Rekenkamer Arnhem

Zaaknr: 224789

Betreft: Rekenkamerbrief vervolgonderzoek informatieveiligheid en privacy

16 mei 2018

Geachte raadsleden,

Inleiding

Op 30 november 2017 hebben wij uw raad geïnformeerd over de start van het vervolgonderzoek naar informatiebeveiliging in het sociaal domein. Dit als vervolg op het in februari 2017 aan u gepresenteerde rapport 'Privacy made in [Arnhem], een onderzoek naar privacy en informatieveiligheid in het sociaal domein'. Dat onderzoek richtte zich op de mate van doeltreffendheid en doelmatigheid van de informatieveiligheid en het privacybeleid in beleidsmatige zin. Hierbij werd gekeken naar het beleid, de governance en werkprocessen, en het bewustzijn aan de hand van documentatie, interviews en bijeenkomsten. Met andere woorden, hoe het gedrag van de betrokken medewerkers is en of dat waarborgen biedt voor een goede informatiebeveiliging. Dat onderzoek schetste een positief beeld.

In dit vervolgonderzoek gaat het erom hoe de informatiebeveiliging in de, met name technische, praktijk werkt: een diepteonderzoek naar de informatiebeveiliging van het sociaal domein. Een ethische hacker heeft daarbij getoetst wat de huidige stand van de beveiliging is en onderzocht of de informatieveiligheid en privacy in technische zin geborgd is. Om aan te tonen dat de beveiliging rondom het sociaal domein op orde is, is ook een gemeentebrede netwerkscan uitgevoerd. Daarin is onderzocht of er geen kwetsbaarheden zijn in andere applicaties die mogelijk indirect een impact hebben op de beveiliging van het sociaal domein.

Bij de uitvoering van het onderzoek heeft de hacker gekozen voor de kortste weg met maximaal resultaat, in die zin dat hij gestart is met de gemeentebrede netwerkscan. Deze scan had als insteek dat als direct doorgedrongen kan worden tot kwetsbare systemen en privacygegevens met een veel breder bereik dan het sociaal domein alleen, de uitkomsten altijd ook het sociaal domein afdekken.

Samenwerking

De Rekenkamer heeft er bewust voor gekozen om in dit gevoelige onderzoek de samenwerking te zoeken met de ambtelijke organisatie (i.c. De Connectie) en is verheugd over de constructieve opstelling van de organisatie. De rekenkamer heeft ook bewust vroegtijdig de samenwerking gezocht vanuit de ervaring dat de uitkomsten dusdanig zouden kunnen zijn, dat direct ingrijpen aan de orde is. De bij een rekenkameronderzoek gebruikelijke periode voor technisch wederhoor op de feiten zou dan gebruikt kunnen worden om de meest urgente kwetsbaarheden te verhelpen, zodat bij de oplevering van het bestuurlijk rapport aan de raad deze spreekwoordelijke 'lekken gedicht zijn'.

Inmiddels is het onderzoek afgerond en informeren wij u over de uitkomsten en over onze conclusies en aanbevelingen. Dat doen wij via deze rekenkamerbrief, die daarmee het karakter heeft van het bestuurlijk eindrapport van het vervolgonderzoek. Wij hebben het concept van deze brief voorgelegd aan het college voor een bestuurlijke reactie. Aan het eind van deze brief gaan wij daar nader op in.

Overigens hebben wij ook de andere partijen die betrokken zijn bij De Connectie geïnformeerd over dit vervolgonderzoek. Pas nadat wij de uitkomsten met uw raad hebben gedeeld hebben wij deze partijen geïnformeerd over de onderzoeksresultaten.

De uitkomsten van het onderzoek

De onderzoekers hebben ernstige onvolkomenheden geconstateerd in de beveiliging van de processen en systemen. Er werd onder andere toegang verkregen tot privacygevoelige informatie van burgers, bestuurders en ambtenaren.

Technisch wederhoor

Vanuit De Connectie is een reactie verkregen op de onderzoeksresultaten in het kader van het technisch wederhoor. Deze reactie vormde geen aanleiding om de onderzoeksresultaten aan te passen, ze zijn feitelijk juist en onweersproken. Daarbij is door De Connectie aangegeven op welke wijze de aangetoonde kwetsbaarheden worden opgepakt. De Rekenkamer had in eerste instantie zorgen bij de gekozen route: er werd na het technisch wederhoor een onvolledige aanpak gevolgd. De geconstateerde tekortkomingen werden niet met de grootst mogelijke daadkracht aangepakt. Onze inhoudelijke zorgen hierbij hebben wij besproken met De Connectie en met de ambtelijke top van Arnhem en aanvullend op schrift gesteld, zodat deze betrokken kon worden bij het verhelpen van de kwetsbaarheden. De directie heeft, na navraag door de Rekenkamer, verzekerd deze zaken daadkrachtig en voortvarend op te pakken. De implementatie ervan gaat voorbij aan de verantwoordelijkheid van de Rekenkamer.

