C2/11

deVolkskrant

de Volkskrant bv
Jacob Bontiusplaats 9
1018 LL Amsterdam
Postbus 1002
1000 BA Amsterdam

Provincie Noord-Holland
t.a.v. Gedeputeerde Staten
Postbus 3007
2001 DA Haarlem

1165351
INGEKOMEN 21 DEC. 2018

Amsterdam, 20 december 2018

Betreft: Indiening Wob-verzoek inzake Black Energy

Geachte heer/mevrouw,

In het Cybersecuritybeeld 2015 worden digitale spionageaanvallen beschreven die Nederlandse bedrijven en vitale infrastructuren of Industrial Control Systems (hierna: ICS) treffen. Specifiek wordt in het rapport het voorbeeld van 'Black Energy' genoemd als malware die ICS, ook wel bekend onder de noemer SCADA-systemen, aanvalt of verkent. Black Energy zou volgens het Cybersecuritybeeld bij verschillende bedrijven zijn aangetroffen. In het kader van een onderzoek van mijn collega [redacted] wil ik namens de Volkskrant bij u informatie hierover opvragen.

De Volkskrant zou graag meer inzicht krijgen in daadwerkelijke registraties van malware als Black Energy in ICS, het beleid ten aanzien van dergelijke malware en maatregelen die zijn genomen om aanvallen te voorkomen.

Met een beroep op de Wet openbaarheid van bestuur (hierna: Wob) verzoek ik u, namens de Volkskrant, om openbaarmaking van hieronder nader te specificeren informatie voor het tijdsvak 2014 tot en met 2018:

1. Kopie van, subsidiair inzage in, documenten betreffende het beleid ten aanzien van malware als Black Energy. Dit omvat informatie over preventiemaatregelen, risicoanalyses over de weerbaarheid van partijen en systemen, nota's over het beleid en documenten over veranderingen in dit beleid. Ook wordt hier gevraagd om informatie over de samenwerkingsverbanden die bestaan tussen de provincie en verschillende partijen, en de rolverdeling binnen die samenwerkingsverbanden, om de (cyber)veiligheid van bedrijven en Industrial Control Systems (ICS) te waarborgen.

2. Kopie van, subsidiair inzage in, een overzicht van de gevallen waar malware als Black Energy in systemen werd vastgesteld. Indien een dergelijk overzicht niet bestaat, dan zou de Volkskrant graag kopieën van brondocumenten, waaronder communicatie, ontvangen waarvan op basis van die documenten zelf een overzicht gemaakt kan worden waaruit blijkt bij welke partij, op welke plaats(en), wat voor soort malware is aangetroffen en, hoe, wanneer en door wie dit verwijderd is met welke kosten.

deVolkskrant

Uiteraard ga ik graag met u in gesprek aangaande de informatie die voorhanden is. Ook als onderdelen van het Wob-verzoek onduidelijk zijn, dan gaat de Volkskrant graag met u in gesprek.

In alle gevallen wordt gevraagd om een kopie van de informatie. U mag de documenten zowel digitaal als op papier doen toekomen. Indien het origineel voorhanden is dan heeft verstrekking in digitale vorm onze voorkeur, voor het overige in de vorm van een papieren kopie. Indien u voornemens bent kosten te berekenen, dan vraag ik u mij vooraf hierover te berichten met een inschatting van de kosten.

Daar waar documenten zich niet onder u bevinden, verzoek ik u zonder oprekken van termijnen doorgeleiding van dit verzoek naar het juiste orgaan. Mocht dat inderdaad gebeuren, dan ontvang ik daar graag een afschrift van.

Voor zover nodig beroep ik mij op de Wet openbaarheid van bestuur. Ik zie uit naar de spoedige overhandiging van de documenten. Deze brief is per post verstuurd op 20 december 2018.

Hoogachtend namens de Volkskrant,

Provincie Noord-Holland

POSTBUS 3007 2001 DA HAARLEM

De Volkskrant bv
T.a.v. [redacted]
Postbus 1002
1000 BA Amsterdam

Gedeputeerde Staten
Uw contactpersoon
[redacted]
CZ/CIO

Telefoonnummer [redacted]
[redacted]@noord-holland.nl

Betreft: Wob verzoek van de Volkskrant om informatie over malware als Black Energy in ICS systemen

Verzenddatum
27 FEB. 2019

Kenmerk
1165351/1178471

Uw kenmerk

Geachte heer [redacted]

Inleiding
Op 21 december 2018 hebben wij uw verzoek ontvangen om openbaarmaking van informatie betreffende registraties van malware als Black Energy in Industrial Control Systems (ICS). De beslistermijn is met vier weken verdaagd bij brief van 24 december 2018 (kenmerk 1165351/1166763) en daarmee bepaald op 15 februari 2019.

