Gemeente
Amsterdam

Bestuurlijke rapportage informatiebeveiliging 2024

Marco van Beek - Chief Information Security Officer



Inhoud

1	Management samenvatting en aanbevelingen	3
2	Inleiding	6
3	Ontwikkelingen in het dreigingslandschap	7
4	Nieuwe regelgeving werpt zijn schaduw vooruit	8
5	Terugblik en vooruitblik	9
6	Verdieping	16
B	Bijlage: Voortgang aanbevelingen autorisatiebeheer 2024	19

1 Management samenvatting en aanbevelingen

Voor u ligt de bestuurlijke rapportage informatiebeveiliging 2024 van de gemeente Amsterdam. De rapportage is opgesteld door de Chief Information Security Officer (CISO) in het kader van zijn coördinerende en toezichthoudende functie op de informatiebeveiliging van de gemeente.

In de rapportage wordt aangegeven hoe de informatie van de gemeente Amsterdam is beveiligd, welke ontwikkelingen zich hierbij hebben voorgedaan en hoe risico's en dreigingen zich in het afgelopen jaar hebben ontwikkeld. Daarbij wordt ook aandacht besteed aan verbonden partijen en het netwerk digitale weerbaarheid Amsterdam-Amstelland.

Het college legt met deze rapportage verantwoording af bovenstaande onderwerpen over het afgelopen jaar en informeert daarmee de gemeenteraad.

De dreigingen en risico's op het gebied van informatiebeveiliging zijn groter dan ooit. Digitale dreigingen zijn er niet alleen door cybercriminaliteit - voor geldelijk gewin - maar ook door statelijke actoren, sabotage, spionage en inbreuk op de digitale infrastructuur.

Amsterdam is als hoofdstad een potentieel doelwit (voor wat betreft de gemeentelijke processen en informatiesystemen) maar het is ook een stad waar in Nederland essentiële bedrijven, instellingen en infrastructuur zijn geconcentreerd.

Nieuwe regelgeving (met name de Cyberbeveiligingswet die in de loop van 2025 van kracht wordt) stelt strenge eisen aan gemeenten, die door de Rijksoverheid voortaan worden gezien als essentiële entiteiten. Dat betekent dat Amsterdam stappen moet zetten en aantoonbaar haar digitale weerbaarheid op orde moet hebben; zover zijn we nu nog niet. Het goede nieuws is dat er een programma is ingericht dat met voorstellen komt hoe we dit gaan realiseren.

Intern is het van groot belang om het "eigen huis" verder op orde te brengen en te houden, zodat de risico's van langdurige uitval, onbetrouwbare of verwijderde informatie, en onvoldoende beveiligde vertrouwelijke informatie worden geminimaliseerd.

Extern is het van belang om als Amsterdam aansluiting te vinden en te houden bij nationale en internationale ontwikkelingen op het vlak van cyberveiligheid, en daarbij samen te werken met partijen in de stad en de regio.

In 2024 zijn er concrete stappen gezet om de informatiebeveiliging op een hoger niveau te brengen. De uitvoering van het BIO-programma (zie hoofdstuk 5 van dit verslag) is voortgezet en heeft ervoor gezorgd dat informatiebeveiliging inmiddels bij alle directies op de agenda staat. Een aantal directies heeft zijn BIO-verbeterprogramma (bijna) afgerond en heeft daarmee een hogere volwassenheid bereikt. Maar er zijn ook directies die achterblijven door onvoldoende commitment of capaciteit.

De nog openstaande verbeteracties worden in 2025 overgenomen in het programma om de nieuwe Cyberbeveiligingswet en de BIO2 (opvolger van de huidige BIO) te implementeren.

In het afgelopen jaar is een onderzoek gedaan naar de effectiviteit van de informatiebeveiligingsorganisatie van de gemeente. Daaruit komen voorstellen om de organisatie beter en meer in samenhang in te richten. Dit krijgt in 2025 zijn beslag.

Binnen het cluster DII wordt in toenemende mate integraal gewerkt aan kwaliteit. De samenwerking tussen de disciplines informatiebeveiliging, privacy en informatiebeheer is daarin essentieel.

Risicomanagement staat op de agenda, maar moet nog handen en voeten krijgen.

Bij de implementatie van een nieuw risicomanagement systeem is de slag gemaakt om risico's op het gebied van informatiebeveiliging (en ook privacy en informatiebeheer) hierin op te nemen. Compliance en risicomanagement op het gebied van informatiebeveiliging krijgen meer aandacht bij elke directie, maar de formalisering hiervan heeft aandacht nodig.

De belangrijkste risico's per eind 2024 zijn:

- logische toegangsbeveiliging;
- beheer van bedrijfsmiddelen;
- leveranciersmanagement;
- bewustwording;
- kwetsbaarheden in hardware en software.

De implementatie van de nieuwe Amsterdamse Digitale Werkomgeving is in 2024 grotendeels voltooid. Het i-domein is bezig om het volledige applicatielandschap onder een éénduidig beheer te brengen.

In 2024 is een nieuw samenwerkingsverband met organisaties in de stad en regio ontworpen: het netwerk digitale weerbaarheid Amsterdam-Amstelland , Komend jaar wordt dit formeel gelanceerd. Samen met specifieke acties richting de met Amsterdam verbonden partijen geeft dat een nieuwe focus op externe organisaties en de ook de digitale weerbaarheid van de Amsterdammer.

