Bestuurlijke rapportage informatiebeveiliging 2023

1. Inleiding

Voor u ligt de bestuurlijke rapportage informatiebeveiliging 2023 van de gemeente Amsterdam. Hierin geven wij aan hoe wij de informatie van de gemeente Amsterdam hebben beveiligd, welke ontwikkelingen zich hierbij hebben voorgedaan en hoe risico's en dreigingen zich in het afgelopen jaar hebben ontwikkeld. Daarbij geven we een doorkijk naar 2024.

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.
Het college legt met deze rapportage verantwoording af over het afgelopen jaar en informeert daarmee de gemeenteraad in het kader van zijn toezichthoudende rol.

2. Oordeel van de CISO

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 digitale infrastructuur.

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

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 hebben bij nationale en internationale ontwikkelingen op het vlak van cyberveiligheid, en daarbij samen te werken met partijen in de stad en de regio.

In 2023 zijn er concrete stappen gezet om de informatiebeveiliging op een hoger niveau te brengen. De uitvoering van het BIO-programma (zie hoofdstuk 3, implementatie van de baseline informatiebeveiliging overheid) is voortgezet en heeft ervoor gezorgd dat informatiebeveiliging inmiddels bij alle directies op de agenda staat.

In het afgelopen jaar is een verkenning gedaan naar de positie van de CISO binnen de gemeentelijke organisatie. Daarbij is o.a. geconstateerd dat in de afgelopen jaren nieuwe informatiebeveiligingsfuncties zijn ontstaan die onvoldoende met elkaar samenhangen. In 2024 wordt daarom het informatiebeveiligingshuis onder de loupe genomen en waar nodig anders ingericht.

Het aantal information security officers (de medewerkers die de lijnorganisatie ondersteunen bij informatiebeveiliging) kent een lichte toename. Daarbij zijn stappen gezet om de rol van deze functionarissen te professionaliseren. De samenwerking tussen de disciplines informatiebeveiliging, privacy en informatiebeheer krijgt daarbij steeds meer gestalte.
Binnen het i-domein wordt in toenemende mate integraal gewerkt aan kwaliteit. Bij de ingezette kanteling naar opgavegericht en wendbaar werken is informatiebeveiliging altijd onderdeel van het Shared Service Team wat vast onderdeel is van een opgave.

Bij de implementatie van het nieuwe risicomanagement systeem in 2023 is informatiebeveiliging (naast privacy en informatiebeheer) expliciet meegenomen. Compliance en risicomanagement op het gebied van informatiebeveiliging krijgen daardoor steeds meer aandacht bij elke directie. Issues die aan de orde zijn worden daardoor beter zichtbaar en belanden op de juiste tafel.

De implementatie van de nieuwe Amsterdamse Digitale Werkomgeving is in 2023 grotendeels voltooid. Het i-domein is bezig om het volledige applicatielandschap onder een éénduidig beheer te brengen. Gedurende 2023 is een groot aantal toepassingen overgezet naar het Amsterdamse cloudplatform dat in 2022 is gerealiseerd.

Het college heeft in 2023 een nieuwe agenda digitale stad 2023-2026 vastgesteld. Daarin is een hoofdstuk opgenomen over digitale weerbaarheid. De kern hiervan is we als Amsterdam samen met andere partijen (o.a. regio-gemeenten, politie, veiligheidsregio) een ecosysteem digitale veiligheid opzetten, waarmee organisaties elkaar helpen hun informatiebeveiliging op een hoger niveau te brengen. Kennisuitwisseling en het samen oefen van mogelijke crisissen zijn hierbij essentieel.

Het beeld is niet alleen positief: er zijn nog belangrijke stappen te zetten om beter in control te komen op het gebied van informatiebeveiliging:

