Informatieprotocol iRvN Q1-2026

ICT Rijk van Nijmegen

INFORMATIEPROTOCOL, iRvN-deel

Dit document geeft inzicht in de werkzaamheden, verantwoordelijkheden en dagelijkse praktijk van iRvN. Het is bedoeld als aanvullende informatie naast de reguliere P&C-documenten (begroting, kaderbrief, tussenrapportages en jaarrekening). Waar die documenten primair sturen op financiën, kaders en verantwoording, laat dit informatieprotocol zien wat iRvN doet, hoe dat gebeurt en welke schaal en complexiteit daarbij horen.

iRvN wordt soms ervaren als een black box: een organisatie die essentieel is voor de gemeentelijke dienstverlening maar waarvan het dagelijkse functioneren grotendeels buiten beeld blijft. Met dit document wordt beoogd dat beeld te nuanceren door feitelijke, toegankelijke en samenhangende informatie te bieden over beheer, beveiliging, dienstverlening en interne processen.

Afbakening en leeswijzer
Dit document is informatief van aard;
- het bevat geen beleidskeuzes en geen besluitvoorstellen;
- het vervangt geen P&C-documenten en voegt daar geen nieuwe financiële kaders aan toe;
- het beschrijft geen ambities maar informeert over de actuele stand van zaken;

De informatie is gegroepeerd langs de hoofdtaken van iRvN. Per onderdeel wordt inzicht gegeven in volumes, processen, risico's en beheersmaatregelen. Waar mogelijk zijn trends en ontwikkelingen benoemd om duiding te geven aan cijfers en feiten.

De informatie in dit document is bedoeld om bestuur en raden beter in staat te stellen hun rol te vervullen:
- door inzicht te geven in de afhankelijkheden van gemeentelijke dienstverlening van ICT en infrastructuur;
- door transparant te zijn over beveiliging, continuïteit en beheersing;
- door context te bieden bij vragen of incidenten die zich gedurende het jaar kunnen voordoen.

Dit document beoogt daarmee niet alleen te informeren maar ook om het gesprek over iRvN te voeren op basis van gedeeld begrip van de praktijk.

De missie van iRvN is om het voor alle medewerkers van de gemeentelijke organisaties in het Rijk van Nijmegen mogelijk te maken dat zij hún dienstverlening aan de inwoners en ondernemers kunnen uitvoeren. iRvN ondersteunt de organisaties daarvoor met een robuuste en veilige infrastructuur en met adequate dienstverlening die voldoet aan de behoeften en verwachtingen. Het beheer en de ontwikkeling van de veilige infrastructuur zijn ondergebracht in de afdeling Beheer en Beveiliging, de uitvoering van de dienstverlening in de afdeling Dienstverlening.

Beheer en Beveiliging, interessante cijfers
Een aantal feiten:
- iRvN beheert circa 600 servers (w.o. webservers, applicatieservers, databaseservers, servers voor beheertaken etc), in de beginjaren van iRvN waren dat er meer dan 1.000;
- Circa 5.600 medewerkers met hun laptops, mobiele telefoons en andere devices maken gebruik van de iRvN-infrastructuur. Toen iRvN startte, waren dat er circa 4.500.

