Gemeente Amsterdam
Bestuurlijke rapportage informatiebeveiliging 2025

Marco van Beek
Chief Information Security Officer
Gemeente Amsterdam

Inhoudsopgave

1 Management samenvatting en aanbevelingen 3

2 Inleiding 6

3 Ontwikkelingen in het dreigingslandschap.....7

4 Regelgeving.....9

5 Terugblik en vooruitblik.....10

6 Samenwerking in het regionale netwerk.....15

7 Nieuwe thema's: weerbaarheid en autonomie 16

8 Incidenten.....17

9 ENSIA.....20

1 Management samenvatting en aanbevelingen

Inleiding

Voor u ligt de bestuurlijke rapportage informatiebeveiliging 2025 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 het netwerk digitale weerbaarheid Amsterdam-Amstelland.
Het college legt met deze rapportage verantwoording af over de beheersing van de informatiebeveiliging in het afgelopen jaar en informeert daarmee de gemeenteraad.

De dreigingen en risico's op het gebied van informatiebeveiliging zijn groot, we zien dat elke dag om ons heen. Digitale dreigingen zijn er niet alleen door cybercriminaliteit - voor geldelijk gewin - maar ook door statelijke actoren, sabotage, spionage en inbreuk op de digitale infrastructuur. Bondgenoten zijn niet meer vanzelfsprekend bondgenoten, dus we moeten rekening houden met inbreuken vanuit alle kanten.
Het aantal incidenten om ons heen neemt toe (zie recente casussen bij o.a. het Openbaar ministerie, Odido, Chipsoft, Booking.com, gemeente Ede) en de impact van AI maakt het mogelijk om zonder menselijke tussenkomst organisaties aan te vallen op kwetsbare plekken.

De Rijksoverheid heeft inmiddels erkend dat gemeenten essentiële entiteiten zijn. Amsterdam is als hoofdstad zeker 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.

De Cyberbeveiligingswet gaat naar verwachting per 1 juli 2026 in en stelt strenge eisen aan organisaties. Dat betekent dat Amsterdam stappen moet zetten en aantoonbaar haar digitale weerbaarheid op orde moet hebben; zover zijn we nu nog niet. Er is een programma ingericht dat stuurt op de voortgang.

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 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 de G4, regiogemeenten en partijen in de stad en de regio. Hierbij schaken we op veel verschillende borden.

Dit jaar is vooral het jaar geweest van het ontwerpen en neerzetten van het informatiebeveiligingshuis. Door de voorheen versnipperde organisatie anders in te richten wordt veel meer samenhang gecreeerd en worden de krachten gebundeld. Dit betaalt zich uit in meer slagkracht en effectiviteit.

Oordeel van de CISO

Het oordeel van de CISO is ten opzichte van een jaar eerder positiever geworden. Op verschillende gebieden zijn verbeteringen gerealiseerd of in gang gezet. Tegelijkertijd is informatiebeveiliging een zaak van lange adem, die nog veel aandacht nodig heeft. De belangrijkste prioriteiten voor het komende jaar zijn het implementeren en verankeren van risicomanagement en het veilig krijgen en houden van het complexe IT-landschap (waarbinnen de kroonjuwelen het meest urgent zijn). Daarbij is bewustwording (zowel bij bestuur, ambtelijke leiding als alle medewerkers) essentieel.

Doorgevoerde verbeteringen

In 2025 zijn er goede stappen gezet om de informatiebeveiliging op een hoger niveau te brengen:

- De organisatie van de informatiebeveiliging is aangepast, zodat integraal kan worden gestuurd.
- De uitvoering van het BIO-programma is voortgezet en heeft ervoor gezorgd dat informatiebeveiliging inmiddels bij veel directies op de agenda staat. Waar dit niet goed genoeg gaat wordt er bijgestuurd.
- Een beleidsagenda is opgesteld, waarbinnen op de noodzakelijke kaders en richtlijnen wordt gestuurd.
- Risico's worden steeds vaker expliciet gemaakt, zodat een goede risicoafweging kan plaatsvinden.
- Voor de implementatie van de Cyberbeveiligingswet is een aanpak en sturing ontwikkeld.
- De belangrijkste informatiesystemen (kroonjuwelen) zijn in kaart gebracht, die aansluiten op de gemeentelijke kernprocessen.
- Vanaf medio 2025 wordt elk kwartaal een specifiek dreigingsbeeld voor Amsterdam opgesteld.
- De implementatie van de Amsterdamse digitale werkomgeving is afgerond en de security monitoring is sterk uitgebreid.
- De beveiliging van werkplekken is verbeterd en de beveiliging van telefoons wordt verbeterd.
- Een bewustwordingsprogramma is vastgesteld.
- Er is aangesloten bij het (bredere) programma maatschappelijke weerbaarheid. Daardoor krijgt informatiebeveiliging extra aandacht.