- Uit het dreigingsbeeld blijkt dat we permanent waakzaam moeten zijn en onze risico's moeten blijven bewaken. Achterover leunen kan niet; nieuwe dreigingen (door statelijke actoren, criminale hackers of door nieuw ontdekte kwetsbaarheden in hard- en software) zullen blijven ontstaan.
- Het cluster DII is bezig om informatiesystemen in beeld te krijgen en onder beheer te brengen, maar dat gaat niet snel. Het zicht op het landschap van informatiesystemen is daarmee nog niet voldoende. Systemen die we niet kennen kunnen we ook niet afdoende beveiligen.
- De aansturing van strategische partners en ICT-leveranciers moet en kan beter, om daarmee goed zicht te krijgen op de feitelijke veiligheid van de ICT-infrastructuur en informatiesystemen.
- Onderdeel van het onderwerp hierboven zijn de applicaties waarbij het beheer is uitbesteed: de zogenoemde Software as a Service (SAAS)-toepassingen. Hierbij is de gemeente afhankelijk van door de externe beheerpartijen getroffen maatregelen. Het zicht en de sturing daarop is onvoldoende.
- Het autorisatiebeheer van onze belangrijkste informatiesystemen is nog niet op orde. Er is een stedelijk proces om 2 keer per jaar de autorisaties van onze informatiesystemen te toetsen, maar die toetsing vindt nog niet altijd plaats.
- Bij de in-dienst/ uit-dienstprocessen hebben we nog de nodige stappen te zetten.
- Het bewustzijn verdient meer aandacht na een aantal jaren wat minder focus te hebben gehad.
- De beveiliging van de industriële automatisering heeft meer prioriteit nodig.
- Het op tafel krijgen van de risico's blijkt lastig; hiervoor is de samenwerking tussen specialisten (information security officers), het i-domein en de directies essentieel.
- Rapportage en sturing is hard nodig om stappen te zetten en verder te komen.
- Tenslotte: nieuwe regelgeving (NIS2, BIO2) komt er snel aan en maakt het nog meer nodig om aantoonbaar in control te zijn..

Resumé: ten opzichte van een jaar eerder zijn goede stappen gezet, maar Amsterdam heeft nog het nodige te doen om het juiste niveau te bereiken. Aandacht en focus voor informatiebeveiliging blijft gezien de toenemende dreigingen hard nodig!

3. Ontwikkelingen in het dreigingslandschap

Bij informatiebeveiliging is het nodig 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 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 2023 (uitgebracht in juli 2023) heeft als thema: verwachte het onverwachte:
"Digitale veiligheid vraagt een voortdurende en complexe evenwichtsoefening om uiteenlopende belangen, digitale dreigingen en digitale weerbaarheid in balans te krijgen of te houden. Vele partijen leveren inspanningen om de digitale weerbaarheid te verhogen en gevrijwaard te blijven van cyberincidenten. Voor organisaties geldt nog altijd dat het implementeren van basismaatregelen op het gebied van cybersecurity al veel effect kan hebben. Toch zijn cyberincidenten niet altijd te voorkomen. Die kunnen zich onverwacht voordoen en zij kunnen een onverwachte oorzaak, aard en impact hebben".

Het CSBN kent de volgende thema's:
- De veiligheid van digitale processen is en blijft essentieel in onze sterk gedigitaliseerde maatschappij en is dus onlosmakelijk verbonden met de nationale veiligheid.
- De digitale dreiging voor Nederland is onverminderd groot en voortdurend aan verandering onderhevig.
- De strategische thema's uit het CSBN 2022 blijven leiden tot complicaties voor het beheersen van digitale risico's.
- Het verkleinen van de scheefgroei tussen de digitale dreiging en de weerbaarheid blijft een grote opgave.
- Ondanks groeiende aandacht voor de weerbaarheid van Operationele Technologie (OT) als bouwsteen van vitale processen, is er ruimte voor verbetering.
- Digitale risico's vragen om een bredere manier van beheersing en moeten worden beschouwd als een integraal onderdeel van de risico's voor de nationale veiligheid. Hierbij kan de invalshoek 'assume breach' (ga ervan uit dat er een cyberincident is) behulpzaam zijn.

De belangrijkste boodschap uit dit dreigingsbeeld is voor Amsterdam dat we permanent waakzaam moeten zijn en onze risico's moeten blijven bewaken. Achterover leunen kan niet; nieuwe dreigingen (door statelijke actoren, criminale hackers of door nieuw ontdekte kwetsbaarheden in hard- en software) zullen blijven ontstaan. In de afgelopen jaren zijn meerdere gemeenten slachtoffer geworden van hackers (Lochem, Hof van Twente en recent Antwerpen). Amsterdam wil niet de volgende in dit rijtje zijn. Het continu versterken en bewaken van de digitale weerbaarheid is dus een cruciale taak van de gemeente.

4. Nieuwe regelgeving werpt zijn schaduw vooruit

In de voorgaande jaren hebben wij onze aanpak van informatiebeveiliging steeds gebaseerd op de Baseline Informatiebeveiliging Overheid (kortweg BIO). Deze baseline schrijft de kaders voor m.b.t. overheidsorganisaties.

