MEMO

Onderwerp	:	Korte toets Rekenkamercommissie Privacy in het sociaal domein
Datum	:	28 februari 2017
Van	:	Burgemeester en wethouders
Aan	:	de Raad

De Rekenkamer BEL heeft onderzoek (zgn. korte toets) gedaan naar de juridische borging van privacy in het Sociaal Domein. In het onderzoeksrapport worden een aantal aanbevelingen gedaan aan zowel de raden als de colleges.
In gevallen dat het een onderzoek betreft, stelt de Rekenkamercommissie de colleges in de gelegenheid hun zienswijze op het onderzoeksrapport kenbaar te maken. Dat is nu conform de Verordening Rekenkamercommissie achterwege gebleven omdat het geen onderzoek maar een korte toets betreft.

Gezien echter zowel het belang van het onderwerp als ook de specifieke materie die het betreft, hecht het college er aan om navolgende reactie op de aanbevelingen aan de raad kenbaar te maken, opdat deze kan worden betrokken bij bespreking door uw raad.

<u>Aanbevelingen voor Gemeenteraden</u>

1. De aanbeveling van de Rekenkamer BEL uit 2015 over de uitvoering van een GAP- en risicoanalyse met betrekking tot digitale veiligheid is nog steeds actueel. Vraag het college om de CISO de GAP- en risicoanalyse te laten uitvoeren en laat u informeren over de uitkomst.

Reactie college:
In 2016 zijn al veel maatregelen getroffen om voor de hand liggende beveiligingsrisico's op te pakken. Zo is een systematische controle op de inrichting van de autorisaties van al onze applicaties door de functioneel beheerders ingevoerd, is een beveiligde omgeving ingericht voor het samen werken aan belangrijke bestanden in bijv. projecten en is een gedetailleerde GAP-analyse uitgewerkt. De uitkomsten van de GAP-analyse 2017 op basis van de landelijke Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) worden in het eerste kwartaal van 2017 nog gerapporteerd aan de directieraad, incl. een risicoanalyse en advisering over de prioritering van te nemen beveiligingsmaatregelen in de vorm van een informatiebeveiligingsplan 2017 – 2018.
De portefeuillehouders van de 3 BEL-gemeenten, zijnde de burgemeesters, alsmede de DB-portefeuillehouder van de GR BEL Combinatie zullen onmiddellijk daarna worden geïnformeerd.

2: Vraag het college om managementinformatie over de risico's rond privacy en informatiebeveiliging.

Reactie college:
Het inrichten van een Information Security Management System zal een vervolg zijn op de GAP-analyse. Er is al afgesproken dat managementinformatie over informatiebeveiliging zal worden meegenomen in de kwartaalrapportages 2017 e.v. als verantwoording aan de directie en het DB en AB van de GR BEL Combinatie. De raden ontvangen ieder kwartaal de scorecard van de BEL Combinatie. Indien zij andere of aanvullende indicatoren in die scorecard opgenomen willen zien, kunnen zij hierom verzoeken.

Aanbevelingen voor colleges van B&W

3. Stimuleer het 'veilig' melden van datalekken. Zorg voor registratie van voorvallen en bijna-voorvallen met betrekking tot privacy, met uitsluitend als doel om daarvan te leren en te verbeteren. Medewerkers moeten te allen tijde incidenten kunnen melden zonder risico op persoonlijke consequenties.

Reactie college:
Deze aanbeveling wordt overgenomen en is voor een belangrijk ook al in de praktijk gerealiseerd. Sinds augustus 2016 is een nieuwe procedure voor de melding en afhandeling van incidenten en bijna-incidenten binnen de BEL Combinatie en BEL-gemeenten van kracht. Alle (bijna-incidenten kunnen medewerkers melden bij:

- hun direct leidinggevende (= coördinator van het vakteam);
- de beveiligingsfunctionaris / CISO;
- de preventiemedewerkers als het om een agressie-incident gaat;
- de (externe) vertrouwenspersoon.

