Bijlage: ICT uitgangspunten

gemeente DE WOLDEN

Gemeente Hoogeveen

Versie

Versienummer	Datum	Opmerking
Versie 1.0	10 oktober 2023	Initiële versie

Inhoudsopgave

1 Uitgangspunten

In dit hoofdstuk worden de uitgangspunten per verschillende ICT-componenten en aandachtsgebieden beschreven waar de geboden oplossing aan dient te voldoen.

1.1 Algemeen

1.1.1 Security

Binnen SWO de Wolden Hoogeveen zijn veel applicaties welke persoonsgegevens verwerken. Dit maakt dat security een belangrijk aspect is binnen het IT-landschap. Daarbij dient de informatiebeveiliging te voldoen aan de geldende normen.

Uitgangspunt: Informatiebeveiliging dient als onderdeel van de geboden oplossing te voldoen aan de standaarden uit de ISO27001 en BIO richtlijnen, waarbij alvast wordt voorgesorteerd op de invoering van de NIS2 richtlijn;

Uitgangspunt: De geboden oplossing dient eventueel gekoppeld te kunnen worden met een SIEM oplossing;

Uitgangspunt: De geboden oplossing moet kunnen functioneren in een ZERO-trust omgeving;

Uitgangspunt: Bij het leggen van koppelingen, dienen de koppelvlakken minstens gebruik te maken van encryptie op basis van certificaten en minimaal TLS1.2 waarbij TLS 1.3 de voorkeur heeft. Bestandskoppelingen dienen minimaal over SMB 3.0 te communiceren;

1.1.2 Taakverdeling en verantwoordelijkheden

De SWO de Wolden Hoogeveen wil graag volledig ontzorgd worden. Dat betekend dat er verwacht wordt dat beheer van de geboden oplossing door de aanbieder wordt verzorgd. Echter is er wel sprake van gedeelde verantwoordelijkheid waarbij de SWO de Wolden Hoogeveen wel over mogelijkheden wenst te beschikken dagelijks operationeel beheer in eigen beheer uit te kunnen voeren.

Uitgangspunt: De geboden oplossing betreft een volledig ontzorgde oplossing, als onderdeel van de aanbesteding worden duidelijke afspraken gemaakt over beheer en verantwoordelijkheden en welke wijzigingen in eigen beheer doorgevoerd kunnen worden en welke wijzigingen vanuit de aanbieder dienen te worden gemaakt;

1.1.3 RBAC

Binnen de SWO de Wolden Hoogeveen is het wenselijk om toegangsrechten vanuit Rollen te definiëren.

Uitgangspunt: De geboden oplossing dient in te kunnen spelen op Role Based Access Control;

1.2 Netwerk technisch

Binnen de SWO de Wolden Hoogeveen wordt gebruik gemaakt van een gesegmenteerd netwerk. Dat wil zeggen dat verschillende soorten systemen in eigen afgescheiden netwerk/vlan zijn opgenomen. Deze verschillende segmenten zijn van elkaar gescheiden met actieve firewalling (Fortinet), waarbij gebruik gemaakt wordt van IPS en Application Control.

Voor ontsluiting van verschillende toegangen tussen de segmenten wordt gewerkt vanuit een zero-trust principe met een minimalistische aanpak. Vanuit het zero-trust principe wordt dan ook

gehanteerd dat internet per definitie niet vertrouwd is en er daarmee per definitie geen standaard internet toegang voor systemen vanuit de segmenten is toegestaan tenzij dit voor de geboden oplossing van toepassing is.

Uitgangspunt: De geboden oplossing kan in een gesegmenteerde omgeving opereren en heeft een duidelijke specificatie van communicatiepoorten en stromingen welke tussen segmenten verwacht worden;

Uitgangspunt: We verlenen geen directe toegang tot internet tenzij dit voor de werking van de geboden oplossing een vereist is. De oplossing biedt een duidelijke specificatie van welke verschillende communicatiepoorten en stromingen van en naar internet verwacht worden;

Uitgangspunt: Indien de geboden oplossing een server vereist met toegang vanaf het internet, dient deze in een DMZ geplaatst te kunnen worden;

Uitgangspunt: Indien de geboden oplossing op een server met toegang vanaf internet vereist, dient de achterliggende data op het interne netwerk opgeslagen en via segmentatie ontsloten. Er worden geen (potentieel) vertrouwelijke gegevens in de DMZ opgeslagen;

1.3 Applicatielandschap

1.3.1 Cloud

Vanuit SWO de Wolden Hoogeveen is besloten om in te zetten op Cloud, tenzij. Concreet betekend dat er zoveel mogelijk gebruik gemaakt wordt van een oplossing die vanuit de Cloud beschikbaar wordt gesteld of minstens Cloud-Ready zijn. Uitzonderingen zijn mogelijk, maar hebben niet de voorkeur.

Uitgangspunt: De geboden oplossing wordt aangeboden vanuit een SaaS platform en is daarmee als Cloud oplossing beschikbaar of minstens Cloud-Ready. Indien hiervan afgeweken dient te worden, dient dit ook duidelijk beschreven in de specificaties;

Er wordt gebruik gemaakt van Microsoft 365 in combinatie met E3 licenties en Azure Active Directory. Alle medewerkers en groepen worden gesynchroniseerd met Azure Active Directory en zijn daarmee als gebruiker met inloggegevens bekend. Er wordt gebruik gemaakt van Single Sign On met Azure Active Directory.

