provincie ZUID HOLLAND

**Gedeputeerde Staten**
Afdeling Bestuur
Bureau Beleidscoördinatie en Advies
Contact
[redacted]

Postadres Provinciehuis
Postbus 90602
2509 LP Den Haag
T 070 - 441 66 11
www.zuid-holland.nl

de Volkskrant B.V.
t.a.v. de heer [redacted]
Postbus 1002
1000 BA Amsterdam

Datum
Zie verzenddatum linksonder
Ons kenmerk
PZH-2019-687321032
DOS-2018-0009277
Uw kenmerk

Bijlagen
diversen

Onderwerp
Wob bezwaarschrift tegen besluit van 8 februari 2019
inzake Black Energy

Geachte heer [redacted],

Op 21 december 2018 hebben wij uw verzoek ontvangen, waarin u met een beroep op de Wet openbaarheid van bestuur (Wob) informatie vraagt over registraties van malware als Black Energy in Industrial Control Systems (ICS) en het beleid ten aanzien van dergelijke malware en maatregelen die zijn genomen om aanvallen te voorkomen over het tijdvak 2014 tot en met 2018. U vraagt naar beleidsdocumenten ten aanzien van malware, informatie over preventiemaatregelen, risico-analyses over de weerbaarheid van partijen en systemen, nota's over het beleid en documenten over veranderingen in dit beleid.

Wij hebben uw verzoek bij brief van 8 februari 2019 beantwoord. Tegen de wijze van beantwoording heeft u op 19 februari jl. een bezwaarschrift ingediend.
In uw bezwaarschrift stelt u dat wij onvoldoende hebben onderbouwd waarom is gekozen voor een integrale weigering van het delen van documenten, waarbij u overigens het belang van beveiliging, namelijk de gevoeligheid van het delen van informatie in documenten als risicoanalyses, niet betwist.

Naar aanleiding van uw bezwaarschrift bent u uitgenodigd voor een gesprek om te bezien in hoeverre wij aan uw bezwaren tegemoet kunnen komen. Dit gesprek heeft op maandag 11 maart jl. plaatsgevonden op het provinciehuis te Den Haag. Bij dit gesprek waren van de zijde van de provincie aanwezig mevrouw [redacted] en de heren [redacted] en [redacted].
Tijdens dit gesprek heeft u uw verzoek en uw bezwaarschrift nader toegelicht. Vervolgens is met u afgesproken dat wij nagaan op welke wijze wij zoveel als mogelijk en op een voor de provincie verantwoorde wijze inzicht kunnen verstrekken in het veiligheidsbeleid en hoe de provincie daaraan uitvoering geeft. Dit doen wij, zoals door u tijdens dit gesprek gevraagd, op een zo concreet mogelijke wijze, eventueel voorzien van een toelichting, en voor zover mogelijk met

Bezoekadres
Zuid-Hollandplein 1
2596 AW Den Haag

Tram 9 en de buslijnen 90, 385 en 386 stoppen dichtbij het provinciehuis. Vanaf station Den Haag CS is het tien minuten lopen. De parkeerruimte voor auto's is beperkt.

(enkele) documenten of een lijst met documenten die bestaan, maar op grond van veiligheidsoverwegingen niet gedeeld kunnen worden.

Onderstaande beantwoording is in aanvulling op onze eerdere brief van 8 februari 2019. Allereerst wijzen wij u erop dat de Wob voorziet in het openbaar maken van bestaande documenten, voor zover die al niet openbaar zijn. De Wob strekt er niet toe op aanvraag nieuwe documenten te maken, te bewerken of van een toelichting of verantwoording te voorzien. Maar zoals in het gesprek op 11 maart jl. aangegeven zijn wij bereid daar waar mogelijk een toelichting te geven per onderwerp. De bezwarenclausule onderaan de brief is niet van toepassing op de toelichting.

Na archiefonderzoek geven wij u de volgende beantwoording door het geven van een toelichting op en inzicht in bestaande documenten. Waar mogelijk maken wij documenten (gedeeltelijk) openbaar. De beantwoording heeft betrekking op de volgende onderwerpen:

- Convenant, baseline en beleid informatieveiligheid
- Sluiscomplexen die onder het begrip vitale infrastructuur vallen
- Het ICS-netwerk en het verkeersmanagementsysteem, waarmee verkeerslichten en dynamische route informatiepanelen (DRIPs) en verkeerscamera's worden aangestuurd
- Het systeem voor centrale objectbediening, waarmee de bruggen op afstand worden bediend
- De aansturing van pompen en gemalen.