Aanbevelingen

Op verschillende gebieden lopen verbeteringen om meer in control te zijn. Daarbij geeft de CISO de volgende aanbevelingen mee aan de gemeente:

- Stuur actief op de voortgang van de implementatie van de Baseline Informatiebeveiliging Overheid bij alle clusters en directies. Realiseer waar nodig commitment bij de directies. Zet dit voort bij de nieuwe regelgeving (Cyberbeveiligingswet en BIO2) die dit jaar van kracht wordt.
- Stuur hierbij met name actief op de beheersing van stedelijke processen waarvan alle directies afhankelijk zijn.
- Definieer welke stedelijke kaders en tactische richtlijnen nodig zijn en stuur op de realisatie daarvan.
- Formaliseer het risicomanagement op het gebied van informatievoorziening, inclusief de relatie met de lijndirecties.
- Stel vast wat de belangrijkste applicaties van Amsterdam zijn (de kroonjuwelen) en geef deze voorrang bij het implementeren van single signon en autorisatiebeheer.
- Richt het beheer van webdomeinen in en zorg ervoor dat deze voldoen aan o.a. eisen op het gebied van veiligheid.
- Rond de implementatie van de generieke security dienstverlening af en blijf alert op risico's die daardoor niet worden afgedekt.
- Maak van de sturing op leveranciers een top-prioriteit, met name bij de strategische ICT-leveranciers.
- Actualiseer het crisishandboek i-domein, zorg ervoor dat de organisatie geëquipeerd is om grote incidenten en crisissen op te vangen en plan oefeningen structureel in.
- Organiseer structurele aandacht voor bewustwording.
- Last but not least: definieer zo concrete mogelijk wat er nodig is vanuit nieuwe regelgeving, vertaal dat in een realistische planning en stuur daarop.

2 Inleiding

Informatiebeveiliging is nooit klaar, alleen al door de ontwikkelingen in de buitenwereld (nieuwe dreigingen, risico's, regelgeving) en in de eigen organisatie (organisatieveranderingen, aangepaste processen, nieuwe informatiesystemen) is het nodig om jaarlijks te bepalen waar we staan en wat er nodig is.

Bij informatiebeveiliging is het essentieel om voortdurend te blijven inspelen op actuele risico's en dreigingen. 100% informatieveiligheid bestaat niet; voldoen aan wet- en regelgeving wil niet zeggen dat zich nooit een beveiligingsincident zal voordoen.
Ons doel is om de weerbaarheid van onze informatievoorziening op een voldoende niveau te houden en in control te zijn en te blijven.

De Chief Information Security Officer heeft binnen Amsterdam een functie als interne toezichthouder voor informatiebeveiliging en rapporteert jaarlijks over de stand van zaken. Hij maakt daarbij gebruik van rapportages die door de organisatie worden opgesteld, aangevuld met eigen waarnemingen.

In deze rapportage wordt het beeld geschetst over het jaar 2024. De ontwikkelingen op het dreigingslandschap worden benoemd. Nieuwe regelgeving is in aantocht, die het nodig maakt om nog scherper te kijken naar de aantoonbaarheid van wat de organisatie doet. Er is een terugblik op uitgevoerde acties en verbeteringen in het afgelopen kalenderjaar en er wordt vooruitgekeken naar 2025. Tenslotte is er een verdieping, gericht op incidenten, kwetsbaarheden en de ENSIA-rapportage.

In maart 2025 heeft het college de eerste stappen gezet om toe te werken naar meer digitale autonomie. Het streven is om minder afhankelijk te worden van niet-europese big-tech bedrijven: Amsterdam wil digitaal eigen keuzes wil kunnen blijven maken om de privacy, online veiligheid van en dienstverlening aan Amsterdammers te waarborgen.

Het is duidelijke dat informatiebeveiliging meer dan ooit een randvoorwaarde is bij het realiseren van deze nieuwe richting.

3 Ontwikkelingen in het dreigingslandschap

De dreigingen op het gebied van informatiebeveiliging ontwikkelen zich snel. Om hierop zicht te hebben en te houden sluiten we aan op het beeld van landelijke organisaties, aangevuld met informatie van onze strategische partners. En uiteraard zien we wat er in onze eigen organisatie gebeurt.

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) brengt jaarlijks het Cyber Security Beeld Nederland (CSBN) uit. Voor Amsterdam als hoofdstad van Nederland is dit een belangrijke bouwsteen voor ons risicobeeld.

Het CSBN 2024 (uitgebracht in oktober 2024) geeft ons een waardvol beeld over de ontwikkelingen in het afgelopen jaar, zowel specifiek in nederland als daarbuiten.

De hoofdbevindigen zijn:

- De digitale dreiging tegen Nederland is groot en divers, en cyberaanvallen zijn voornamelijk afkomstig van statelijke en criminele actoren. In deze turbulente geopolitieke tijden intensiveren statelijke actoren hun activiteiten en verbreden zij hun capaciteiten, waarbij zij gebruik maken van een bredere gereedschapskist. Criminele actoren voeren op grote schaal aanvallen uit en handelen daarbij opportunistisch. Grootschalige uitval van digitale processen vormt eveneens een dreiging.
- Digitale risico's vragen om een brede manier van beheersing. Ze zijn dynamisch en worden beïnvloed door vele verschillende factoren. Het bredere digitale ecosysteem, met daarbinnen monoculturen, en de hoge mate van digitalisering zorgen ervoor dat risico's met elkaar verbonden raken.
- De veiligheid van digitale processen is en blijft essentieel in onze maatschappij en is dus onlosmakelijk verbonden met de nationale veiligheid. Het belang van digitale veiligheid concurreert met andere belangen.