Op dinsdag 22 januari 2019 heeft naar aanleiding van uw verzoek een gesprek plaatsgevonden tussen u en drie vertegenwoordigers van de provincie Noord-Holland, waarin u een toelichting heeft gegeven op uw verzoek. Tijdens dit gesprek zijn door u twee uitbreidingen gevraagd op het oorspronkelijke WOB-verzoek:

1) Volgens de definitie van het Ministerie van Justitie en Veiligheid/ Nationaal Coördinator Terrorismebestrijding en Veiligheid, beschreven in de "Factsheet Weerbare Vitale Infrastructuur" van december 2017, is van de 26 vermelde vitale processen alleen het vitale proces "Scheepvaartafwikkeling" van toepassing op de provincie. De domeinen "Tunnelbediening" en "Verkeersmanagement (VM)" vallen binnen geen enkel vitaal proces uit deze factsheet. De definitie voor vitale infrastructuren volgens de Volkskrant is: iets is een vitale infrastructuur, indien falen hiervan leidt tot grote maatschappelijke verstoring. Het verzoek is daarom om het WOB-verzoek uit te breiden met de domeinen "Tunnelbediening" en "Verkeersmanagement"

2) Hoewel het WOB-verzoek specifiek vraagt naar "documenten betreffende het beleid" is de Volkskrant ook geïnteresseerd in een

Postbus 3007
2001 DA Haarlem
Telefoon (023) 514 3143
Fax (023) 514 3030

Houtplein 33
2012 DE Haarlem
www.noord-holland.nl

beschrijving van de bestaande uitvoeringspraktijk, die wellicht nog niet in officiële beleidsdocumenten is beschreven.

Om te kunnen voldoen aan de uitbreidingen op uw oorspronkelijke verzoek, is voorgesteld de uiterste beslistermijn uit te stellen naar 1 maart 2019. Hiermee bent u akkoord gegaan.

Wij geven hieronder uitleg over onze uitvoeringspraktijk en daarna maken wij onze beslissing op uw verzoek om openbaarmaking van informatie inzake Black Energy, kenbaar.

Algemeen - uitvoeringspraktijk
Informatie is één van de voornaamste bedrijfsmiddelen van de provincie Noord-Holland. Het verlies van gegevens, uitval van ICT, objecten of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie of objecten kan ernstige gevolgen hebben voor de primaire taakuitvoering, de bedrijfsvoering en leiden tot verminderd vertrouwen van de burger in de overheid. Daarnaast hebben ernstige incidenten mogelijk negatieve gevolgen voor burgers, bedrijven, partners en de eigen organisatie en de bestuurders ervan. Informatieveiligheid is daarom van groot belang. Informatiebeveiliging is het proces dat dit belang dient. Bovendien hebben we te maken met toenemende digitalisering, ketenafhankelijkheden, nieuwe ICT middelen, nieuwe wetgeving met impact op informatievoorziening en ICT en met tijd - en plaats onafhankelijk werken.

De provincie Noord-Holland is een publieke organisatie waarbij transparantie en integriteit hand in hand gaan. De 'provinciale' informatie behoort openbaar en toegankelijk te zijn, tenzij er wettelijke belemmeringen zijn (privacy, auteursrechten, etc.), concurrentieverhoudingen of het economische of financiële belang van de provincie worden geschaad. De provincie behoort tegelijkertijd prudent om te gaan met de door haar verwerkte en beheerde informatie. Burgers, bedrijven en overheidspartners moeten er te allen tijde op kunnen rekenen dat de informatie goed is beveiligd. Een professioneel uitgevoerde informatiebeveiliging behoort dan ook standaard onderdeel te zijn van de bedrijfsvoering, waar we ons bewust zijn van de risico's en dat we die maatregelen nemen, die we nodig achten. De provincie maakt al deze afwegingen om te komen tot een juiste balans tussen openbaarheid, transparantie en waarborg binnen een professioneel opererende organisatie.