Aanbevelingen

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

- Blijf actief sturen op de voortgang van de implementatie van de Cyberbeveiligingswet en Baseline Informatiebeveiliging Overheid (inmiddels de BIO2) bij alle clusters en directies. Realiseer waar nodig meer commitment bij de directies.
  Onderwerpen als autorisatiebeheer, risicomanagement, leveranciersmanagement en operationele technologie zijn hierbij belangrijke speerpunten.
- Maak gebruik van de voorgenomen samenvoeging van de clusters Bedrijfsvoering en DII door te sturen op de beheersing van stedelijke processen waarvan alle directies afhankelijk zijn (zoals instroom/doorstroom/uitstroom en fysieke beveiliging van panden

en specifieke ruimtes). Versterk waar nodig de stedelijke rol van Facilitair Bureau: afzonderlijke directies zijn niet geëquipeerd om panden te beveiligen of camera's te beheren.

- Formaliseer het risicomanagement op het gebied van informatievoorziening (onderdeel van het integrale risicomanagement binnen de gemeente), stel dit vast in het GMT en besteed daarbij met name aandacht aan de rol van de lijndirecties. Investeer in de relatie i-domein <> lijndirecties.
- Ga de komende jaren vooral sturen op de veiligheid van de belangrijkste applicaties van Amsterdam (de kroonjuwelen) en geef deze voorrang bij het implementeren van bijvoorbeeld veilige toegang, autorisatiebeheer en leveranciersmanagement.
- Stuur actief op het doorvoeren van security patches in het totale IT-landschap (informatiesystemen en IT-infrastructuur).
- Richt het beheer van webdomeinen in en zorg ervoor dat deze voldoen aan o.a. eisen op het gebied van veiligheid.
- Acteer op het toenemende aantal incidenten in combinatie met de groei van AI bij aanvallers, waardoor risico's toenemen. Gebruik waar mogelijk AI als verdedigingsmiddel.
- Bouw specifiek voor de directie Digitale Voorzieningen een eenduidig risicobeeld op in samenwerking met de strategische leveranciers en de partij die de security monitoring vervult.
- Actualiseer het crisishandboek i-domein en zorg voor actuele informatie over leveranciers, het applicatielandschap en de ICT-infrastructuur, zodat dat de organisatie geëquipeerd is om grote incidenten en crises op te vangen. Plan crisisoefeningen (binnen het i-domein, met directies en met partners) structureel in.

2 Inleiding

In deze rapportage schetst de Chief Information Security Officer van de gemeente Amsterdam zijn beeld over de staat van de informatiebeveiliging in de organisatie in 2025. Daarbij worden de ontwikkelingen op het dreigingslandschap benoemd, wordt inzicht gegeven in nieuwe regelgeving, wordt teruggeblikt op uitgevoerde acties en verbeteringen in het afgelopen kalenderjaar en wordt vooruitgekeken naar 2026. Daarna wordt aandacht besteed aan samenwerking in het regionale netwerk en worden nieuwe thema's (weerbaarheid en autonomie) belicht. Tenslotte worden incidenten en de ENSIA-rapportage benoemd.

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.

Het doel van deze rapportage is om het gemeentebestuur (college en gemeenteraad) inzicht te gegeven de status van de informatiebeveiliging en de belangrijkste ontwikkelingen en risico's daarin.
Hiermee kan de organisatie de weerbaarheid van onze informatievoorziening op een voldoende niveau brengen en in control blijven.

3 Ontwikkelingen in het dreigingslandschap

De dreigingen op het gebied van informatiebeveiliging ontwikkelen zich ook in 2025 snel.
Om hierop zicht te hebben en te houden sluiten we aan op het beeld van landelijke organisaties en de G4-gemeenten, aangevuld met informatie van de strategische partners waarmee de gemeente samenwerkt. En uiteraard zien we wat er in onze eigen organisatie gebeurt.

Hierna wordt vanuit verschillende invalshoeken het dreigingsbeeld geschetst: vanuit de Rijksoverheid, vanuit de VNG en specifiek voor de gemeente Amsterdam.

Cyber Security Beeld Nederland

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 2025 (gepubliceerd in november 2025) schetst het volgende beeld:

Het digitale dreigingslandschap wordt steeds diverser en onvoorspelbaarder. Er is een grote verscheidenheid aan aanvallen door statelijke actoren, cybercriminelen, en andere kwaadwillenden. Daarnaast vertaalt geopolitieke onvoorspelbaarheid zich naar het digitale domein. Cyberprogramma's worden opgezet door statelijke actoren of uitgebreid met inzet van niet-statelijke actoren of private organisaties. Ook kunnen veranderende geopolitieke verhoudingen ervoor zorgen dat digitale afhankelijkheden risicovol worden, terwijl ze dat eerder niet waren. Verder kunnen kwaadwillenden generatieve AI inzetten, wat betekent dat aanvallen eenvoudiger en op grotere schaal zijn in te zetten. Deze ontwikkelingen vinden gelijktijdig en in samenhang met elkaar plaats, waaruit voortvloeit dat het dreigingslandschap in toenemende mate complex wordt. Dit illustreert dat er continu aandacht moet blijven voor de weerbaarheid en de ontwikkelende dreiging en dat de basisprincipes van belang blijven – ondanks de toegenomen complexiteit. De diversiteit, onvoorspelbaarheid en het toenemende belang van digitale veiligheid maakt dat het steeds minder enkel een vraagstuk is voor technische experts, maar juist ook voor bestuurders.