Conclusies

Op basis van de resultaten concludeert de Rekenkamer dat de veiligheid van de systemen waar de gemeente Arnhem gebruik van maakt onvoldoende is. Het vervolgonderzoek heeft aangetoond dat feitelijk alle kernprocessen van Arnhem toegankelijk en manipuleerbaar waren voor een door de Rekenkamer ingeschakelde ethische hacker en dat deze toegang heeft verkregen tot privacygevoelige informatie. In het onderzoek is de daadwerkelijke informatieveiligheid op de proef gesteld, waarbij een groot aantal tekortkomingen in de informatiebeveiliging is vastgesteld.

Daarnaast concludeert de Rekenkamer dat De Connectie niet in control is op het gebied van informatiebeveiliging en privacybescherming, gelet op de wijze waarop de aanpak van de aangetoonde tekortkomingen worden gekoppeld aan lopende projecten zonder dat deze tekortkomingen daarmee inhoudelijk worden verholpen. Hierdoor is Arnhem, en daarmee ook de andere deelnemers aan De Connectie, kwetsbaar.

Tenslotte concludeert de Rekenkamer dat er sprake is van een ontkoppeling tussen gedrag, beleid en uitvoering op het gebied van informatieveiligheid en privacybescherming, gelet op het opvallend grote verschil tussen de uitkomsten van het in 2017 uitgevoerde beleidsmatige onderzoek en de uitkomsten van het (technische) vervolgonderzoek. Het roept de (niet door de Rekenkamer onderzochte) vraag op of dit zich beperkt tot dit onderwerp of dat er sprake is van een bredere reikwijdte in relatie tot het takenpakket van De Connectie.

Wat de Rekenkamer niet heeft onderzocht, is of de systemen die door Arnhem aan de Connectie zijn overgedragen, eerder beter beveiligd waren.

Aanbevelingen

Op basis van het onderzoek beveelt de Rekenkamer aan de raad aan het college opdracht te geven om:

1. Via haar positie binnen De Connectie met hoge urgentie de aangetoonde kwetsbaarheden te laten verhelpen;
2. De informatiebeveiliging binnen De Connectie op een dusdanige wijze te laten organiseren dat De Connectie op korte termijn 'in control' komt op dit onderwerp, waarmee de koppeling wordt hersteld tussen gedrag, beleid en uitvoering;
3. De gemeenteraad van Arnhem binnen drie maanden te informeren over de aanpak en uitkomsten van de aanbevelingen 1 en 2.

Bestuurlijke reactie van het college

Rekenkamer Arnhem
P/a Stadhuis

Zaaknr: 255693

Bestuurlijke reactie in het kader van Vervolgonderzoek informatieveiligheid in het sociaal domein

Op 19 april jl. stelde uw rekenkamer ons college in de gelegenheid om een reactie te geven op uw (concept) conclusies en aanbevelingen naar aanleiding van het 'vervolgonderzoek informatieveiligheid in het sociaal domein'. Laatstgenoemd onderzoek richt zich op de technische aspecten van de praktijk, en vormt een vervolg op het eerder gehouden rekenkameronderzoek 'Privacy made in [Arnhem], een onderzoek naar privacy en informatieveiligheid in het sociaal domein', dat zich juist richtte op beleidsmatige aspecten. In het rapport 'Privacy made in [Arnhem]' schetste de rekenkamer een (overwegend) positief beeld.

Voor het technische vervolgonderzoek heeft u bewust de samenwerking gezocht met de ambtelijke organisatie (hoofdzakelijk De Connectie, die immers de ict-dienstverlening voor de gemeente Arnhem verzorgt), juist ook vanwege het feit dat de uitkomsten van het onderzoek zodanige kwetsbaarheden aan het licht zouden kunnen brengen dat direct ingrijpen geboden is om ernstige benadeling van de gemeente Arnhem én van haar burgers te voorkomen. Ons college waardeert deze prudente handelwijze van uw rekenkamer.

Ons college is geschrokken van de uitkomsten van het nu verrichte (technische) vervolgonderzoek. Het bleek voor een door de rekenkamer ingeschakelde ethische hacker namelijk mogelijk om zich met behulp van enkele relatief eenvoudige kunstgrepen de rechten van een systeembeheerder ('admin-account') toe te eigenen, waardoor hij in principe controle had over de complete infrastructuur van de gemeente Arnhem. Op die manier kon de ethische hacker zich ook toegang verschaffen tot privacygevoelige informatie van burgers, ambtenaren en bestuurders.

