ICT Infrastructuur gemeente Eemsdelta

Datum: februari 2022
Auteur(s): Marko Overzet
Versie: 13.0

Inhoud

Inleiding
De ICT infrastructuur van de gemeente Eemsdelta is gehuisvest in twee datacenters. Beide datacenters bevinden zich in Groningen. Eén van de datacenters is gevestigd op het bedrijventerrein Westpoort en de andere aan de Zernikelaan.

Netwerk
De bestaande gemeentehuizen van Appingedam, Delfzijl en Loppersum zijn met 1Gb glasverbindingen met elkaar en beide datacenters verbonden.

Beide datacenters zijn middels een redundante 10Gb verbinding met elkaar verbonden.

Het bekabelde netwerk heeft een 1Gb ontsluiting naar het internet. Het Wifi netwerk dat op de drie gemeentehuizen aanwezig is, heeft een 400Mb internetverbinding. Dit Wifi netwerk is fysiek gescheiden van het bekabelde netwerk.

Servers
Het virtualisatieplatform, gebaseerd op technologie van VMware, is ondergebracht in het datacenter en is verdeeld in twee VMware clusters:
- Frontend voor de hosting van de virtuele Citrix Farm.
- Backend voor de hosting van de applicatieservers.

Alle storage wordt via VMware gekoppeld aan de vm's. Er wordt geen directe koppeling vanuit vm's aan storage shares toegestaan. Dit onder meer vanwege de back-up tool die gebruikt wordt voor het veiligstellen van de omgeving. Alle applicatieservers moeten middels VMware worden gevirtualiseerd op de bestaande infrastructuur. Het plaatsen van fysieke servers is niet toegestaan.

Operating systemen
De standaard operating system voor de kantooromgeving is Microsoft Windows. Op de applicatieservers en de Citrix servers is de standaard Windows 2016.
De autorisaties zijn geregeld via Active Directory. Er is één forest en één domein voor alle gebruikers. Voor mail, agenda en dergelijke wordt gebruik gemaakt van een hybride Exchange omgeving (Exchange Online met een on-premise Exchange 2016). De laatste zorgt mede voor de mailroutering naar het zogenaamde SuwiNet. Alle gebruikers vallen onder één Exchange omgeving.

Databases
De Aanbestedende Dienst heeft een nadrukkelijk SAAS, tenzij beleid, maar biedt in haar datacenter ruimte en capaciteit voor on-premise oplossingen. On-premise applicaties kunnen op het bestaande virtualisatieplatform worden geïnstalleerd. Over de sizing van applicatieservers dient vooraf afstemming plaats te vinden. Voor eventuele databases hebben we alleen de beschikking over een Microsoft SQL en een PostgreSQL server. De Aanbestedende Dienst heeft de ambitie om een variëteit aan databasesystemen sterk te beperken. Niet Microsoft SQL en PostgreSQL databases dient de inschrijver op een door haarzelf, of door een derde, beheerde omgeving te installeren. Deze kosten zoals bijvoorbeeld hardware, beheer, verbindingen en licentiekosten, dienen in de aangeboden prijs verdisconteerd te zijn.

Datagedreven werken

Om beter onderbouwde beslissingen te nemen en als organisatie beter aan te sluiten op de maatschappelijke opgaven, zet de gemeente Eemsdelta in op datagedreven werken. Voor het presenteren van analyses wordt gebruik gemaakt van Power BI dashboards. Applicaties, SAAS en on premise, die gebruik maken van een database, bieden de mogelijkheid om op gezette tijden (dagelijks, wekelijks) een extract van de database te maken naar een csv-bestand die vervolgens kan worden ingelezen in Azure Data Factory. Het maken van het database extract en het plaatsen van het csv-bestand op een on premise locatie wordt middels een geautomatiseerd proces uitgevoerd.