Belangrijke constateringen in het CSBN zijn:

- *Statelijke cybercapaciteiten nemen toe en vermengen zich met niet-statelijke organisaties*
- *Geopolitieke ontwikkelingen leggen afhankelijkheden nadrukkelijk bloot. Europa, en daarmee Nederland, is voor vele verschillende digitale processen en diensten afhankelijk van aanbieders uit veelal niet-Europese landen.*
- *Juist die geopolitieke ontwikkelingen kunnen er voor zorgen dat de afhankelijkheid van digitale diensten en processen uit andere landen risicovol is of kan worden.*
- *Generatieve AI versterkt bestaande dreigingen voor digitale veiligheid*
- *In de afgelopen jaren is de ontwikkeling van generatieve AI in een versnelling gekomen. De technologie achter generatieve AI vormt geen dreiging op zichzelf, maar door specifieke toepassingen van de techniek en intenties van de actor die het inzet kunnen hier wel dreigingen uit voortvloeien.*

- *Hoewel nuances veranderen, hebben er geen grote verschuivingen plaatsgevonden in het dreigingsbeeld. Er is sprake van een grote verscheidenheid aan typen incidenten, oorzaken, aanvallers, en mate van impact. Zowel statelijke actoren als cybercriminelen voeren cyberaanvallen uit op Nederlandse doelen en/of raken Nederlandse belangen. Daarbij is apparatuur die netwerken beveiligt blijvend interessant voor kwaadwillende actoren. Ook blijft er sprake van DDoS-aanvallen. Daarnaast zijn er met regelmaat cybersecurityincidenten bij toeleveranciers/dienstverleners die leiden tot datalekken bij afnemers. Naast incidenten die veroorzaakt zijn door cyberaanvallen, zijn er opnieuw tal van voorbeelden van storingen als gevolg van niet moedwillig handelen, zoals door softwarefouten.*

Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten

De informatiebeveiligingsdienst van de VNG (IBD) brengt elke 2 jaar een dreigingsbeeld informatiebeveiliging Nederlandse gemeenten uit. In het dreigingsbeeld 2025-2026 wordt het volgende geschetst:

Gemeenten staan in 2025-2026 voor een onverminderd complex digitaal dreigingslandschap. Ransomware, datalekken en uitval van processen door incidenten vormen de grootste bedreigingen. Dit vraagt om een proactieve aanpak om digitale veiligheid te waarborgen en vertrouwen van inwoners en ondernemers te behouden. Dit alles in het licht van financiële en personele krapte.

Over de huidige situatie en uitdagingen:
- *Ransomware blijft de grootste dreiging. Criminelen gebruiken kwetsbare systemen om gevoelige data te stelen en organisaties af te persen, met aanzienlijke gevolgen zoals privacyschendingen, imagoschade en financiële verliezen.*
- *Incidenten bij leveranciers leiden tot verstoringen in gemeentelijke processen. Gemeenten zijn afhankelijk van externe partijen, wat de noodzaak benadrukt van duidelijke afspraken over beveiliging.*
- *Beperkte capaciteit, kennis en middelen bemoeilijken investeringen in digitale veiligheid.*

Dreigingsbeeld gemeente Amsterdam

Vanaf het 2e kwartaal van 2025 stelt Amsterdam elk kwartaal een specifiek dreigingsbeeld op. Op basis van de analyse van aanvalsgroepen, incidenten, aanvalstechnieken en kwetsbaarheden wordt het dreigingsniveau elk kwartaal ingeschat op de schaal laag / gemiddeld / hoog/ kritiek. In het tweede en derde kwartaal werd het dreigingsniveau gemiddeld ingeschat, in het vierde kwartaal is dit bjgesteld naar dreigingsniveau hoog. In hoofdstuk 5 van dit rapport lichten we dit toe.

De belangrijkste conclusie die we kunnen trekken is dat elke organisatie en elke leverancier (hoe professioneel ook) slachtoffer kan worden, en dat het belangrijk is om onze informatiebeveiliging op orde te hebben en te houden, en daarbij te bijven anticiperen op nieuwe dreigingen.

Een belangrijk risico voor Amsterdam is dat via bijvoorbeeld phishing wordt geprobeerd een account te compromitteren om daarna malware te installeren en data te stelen. Zowel bewustwording als technische maatregelen om dit soort incidenten te voorkomen / signaleren zijn essentieel.

Het bewustzijn is groeiend dat inbreuken bij leveranciers en ketenpartners effect kunnen hebben op onze eigen organisatie en gegevens en dat wij daarom ook daarop moeten sturen.
Het voorbereiden op mogelijke incidenten is cruciaal, o.a. door het oefenen van cybercrises.

4 Regelgeving

De Europese Unie heeft enkele jaren geleden de Network and Security Directive (beter bekend als de NIS-2 richtlijn) vastgesteld. In Nederland is deze richtlijn vertaald in de Cyberbeveiligingswet, die naar verwachting rond 1 juli 2026 van kracht gaat worden.

