Algemeen overzicht van de huidige situatie

Inleiding

Het huidige ICT-landschap van de provincie Noord-Brabant is sterk onderhevig aan veranderingen. Hiermee wordt mede aangeduid dat de huidige situatie is gebaseerd op de stand van zaken bij de start van deze aanbesteding. De provincie Noord-Brabant kan dan ook niet uitsluiten dat er géén wijzigingen plaatsvinden tussen het moment van aanbesteden en contracteren van deze aanbesteding.
Het verandertraject waar de provincie zich in bevindt komt niet alleen voort uit het uitbesteden van diensten, maar ook uit het uitvoeren van onder andere een cloudstrategie met een impact op applicaties, digitale werkplekken, dataopslag en daarmee natuurlijk informatiebeveiliging. Clouddiensten zoals Microsoft 365 en Azure zijn volop in ontwikkeling bij de provincie en daar horen ook gepaste en moderne cybersecuritymaatregelen bij. Bij de provincie vertalen die zich onder andere naar systemen zoals Darktrace monitoring en detectie, Microsoft Sentinel, MS Azure ARC en Tenable Nessus kwetsbaarhedenscanner. Het doel is om deze beveiligingsmaatregelen/-systemen medio 2024 te optimaliseren en standaard ingebed te krijgen in de gehele ICT-infrastructuur van de provincie Noord-Brabant. Een en ander brengt ook met zich mee dat de provincie zich buigt over verscheidene proces- en capaciteitsvraagstukken om alles goed te laten functioneren na implementatie. Kortom, de security-omgeving van de provincie Noord-Brabant op dit moment verre van statisch.

Team Informatiebeveiliging & Privacy

Binnen de provincie werkt een klein team van informatiebeveiliging in een strategische en taktische rolverdeling. Operationele rollen worden niet door de provincie zelf ingevuld. Het team bestaat uit de volgende functies en aantallen:

- 1 CISO
- 3 ISO’s
- 1 Functionaris Gegevensbescherming
- 1 Privacy Officer

ICT-(gebruikers)omgeving

Assets	Geschat aantal
Actieve (gebruikers-) accounts	2200
Beheerde laptops	1350
Actieve virtuele desktops in het LAN	750-900
Fysieke PC’s op locatie (FAT client)	45
Beheerde smartphones o.b.v. MAM	1350
Servers	250

Buiten de beheerde werkplekken/laptops is de situatie nu dat een grote populatie gebruik maakt van voor de provincie niet vertrouwde apparatuur waarmee wordt ingelogd op bijvoorbeeld MS365. Dit moet in de nabije toekomst worden ondervangen door de inzet van Azure Virtual Desktop.

Behalve de huidige virtuele desktop en FAT-clients op locatie bevinden laptops en andere apparaten van gebruikers zich niet op het LAN.

Provincie Noord-Brabant werkt met Microsoft 365 waarbij alle gebruikersaccounts medio april 2024 over een E5-licentie beschikken.

Op de beheerde laptops wordt gebruik gemaakt van Defender for endpoint en er wordt centraal gemonitord. De virtual desktops en servers in het LAN zijn voorzien van Trellix Move AV (voorheen McAfee Move).

Security infrastructuur

De ICT-security infrastructuur bestaat uit een divers aan onderdelen om bedreigingen buiten de deur te houden en daarmee de risico's zoveel als mogelijk tot nul te reduceren. Denk dan aan firewalls, mailfiltering, proxy- en webfiltering en antivirusdetectie. Voor monitoring en detectie en kwetsbaarhedenscan zijn de onderstaande producten door de provincie in gebruik.

Tenable Nessus Expert

Deze kwetsbaarhedenscanner is eigendom van de provincie en operationeel vanuit de virtuele server infrastructuur binnen het provinciehuis. Nessus wordt op dit moment incidenteel ingezet om kwetsbaarheden te scannen. In de eerste plaats voor websites en/of webbased applicaties, maar meer en meer ook voor interne serversystemen. De provincie erkend dat dit pakket niet toereikend is voor een uitgebreide dienst als het gaat om kwetsbaarhedenscanning en opvolging ervan.

Darktrace

Een monitoring- en detectiesysteem dat sinds eind 2022 is geïmplementeerd door Darktrace. Voor de dienst zijn momenteel 3 hardware sensoren beschikbaar. Eén master en twee slaves. Eén sensor t.b.v. het Equinix datacenter is nog niet operationeel ingezet. De sensoren zijn gesitueerd in het LAN en de DMZ.
DarkTrace wordt vooral ingezet voor monitoring en detectie van de netwerk infrastructuur, Microsoft MS365 en e-mail. Een koppeling met Sentinel is voorzien, maar op dit moment nog niet operationeel.
De functionaliteit van Darktrace die momenteel is uitgerold is een netwerk IDS/IPS om ongeautoriseerde activiteiten op het netwerk te detecteren. Met Darktrace worden momenteel de volgende mgevingen gemonitord:

- Netwerkdetectie (PNB Den Bosch on premise gegevens LAN en DMZ)
- MS365 plugin
- Mail filtering MS365 Exchange Online

Microsoft Sentinel

Sentinel draait in de Azure-omgeving van PNB. De licenties zijn eigendom van PNB. Het platform waarop Sentinel binnen Azure functioneert is in beheer bij een externe dienstenleverancier. Sentinel wordt ingezet als een ondersteunend systeem voor SIEM (Security Incident and Event Management) door het gecentraliseerd verwerken van de daarop aangesloten logbronnen. Om Sentinel optimaal te laten functioneren zal er nog een verbeterslag moeten worden gemaakt t.a.v. de informatie vanuit de verscheidene logbronnen.

De status van het SIEM binnen de provincie beperkt zich op dit moment tot Sentinel als

vergaarbak van logbronnen. Procedures rondom monitoring en opvolging van incidenten zijn nog niet operationeel.
Het uitgangspunt van de provincie t.a.v. Sentinel en een SIEM is dat zij hiermee verwacht te voldoen aan de BIO-maatregelen t.a.v. onder andere gebeurtenislogging en SIEM/SOC.

Beheer

De provincie bevindt zich op dit moment in een overgangssituatie als het gaat om ICT-dienstverlening. Systemen Darktrace, Nessus en Sentinel zijn op initiatief van de provincie geïmplementeerd en niet, of slechts ten dele, in beheer bij de ICT-dienstverlener.

- Tenable Nessus Expert
  Dit product is in eigendom van PNB en geïnstalleerd op de virtuele server infrastructuur binnen het provinciehuis. Het technisch beheer tot op het niveau van het besturingssysteem wordt uitgevoerd door de huidige IT dienstverlener. Het functioneel beheer van Nessus wordt door de provincie zelf gedaan.

- DarkTrace
  Het systeem is ingericht met fysieke servers van Darktrace en daarmee is het technisch beheer ook belegd bij deze leverancier. In principe is het functioneel beheer belegd bij de provincie, maar daarbij leunt de provincie wel sterk op ondersteuning vanuit Darktrace. Operationele werkzaamheden zijn op dit moment belegd binnen de provincie met daarnaast de (geautomatiseerde) SOC-dienstverlening van Darktrace. Door gebrek aan capaciteit, kennis en dienstverlening functioneert detectie en monitoring, en daarmee ook Darktrace, op dit moment niet conform wens.

- Microsoft Sentinel
  Het platform waarop Sentinel binnen Azure functioneert is nog in ontwikkeling en in technisch beheer van de ICT-dienstverlener.

Overige aandachtspunten inzake beheer.

- Als het gaat om de systemen Darktrace, Nessus en Sentinel is er op dit moment geen sprake van een gecontracteerde managed of een as a Service-dienst, noch is er een Service Level Agreement (SLA) met een van de partijen. Bij Darktrace is er wel sprake van ondersteuning in de vorm van een supportportal, een toegewezen customer succes manager en van technical support specialisten en de SOC dienstverlening.
- Het interne service window is van 8.00-17.00 uur op werkdagen (middels een interne helpdesk).
- Het beheren van de logbronnen en het beheer van de Azure-connectie is onderdeel van het SLA met de huidige ICT-dienstenleverancier OGD.
- Darktrace notificeert IB (PNB) bij melding (24*7 d.m.v. een geautomatiseerd proces). De provincie besluit welke actie hierop volgt.
- Bij calamiteiten reageert de ICT-dienstverlener 24*7. Dit is niet in het SLA vastgelegd.

Leveranciers en/of oplosgroepen

Het beheer c.q. de ondersteuning op het gebied van security operations wordt ingevuld door de volgende partijen:

- Sinds 2019 beheert Operator Group Delft (OGD) het overgrote deel van de ICT-infrastructuur van de provincie. OGD levert zelf geen actieve security dienstverlening en acteert voornamelijk op incidenten. Daarnaast is er een kwetsbaarhedenmanagement dat o.a. wordt gevoed met meldingen vanuit het Nationaal Cyber Security Centrum (NCSC). Als het aankomt op het beheer van security componenten binnen de ICT-infrastructuur levert OGD het technisch beheer.

- De dienstverlening vanuit het Darktrace SOC signaleert hoge prioriteit incidenten richting de provincie. Er is geen geautomatiseerde opvolging en met die reden worden deze incidenten handmatig verwerkt om opgepakt te kunnen worden in de (security) incidentenprocedure.

- Intern serviceloket/1ste-lijns helpdesk (Ons Loket): Ontvangt (security) incidenten van gebruikers en routeert deze naar de juiste oplosgroep. Security is geen specialisme binnen het interne serviceloket.