- Dagelijks verwerken we ongeveer 1,5 TB aan logging ten behoeve van onze security-monitoring. Dus continu stroomt er ruwweg een kleine USB-stick per minuut aan logdata binnen. De bewaartermijn hiervan is 1 jaar. Voor 2025 bewaren we ongeveer 500 TB aan security-logging;
- We beheren zo'n 1.000 (WiFi) access points, verspreid in de regio;
- We hebben 250 switches in de regio om te zorgen dat de communicatie binnen ons netwerk goed verloopt (en dit zijn geen switches zoals u die thuis heeft liggen, dit zijn grote jongens).
- Sinds dit jaar beschikt iRvN over een backbone met een capaciteit van 100 GB. Dit is een zeer snelle kernverbinding binnen de IT-infrastructuur, vergelijkbaar met wat wordt gebruikt in moderne datacenters en telecomnetwerken.
- Deze verbinding zorgt ervoor dat grote hoeveelheden data snel en betrouwbaar kunnen worden uitgewisseld tussen verschillende onderdelen van het netwerk, zoals netwerksegmenten of gebouwen.
- Door deze backbone kan de infrastructuur huidige én toekomstige belasting goed aan. Daarmee is zij geschikt voor verdere groei en nieuwe toepassingen.
- iRvN beheert meerdere Microsoft-omgevingen (de zogenaamde tenants). Voorheen deelden de deelnemers één omgeving, nu heeft iedere deelnemer een eigen tenant. Dit heeft te maken met veiligheid, schaalbaarheid en ook met het scheiden van verantwoordelijkheden en autonomie. De beheercomplexiteit is daardoor toegenomen, zo ook vraagstukken rondom integraties en samenwerken;
- Elke tweede dinsdag van de maand rolt Microsoft zijn geplande updates en patches uit, waaronder: Beveiligingsupdates, kritieke kwetsbaarheidsdichtingen en kwaliteits- en stabiliteitsverbeteringen. Als het nodig is, voeren wij die wijzigingen meteen door wanneer we ze binnen krijgen.
- De andere updates van Microsoft worden maandelijks doorgevoerd. De Microsoft-omgeving moet up tot date zijn en dat is ze.
- Maandelijks voeren wij een serviceweekend uit. Het gaat om (andere) patches en aanvullende infrastructurele zaken. Dat raakt de kantoorautomatisering van de eindgebruikers en ook de MS-beheersoftware en -tooling die iRvN zelf gebruikt om de MS-omgeving te beheren en te ontwikkelen.
- Daarnaast worden er applicatie-updates gedraaid in de overige weekenden en de PinkRoccade-omgeving wordt eens per maand ge-updatet. Bijna elk weekend vinden dergelijke activiteiten plaats;
- We monitoren dag en nacht op cyberdreigingen en acteren als dat nodig is. Het Computer Security Incident Response Team (CSIRT) is een gespecialiseerd team binnen iRvN dat verantwoordelijk is voor het opsporen, analyseren en oplossen van beveiligingsincidenten;
- De externe omgeving en interne organisatie worden 24 uur per dag gemonitord op cyberincidenten. Wij monitoren zelf onze interne infrastructuur en een externe partij houdt onze 'buitenkant' in de gaten;
- Wij worden door externe partijen actief en onmiddellijk op de hoogte gesteld wanneer cyberdreigingen zich voordoen of voor kunnen doen. Zoals door de Informatiebeveiligingsdienst (IBD, onderdeel van de VNG, en biedt gemeenten dreigingsbeelden, incidentrespons en advies), Nationaal Cyber Security Centrum (NCSC, dat richt zich op vitale infrastructuur, maar deelt ook algemene dreigingsinformatie en waarschuwingen) en VNG Realisatie (dat ondersteunt gemeenten bij digitale veiligheid en samenwerking op het gebied van informatieveiligheid);
- Door middel van het Programma Beveiliging brengen wij ons beveiligingsniveau op peil en volgen wij de ontwikkelingen. De onderdelen van het programma zijn
    - de continue monitoring, detectie en response van de totale infrastructuur (MDR);
    - de beveiliging van de ActiveDirectory (de digitale sleutelkluis die bepaalt wie wat mag binnen het computernetwerk);
    - rechten van beheerders en hun werkplek;
    - pentest-programma (bewuste pogingen om in te breken in de infrastructuur);
    - patchmanagement (het zorgdragen voor up to date zijn);

  - asset management (de registratie van hard- en software);
  - baselines (de beschrijving van alle procedures en werkwijzen) en de segmentatie van de datacenters.
- Regionaal wordt eens per jaar de Nymacon georganiseerd waar studenten en professionele ethische hackers gevraagd worden in de infrastructuur in te breken.

Regelmatig analyseren wij onze omgeving om inzicht te krijgen in de stand van zaken rond informatieveiligheid binnen onze organisatie. Deze analyse is gebaseerd op de CIS Controls, een internationaal erkend raamwerk van best practices voor cyberbeveiliging. Op basis daarvan optimaliseren wij ons beheer en beveiliging, o.a. door het aanpassen van het Programma Beveiliging en het borgen van de projectresultaten in de organisatie.

Mobile devices, hoe houden we het veilig?
Wanneer elk van de medewerkers in de regio een laptop én een telefoon heeft, zijn dat al snel meer dan 12.000 devices. Mobiele devices vormen een directe toegang tot applicaties, gegevens en netwerken. Dat maakt ze praktisch onmisbaar, maar ook kwetsbaar. Want elk van die devices is een potentiële ingang tot onze infrastructuur voor kwaadwillenden.

