

ICT-OMGEVING BAR-ORGANISATIE

Colofon

Naam document

ICT-omgeving BAR-Organisatie

Versienummer

1.6 DRAFT

Versiedatum

Augustus 2021

Versiebeheer

Het beheer van dit document berust bij de Team OPD

Copyright

© 2021 GR BAR-Organisatie

Alle rechten voorbehouden. Verveelvoudiging, verspreiding en gebruik van deze uitgave voor het doel zoals vermeld in deze uitgave is met bronvermelding toegestaan voor alle gemeenten en overheidsorganisaties.

Inhoud

Inhoud	3
1 Algemene beschrijving ICT-omgeving	4
2 Specificaties	5
2.1 Infrastructuur	5
2.1.1 LAN	5
2.1.2 WLAN	5
2.1.3 GEMNET / GGI-Netwerk	5
2.1.4 WAN (ISP)	5
2.2 Servers	5
2.3 Databases	5
2.4 Email (SMTP)	5
2.5 Werkplek	6
2.6 Applicatie Omgevingen (Servers)	6
2.6.1 Ontsluiting vanaf het internet:	6
2.6.2 Ontsluiting naar het internet:	6
2.6.3 Ontsluiting Intern	6
2.6.4 Gebruikers authenticatie/authorisatie	6
2.7 Applicatie architectuur	7
2.8 Remote Toegang voor leveranciers	7
2.9 SaaS specifieke eisen:	7
2.9.1 Ontsluiting via GEMNET / GGI-Netwerk	7
2.9.2 Ontsluiting vanaf het internet:	7
2.9.3 Gebruikers authenticatie/authorisatie	7
2.9.4 Email: (SMTP)	7
2.9.5 Koppeling met interne applicaties:	7

1 Algemene beschrijving ICT-omgeving

De BAR-Organisatie heeft een compleet redundante infrastructuur in eigen beheer en ondergebracht in eigen voorzieningen. Uitgangspunt hierbij is dat alle hardware verdeeld staat over de twee actieve datacenters. Basis uitgangspunt is dat voor alle onderdelen er een volledige uitwijk mogelijk moet zijn. Onderling zijn de (hoofd) vestigingen met elkaar verbonden via een eigen glasvezelring (dark fiber). In het netwerk wordt gebruik gemaakt van vlan's. De algemene netwerkinfrastructuur is gebaseerd op ethernet en minimaal CAT 5E voor UTP. Er is een Microsoft Windows Active Directory domein waar alle bestaande resources in zijn ondergebracht.

In de omgeving wordt gebruik gemaakt van Microsoft Hyper-V (2019) als hypervisor. Het standaard besturingssysteem software is Windows Server 2019. Als standaard database platform maakt de BAR-Organisatie gebruik van Oracle V19 op Linux Red Hat (V8).

Het netwerk is dagelijks in gebruik voor meer dan 1.350 eindgebruikers. Medewerkers hebben op de werkplek alleen de rechten op het niveau van "gebruiker"

Als werkplek hebben alle gebruikers zowel intern als extern toegang tot de "BAR-Workspace". Dit is een centrale oplossing gebaseerd op Windows 2019 Remote Desktop Server in combinatie met Ivanti Workspace manager. Daarnaast hebben de medewerkers de beschikking over een persoonlijke laptop of desktop (Windows 10) die eveneens rechtstreeks toegang geeft tot de netwerkomgeving zonder gebruik te maken van de BAR-Workspace. Deze is als los device te gebruiken alsmede zijn op de bureaus voorzieningen beschikbaar om door middel van Displaylink een externe monitor, toetsenboard en muis aan te sluiten. Binnen de kantooromgeving wordt als software gebruik gemaakt van MS Office 2016 op Windows 10 en Microsoft Edge/Firefox 87.0 (of hoger).

De BAR-Organisatie heeft een Cloud-beleid. Nieuwe toepassingen worden door de BAR-Organisatie als SaaS oplossing bij een leverancier afgenomen. Daarnaast zullen bestaande software de komende jaren gaan migreren naar SaaS.

Voor ondersteuning door de leverancier heeft de BAR-Organisatie de voorkeur dat bij werkzaamheden aan de oplossing dit op locatie zal plaatsvinden. Voor ondersteuning op afstand bij calamiteiten kan remote toegang gegeven worden.

De hieronder beschreven onderdelen en eigenschappen dienen als "eisen" te worden gelezen. Verder zijn ook de GIBIT 2020 (incl. ICT-kwaliteitsnormen) en het uitvoeren van een DPIA van toepassing.

2 Specificaties

2.1 Infrastructuur

2.1.1 LAN

De Gemeentehuizen de Gemeenten Albrandswaard, Barendrecht en Ridderkerk zijn via redundant glasvezelnetwerk met elkaar verbonden.

1 GB Switched UTP Netwerk (Ethernet, TCP/IP) met minimal CAT 5e bekabeling.

De cliënt switches in het netwerk zijn via minimaal één 1 GB-(glasvezel-)verbinding verbonden met een core-switch. Een aantal kleinere externe locaties zijn met glasvezel (100 MB), Dial-up VPN verbonden met het LAN.

2.1.2 WLAN

Gebouwdekkende Wifi Infrastructuur (minimaal) op basis van 802.11b/g/n

2.1.3 GEMNET / GGI-Netwerk

De BAR-Organisatie is redundant aangesloten op het GGI-Netwerk.