De provincie Noord-Holland beschikt over één verkeerscentrale van waaruit 2 tunnels, een aquaduct, circa 300 verkeersregelinstallaties (VRI's), circa 30 Dynamische Route Informatie Panelen (DRIP's), en circa 200 camera's op afstand worden bediend. Verder beschikt de provincie

over een bediencentrale, waar vandaan straks circa 44 bruggen en sluizen op afstand zullen worden bediend.

De provincie baseert informatiebeveiliging op de door de overheid beschikbaar gestelde kaders (baseline informatiebeveiliging overheid - BIO) onder andere voor het omgaan met malware voor de domeinen Tunnelbediening, Brug- / sluisbediening en Verkeersmanagement. In het afgelopen jaar (vanaf 1 februari 2018 t/m 10 januari 2019) is op de gemonitorde systemen in het Verkeersmanagement domein geen malware aangetroffen. Hierna geven wij daarom de algemene aanpak weer om de weerbaarheid tegenover malware aanvallen te vergroten, verdeeld in de onderwerpen:

1) Algemene weerbaarheidsaanpak voor de drie provincie domeinen
2) Weerbaarheidsaanpak voor domein Tunnelbediening
3) Weerbaarheidsaanpak voor domein Brug- en sluisbediening
4) Weerbaarheidsaanpak voor domein Verkeersmanagement (VM).

Ad 1 - Algemene weerbaarheidsaanpak voor de drie provincie domeinen

1) In 2018 besloot de provincie het team dat verantwoordelijk is voor Information security van de provincie uit te breiden.

2) Tussen Rijkswaterstaat en de provincie is een intentieverklaring getekend om gezamenlijk te verkennen hoe we onze organisaties kunnen beveiligen tegen aanvallen van buitenaf. De provincie werkt samen met Rijkswaterstaat (RWS) en is van plan om alle tunnels, bruggen, sluizen, VRI's, DRIP's en camera's aan te gaan sluiten op hun Security Operations Centre (SOC).

3) Komende jaren wordt extra geïnvesteerd in de security van Industrial Control Systems.

Ad 2 - Weerbaarheidsaanpak voor domein Tunnelbediening

De tunneloperators en bedienaren krijgen een periodieke opleiding om hun kennis rondom Cybersecurity bedreigingen te vergroten.

Daarnaast worden ook proces- , systeem en technische maatregelen genomen om de tunnelsystemen af te schermen tegen mogelijke aanvallen. Bovendien worden er periodieke audits gehouden om te borgen dat deze maatregelen actueel blijven en voldoen.

Ad 3 - Weerbaarheidsaanpak voor domein Brug- en sluisbediening

Voor het project centrale bediening kunstwerken heeft de provincie een samenwerkingsovereenkomst afgesloten met Rijkswaterstaat om de deskundigheid van Rijkswaterstaat in te zetten. Zo zijn er cybersecurity

proces- en systeemeisen geformuleerd die zijn opgenomen in het ontwerp en contract van de centrale bediening.

Daarnaast heeft de aannemer een Cybersecurity Beveiligingsplan opgesteld en krijgen de bedienaren, beheerder en andere medewerkers in de bediencentrale een opleiding in cybersecurity.

De meeste kunstwerken (bruggen en sluizen) van de provincie worden lokaal (ter plekke), door een bedienaar bediend. Voor de bediening van deze kunstwerken wordt momenteel gebruik gemaakt van een SCADA systeem. Niet als hoofdsysteem, maar als ondersteunend systeem voor het bedieningsproces. Dit systeem is niet aan internet gekoppeld en daardoor is er geen mogelijkheid om dit systeem te ontregelen. De bediening, beheer en onderhoud van al deze objecten worden uitgevoerd door gespecialiseerde derden.

Ad 4 - Weerbaarheidsaanpak voor domein VerkeersManagement (VM)

Het Cybersecurity ontwerp van alle nieuwe ICT-systemen in het Verkeersmanagement domein is gebaseerd op de door de overheid beschikbaar gestelde informatiebeveiligingskaders en is binnen de provincie vertaald naar diverse Zakboekjes Informatiebeveiliging.

