

Rapportage 2024

Informatiebeveiliging



Deventer, Olst-Wijhe en Raalte: samen staan we sterker.

CISO | Februari 2025

1. Inleiding

In 2024 hebben de DOWR-gemeenten belangrijke stappen gezet op het gebied van informatiebeveiliging. Zo zijn er aanzienlijke verbeteringen doorgevoerd op het vlak van technische informatiebeveiliging, zijn er meerdere bewustwordingscampagnes georganiseerd en hebben we het cybercrisisplan geoefend.

De toenemende digitalisering van gemeentelijke diensten, gecombineerd met een stijgend aantal cyberdreigingen, benadrukt het belang van een sterke beveiligingsstrategie. Dit jaarverslag biedt een overzicht van de belangrijkste ontwikkelingen, risico's en verbetermaatregelen.

1.1. Successen

Betrokkenheid van medewerkers: Steeds meer collega's melden verdachte situaties en we hebben een actief en vast aantal deelnemers dat aan onze bewustwordingstrainingen (Nanolearning) deelneemt. Dit toont aan dat informatiebeveiliging binnen de organisaties leeft. Ook de IT-teams tonen steeds meer pro-activiteit in het verbeteren van de beveiligingsmaatregelen, wat essentieel is voor het minimaliseren van risico's.

1.2. Uitdagingen

Complexiteit van informatiesystemen: De variëteit aan IT-systemen, van verouderd tot modern, vraagt om risicomanagement, regelmatige updates en uitfasering van oude systemen.

Menselijke factor: Ondanks vooruitgang in bewustwording blijft de menselijke factor een kwetsbare schakel in onze beveiligingsstrategie. Fouten en onzorgvuldigheid brengen risico's met zich mee. Het is een doorlopend proces om medewerkers alert te houden en hen de juiste middelen en kennis te bieden voor een effectieve omgang met cyberdreigingen.

Proceseigenaarschap & vindbaarheid: Medewerkers raken steeds meer betrokken bij informatieveiligheid, maar er is vaak onduidelijkheid over proceseigenaarschap en de verantwoordelijkheden voor beveiliging. Het informatieveiligheidsteam wordt niet altijd tijdig betrokken bij nieuwe initiatieven. Dit benadrukt de noodzaak van betere communicatie en vindbaarheid, zodat informatieveiligheid vanaf het begin in alle projecten wordt geïntegreerd.

Risicomanagement: We hebben belangrijke stappen gezet, maar risicomanagement moet verder in de organisatie worden ingebed. De veranderende cyberdreigingen vereisen een dynamische aanpak en nauwe samenwerking tussen interne teams en externe partners.

2. Weerbaarheid

In 2024 zagen we een toename in het aantal cyberrisico's die een reële dreiging vormden voor de DOWR-gemeenten. Deze risico's bedreigen niet alleen onze systemen, maar ook de dienstverlening aan burgers. Enkele van deze risico's zijn:

- Datalekken: Bijvoorbeeld door phishing of menselijke fouten.

- Verstoringen: Dreigingen gericht op systemen van dienstverleners of partners, zoals DigiD.
- Afhankelijkheid van leveranciers: Beveiligingsproblemen bij externe partijen hebben ook impact op ons.

Om deze risico's te beheersen, hebben we onze processen aangescherpt en aanvullende maatregelen geïmplementeerd om de weerbaarheid van organisaties te verhogen.

2.1. Schaduw-IT incident

In 2024 werd in Deventer een beveiligingsincident vastgesteld via een niet-zakelijke internetverbinding, veroorzaakt door een fout in de netwerkinstellingen. Dit systeem viel buiten het beheer en de infrastructuur van onze organisatie, maar werd wel door een leverancier gebruikt. Dankzij de snelle detectie en het directe ingrijpen van DOWR-i kon schade worden voorkomen. Dit benadrukt niet alleen het belang van effectieve detectie- en responsmechanismen, maar ook de noodzaak om het gebruik van niet-goedgekeurde IT-systemen, software of clouddiensten terug te dringen en systemen structureel te beheren.

2.2. Informatiebeveiligingsdienst meldingen

Als overheidsorganisatie ontvangen wij meldingen van de Informatiebeveiligingsdienst (IBD) over kwetsbaarheden in onze applicaties, apparatuur en diensten, die wij vervolgens verifiëren en verhelpen.

