Nummer VN2021-018827
Directie ICT

Gemeente Amsterdam

College van burgemeester en wethouders B&W

Voordracht voor de College vergadering van 06 juli 2021

Portefeuille: ICT en Digitale Stad (42)

Agendapunt: B40

Tekst van openbare besluiten wordt gepubliceerd

Onderwerp

Kennisnemen van de Rapportage 2020 Informatiebeveiliging en de Rapportage 2020 Functionaris gegevensbescherming

Het college van burgemeester en wethouders besluit

1. Kennis te nemen van de Rapportage 2020 Informatiebeveiliging. De rapportage beschrijft de activiteiten, incidenten en ontwikkelingen ten aanzien van informatieveiligheid bij de gemeente Amsterdam over het jaar 2020 en geeft ook een vooruitblik op 2021. In de rapportage zijn ook de uitkomsten opgenomen van de ENSIA-audit op de gemeentelijke DigiD-portalen. Uit deze audit blijkt dat deze portalen aan de eisen voldoen, met uitzondering van een aandachtspunt dat geen directe impact heeft op de informatieveiligheid. De rapportage beschrijft ook de uitkomsten van de zelfevaluatie naar het voldoen aan de landelijk voorgeschreven normen voor informatiebeveiliging (Baseline Informatiebeveiliging Overheid (BIO). Het beeld van eind 2020 laat zien dat alle aspecten van de BIO globaal op orde zijn, maar dat er nog verbeteringen nodig zijn in de beheersing van risico's en het voldoen aan de basisnormen van de BIO);
2. Kennis te nemen van de Rapportage 2020 Functionaris gegevensbescherming. De rapportage beschrijft de activiteiten, de 53 datalekken die bij de Autoriteit Persoonsgegevens zijn gemeld, de 120 verzoeken en de 27 klachten van burgers ten aanzien van gegevensbescherming bij de gemeente Amsterdam over het jaar 2020 en geeft ook een vooruitblik op 2021. Ook beschrijft de rapportage waar nog aandacht voor nodig is. Deze aandachtspunten zijn divers en omvatten onder meer: de inrichting van operationeel risicomanagement, een standaardaanpak voor privacy-by-design, het uitvoeren van een stedelijk plan van aanpak voor de bewaartermijnen en een externe audit op de uitvoering van de Wet politiegegevens;
3. In te stemmen met de raadsbrief, waarmee de rapportages onder 1) en 2) worden aangeboden aan de raad.

Kernboodschap

Het college heeft kennisgenomen van de Rapportage Informatiebeveiliging 2020 en de Rapportage 2020 Functionaris gegevensbescherming. De rapportages beschrijven de activiteiten en ontwikkelingen op het gebied van de informatiebeveiliging en gegevensbescherming bij de gemeente Amsterdam over het jaar 2020 en geven ook een vooruitblik op 2021. De rapportages worden ter kennisname aangeboden aan de raadscommissie Kunst, Diversiteit en Democratisering.

Bestuurlijke achtergrond

Bij de vaststelling van het *Stedelijk kader informatiebeveiliging gemeente Amsterdam* door het college 15 december 2020 (VN2020-029441) is bepaald dat er jaarlijks door het college aan de raad wordt gerapporteerd over de informatiebeveiliging.

De rapportage van de Functionaris gegevensbescherming komt voort uit haar wettelijke verplichting om verslag uit te brengen aan de hoogste leidinggevende van de verwerkingsverantwoordelijke (in dit geval het college en de raad).

Bestuurlijke prioriteit

N.v.t.

Wettelijke grondslag

- Artikel 160, eerste lid onder a, Gemeentewet: het college is bevoegd om het dagelijks bestuur van de gemeente te voeren.
- Artikel 169, eerste en tweede lid, Gemeentewet: het college van burgemeester en wethouders en elk van zijn leden afzonderlijk zijn aan de gemeenteraad verantwoording schuldig over het door het college gevoerde bestuur. Zij geven de raad alle inlichtingen die de raad voor de uitoefening van zijn taak nodig heeft.
- Artikel 38, derde lid, van de Algemene verordening gegevensbescherming (AVG) schrijft voor dat de Functionaris gegevensbescherming rechtstreeks verslag uitbrengt aan de hoogste leidinggevende van de verwerkingsverantwoordelijke (in dit geval het college en de raad). De Functionaris gegevensbescherming is de interne toezichthouder op de gemeentelijke omgang met persoonsgegevens.

