhuis beschikbaar gesteld dient te worden, brengt dit extra risico's met zich mee. Daarom wordt er een Security Architectuur geadviseerd en voorgedragen, die aansluit bij de door de NEN opgestelde NEN7510 norm.

4.3 Op te leveren producten en onderzoeksresultaten

Het project levert de volgende hoofdproducten op:

- Een geïmplementeerde oplossing zoals overeengekomen:
- Een Projectplan, bevat alle gemaakte plannen/ afspraken;
- Een Technisch Ontwerp, beschrijving hard- en software;
- Acceptatierapport, test rapport waarin beschreven staat waaraan de ingebruikgenomen hard-software aan dient te voldoen;
- Technische documentatie (standaard Installatie Configuratie Rapport);
- Actielijst;
- Evaluatierapport.

Verder zijn voor dit project van belang:

- Flexibiliteit;
- Doorgroei;
- Schaalbaarheid;
- Toekomstvast/gericht;
- Beheersbaarheid.

Bovenstaande kenmerken dienen tot uiting te komen in het ontwerp voor de vervanging van de huidige ZIS infrastructuur. Hiermee wil ZB inspelen op toekomstige vraagstukken die vanuit de business gesteld worden.

Nadat het projectplan door beide partijen is goedgekeurd en ondertekend, kan worden overgegaan tot de implementatie. Na afronding van de implementatie volgt er een acceptatietest. Deze acceptatietest is in onderling overleg tussen ZB en VCD opgesteld.

Middels de ondertekening van deze acceptatietest wordt het project officieel afgerond en overgedragen. Hierna volgt er evaluatie van het project.

Na de vervanging van de hardware van de ZIS omgeving wordt tevens een nieuwe versie van de ZIS applicatie operationeel gebracht. Dit valt buiten de verantwoordelijkheid van VCD maar zal in samenspraak met McKesson worden opgepakt.

5 Plan van Aanpak en de gebruikte methode

5.1 Aanleiding

Een aantal punten zijn aanleiding geweest voor ZB om de huidige oplossing te gaan vervangen. Deze punten zijn samen te vatten in een te kort aan:

- Performance;
- Flexibiliteit;
- Doorgroei mogelijkheid;
- Schaalbaarheid;
- Toekomstvast/gericht;
- Beheersbaarheid;
- Leeftijd hardware.

5.2 Doelstelling

Binnen dit project wordt een volledig nieuwe storage omgeving ingericht, die als basis dient voor het verder uitbouwen in de toekomst. De hardware voor de volgende applicaties zullen worden vervangen:

- X/Care;
- Foodcare;
- Horizon.

De bedrijfskritische systemen worden aangesloten op de nieuwe centrale SAN omgeving. De configuratie van de SAN zal in overleg met de klant worden ingericht.

De back-up zal worden ingericht op basis van een nieuwe Virtual Library System (VLS). Dit is een backup van disk–to-disk (d2d). Daarnaast wordt ook een nieuwe tape-library voor het maken van back-up naar tape. De keuze voor het gebruik van twee back-up devices is tweeledig.

De VLS zal worden ingezet voor het maken van back-ups van d2d. Op deze wijze wordt het back-up window aanzienlijk verkort. De huidige back-up biedt alleen de mogelijkheid voor het maken van een back-up naar tape. Het maken van een back-up op de traditionele wijze, brengt gezien de omvang van de database en overige data de nodige problemen met zich mee. Dit heeft te maken met de doorlooptijd voor het maken van back-up naar tape.
Verder is er gekozen voor een tape-library voor het maken van een back-up op traditionele wijze (van disk naar tape). Deze back-up wordt dan ook gemaakt van de VLS naar de tape-library. Dit proces kan op een later tijdstip worden uitgevoerd. Het back-up window wordt op deze manier vergroot.

5.3 Huidige situatie en gewenste situatie

De huidige infrastructuur bestaat uit een vijf jaar oud HP-UX (HP9000) cluster met daarop aangesloten dedicated storage. Dit brengt een groot nadeel met zich mee aangaande de flexibiliteit van de omgeving. De huidige situatie kan worden aangemerkt als zijnde een statische omgeving.

Mede door het feit dat producten niet meer worden ondersteund en/of obsolieet raken of zijn, is verdere uitbreiding op de huidige omgeving niet mogelijk. Dit heeft ZB dit doen beslissen uit te kijken naar een nieuwe oplossing.

Voor ZB is het noodzakelijk dat de nieuwe omgeving gebruik maakt van Microsoft Windows operating systeem. Deze eis is gesteld omdat men wil verder standaardiseren wat betreft het operating systeem platform. Van dit operarting systeem is voldoende kennis aanwezig binnen ZB.

De eerder genoemde punten bij paragraaf 5.1 dienen als uitgangspunt. ZB geeft aan het huidige cluster ten behoeve van de ZIS applicatie X/Care te willen vervangen. Op het huidige cluster draaien naast het ZIS ook de volgende applicaties: Horizon en Foodcare.

In samenwerking met de klant zal een document voor de acceptatietest worden opgesteld. Voor de applicatie X/Care zal dit in samenwerking gaan met de leverancier McKesson. Dit om aan te tonen dat de applicatie weer beschikbaar wordt bij het optreden van een calamiteit.

5.4 Afbakening

Dit project is een combinatie tussen VCD en McKesson. Voor beide is een afzonderlijke afbakening te benoemen. Op verzoek van ZB is alles van VCD en McKesson geïntegreerd in één gezamelijk projectplan.

Het project kent de volgende doelstellingen en verantwoordelijkheden welke van toepassing zijn voor VCD:

- Levering / installatie / configuratie van de hardware;
- Inventarisatie huidige omgeving ZIS applicatie (X/Care);
- Installatie & configuratie cluster voor X/Care servers;
- Installatie & configuratie SAN infrastructuur;
- Installatie & configuratie VLS en MSL6030 ten behoeve van back-up;
- Installatie & configuratie Dataprotector tbv. Back-up;
- Configuratie Backup schedule Online-backup tbv. X/Care;
- Installatie & configuratie ZIS ondersteunende servers (Foodcare/Horizon/Batchdeamon);
- Standaard documentatie ICR.

Binnen het project zullen ook een aantal onderdelen buiten de verantwoordelijkheid van VCD vallen:

- Installatie van Oracle op de benodigde servers;
- Installatie van de ZIS applicatie X/Care, Foodcare en Horizon op de daarvoor bestemde servers;
- Overzetten van scripts voor het starten/stoppen van de X/Care database en overige McKesson applicaties;
- Aanpassen scripts pre/post scripts voor overige applicaties;
- Configuratie overige back-up instellingen voor overige applicaties;
- Migratie van de bestaande servers;
- Upgrade Firmware van bestaande HBA adapters;
- Beheerdocumentatie;
- Bouwkundige aanpassingen op de locaties;
- Aanleg van stroom (220V) voorzieningen;
- Interne projectcommunicatie ZB;
- Verzekering geïnstalleerde apparatuur;
- Afspraken met externe leveranciers voor beschikbaarheid tijdens installatie, configuratie, testen en/of vragen.

Een aantal van de punten welke buiten de afbakening van VCD vallen kunnen worden toegekend aan de verantwoordelijkheid van McKesson.

Het project kent de volgende doelstellingen:

- Installatie van Oracle op de benodigde servers;
- Installatie van X/Care, Foodcare en Horizon op de daarvoor bestemde servers;
- Overzetten van scripts voor het starten/stoppen van de X/Care database en overige McKesson applicaties;
- Installatie en configuratie van de batch-/connectdemon;
- Configuratie tbv online back-up van X/Care;
- Migratie van de bestaande servers.

De volgende onderdelen maken geen deel uit van het project:

- Installatie en configuratie van de hardware componenten;
- Migratie van applicaties, anders dan hierboven vermeld.

Bovenstaande aspecten worden onderverdeeld in vier componenten:

- Organisatie;
- Informatie;
- Applicatie;
- Infrastructuur.

Niet alle componenten zullen evenveel aandacht krijgen. De onderdelen technisch ontwerp en Security Architectuur zullen het diepgaands besproken worden. VCD wordt geacht in deze rol mee te denken om een visie te ontwikkelen om aan de gestelde eisen/wensen een oplossing aan te dragen.

5.5 Deelnemers aan het project

5.5.1 Projectgroep

De projectgroep begeleidt de installatiefase en verzorgt de afstemming van alle activiteiten. De projectgroep is gerechtigd beslissingen te nemen binnen de door de stuurgroep vastgestelde begroting en planning. In geval van (verwachte) afwijkingen worden deze gemeld aan de stuurgroep. Indien beslissingen moeten worden genomen over voorgestelde oplossingen binnen het project, worden deze eveneens voorgelegd aan de stuurgroep. De projectleider functioneert als intermediair tussen de projectgroep en de stuurgroep.

Rol	Persoon	Toelichting
Voorzitter	L. Poulussen of P.H. Klijs	Hoofd ICT / Sr. Projectleider(VCD)
Leden	A. Ardonne	Projectleider ICT project (ZB)
	J.A. Groeneveld	Systems Engineer (VCD)
	L. Tepper	Systems Engineer Sr. (VCD)
	R. Degens	Projectleider (McKesson)
	T. Wijtenburg	Sr. DBA (McKesson)
	J. Gooren	DBA (McKesson)
	P. van Dongen	Support Engineer (McKesson)

Tabel 1 Projectleden

5.5.2 Stuurgroep

De stuurgroep neemt beslissingen over de planning, het budget en vragen vanuit de projectgroep. Tevens wordt de voortgang van het project door de stuurgroep bewaakt. Tenslotte heeft de stuurgroep als taak om formeel de eindproducten te accepteren.

5.5.3 Vergaderfrequentie

De projectgroep komt voor een kick-off bij elkaar. Er zal eens keer per week een projectgroep overleg worden gevoerd. Adhoc kan een vergadering voor de stuurgroep en/of projectgroep worden ingepland. Alle bijeenkomsten worden genotuleerd en wordt naar alle projectleden.