Er is een Gestandaardiseerde ITIL (Information Technology Infrastructure Library) Change Management procedure voor het gecontroleerd doorvoeren van wijzigingen aan ICT systemen. In geval van wijzigingen in de ICT infrastructuur, dienen projectleiders/ uitvoerders zich te houden aan voorgeschreven processen en technologieën.

Er is een voorgeschreven proces om autorisaties / rechten te verschaffen aan gebruikers en processen om applicaties en diensten binnen het DVM Areaal te kunnen gebruiken.

Er is een patch beleid dat beschrijft welke ICT-componenten van het VM domein hoe vaak voorzien moeten worden van software updates, en op basis van welke triggers.

Er wordt gebruik gemaakt van anti virus- en anti malware software en deze zal dit jaar ook voorzien worden van een Intrusion Protection Module.

Er zijn firewalls voor interne en externe compartimentering.

Er is een geformaliseerd ITIL proces voor afhandelen van alle typen incidenten (inclusief security incidenten).

Er is geld beschikbaar om periodiek penetratietesten te laten uitvoeren in het VM domein of externe audits te laten uitvoeren op de kwaliteit van de Cybersecurity maatregelen.

Ten aanzien van uw verzoek d.d. 21 december 2018
Ad 1 Wij hebben alle documenten die binnen de reikwijdte van uw verzoek vallen geïnventariseerd en op een inventarislijst (zie bijlage) vermeld. Deze documenten hebben wij getoetst aan de Wet openbaarheid van bestuur (Wob). Zoals op de inventarislijst is aangegeven, zullen wij een aantal documenten in geanonimiseerde vorm en daar waar nodig onleesbaar gemaakt, openbaar maken via publicatie op onze website www.noord-holland.nl/wob. De overige documenten worden niet openbaar gemaakt. In de inventarislijst is aangegeven om welke documenten het gaat. Hieronder treft u onze motivering aan om deze documenten niet openbaar te maken met een beroep op de in de inventarislijst genoemde artikelen uit de Wob.
Ad. 2 Wij beschikken niet over overzichten van gevallen waarin malware als Black Energy in systemen werd vastgesteld.

Artikel 10, eerste lid, sub b, Wob - schaden veiligheid staat
Documenten worden niet openbaar gemaakt, omdat hierdoor de veiligheid van de staat wordt geschaad. Als de provincie deze documenten openbaar zou maken, kan zij een makkelijk(er) doelwit worden voor kwaadwillenden. Hiermee zou inzicht kunnen worden verkregen in het weerstandniveau en de mate van beveiliging van provinciale systemen.

Artikel 10, tweede lid, sub e, Wob - eerbiediging persoonlijke levenssfeer
Documenten worden niet openbaar gemaakt, omdat hierdoor de privacy van personen in het geding komt. Om die reden zijn persoonsgegevens van natuurlijke personen (niet zijnde bestuurders of andere publieke figuren) weggelakt.

Artikel 10, tweede lid onder g, Wob - onevenredige benadeling betrokken derden
Informatie van door de provincie ingehuurde bedrijven wordt niet openbaar gemaakt, omdat hierdoor inzicht wordt gegeven in de werkwijze en (mate van bescherming van) systemen van die derden. Zij kunnen daardoor onevenredig benadeeld worden. Het belang dat deze bedrijven geen nadeel ondervinden van openbaarmaking van de door hun verstrekte informatie, weegt naar onze mening zwaarder dan het belang van openbaarmaking ervan.

Afsluiting

Binnen enkele dagen na verzending van dit besluit treft u de stukken met uw verzoek en deze beslissing (eveneens in geanonimiseerde vorm) aan op onze website, www.noord-holland.nl/wob.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd. Mocht u naar aanleiding van dit besluit en de openbare documenten nog vragen hebben kunt u contact opnemen met de behandelend ambtenaar.

Hoogachtend,
Gedeputeerde Staten van Noord-Holland,

[redacted]

provinciesecretaris
R.M. Bergkamp

voorzitter
A.Th.H. van Dijk

1 bijlagen
Inventarislijst

Bezwaar
Als u belanghebbende bent kunt u binnen zes weken na de verzending, uitreiking of publicatie van dit besluit schriftelijk bezwaar aantekenen. Het bezwaarschrift kunt u sturen aan Gedeputeerde Staten van Noord-Holland, ter attentie van de secretaris van de Hoor- en adviescommissie, Postbus 3007, 2001 DA Haarlem.
Voor meer informatie kunt u de provinciale website bezoeken: www.noord-holland.nl.