In de regio is beleid geformuleerd om het die kwaadwillenden zo moeilijk mogelijk te maken. Zodra dat beleid is vastgesteld, kunnen we verder werk maken van de veiligheid rondom de devices door binnen het MDM-beleid onder meer vast te leggen:

- welke apparaten toegang mogen krijgen tot de infrastructuur;
- aan welke minimale beveiligingseisen deze apparaten moeten voldoen, zoals versleuteling en vergrendeling;
- hoe updates en beveiligingspatches worden afgedwongen;
- wat er gebeurt bij verlies, diefstal of uitdiensttreding, bijvoorbeeld het op afstand blokkeren of wissen van een device.

Zo kan iRvN grip houden op het gebruik van mobiele devices en kan voldaan worden aan de eisen uit de BIO, de ‘baseline’ van de Overheid.

We worden continu aangevallen!
100% veilig kan niet, er zal altijd een keuze gemaakt worden op basis van kans, impact en middelen.
De infrastructuur van iRvN wordt continu aangevallen. Geen van die aanvallen heeft geleid tot een binnendringing door kwaadwillenden. In een overzicht per kwartaal in 2024:

Kwartaal jaar	Aantal geconstateerde aanvallen	aantal aanvallen dat geanalyseerd is vanwege het dreigingsniveau en daarna is afgewend en opgelost	aantal aanvallen dat geëscaleerd moest worden om daarna afgewend en opgelost te worden
Q1 2025	11.600	2.086	14
Q2 2025	8.930	950	18
Q3 2025	4.960	1.130	16
Q4 2025	56.311	4.050	26

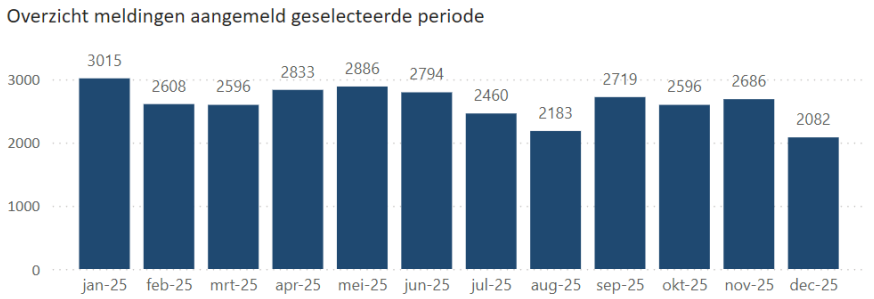
Ten opzichte van 2024 is een afname zichtbaar in het aantal geconstateerde cyberaanvallen. Het aantal aanvallen dat nader is geanalyseerd en afgewend is daarbij in grote lijnen gelijk gebleven, ook in absolute aantallen. Dit geldt in vergelijkbare mate voor het aantal aanvallen dat heeft geleid tot escalatie.

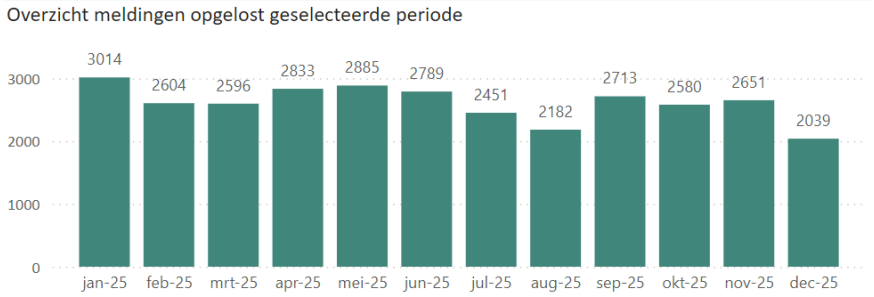
Voor deze ontwikkeling is geen eenduidige verklaring te geven. Het beeld wordt waarschijnlijk beïnvloed door meerdere factoren. Een mogelijke verklaring is dat het dreigingslandschap verschuift. Waar aanvallen eerder vaak grootschalig en generiek van aard waren, is er een toenemende focus op aanvallen die zijn gericht op individuele gebruikers, zoals Business Email Compromise. Dit zijn o.a. de phishing mails waar iedereen zeer alert op moet zijn! Dit type aanvallen kent doorgaans een ander patroon en komt in lagere aantallen voor.
Daarnaast hebben onze doorontwikkelingen in monitoring, detectie en analyse geleid tot een nauwkeuriger duiding van signalen. Hierdoor worden minder meldingen als aanval (false positives) aangemerkt, zonder dat dit afbreuk doet aan het zicht op daadwerkelijke dreigingen.
Tot slot geldt dat aantallen cyberaanvallen van nature fluctueren. Schommelingen over kwartalen heen zijn gebruikelijk en laten zich niet eenvoudig herleiden tot één oorzaak.
De toename van het aantal geconstateerde aanvallen in het laatste kwartaal van het jaar hangt samen met de Nymacon, waarbij studenten en ethische hackers gericht worden uitgenodigd om de infrastructuur te testen.