5.5.4 Rollen en verantwoordelijkheden

Persoon	Rol
Dhr. L. Poulussen	Projectleider vanuit ZB, verantwoordelijk voor de coördinatie van de werkzaamheden welke uitgevoerd worden door ZB medewerkers, interne project communicatie binnen ZB.
Dhr. A. Ardonne	Projectleider vanuit ZB, verantwoordelijk voor de coördinatie van de werkzaamheden welke uitgevoerd worden door ZB medewerkers.
Dhr. P.H. Klijs	Projectleider vanuit VCD, verantwoordelijk voor de coördinatie van de werkzaamheden welke uitgevoerd worden door VCD medewerkers
Dhr. L. Tepper	Projectmedewerker vanuit VCD, verantwoordelijk voor de coördinatie en installatie op locatie bij de klant.
Dhr. J.A. Groeneveld	Projectmedewerker vanuit VCD, verantwoordelijk voor installaties en configuratie op locatie bij de klant
Dhr. H. van den Broek	Accountmanager McKesson en verantwoordelijk als opdrachtnemer van dit hele project.
Dhr. R. Degens	Projectleider vanuit McKesson, verantwoordelijk voor het op tijd inzetten van resources van McKesson en overige zaken die met de McKesson applicaties hebben te maken.
Dhr. T. Wijtenburg	Sr. DBA vanuit McKesson, verantwoordelijk voor de installatie/configuratie en migratie van Oracle, X/Care en Horizon.
Dhr. J. Gooren	DBA vanuit McKesson, verantwoordelijk voor de installatie/configuratie en migratie van X/FIS
Dhr. P. van Dongen	Consultant Foodcare vanuit McKesson, verantwoordelijk voor de installatie/configuratie en migratie van Foodcare.

Tabel 2 Rollen en verantwoordelijkheid

5.5.5 Voorwaarden aan derden

Voor het uitvoeren zijn ook werkzaamheden nodig van McKesson. Er zal afstemming plaatsvinden tussen de projectmanager van VCD en de projectmanager van McKesson m.b.t. de afstemming van de werkzaamheden.

5.6 Planning in schemavorm

Binnen het totale project zijn een aantal bij naam te benoemen mijlpalen. Zoals al eerder genoemd worden deze mijlpalen middels continu overleg besproken en gehaald.

Mijlpalen:

- Werking SAN infrastructuur (switches / EVA4000 / management appliance);
- Werking Horizon cluster;
- Werking Foodcare servers;
- Werking Batchdeamon servers;
- Werking VLS en MSL6030;
- Restore van VLS;
- Restore van MSL6030;
- Documentatie nieuwe ZIS platform;

Bovengenoemde mijlpalen zullen in de planning en later in de acceptatietest terug komen. Als bijlage aan dit verslag is de planning opgenomen (Bijlage 1).

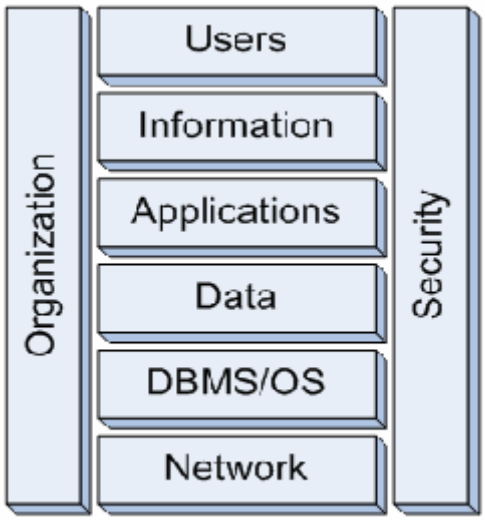
6 Logisch ontwerp - Architectuur

6.1 Inleiding

Als methode voor de ontwikkeling voor het ZIS architectuur gebruiken we de methode van James D. McCabe. Deze methode is vooral bedoeld als ontwikkelmethode voor computernetwerken, maar een zeer belangrijk onderdeel hiervan is de ontwikkeling van beveiliging voor deze netwerken.

McCabe gebruikt een systeembenadering, die vooral bij dit project zo goed toepasbaar is, omdat er door McCabe uitgegaan wordt van de niveaus users – applications – devices - networks. Op elk van deze niveaus speelt security een belangrijke rol, maar op elk van deze niveaus zal de security vanuit een ander perspectief worden opgezet.

Wij zullen de systeembenadering van James McCabe gebruiken volgens de indeling, zoals in figuur 3.



Figuur 3 Systeembenadering McCabe

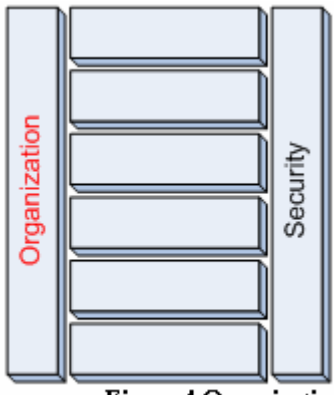
McCabe hanteert bij de ontwikkeling van een systeem de volgende fasering: Vooronderzoek – Analyse – Architectuur – Ontwerp. Deze fasering zal in grote lijnen worden overnemen.

6.2 Analyse van eisen uit de organisatie

ZB heeft in zijn vraag zich willen niet beperken tot alleen een ontwerp aangaande hun ZIS maar ontvangt graag een nieuwe handreiking / visie. Om in de toekomst in te kunnen spelen op ICT vraagstukken. Zal onderstaande dan ook breder toegelicht worden. Om ZB op deze manier een totaalplaatje te geven, aangaande de toekomstige ZIS omgeving met alle daarbij behorende vraagstukken en gekoppelde systemen.

Door de systeembenaderingsmethode van James McCabe in praktijk toe te passen, moeten er eisen verzameld worden op elk niveau van het 'systeem'. Op het hoogste niveau vinden we de eisen met betrekking tot beveiliging van de gebruikers en op het laagste niveau het netwerk in de vorm van perimeterbeveiliging.

Figuur 4 geeft aan op welke plaats in het McCabe systeem deze eisen thuishoren.
Gezien het feit dat het een ZIS omgeving betreft blijkt dat organisatorische maatregelen noodzakelijk zijn voor een goede beveiliging.



Figuur 4 Organisatie

De volgende beheerprocessen dienen minimaal ingevuld te worden:

- *Autorisatiebeheer*
  Veel gegevens van het platform hebben een vertrouwelijk karakter. Het op de juiste manier uitdelen, wijzigen en intrekken van autorisaties is hierbij van wezenlijk belang. We maken hier een onderscheid tussen tactisch/operationeel en business/ICT.

- *Configuratiebeheer*
  Er zijn diverse redenen te noemen voor het beheren van hardware en software:
  a) Bij een storing is het noodzakelijk om te achterhalen welke afspraken en contracten er lopen t.a.v. het systeem dat de storing veroorzaakt.
  b) Als er misbruik wordt gemaakt is het noodzakelijk om bijvoorbeeld te kunnen achterhalen op welke wijze deze credentials zijn verkregen.
- *Incidentbeheer*
  Aan het platform worden hoge eisen gesteld m.b.t. beschikbaarheid. Mocht zich een storing voordoen dan is het zeer belangrijk om heldere procedures te hebben om de storing zo snel mogelijk te verhelpen.
- *Wijzigingsbeheer*
  Eén bron van mogelijke storingen is het aanbrengen van wijzigingen aan de operationele omgeving. Wijzigingsbeheer is er op gericht om op een gestructureerde en doordachte manier wijzigingen aan te brengen en om tevens een noodprocedure gereed te hebben, mocht de wijziging falen.
- *Operationeel beheer*
  Hardware en software hebben periodiek onderhoud nodig zoals het aanbrengen van een nieuwe release van een operating system en/of een bug-fix. Monitoring en logging zijn hierin de eerste stap.
- *Beveiligingsbeheer*
  Beveiliging is een dynamisch geheel, immers de ontwikkelingen in de (anti-) beveiligingswereld staan niet stil. Maar ook de eigen organisatie is dynamisch. Het is dus reëel om aan te nemen dat de beveiliging en de daarvoor geldende eisen periodiek zullen veranderen. Je moet hierop kunnen anticiperen. Een procesmatige aanpak is dus ook hier vereist.

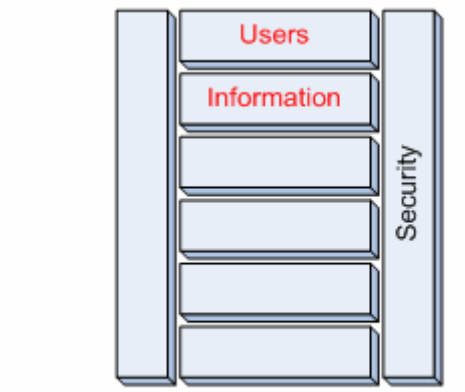
Naast bovenstaande processen zijn er nog andere processen die ik wil aanbevelen. Deze zijn wellicht op korte termijn niet noodzakelijk, maar zullen op termijn het nodige kunnen bijdragen:

- ITIL-processen
  Hierboven hebben we een aantal cruciale ITIL-processen genoemd. ITIL kent echter nog een aantal processen, zoals capacity managenement en problem management, die op den duur waardevol zijn voor een organisatie.
- ASL
  De software in een organisatie wordt echter ook steeds complexer wat een gestructureerd beheer hiervan noodzakelijk maakt. Hiervoor is ook een best-practice methodiek ontwikkeld, namelijk de Application Service Library (ASL).

6.3 Gebruikers- en informatie-eisen

Juiste en betrouwbare informatie is wat ieder bedrijf wenst te realiseren. Om te komen tot informatie die:

- Bruikbaar;
- Betrouwbaar;
- Up to date;
- Toegankelijk;
- Juiste informatie is.



Figuur 5 Gebruikers- en informatieeisen

In een later stadium zal een opzet worden gemaakt aangaande de systemen welke zorg gaan dragen voor alle informatie. Er zijn meerdere eisen te definiëren aangaande informatie. Om te voorkomen dat bepaalde eisen onvoldoende worden belicht of worden benoemd in dit verslag, volgt er samenvatting waaraan de informatie zal moeten voldoen:

Alle informatie dient te allen tijde middels een juiste autorisatie beschikbaar te zijn voor een geautoriseerd persoon of proces.