Wij willen bezwaren tegen besluiten graag op informele wijze behandelen. Als uw bezwaar in aanmerking komt voor deze informele behandeling nemen wij op korte termijn telefonisch contact met u op. In verband hiermee verzoeken wij u om in uw bezwaarschrift het telefoonnummer te vermelden waarop u overdag bereikbaar bent.

Bovenstaand besluit treedt in werking, ook al wordt een bezwaarschrift ingediend. Gelijktijdig met het indienen van een bezwaarschrift kunt u – bij een spoedeisend belang - een voorlopige voorziening vragen bij de Voorzitter van de Rechtbank Noord-Holland.

Provincie Noord-Holland

POSTBUS 3007 | 2001 DA HAARLEM

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

Gedeputeerde Staten

Uw contactpersoon

[redacted]

CZ/CIO

Telefoonnummer [redacted]

[redacted]@noord-holland.nl

Verzenddatum

27 FEB. 2019

Kenmerk

1165351/1178122

Uw kenmerk

Betreft: Wobverzoek van de Volkskrant inzake Black Energy

Geachte leden,

Ter uitvoering van artikel 167, tweede lid, van de Provinciewet (inzake de actieve informatieplicht) informeren wij u over het volgende.

Op 21 december 2018 hebben wij een verzoek om informatie in het kader van de Wet openbaarheid van bestuur ontvangen betreffende openbaarmaking van informatie inzake registraties van malware als Black Energy in Industrial Control Systems (ICS).

Onze beslissing op dit verzoek zal met het verzoek en de openbare informatie in geanonimiseerde vorm gepubliceerd worden via www.noord-holland.nl/Wob.

Vertrouwende u hiermee voldoende geïnformeerd te hebben,

Hoogachtend,

Gedeputeerde Staten van Noord-Holland,

[redacted]

provinciesecretaris
R.M. Bergkamp

voorzitter
A.Th.H. van Dijk

Postbus 3007
2001 DA Haarlem
Telefoon (023) 514 3143

Dreef 3
2012 HR Haarlem
www.noord-holland.nl
Kvk nummer 34362354
Btw nummer NL.0010.03.124.B.08

Inventarislijst behorende bij Wob-dossier van de Volkskrant inzake Black Energy kenmerk 1165351