Werkstation omgeving

Er wordt gebruik gemaakt van Citrix XenApp en Ivanti Workspace Control, toegankelijk vanaf thin clients.
De Windows Server versie op de XenApp servers is Windows 2016. Voor de applicatievirtualisatie wordt gebruik gemaakt van Microsoft AppV.
Het momenteel gebruikte office pakket is de 32-bits versie van Microsoft Office ProPlus. Voor mail wordt gebruik gemaakt van de Outlook client.
Voor printen wordt een Ricoh Follow Me print-service ter beschikking gesteld waarbij het mogelijk is om prints in een wachtrij te plaatsen en vervolgens op één van de beschikbare Follow Me printers via een authenticatie op te roepen en af te drukken. De printers kunnen allemaal A4 en A3 in kleur en grijstinten, enkel of dubbelzijdig printen.
Als antivirus programma wordt op alle servers Sophos Endpoint Security and Control toegepast.
Gebruikers kunnen het internet alleen benaderen via web-proxy servers en firewalls. Het is niet toegestaan om vanaf servers of desktopomgevingen rechtstreeks verbinding met servers op het internet te maken.
Gebruikers kunnen vanaf mobile werkstations (laptops, tablets, smartphones) mail uitwisselen met de Exchange Online oplossing en verbinding maken met de Citrix Netscaler en vervolgens hun desktop omgeving benaderen. Dit laatste werkt via two-factor authenticatie. Mobile werkstations maken via een Wifi-netwerk verbinding met het internet. Mobiel werkstations hebben geen bekabelde verbinding met het interne netwerk.

Remote support

Het is mogelijk om middels Teamviewer vanaf de leverancier een sessie naar een zogenaamde inbelmachine te krijgen. Vanaf deze inbelmachine wordt toegang naar de applicatieserver verzorgd. Inbellen gaat altijd in overleg met de applicatiebeheerder en, indien de applicatiebeheerder akkoord is, via de ICT servicedesk van de gemeente Eemsdelta.

Privacy by design

Met de aanschaf van (nieuwe) technologieën en applicaties is het van belang dat Privacy by Design en Privacy by Default wordt toegepast. Onderstaand is de checklist die wordt gebruikt bij de aanschaf van die (nieuwe) technologieën en applicaties.

A. De basis: Privacy by Design bestaat uit de volgende zeven grondbeginselen:

1. **Proactief, niet reactief; Preventief, niet corrigerend**
   Privacy by design voorkomt en anticipeert in een vroeg stadium op inbreuken voordat deze zich voordoen. Dit, in plaats van te wachten op het zich voordoen van privacyrisico's. Standaard zijn privacycontroles onderdeel van de systeemtechnische vereisten. Ze worden getest op effectiviteit en continu gecontroleerd.
2. **Privacy als standaard**
   Wanneer privacy als standaard wordt gebruikt, hoeven gebruikers geen actie te ondernemen om hun privacy te behouden; het is standaard in het systeem ingebouwd.
3. **Privacy ingebed in ontwerp**
   Privacy is een essentieel onderdeel van de kernfunctionaliteit die wordt ontworpen en geleverd. Bedrijven dienen de privacy van consumenten in de hele organisatie en in elke fase van productontwikkeling te bevorderen.
4. **Volledige functionaliteit-positieve som, geen nulsom**
   Privacy by Design probeert tegemoet te komen aan alle legitieme belangen en doelstellingen van zowel gebruikers als leveranciers, in plaats van onnodige compromissen te sluiten.
5. **End-to-end beveiliging - volledige levenscyclusbescherming**
   Sterke beveiligingsmaatregelen zijn essentieel voor privacy, van begin tot eind van de levenscyclus van (persoons)gegevens. Dit houdt in dat privacycontroles in systemen en applicaties worden geplaatst, ze worden gecontroleerd op naleving van de regelgeving en worden geëvalueerd wanneer nieuwe bedreigingen voor informatiesystemen worden ontdekt.
6. **Zichtbaarheid en transparantie**
   Componenten en bewerkingen blijven in de geleverde technologie zichtbaar en transparant voor zowel gebruikers als providers. Zichtbaarheid en transparantie zijn essentieel om verantwoording en vertrouwen te creëren.
7. **Respect voor de privacy van gebruikers**
   Privacy by Design vereist dat de belangen van het individu worden gewaarborgd door het aanbieden van maatregelen zoals strenge privacy-standaardwaarden, passende kennisgeving en het verlenen van gebruiksvriendelijke opties. Privacy- en beveiligingsopties kunnen op transparante wijze naast elkaar bestaan voor een gebruiker. Ze verminderen niet de noodzakelijke autorisaties voor toegang tot gegevens. De bescherming van organisatorische informatiemiddelen is mogelijk zonder onnodige afwegingen.