Deze wet betekent echt een “next step” voor de verhogen van de digitale weerbaarheid in Nederland. Belangrijke elementen zijn:

- Een zware betrokkenheid van bestuurders. Bestuurders worden verantwoordelijk gesteld voor het voldoen aan de wet. Ze moeten worden getraind en worden geacht de risico’s te kennen en hierover te besluiten.
- Informatiebeveiliging moet aantoonbaar op orde zijn. Het gaat hierbij niet alleen om de beveiliging van kantoorautomatisering, maar nadrukkelijk ook van de operationele technologie zoals (de bediening van) sluizen, tunnels en bruggen.
- Risicomanagement moet formeel en organisatiebreed zijn ingericht.
- Organisaties moeten sturen op de risico’s bij hun leveranciers.
- Significante incidenten moeten worden gemeld bij een nieuwe (landelijke) toezichthouder.
- De Baseline Informatiebeveiliging Overheid, waarin regels zijn gesteld voor overheidsorganisaties, is geactualiseerd en wordt een wettelijk verplichte norm.
- Gemeenten worden aangewezen als essentiële entiteit. Dit zal leiden tot nieuwe verantwoordings- en auditverplichtingen.

Binnen de Gemeente Amsterdam is al veel geregeld op de verplichte onderdelen van de wet.
Om aantoonbaar te voldoen aan de wet moeten er echter nog wel een aantal stappen genomen worden.

In september 2024 is een programma ingericht onder voorzitterschap van de CIO dat in kaart heeft gebracht wat er nodig is om ervoor te zorgen dat de Gemeente Amsterdam aan de Cyberbeveiligingswet gaat voldoen. Het programma bestaat uit 9 sporen:

- Beleid en governance
- Risicomanagement
- Incidentmanagement (inclusief melden van significante incidenten aan de landelijke toezichthouder)
- Logging en monitoring
- Bewustwording
- BCM en crisismanagement
- Leveranciersmanagement
- BIO2
- Operationele technologie

Voor de GGD Amsterdam-Amstelland (onderdeel van de gemeente Amsterdam is naast de BIO een specifieke norm van kracht: de NEN7510 (informatiebeveiliging in de zorg).
De GGD is voornemens om zich te laten *certificeren* op basis van deze norm, net als andere GGD-en in Nederland al hebben gedaan.

5 Terugblik en vooruitblik

Informatiebeveiliging is een breed terrein. In dit hoofdstuk wordt stilgestaan bij een aantal thema's en wordt aangegeven wat hierop in 2025 is gebeurd. Ook wordt vooruitgekeken naar 2026.

De organisatie van de informatiebeveiliging

In 2024 is onderzocht hoe we meer samenhang kunnen creëren in de informatiebeveiligingsorganisatie van Amsterdam. Er waren verschillende informatiebeveiligingsfuncties/rollen ingericht die nog te veel werkten vanuit hun eigen doelstellingen, zonder de juiste samenhang. Daardoor werkte het geheel niet optimaal als één organisatie.
Op basis van de uitkomsten is begin 2025 het *Informatiebeveiligingshuis* ingericht, waarmee integraal wordt gestuurd op informatiebeveiliging. Gedurende dit jaar is de organisatie van het informatiebeveiligingshuis verder uitgewerkt, waarmee een duidelijker en samenhangende organisatie is ontworpen. Formele besluitvorming (met betrokkenheid van de ondernemingsraad) vindt in 2026 plaats.
Het kernteam informatiebeveiliging (met de CISO als voorzitter) komt wekelijks bijeen. Vanaf 2026 zal in een kwartaalcyclus worden bepaald hoe en waarop wordt gestuurd.

De afgelopen jaren hebben steeds meer organisatieonderdelen compliance functionarissen aangesteld. Dat zijn medewerkers die in de directies opereren en daar meestal voor verschillende vakgebieden een vraagbaak / ondersteunende functie hebben om de compliance te organiseren, met specifieke organisatie- en proceskennis. Dit helpt enorm om de verbinding te maken tussen de afzonderlijke directies en de directie Digitale Strategie en Informatie, waar de information security officers en andere specialisten werken.

Amsterdam heeft als hoofdstad veel relaties met allerlei partijen. Ook participeert Amsterdam waar nodig in landelijke gremia. In 2025 is er met name in G4-verband veel contact geweest op het gebied van informatiebeveiliging om aanpak, best practices en risico's met elkaar te delen. In het najaar is in Amsterdam de 2e G4-security dag georganiseerd, waar meer dan 100 informatiebeveiligingsprofessionals uit de G4 een inspirerende dag hebben meegemaakt.

Zorgplicht en bewustwording

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 binnen de gemeente Amsterdam er relatief weinig aandacht gegeven aan bewustwording. We merken we dat informatiebeveiligingsincidenten nogal eens veroorzaakt worden door medewerkers die onwetend zijn of onzorgvuldig handelen.

2025 is een kantelpunt geweest: door het aanstellen van een compliance awareness officer is er nu structurele aandacht voor bewustzijn en bewustwording, zowel voor informatiebeveiliging als andere vakgebieden. Eind 2025 is er een plan vastgesteld oor bewustwordingsacties naar de organisatie.