	Datum	Kenmerk	Omschrijving	Reeds openbaar: Ja (vindplaats) / Nee	Openbaar te maken: Ja / Nee / N.v.t.	Weigeringsgrond Wob
1	14-12-18	Baseline Informatiebeveiliging Overheid		https://zoek.officielebekendmakingen.nl/kst-26643-574.html	n.v.t.	
2	19-04-17	Governance - Wie doet wat bij informatiebeveiliging		Nee	Ja	Voor afgeschermde delen: art 10 lid 2 onder e
3	29-11-17	IB-Zakboekje 'Eigenaarschap van ICT-systemen en -verwerkingen'		Nee	Ja	Voor afgeschermde delen: art 10 lid 2 onder e
4	13-07-17	IB-Zakboekje 'Classificatie'		Nee	Ja	Voor afgeschermde delen: art 10 lid 2 onder e
5	23-03-17	IB-Zakboekje 'Werkplek'		Nee	Ja	Voor afgeschermde delen: art 10 lid 2 onder e
6	15-06-17	IB-Zakboekje 'Identiteiten, Rollen en Rechten'		Nee	Ja	Voor afgeschermde delen: art 10 lid 2 onder e
7	28-07-15	Identiteits en autorisatie management PNH Verkeerscentrale	Manier waarop accountbeheer, authenticatie, autorisatie en accounting plaatsvinden binnen het VM-domein	Nee	Nee	art. 10, lid 1, onder b.
8	11-04-17	Cyber security plan Abdijtunnel	Adressering van de eisen uit het contract op het gebied van cybersecurity.	Nee	Nee	art 10, lid 1, onder b.
9	20-04-18	Offerteaanvraag	Offerteaanvraag met betrekking tot (aanvullende) cybersecuritymaatregelen voor de Abdijtunnel	Nee	Ja, gedeeltelijk	Art 10, lid 2 onder g; voor afgeschermde delen: art 10 lid 2 onder e.
10	20-04-18	Gewijzigde offerte cybersecurity Abdij tunnel	Offerte met betrekking tot cybersecuritymaatregelen voor de Abdijtunnel	Nee	Nee	art 10, lid 1, onder b, alsmede art 10, lid 2 onder g.
11	04-05-17	Bijlage A,PNH Abdijtunnel (Bevindingen-Risico's-Advies-Prioritering)	Prioritering van de diverse cybersecuritymaatregelen.	Nee	Nee	art 10, lid 1, onder b.
12	17-05-16	Cybersecurity implementatierichtlijn PNH		https://www.tenderned.nl/tenderned-tap/aankondigingen/143104;section=2	n.v.t.	
13	14-06-16	Richtlijnen cybersecurity PNH		https://www.tenderned.nl/tenderned-tap/aankondigingen/143104;section=2	n.v.t.	
14	17-05-16	Template beveiligingsplan		https://www.tenderned.nl/tenderned-tap/aankondigingen/143104;section=2	n.v.t.	
15	11-09-17	Proces-beschrijving Acces management	Proces om autorisaties / rechten te verschaffen aan gebruikers en processen om applicaties en diensten binnen het VM domein te kunnen gebruiken	Nee	Nee	art 10, lid 1, onder b.
16	16-10-17	Storingsafhandeling-Bwise	Geformaliseerd ITIL (Information Technology Infrastructure Library) proces voor afhandelen van alle typen incidenten (inclusief Security incidenten) binnen het VM domein	Nee	Nee	art 10, lid 1, onder b.
17	17-10-17	Storingsafhandeling overig-Bwise.rtf	Geformaliseerd ITIL proces voor afhandelen van alle typen incidenten (inclusief Security incidenten) binnen het VM domein; overig	Nee	Nee	art 10, lid 1, onder b.
18	31-10-17	Patch beleid ICT Infrastructuur Verkeerscentrale	Aan te passen ICT-componenten van het VM domein, trigger-bronnen en frequentie voor het uitrollen van software updates	Nee	Nee	art 10, lid 1, onder b.
19	2018-onbekend	Applicatie Koppelvlakken Overview	Beveiligingsarchitectuur en beveiligingsregels van de firewalls in het VM domein	Nee	Nee	art 10, lid 1, onder b.
20	20-04-18	GS Themaberaad Informatie-beveiliging en cybersecurity	"hoog-over" beschrijving cybersecurity van de domeinen Tunnelbediening, brugbediening, verkeersmanagement, met voorstellen voor verbetering cybersecurity	Nee	Nee	art 10, lid 1, onder b.
21	21-05-18	Nota GS staf Cybersecurity Bruggen Sluizen Tunnels VRIs	Detailbeschrijving over informatiebeveiliging van de 3 domeinen.	Nee	Nee	art 10, lid 1, onder b.
22	25-06-18	1074883-1074899 Kaderbrief 2019 PS	Over meerjaren investeringsbudgetten voor verbetering cybersecurity van de 3 domeinen	Nee	Nee	art 10, lid 1, onder b.
23	27-08-18	DVM Beheer Technical Requirements (Internal)	Voorgeschreven processen en technologieën voor het VM domein	Nee	Nee	art 10, lid 1, onder b.
24	20-09-18	PNH SIM3 rapportage vertrouwelijk.pdf	Score op Security Incident Management proces voor de 3 domeinen	Nee	Nee	art 10, lid 1, onder b.
25	19-11-18	DVM Beheer Technical Requirements (SaaS).docx	Voor wijzigingen en projecten: voorgeschreven processen en technologieën in het VM domein (in geval van hosting bij een externe partij)	Nee	Nee	art 10, lid 1, onder b.
26	29-11-18	Procesbeschrijving Changemanagement	Gestandaardiseerde ITIL werkwijze voor het gecontroleerd doorvoeren van wijzigingen aan ICT systemen in het VM domein	Nee	Nee	art 10, lid 1, onder b.
27	31-05-18	Cybersecurity beveiligingsplan 24-uurs bediencentrale	Beschrijving van geimplementeerde beveiligingsmaatregelen ten gunste van de systemen t.b.v. de bediening, bewaking en besturing van de 24-uurs bediencentrale PNH Heerhugowaard, inclusief alle hierop aangesloten kunstwerken	Nee	Nee	art 10, lid 1, onder b.