Definitie SAAS

De gemeente Eemsdelta heeft gekozen voor een SAAS, tenzij beleid bij de aanschaf van nieuwe applicaties. De definitie, afgezien van specifieke functionele eisen, die de gemeente Eemsdelta voor SAAS hanteert is als volgt:

Algemeen

- Voor het gebruik van de oplossing volstaat de webbrowser Edge Chromium. De browser is qua versie/updates maximaal 1 jaar oud en ondersteund door de ontwikkelaar van de browser.
- Gebruik van een plug-in (o.a. Java/Flash/Silverlight) is in verband met informatieveiligheid, beheer en onderhoud niet toegestaan.
- Er is geen installatie van software(componenten) nodig om de oplossing te kunnen gebruiken. Een uitzondering hierop is de eventuele installatie van software die zorgdraagt voor beveiligde gegevensuitwisseling tussen de on premise omgeving en de SAAS oplossing. Deze software voldoet aan de onderstaande eisen:
    - Indien de applicatie op de werkplek (XenApp server) wordt aangeboden, is de applicatie multi-user aware, compatible met Citrix XenApp en Ivanti Workspace Control en draait deze niet als een Windows service.
    - De gegevensuitwisseling is versleutelt.
- Onder een eindgebruiker worden alle gebruikers verstaan die gebruik maken van de SAAS oplossing.
- De oplossing draait volledig in het datacenter van de opdrachtnemer.
- De leverancier zorgt er voor dat de opdrachtgever geen last heeft van onwenselijk gedrag van andere klanten. (Bijv. spamming vanuit eenzelfde ip-adres)
- De leverancier zorgt er voor dat het netwerkverkeer tussen de verschillende omgevingen niet kan worden onderschept door andere klanten die actief zijn binnen de systeemomgevingen van de leverancier.
- De leverancier voorkomt dat gebruik van gedeelde componenten door andere klanten in de infrastructuur de performance bedreigen.
- De oplossing behoort in een werkende productiefase een acceptabele performance te vertonen voor circa 100 gelijktijdige gebruikers. Dat is inclusief het openen van documenten van 8MB en het tonen van complexe zoekacties. De opdrachtgever beseft dat een acceptabele performance niet altijd direct kan worden vastgesteld middels cijfers, maar ook afhankelijk is van de belevenis van de gebruikers.
- Overschakelen tussen schermen en overzichten binnen de applicatie duren niet langer dan 1 seconde. Het opstarten van de applicatie na inloggen gebeurt binnen 3 seconden.
- De dienstverlening voldoet aan de ISAE 3402 normering.

Authenticatie

Authenticatie verloopt via lokale, on-premise Active Directory. Dit op basis van SAML 2.0 en ADFS 3.0. Tevens is authenticatie op basis van een Kerberos ticket toegestaan. Kosten hiervan zijn volledig inbegrepen in de aanbieding.
Na authenticatie via de Active Directory hebben gebruikers door middel van Single Sign On (SSO) direct toegang tot alle onderdelen van de oplossing. Uiteraard voor zover ze daartoe zijn geautoriseerd. Met SSO hoeft de gebruiker niet apart in de loggen in de oplossing nadat de gebruiker is aangemeld op het netwerk (via Active Directory).
Alleen om specifieke functioneel beheer-rechten te krijgen is het toegestaan dat er een handmatige login nodig is.