In 2023 is op Europees niveau een nieuwe norm vastgesteld, de NIS2 (netwerk information security directive-2). De NIS2-richtlijn zal in oktober 2024 van kracht worden en werpt zijn schaduw vooruit. NIS2 gaat niet alleen over het beveiligen van informatie maar over de bredere digitale weerbaarheid van organisaties. Zorgplicht, meldplicht en toezicht worden aangescherpt. Beveiliging van industriële automatisering wordt een speerpunt. Aan het risicomanagement en de aantoonbaarheid van informatiebeveiliging worden zware eisen gesteld.
Gemeenten zullen in het kader van NIS2 door de Rijksoverheid worden gezien als essentiële entiteiten, waar dat tot nu toe nog niet het geval is.
De vertaling van de Europese NIS-2 richtlijn naar Nederlandse wetgeving is vertraagd en wordt in de loop van 2024 pas verwacht. Desalniettemin wordt van organisaties verwacht dat ze zsm na oktober 2024 aan de richtlijn voldoen.

Naast de NIS2 is ook de BIO2 in aantocht. De huidige BIO dateert uit 2020 en is in het afgelopen geëvalueerd (met betrokkenheid vanuit Amsterdam) en zal flink worden aangepast. De verwachting is dat de BIO2 meer gebaseerd zal zijn op de internationale standaard ISO27000 en minder specifieke overheidsmaatregelen zal bevatten. De BIO2 zal ook in 2024 worden vastgesteld door de Rijksoverheid.

Conclusie is dat de regelgeving waaraan wij moeten voldoen op meerdere gebieden gaat wijzigen, wat vraagt om alertheid en bijsturing van onze aanpak.

5. Informatiebeveiliging gemeente Amsterdam

De basis: Baseline Informatiebeveiliging Overheid

Alle directies binnen de gemeente Amsterdam hebben indertijd analyses uitgevoerd om te bepalen wat er nodig is om in control te zijn ten aanzien van de BIO. Deze analyses zijn vertaald in verbeterplannen die door de directies formeel zijn vastgesteld.
Eind 2023 is de implementatie van de BIO-verbeterplannen zeker nog niet afgerond. Enkele directies zijn (bijna) gereed, maar de meerderheid heeft hierop nog het nodige werk te doen. Directies bijven hierover elk kwartaal rapporteren. Sturing hierop blijft heel hard nodig.

In hoofdstuk 7 worden de speerpunten voor 2024 benoemd. Waar nodig worden onderwerpen uit de BIO hierin meegenomen.

Er is inmiddels opdracht gegeven aan de interne audit dienst om in 2024 de voortgang en status van de BIO implementatie bij een aantal directies expliciet te toetsen.

Agenda digitale veiligheid: de 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.

Sinds 2020 richten we ons in het kader van informatiebeveiliging niet alleen op de eigen (gemeentelijke) organisatie, maar ook op andere organisaties in de stad en de regio.
De digitale veiligheid van de Amsterdammer staat daarin nadrukkelijk op de agenda.

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 zijn gesprekken gevoerd met de 5 gemeenten in de veiligheidsregio de politie, de veiligheidsregio zelf en allerlei publieke en private partijen om de samenwerking op het gebied van digitale veiligheid te intensiveren. Er blijkt in de regio veel draagvlak te zijn voor dit onderwerp.
Dit zal leiden tot op het oprichten van een ecosysteem digitale veiligheid in 2024.

In het ecosysteem worden de volgende sporen benoemd:

1. *Bewustwording omtrent digitale veiligheid*

Het spoor bewustwording omtrent digitale veiligheid draait om het vergroten van 'awareness' op het gebied van digitale veiligheid voor iedereen die woonachtig, werkzaam of aanwezig is binnen de regio Amsterdam-Amstelland.

2. *Talent- en expertiseontwikkeling*

Doel hiervan is het verkrijgen van een actueel beeld over talent en expertise in de regio en hoe dat verder te ontwikkelen om de arbeidstekorten op het gebied van digitale veiligheid terug te dringen, staat bij dit spoor centraal.

3. *Informatie-uitwisseling en gevolgbestrijding*

Doelstellingen zijn: het opzetten van een effectief netwerk van CISO's van organisaties in de regio en over sectoren heen. En daarnaast om voorbereid zijn met crisispartners, gemeenten en vitale sectoren op grootschalige uitval van digitale voorzieningen met grote maatschappelijke effecten."