Alle incidenten moeten via een standaard format geregistreerd worden en hiervoor is ook ondersteunende software (Topdesk) voor beschikbaar. Het is daarnaast ook mogelijk om een papieren incidentenmeldingsformulier in te vullen, te ondertekenen en daarna bij de beveiligingsfunctionaris/CISO in te leveren, die dan zorgt voor de registratie.
De afhandeling van incidenten is ook gestandaardiseerd. Er wordt bij een groter incident altijd een zogenaamde 'Werkgroep Incident' ingesteld, die qua samenstelling maatwerk is, afhankelijk van het type incident. Doel van de werkgroep is om het incident grondig te analyseren en aanbevelingen te doen voor het nemen van repressieve, corrigerende en preventieve maatregelen.
Repressieve maatregelen zijn vooral van toepassing bij agressie-, diefstal- en fraude-incidenten en worden ook wel 'lik-op-stuk'-maatregelen genoemd, dus dan gaat het bijvoorbeeld om het verbieden van toegang in de gemeentehuizen, c.q. BEL-kantoor van een agressieve klant, of om het op tijdelijk non-actief zetten van een of meer medewerkers, indien er een verdenking is van fraude.
Corrigerende maatregelen zijn gericht op het herstellen van eventueel aangerichte schade en het voorkomen van verdere schade. Dit kan dus bij een IT-incident het herstellen van een back-up van het systeem zijn, het herstellen van het gebouw bij een inbraak of het informeren en zo nodig adviseren van getroffen inwoners bij een (vermoeden van) een datalek. Ook het verplicht melden van het (vermeend) datalek aan de Autoriteit Persoonsgegevens is een van de te nemen corrigerende maatregelen.
En *preventieve maatregelen* richten zich op het in de toekomst voorkomen dat zo'n incident zich nogmaals kan voordoen. Eigenlijk gaat het daarbij om het aantoonbaar leren van de organisatie n.a.v. het zich voordoen van een incident. Hierbij gaat het om een heel scala van maatregelen die niet alleen op papier staan, maar ook in de praktijk gerealiseerd zijn. Met het voldoen aan alle BIG-normen heeft een organisatie feitelijk al veel preventieve maatregelen genomen, maar omdat informatieveiligheid continu in beweging is, kunnen zich altijd incidenten blijven voordoen en dan is het de kunst om daarvan telkens te leren.
Ook in de gemeente Huizen / HBEL-uitvoeringsorganisatie is beleid geformuleerd rondom het veilig melden van datalekken. Alle medewerkers hebben daar via het intranet toegang tot de procedure voor het melden van datalekken.

4. Breid het beveiligd mailen uit tot alle relevante ketenpartners in het sociaal domein. Evalueer de toepassing van het beveiligd mailen en betrek daarbij zowel de ervaring van de gemeenten als van de ketenpartners.

Reactie college:
Deze aanbeveling wordt overgenomen.
Data-uitwisseling vindt ook bij de BEL Combinatie en de BEL-gemeenten op vele manieren plaats, waaronder ook per mail. De standaard mailsoftware, zoals Outlook is niet veilig genoeg om vertrouwelijke informatie of data die vallen onder de Wet bescherming persoonsgegevens uit te wisselen. Het veilig maken van de onderlinge datacommunicatie is niet van de een op andere dag geregeld. In de HBEL-uitvoeringsorganisatie loopt op dit moment een pilot met beveiligd mailen onder de jeugdconsulenten. Die pilot wordt binnenkort geëvalueerd. Binnen de BEL Combinatie zijn inmiddels diverse maatregelen doorgevoerd:

- uitwisseling van data die vallen onder de Wbp mag nooit per onbeveiligde mail plaatsvinden;