Dienstverlening

Binnen de ServiceDesk van iRvN komen dagelijks veel meldingen binnen. Deze meldingen bereiken iRvN via verschillende kanalen, zoals e-mail en telefoon. Het gaat daarbij om vragen, verzoeken en verstoringen die medewerkers ervaren bij het gebruik van de IT-dienstverlening. Een vergeten wachtwoord is zo’ melding, maar ook de mededeling dat een systeem het niet doet of dat de laptop gestolen is, zijn voorbeelden van meldingen. Aan de Servicedesk de taak om die meldingen zo snel en goed mogelijk af te handelen! In onderstaande grafiek is het aantal meldingen en de spreiding over het jaar te zien:

Meldingen en incidenten

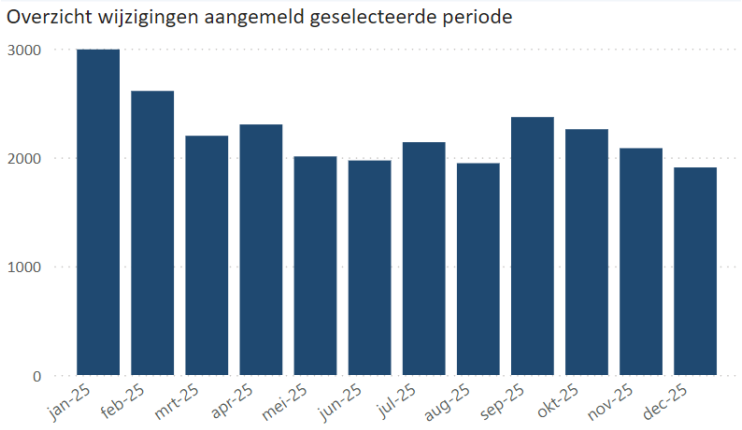


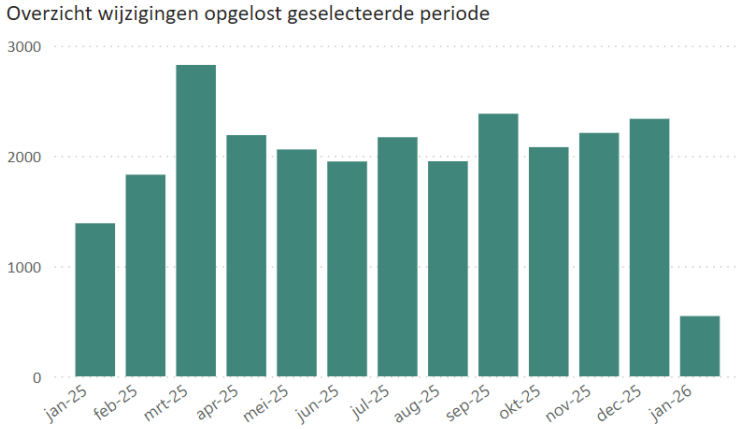


- Alle binnenkomende meldingen worden door iRvN geregistreerd en opgevolgd. Hiervoor wordt gebruikgemaakt van TopDesk als registratiesysteem, waarin zowel meldingen als wijzigingen worden vastgelegd;
- Door iedere melding vast te leggen ontstaat inzicht in aard, omvang en doorlooptijd, en kan de afhandeling worden gemonitord en waar nodig bijgestuurd;
- In 2025 zijn er ruim 31.450 meldingen gedaan. En daarvan waren er 23.565 zogenaamde incidenten. Een **incident** is een specifieke vorm van een melding. Het gaat om een verstoring die de normale werking van de IT-dienstverlening aantast of dreigt aan te tasten, bijvoorbeeld wanneer een applicatie niet beschikbaar is of wanneer meerdere gebruikers worden geraakt;
- Voor het oplossen van meldingen hebben we afspraken met de gemeenten gemaakt. In 2025 zijn de meldingen voor 83% binnen die afspraken opgelost.