Voorbeeld van incidenten in 2024 zijn:

- Aanvallen met Ransomware, met als doel losgeld danwel verstoring van cruciale bedrijfsprocessen.
- DDOS-annvallen, bedoeld om websites onbereikbaar te maken.
- Landelijke storingen, zoals de uitval van het NAFIN-netwerk van Defensie, waardoor ook DIGID een tijdlang onbruikbaar was.
- Wereldwijde storingen, zoals bij Crowdstrike (nota bene een 'zeer toonaangevend ICT-beveiligingsbedrijf.
- Cyberaanvallen door statelijke actoren.

De belangrijkste boodschap uit dit dreigingsbeeld voor Amsterdam is dat elke organisatie en elke leverancier (hoe professioneel ook) slachtoffer kan worden, en dat het loont om de informatiebeveiligng beter op orde te hebben dan anderen (met name cybercrimielen kiezen als eeste voor relatief makkelijke doelwitten). Het voorbereiden op mogelijke incidenten is essentieel, o.a. door het oefenen van cybercrises.

4 Nieuwe regelgeving werpt zijn schaduw vooruit

Eind 2022 is de Europese richtlijn Network and Information Security 2 (NIS2) aangenomen. De richtlijn wordt in Nederland omgezet naar de Cyberbeveiligingswet, die naar verwachting in oktober 2025 van kracht wordt. Ook de gemeente Amsterdam moet aan de Cyberbeveiligingswet voldoen. De Cyberbeveiligingswet stelt het college van B&W verantwoordelijk voor een juiste uitvoering van de wet.

De Gemeente Amsterdam zal volgens de wet ‘passende en evenredige maatregelen’ moeten treffen op geïdentificeerde risico’s ten aanzien van de beveiliging van netwerk- en informatiesystemen. Het gaat hierbij niet alleen om de beveiliging van kantoorautomatisering, maar nadrukkelijk ook van de operationele techniek zoals (de bediening voor) sluizen, tunnels en bruggen. De wet stelt onder meer verplichtingen op het gebied van risicomanagement, leveranciersmanagement, functioneel beheer en specifieke beveiligingsmaatregelen. Daarnaast verplicht de wet organisaties om melding te maken van alle (bijna) incidenten die (kunnen) leiden tot een significante verstoring van de belangrijkste processen van de organisatie. Een groot deel van de verplichte maatregelen is uitgewerkt in de Baseline Informatiebeveiliging Overheid 2 (BIO2). Deze BIO2 zal voor overheidsorganisaties verplicht worden gesteld onder de Cyberbeveiligingswet. De Gemeente Amsterdam is, in navolging van het BIO1 traject, al gestart met de voorbereidingen op de implementatie hiervan.

De Rijksdienst voor Digitale Infrastructuur (RDI) is aangewezen als toezichthouder voor de overheidsorganisaties waarop de wet van toepassing is. De RDI is nog bezig het toezicht vorm te geven en heeft aangegeven zoveel mogelijk aan te willen sluiten op bestaande verantwoordingsmechanismen zoals de ENSIA. Komend jaar zal de RDI hier naar verwachting meer duidelijkheid over geven.

In september 2024 is een programmateam gevormd dat moet zorgen dat de Gemeente Amsterdam aan de Cyberbeveiligingswet gaat voldoen. Uit een eerste analyse van het programmateam blijkt dat er binnen de Gemeente Amsterdam al veel is geregeld op de verplichte onderdelen van de wet. Om te voldoen aan de wet moeten er echter nog wel een aantal stappen genomen worden. Belangrijke onderdelen zijn daarbij de verdere professionalisering van het risicomanagement, het actualiseren en aanpassen van het incidentmanagementproces, het op orde krijgen van het functioneel beheer voor IT en OT en het samenbrengen van de IT- en OT-domeinen op deze processen. Het programmateam heeft een voorstel uitgewerkt voor het inrichten van de governance op het programma. Vanwege de stedelijke impact van het programma is het voorstel om het opdrachtgeverschap te beleggen bij de CIO/Stedelijk Directeur DII en een stuurgroep in te richten met de belangrijkste interne stakeholders. Met behulp van de opdrachtgever en stuurgroep zal het programmateam de benodigde acties uitzetten binnen de organisatie.

5 Terugblik en vooruitblik

De organisatie van de informatiebeveiliging

In 2024 is onderzocht hoe we meer samenhang kunnen creëren in de informatiebeveiligingsorganisatie van Amsterdam. Er zijn verschillende informatiebeveiligingsfuncties/rollen ingericht die nog te veel werken vanuit hun eigen doelstellingen, zonder de juiste samenhang. Daardoor werkt het geheel niet optimaal als één organisatie en is daarmee onvoldoende effectief.

De uitkomst van het onderzoek is dat we een Informatiebeveiligingshuis inrichten, waarmee we integraal gaan sturen op informatiebeveiliging. Een kernteam werkt dit uit. Implementatie hiervan vindt plaats in 2025.

Amsterdam heeft als hoofdstad veel relaties met allerlei partijen. In 2024 is er met name in G4-verband veel contact geweest op het gebied van informatiebeveiliging om aanpak en risico's met elkaar te delen. Ook participeert Amsterdam waar nodig in landelijke gremia.

Voortgang implementatie Baseline Informatiebeveiliging Overheid

Gemeenten moeten voldoen aan de Baseline Informatiebeveiliging Overheid (BIO), waarin de kaders voor alle overheidsorganisaties zijn gesteld.