Figuur 5 geeft aan op welke plaats in het McCabe systeem deze eisen thuishoren. De volgende tabel geeft de gebruikers- en informatie-eisen weer:

I1	Informatieverstrekking aan alle eindgebruikers dien middels een Authenticatieprocedure te worden afgehandeld;
I2	Informatieverstrekking dient te worden afgevangen binnen de gebruikte applicaties middels het gebruik van rolen en rechten;
I3	Informatietoegang welke kan worden verkregen middels een account op de desbetreffende systeem om daadwerkelijk (fysiek) in te loggen op het systeem, wordt alleen toegestaan aan medewerkers die werkzaam zijn binnen de afdeling automatisering;
I4	System management dient een hoog niveau van authenticatie te bezitten. Voorgesteld wordt om tokens te gebruiken. Dit wordt gebruikt voor leveranciers;
I6	De nieuwe ZIS omgeving dient een beschikbaarheid te hebben van 99,95% . Dit betreft geplande downtime. Dit betekent dat het systeem per week gemiddeld 5 minuten down mag zijn. Als maximale downtijd definiëren we 60 minuten. Downtijden van meer dan 30 minuten mogen slechts eens per half jaar voorkomen.
I7	In geval van ongeplande downtime dient men binnen 6 uur weer operationeel te zijn.

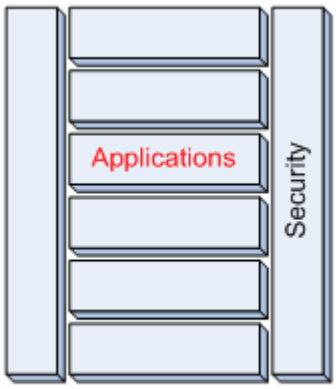
Tabel 3 Gebruikers- en informatieeisen

Onder gebruikers worden niet alleen eindgebruikers verstaan. Maar ook beheerders, medewerkers van leveranciers en in de toekomst consumenten.

6.4 Eisen aan applicaties

Onderstaande eisen zijn ontstaan door het lezen en verwerken van de door McKesson opgestelde systeemeisen welke voor de verschillende applicaties noodzakelijk zijn. Figuur 6 aan op welke plaats in het McCabe systeem deze eisen thuishoren.

Door in eerste instantie de systeemeisen op te vragen bij McKesson kunnen onderstaande eisen worden opgesomd. Figuur 6 geeft aan op welke plaats in het McCabe systeem deze eisen thuishoren. Onderstaande tabel geeft dan ook een opsomming als het gaat om de eisen van de applicatie.



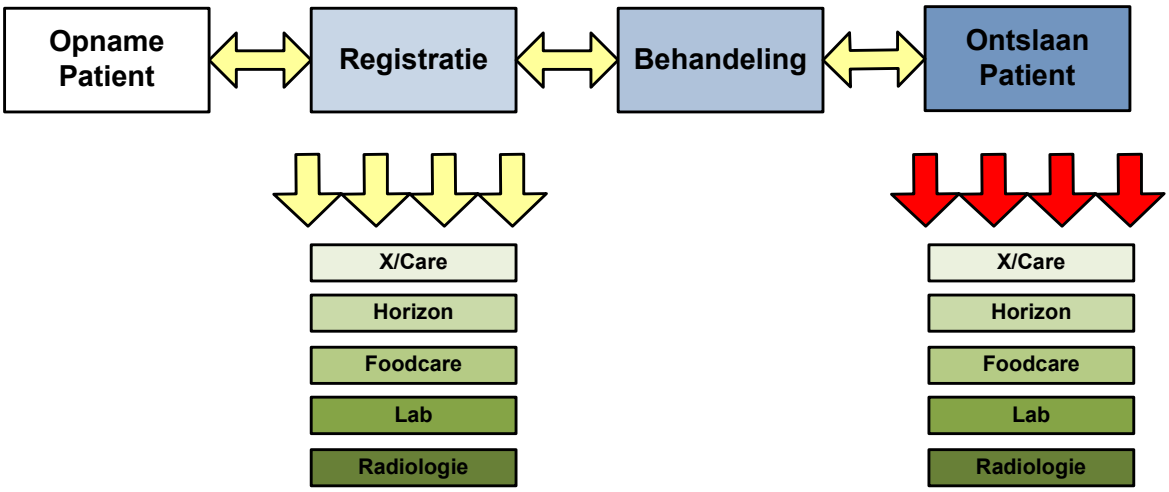
Figuur 6 Applicatie

A1	X/Care cliënt, gebruikt gemiddeld zo´n 5 á 10MB per ingelogde cliënt;
A2	X/Care vereist een Oracle Database, met minimaal de versie van Oracle 9. Oracle v8 wordt niet meer ondersteund. De laatste versie waarop tevens de applicatie komt te draaien betreft de versie Oracle v10);
A3	Horizon vereist een Oracle database. Aangezien Horizon is een webbased applicatie, en maakt gebruik van BEA Weblogic versie 8.1.6;
A4	Horizon dient aangemerkt te worden als een intensieve CPU gebruiker;
A5	Foodcare vereist DBC versie 9 en een interface/koppeling met X/Care.

Tabel 4 Eisen aan applicatie

6.5 Eisen aan de datastromen

Figuur 7 laat het proces zien wat doorlopen wordt als een patiënt wordt opgenomen, tot het moment waarop deze wordt ontslagen.

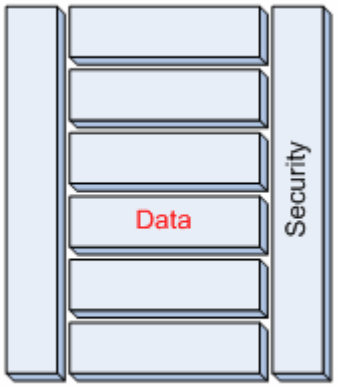


Figuur 7 ZIS Proces

De weergegeven figuur geeft weer welke datastromen er binnen het ZIS proces ontstaan deze zijn in tabel 5 opgesomd:

D1	Patiënt wordt opgenomen en registratie volgt;
D2	Patiënt gegevens worden opgeslagen in weergegeven applicaties, genoemde applicaties informeren elkaar over de ontstane wijziging;
D3	Gegevens wijzigen naarmate de behandeling vordert, deze gewijzigde gegevens worden onderling tussen de applicaties uitgewisseld;
D4	Patiënt wordt ontslagen er volgt een wijziging binnen de applicaties.

Tabel 5 Eisen aan de datastromen

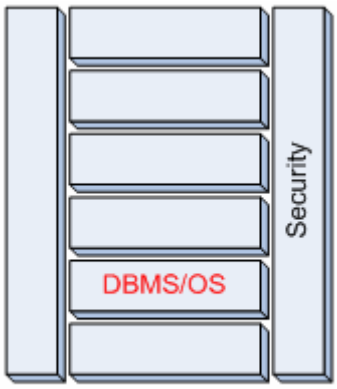


Figuur 8 Datastromen

Figuur 8 geeft aan op welke plaats in het McCabe systeem deze eisen thuishoren.

6.6 Eisen aan DBMS-OS

Het operationele platform is gebaseerd op Oracle.
De systemen welke de Oracle omgeving gaan ondersteunen dienen een backend positie in het netwerk te krijgen.



Figuur 9 DBMS-OS

De ZIS applicatie van McKesson maakt gebruik van een Oracle database. McKesson ondersteund multiple operating systemen waar de applicatie op kan draaien. Specifiek kijkende naar ZB is het volgende te melden. De huidige omgeving wordt nu ondersteund door 2 HP-UX machines met daarop een centrale Oracle database.

In het toekomstige plaatje komt de database te draaien op een Itanium 64 bit Windows cluster. In een later stadium zal worden ingegaan op de overgang van deze database met de daarbij behorende impact als het gaat om:

- Beveiliging;
- Beheer;
- Continuïteit.

In de figuur 9 wordt de positie van database/OS eisen in het McCabe model aangegeven.
De volgende eisen gelden voor de DBMS:

A1	Het platform dient een hoge beschikbaarheid te hebben. Bij de gebruikerseisen is reeds een percentage genoemd. Daarnaast dient het platform over voldoende redundantie te beschikken om Single Points of Failure uit te sluiten;
A2	De database dient een gebruikersaantal van 400 tot 500 actieve gebruikers te kunnen ondersteunen;
A3	De database ondersteund dient minimaal versie Oracle 9 of hoger;
A4	De huidige database komt op het nieuwe cluster te draaien onder de Oracle 9.

Tabel 5 Eisen aan DBMS-OS

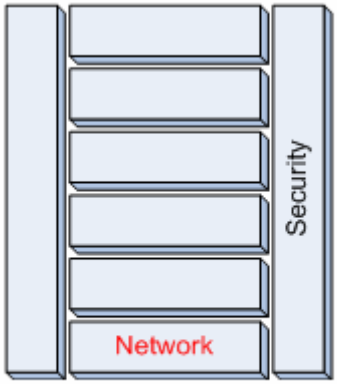
6.7 Eisen aan het netwerk

Onder het netwerk wordt verstaan:

- Het bekabelingsysteem;
- De computerinterfaces;
- Verbindingsapparatuur (switches/routers/firewalls);

Ook alle gehanteerde protocollen in de TCP/IP stack vallen hier onder. Voor het netwerk zullen ook vooral eisen gelden, die te maken hebben met de topologie en de compartimentering.

