Huidige situatie ICT

De huidige werkplek van de gemeente Katwijk is een moderne werkplek, op basis van Microsoft 365, Liquit en Exchange online. De werkplek wordt aangeboden via laptops en Cloud pc's.
Het applicatielandschap (ongeveer 250 applicaties) is grotendeels SaaS, maar bevat nog een aantal legacy applicaties. Voor gebruik van de legacy applicaties of applicaties met specifieke netwerkvereisten (Diginet/Gemnet of anders) wordt gebruik gemaakt van Always On VPN.
Authenticatie van SaaS applicaties loopt via de Azure AD (Entra) van Katwijk. User provisioning vindt plaats op basis van een RBAC koppeling met het HR systeem Motion.
Voor applicaties die een Oracle database gebruiken is een Oracle Cloud Infrastructure beschikbaar, maar de gemeente streeft ernaar te standaardiseren op SQL databases.

De gemeente Katwijk heeft geen on-prem datacenter meer.

Gemeentelijke I-visie

De ICT-voorziening van de gemeente Katwijk is primair gericht op de Cloud en op het Microsoft platform. De digitale werkomgeving is flexibel en schaalbaar.

Binnen afzienbare termijn wil de gemeente volledig Cloud gebaseerd zijn. Daar waar nog legacy applicaties draaien, worden deze vervangen door een Cloud "no code/ low code" oplossing. Het ERP (MS Dynamics) platform is leidend bij het vervangen van legacy applicaties. Indien dit niet mogelijk is, is het powerplatform de gewenste oplossing.

Op termijn willen we af van legacy applicaties in de Azure tenant en alleen nog gebruik maken van 'echte' SaaS oplossingen.

Het cluster I&A

Het cluster I&A ontwikkelt zich steeds meer tot een regieorganisatie. Conform de I-visie worden steeds meer beheertaken uitbesteed en richt de afdeling zich op het bewaken van de (informatie) architectuur, innovatie en de regievoering over de leveranciers. Op termijn is het de bedoeling dat het (technisch/applicatie) beheer zo veel mogelijk door derden wordt uitgevoerd. De gemeente Katwijk werkt in multidisciplinaire teams (Agile/Scrum).

Architectuurprincipes

Gemeente Katwijk hanteert de volgende architectuurprincipes:

- secure by design;
- streven naar zero trust;
- gegevensuitwisseling wordt gerealiseerd op basis van standaard API's;
- actief regie voeren over uitbestede applicaties/diensten;
- hergebruik van gegevens: enkelvoudige opslag, meervoudig gebruik;
- de gemeente is 24/7 online beschikbaar;
- geen maatwerk in applicaties van leveranciers;
- doorontwikkelen van tijd- en plaats onafhankelijk werken;
- werken vanuit een platformgedachte en inzetten van alle beschikbare mogelijkheden van het platform;
- applicaties alleen vervangen om te innoveren;
- bij het vervangen van legacy applicaties wordt uitgegaan van het cloud-only principe;
- legacy systemen vervangen door "no code low code" oplossingen;
- een flexibele en schaalbare digitale werkomgeving.

Eisen aan gemeentelijke oplossingen

Aan oplossingen die de gemeente Katwijk gebruikt, worden een aantal eisen gesteld, naast onze architectuurprincipes:

- de gemeente hanteert een cloud-only beleid:
    1) SaaS
    2) PaaS
    3) IaaS
- applicaties en de gegevens van de gemeente Katwijk mogen alleen in een Europees datacentrum worden gehost;
- applicaties zijn echte SaaS applicaties, via een HTML(5) browser via HTTPS (TLS 1.3);
- applicaties gebruiken geen Office of browser plugins, functionaliteit is native beschikbaar in de applicatie;
- authenticatie verloopt altijd via de Azure AD (Entra) van de gemeente;
- applicaties draaien op de laatste versie van Windows of bij hoge uitzondering op Linux;
- voordat een oplossing wordt geïmplementeerd is duidelijk wie de eigenaar is en waar het beheer ligt.
- live-data in een applicatie moet altijd via PowerBi direct benaderbaar zijn voor rapportage;
- applicatiedata moet beschikbaar en direct toegankelijk zijn voor verwerking in de Azure Datafactory van de gemeente;
- een beschrijving van eventuele algoritmen in applicaties moet beschikbaar zijn voor de gemeente;
- oplossingen maken geen gebruik van fysieke fileshares;
- met updates loopt de gemeente maximaal één update achter op de meest recente versie;
- geen directe LDAP(S) verbindingen naar de domain controllers van Katwijk;
- directe toegang tot applicaties verloopt via MFA (Entra) of alleen via uitgaande IP-adressen van gemeente Katwijk;
- directe VPN verbindingen van of naar het server subnet van Katwijk zijn niet toegestaan;
- applicaties moeten passen in de technische infrastructuur van Katwijk en voldoen aan het BIO2 normenkader;
- oplossingen worden geleverd met een duidelijk vastlegde architectuur(plaat) van de oplossing.
- servers in Azure hebben standaard geen toegang tot internet. Indien internet toegang toch nodig is, dient er door de leverancier een lijst van hosts\sites te worden aangeleverd.

Privacy en Security

Op gebied van privacy en security hanteert de gemeente Katwijk de volgende eisen

- applicaties voldoen aan BIO2 (Baseline Informatiebeveiliging Overheid) en relevante normen, zoals ISO 27001 en NEN 7510;
- applicaties zijn AVG compliant;
- applicaties gebruiken het HTTPS protocol TLS 1.3;
- publiek toegankelijke webservers hebben een 100% score op internet.nl of een gemotiveerde afwijking;
- gemeente Katwijk verwacht van haar leveranciers een pro-actieve houding ten aanzien van privacy en security. Onder meer door het aanleveren van een jaarlijkse incident rapportage;
- leveranciers kunnen hun beveiliging aantonen middels certificering door een IT-auditor;
- gegevensuitwisseling alleen via encryptie, bij voorkeur via EnableU;
- zorgdata wordt via mail gedeeld op basis van de NTA 7516 norm;
- bij het gebruik van (bijzondere) persoonsgegevens in applicaties, moet altijd een verwerkersovereenkomst worden afgesloten met de leverancier.

Email

Mailverkeer gericht aan de eigen organisatie.

- 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 applicatie zelf inregelen dat de afzender gecontroleerd kan worden d.m.v. SPF, DKIM en DMARC.
- Voor applicaties die via mail alleen berichten willen sturen naar adressen binnen het katwijk.nl domein 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 applicatie t.b.v. notificaties.

Mailverkeer gericht aan derden.

- Voorkeur voor het versturen van e-mail via de Exchange Online omgeving van gemeente Katwijk.
- Voor applicaties die namens Katwijk mailen 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 moet worden afgesloten. Alleen bij hoge uitzondering, met instemming van de CISO en met een duidelijk aantoonbare noodzaak, machtigt Katwijk een mailserver van derden.

Domeinen

Registreren van domeinnamen t.b.v tijdelijke doelen.

- De gemeente Katwijk is zeer terughoudend met het registreren van domeinnamen voor tijdelijke doelen zoals projecten of enquêtes. Na registratie kunnen deze domeinnamen om beveiligingsredenen niet meer worden opgezegd, omdat derden de domeinnamen anders kunnen registreren en er misbruik van kunnen maken. Uitgangspunt is om hiervoor een subdomein van het katwijk.nl domein te gebruiken, zoals bijvoorbeeld valkenhorst.katwijk.nl.