De Cyberbeveiligingswet richt zich onder andere op het *bestuur* van organisaties. Het bestuur dient de maatregelen (zoals bedoeld in de zorgplicht, Cbw, Artikel 21) goed te keuren en toe te zien op de uitvoering ervan. Daarnaast dienen de leden van het bestuur te beschikken over (actuele) kennis en vaardigheden om de risico's voor de beveiliging van netwerk- en informatiebeveiliging te identificeren en de beheersmaatregelen te beoordelen.

Voor bestuurders (bij gemeenten het College van B&W) eist de Cyberbeveiligingswet dat zij hiertoe elke twee jaar een training volgen. Dit is geen sinecure bij een zo specifiek vakgebied als informatiebeveiliging, dat bovendien sterk in ontwikkeling is en een vrij technisch imago heeft.

In G4-verband is in 2025 afgestemd hoe dit kan worden aangepakt. Er zal worden gewerkt aan een gezamenlijke G4-training voor bestuurders, met daarbij ruimte voor een lokale verdieping.
Het streven is om deze training voor het nieuwe College in 2026 te verzorgen.

Voortgang implementatie Baseline Informatiebeveiliging Overheid

Information Security Officers helpen alle 42 organisatieonderdelen bij het implementeren van de BIO. De samenwerking tussen deze experts en de lijnorganisatie is cruciaal.

Elk kwartaal wordt nagegaan welke verbeteracties (om te kunnen voldoen aan de BIO) nog openstaan. De BIO2 en Cyberbeveiligingswet leiden tot nieuwe dan wel aangescherpte eisen, die hierbij stap voor stap worden meegenomen.
Gedurende 2025 is geconstateerd dat bij een 9-tal (vande 42) directies de voortgang op de BIO niet voldoende was. De CISO heeft hierover escalatiegesprekken gevoerd met de betreffende directeuren. De voortgang wordt getoetst.

In 2025 is een begin gemaakt met compliance-rapportages voor informatiebeveiligng, privacy en informatiebeheer per cluster. Elk kwartaal wordt gerapportered over de status van de compliance per vakgebied wat input is voor afstemming tussen de CIO en elke stedelijk directeur. De hierboven genoemde BIO-voortgang is hiervan een onderdeel.

Beleid en kaders

Het strategisch beleidskader informatiebeveiliging is in 2025 herzien, o.a. op basis van de nieuwe wetgeving en de vernieuwde informatiebeveiligingsorganisatie. Vaststelling zal in 2026 door het College plaatsvinden.

Dit jaar is een beleidsagenda opgesteld waarin kaders en richtlijnen worden benoemd die moeten worden opgesteld zijn om te voldoen aan de Cyberbeveiligingswet, de BIO en de NEN7510. Vanuit de gemeentelijke organisatie is veel vraag naar deze richtlijnen. Een werkgroep is ingericht die deze kaders uitwerkt.

Implementatie risicomanagement

Het belang van risicomanagement bij informatiebeveiliging wordt steeds groter en krijgt terecht meer aandacht in de nieuwe wetgeving.

Amsterdam heeft ervoor gekozen om één risicomanagement aanpak en -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 het risicomanagement-systeem zodanig ingericht dat directies ook hun informatiebeveiligingsrisico's hierin kunnen vastleggen en de afhandeling hiervan kunnen monitoren.

Doordat de information security officers beter betrokken zijn bij directies (via de BIO-aanpak en bij projecten en opgaven) ontstaat meer zicht op risico's. Ook het aanstellen van compliance officers bij de directies helpt daarbij. Door het signaleren van risico's bij directies kan op het juiste niveau een risicoafweging plaatsvinden en worden bijgestuurd.

Inmiddels leggen alle directies informatiebeveiligingsrisico's vast. De *registratie* gaat steeds beter. Dit betekent nog niet dat directies zich bewust zijn van hun risico's en daarnaar handelen. We zien nog te vaak dat in de "waan van de dag" risico's niet worden gezien of te gemakkelijk worden geaccepteerd. Een formeel vastgestelde werkwijze is hard nodig om hierop grip te krijgen.
Deze werkwijze is eind 2025 / begin 2026 uitgewerkt. Implementatie zal alle organisatie-onderdelen raken en vraagt om een veel meer bewuste *mindset* van de hele organisatie. Dit is essentieel om ook op concern-niveau een overall risicobeeld te krijgen en ook op dat niveau te kunnen sturen.

Kroonjuwelen

De BIO is lang uitgegaan van de baseline-nadering: bij elk proces en informatiesysteem moeten dezelfde maatregelen worden doorgevoerd en is dezelfde mate van beheersing nodig, zonder te kijken naar risico's en kosten.
De Cyberbeveiligingswet en BIO2 brengen daar verandering in: de organisatie kan voortaan risicogericht kiezen en bepalen waarop de focus wordt gelegd. Voor een organisatie als de gemeente Amsterdam, met vele honderden processen en ongeveer 1200 verschillende informatiesystemen, is dit een groot voordeel.
In het afgelopen jaar is daarom geanticipeerd door de 85 belangrijkste informatiesystemen (kroonjuwelen) in kaart te brengen. De lijst met kroonjuwelen sluit aan op de door het Gemeentelijk Management Team vastgestelde overzicht van gemeentelijke kernprocessen. Vaststelling van de lijst met kroonjuwelen staat in de eerste helft van 2026 op de agenda.