Wijzigingen

Een wijziging is een aanpassing aan de IT-dienstverlening. Dit wordt ook wel een change genoemd. Het kan gaan om een technische aanpassing, een uitbreiding van functionaliteit of een wijziging in de inrichting van systemen. Wijzigingen ontstaan vaak naar aanleiding van meldingen, incidenten of nieuwe wensen.





Alle wijzigingen worden, net als de meldingen, geregistreerd en opgevolgd in TopDesk. Zo houdt iRvN overzicht op wat wordt aangepast, waarom dat gebeurt en welke impact dit heeft op de dienstverlening. Binnen iRvN wordt onderscheid gemaakt tussen verschillende soorten wijzigingen:

- Standaardwijzigingen: dit zijn vooraf bekende en veel voorkomende aanpassingen met een laag risico, zoals het aanmaken van een account of het doorvoeren van een kleine instelling. Deze wijzigingen kunnen volgens vaste afspraken worden uitgevoerd.
- Normale wijzigingen: dit zijn wijzigingen die niet standaard zijn en daarom vooraf worden beoordeeld op impact, risico en planning, bijvoorbeeld het aanpassen van infrastructuur of het doorvoeren van grotere technische aanpassingen.
- Functionele wijzigingen: dit zijn wijzigingen die de werking of het gebruik van applicaties veranderen, bijvoorbeeld aanpassingen in processen, schermen of functionaliteit voor gebruikers.

In 2025 heeft de afdeling Dienstverlening 26.797 wijzigingen aangemaakt en bijna 26.000 zijn er ook daadwerkelijk uitgevoerd!
Een wijziging bestaat zelden uit slechts één activiteit: de 26.797 wijzigingen uit 2025 telden gezamenlijk 75.316 activiteiten!

TPM-audit en BIO

iRvN legt verantwoording af over de beheersmaatregelen die zij treft ten behoeve van haar deelnemers via een BIO Third Party Mededeling (TPM)-audit. Deze audit geeft inzicht in de mate waarin de inrichting en werking van deze maatregelen voldoen aan de eisen uit de Baseline Informatiebeveiliging Overheid (BIO) en verschaft deelnemers zekerheid en vertrouwen over de beveiliging van de door iRvN verleende dienstverlening.

Waar iRvN aantoonbaar wordt geaudit, hoeven afzonderlijke gemeenten deze onderdelen niet opnieuw te laten auditen. Dit draagt bij aan een efficiënte inrichting van toezicht en aan een duidelijke rolverdeling tussen iRvN en haar deelnemers.

Eind 2024 heeft de eerste formele TPM-audit plaatsgevonden. Deze audit betrof een deel van de BIO- en BIO2-maatregelen (waaronder * back-up en restore, * beheer van technische kwetsbaarheden, * change management, * cryptografie, * security incident management, * gebruikersauthenticatie, * autorisatiemanagement en * logging en monitoring). Van de circa zeventig beoordeelde maatregelen voldeed iRvN op slechts drie maatregelen gedeeltelijk. Vanuit veiligheidsoverwegingen worden deze maatregelen niet schriftelijk gespecificeerd. Desgewenst kan hierover mondeling toelichting worden gegeven.

Eind 2025 heeft de tweede TPM-audit plaatsgevonden. In deze audit is het aantal beoordeelde onderwerpen uitgebreid ten opzichte van de voorgaande audit. Naast eerder beoordeelde processen zijn onder meer

- identity and access management,
- netwerkbeveiliging,
- gegevensopslag en -uitwisseling,
- incident management en
- fysieke beveiliging

betrokken. Hiermee is sprake van een bredere dekking van de BIO-maatregelen.

De bevindingen bevestigen de voortgang die iRvN boekt in de continue ontwikkeling van haar informatiebeveiliging. Tegelijkertijd is vastgesteld dat met name op het gebied van rapportage nog duidelijke verbeterpunten bestaan. Deze bevindingen worden betrokken bij het verder verbeteren van processen en bij de inrichting van de verantwoording richting deelnemers.

Voor 2026 wordt in overleg met de deelnemers vastgesteld welke beheersmaatregelen uit de BIO2 in de volgende audit worden betrokken. Daarmee wordt het meerjarige groeipad richting een voorspelbare en herhaalbare uitvoering van informatiebeveiligingsprocessen voortgezet.