- indien mogelijk maken we gebruik van data-uitwisseling over beveiligde lijnen, waarbij de ata dus tijdens 'het transport' digitaal versleuteld (encrypted) worden – we gaan niet eerder over op het werken met beveiligde lijnen, voordat wij er van overtuigd zijn dat die lijnen ook echt voldoen aan de hiervoor geldende IT-normen;
- data-uitwisseling kan ook plaatsvinden door externen per uitwisseling toegang te geven tot een apart beveiligde data-omgeving, die door ons is ingericht. Met het gebruik die beveiligde omgeving wordt inmiddels ook geëxperimenteerd. Deze beveiligde omgeving biedt daarnaast extra garanties voor het samen werken aan de totstandkoming van één integraal advies of bestand, waarbij alle wijzigingen worden gelogd en achteraf ook weer ongedaan gemaakt kunnen worden (indien gewenst en nodig). Ook externen kunnen op initiatief van de verantwoordelijke BEL-medewerker worden uitgenodigd om tijdelijk toegang te hebben tot die beveiligde werkomgeving. Dat gebeurt dan door middel van een zogenaamde 2-way identificatie methode, waarbij naast gebruikersnaam en password ook een code per SMS naar een mobiele telefoon wordt verzonden, die vervolgens ook moet worden ingevoerd.
- wij hanteren een inbelbeleid als technische specialisten in onze software moeten werken, zodat vooraf toestemming moet zijn verkregen voor die toegang en dat ook geregistreerd is.
- alle medewerkers leggen na hun aanstelling de ambtseed en ondertekenen een integriteitsverklaring. Externe inhuurkrachten tekenen altijd een geheimhoudingsverklaring.
- wij zijn bezig om met onze leveranciers die persoonsgegevens verwerken zogenaamde bewerkersovereenkomsten af te sluiten, waarmee afspraken over veilig gebruik van privacygevoelige data door de leverancier worden gemaakt, incl. het regelen van aansprakelijkheid en het zich verantwoorden over de uitvoering van beveiligingsmaatregelen.
- Het Jeugd- en Gezinsteam Eemnes maakt gebruik van beveiligd mailverkeer met de huisartsen via Zorgmail.

5. Onderzoek de werking en toepassing van het privacyprotocol in de praktijk. Breng in kaart waar de gemeentelijke uitvoeringsorganisatie knelpunten ervaart.

Reactie college:
Deze aanbeveling wordt overgenomen.
Privacybescherming is onderdeel van het informatieveiligheidsbeleid van de BEL Combinatie en zal als zodanig ook bij de GAP-analyse worden meegenomen. Wij richten ons beleid ook op het voldoen aan de Algemene Verordening Gegevensbescherming die door de EU is vastgesteld en in 2018 van kracht zal worden en dan o.a. de Nederlandse Wbp zal vervangen. Het huidige privacyprotocol zal ook worden getoetst aan de eisen die de AVG hier aan stelt en zal zo nodig hierop worden aangepast. Deze actie zal in het beveiligingsplan 2017-2018 worden opgenomen. Ook in de Uitvoeringsorganisatie HBEL zal werking en toepassing van het privacyprotocol een vast onderdeel worden van de risicoanalyses.

6. Onderzoek in hoeverre er verschillen zijn tussen de privacyreglementen van ketenpartners en het privacyprotocol van de BEL-gemeenten. Breng in kaart waar de ketenpartners knelpunten ervaren. Leg vast dat ook voor ketenpartners het privacyprotocol van de BEL-gemeenten als richtlijn geldt.

Reactie college:
De aanbeveling wordt deels overgenomen. Naar aanleiding van het rapport "De rol van toestemming in het sociaal domein" van de Autoriteit Persoonsgegevens van april 2016 hebben de gemeenten in de Gooi en Vechtstreek een onderzoek laten doen naar de grondslagen van de persoonsgegevensverwerking die zij in het sociaal domein uitvoeren. Het onderzoek is momenteel in de afrondende fase. De uitkomsten van het onderzoek dienen als basis voor het maken van werkafspraken met samenwerkingspartners. De verwachting is namelijk dat het onderzoek licht zal werpen op welke persoonsgegevens rechtmatig en proportioneel zijn bij het uitvoeren van het werk en dus ook in de samenwerking met andere partners. In zoverre wordt de aanbeveling overgenomen. De aanbeveling wordt niet overgenomen als het gaat om het opleggen van het privacyprotocol als richtlijn voor de ketenpartners. Wij zijn hierin van mening dat ketenpartners zelf verantwoordelijk zijn voor de borging van privacy conform de wet, maar gaan hierover wel in overleg, zoals in de vorige alinea aangegeven.

****