4. *Proeftuinmogelijkheden*

Doel is het kunnen testen van vernieuwende producten en diensten in een gecontroleerde omgeving om innovatie op het vlak van digitale veiligheid te versnellen.

Verbonden partijen

Bij een aantal partijen waarmee Amsterdam samenwerkt of verbonden is (o.a. Waternet, Artis, Pantar) 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.

In de september 2023 heeft het college de *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 worden in 2024 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.

Business Continuity Management

Informatiebeveiliging richt zich op de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid van informatie.
Beschikbaarheid is nauw verweven met het onderwerp Business Continuity Management (BCM).

In de eerste helft van 2023 is de aanpak van BCM voor de gemeente Amsterdam uitgewerkt en door het GMT vastgesteld. De regie hierop is ingeregeld en de eerste stappen zijn gezet.

Inmiddels wordt bij drie belangrijke directies gewerkt aan het inrichten van BCM. Daarbij worden concrete oefeningen uitgevoerd. Op basis hiervan worden de vervolgstappen vormgegeven.

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.

In de 2023 is het crisisdraaiboek voor het i-domein geactualiseerd en hebben twee crisisoefeningen plaatsgevonden.

De eerste oefening was gericht op het i-domein en de directie dienstverlening en had een beperkt omvang.
De tweede oefening was veel omvangrijker: Amsterdam deed mee aan de landelijke ISIDOOR cyberoefening die elke 2 jaar wordt gehouden. Aan deze oefening deden 120 organisaties uit de publieke en private sector mee, waarmee het de grootste cyberoefening was uit de Nederlandse geschiedenis.
Beide oefeningen leverden de nodige leerpunten op die in de komende tijd worden opgepakt. Voor 2024 staan weer nieuwe oefeningen op de rol.

6. Verbeteringen in 2023

In het afgelopen jaar zijn op de volgende gebieden verbeteringen doorgevoerd.

Autorisatiebeheer
Mede naar aanleiding van signalen van de accountant is in 2023 veel aandacht besteed aan het autorisatiebeheer van onze belangrijkste informatiesystemen. Beleid is dat 2 x per jaar de autorisaties van de systemen worden getoetst. Na een wat moeizame start is dit op steeds meer plekken goed ingericht. Aandacht hiervoor blijft de komende jaren zeker nodig.

Pentests
Het uitvoeren van pentests (een in onze opdracht uitgevoerde poging om de beveiliging van een toepassing te doorbreken) is in 2023 geprofessionaliseerd. We werken met vaste externe partijen die deze testen uitvoeren en de werkwijze is geformaliseerd. Het bewustzijn dat pentests noodzakelijk zijn is steeds beter aanwezig.

Verbeteren van inzicht in compliance en risico's
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 2023 hard gewerkt om een eenduidige wijze van risicomanagement op te zetten voor deze aspecten. Eind 2023 is het nieuwe risicomanagement-systeem zodanig ingericht dat directies ook hun informatiebeveiligingsrisico's hierin kunnen vastleggen en de afhandeling hiervan kunnen monitoren. De implementatie hiervan (het gaan werken volgens de afgesproken systematiek) zal in 2024 veel aandacht krijgen.

De compliance aan de BIO wordt in 2023 in dit systeem vastgelegd en vanaf 2024 gebruikt, het onderdeel risicomanagement volgt in de loop van 2024.

Applicaties beter beschermd
Gedurende 2023 zijn steeds meer applicaties die door Amsterdam worden gebruikt voorzien van een extra beveiligingslaag. Door het gebruik van zogenaamde multi-factor authenticatie is het risico op misbruik op basis van gelekte of gedeelde wachtwoorden sterk teruggedrongen. Doordat bovendien steeds meer gebruik wordt gemaakt van single sign on (eenmalig inloggen om toegang te krijgen tot de informatiesystemen die de gebruiker nodig heeft) hoeven gebruikers niet langer allerlei wachtwoorden te onthouden en kunnen gebruiksgemak en beveiliging hand in hand worden verbeterd.