- Team Informatiebeveiliging & Privacy: Dit team vanuit de provincie bestaat uit een CISO, ISO's, een Functionaris Gegevensbescherming (FG) en een Privacy Officer (PO). Binnen dit relatief kleine team zijn geen functies gedefinieerd om mee te werken aan operationele zaken. Operationele (security) taken zou eigenlijk binnen ieder team functioneel of technisch beheer of support belegd moeten zijn, echter dit is (nog) niet geregeld.

- Functioneel Beheer: Het functioneel beheer van applicaties is binnen de provincie (nog) gespreid georganiseerd. Voor kritieke en/of omvangrijke applicaties is dat belegd binnen de ICT-afdeling 'Dienstverlening en ICT'. Echter het functioneel beheer van specifieke/programma gebonden applicaties is veelal belegd binnen de programma's zelf.

Processen, procedures en werkvormen

De provincie is een inhaalslag aan het maken waar het gaat om het inrichten van ITIL-processen en daarmee samenhangende procedures. Informatiebeveiliging is daar een onderdeel van.

Omdat de provincie ISO27001 is gecertificeerd is er vanuit het ISMS een security incidentproces vastgesteld. Daarnaast zijn er binnen het incidentenproces voor de meest voorkomende use cases procedures vastgelegd. Denk dan aan incidenten die te maken hebben met phishing, datalekken, ongeautoriseerde toegang of gestolen/verloren apparatuur.

Het aanbrengen van ICT-incidenten wordt o.a. gedaan door gebruikers, beheerders, dienstverleners en (detectie-)systemen. Deze meldingen worden verwerkt in een helpdeskapplicatie waarbinnen diverse oplosgroepen zijn gedefinieerd die zorg dragen voor een adequate afhandeling.

De provinciale organisatie is verplicht zich te houden aan de Baseline Informatiebeveiliging Overheid (BIO). De BIO is gebaseerd op de ISO27001 met daarbij een uitgebreidere set met maatregelen op de al bestaande paragrafen van de ISO-normering.
Vanuit de paragrafen en onderliggende maatregelen vanuit de BIO zijn er door de provincie richtlijnen opgesteld die zijn vastgesteld op directieniveau.
Naast deze algemene maatregelen en richtlijnen wordt over specifieke vraagstukken in het kader van de geldende wet-, regelgeving, kaders en richtlijnen afzonderlijke uitwerkingen gemaakt. Denk dan aan bijvoorbeeld aan de inzet van 'Single Sign On', het gebruik van browserextensies of rechten en rollen van verschillende accounts.

De provincie hecht veel waarde aan gecertificeerde dienstverlening als het gaat om informatiebeveiliging. De provincie heeft t.a.v. het handhaven van de BIO en voor ondersteuning van de eigen certificering immers belang bij gecertificeerde diensten. Met die reden laat de provincie waar nodig onafhankelijke audits uitvoeren bij nieuwe en bestaande dienstverleners inzake NEN-ISO27001.

Buiten de periodieke audit die de provincie ondergaat voor de ISO-certificering met daaraan gekoppeld de BIO, worden er van tijd tot tijd pentesten uitgevoerd en wordt de weerbaarheid van de organisatie op de proef gesteld door de inzet van mysterie guests of e-mail phishing campagnes.

Op landelijk niveau is provincie Noord-Brabant samen met andere provincies georganiseerd in het CIBO, een kring van provinciale CISO's en sinds kort is er het IP-ISAC geformeerd waarin ISO's in een soortgelijk samenwerkingsverband om kennis en ervaring uitwisselen, maar wat ook kan worden ingezet bij calamiteiten.

Bij omvangrijke incidenten/calamiteiten (denk bijvoorbeeld aan Apache Log4j eind 2021) wordt er binnen de provincie een CERT geformeerd met daarin de meest relevante spelers om de probleemoplossing te coördineren.

Dataconnectoren

Er zijn op dit moment 28 dataconnectoren, waarvan er 24 connected zijn.

Nummer	Omschrijving
1	Azure Activity
2	Azure Firewall
3	Azure Key Vault
4	Citrix ADC (former NetScaler)
5	Common Event Format (CEF) via AMA (Preview)
6	Juniper SRX
7	McAfee ePolicy Orchestrator (ePO)
8	Microsoft 365
9	Microsoft 365 Insider Risk Management (preview)
10	Microsoft Defender for Cloud Apps
11	Microsoft Defender for Endpoint
12	Microsoft Defender for Identity
13	Microsoft Dedender for Office 365 (Preview)
14	Microsoft Defender XDR
15	Microsoft Entra ID
16	Microsoft Entra ID protection
17	Microsoft Purview Information Protection (Preview)
18	Microsoft Security Groups
19	Palo Alto Networks (Firewall)
20	Security Events via Legacy Agent
21	Subscription-based Microsoft Defeneder for Cloud (legacy)
22	Syslog via Legacy Agent
23	Windows Forwarded Events
24	Windows Security Events via AMA

Provincie Noord-Brabant