Provincie Noord-Holland

POSTBUS 3007 | 2001 DA HAARLEM

Provinciale Staten van Noord-Holland
door tussenkomst van de statengriffier mw. drs. K. Bolt
Dreef 3, tweede etage
2012 HR HAARLEM

Gedeputeerde Staten

Uw contactpersoon
dhr. P. de Ruiter
CZ/CIO

Telefoonnummer +31235143803
ruiterp@noord-holland.nl

Verzenddatum

18 MAART 2021

Kenmerk
1594225 / 1594230

Uw kenmerk

Betreft: Toelichting op informatiebeveiligingsissues bij BIJ12

Geachte leden,

Naar aanleiding van de PS vergadering van 1 februari jongstleden informeren wij u over de beveiliging van de informatiesystemen van BIJ12. BIJ12 werkt als uitvoeringsorganisatie in opdracht van de twaalf provincies. De provincies maken gebruik van gemeenschappelijke applicaties en informatiesystemen die bij BIJ12 zijn ondergebracht. Dit betreft onder andere databanken en registers voor natuurbeheer, monitoring, subsidieverlening, schade-uitkeringen.

In december 2019 heeft BIJ12 op basis van het rapport Advies Informatieveiligheid van ATOS, de ICT-leverancier van BIJ12, mondeling de beveiligingssituatie gedeeld in een overleg van de provinciale Chief Information Security Officers (CISO overleg). Tijdens dit overleg kwamen kwetsbaarheden op de systemen aan het licht, waar BIJ12 direct mee aan de slag is gegaan. De kwetsbaarheden konden relatief snel worden opgelost.

In september 2020 heeft BIJ12 opnieuw een dergelijk rapport gedeeld tijdens een CISO overleg. Het wekte verbazing dat dezelfde kwetsbaarheden op de systemen bij BIJ12 boven water kwamen die eerder als opgelost waren gekwalificeerd. Hierop heeft de provincie Gelderland hun kwetsbaarheden-tool ter beschikking gesteld, waarmee in oktober 2020 een extra scan is uitgevoerd op de netwerkvoorzieningen in beheer van BIJ12. Hieruit kwam naar voren dat de hardware en software van de systemen bij BIJ12 sterk waren verouderd. Er kon op basis van beide rapporten niet anders worden geconcludeerd dan dat het verouderingsproces van de applicaties geleidelijk aan zover was gevorderd, dat het niet langer mogelijk was om de benodigde en actuele beveiligingsmaatregelen te plannen voor de betreffende applicaties. De kwetsbaarheden nemen daardoor snel toe en betreffen situaties waarbij het voor niet-geautoriseerden en/of

Postbus 3007
2001 DA Haarlem
Telefoon (023) 514 3143

Houtplein 33
2012 DE Haarlem
www.noord-holland.nl
Kvk-nummer 34362354
Btw-nummer NL.0010.03.124.B.08

kwaadwillenden mogelijk is om ongeautoriseerde toegang te hebben tot systemen en/of gegevens in te zien. De provinciale CISO's hebben daarop in december 2020 expliciet geadviseerd de systemen off-line te halen. Dit is in januari 2021 ook daadwerkelijk gebeurd.

Een gespecialiseerd bureau heeft onderzocht of de systemen van BIJ12 zijn gecompromitteerd. Dit onderzoek is recentelijk afgerond en er is geen bewijs gevonden dat dit daadwerkelijk het geval is. Hierop is de pro forma melding bij de Autoriteit Persoonsgegevens ingetrokken.

De beveiligingsproblematiek is in feite terug te voeren naar onvoldoende aandacht voor het op peil houden van het benodigde beheer van de informatiesystemen bij BIJ12. Een aantal applicaties kon na verloop van tijd gewoonweg daardoor niet meer worden bijgewerkt met de benodigde en actuele beveiligingsupdates. Dit kwam mede omdat voor betrokkenen niet altijd voldoende helder was wie waarvoor verantwoordelijk was. Ook de applicatievoorzitters bij de provincies hebben achteraf gezien te weinig gestuurd op het onderhoud en de beveiliging.

Op de vraag van uw Staten of het College niet eerder informatie had kunnen verstrekken, het volgende. BIJ12 is een uitvoeringsorganisatie van het IPO en het College is vertegenwoordigd in het bestuur van het IPO. Het College heeft geen eerdere signalen ontvangen anders dan eerder aangegeven in de brief aan Provinciale Staten op 25 januari 2021. Toen de signalen binnenkwamen bij het IPO bestuur is hier zo snel mogelijk op geacteerd.

Nu de informatiesystemen zijn beveiligd, is BIJ12 aan zet om de informatiebeveiliging duurzaam op orde te brengen.

Op dit moment worden de benodigde stappen gezet om de informatiebeveiliging en het beheer en onderhoud structureel te borgen in beheerprocessen, organisatie en governance / besluitvorming. Hierbij wordt aangemerkt dat BIJ12 zich heeft gecommitteerd om in 2023 certificering te bereiken op de informatiebeveiligingsnorm NEN/ISO IEC 27001:2017[1]. De processen die daarvoor moeten worden ingericht, hebben als doel om dit soort problemen te voorkomen.

Het op orde krijgen van de beveiliging van de systemen brengt kosten met zich mee. Alhoewel nog veel onzeker is, worden deze vooralsnog door BIJ12 begroot op maximaal EUR 1,4 mln. Indien dit bedrag via de

[1] De NEN-ISO/IEC 27001-standaard bevat eisen waar het managementsysteem voor informatiebeveiliging aan dient te voldoen. Het is deze norm waartegen wordt geaudit bij certificering. Deze standaard specificeert eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's.

verdeelsleutel aan de provincies wordt doorberekend, impliceert dit voor de provincie een kostenpost van max. circa EUR 120.000 (eenmalig). De financiële consequenties voor de structurele borging van het beheer en onderhoud in beheerprocessen, organisatie en governance / besluitvorming worden na uitvoering hiervan inzichtelijk gemaakt.

In de bijlage treft u het meest recente voortgangsbericht aan van de aanpak van de informatiebeveiliging bij BIJ12.

Hoogachtend,
Gedeputeerde Staten van Noord-Holland,

provinciesecretaris
R.M. Bergkamp

voorzitter
A.Th.H. van Dijk

1 bijlage(n)

Voortgangsbericht beveiliging BIJ12 210211