Het netwerk dient te voldoen aan de volgende eisen:



Figuaar 10 Netwerk

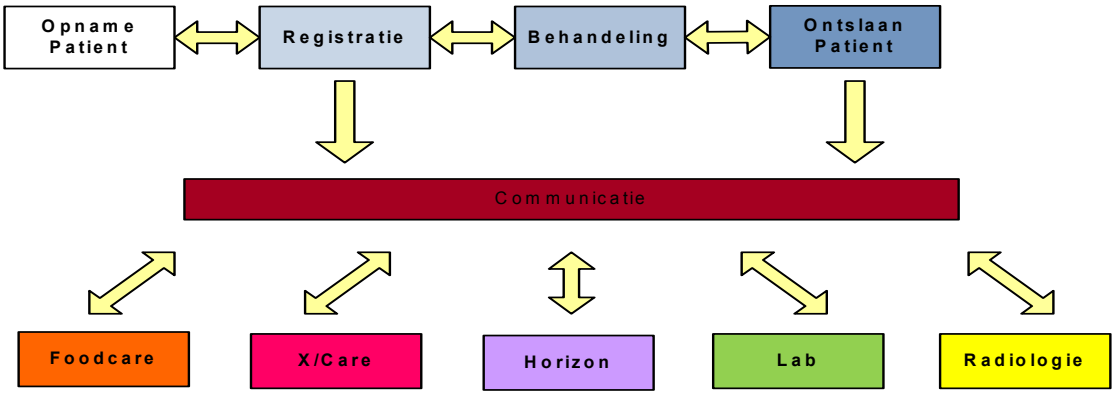
N1	Het bekabelingssysteem van het bedrijfsnetwerk dient gestandaardiseerd te zijn volgens de standaard TIA/EIA 568B en officieel worden gecertificeerd;
N2	Er dient een automatische bewaking te bestaan met betrekking tot het aansluiten van apparatuur aan het netwerk op basis van het MAC-adres. Uitsluitend hiertoe gedelegeerd personeel van systeem- en netwerkbeheer mag deze apparatuur aansluiten;
N3	Switches en routers dienen manageable te zijn, voorzien van SNMP-agents en een MIB. De toegang tot deze apparatuur is uitsluitend voorbehouden aan hiertoe gedelegeerd personeel;
N4	Het interne netwerk dient minimaal te beschikken over een snelheid van 100Mbps. Gewenst is een snelheid van 1000 Mbps.

Tabel 6 Eisen aan het netwerk

Figuur 10 geeft aan op welke plaats in het McCabe systeem deze eisen thuishoren.

6.8 Analyse van de informatiestromen

Het ZIS platform kent een aantal functionaliteiten, die samenhangen op een wijze zoals in figuur 11 is weergegeven. Tussen deze functionaliteiten lopen informatiestromen ten behoeve van mutaties, afhandeling en informatieverstrekking/verwerking.



Figuur 11

Centraal binnen deze stromen is de onderlinge communicatie van systemen welke mutaties krijgen te verwerken. De spil binnen al deze stromen is de communicatie(server). Hierop zijn meerdere rules aangemaakt als het gaan om informatieverstrekking. Als bijvoorbeeld een patiënt wordt verhuisd naar een andere kamer binnen het ziekenhuis. Dient dit doorgegeven te worden aan Foodcare. De overige systemen hoeven niet te beschikken over deze specifieke informatie.

Foodcare
Betreft een voedingsmanagement product. Deze applicatie geeft inzicht in alle voedings- en voedselstromen binnen productiekeukens, ziekenhuizen, GGZ- en zorginstellingen. Een op zich zelf staand product. Beschikt over een eigen database en werkt via het Cliënt / Server principe.

X/Care
Elektronische kaartenbak met daarin alle relevante patiëntinformatie. Cliënt / Server applicatie welke gebruikt maakt van onder andere de centrale Oracle database. X/Care is opgebouwd in modules:

- Afspraken;
- OK;
- Opnameplanning;
- Ordermanagement;
- DBC-registratie.

Horizon
Webbased product wat het mogelijk maakt informatie te ontsluiten uit bronnen van derden. De mogelijkheden hierin zijn: Huisartensportal / Specialistenportal/Verpleegkundige portal /Patiënt portal.

Lab
Laboratorium voor allerhande waarde bepalingen., dat gekoppeld worden aan de juiste patiënt binnen X/Care.

Radiologie
Opslag van digitaal beeldmateriaal, dat gekoppeld wordt aan de juiste patiënt binnen X/Care.

6.9 Analyse database overgang HP-UX → Windows

De huidige database functioneert onder een HP-UX Oracle database. De Oracle versie van deze database betreft Oracle 9. Voor de overgang naar het nieuwe Windows platform dienen de nodige stappen te worden gezet. Dit alles heeft te maken met de wijziging van os en hardwareplatform.

Door McKesson zijn de volgende stappen aangedragen welke tijdens de test en daadwerkelijke overgang worden uitgevoerd:

- Stoppen van de database;
- Exporteren van de database op de (HP-UX);
- Installatie Oracle onder Windows;
- Aanmaken nieuwe omgevingen;
- Importeren van de database files naar de nieuwe omgeving;
- Installatie Batch/connectdeamon.

6.10 Patchbeleid Windows

Het patchbeleid van Windows verdient enige aandacht. De huidige omgeving bevindt zich op een HP-UX platform met HP-UX als OS. Dit OS heeft een reputatie met weinig patches wat een uiterst stabiele omgeving oplevert. Echter biedt Windows een operating systeem voor zowel cliënt als server. Mede door de gebruikersvriendelijkheid wordt een OS van Microsoft Windows het meest gebruikt. Dit maakt het een geschikte kandidaat maakt om een virus of aanval op te plannen. Uit de site survey blijkt dat de machines van ZB zich achter een redundate firewall bevinden. De kans op infectie/aanvallen worden hierdoor verkleind.

Maar wat als er een patch wordt uitgebracht?

Om hier de juiste keuze in te maken worden is van alle partijen gevraagd om hun visie aangaande het patchen van Windows.

VCD
De patchen van Windows veroorzaakt tegenwoordig niet of nauwelijks nog problemen. Wel is het aan te raden een patch uit te proberen op een test machine en ten tweede niet direct bij het uitbrengen van de patch deze direct in een productieomgeving te plaatsen. Dit om te voorkomen dat een nieuwe patch wordt geïnstalleerd terwijl deze door Microsoft is teruggetrokken als het gaat om de uitlevering hiervan.

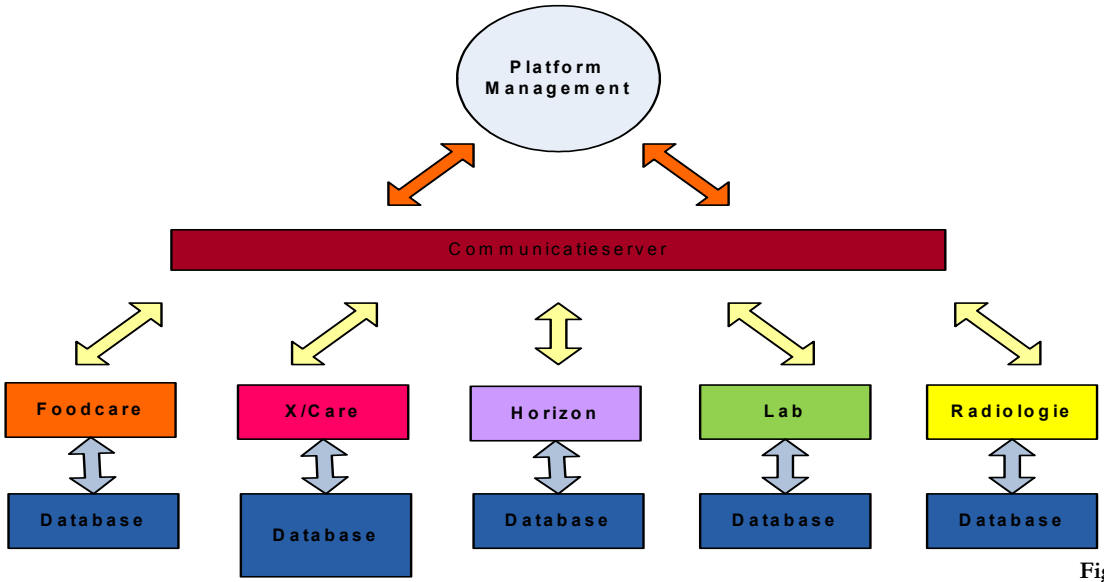
McKesson
McKesson heeft alleen te maken van de patches welke worden uitgebracht door Oracle en BEA Weblogic. Dit zijn de producten die worden gebruikt.

Ziekenhuis Bernhoven
Nadat er door Windows een patch is uitgebracht test ZB deze patch op een testsysteem. Dit systeem heeft dan ook binnen ZB geen andere functie of rol, dan het controleren en testen van patches.

Alle productieomgeving worden op een node geplaatst welke nog niet zal worden voorzien van een patch. ZB maakt eens per maand van de complete machine een Ghost image. Dit om het totale verlies van een totale server snel te kunnen herstellen.

6.11 Applicatieopbouw

Zoals in figuur 12 aangegeven beschikt iedere applicatie over een eigen database. Het grootste is de database van X/Care. Het doel van de communicatieserver is reeds in paragraaf 6.8 genoemd. Als aanvulling hierop dan worden genoemd dat het de taak is van deze communicatieserver alle aangesloten systemen op de juiste wijze en tijdig te informeren.



Figuur 12

7 Technisch ontwerp

Om een invulling te geven wordt een opsomming worden gegeven welke hardware er noodzakelijk is.

De onderliggende hardware dient te beschikken over voldoende resource om aan de vraag van de totale ZIS omgeving te kunnen voldoen. Gezien de resource eisen van deze applicatie is gekozen voor een Itianium 64-bit server met een Windows Server 2003 Enterprise 64-bits OS. Reden voor deze keuze betreft de beperking in geheugenadressering bij een 32-bits platform.

Binnen ZB maken momenteel ongeveer 500 mensen gebruik van de X/Care applicatie. Iedere sessie alloceert een hoeveelheid van 5-10 MB geheugen. Gekozen is voor een cluster oplossing welke beschikt over voldoende mogelijkheden om aan huidige en toekomstige vraagstukken te voldoen. Aangezien het een cluster betreft, is het gebruik van shared storage een vereiste. Dit wordt ingevuld door een HP EVA 4000 SAN oplossing.