Autorisatiebeheer

Autorisatiebeheer is een sleutelmaatregel voor informatiebeveiliging: Van de belangrijkste informatiesystemen worden 2x per jaar de autorisaties getoetst. Uit een in 2025 uitgevoerde audit blijkt echter dat het beheer van autorisaties nog niet op orde is:

- de kaders op dit gebied zijn onvoldoende bekend in de organisatie;
- het beheer van autorisaties is verschillend ingericht;
- autorisatiematrices (de basis van autorisatiebeheer) ontbreken veelal;
- geconstateerde afwijkingen worden niet als incident behandelend, mede daardoor leert de organisatie hierdoor onvoldoende.

De accountant (ACAM) toetst jaarlijks het autorisatiebeheer bij applicaties met een groot financieel belang. Aanvullend op bovenstaande punten heeft de accountant aanbevelingen gedaan op het gebied van:

- periodieke controle van speciale rechten;
- logging en beoordeling van logs op afwijkingen en onregelmatigheden;
- het monitoren op ongewenste functievermenging en risicoafweging/beoordeling bij eventuele bevindingen.

Vanuit directie Digitale Voorzieningen (vakgroep functioneel beheer) wordt een verbeterplan opgesteld.

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 2025 stabiel gebleven: in 2025 zijn 47 verschillende toepassingen getest en zijn de hierbij gesignaleerde bevindingen weggewerkt.
Ook op de ICT-infrastructuur worden regelmatig dit soort tests uitgevoerd.

Veilige toegang tot applicaties

In de afgelopen jaren is een nieuwe, veilige, stedelijke ICT-werkomgeving ontworpen. De uitrol daarvan is in 2025 afgerond.
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 de generieke IAM-voorziening (IAM staat voor Identity en Access Management) 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.
Eind 2025 zijn enkele applicaties aangesloten op deze voorziening. Er is een planning opgesteld om de applicaties op basis van risico (aard van de applicatie, gevoeligheid, aantal gebruikers) te kunnen aansluiten. Sturing hierop blijft wel nodig.

Werkplekken en telefoons

De afgelopen jaren is de beveiliging van o.a. laptops, vaste computers en telefoons sterk verbeterd. Daarmee kan o.a. de sterke toename van phishing beter worden beheerst.
Eind 2025 is de stap genomen om, gezien de sterke toename van phishing en ramsomware, de beveiliging van de laptops verder op te schroeven. Voor telefoons wordt eenzelfde actie voorbereid.

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.
Amsterdam heeft een eigen tool ontwikkeld: ChatAmsterdam, die inmiddels breed wordt gebruikt. ChatAmsterdam biedt een veilige en betrouwbare oplossing die voldoet aan het strikte Amsterdamse beleid rondom privacy, security en informatiebeheer. Periodiek wordt gemeten welke andere AI-tooling wordt gebruikt.

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 zeer 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: volgens www.basisbeveiliging.nl zijn er in Amsterdam 207 domeinen met een hoog risico. Daarmee staat Amsterdam bovenaan de lijst van gemeenten met de meeste hoog-risico domeinen. Het beheer van webdomeinen is binnen de gemeente nog steeds onvoldoende ingericht. Initiatieven om dit te verbeteren hebben tot nu toe nauwelijks 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 in te richten, zodat we direct kunnen reageren op dreigingen en incidenten, ook buiten kantooruren. We maken daarbij gebruik van een gespecialiseerde externe partij.

Amsterdam heeft vier strategische leveranciers die veel ICT-diensten leveren (werkplek, hosting, cloudplatform, netwerk) en beheertaken vervullen. In 2025 zijn deze partijen deels aangesloten op het SOC; er wordt nog gewerkt om dit af te ronden. Ook het Amsterdamse cloudplatform gaat worden aangesloten. Dit zijn zeer belangrijk stappen voorwaarts om ons ICT-landschap te beschermen. De aansluiting van andere partijen (met name leveranciers van SAAS-applicaties) staat op de planning.

Sturing op leveranciers

In de afgelopen jaren zijn door Amsterdam steeds meer ICT-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 bij twee segmenten:

- bij de vier 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 2025 verbeterd: tactische riskmanagement overleggen worden uitgevoerd en assurance-rapportages zijn deels beoordeeld. Een overall beeld ontbreekt nog.
- SAAS-leveranciers. Dit zijn leveranciers van software as a service: wij 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. De accountant heeft hierover al meerdere jaren opmerkingen gemaakt dat sturing op deze assurance rapportages meer aandacht behoeft. De voortgang hierop is, ondanks alle inspanningen, moeizaam.

Voorbereid zijn op grote incidenten

Als iets de afgelopen jaren wel duidelijk is, is het wel dat organisaties voorbereid moeten zijn op grote cyber-incidenten. Amsterdam heeft in de afgelopen jaren een crisisteam i-domein ingericht, dat regelmatig oefent. In 2025 is geparticipeerd in de overheidsbrede cyberoefening. In 2026 worden stappen gezet om mee te doen aan de meerdaagse landelijke oefening ISIDOOR in 2027. In het kader van Business Continuity Management hebben vele directies de afgelopen jaren ook continuiteitsoefeningen gehouden. Hiermee zijn goede stappen gezet.