Uitgangspunt: De geboden oplossing dient bij voorkeur inloggegevens op te halen uit en te koppelen met Azure Active Directory op basis van de Graph API of SAML voor SingleSignOn;

E-mail maakt volledig gebruik van Exchange Online, de mailflow loopt echter nog via een interne Fortimail appliance en wordt van daaruit afgeleverd binnen Exchange Online. Voor het verzenden van e-mail vanuit de domeinen dewoldenhoogeveen.nl, dewolden.nl en hoogeveen.nl wordt gebruik gemaakt van Exchange Online.

Uitgangspunt: De geboden oplossing dient, indien gebruik gemaakt van de mogelijkheid tot sturen van e-mail, gebruik te kunnen maken van e-mail via Exchange Online op basis van integratie met de Graph API;

1.3.2 Testomgeving

Van de omgeving van de SWO de Wolden Hoogeveen draait een geïsoleerde kopie welke voor test en acceptatiedoeleinden gebruikt worden alvorens de wijzigingen in de productieomgeving door te voeren. Elke wijziging dient in een testomgeving getest te worden alvorens deze in productie door te voeren;

Uitgangspunt: De geboden oplossing dient te beschikken over een testomgeving welke periodiek vernieuwd (kan) worden;

Uitgangspunt: Data in de testomgeving dient geanonimiseerd te zijn;

Uitgangspunt: Indien de geboden oplossing nog op een server on-premisse dient te draaien, dient deze licentie technisch te kunnen worden voorzien van een testomgeving;

1.4 Server landschap

1.4.1 Virtualisatie

De IT omgeving van de SWO de Wolden Hoogeveen is volledig gevirtualiseerd. Er wordt gebruik gemaakt van verschillende virtualisatieplatformen voor verschillende doeleinden:

- Nutanix Acropolis Hypervisor: Het primaire virtualisatieplatform waar de omgeving van de SWO de Wolden Hoogeveen op draait;
- vmWare ESXi: vmWare wordt excpliciet gebruikt voor de Oracle servers welke binnen de SWO de Wolden Hoogeveen draaien;
- Citrix XenServer: XenServer is het virtualisatieplatform waar de Citrix XenDesktop omgeving op draait;

Uitgangspunt: Indien de geboden oplossing op een server on-premisse dient te draaien, dient deze op een Nutanix Acropolis Hypervisor, vmWare ESXi of XenServer omgeving ondersteund te worden;

1.4.2 Windows Server

In gebruik binnen de SWO de Wolden Hoogeveen zijn primair Windows Servers, waarbij Windows Server N – 1 (De laatste versie en de voorlaatste versie) de geldende standaard is.

Uitgangspunt: De geboden oplossing, indien deze op een server on-premisse dient te draaien, is deze compatible met Windows Server N-1;

1.4.3 Databases

Binnen de SWO de Wolden Hoogeveen wordt gebruik gemaakt van databases op zowel Microsoft SQL Server als Oracle platform. Van de Oracle omgeving worden versies 19 en 21 ondersteund, waarbij SQL-server de voorkeur kent echter omwille van performance Oracle de voorkeur heeft.

Uitgangspunt: Indien de geboden oplossing op een database server on-premisse dient te draaien, dient deze op een Oracle of Microsoft SQL Server geplaatst te worden. Afstemming hierover met de DBA is een vereiste;

1.5 Managed Werkplek

Gebruikers binnen de SWO de Wolden Hoogeveen benaderen applicaties en systemen vanaf een Managed Werkplek. Deze werkplek wordt gemanaged middels een combinatie van Group Policy en Microsoft Intune. Gebruikers beschikken fysiek over een laptop, er wordt echter op enkele uitzonderlijke situaties nog gebruik gemaakt van een Thin Client of mini desktop PC. Standaard besturingssysteem is Windows 10.

Applicaties kunnen daarmee lokaal beschikbaar gesteld worden als installatie op de werkplek.

Er draait nog een Citrix XenDesktop omgeving waar een selecte groep gebruikers nog op inlogt, echter is het uitgangspunt om deze uit te faseren.

Uitgangspunt: Indien de geboden oplossing een installatie op de werkplek bevat, dient deze compatible te zijn met ten minste Windows 10;

Uitgangspunt: Indien de geboden oplossing een installatie op de werkplek bevat, dient deze bij voorkeur via Microsoft Intune gedistribueerd te kunnen worden;

Uitgangspunt: Er wordt geen gebruik gemaakt van XenDesktop voor het aanbieden van de geboden oplossing aan de eindgebruiker;

Toegang tot verschillende achterliggende systemen, zoals database servers en applicatieservers welke nog on-premisse blijven draaien worden via de werkplek ontsloten via een VPN-verbinding met de server-omgeving.

Uitgangspunt: Indien de geboden oplossing een installatie op de werkplek bevat en deze gebruik maakt van data op on-premisse geïnstalleerde applicatie/databaseservers, dient deze het gebruik van een VPN-verbinding te ondersteunen en hier voldoende performance op te bieden;