Onderbouwing besluit

Ad 1: Kennisnemen van de Rapportage 2020 Informatiebeveiliging:

Met ingang van 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO kent een 130-tal beheersmaatregelen om een basisbeveiligingsniveau te kunnen doorvoeren. Een groot deel van de beheersmaatregelen is verplicht. Voor de invoering van de BIO is in 2020 in opdracht van het GMT een aanpak opgesteld in de vorm van een meerjarenplan, dat gebaseerd is op het beheersen van risico's. Er is een brede betrokkenheid georganiseerd, omdat informatiebeveiliging alle organisatieonderdelen van de gemeente raakt.

Binnen de gemeente Amsterdam zijn met name de volgende risico's relevant:

- De complexe Amsterdamse informatievoorziening maakt dat het zicht op de beveiliging van apparatuur en informatie nog niet op alle vlakken voldoende is;
- Het beheersen van toegang tot informatie en de beveiliging van Internet –of-Things –toepassingen (IoT) en mobiele apparatuur is een aandachtspunt;
- Het zicht op de informatiebeveiliging bij uitbestede werkzaamheden is onvoldoende;
- Het structureel testen van cybercrisissituaties krijgt nog onvoldoende aandacht.

In het kader van de jaarlijkse ENSIA-audit is er een zelfevaluatie uitgevoerd om te zien in hoeverre de gemeente voldoet aan de Baseline Informatiebeveiliging Overheid. Het algemene beeld laat zien dat alle aspecten van de BIO globaal op orde zijn, maar dat er nog verbeteringen mogelijk zijn in de beheersing van risico's en het voldoen aan de basisnormen van de BIO.

De uitkomst van deze zelfevaluatie is gebruikt bij het bepalen van de speerpunten voor 2021. De speerpunten voor 2021 zijn:

- Doorvoeren Baseline informatiebeveiliging overheid: zicht krijgen op en aanpakken van risico's;
- Monitoring en response: doorontwikkelen van het gemeentelijk Security operations center;
- Standaardisatie en vernieuwing: toetsen websites en internetdomeinen, invoering nieuwe ICT-werkplek, realisatie van het cloud competence center;

- Toetsen ICT-infra en informatiesystemen, ook via ethical hackers;
- Beveiliging van industriële automatiseringssystemen, te beginnen met het verhogen van de weerbaarheid in de watersector en de verkeerssector, in samenwerking met de rijksoverheid;
- Bevorderen bewustzijn en digitale vaardigheden medewerkers;
- Continuïteit en veerkracht: opzetten van Business Continuity Management en het oefenen met cyberincidenten;
- Agenda veilige stad: uitwerken ecosysteem rond de vitale infrastructuur van de stad met maatschappelijke partijen;
- Sturing op verbonden partijen (partijen die taken voor ons verrichten).

De rapportage bevat ook de uitkomsten van de (verplichte) jaarlijkse ENSIA-audit naar de staat van de informatiebeveiliging van onze DigiD-portalen, waarover aan de landelijke toezichthouder Logius gerapporteerd is. Via de landelijke DigiD-voorziening kunnen burgers toegang krijgen tot de digitale dienstverlening van de overheid. De gemeente Amsterdam beschikt over zeven verschillende DigiD-portalen. Bij 4 portalen is een aandachtspunt geconstateerd dat geen directe impact heeft op de informatieveiligheid. Deze punten worden binnen de door Logius gestelde termijn opgelost.

De rapportage biedt tot slot cijfermatig inzicht in het aantal incidenten met een hoge impact. Dit zijn (concernbrede) incidenten waarbij bijvoorbeeld de dienstverlening verstoord wordt of waarbij voorzieningen die iedere medewerker nodig heeft (ADW-werkplek, e-mail, internet) niet beschikbaar zijn. In 2020 waren er 30 incidenten met een hoge impact. Dit is lichte daling ten opzichte van de 32 incidenten in 2019. De meeste incidenten zijn het gevolg van hardware- of software storingen.