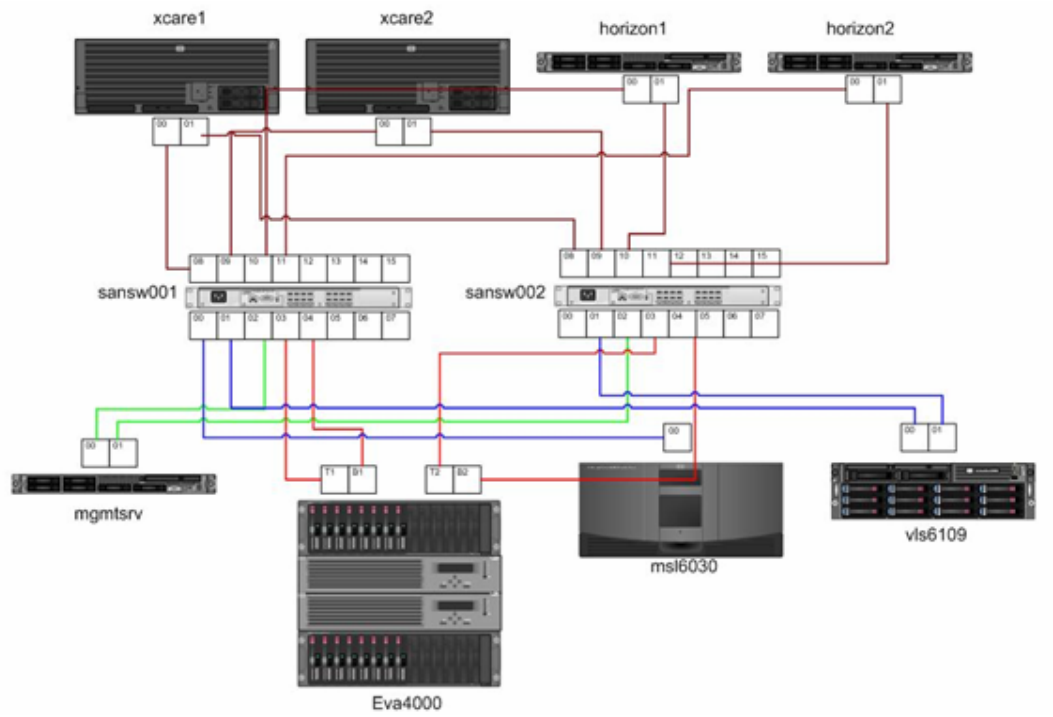
Horizon is een cluster bestaande uit twee 32-bits Windows Server 2003 Enterprise OS. Op beide clusters worden meerdere omgevingen aangemaakt. Zo bestaat er naast de noodzakelijke productieomgeving een test en een conversie omgeving. Dit is noodzakelijk als er door McKesson een patch/release wordt uitgebracht.

Verder worden er twee Windows 2003 Server machines ingericht voor de batchdeamon (achtergrondprocessen X/Care). Voor Foodcare is gekozen voor twee Windows machines. Een machine zal worden ingezet als productie, de tweede als test. Bij calamiteit zal door een handmatige actie de testmachine ingezet worden voor productie.

Voor back-up worden er twee hardwarematige oplossingen ingezet. Allereerst de traditionele tape oplossing door middel van een MSL6030. Deze beschikt over twee tapedrives wat het mogelijk maakt om tegelijkertijd twee tapes te kunnen beschrijven. Naast deze traditionele tape oplossing wordt ook gebruik gemaakt van nieuwe technologie namelijk een VLS. Deze VLS wat staat voor Virtual Libary System maakt het mogelijk om back-ups te maken naar disk. Een back-up wordt dus gemaakt van disk to disk. Deze technologie maakt het mogelijk het back-up schema/doorlooptijd enorm te verkorten. Een traditionele back-up op tape gebeurd vaak 's nachts om de performance niet negatief te beïnvloeden. Door het gebruik van de VLS is het nu mogelijk om overdag (meerdere) d2d back-ups te maken en op een later te bepalen tijdstip over te gaan tot het maken van een disk naar tape back-up (VLS naar tape).

Back-up is noodzakelijk maar voor een restore wordt de doorlooptijd enorm verkort. Door een restore van d2d (VLS naar EVA) te laten lopen bied dit vooral een snelheidswinst op.

Na uitfasering van huidige machines zullen nieuwe in te zetten machine ook op het SAN middels een HBA aangesloten worden. In figuur 15 worden deze nieuwe machines weergegeven:



Figuur 15 Blauwdruk technische oplossing

In eerste instantie lijkt het of dat alle machines elkaar middels deze HBA's kunnen 'zien'. Dit is echter niet het geval. Binnen de fiberswitches zijn een aantal zones aangemaakt. Dit maakt het mogelijk om aan te geven welke machines met elkaar kunnen communiceren.

De volgende zones zijn bij naam te benoemen:

- Management;
- X/Care cluster;
- Horizon cluster;
- Back-up VLS;
- Back-up MSL.

Om te voorzien in eventuele stroomstoringen is er gekozen voor een aparte UPS oplossing. Deze UPS beschikt over voldoende capaciteit om te totale ZIS oplossing gedurende 60 minuten operationeel te houden en in geval van blijvende stroomuitval de machines een shutdown te laten uitvoeren om zo dataverlies en/of datacorruptie te voorkomen.

8 Implementatieplan en –beschrijving

De implementatie dient gefaseerd opgeleverd te worden. De implementatiefase is binnen het project een belangrijke fase. Binnen deze scriptie is de implementatie een deel van het project.

De implementatie dient op een bepaalde wijze gefaseerd opgeleverd te worden. Middels het gebruik van shared storage dient deze storage eerst opgeleverd te worden, voor dat de aangesloten machines van deze resources gebruik kunnen maken. Middels onderstaande tabel worden de genomen stappen inzichtelijk gemaakt:
In tabel worden 7 worden de genomen stappen benoemd:

1.	Uitpakken van de systemen;
2.	Monteren van de systemen zoals eerder aangegeven via de rackindeling;
3.	Aansluiten van de machines en tevens controleren op DOA's;
4.	Installatie van OS;
5.	Installatie EVA;
6.	Configuratie EVA, aanmaken van shared storage resources;
7.	Installatie cluster (X/Care & Horizon);
8.	Installatie Switches (HBA's Zoning);
9	Installatie Foodcare;
10	Installatie Oracle;
11	Installatie Batchdeamon servers;
12	Installatie Backup;
13	Acceptatietest;
14	Documentatie.

Tabel 7 Implementatieplan

9 Security Architectuur Analyse.

In dit hoofdstuk wordt ingegaan op de gestelde eisen van ZB. Deze hebben te maken met het beschikbaar stellen van patiënt gerelateerde informatie aan externe partijen/ gebruikers. Hierbij speelt de security architectuur in combinatie met de NEN 7510 norm een belangrijke rol.
Om te komen tot een voorstel, dient eerst de achterliggende theoretische gedachte te worden toegelicht. De security architectuur is opgedeeld in twee essentiële stukken:

- Beveiligingszaken;
- Infrastructuur.

Deze zullen in de komende paragrafen verder worden toegelicht.

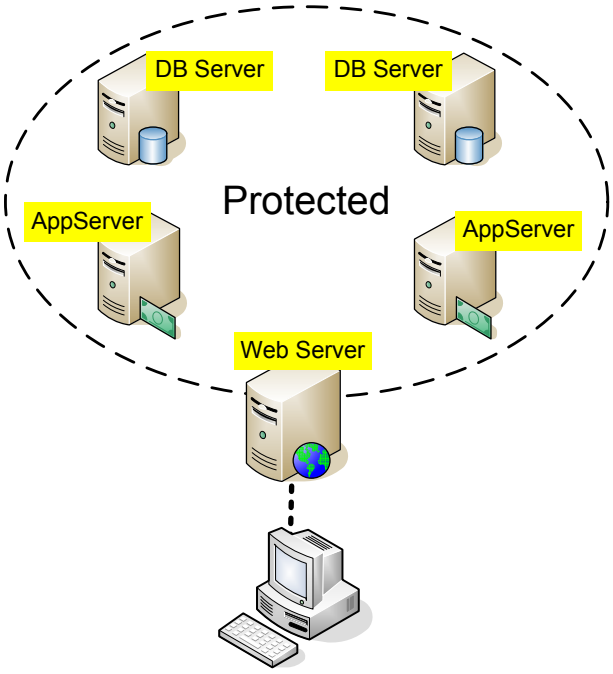
9.1 Beveiligingszaken m.b.t. applicatie

Gegevensintegriteit
Doordat slechts één bedrijfscomponent gerechtigd is om bepaalde gegevens te muteren is het mogelijk op één plaats de integriteit van een component te regelen. Elke applicatie maakt gebruik van dezelfde controle welke op een plaats is vastgelegd.

Authenticatie en autorisatie
Voor dit onderdeel willen we gebruik maken van een model dat is afgeleid van het zogenaamde Woods-Hole model. Bij dit model wordt als het ware een schil om de gegevens en de gegevensverwerking heen gelegd en is alleen de presentatielaag bereikbaar. Dit komt er op neer dat een eindgebruiker alleen autorisatie krijgt op een procesinteractie-component. Dit component gaat dan door naar de bedrijfslaag. Deze bedrijfslaag gaat vervolgens met eigen credentials naar de datalaag.

Hierbij kan een aantal beveiligingsvoordelen worden genoemd:

- Zowel op de datalaag als de bedrijfslaag hoeven geen rechten uitgedeeld te worden aan eindgebruikers. Deze hebben dus geen toegang tot deze lagen;
- Mutaties op gegevens gaan altijd via de bedrijfscomponent dat het beheer voert over de gegevens. Hierdoor blijft de integriteit van de gegevens gewaarborgd.



Figuur 12

Doordat de bedrijfscomponenten en de procesinteractiecomponenten eigen credentials hebben, heeft dit wel consequenties voor de omgaan met wachtwoorden. In de meest eenvoudige, maar niet meest veilige variant, ligt dit in de programmacode. Een betere oplossing is het gebruik van een digital vault. Dit is een oplossing op basis van een aantal identificerende gegevens. Deze gegevens (credentials) worden verstrekt aan een component.