Beveiliging en privacy

Geboden oplossingen voldoen aan de beveiligingseisen die in de Baseline Informatiebeveiliging Overheid (BIO) en de GIBIT worden gesteld, zoals (niet-limitatief):

- Toe te passen ICT-kwaliteitsnormen, interoperabiliteitseisen en standaarden (artikel 6 GIBIT).
- Het hebben van een acceptatieprocedure (artikel 7 GIBIT).
- Aansprakelijkheid (artikel 13 GIBIT).
- Geheimhouding (artikel 15 GIBIT).
- Toegang tot data en autorisaties (artikel 18 GIBIT).
- Controlerecht en medewerking bij audits (artikel 21 GIBIT).
- Exitplan en -scenario (artikel 22 GIBIT).
- Verwerkersrelatie, in de zin van de AVG (artikel 24 GIBIT).
- Verwerking persoonsgegevens (artikel 25 GIBIT).
- Informatiebeveiliging(sniveau) (artikel 26 GIBIT).
- Meldplicht informatiebeveiligingsincidenten (artikel 27 GIBIT).
- Waarborging continuïteit, waaronder data-escrow (artikel 32 GIBIT).
- Gegevens die van een naar het systeem worden getransporteerd, in welke vorm dan ook, dienen beveiligd te worden door middel van encryptie. Hierbij dient gebruik te worden gemaakt van het SSL protocol op basis van TLS 1.2 of beter of gelijkwaardig. Cypher suites die conform NCSC TLS richtlijnen[1] "goed" scoren zijn toegestaan.
- Gegevens binnen het systeem dienen versleuteld opgeslagen te worden waarbij minimaal gebruik wordt gemaakt van AES-256.
- Bij het opslaan van wachtwoorden is hashing en salting gebruikt.
- Binnen de OTA-omgevingen wordt geen gebruik gemaakt van productie data. De leverancier faciliteert test data via scripts of andere wijze zodat gegevens niet herleidbaar zijn naar bijvoorbeeld personen.
- Applicaties worden ontwikkeld en getest op basis van landelijke normen en richtlijnen voor beveiliging, zoals de richtlijnen voor beveiliging van webapplicaties. Er wordt tenminste getest op bekende kwetsbaarheden zoals vastgelegd in de Open Web Application Security Project (OWASP) top 10[2].
- Alle netwerkverkeer verloopt via https (waar relevant).
- Op het moment van ingebruikname in productie, dienen alle standaard wachtwoorden (waaronder administrator) aangepast te worden.
- Een actieve sessie met de software heeft een timeout van maximaal 15 minuten. Na deze periode moet de sessie worden afgebroken.
- De infrastructuur en organisatie van de opdrachtnemer zijn adequaat beveiligd volgens ISO/IEC 27001 of vergelijkbaar en voldoen aan de voorwaarden genoemd in de Algemene Verordening Gegevensbescherming (AVG). De opdrachtnemer verzorgt jaarlijks via een onafhankelijke derde partij, een verklaring van getrouwheid (of vergelijkbaar) om aan te tonen dat zij als contractant veilig omgaat met vertrouwelijke informatie.
- De opslag en verwerking van gegevens vindt plaats binnen Nederland en alle infrastructuur bevindt zich fysiek in een datacenter in Nederland.
- De oplossing ondersteunt DNSSEC voor de webservices.
- De opdrachtnemer zal indien hij (pogingen tot) ongeautoriseerde toegang tot de systeemomgeving signaleert, alle noodzakelijke maatregelen nemen teneinde de eventuele schade tot een minimum te beperken en herhaling te voorkomen. De poging tot ongeautoriseerde toegang alsmede alle getroffen maatregelen zullen binnen 5 werkdagen aan de opdrachtgever worden gerapporteerd. Ongeautoriseerde toegang alsmede getroffen maatregelen worden meteen aan de opdrachtgever gerapporteerd.
- Systeemsoftware die bij de opdrachtnemer in gebruikt is, wordt up-to-date gehouden. De laatste (beveiligings)patches zijn geïnstalleerd en deze worden volgens een patchmanagement proces doorgevoerd.