Invoering van een nieuwe veilige werkomgeving
In 2023 is de implementatie van de nieuwe Amsterdamse Digitale Werkomgeving grotendeels afgerond. Deze (cloudgebaseerde) werkomgeving biedt een aanzienlijk hoger niveau van beveiliging dan voorheen en maakt het onder andere mogelijk om op een veel veiliger manier samen te werken, zowel binnen de gemeente als met externe partijen. Onderdeel hiervan is dat aan bijna alle medewerkers beveiligde laptops zijn verstrekt, waarmee een gecontroleerd ICT-landschap is ingericht. Het risico op virussen, malware en dergelijke is hierdoor sterk teruggedrongen.

Weren van bepaalde apps
In navolging van de Rijksoverheid is in 2023 bepaald welke apps op gemeentelijke apparatuur (in het kader van veiligheid en spionage) niet langer zijn toegestaan. Hierover is aan medewerkers gecommuniceerd.

Doordat smartphones en tablets in de afgelopen jaren onder beheer van de gemeente zijn gebracht is het mogelijk om niet-toegestane apps automatisch te verwijderen. Dit wordt voorbereid om in 2024 te realiseren.

Uitwerken en verankeren van het werken in opgaven.
In 2023 is hard gewerkt aan het organiseren van structurele betrokkenheid vanuit informatiebeveiliging (en andere disciplines) bij stedelijke opgaven.
Informatiebeveiliging is betrokken bij elke opgave. Samen met privacy en informatiebeheer wordt gewerkt aan de borging van de benodigde beheersmaatregelen. Hiermee wordt als onderdeel van de implementatie van nieuwe processen en systemen actief gewerkt aan kwaliteitsborging.

7. Wat zijn onze speerpunten voor 2024?

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

Met stip op 1: NIS2

In 2024 wordt de aanpak voor NIS2 uitgewerkt en programmatisch opgepakt. We nemen daarin lopende verbeteracties mee om hier waar nodig meer druk op te zetten. Belangrijke onderdelen zullen zijn:

Evaluatie van de BIO status. NIS2 betekent dat de eisen ten aanzien van de aantoonbaarheid van de digitale weerbaarheid toenemen. Het is dus belangrijk om de status van de BIO scherp in beeld te hebben en vervolgens te bepalen wat er extra nodig is.

Risicomanagement, rapportages en intern toezicht. Zoals eerder aangegeven is er al hard gewerkt aan het inrichten van risicomanagement voor informatiebeveiliging; de volgende stap is dat we dit toepassen op het voor het gehele applicatie-en ICT-landschap. We noemen dat de *feitelijke veiligheid*: zijn onze toepassingen en infrastructuur daadwerkelijk veilig genoeg? We kiezen daarvoor een risicogerichte benadering; de kernprocessen en kritische toepassingen willen als eerste op orde hebben.
Aandachtspunt is het verder verbeteren van risicorapportages en het versterken van het toezicht.

Verbetering van beheer en sturing op leveranciers. Het beheer van het applicatielandschap en de sturing op onze leveranciers moet beter. Het beheer van het applicatielandschap wordt de komende jaren stap voor stap geprofessionaliseerd. Webdomeinen worden daarin meegenomen. De sturing op onze strategische leveranciers en SAAS-leveranciers wordt verbeterd, zodat wij beter kunnen steunen op door hen geleverde diensten en producten. Door een nieuwe security management dienst kunnen wij veel beter de veiligheid van ons volledige ICT-landschap monitoren en bewaken.

Industriële automatisering. NIS2 legt een zoeklicht op de industriële automatisering, ook wel Operationele Technologie (OT)-systemen genoemd. Het betreft hier een breed scala aan toepassingen: van afvalwaterbehandeling en verkeerscontroles tot openbare voorzieningen zoals zwembaden en parkeergarages. Daarnaast integreren slimme stadsinitiatieven vaak Internet of Things (IoT) apparaten die bijdragen aan automatisering.
In de BIO werden deze systemen niet expliciet benoemd, in de NIS2 juist wel. Kenmerk van deze systemen is dat ze gebruik maken van zeer specifieke technieken, dat beveiliging niet altijd in het ontwerp is meegenomen, dat leveranciers niet altijd voldoende bewust zijn van de beveiligingsrisico's en dat het beheer van dit soort systemen versnipperd is.
Binnen Amsterdam is de status van de beveiliging van deze systemen nog onvoldoende in beeld. Prioriteit is om dit inzicht te verbeteren en hierop te sturen.