9.1.1 Sessie-informatie

Een webapplicatie is stateless. Dat wil zeggen dat het niet zonder voorzieningen mogelijk is om meerdere invoerschermen te zien als één enkele transactie. Om hierin te kunnen voorzien wordt sessiemanagement toegevoegd aan webapplicaties. Aangezien er meerdere sessies tegelijk kunnen bestaan is het noodzakelijk om te kunnen onthouden met welke eindgebruikers een sessie is opgezet. Hiervoor moet informatie bij de cliënt worden opgeslagen of meegestuurd met webpagina's. Aangezien dit risico's met zich meebrengt moet er allerlei voorzieningen getroffen worden om misbruik van sessiegegevens te voorkomen:

- Voorkomen van een replay-attack;
- Voorkomen van manipulatie van identificerende gegevens;
- Voorkomen dat een fake-sessie wordt gegenereerd.

In de begintijd van webapplicaties, bij het gebruik van CGI, waren hier programmatische controls nodig. Tot op heden wordt gebruik gemaakt van hashing en versleuteling. Tegenwoordig bieden platformen als dotNet en Java hier standaardvoorzieningen voor.

9.1.2 Gegevensvalidatie

Met betrekking tot gegevensvalidatie maken we onderscheid tussen drie vormen:
- Integriteitscheck;
- Validatie;
- Bedrijfsregels.

Integriteitscheck
Een integriteitscheck is bedoeld om te controleren of gegevens al dan niet gemanipuleerd zijn. Deze check het beste uitgevoerd worden als gegevens van zone wisselen. Deze vorm kenmerkt zich door het gebruik van hashwaarden, versleuteling of checksums.

Validatie
Validatie controleert of gegevens voldoen aan de eisen m.b.t. gegevens zoals het juiste type, binnen de gestelde grenzen van het datatype en/of het de juiste karakters bevat. Dit soort controles kan plaats vinden op de servers die zich hier het best voor lenen. Hierbij valt te denken aan web-regels op de webserver, de bedrijfscomponent voor opslagproblemen zoals SQL-injection.

Bedrijfsregels
Dit soort regels worden dan ook geprogrammeerd in de code, waar ook de validaties plaatsvinden. Dit soort controles moet bij voorkeur nooit door programmacode aan de cliëntzijde worden gedaan.Hierdoor is er een kans op manipulatie aanwezig.

9.1.3 Encryptie

Het behoeft geen betoog dat er allerlei vormen van versleuteling bestaan ieder met een bepaalde sterkte en ieder met een bepaald toepassingsgebied. Vanuit beveiligingsoogpunt is het belangrijk om een algoritme te gebruiken dat openbaar is gemaakt. Immers niet de geheimhouding maar de opzet van een algoritme bepaald de kracht van het algoritme. In verband met brute-force attacks moet je wel rekening houden met de gebruikte sleutellengte.De volgende sleutellengtes zijn op dit moment aan te bevelen:

Symmetrische sleutels
- 128-bits voor normale toepassingen;
- 168-256 bits voor kritische toepassingen (bijvoorbeeld grote financiële transacties).

Asymmetrische sleutels
- Voor normale toepassingen is 128-bits toereikend (o.a. consumentenverkopen);
- Voor toepassingen waar een redelijke beveiliging nodig is, wordt 1536 bits aan geraden (o.a. grotere financiële transacties);
- Bij hoge beveiliging is 2048-bits aan te raden (o.a. militaire omgeving etc).

9.1.4 Logging

Logging wordt gebruikt om te kunnen achterhalen wat voor acties en/of door een applicatie hebben plaatsgevonden. Het doel van logging is meerledig:

- Een applicatie kan melden als er bepaalde fouten worden geconstateerd. Dit kan informatie zijn voor systeemontwikkelaars om programmeerfouten op te sporen;
- Als er een beveiligingsincident is, kan aan de hand van de logging worden nagegaan wat er allemaal gebeurd is;
- Voor auditors (zowel intern als extern) kan het een bron van informatie zijn om de werking van een applicatie te toetsen tegen het beleid en/of wetgeving.

Aan logging zitten zowel beveiliging als wettelijke aspecten:

- Beveiligingsaspecten
    c) Logging data moeten op een veilige plaats worden opgeslagen. Immers, de logging moet aangeven wat er *werkelijk* gebeurd is. Manipulatie moet dus uitgesloten worden;
    d) Logs moeten op een apart systeem komen omdat de hoeveelheid gegevens niet de diskruimte van het O.S. in gevaar mag brengen;
    e) Ook logs moeten meelopen in de back-upcyclus en ook de back-ups mogen niet gewijzigd kunnen worden.

- Wettelijke aspecten
    f) De Nederlandse wetgeving (o.a. wet bescherming persoonsgegevens, wet omzetbelasting, burgerlijk wetboek) stelt eisen aan de informatie die in een log mag worden opgeslagen en hoe lang bepaalde gegevens bewaard mogen/moeten worden;
    g) Een logging kan alleen als forensisch middel worden gebruikt als aantoonbaar is dat de logging niet gemanipuleerd is/kan worden.

9.2 Analyse van de infrastructuur

De applicaties van het platform zullen moeten werken op computersystemen in het netwerk. Het netwerk met de daarin werkende computersystemen en de koppelcomponenten zoals switches, routers en firewalls vatten we kortweg samen tot 'infrastructuur'. Ook beveiligingssystemen zoals intrusion detection- en intrusion prevention systemen vallen daaronder.

Analoog aan de opbouw van een ui, die uit verschillende lagen of schillen bestaat, zal een goed opgebouwde beveiligingsarchitectuur ook zo in elkaar zitten. Zodra de buitenste schil wordt afgepeld, komt er een nieuwe schil te voorschijn met zijn eigen specifieke beveiligingsmechanismen. Beveiliging moet niet uitsluitend tegen de externe omgeving gericht zijn. Ook zal het platform bescherming moeten bieden tegen bedreigingen die van binnenuit opgestart kunnen worden.

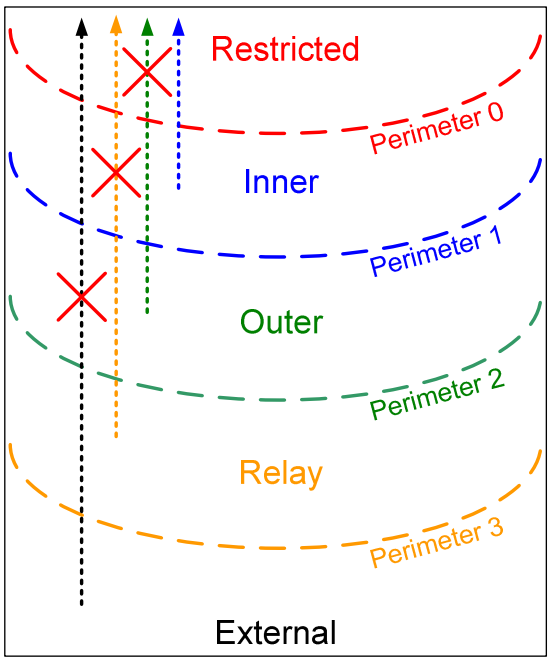
De lagen of schillen worden gescheiden door zogenoemde perimeters. Vanwege het grote belang van Confidentiallity, Integrity en Availability van het ZIS platform, zouden we een infrastructuur, bestaande uit vijf schillen kunnen opzetten:

- External: de externe omgeving (het internet);
- Relay: een proxy segment, waar alle sessies vanuit External connecten;
- Outer: een segment, waarin zich de webserver bevindt;
- Inner: het segment met de applicatie servers en de data, die door de buitenwereld gezien mag worden;
- Restricted: de backend met daarin de essentiële gegevens voor het bedrijfsproces.

In de nevenstaande figuur 13 wordt het principe weergegeven van defense-in-depth bij ons platform. In de pijlen wordt met kruisen aangegeven hoever een sessie of een bericht mag reiken bij het passeren van de perimeters.

In de omgekeerde richting gelden vergelijkbare restricties. Er is al sprake van een 3-tier constructie wanneer de berichten van de Inner via de Relay naar External worden gestuurd. In die gevallen kan de Outer worden overgeslagen

De perimeters kunnen worden beveiligd met packet filters, statefull- en proxy firewalls, VPN-devices en intrusion prevention systemen. Deze componenten spelen een belangrijke rol bij het defense-in-depth principe.



Figuur 13 Defence in Depth

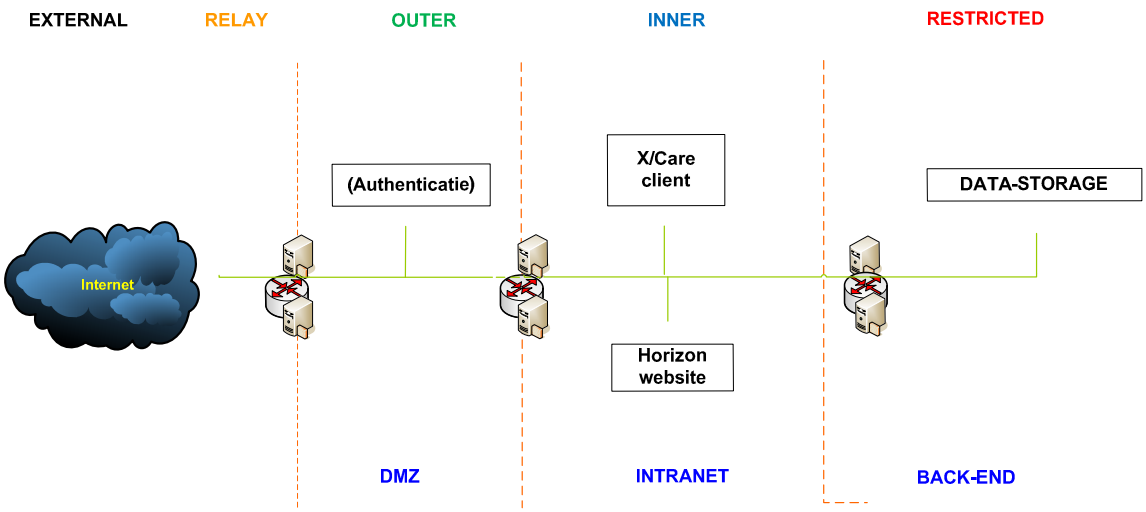
Intrusion detection systemen kunnen binnen elke laag worden aangebracht om toezicht te houden op de netwerkactiviteiten binnen die schil. Het geheel wordt gecompleteerd door zogenoemde 'honeypots' om illegale activiteiten uit te lokken en te signaleren voordat de voor het bedrijfsproces belangrijke systemen worden gecompromitteerd. Op de hostsystemen zelf, zowel servers als werkstations, dienen host-based firewalls te worden aangebracht, zoals in de paragraaf over de analyse van eisen reeds is gesteld. Aangezien de capaciteit van het Internet de laatste tijd zo'n enorme

groei heeft doorgemaakt en zelfs voor alledaagse toepassingen zoals telefonie in de lift zit, ligt het voor de hand om geen permanente verbindingen meer te nemen voor dit doel. Voor nagenoeg elke toepassing heeft men in de toekomst 'all-IP netwerken' op het oog. In het overleg met de architecten van het operationele platform vindt deze gedachte ook steeds meer voedingsbodem. SSL lijkt dan de beste oplossing als versleuteling van alle externe verbindingen.