Binnen Amsterdam wordt een programmatische aanpak gehanteerd. Directies hebben analyses uitgevoerd en verbeterplannen vastgesteld. Security officers adviseren hierbij en helpen de voortgang te bewaken.

Eind 2024 is de implementatie van de BIO-verbeterplannen bij 7 directies afgerond. Bij alle directies tezamen is omgeveer 2/3 van het verbeteracties afgerond. Er zijn finke verschillen in voortgang: er zijn directies die goede voortgang maken, maar er zijn ook directies waarbij veel te weinig voortgang zichtbaar is. Ook de verschillen tussen de clusters zijn opvallend. Commitment vanuit directies is essentieel voor de komende periode.

Aansluiting directies op stedelijke processen

Informatiebeveiliging is afhankelijk van een aantal stedelijke processen. Denk aan:

- bewustwording (weten medewerkers hoe ze met informatie moeten omgaan);
- leveranciersmanagement (welke eisen stellen we aan leveranciers en hoe sturen we als concern daarop);
- het beheer van onze generieke ICT-voorzieningen en applicaties;
- Het indienst-, doorstroom- en uitstroomproces van medewerkers.

De beheersing van deze processen is nog niet altijd op het juiste niveau. Bij het BIO-programma is vooral gestuurd op de implementatie bij afzonderlijke directies en minder op het op orde krijgen van deze stedelijke processen. Afzonderlijke directies weten daardoor onvoldoende of ze kunnen steunen op de kwaliteit van de stedelijke processen.

Beleid en kaders
Het strategisch beleidskader informatiebeveiliging is vastgesteld door het College in 2020. Actualisatie was gepland in 2024, maar gedurende het jaar is besloten om dit uit te stellen, zodat daarin de impact van nieuwe wetgeving en de vernieuwde informatiebeveiligingsorganisatie kan worden meegenomen

Tactische richtlijnen (de vertaling van abstracte normen naar concrete richtlijnen voor de Amsterdamse organisatie) hebben bij de implementatie van de BIO te weinig aandacht gekregen. Daardoor missen organisatie-onderdelen soms scherpte in wat ze moeten doen.

In 2024 zijn wel enkele richtlijnen opgesteld, maar formele vaststelling hiervan en communicatie hierover naar de lijndirecties heeft nog onvoldoende plaatsgevonden.

Implementatie risicomanagement
Informatiebeveiliging gaat niet alleen over het implementeren van maatregelen die in de BIO (of andere richtlijnen) staan benoemd, het gaat ook (en steeds meer) over het afwegen en beheersen van risico's.

Doordat onze security officers beter betrokken zijn bij directies (via de BIO-aanpak en bij projecten en opgaven) dan in het verleden ontstaat een steeds beter zicht op risico's. Door het signaleren hiervan bij directies kan op het juiste niveau een risicoafweging plaatsvinden en worden bijgestuurd.

Amsterdam heeft ervoor gekozen om één risicomanagement systeem te implementeren, waarin organisatiebreed de status van compliance en risicomanagement wordt vastgelegd, zodat daarop kan worden gestuurd.

In samenwerking met de vakgebieden privacy en informatiebeheer en directie Middelen en Control is in 2024 is het nieuwe risicomanagement-systeem zodanig ingericht dat directies ook hun informatiebeveiligingsrisico's hierin kunnen vastleggen en de afhandeling hiervan kunnen monitoren.

Inmiddels (eind 2024) hebben alle directies informatiebeveiligingsrisico's vastgelegd die in het kader van de BIO zijn gesignaleerd, aangevuld met risico's die vanuit de dagelijkse praktijk zijn gesignaleerd.

De belangrijkste risico's per eind 2024 liggen op het gebied van:

- logische toegangsbeveiliging;
- beheer van bedrijfsmiddelen;
- leveranciersmanagement;
- bewustwording;
- kwetsbaarheden in hardware en software.

De risico's zijn per directie vastgelegd. Het aggregeren van deze risico's op stedelijk niveau is nog niet ingericht en is een belangrijk aandachtspunt voor 2025. Ook de *formalisering* van het risicomanagement (risico-afweging, risico-acceptatie en het sturen op het wegwerken van gesignaleerde risico's door zowel lijndi-

recties als het i-Domein) is nog een belangrijk verbeterpunt.

Autorisatiebeheer
In 2024 is (opnieuw) veel aandacht besteed aan het verbeteren van het autorisatiebeheer van onze belangrijkste informatiesystemen. De afspraak is dat voor relevante informatiesystemen 2x per jaar de autorisaties worden getoetst. Eind 2024 is dit voor het grootste deel van de bij het i-domein in beheer zijnde informatiesystemen gerealiseerd. Het verbeteren van het zicht is een blijvend aandachtspunt. In 2025 gaat worden gewerkt aan privileged access (het monitoren van bijzondere rechten) en het oppakken van logging en monitoring in algemene zin.

Een aandachtspunt blijft het autorisatiebeheer bij informatiesystemen die (nog) niet in beheer zijn bij het i-domein.

Pentests
Amsterdam beveiligt zijn informatiesystemen met diverse preventieve en detectieve maatregelen, maar het is daarnaast nodig om de robuustheid van de beveiliging expliciet te testen. Het uitvoeren van pentests (een in onze opdracht uitgevoerde technische test om de beveiliging van een toepassing te doorbreken) is in 2024 geprofessionaliseerd. Amsterdam werkt met vaste externe partijen die deze testen in onze opdracht uitvoeren. Het bewustzijn dat pentests noodzakelijk zijn is steeds beter aanwezig. Het aantal uitgevoerde tests is in 2024 toegenomen: in 2024 zijn 48 verschillende toepassingen getest en zijn de hierbij gesignaleerde bevindingen weggewerkt.