6 Samenwerking in het regionale netwerk

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 de afgelopen jaren is het *Netwerk digitale weerbaarheid Amsterdam-Amstelland* ontworpen.

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 en 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. Met gemeenten bestaan dit soort kringen al.

Inmiddels wordt de samenwerking gezocht met organisaties in de stad en de regio, o.a. via het netwerk van de Amsterdam Economic Board. Ook wordt met AMSEC (het Amsterdam Cybersecurity Center, een samenwerkingsverband dat voortkomt uit de Amsterdamse universiteiten) verkend of de krachten kunnen worden gebundeld.
Zowel vanuit de netwerkgedachte van het Netwerk digitale weerbaarheid als vanuit de preventie- en met name de onderzoekskant van Amsec is het een logische stap om de (strategische) verbinding te zoeken.

7 Nieuwe thema's: weerbaarheid en autonomie

In 2025 zijn de onderwerpen weerbaarheid en autonomie volop op de agenda gekomen. Beide onderwerpen hebben een relatie met informatiebeveiliging; daarom worden ze hier ook belicht.

Door de geo-politieke ontwikkelingen wordt landelijk én regionaal ingezet op het versterken van *weerbaarheid* bij stroomuitval. In onze regio zijn zowel de Veiligheidsregio Amsterdam-Amstelland als de gemeente Amsterdam in actie gekomen om de weerbaarheid van organisaties en inwoners en ook de gemeente zelf in kaart te brengen en waar nodig te versterken.

De relatie met digitale weerbaarheid (of cyberweerbaarheid) was snel gelegd: de weerbaarheid van digitale systemen kan essentieel zijn om de beschikbaarheid van informatie of essentiële diensten te kunnen borgen.
Binnen de gemeente Amsterdam wordt met name ingezet op het in kaart brengen van de veiligheid van informatiesystemen die essentieel zijn voor een beperkt aantal kritieke processen. Begin 2026 is een week van de weerbaarheid georganiseerd om de effectiviteit van de betreffende maatregelen te toetsen. Het is nu al wel duidelijk dat deze aanpak voordelen biedt, ook voor andere systemen.

Amsterdam heeft in het afgelopen jaar een speerpunt gemaakt van het onderwerp *digitale autonomie*, o.a. door het opstellen van een Meerjarenstrategie Digitale Autonomie 2026 – 2035. Hierin wordt uitgewerkt hoe de gemeente de komende 10 jaar veel minder afhankelijk gaat worden van grote Amerikaanse Big-Tech-partijen. Ook wil Amsterdam daarbij samen optrekken met de G4-gemeenten, de VNG en de Rijksoverheid.
Dit is een grote verandering; vanuit informatiebeveiliging steunen we momenteel op maatregelen die de genoemde Big-Tech partijen hebben getroffen. Als gemeente is het onze taak om de veiligheid en beheersing van nieuwe/andere Europese/Nederlandse aanbieders te (blijven) toetsen. Dat is geen nieuwe taak, maar de mate van verandering maakt dit tot een uitdaging. Tegelijkertijd biedt het ook veel kansen: als wij meer gaan samenwerken met mede-overheden dan kunnen we onze krachten bundelen en steunen op wat er al is.

8 Incidenten

Het is inmiddels zo dat informatiebeveiligingsincidenten veelvuldig het nieuws halen.

Het is niet mogelijk om incidenten op het gebied van informatiebeveiliging te voorkomen.
Ons IT landschap is continu in beweging en vrijwel dagelijks worden er wel risico's in door de Gemeente gebruikte software en IT-infrastructuur ontdekt. Er zullen zich altijd informatiebeveiligingsincidenten voordoen waarvan we vervolgens kunnen leren en het geleerde kunnen toepassen binnen de Gemeente.

Binnen de organisatie is er een vastgesteld proces om informatiebeveiligingsincidenten te melden, registreren en af te handelen. In 2025 is dit proces volledig herzien en in lijn gebracht met de verantwoordelijkheden in de interne organisatie. Ook de uitbestede security-taken hebben hierin een plek gekregen. Tenslotte is een nieuwe (Europese) categorie-indeling van incidenten doorgevoerd.
Informatiebeveiligingsincidenten die door medewerkers worden gemeld worden centraal geregistreerd, geanalyseerd en afgehandeld.
Daarnaast verwerkt het security operations center (SOC) grote aantallen technische security alerts (meldingen) die voor het overgrote deel geautomatiseerd worden opgelost. Een klein deel hiervan betreft een daadwerkelijk Informatiebeveiligingsincident.

Informatiebeveiligingsincidenten die een relatie hebben met Datalekken worden apart geregistreerd richting de privacy officers en inhoudelijk 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 jaarrapportage.

Informatiebeveiligingsincidenten menselijk gemeld

Binnen de gemeente is er een centrale mogelijkheid voor medewerkers om een informatiebeveiligingsincident te registeren. Dit gebeurt via de Self Service Portal van het servicepunt door middel van een "tegel" datalekken, privacy en informatiebeveiliging.

