Retouradres: Postbus 94652, 1090 GR Amsterdam

Gemeente Amsterdam

Commissie Persoonsgegevens

PER E-MAIL
CISO [redacted].
De heer 5.1, 2, e
Kopie: CIO, J. Flippo

Datum	23 december 2015
Ons kenmerk	U150142
Behandeld door	Mw. [redacted], 5.1, 2, e
Doorkiesnummer	5.1, 2, e
Faxnummer	nvt
E-mail	5.1, 2, e @amsterdam.nl
Bijlage	1
Onderwerp	Advies Commissie Persoonsgegevens Amsterdam

Geachte heer 5.1, 2, e ,

Op de vergadering van de Commissie Persoonsgegevens Amsterdam (CPA) van 5 november jl. was u in uw hoedanigheid van Chief Information Security Officer aanwezig. Bij het agendapunt "Kennismaking met de CISO [redacted]." heeft de CPA het navolgende besproken.

De CPA stelt vast dat per 1 januari 2016 de Wetmeldplicht datalekken en uitbreiding boetebevoegdheid CBP in werking treedt. De raakvlakken tussen privacy en security worden daardoor verder versterkt. De CPA signaleert dat het zicht op bewerkers en actuele bewerkersovereenkomsten die voldoen aan de Richtsnoeren beveiliging van persoonsgegevens van het CBP en de nieuwe wetgeving over het melden van datalekken van groot belang is. De CPA gaat er vanuit dat dit gegeven een hoge prioriteit krijgt daar het informatieveiligheid met betrekking tot vaak gevoelige gegevensverwerkingen met persoonsgegevens betreft.

De CPA vraagt , mede in dit verband, naar de bevoegdheden van de CISO en de naar de status van bevindingen en een beveiligingsadvies van de CISO in concrete gevallen.

Tot slot vraagt de CPA aan de CISO om tegen september 2016 de stand van zaken met betrekking tot de implementatie van de Baseline Informatiebeveiliging Gemeenten (BIG) te bespreken.

Bijgaand treft u het deel van de notulen van de vergadering aan over het betreffende agendapunt.

Ik vertrouw er op u aldus voldoende geïnformeerd te hebben.

Hoogachtend,

De heer mr. dr U. van de [5:1, 2, e]
Voorzitter Commissie Persoonsgegevens Amsterdam

Commissie Persoonsgegevens Amsterdam
Uittreksel van het verslag van de openbare vergadering op donderdag 5 november 2015

6. Kennismaking met de CISO [redacted]i. (CIO Office)
De CPA verwelkomt de CISO. De volgende aandachtspunten komen aan de orde:
- de ambitie voor de komende jaren;
- de raakvlakken tussen privacy en security;
- de meldplicht datalekken per 1 januari 2016;
- of er voldoende bekendheid over is in de stad;
- of er voldoende zicht is op bewerkers;
- andere prioriteiten voor informatiebeveiliging die actueel zijn;
- wat er aan bewustwording wordt gedaan;
- wat de bevoegdheden van de CISO zijn;
- de jaarlijkse audit naar Wigo4it.

De heer 5.1, 2, e is bestuurskundige en politicoloog en opgeleid als IT-auditor. Hij was lange tijd werkzaam voor KPMG. Daarna was hij lange tijd werkzaam als auditmanager IT bij ACAM. Per 1 september is hij CISO [redacted]i. De CIO heeft hem gevraagd.
Zijn expertise is systemen, toegang, netwerken, beveiliging en architectuur.
Het is een uitdaging om de handschoen op te pakken en zaken te verbeteren. Het doel is om de gemeente verder te brengen. Van belang is dat de CISO kennis heeft van de stad en weet waar e risico's en uitdagingen zijn.

De implementatie van de BIG is erg belangrijk. Dit wordt vanuit de VNG en het Rijk gevolgd. Het gaat om de implementatie van een standaard met een normenkader en maatregelen. Amsterdam is groot en vanuit het verleden werkten onderdelen zelfstandig en langs elkaar heen. Het doel is om de situatie bestendig beheersbaar te maken en om dit in de dynamiek van de verandering naar een centraal aangestuurde organisatie te doen. Er is zowel een reorganisatie gaande als een ICT-centralisatie. Het doel is om het samen met de stad te doen, dat wil zeggen dat de informatiebeveiligers bij de Informatievoorzieningseenheden van de clusters in positie gebracht moeten worden.

Besproken wordt dat er een relatie is tussen privacy- en informatiebeveiliging. Bij de CIO office is de ambtelijk secretaris te werk gesteld. Daarnaast zal een privacycoördinator geworven worden (1 FTE) voor de coördinatie in het privacydossier. Een vakoverleg privacy is gestart. Dit overleg bestaat uit stafjuristen, DJZ, de ambtelijk secretaris en de privacycoördinatoren per Cluster.

Het raakvlak tussen privacy en security toont zich ook bij datalekken. Per 1 januari 2016 moet de gemeente Amsterdam zijn voorbereid op de meldplicht datalekken. Een procedure voor het melden van datalekken is in voorbereiding als ook een brief aan bewerkers van de gemeente Amsterdam en de ambtelijk verantwoordelijken. Er komt één centraal punt waar datalekken gemeld moeten worden. Dat centrale meldpunt is de CISO. De Clusters gaan vervolgen de betreffende zaak onderzoeken en treffen maatregelen die de impact moeten

beperken en ook zal een kennisgeving aan betrokkenen en een melding aan het CBP verricht moeten worden. Daarbij is het de vraag wanneer een datalek als ernstig is te kwalificeren. Er is geen illusie dat 100% van de bewerkers in beeld zijn; daarom wordt gesteund op de privacycoördinatoren om de brieven aan de juiste entiteiten te adresseren. Het onderwerp leeft in de stad; er zijn veel vragen over. De VNG heeft een ledenbrief over het onderwerp naar gemeenten gestuurd.

Andere prioriteiten zijn: toegangsbeheer en autorisaties. Van belang is dat helder is wie, wie is, wie bij de gemeente werkt en waar en tot welke systemen de betreffende persoon toegang moet hebben voor de uitoefening van zijn functie.

Met medewerkers van het CIO office wordt gewerkt aan een bewustwordingscampagne. Het gaat om het informeren van omstreeks 14.000 medewerkers. Het is de bedoeling dat de communicatie specifiek gemaakt wordt en gericht wordt aan een doelgroep bv informatieveiligheid betekent iets anders voor een boa dan voor jeugdzorg. De communicatiebehoefte wordt op de doelgroep afgestemd.

De CISO wordt vaak gevraagd of iets mag, of een maatregel of oplossing goed is of een juiste keuze. Ook kosten worden daarbij als argument gebruikt. Bij een go-no go besluit moet er zicht zijn op de vraag of het veilig is. Dat is het streven. De CISO neemt niet het uiteindelijke besluit dat is aan de ambtelijk verantwoordelijken. Wel moet er voor gezorgd worden dat de CISO tijdig heeft geadviseerd. De betreffende clusterdirecteur die verantwoordelijk is voor het proces is degene die de beslissing neemt. Ook wordt via dia lijn de vakwethouder geïnformeerd.

Tot slot wordt opgemerkt dat de audit Wigo4it 2015 gaande is.

Actiepunt voor de Actielijst: gevraagd wordt om tegen de zomer van 2016 een stand van zaken te bespreken inzake de implementatie van de BIG.