Single signon
In de afgelopen jaren is een nieuwe, veilige, stedelijke ICT-werkomgeving ontworpen. De uitrol daarvan is inmiddels bijna afgerond; alleen de GGD moet de werkomgeving in 2025 nog invoeren.

De toegang tot deze werkomgeving is voorzien van multi-factor authenticatie (een wachtwoord in combinatie met een token) en is daardoor aanzienlijk veiliger dan in het verleden.

De gedachte achter deze werkomgeving is dat alle applicaties uitsluitend via deze voorziening worden ontsloten. Daarmee wordt voorkomen dat verschillende toegangssystemen moeten worden beheerd, beveiligd en gemonitord en dat gebruikers veel verschillende wachtwoorden moeten onthouden. Kortom: meer veiligheid en meer gebruiksgemak. Zover is het nog niet; eind 2024 is minder dan de helft van onze applicaties aangesloten op deze voorziening. Er wordt een planning opgesteld om de applicaties op basis van risico (aard van de applicatie, gevoeligheid, aantal gebruikers) te kunnen aansluiten.

Toegestane en niet toegestane applicaties
Laptops en telefoons van medewerkers worden door de gemeente actief beheerd. Patches die (bijvoorbeeld vanuit veiligheid) nodig zijn worden verplicht doorgevoerd. Toepassingen vanuit landen met offensieve cybercampagnes tegen Nederland worden (in navolging van de Rijksoverheid) geweerd. Hierover is aan medewerkers gecommuniceerd.

Eind 2024 is het stedelijke beleid voor generatieve AI vastgesteld. Daarin is aangegeven dat het niet is toegestaan om generatieve AI-toepassingen te gebruiken, tenzij deze aantoonbaar voldoen aan onze eisen, onder andere vanuit privacy. Dat betekent concreet dat ambtenaren geen gebruik mogen maken van gratis online GenAI-toepassingen zoals *ChatGPT, Deepseek, Gemini* en *Midjourney.* Ook ten aan zien van *Micosoft Copilot* wordt erop gestuurd dat aan de eisen wordt voldaan voordat Amsterdam dit overweegt om te gaan gebruiken.

Webdomeinen
Amsterdam beschikt over een groot aantal websites en webdomeinen, waarmee informatie wordt aangeboden op internet. Webdomeinen moeten voldoen aan landelijke open standaarden, o.a. op het gebied van veiligheid en toegankelijkheid. Dat is op dit moment maar ten dele het geval: www.amsterdam.nl voldoet aan de landelijke eisen, maar vele andere webdomeinen van de gemeente Amsterdam voldoen er niet of niet volledig aan. Het beheer van webdomeinen is binnen de gemeente nog steeds onvoldoende ingericht. Initiatieven om dit te verbeteren hebben tot nu toe onvoldoende effect gehad.

Security monitoring
Amsterdam heeft enkele jaren geleden, als reactie op toegenomen dreigingen, een security operations center (SOC) ingericht. Het doel daarvan was om niet alleen preventief de beveiliging op orde te hebben maar ook dag en nacht monitoring daarop in te richten, zodat we direct kunnen reageren op dreigingen en incidenten, ook buiten kantooruren.

In 2024 is de SOC-dienstverlening vernieuwd en uitgebreid, zodat we nog beter weerbaar zijn en sneller kunnen reageren op dreigingen. We maken daarbij gebruik van een nieuwe, zeer gespecialiseerde externe partij. Eind 2024 is de basis hiervoor ingericht en er worden stappen gezet om de security monitoring als een schil over ons hele landschap (ICT-infrastructuur en applicaties) te leggen, zodat dit landschap als geheel kan worden beschermd tegen de toenemende dreigingen. In 2025 moet dit worden afgerond.

Cloud platform
Amsterdam heeft in de afgelopen jaren een cloud platform ingericht, waarop applicaties kunnen worden ontwikkeld en worden verwerkt. Bij de inrichting hiervan is zeer veel aandacht besteed aan informatiebeveiliging en privacy. Applicaties moeten voldoen aan strenge eisen vanuit dit platform. In 2025 is gepland om daar bovenop een extra beveiligde omgeving in te richten voor applicaties met hoog vertrouwelijke gegevens.

Sturing op leveranciers
In de afgelopen jaren zijn door Amsterdam steeds meer I-taken uitbesteed aan externe partijen.

Uitbesteding vraagt om actieve regie en sturing, zodat de gemeente (als eigenaar van de gegevens) kan vaststellen of de beveiliging op orde is en waar nodig kan bijsturen.

Amsterdam maakt gebruik van een veelheid aan partijen en de regie is nog niet altijd op orde.

Dat is zichtbaar op twee segmenten:

- bij de strategische ICT-leveranciers (werkplek, hosting, netwerk). Issues hierbij kunnen effect hebben op de veiligheid en continuïteit van de generieke ICT-diensten aan de Amsterdamse organisatie. Het risicomanagement op deze leveranciers is in 2024 verbeterd, maar er zijn nog stappen nodig om beter in control te komen.
- SAAS-leveranciers. Dit zijn leveranciers van software as a service: we nemen een dienst af, de leverancier beheert de software. Hierdoor moeten wij kunnen steunen op de kwaliteit van de beheerorganisatie via certificeringen en Assurance rapportages. In 2024 zijn hierop goede stappen gezet om het zicht te kunnen krijgen en hierop te sturen, met name bij een 20-tal belangrijke applicaties. Voor de overige applicaties wordt een plan van aanpak opgesteld.