Gedurende 2025 zijn er in totaal 707 meldingen via deze "tegel" ontvangen en behandeld. Het betreft 480 privacy gerelateerde meldingen en 227 informatiebeveiligingsmeldingen. De meest voorkomende Informatiebeveiligingsincidenten van medewerkers zijn frauduleuze sms/appjes (18,5%, vorig jaar 44%), verdachte mail/post (16%, vorig jaar 18%), en frauduleuze telefoontjes (22%, vorig jaar 10,5%). Het grootste deel van de meldingen blijft generiek van aard (34%) en niet eenduidig te classificeren.

Informatiebeveiligingsincidenten technisch gemeld
Met de strategische leveranciers van IT diensten zijn afspraken gemaakt om informatiebeveiligingsincidenten van ernstige omvang te rapporteren. Daarnaast is een generieke security monitoring ingericht. In 2025 zijn er in totaal 17674 technische security alerts vastgesteld door onze security monitoring. Ten opzichte van vorig jaar is dit een daling 35%. Dit komt doordat 2025 een overgangsjaar was: het eigen datacenter van de gemeente is gedurende dit jaar buiten gebruik gesteld en nog niet alle strategische leveranciers zijn volledig aangesloten op de generieke monitoring.

Hieronder een overzicht van de meldingen, per prioriteit, die door de security dienst cyber fusion center en/of strategisch partner zijn voorzien van een beoordeling.

Informatiebeveiligings (aantallen)	Prio1 (kritiek)	Prio2 (hoog)	Prio3 (gem)	Prio4 (laag)	Totaal
Incident	3	67	285	818	1173

In 2025 heeft 32% van alle technische security meldingen betrekking gehad op de werkplekken van de gemeente (vorig jaar 15%), 65% op de externe beheerde IT-systemen en applicaties (vorig jaar 78%), 4,2% op de eigen beheerde IT-systemen (vorig jaar 6%) en 9% heeft betrekking gehad op de infrastructuur die door de gemeente op alle locaties wordt gebruikt (vorig jaar 1%).

in 2025 kwamen in de niveaus Prio1 & Prio2 de volgende categorieën incidenten het meeste voor:

1. Malware op werkplekken.
2. Inlogpogingen (bijvoorbeeld via gelekte wachtwoorden of door medewerkers te verleiden in te loggen op malafide omgevingen).

Kwetsbaarheden

Amsterdam ontvangt van het Nationaal Cyber Security Centrum (NCSC) en de Informatiebeveiligingsdienst (IBD) zeer regelmatig signalen over kwetsbaarheden in hardware en software. Bij een dergelijke melding wordt, afhankelijk van het risico, actie ondernomen. In 2025 was dit van toepassing bij 19 (vorig jaar 18) high/high (hoog risico/ hoge impact) geclassificeerde meldingen.

In 2025 is er een generieke kwetsbaarheden monitoring op de IT systemen van de Gemeente operationeel geworden (datacenters en deel infrastructuur). Op deze gemonitorde systemen zijn dit jaar 4880 nieuwe kwetsbaarheden gedetecteerd (naast de kwetsbaarheden die al bekend waren). Gedurende 2025 is het de gemeente gelukt om 5307 kwetsbaarheden op te lossen. Door het tijdig afhandelen van deze meldingen is voorkomen dat aanwezige kwetsbaarheden, op technische systemen van de Gemeente, door kwaadwillende konden worden uitgebuit.

De gemeente zelf heeft in totaal 33 verzoeken tot beoordeling van een mogelijke dreiging aangevraagd bij de strategisch partner.

Meldingen door ethische hackers

Het in november 2022 ingestelde digitale meldpunt voor ethisch hackers heeft de gemeente 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. Van de 82 ontvangen meldingen zijn er 37 ook daadwerkelijk als kwetsbaarheid verder afgehandeld. De ethische melders van deze kwetsbaarheden kunnen naar wens een vermelding krijgen op de digitale Hall of Fame van de informatiebeveiligingsdienst voor gemeenten. Er zijn 27 vermeldingen op de Hall of Fame geplaatst door de Gemeente.

De voorbereidingen zijn gestart voor het organiseren van een hacking event in 2026, met als voorlopige werktitel Hack020. Dan zullen ethische hackers danwel studenten worden uitgenodigd om op een specifieke dag en locatie de veiligheid van systemen van de gemeente Amsterdam te testen.

9 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 bestuurlijke rapportage benoemen we enkele hoofdlijnen.

Binnen ENSIA wordt o.a. getoetst of de gemeente voldoet aan de eisen die worden gesteld aan het gebruik van Suwinet (een systeem dat UWV, SVB en gemeenten gebruiken om onderling gegevens uit te wisselen). Hierbij is geconstateerd dat er afwijkingen zijn op het gebied van:

- Controle op toegangsrechten en gebruikersbeheer.
- Aantoonbaar volgen van bewustwordingstrainingen.
- Specifieke beleidskaders.

De geconstateerde afwijkingen worden door de gemeente herkend en zijn niet nieuw: er is in eerdere jaren ook over gerapporteerd. Ze zijn ook in generieke zin herkenbaar en zijn benoemd in de eerdere hoofdstukken van deze rapportage.