

Inleiding

Steeds meer applicaties en diensten worden tegenwoordig afgenomen vanuit de Cloud en ondergebracht bij leveranciers. Voordat er een applicatie in de Cloud wordt weggezet, zijn er een aantal spelregels en technische randvoorwaarden waaraan moet worden voldaan.

Dit document kan hierbij als een checklist worden gebruikt.

- Volg altijd het wijzigingsproces als er wijzigingen worden doorgevoerd aan de technische infrastructuur van Katwijk. De juiste mensen kunnen op deze manier naar de aanvraag kijken.
- Uitgangspunt bij een gang naar de Cloud is dat het Katwijk iets moet opleveren, denk hierbij b.v. aan minder beheerlasten, groter gebruiksgemak, verbeterde functionaliteit, lagere kosten of het gebruik van kennis en kunde van derden.
- Een Cloud oplossing moet altijd voldoen aan de technische eisen van Katwijk.

Technisch algemeen

- Geen directe koppelingen van extern naar interne servers van Katwijk.
- Uitwisselen van gegevens alleen met encryptie en bij voorkeur via JNet.
- Externe verbindingen lopen wanneer noodzakelijk via onze DMZ (front-end servers).
- Geen directe LDAP(S) verbindingen naar de domain controllers van Katwijk.
- Autorisatie 'Enterprise Application' via het standaard koppelvlak van Azure AD.
- Cloud applicaties als echte SAAS applicatie via een HTML(5) browser via HTTPS (tenminste TLS 1.2 voorkeur TLS 1.3).
- Directe toegang tot SAAS applicatie via MFA (Azure AD) of alleen via public IP van gemeente Katwijk.
- Geen directe VPN verbindingen van/naar het server subnet van Katwijk.
- Cloud applicaties en de bijbehorende data mogen alleen in een Europees datacentrum worden gehost.
- Applicatie moet passen in de technische infrastructuur van Katwijk en voldoen aan de BIO (Baseline Informatiebeveiliging Overheid).
- Bij het gebruik van (bijzondere)persoonsgegevens in de Cloud applicatie moet altijd een verwerkersovereenkomst worden afgesloten met de leverancier van de applicatie.

Technisch mail

Mailverkeer gericht binnen de eigen organisatie.

- Cloud applicaties kunnen berichten sturen via een "katwijk" sub domein onder het domein van de leverancier (b.v. "afzender@katwijk.leverancier.nl"). Op deze manier kan en moet de leverancier van de Cloud applicatie zelf inregelen dat de afzender gecontroleerd kan worden d.m.v. SPF, DKIM en DMARC.
- Voor Cloud applicaties die via mail alleen berichten willen sturen naar adressen binnen het katwijk.nl domain is het eventueel mogelijk om in de mailgateway een uitzondering op te nemen zodat dit specifieke verkeer zonder de inrichting van SPF, DKIM en DMARC toch kan worden ontvangen. Op deze manier is het niet noodzakelijk om de hele mailservers van derden te machtigen om mail namens @katwijk.nl te versturen, maar wordt één specifiek katwijk.nl mailadres doorgelaten (b.v. "personeelszaken@katwijk.nl") als afzender adres voor de cloud applicatie t.b.v. notificaties.

Mailverkeer gericht buiten de eigen organisatie.

- Voorkeur voor het versturen van e-mail via een Microsoft Exchange connector.
- Voor Cloud applicaties die namens Katwijk officiële berichten via mail moeten versturen naar ontvangers buiten de eigen organisatie moet een configuratie van SPF, DKIM en DMARC worden ingericht in de DNS registratie van Katwijk. Met deze configuratie wordt de mailserver van de leverancier gemachtigd om mail berichten als "afzender@katwijk.nl" namens Katwijk te versturen. Een ontvanger van zo'n bericht kan dan de afzender controleren en verifiëren als Katwijk. Het spreekt voor zich dat er in dit geval een verwerkersovereenkomst met deze leverancier moet worden afgesloten. Alleen bij hoge uitzondering en met een duidelijk aantoonbare noodzaak, mag Katwijk een mailserver van derden.