9.3 Infrastructuur

Middels de logisch/schematische weergave van de applicatieopbouw uit paragraaf 6.11, is te komen tot een fysiek ontwerp aangaande de infrastructuur.

De link met de infrastructuur
De opdeling maakt het mogelijk data en verwerking van de applicatie los te koppelen van de communicatie met de gebruiker en deze op een goed beschermd gedeelte van het netwerk te plaatsen. Alleen de communicatielaag hoeft op een plaats te komen waar een eindgebruiker toegang toe heeft. Om in termen van de hieronder beschreven infrastructuur te praten plaatsen we de datalaag op de zone RESTRICTED, de bedrijfslaag op de zone INNER en de communicatielaag op de zone OUTER.
Tussen elke zone kunnen vervolgens beperkingen worden opgelegd aan de communicatie die toegestaan is. Globale indeling geeft figuur 14 weer. In de bijlage (bijlage 2) is een gedetailleerde figuur opgenomen.



Figuur 14 Schematisch weergave beveiligingszones

10 Security Architectuur Advies

10.1 Algemeen

Om een oplossing aan te bieden, dient een aantal uitgangspunten en aannames gedefinieerd te worden:

- Huisartsen/Apothekers toegang bieden tot X/Care middels Horizon;
- De toegang dient secure te zijn (versleutelde data);
- Aanbieden van de Horizon webserver mag de integrale beveiliging niet negatief beïnvloeden;
- Gebruik maken van de reeds aanwezige Checkpoint Firewall;
- Gebruik maken van de Internet toegangsmogelijkheden via E-VPN van KPN.

Uitgangspunt voor het maken van dit voorstel is huisartsen en apothekers toegang te bieden tot de interne Horizon webapplicatie, de web front-end voor X/Care. Hierbij dient de functionaliteit van de huidige Horizon webserver niet aangepast te worden. Het is alleen noodzakelijk om op de webserver SSL te configureren.

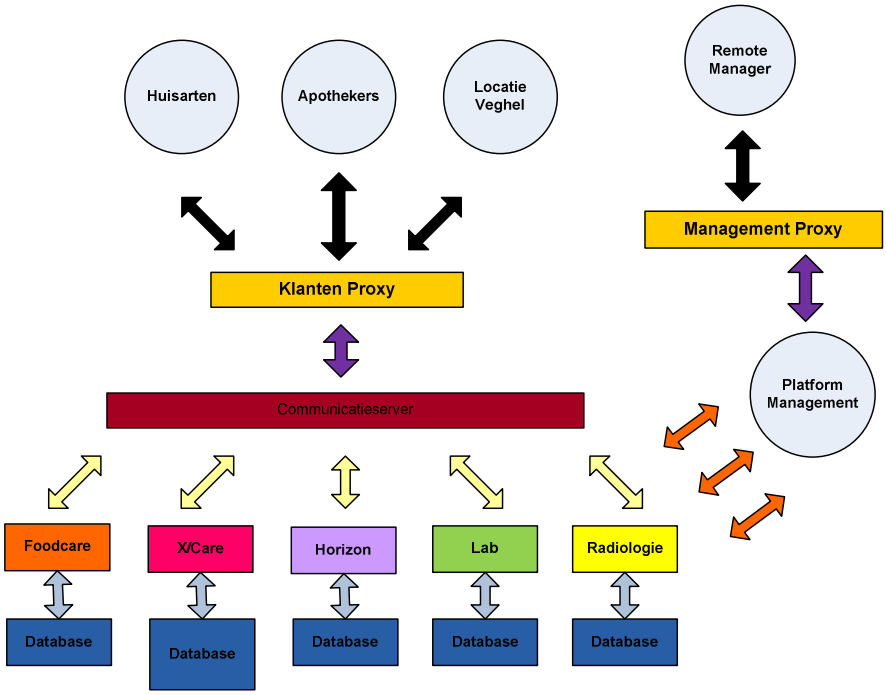
De interne webserver zal niet rechtstreeks aan het internet gekoppeld worden. Hiervoor worden op de back-end firewall webpublishing rules aangemaakt.
Het heeft altijd de voorkeur om alle webservices die beschikbaar zijn over het internet vanuit een DMZ aan te bieden. In dit DMZ kunnen ook andere webservers geplaatst worden zoals bijvoorbeeld een Citrix Portal Server.

De ISA server in de DMZ verzorgt in dit geval de authenticatie. Hierbij wordt onderscheid gemaakt van waar de cliënt (huisarts) connect (dit kan vanuit intern/extern). Een sessie vanaf het internet vereist echter een extra authenticatie middels een hardware token. In beide gevallen wordt overigens wel gebruik gemaakt van SSL.

Voor de authenticatie wordt in het LAN een authenticatie server geplaatst, met daarin een eigen user database. Er wordt geen gebruik gemaakt van de user store (Active Directory) van het ZB. Dit is ook niet nodig en niet gewenst aangezien de huisartsen geen actieve gebruikers zijn op het interne netwerk van ZB. De huisartsen behoeven alleen toegang tot de Horizon webserver met de daarop beschikbare gegevens.

10.2 Applicatie Architectuur

De applicatie-architectuur wordt weergegeven in de volgende figuur. In deze figuur 15 zijn ook de informatiestromen geïntegreerd.



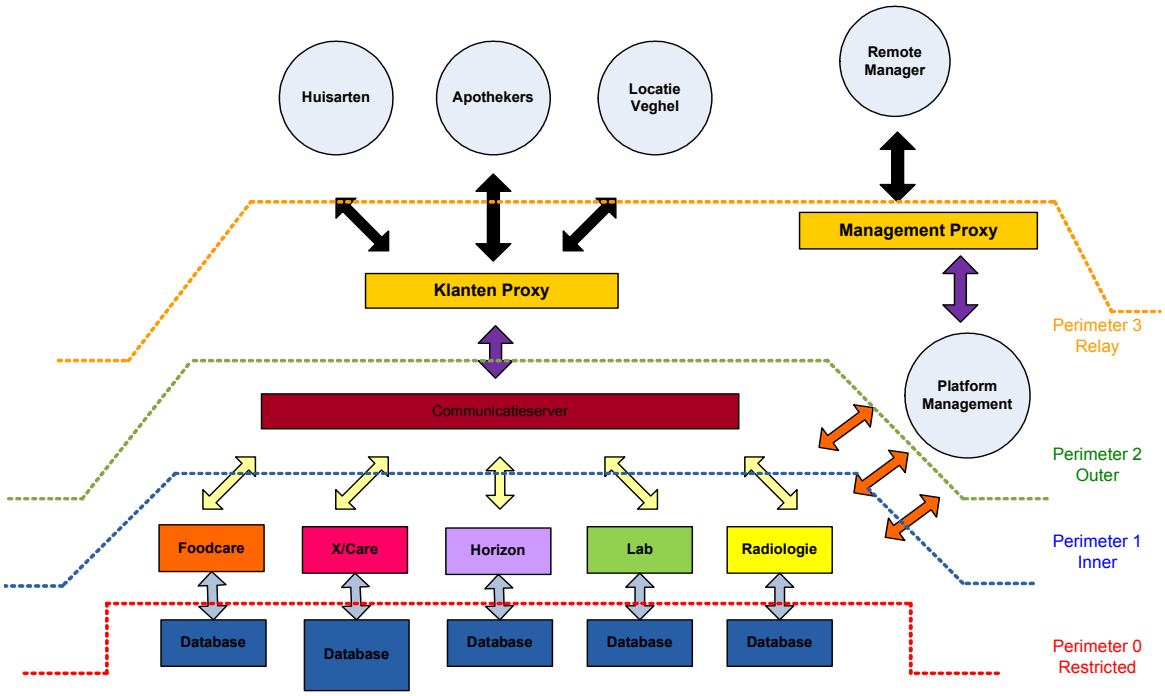
Figuur 15

De zwarte pijlen geven het contact tussen het externe en interne netwerk van ZB aan. De oranje pijlen geven Platformmanagementactiviteiten/contacten aan. De gele pijlen vertegenwoordigen een interface tussen de communicaties server de ZIS applicaties. De paarse pijlen zijn bedoeld om de kern van het ZIS platform te verbinden met de Proxy-omgeving.

10.2.1 Het concept

Het defense-in-depth concept is al duidelijk herkenbaar in figuur 15 uit de vorige paragraaf. Huisarten/apothekers eindigen met hun sessies op een Klanten Proxy, Remote Managers op een Management Proxy. Niemand mag vanuit exteren omgeving rechtstreeks contact maken of berichten sturen naar de Horizon website. Het enige systeem dat heeft op de backup zijn de interne applicaties.

Met betrekking tot het hele ZIS systeem wordt gesteld dat geen enkel proces meer dan één perimeter mag passeren in het contact met een ander proces.



Figuur 16

10.2.2 Perimeterbeveiliging

Op elke perimeter staat een router om een grens tussen de netwerkdelen External – Relay – Outer – Inner – Restricted van elkaar te scheiden. De perimeters worden beveiligd met Stateful Firewalls, al of niet in de routers aangebracht. In principe wordt binnen Perimeter 3 niet met openbare, maar met privé-adressering gewerkt.

Tussen External en Relay wordt een Intrusion Prevention systeem aangebracht, dat in geval van nood (bijvoorbeeld een grootscheepse aanval op het eBusiness Platform) het hele netwerk kan afkoppelen.