Het aantal gemelde kwetsbaarheden is aanzienlijk afgenomen, voornamelijk doordat we verouderde software hebben uitgefaseerd. We ontvangen ook

meldingen die, na controle door de specialisten, niet meer relevant zijn voor ons (n.v.t.).

Tabel 1: Afname gemelde kwetsbaarheden

Gemelde kwetsbaarheden	2022	2023	2024
Totaal aantal gemelde kwetsbaarheden	282	240	134
Kwetsbaarheden n.v.t.	76	59	42
Kwetsbaarheden doorgezet naar oplosgroep	206	181	92

3. Beveiligingsmaatregelen

In 2024 hebben we diverse acties genomen om onze informatiebeveiliging te versterken, waaronder:

3.1. Technische verbeteringen

Wij hebben veelal geplande beveiligingsupdates doorgevoerd, verouderde systemen uitgefaseerd en technische versterking toegepast om kwetsbaarheden te minimaliseren. Dit proces versterkt onze systemen door onnodige onderdelen te verwijderen, rechten te beperken en beveiligingsmaatregelen zoals (moderne) encryptie te implementeren.

De technische beveiliging van onze systemen voldoet volledig aan de Baseline Informatiebeveiliging Overheid (BIO) en de opmaat naar de nieuwe versie van de BIO (2.0).

Hoewel deze stappen essentieel zijn, blijft het belangrijk om ook onze applicaties goed in te richten, gebruikersrechten zorgvuldig te beheren en bewust om te gaan met de informatie in deze systemen.

3.2. Samenwerking regio

Ook hebben we extra aandacht besteed aan het verbeteren van samenwerking met omliggende gemeenten om informatie te delen en gezamenlijk op te treden tegen dreigingen. Dit speelt onder andere in de veiligheidsregio IJsselland, alsook politie Oost-Nederland.

3.3 Compliance / ENSIA

Met ENSIA verantwoordt we ons gemeentebreed over informatieveiligheid. De kern is om de informatiebeveiliging op een hoog niveau te houden. Hiermee zorgen we ervoor dat de inwoners van onze gemeente erop kunnen vertrouwen dat hun gegevens in veilige handen zijn. Ook maakt dit ons een betrouwbare partner voor bedrijven en andere organisaties.

3.4. Naleving informatieveiligheidsstandaarden

In 2024 zijn er stappen gezet met de webteams om meer beheersing te krijgen over de naleving van de informatiebeveiligingsstandaarden op onze websites. Dit heeft geleid tot een aanzienlijke vermindering van het aantal hoog-risico webdomeinen sinds begin 2024. Daarmee versterken we de digitale weerbaarheid van onze organisatie en komen we steeds beter in lijn met de geldende overheidsnormen voor informatieveiligheid van webdomeinen.

Abbeelding 2: Naleving informatiebeveiligingsstandaarden Deventer over 2024



Abbeelding 3: Naleving informatiebeveiligingsstandaarden Raalte over 2024



Abbeelding 4: Naleving informatiebeveiligingsstandaarden Olst-Wijhe over 2024



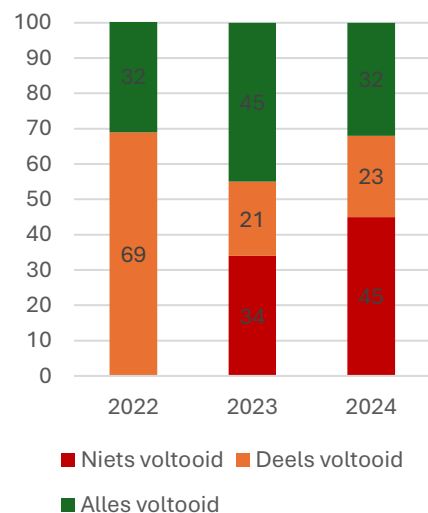
4. Bewustwording en training

Een weerbare organisatie begint bij goed geïnformeerde en getrainde medewerkers. In 2024 hebben we:

- **Cybercrisis oefening:** We hebben eind 2024 een succesvolle cybercrisis oefening gehouden om ons crisisplan en de communicatielijnen te testen, met duidelijke leerpunten voor verbetering.
- **Securityblog:** We hebben een securityblog opgezet en zijn actiever op het intranet, wat onze zichtbaarheid en communicatie over cybersecurity vergroot.