De ethische hacker heeft - met succes - getracht om het gemeentelijke netwerk 'inside-out' binnen te dringen. Dit betekent, dat hij van binnenuit een fysieke verbinding tot stand wist te brengen met het gemeentelijke netwerk. Van deze inside-out kwetsbaarheid waren wij ons weliswaar bewust, maar er bestond een achterstand in de te nemen maatregelen. Onze eigen reguliere informatiebeveiligingsaudits (zelftesten) richten zich primair op outside-in aanvallen, waarbij van buitenaf wordt getracht binnen te dringen op ons netwerk (en waarbij de aanvaller zich dus niet in een gemeentelijk gebouw hoeft te begeven). De meeste aanvallen vinden namelijk ook op deze manier plaats. Van buitenaf zijn bij het nu gehouden onderzoek ook geen kwetsbaarheden gevonden. Zelftesten op 'inside-out' aanvallen zijn echter tot dusverre niet gehouden. De aangetroffen kwetsbaarheden bleken daar te zitten. Het ict systeem gaf wel op een later moment een alarmering af, maar het had absoluut nooit zover mogen komen.
Deze grote kwetsbaarheid voor aanvallen van binnenuit vormt voor ons het belangrijkste leerpunt van dit onderzoek van de rekenkamer.

Op deze gevonden kwetsbaarheid is onmiddellijk - mede na toelichting door de ethische hacker - actie ondernomen. Er zijn maatregelen genomen om het voor een hacker minder eenvoudig te maken zich de rechten van de systeembeheerder toe te eigenen, indien hij zich ondanks getroffen beveiligingsmaatregelen toegang tot het netwerk weet te verschaffen. Arnhem is wel een gastvrije

gemeente, en dat willen we - waar mogelijk - ook tot uitdrukking brengen in de toegankelijkheid van onze gemeentelijke gebouwen. De kwetsbaarheid voor aanvallen van binnenuit moet dan ook via technische oplossingen worden verminderd. We kiezen er nadrukkelijk niet voor om de fysieke toegankelijkheid van onze gebouwen voor onze burgers te verminderen.

Door de uitkomsten van het rekenkameronderzoek zijn alle betrokkenen op scherp gezet en er nog eens op gewezen dat informatiebeveiliging continu up-to-date moet blijven. Bij dit alles is het wel relevant om ons te beseffen dat De Connectie, waarbij het beheer van het gemeentelijke ict-netwerk is belegd, nog geen jaar geleden van start is gegaan. In deze nieuwe situatie is het nog nodig om afspraken en procedures nader aan te scherpen. Bovendien is in de periode voor de start van De Connectie - juist met het oog op die aanstaande start - slechts beperkt geïnvesteerd in het beheer van de gemeentelijke ict infrastructuur en in (nieuwe) informatieveiligheidsmaatregelen.
De Connectie was de afgelopen periode al bezig een flink aantal zaken op het gebied van informatieveiligheid - ten aanzien waarvan nu in het rekenkameronderzoek kwetsbaarheden zijn aangetroffen - te verbeteren. De uitkomsten van het nu gehouden rekenkameronderzoek maken de urgentie van deze verbeteringen wel bijzonder duidelijk.

Als opdrachtgever voor De Connectie, en als deelnemer aan de gemeenschappelijke regeling De Connectie, stuurt ons college - binnen de ons toekomende bevoegdheden - er vanzelfsprekend op dat de werkwijze van De Connectie voldoet aan eisen op het gebied van informatie- en privacybescherming en meer in het bijzonder dat zij de nu noodzakelijk gebleken verbetermaatregelen op korte termijn treft. Het door uw rekenkamer gehouden vervolgonderzoek draagt aan ons aller scherpte bij.

In het vervolgonderzoek van de rekenkamer is nog een aantal andere specifieke kleinere kwetsbaarheden aan het licht gekomen. De Connectie heeft een plan van aanpak opgesteld om ook deze issues op korte termijn te verhelpen. Na implementatie van alle verbetermaatregelen, zal in de loop van de komende maanden een nieuwe test worden gehouden om het beveiligingsniveau van het netwerk opnieuw door middel van een hackpoging te testen. Zo zal blijken of de getroffen maatregelen voldoende effectief zijn.

Tot slot nog het volgende. Het door u gehouden onderzoek en de in uw brief van 19 april jl. vervatte bevindingen en conclusies hebben voornamelijk betrekking op De Connectie, de bedrijfsvoeringorganisatie waaraan de gemeente Arnhem met twee andere gemeenten deelneemt. Uw brief van 19 april jl. is samen met een concept van de onderhavige bestuurlijke reactie van ons college ter kennisneming aan het bestuur van De Connectie gezonden, zodat dat bestuur - indien het dat wenst - nog een reactie kan geven op uw brief van 19 april jl. en/of het uiteindelijke rapport van uw rekenkamer.

Zoals vastgesteld in het college van 8 mei 2018.