In elk van de netwerkdelen Outer, Inner en Restricted wordt een Honeypot en een Intrusion Detection System geplaatst. De Honeypot moet aanvallen uitlokken zoals illegale sessies van binnen en van buiten. Verder zal deze maatregelen nemen voordat de interne servers bereikt kunne worden.

Het Intrusion Detection System moet het verkeer op het netwerk monitoren en bij verdachte activiteiten dit melden aan Platform Management. Teven dienen daarnaast de noodzakelijke logging-activiteiten te worden uitgevoerd.

10.3 Oplossing

Gezien het feit dat er SSL wordt toegepast om Horizon te publiceren aan het internet, is het nodig een certificaat te installeren op de webserver.

Dit certificaat is te gebruiken voor een geheel domein; derhalve is het niet nodig voor elke webserver een apart certificaat aan te schaffen.

Als front-end firewall zal de bestaande Checkpoint Firewall worden ingezet. Deze firewall zal wel enige configuratie behoeven.

Als back-end firewall worden de volgende producten aangeboden:
- HP ProLiant DL360R05 server met o.a. een dual core processor, 2 GB geheugen, twee 36 GB disken en een redundante power supply;
- Windows Server 2003 licentie;
- ISA licentie.

Voor de authenticatie bieden wordt het product PremierAccess van Secure Computing aangeboden. Met dit product is het mogelijk een eigen user database te creëren.
Verder wordt Safeword PremierAccess aangeboden voor 30 gebruikers, inclusief 30 Silver tokens en bijbehorend support.

Voor PremierAccess is een extra server benodigd waarop de software geïnstalleerd kan worden. Hiervoor worden de volgende producten aangeboden:

- HP ProLiant DL360R05 server met o.a. een dual core processor, 2 GB geheugen, twee 36 GB disken en een redundante power supply;
- Windows Server 2003 licentie.

11 Conclusies en aanbevelingen

Omdat de implementatie een deel uitmaakt van het project zijn mijn adviezen verwerkt binnen dit verslag. Toekomstige aanbevelingen zijn:

- Investering tweede SAN, verhoging van beschikbaarheid in geval van calamiteiten;
- Uitsplitsen hardware, verdelen van bedrijfskritische systemen over meerdere locaties;

12 Evaluatie

Het kunnen inleven in de problematiek van de klant en dit te vertalen naar mogelijke oplossing heeft zeker mijn belangstelling. Gedurende dit project heeft de rol van projectleider mijn interesse gewekt.

Tijdens het project ben ik begonnen met het schrijven van mijn scriptie, dit is een ieder aan te raden. Ook veelvuldig contact met je begeleiders biedt veel voordelen. Zij interpreteren je gemaakte verslag soms nog iets anders. Je begint op dat moment echt woorden te wegen. Wat wil ik eigenlijk zeggen? Hoe krijg ik dit verwoord op papier. Wie is mijn eindgebruiker?

Nu ik aan het einde ben gekomen van deze scriptie hoop ik mijn opleiding af te ronden. Mijn interesse gaat echter verder, waardoor ik mij ga oriënteren op nieuwe mogelijkheden na deze opleiding.

Jaap Groeneveld

13 Literatuurlijst

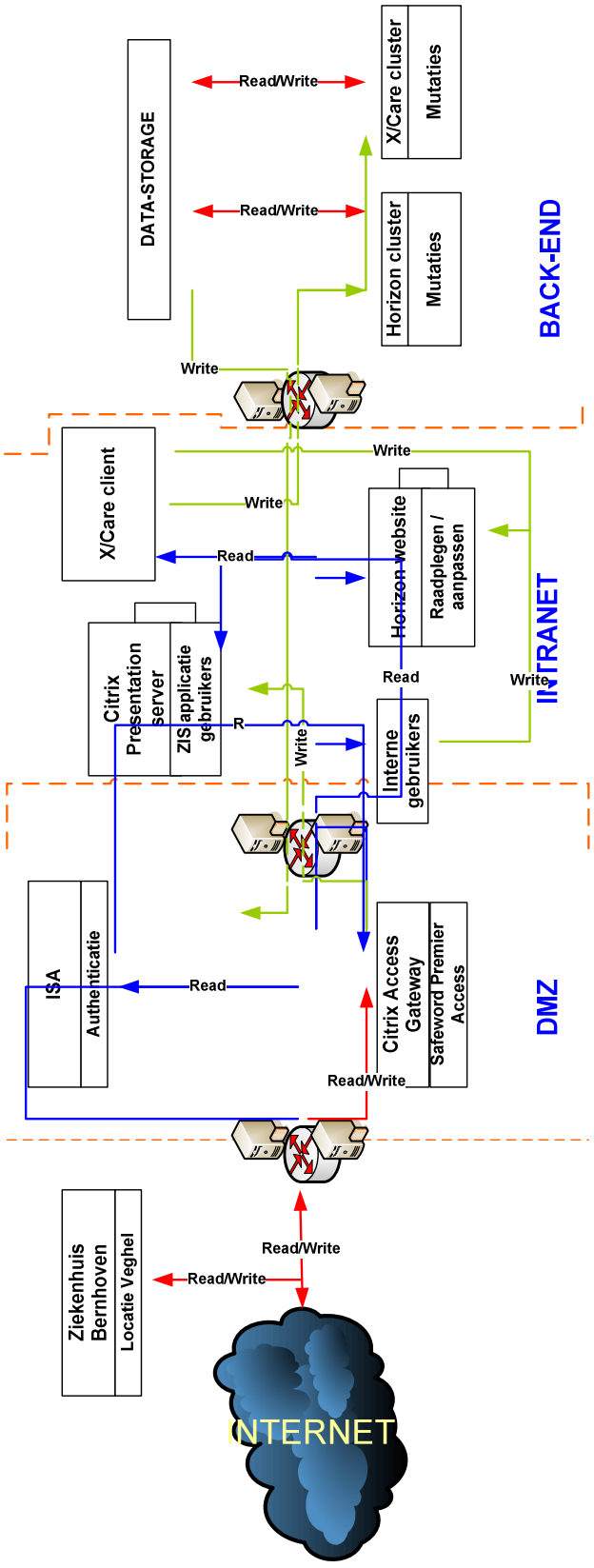
- James D. McCabe, ISBN 9781558608870, Network Analysis, Architecture, and Design;
- Windows Server 2003, Network Infrastructure;
- http://www.mckesson.nl;
- www.hp.com/storage;
- http://www.prince2.com/.

Bijlage 1 Planning

Actie	Actie omschrijving Taken	Actiehouder	Planning Start	 Gereed
Algemeen				
Projectleiding				
	Project plan	PK/JG	2-jan	16-jan
	Actielijst	PK	2-jan	20-jan
	Planning	PK/JG	2-jan	31-aug
Overleg				
	Project overleg	Allen	29-dec	29-dec
Voorbereiding				
Inventarisatie				
	Serverruimte	PK	12-jan	12-jan
	Stroomvoorziening	PK	12-jan	12-jan
	Doorgang van buiten tot aan serverruimte	PK	12-jan	12-jan
-	Type aansluiting voor FC connecties 2e ruimte	PK	12-jan	12-jan
-	Inventarisatie McKesson huidige omgeving X/Care	PK	12-jan	
-	Ondertekend Projectplan			
-				
Ontwerp				
	Functioneel Ontwerp	LT		
	Migratieplan	LT		
	Acceptatieplan	PK / JG		
Implementatie				
Bestellingen				
	HW bestellen	VCD	week 2	week 6/7
	2x RX4640 (tbv. X/Care + Beaufort)	VCD	week 2	week 6/7
	1x HW bestaande DL360 (tbv. management appliance)	VCD	week 2	week 6/7
	2x HW bestaande DL360 (tbv. cluster Horizon)	VCD	week 2	week 6/7
	2x HW bestaande DL380 (tbv. batchdaemon)	VCD	week 2	week 6/7
	2x HW bestaande DL380 (tbv. Foodcare)	VCD	week 2	week 6/7
	1x EVA4000 + SAN infrastructuur	VCD	week 2	week 6/7
	1x VLS6109	VCD	week 2	week 6/7
	1x MSL6030	VCD	week 2	week 6/7
	1x Dataprotector (SAN backup licenties)	VCD	week 2	week 6/7
	2x UPS	VCD	week 2	week 6/7
Basisinstallatie				
	SAN infrastructuur	LT / JG	week 7	week 9
	EVA4000	LT / JG	week 7	week 9
	1x Management Appliance	LT / JG	week 7	week 9
	2x RX4640	LT / JG	week 8	week 9
	2x Horizon (cluster)	PB/JG	week 7	week 9
	2x Batchdaemon (geen cluster)	PB/JG	week 8	week 9
	2x Foodcare (geen cluster)	PB/JG	week 8	week 9
	1x VLS 6109	LT	week 8	week 9
	1x MSL6030	LT	week 8	week 9
	2x UPS	LT / JG	week 8	week 9
Klantspecifieke configuratie				
	2x RX4640	PB/JT	week 10	

	1x Management Appliance	PB/JT	week 10	
	1x VLS 6109	LT	week 10	
	1x MSL6030	PB/JT	week 10	
	1x Dataprotector + backupschema	PB/JT	week 10	week 14
	Installatie Oracle + Oracle Failsafe + X/Care	McKesson	week 10	
	Intallatie batch-/connectdaemon	McKesson	week 10	
	Installatie RMAN	McKesson	week 10	
	Inrichting backup X/Care	McK / VCD	week 10	
	proef Migratie X/Care naar nieuwe cluster	McKesson		
	Installatie Foodcare op Windows omgeving	McKesson		
	Migratie Foodcare	McKesson		
	Inrichting backup Foodcare	McK / VCD		
	Installatie Horizon op Windows omgeving	McKesson		
	Migratie Horizon naar nieuwe omgeving	McKesson		
	Inrichting backup Horizon	McK / VCD		
Ingebruikname, Nazorg en Evaluatie				
Orderafsluiting				
	Evaluatie	Allen		
	Acceptatie door klant	ZB / VCD		
	Nazorg	ZB / VCD		

Bijlage 2 Infrastructuur



Bijlage 3 Rackindeling