Bewustwording, meldplicht en extern toezicht. NIS2 geeft aan dat bewustwording (zowel bij bestuurders als bij medewerkers) essentieel is om de veiligheid op orde te hebben.
In Amsterdam is in de afgelopen 2 jaar op concern-niveau minder aandacht gegeven aan bewustwording. Wel zijn bij afzonderlijke directies bewustwordingssessies gehouden met MT's en bij medewerkersbijeenkomsten. Speerpunt voor komend jaar is om dit weer op te pakken (E-learnings, trainingen, etc.). Dit in samenwerking met andere disciplines.
Bij grote incidenten wordt een meldplicht van kracht; binnen een kort tijdsbestek moet een

melding plaatsvinden bij een landelijke autoriteit. Om dit goed in te richten zal het incidentenproces opnieuw worden ingericht. Daarbij zal de grotere aandacht voor bewustwording ertoe bijdragen dat incidenten eerder worden gesignaleerd.
Nieuw in NIS2 is dat een landelijke organisatie is benoemd (de Rijksdienst voor Digitale Infrastructuur) die vooraf en achteraf toezicht zal gaan uitoefenen op essentiële entiteiten. Hoe dit toezicht eruit gaat zien is nog onduidelijk, maar dat er meer druk zal komen op het verantwoordingsproces is al wel duidelijk.

Organisatie van de informatiebeveiliging

Eind 2023 is geconstateerd dat we (na de inrichting van het i-domein in 2022) nog te weinig samenhang hebben gecreëerd in de informatiebeveiligingsorganisatie. Er zijn verschillende functies ingericht die teveel werken vanuit hun eigen doelstellingen, zonder de juiste samenhang, Daardoor werkt het geheel niet optimaal en effectief.
In 2024 zullen we de organisatie tegen het licht houden en waar nodig aanpassingen doorvoeren in organisatie, sturing en/of bezetting.

8. 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 incidenten voordoen waarvan we vervolgens kunnen leren.
Binnen de organisatie is er een vastgesteld proces om informatiebeveiligingsincidenten te melden, registreren en af te handelen. . Informatiebeveiligingsincidenten worden centraal geregistreerd, geanalyseerd en afgehandeld. Incidenten krijgen de classificatie laag, midden of hoog.
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.
Jaarlijks rapporteren we hierover op hoofdlijnen in deze rapportage.

In 2023 is het aantal *door gebruikers* gemelde incidenten afgenomen ten opzichte van het jaar ervoor, het aantal meldingen vanuit strategische partners (die in opdracht van Amsterdam beheerwerkzaamheden verrichten) en het security operations center is juist *toegenomen*.

In 2023 zijn er 401 security incidenten vastgesteld. Van de incidenten betreft ongeveer 69% Phishing mails en brute force aanvallen , 7% zijn incidenten op Cloud en Applicaties, 24% betreft verdacht netwerkverkeer.

De meest voorkomende meldingen door medewerkers zijn Frauduleuze SMS/APP's (49%), verdachte mail/post (24%), en Frauduleuze Telefoontjes (8%).
Hierbij is in de meeste gevallen correct gehandeld door de medewerkers door de poging te herkennen en hiervan melding te doen.

Ten opzichte van het vorige jaar is het aantal incidenten met 35% gegroeid. We zien met name een toename in het aantal phishing meldingen en meldingen op het Cloud Platform, dit komt door de uitrol van de nieuwe werkplek en het in gebruik nemen van het Cloud Platform. Op beide omgevingen wordt de beveiliging stringent bewaakt, waardoor issues eerder / beter worden opgemerkt.

De meeste incidenten hebben de classificatie laag of midden, er zijn in 2023 4 incidenten geweest met de classificatie hoog. Dit is in lijn met voorgaande jaren.

Classificatie	Laag	Midden	Hoog	Totaal
Security Incidenten	335	62	4	401

De vier security incidenten met de classificatie hoog betreffen twee hoge impact phishing incidenten, een Ransomware bestand wat op een fileshare gedetecteerd is en een incident bij een organisatie die in opdracht van Amsterdam systemen beheert.

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

In 2023 is een aanbesteding uitgevoerd om een aantal specifieke security taken bij een externe, onafhankelijke partij te beleggen. De partij die inmiddels is gecontracteerd zal onder andere security monitoring gaan verrichten op de diensten die de strategische partners uitvoeren. De wijze waarop incidenten worden afgehandeld wordt daar uiteraard in meegenomen.