Business Continuity Management

De continuïteit van de informatievoorziening is nauw verweven met het onderwerp Business Continuity Management (BCM).

In de eerste helft van 2024 is de aanpak van BCM voor de gemeente Amsterdam uitgewerkt en is stedelijk beleid vastgesteld. De kern hiervan is dat bij elke directie een continuïteitsoefening wordt uitgevoerd en op basis daarvan een BCM-plan wordt vastgesteld. In 2024 hebben 17 directies hun continuïteitsplannen reeds opgeleverd en is deze aanpak bij nog eens 17 directies opgestart. Hiermee staat de bewustwording van bedrijfscontinuïteit bij veel directies duidelijk op de agenda. Voor 2025 is er een planning vastgesteld om ook bij de andere directies hiermee te starten.

Weerbaarheid bij cybercrises

Om snel en adequaat te kunnen reageren bij grote incidenten en cybercrises is het belangrijk om de organisatie daarop voor te bereiden, crisisdraaiboeken klaar te hebben liggen en vooral om regelmatig te oefenen. Binnen het i-domein van de gemeente is daartoe een crisisteam ingericht en crisishandboek opgesteld.

Begin 2024 heeft de evaluatie plaatsgevonden van de landelijke ISIDOOR cyberoefening die elke 2 jaar vanuit de Rijksoverheid wordt georganiseerd. Amsterdam heeft daaraan voor de 1e keer meegedaan.

In november 2024 heeft een cyberoefening plaatsgevonden met gemeenten in de regio, de politie en de veiligheidsregio. Hierbij is vooral ingezoomd op de impact van een cybercrisis en op de rol die organisaties daarbij hebben.

Het is de bedoeling om jaarlijks oefeningen te blijven organiseren met het crisisteam i-Domein, in wisselende samenstellingen.

Bewustwording

NIS2 geeft aan dat bewustwording (zowel bij bestuurders als bij medewerkers) essentieel is om de veiligheid op orde te hebben. Amsterdam is een grote en complexe organisatie met veel

directies en werkprocessen. De effectiviteit van informatiebeveiliging is afhankelijk van technische en procedurele maatregelen maar zeker ook van de wijze waarop alle medewerkers omgaan met informatie.

In de afgelopen jaren is er relatief weinig aandacht gegeven aan bewustwording. Wel zijn bij afzonderlijke directies bewustwordingssessies gehouden met MT's en bij medewerkersbijeenkomsten. Voor 2025 is gepland om de e-learnings voor privacy en informatiebeveiliging te actualiseren, informatie beter beschikbaar te maken, gericht te werken aan bewustwording bij het management en een bewustwordingscampagne uit te voeren.

Netwerk digitale weerbaarheid: externe focus

De risico's op het gebied van informatiebeveiliging beperken zich niet tot de grenzen van onze organisatie en de eigen processen en informatiesystemen. Organisaties werken steeds meer samen in ketens, maken gebruik van gedeelde informatiesystemen en wisselen informatie uit.

In november 2023 is voor de tweede keer een agenda digitale stad vastgesteld. Hierin geeft het college aandacht aan digitale toegankelijkheid, digitale vaardigheden van Amsterdammers en onderwerpen als AI en Algoritmen.

Digitale weerbaarheid/veiligheid is het laatste (maar niet het minst belangrijke) thema in de agenda digitale stad. Daarmee wordt ook bestuurlijk en richting de buitenwereld bevestigd dat veiligheid een essentiële randvoorwaarde is bij de digitale stad.

In het afgelopen jaar is het *netwerk digitale weerbaarheid Amsterdam-Amstelland* ontworpen, dat in 2025 officieel wordt gelanceerd.

Hierin worden de volgende sporen benoemd:

- Het versterken van de **digitale veerkracht**: onder jongeren, ondernemers, senioren en laaggeletterden om de weerstand tegen cybercriminaliteit te vergroten door het borgen opschalen van preventieve interventies om dader- en slachtofferschap te voorkomen.
- Het versterken van **kennis, talent en expertise**: door enerzijds een actueel beeld te verkrijgen van het arbeidstekort omtrent cybersecurity en het arbeidstekort op dit vlak terug te dringen en anderzijds het structureel vormgeven van de kennisontwikkeling van betrokken organisaties.
- Het **versterken van de informatiepositie**: om betrokken organisaties beter te beschermen tegen de hybride dreigingen door een netwerk te bouwen op het niveau van de Chief Information Security Officer (CISO) waar in besloten kring informatie en ervaringen kunnen worden uitgewisseld.

Verbonden partijen

Bij een aantal partijen waarmee Amsterdam samenwerkt of verbonden is hebben in de afgelopen jaren incidenten plaatsgevonden op het gebied van informatiebeveiliging. Daarbij bleek steeds weer dat het is belangrijk om, onder andere vanuit het aandeelhoudersbelang, hierop de vinger aan de pols te houden (toezicht op afstand) zonder de verantwoordelijkheid van de betreffende organisatie over te nemen.

Amsterdam heeft *i-kaders verbonden partijen* vastgesteld. Hierin wordt aangegeven welke afspraken wij willen maken met verbonden partijen over o.a. informatiebeveiliging, informatiebeheer en privacy. Op basis hiervan zijn acties in gang gezet om met de verbonden partijen -deelnemingen van de gemeente Amsterdam - afspraken te maken over de afspraken, rapportages en verantwoording over onder andere informatiebeveiliging. In 2025 wordt als eerste gefocust op een drietal belangrijke deelnemingen.