[1] https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls

[2] https://owasp.org/www-project-top-ten/

- Alle wijzigingen worden door de opdrachtnemer altijd eerst getest voordat deze in productie worden genomen en worden via een wijzigingsbeheer proces doorgevoerd.
- De opdrachtnemer maakt gebruik van een hardeningsproces zodat alle ICT-componenten zijn gehard tegen aanvallen. Hardening van systemen bestaat uit verschillende stappen om een gelaagde bescherming te bieden. Met behulp van antivirus, -spyware, -spam en -phishing software, regelmatig installeren van de laatste patches van de leverancier, het uitschakelen van onnodige software en diensten leidt tot een beter beschermd systeem dat moeilijker door kwaadwillenden is te misbruiken.
- Er wordt minimaal 1 x per 2 jaar een Black Box Penetratietest[3] uitgevoerd en aan de opdrachtgever gerapporteerd.
- Vulnerability assessments (controles op kwetsbaarheden) worden periodiek uitgevoerd (minimaal 1 x per kwartaal) en aan de opdrachtgever gerapporteerd.

Toegankelijkheid

De gemeente Eemsdelta wil voldoen aan de wettelijke eisen die de overheid stelt aan digitale toegankelijkheid. Bevat uw applicatie een online component, dan voldoet deze aan de WCAG 2.1.

Continuïteit

Onderliggende softwarecomponenten, zoals besturingssystemen, databasesoftware, browser versie, programmeer framework, enz., waarop de software is gebouwd en draait dienen altijd een door de oorspronkelijke leverancier van de betreffende software of framework ondersteund te zijn.

Integraties

- Indien de opdrachtgever er voor kiest om tussen de oplossing en andere systemen basisgegevens uit te wisselen, gebeurt dit conform het sectormodel StUF BG v2.04 of StUF BG v3.10[4]. Indien binnen de looptijd van het contract een nieuwe StUF formaat wordt uitgebracht, dient de opdrachtnemer deze binnen 1 jaar na vaststelling van de nieuwe StUF formaat te ondersteunen.
- De opdrachtnemer waarborgt dat de oplossing niet meer dan één major versie achterloopt ("backwards compatible") op de open standaarden van het Forum Standaardisatie. Daarnaast wordt de oude versie nog minimaal 12 maanden ondersteund.
- Databases zijn volledig toegankelijk voor leesacties (zoals t.b.v. Cognos).

Service Level Agreement (SLA)

- De opdrachtnemer garandeert dat ongeautoriseerde personen geen toegang hebben tot gegevens of gegevensdragers (zoals harde schijven en back-up media) die tussentijds of na beëindiging van de overeenkomst worden verwijderd c.q. worden vervangen.
- Buiten kantooruren, werkdag van 07:30u tot en met 18:00u, is de beschikbaarheid van de oplossing voor minimaal 99,0% per maand gegarandeerd. Tijdens kantooruren is de beschikbaarheid 99,5%, met uitzondering van gepland onderhoud. Gepland onderhoud is altijd buiten kantooruren.
- De opdrachtnemer levert een uitwijkomgeving waardoor real time kan worden uitgeweken naar een andere locatie waarbij tijdens kantooruren, werkdagen van 07:30u tot en met 18:00u, het verlies van gegevens maximaal 2 uur mag bedragen. Deze uitwijkomgeving wordt jaarlijks getest en de resultaten worden naar de opdrachtgever gerapporteerd.
- Er moet een recovery proces zijn ingericht waar back-up en restore een onderdeel vanuit maken. Het verlies van gegevens mag maximaal 2 uur bedragen. De recovery proces wordt jaarlijks getest en de resultaten worden naar de opdrachtgever gerapporteerd.

[3] https://nl.wikipedia.org/wiki/Penetratietest
[4] https://www.gemmaonline.nl/index.php/Sectormodel_Basisgegevens:_StUF-BG#Documenten