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

In 2023 zijn er 31 incidenten geweest die een serieuze impact hebben gehad op de beschikbaarheid van ICT dienstverlening richting de gemeentelijke organisatie.
Het type incidenten betreft voornamelijk verstoringen op applicaties, de werkplek en netwerken binnen kantoorpanden.

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 2023 was dit van toepassing bij 27 high/high meldingen (hoog risico / hoge impact) en bij 3 lager geclassificeerde meldingen.

Door het tijdig afhandelen van deze meldingen is voorkomen dat aanwezige kwetsbaarheden door kwaadwillenden konden worden uitgebuit.

Meldpunt ethisch 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 kwetsbaarheden1 vallen.

87 Relevante kwetsbaarheidsmeldingen door ethisch hackers

Vanaf de start van het meldpunt in november 2022 zijn er 87 meldingen gedaan die voor de gemeente Amsterdam relevant waren, waarvan 10 meldingen met de status ‘kritiek’ of ‘hoog’.

51 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 daar 51 vermeldingen op geplaatst, zie https://www.informatiebeveiligingsdienst.nl/responsible-disclosure/2023-coordinated-vulnerability-disclosure-hall-of-fame/

62 Uitgereikte beloningen
Voor meldingen uit 2023 hebben we 62 beloningen verstuurd aan melders die afkomstig zijn uit landen over de hele wereld. Deze bestaan uit typisch Amsterdamse attenties van het merk iAmsterdam. De attentie varieert, afhankelijk van de ernst van de kwetsbaarheid.

2 Raadsinformatiebrieven

De gemeenteraad is twee keer geïnformeerd over de status van het meldpunt ethisch hackers (VN2023-013147 en TA2023-000065).

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 aan de gemeenteraad en aan de diverse landelijk toezichthouders.
De ENSIA-rapportages zijn in april 2024 door het college van B en W vastgesteld en worden vervolgens aangeboden aan de toezichthouders.

Een korte samenvatting van de via ENSIA getoetste informatiestelsels en de resultaten over 2023:

Stelsel	Resultaten
Basisregistratie Adressen en Gebouwen	Het onderdeel Proces & Organisatie voldoet wel en het onder deel Gegevenskwaliteit voldoet niet aan de landelijke norm.
Basisregistratie Grootschalige Topografie	Beide getoetste onderdelen Proces & Organisatie en Gegevenskwaliteit voldoen aan de landelijke norm.
Basisregistratie Ondergrond	Beide getoetste onderdelen Proces & Organisatie en Gegevenskwaliteit voldoen aan de landelijke norm.
Suwinet (Inkijk en Inlezen)	Voldoet niet op alle getoetste onderdelen voor informatiebeveiliging.
Suwinet Belastingdeurwaarders	Voldoet op alle getoetste onderdelen voor informatiebeveiliging.
Suwinet Adresfraudeonderzoek	Voldoet niet op alle getoetste onderdelen voor informatiebeveiliging.
Suwinet Doorstroompunt	Voldoet niet op alle getoetste onderdelen voor informatiebeveiliging.
Baseline Informatiebeveiliging Overheid	Voldoet niet op alle onderdelen.

De bevindingen zijn opgenomen in verbeterplannen en worden gemonitord.
Naar verwachting zal de ENSIA-methodiek de komende jaren worden uitgebreid met meer informatiestelsels.

DigiD
Via de landelijke voorziening DigiD krijgen burgers toegang tot bepaalde digitale dienstverlening van de gemeente. De Amsterdamse aansluitingen zijn zoveel mogelijk gestandaardiseerd via de centrale DigiD-portaal ‘Toegangsmakelaar Amsterdam’.

Aansluiting	Omschrijving	Status
Toegangsmakelaar Amsterdam	Dit portaal fungeert als toegangsmakelaar tot diverse digitale dienstverlening van de gemeente Amsterdam.	Voldoet
GGD Ouderportaal Amsterdam	Ouders kunnen via het ouderportaal online afspraken maken en het	Voldoet

	cliëntdossier van hun kind inzien.	
GGD Ouderportaal Amstelland	Ouders kunnen via het ouderportaal online afspraken maken en het cliëntdossier van hun kind inzien.	Voldoet

De DigiD-aansluitingen worden jaarlijks getoetst op een selectie aan beveiligingsnormen die door de landelijk toezichthouder Logius namens het ministerie van BZK worden bepaald. Met deze ICT-beveiligingsassessments houdt Logius toezicht op de DigiD-aansluitingen met als doel landelijk het gebruik van DigiD veilig te houden.