Ad 2: Kennis te nemen van de Rapportage 2020 Functionaris gegevensbescherming:

Adequaat omgaan met persoonsgegevens is een continu proces en vraagt doorlopend aandacht en daarmee tijd en middelen, van zowel bestuur, management als medewerkers. De rapportage beschrijft welke maatregelen de gemeente Amsterdam in 2020 heeft getroffen om de beginselen van de AVG verder te waarborgen en waar nog actie is vereist. De directies zijn opgeroepen om het verwerkingsregister te actualiseren en het loket Persoonsgegevens heeft ingezet op termijnbewaking. De gemeente heeft in het kader van de transparante overheid een algoritmeregister gelanceerd. De Functionaris gegevensbescherming heeft onderzoek laten doen naar de stand van zaken met betrekking tot Data Protection Impact Assessments (DPIA's). Dit zijn wettelijk voorschreven risicoanalyses. Het eerste deel van het onderzoek is afgerond en daaruit blijkt dat de gemeente nog niet voor al haar risicovolle verwerkingen een DPIA heeft uitgevoerd. De doorlopende bewustwordingscampagne 'Weet wat je deelt 2.0' draagt bij aan het interne bewustzijn over gegevensbescherming. Dit krijgt een extra stimulans door de e-learnings die zijn ontwikkeld een meer verplichtend karakter te geven.

In de periode 2018-2020 zijn belangrijke stappen gezet om de AVG te implementeren. De Functionaris gegevensbescherming constateert dat het plan van aanpak nog niet is afgerond. De aandachtspunten en activiteiten voor het jaar 2021 zijn divers:

- De organisatie zal voor inzicht zorgen in de actuele status van gegevensbescherming met de inrichting van operationeel risicomanagement;
- Formuleren van een gemeentelijke standaardaanpak om invulling te geven aan het principe van privacy by design;
- Uitvoeren van een stedelijk plan van aanpak voor de bewaartermijnen. Voor elke verwerking van persoonsgegevens moet een bewaartermijn zijn bepaald en deze moet worden nageleefd;

- Sinds 2019 hebben BOA's bij de uitoefening van hun taken te maken met de Wet politiegegevens (Wpg). Deze wet verplicht de gemeente om in 2021 een externe audit uit te laten voeren op de gegevensverwerking onder de Wpg. Samen met de CIO zal de FG deze audit begeleiden.

De gemeentesecretaris draagt namens het college en de burgemeester zorg voor de opvolging van de aandachtspunten en activiteiten. De Functionaris gegevensbescherming voorziet hem van de benodigde informatie over de voortgang en knelpunten.

De rapportage biedt ook cijfermatig inzicht in klachten en verzoeken van burgers en in de gemelde datalekken:

- In 2020 heeft de Functionaris gegevensbescherming 27 klachten ontvangen tegen 38 in 2019.
- Via het digitale Loket Persoonsgegevens kan de Amsterdammer een verzoek indienen tot inzage, verwijdering of correctie van persoonsgegevens. In 2020 heeft het loket 120 AVG verzoeken in behandeling genomen. Dit betekent een kleine stijging (+7) ten opzichte van 2019.
- In 2020 zijn 180 datalekken geregistreerd waarvan er 53 bij de landelijke toezichthouder, (Autoriteit Persoonsgegevens) zijn gemeld. Datalekken moeten worden gemeld wanneer er een risico bestaat op nadelige gevolgen voor de burger of werknemer. In 2019 was er sprake van 156 geregistreerde datalekken, waarvan er toen 38 gemeld zijn bij de Autoriteit Persoonsgegevens. Het feit dat het aantal interne meldingen wederom is gestegen ten opzichte van het vorige jaar, wijst erop dat het bewustzijn rondom datalekken is toegenomen.

Participatie

N.v.t.

Financiële onderbouwing

Conclusie

De genoemde beslispunten in de voordracht hebben geen financiële consequenties.

Communicatie

Binnen de gemeente

Het besluit wordt opgenomen in de te publiceren besluitenlijst. De raadsinformatiebrief en rapportages worden ook via de dagmail verzonden.

Buiten de gemeente

N.v.t.

Documenten

Registratienr.	Naam
AD2021-069700	Advies (pdf)
AD2021-069665	College van B&W Voordracht (pdf)
AD2021-074557	GEWIJZIGDE VERSIE Raadsinformatiebrief_DEF.pdf (pdf)
AD2021-069678	Rapportage 2020 Functionaris gegevensbescherming.pdf (pdf)
AD2021-069676	Rapportage 2020 Informatiebeveiliging.pdf (pdf)
AD2021-069675	TEKENEN Raadsinformatiebrief.docx (msw12)

Behandelend ambtenaar (naam, telefoonnummer en e-mailadres)

Chief Information Security Officer: [redacted]@amsterdam.nl of 06 – [redacted]) Functionaris Gegevensbescherming: [redacted]@amsterdam.nl of 06 – [redacted]

Besluit college van burgemeester en wethouders

Conform besloten, voorts wordt de portefeuillehouder gemachtigd tot het maken van tekstuele wijzigingen