6 Verdieping

Incidenten

Het is niet mogelijk om incidenten op het gebied van informatiebeveiliging te voorkomen.

De IT-wereld is continu in beweging en vrijwel dagelijks worden lekken in software ontdekt.

Er zullen zich altijd op enig moment informatiebeveiligingsincidenten voordoen waarvan we vervolgens kunnen leren en het geleerde kunnen toepassen binnen onze securityprocessen.

Binnen de organisatie is er een vastgesteld proces om informatiebeveiligingsincidenten te melden, registreren en af te handelen. Informatiebeveiligingsincidenten van medewerkers worden centraal geregistreerd, geanalyseerd en afgehandeld. Incidenten krijgen de classificatie laag, midden of hoog. Daarnaast ontvangen we grote aantallen technische security meldingen die voor het overgrote deel geautomatiseerd worden opgelost.

Jaarlijks rapporteren we over het geheel op hoofdlijnen in deze rapportage.

Daarbij is het volgende van belang:

- Datalekken worden apart geregistreerd en gerapporteerd via de jaarrapportage van de Functionaris Gegevensbescherming.
- Informatiebeveiligingsincidenten die een relatie hebben met fraude / integriteit worden behandeld door Bureau Integriteit en maken onderdeel uit van hun rapportage.

In 2024 is het aantal *door medewerkers* gemelde incidenten afgenomen ten opzichte van het jaar ervoor. Het aantal technische security meldingen vanuit strategische partners (die in opdracht van Amsterdam beheerwerkzaamheden verrichten) is in deze rapportage voor de eerste keer inzichtelijk gemaakt.

15% van alle security meldingen heeft betrekking gehad op de werkplekken van de gemeente, 78% op de externe beheerde IT-systemen en applicaties, 6% op de eigen beheerde IT-systemen en minder dan 1% heeft betrekking gehad op de infrastructuur die door de gemeente op alle locaties wordt gebruikt.

De meest voorkomende Informatiebeveiligingsincidenten van medewerkers (in totaal 135 meldingen) zijn frauduleuze SMS/APP's (44%, vorig jaar 49%), verdachte mail/post (18%, vorig jaar 24%), en frauduleuze telefoontjes (10,5%, vorig jaar 8%).

Ten opzichte van het vorige jaar (2023) is het aantal Informatiebeveiligingsincidenten gemeld door medewerkers gedaald met 66%. Wel zien we een groot aantal technisch security incidenten, maar door de geautomatriseerde manier van oplossen hebben deze hebben relatief gezien tot weinig langdurige verstoringen geleid voor de medewerkers.

De meeste incidenten hebben de classificatie laag of midden, er zijn in 2024 131 incidenten geweest met de classificatie hoog.

Op de security incidenten is tijdig actie ondernomen waardoor de medewerker en de BOB minimale verstoring hebben ervaren van de IT dienstverlening.

Incidenten die impact hebben gehad op de beschikbaarheid van ICT voorzieningen.

In 2024 zijn er 41 incidenten geweest die een serieuze impact hebben gehad op de potentiële beschikbaarheid van ICT-dienstverlening richting de gemeentelijke organisatie (en soms de burger). Het betrof hier vooral storingen in netwerken en servers, storingen bij externe leveranciers/beheerpartijen, fouten bij wijzigingen en issues met certificaten.

Vanuit directie Digitake Voorzieningen zijn verbeteracties gedefinieerd om toekomstige incidenten te voorkomen.

Kwetsbaarheden

Amsterdam ontvangt van het NCSC en de Informatiebeveiligingsdienst zeer regelmatig signalen over kwetsbaarheden in hardware en software. Bij een dergelijke melding wordt, afhankelijk van het risico, actie ondernomen. In 2024 was dit van toepassing bij 17 (vorig jaar 27) high/high meldingen (hoog risico / hoge impact) geclassificeerde meldingen.

Door het tijdig afhandelen van deze meldingen is voorkomen dat aanwezige kwetsbaarheden, op technische systemen van de Gemeente, door kwaadwillende konden worden uitgebuit.

Meldpunt ethische hackers

Het in november 2022 ingestelde digitale meldpunt voor ethisch hackers heeft de stad geholpen om kwetsbaarheden eerder te identificeren en weg te nemen en draagt daardoor bij aan de veiligheid van onze informatievoorziening. Bij het meldpunt worden alleen die kwetsbaarheden geaccepteerd die aantoonbaar zijn en binnen het beleid van de op gecoördineerde wijze omgaan met het openbaar maken van gemelde kwetsbaarheden vallen.

Totaal 74 Vermeldingen op de Hall of Fame

Melders van kwetsbaarheden kunnen naar wens een vermelding krijgen op de digitale Hall of Fame van de informatiebeveiligingsdienst voor gemeenten. Voor Amsterdam zijn ook in 2024 weer verschillende vermeldingen op geplaatst, zie https://www.informatiebeveiligingsdienst.nl/responsible-disclosure/2023-coordinated-vulnerability-disclosure-hall-of-fame/

ENSIA
Via de landelijke ENSIA-methodiek (Eenduidige Normatiek Single Information Audit) legt de gemeente jaarlijks verantwoording af over de kwaliteit en veiligheid van enkele informatiestelsels. U wordt daarover separaat geïnformeerd. In deze rapportage wordt, voorzover dat nodig is, de relatie met informatiebeveiliging gelegd.