- Bewustwordingscampagnes georganiseerd: Gerichte campagnes voor het herkennen van cyberdreigingen. Dit doen we onder andere door middel van korte lessen elke 3 weken per e-mail over Privacy en Informatiebeveiliging en intranetberichten met specifieke onderwerpen.
- Het gemiddelde percentage medewerkers dat deelnam aan de trainingen in 2024 ligt rond de 40%. Over het gehele jaar zien we echter dat het aantal medewerkers dat de lessen actief volgt terugloopt t.o.v. voorgaande jaren, zie figuur 1.

Figuur 1: Nanolearning deelname over 2022-2024 (%)



- Red Teaming oefening: Tijdens een Red Teaming oefening (waarbij onze beveiliging wordt getest door een 'tegenpartij') zijn er verbeterpunten geïdentificeerd in zowel de digitale als fysieke beveiliging. Ook werd duidelijk dat het bewustzijn van

medewerkers verhoogd moet worden. Deze bevindingen worden meegenomen in onze acties.

5. Informatiebeveiligingsplan 2024

In lijn met het Informatiebeveiligingsplan 2024 zijn er belangrijke stappen gezet op het gebied van informatiebeveiliging binnen de gemeente. Echter, een aantal belangrijke onderdelen zoals de implementatie van risicomanagement, het beleid uitlijnen in de organisaties en dataclassificatie bevinden zich nog in uitvoering. Deze vertraging is deels het gevolg van de uitgestelde vaststelling van de Cyberbeveiligingswet en de afhankelijkheid van lopende organisatorische processen.

Onderwerp	Voortgang
Techniek	
Toepassen geoblocking	Afgerond
Meer functionaliteit op laptops	Afgerond
Pilot: sneller en beter reageren met Security AI	Afgerond
Zorgen voor een basisbeveiliging	Afgerond
Organisaties toetsen met ENSIA	Afgerond
Mens	
Vormgeven sturingsinformatie directie	Afgerond
Nanolearning lessen	Afgerond
Cybercrisis oefenen	Afgerond
Introductietraining medewerkers	In uitvoering
Organisatie	
Red Teaming	Afgerond
Beleid uitlijnen met organisaties	In uitvoering
Implementeren risicomanagement / ISMS	In uitvoering
Inzichtelijk maken impact NIS2 / ISO27001	In uitvoering
Implementeren Dataclassificatie	In uitvoering

6. Vooruitblik 2025

Voor 2025 zijn er een aantal strategische prioriteiten opgesteld in het jaarplan met als thema een 'Digitaal verantwoord DOWR':

- **Bewustzijn vergroten:** Zorgen dat iedereen in de organisatie begrijpt wat er nodig is om gegevens veilig en privacyvriendelijk te verwerken.
- **Eigenaarschap versterken:** Duidelijk toewijzen van verantwoordelijkheden binnen processen, zodat informatiebeveiliging en privacy niet alleen op papier geregeld zijn, maar ook daadwerkelijk worden toegepast.
- **Dataclassificatie toepassen:** Investeren in het juist classificeren van data, zodat gevoelige informatie op een passende manier wordt beschermd en verwerkt.
- **Risico's beheersen:** Door Information Risk Management (IRM) systematisch toe te passen, kunnen risico's tijdig worden geïdentificeerd en gemitigeerd.

7. Reflectie van de CISO

Informatiebeveiliging gaat niet alleen om het voorkomen van incidenten, maar ook om het bouwen van vertrouwen bij onze inwoners. Zij vertrouwen erop dat hun gegevens veilig zijn bij ons en dat wij altijd in staat zijn om onze diensten te leveren.

De inzet voor komend jaar is om samen met de organisaties informatiebeveiliging verder te integreren in ons dagelijkse werk. Het moet niet alleen een verantwoordelijkheid zijn van IT of de (C)ISO, maar een gedeelde verantwoordelijkheid van iedereen. Samen kunnen we een digitale omgeving creëren die veilig, betrouwbaar en toekomstbestendig is.