GEMNET wordt 2022 uitgefaseerd.

2.1.4 WAN (ISP)

(geografisch gescheiden) Redundante Internet verbinding op basis van IPv4, voorzien van HA firewall met IPS. (Externe IPv6 ondersteuning Q4 2021)

2.2 Servers

De door de BAR-Organisatie aangeboden server omgeving heeft de volgende kenmerken:

- Volledige virtualisatie op basis van Microsoft Hyper-V 2019
 - Gerealiseerd in een HA TwinDC
- Server OS: Windows 2019
 - Altijd voorzien van recente Microsoft Patches en updates.
- IPv4 only
 - Voorzien van lokale Windows Firewall
- Voorzien van (in rechten) beperkt server specifiek Service account voor de services.
- Dagelijks Snapshot back-ups

2.3 Databases

- Oracle 19
- Microsoft MSSQL 2012
- Dagelijks integrale back-ups

2.4 Email (SMTP)

- Interne SMTP server (exchange 2019)
- Alleen geauthentiseerd mail naar externen (relay)
- TLS1.2

2.5 Werkplek

- De door de BAR-Organisatie aangeboden werkplek heeft de volgende kenmerken:
 - Desktop
 - Windows 10 64Bit
 - Wlan and LAN connected
 - Applicatie distributie op basis van MSI/installer/SCCM
 - MS Office 2016
 - BAR-Workspace (Microsoft RDS)
 - Windows 2016 / Ivanti Workspace Manager
 - Applicatie distributie op basis van MSI/installer/Ivanti
 - MS Office 2016

2.6 Applicatie Omgevingen (Servers)

2.6.1 Ontsluiting vanaf het internet:

- Wordt door BAR-ICT altijd voorzien van IPS/Virus scanning in de Firewall.
- Inbound WEB/API/Client traffic via aanwezige reverse proxy OF eigen DMZ server.
- API toegang altijd op basis van ACL.
- Op basis van DNS (.bar-organisatie.nl).
- Maximaal 1 extern IPv4 adres beschikbaar.
- Alleen HTTPS: op 443 (minimaal TLS1.2 Intermediate_compatibility)
 - https://wiki.mozilla.org/Security/Server_Side_TLS#Intermediate_compatibility_.28recommended.29
- Overheid PKI certificaat (KPN via BAR-Organisatie)

2.6.2 Ontsluiting naar het internet:

- Outbound traffic standaard niet toegestaan.
 - Uitzonderingen altijd op basis van TLS

2.6.3 Ontsluiting Intern

- Op basis van DNS
- Alleen IPv4 adres beschikbaar.
- Alleen HTTPS: op 443 (minimaal TLS1.2 Intermediate_compatibility)
 - https://wiki.mozilla.org/Security/Server_Side_TLS#Intermediate_compatibility_.28recommended.29

2.6.4 Gebruikers authenticatie/authorisatie

- SSO op basis ADFS eventueel in combinatie met 2FA.

2.7 Applicatie architectuur

(primair) client-server op basis van RDP, cliënt programmatuur ook ondersteund op Microsoft Remote Desktop servers

2.8 Remote Toegang voor leveranciers

- Alleen via applicatiebeheer / IT, geen zelfstandige toegang.
- Op basis van NETOP (monitoring en logging)

2.9 SaaS specifieke eisen:

2.9.1 Ontsluiting via GGI-Netwerk

Bij voorkeur worden SaaS oplossingen verbonden via GGI-Netwerk.

Ontsluiting vanaf het internet:

- API toegang altijd op basis van ACL.
- Op basis van DNS (.bar-organisatie.nl).
- Alleen HTTPS: op 443 (minimaal TLS1.2 Intermediate_compatibility)
 - https://wiki.mozilla.org/Security/Server_Side_TLS#Intermediate_compatibility_recommended.29
- Overheid PKI certificaat (KPN via BAR-Organisatie)
- Bij het verwerken van “bijzondere Persoonsgegevens” voorzien van 2 factor authenticatie

2.9.2 Gebruikers authenticatie/authorisatie

- Op basis van aanwezige ADFS/Azure AD service van BAR-Organisatie

2.9.3 Email: (SMTP)

Indien er gebruik gemaakt wordt van door de BAR-Organisatie beheerde domeinen zal email namens de BAR-Organisatie zal voorzien moeten worden van :

- SFP records (DNS beheer: BAR-Organisatie)
- DKIM Signature (DNS beheer: BAR-Organisatie)
- DMARC

2.9.4 Koppeling met interne applicaties:

- Op basis van aanwezige ESB: Opentunnel van JNET
- Inbound (to BAR) WEB/API/Client traffic via aanwezige reverse proxy OF eigen DMZ server.
 - Wordt door BAR-ICT altijd voorzien van IPS/Virus scanning in de Firewall.
 - API toegang altijd op basis van ACL.
 - Op basis van DNS (.bar-organisatie.nl).
 - Maximaal 1 extern IPv4 adres beschikbaar.
 - Alleen HTTPS: op 443 (minimaal TLS1.2 Intermediate_compatibility)
 - https://wiki.mozilla.org/Security/Server_Side_TLS#Intermediate_compatibility_recommended.29
 - Overheid PKI certificaat (KPN via BAR-Organisatie)