Suwinet
De gemeente voldoet voor Suwinet niet aan alle landelijke normen voor informatiebeveiliging. De volgende risico's zijn hierbij benoemd:

- Als toegangsrechten niet bijtijds worden beëindigd of gewijzigd, bestaat het risico op onbevoegde kennisname van Suwinet-gegevens.
- Indien gebruikers van Suwinet-gegevens zich niet of onvoldoende bewust zijn van de (hoge) vertrouwelijkheid, bestaat het risico dat deze gegevens onvoldoende worden beschermd.
- Als de verwerking van Suwinet (persoons)gegevens niet overeenkomstig toepasselijke wet- en regelgeving plaatsvindt, wordt hierdoor de Algemene verordening gegevensbescherming overtreden.

De bij Suwinet geconstateerde risico's zijn in lijn met wat er in hoofdstuk 5 van deze rapportage is benoemd.

Voor de verschillende aansluitingen op Suwinet die niet voldoen zijn verbeterplannen opgesteld. De verbetermaatregelen bestaan uit het zorgen dat elke nieuwe medewerker binnen 3 maanden na indiensttreding een bewustwordingstraining heeft gevolgd, dat deze deelname wordt vastgelegd, en dat hierop door het management wordt gemonitord. Daarnaast wordt de toegang en toekenning van autorisaties verbeterd en bijgehouden, en wordt het verwerkingsregister op de juiste wijze bijgewerkt.

DigiD
De DigiD-aansluitingen van de gemeente Amsterdam voldoen aan de gestelde eisen, met de aanbeveling dat het beleidskader informatiebeveiliging geactualiseerd moet worden.

BIO
ENSIA werkt met een jaarlijks zelfevaluatie waarin status van de BIO-controls wordt uitgevraagd. Amsterdam heeft er al eerder voor gekozen om destatus en vootgang op de BIO via voortgangsrapportages per directie/cluster in beeld te brengen. Het voordeel hiervan is dat een beter en fijnmaziger beeld bestaat. Voor dit beeld wordt verwezen naar hoofdstuk 5 van dit verslag.

B Bijlage: Voortgang aanbevelingen autorisatiebeheer 2024

In deze bijlage wordt de status aangegeven van de verbeteracties op het gebied van autorisatiebeheer per eind 2024.

Hierin worden de onderstaande termen gebruikt:

- Klaar als — Wat moet er (nog) gebeuren om de realisatie vd aanbeveling af te ronden?
- Planning — Wanneer (welk kwartaal) wordt afronding gepland? (gearceerd is laatste planning, dus datum afronding aanbeveling)
- StaVaZa — Hoe staat het er nu, op moment van rapportage, mee?
- Dus — Groen = geen zorgen, oranje = in de gaten houden, rood = probleem.

ACAM: Autorisatiebeheer van applicaties in scope jaarrekeningcontrole: Wij vragen er aandacht voor dat:

1. De periodieke controle in 2024 in lijn met de BIO wordt uitgevoerd, dat is (minimaal) twee keer per jaar.
2. De periodieke controle van uitgegeven speciale rechten, eveneens in lijn met de BIO, per kwartaal wordt uitgevoerd.
3. De monitoring op ongewenste functievermenging in lijn met de BIO wordt uitgevoerd.

Klaar als:	Planning:	Stand van zaken:	Dus
De 20 ACAM-applicaties op orde zijn qua gebruikers-toegang (controle per 6 maanden)	Q4-24	3 applicaties nog niet op orde, risico's wel geaccepteerd. De risicoacceptaties hierover zijn formeel vastgelegd in het risicomanagementsysteem. Daarmee voldoen we aan de BIO.	(1)
De 20 ACAM-applicaties op orde zijn qua speciale toegang (controle per 3 maanden)	Q1-25	Het aangepaste proces is vastgesteld in Q4-24 en gestart in Q1-25. De eerste controles zijn inmiddels uitgevoerd en vastgelegd voor zeven van de twintig applicaties. In de loop van Q2 is dat naar verwachting gereed voor allemaal. In Q2 volgt de tweede ronde controles.	(2)
De 20 ACAM-applicaties op orde zijn qua controle functievermenging	Q1-25	Voor de 20 betreffende applicaties wachten we op het oordeel van de ACAM. Er is een initiatief gestart om met een groep specialisten een taskforce in te richten die met een aanpak komt op het gebied van functievermenging, in combinatie met het onderwerp logging en monitoring, dat hieraan verbonden is. Deze taskforce zal op basis van een grondige analyse een concrete aanpak vormgeven (Q2 gereed). Het operationaliseren van deze aanpak zal in Q3 starten.	(3)
Het proces voor álle applicaties is ingericht en werkt	Q2-25	Alle controles conform BIO (per 6 of per 3 maanden) ingeregeld. Van alle applicaties is geregistreerd welke per 3 of per 6 maanden moeten worden gecontroleerd.	(4)

Toelichting: het gaat in eerste instantie om de 20 applicaties in scope van ACAM. En van die applicaties dan de controles op gebruikerstoegang, op speciale toegang en op functievermenging. En als dat allemaal voor die 20 goed gaat wordt het voor álle applicaties ingeregeld.

1. Op schema.
2. Oranje, want enige vertraging
3. Oranje, want vertraging t.o.v. oorspronkelijke planning
4. Ongewijzigd en op schema. Het betreft de applicaties in beheer bij het i-domein en die in aanmerking komen voor deze controles.