**1. Convenant, baseline en beleid informatieveiligheid**

Op 13 november 2014 is het 'Convenant interprovinciale regulering informatieveiligheid' vastgesteld door het bestuur van het Interprovinciaal Overleg (IPO). Op 10 februari 2015 is het convenant ook door ons vastgesteld. In het convenant wordt verwezen naar de Interprovinciale Baseline voor Informatieveiligheid. Deze is gebaseerd op de ISO/IEC27000 serie. Ook het Rijk en de gemeenten hebben op basis van deze normen een Baseline opgesteld. Kort geleden zijn deze gezamenlijk ondergebracht in het BIO (Baseline Informatiebeveiliging Overheden). Op 16 juli 2014 is op hoog ambtelijk niveau van de provincie het informatiebeveiligingsbeleid 2014-2018 vastgesteld.

<u>Documenten:</u>

Onderstaande documenten maken wij openbaar:

- *Convenant Interprovinciale Regulering Informatieveiligheid,* september 2014. Zie bijlage.
- *Beleid informatieveiligheid Provincie Zuid-Holland 2014-2018*, 16 juli 2014. Zie bijlage.
- *Interprovinciale Baseline Informatieveiligheid 2.0,* 3 mei 2016. Zie bijlage.

**2. Sluiscomplexen**

De provinciale assets worden op vier sluiscomplexen na niet aangemerkt als vitale infrastructuur op basis van de Wet gegevensbescherming en meldplicht cybersecurity. De sluizen zijn niet verbonden met het internet en bediening op afstand is niet mogelijk. De bediening (middels PLC-besturing) vindt alleen op locatie plaats door geautoriseerd personeel. De fysieke beveiliging van de toegang tot provinciale locaties is georganiseerd via een centraal systeem en beschreven in

procedures. Opdrachtnemers en eigen personeel kunnen tijdelijk en onder toezicht toegang tot de locaties krijgen. Opdrachtnemers krijgen slechts toegang nadat zij een cursus hebben gevolgd.

**3. ICS netwerk en verkeersmanagementsysteem**

Verschillende partijen hebben (als gebruiker, netwerkbeheerderof softwareleverancier) toegang tot het provinciale ICS-netwerk, waarop het verkeersmanagementsysteem en het cameramanagementsysteem draaien. Voordat een partij toegang krijgt tot het ICS-netwerk, wordt een initiële audit uitgevoerd. Tweejaarlijks wordt een volgende audit uitgevoerd. De provincie geeft daarbij periodiek (2016, 2018) opdracht aan gerenommeerde marktpartijen om te toetsen of de softwareleveranciers en netwerkbeheerders voldoen aan de gestelde beveiligingsvereisten. Een belangrijke aangesloten partner is de Regiodesk van BEREIK! Dit is een samenwerkingsplatform voor wegbeheerders. Deze organisatie verzorgt de coördinatie op het gebied van verkeersmanagement en heeft als doel het bereikbaar houden van Zuid-Holland, nu en in de toekomst. Ook Rijkswaterstaat, de Metropoolregio Rotterdam- Den Haag, de gemeenten Rotterdam en Den Haag en het Havenbedrijf Rotterdam zijn hierbij aangesloten. De taken worden onder meer uitgevoerd vanuit de verkeerscentrale in Rhoon.

Samenwerkende partijen (gebruikers)

De provincie Zuid-Holland maakt voor het uitvoeren van verkeersmanagement gebruik van twee systemen: een verkeersmanagementsysteem en een cameramanagementsysteem. Het verkeersmanagementsysteem is samen met de gemeente Den Haag in beheer genomen. Daarvoor is een beheerorganisatie opgezet en een samenwerkingsovereenkomst gesloten, waarin ook informatiebeveiliging wordt benoemd. Op dit systeem zijn ook de verkeerslichten en Dynamische Route Informatiepanelen (DRIPs) van een tiental gemeenten aangesloten. Op het cameramanagementsysteem zijn ook camera's van enkele andere gemeenten aangesloten. Met die gemeenten zijn samenwerkingsovereenkomsten gesloten, waarin de toelatingsvereisten en beveiligingsmaatregelen worden benoemd. De door de provincie verlangde beveiligings-maatregelen zijn gebaseerd op de Interprovinciale Baseline Informatieveiligheid (en de daaraan ten grondslag liggende ISO27002 norm voor informatiebeveiliging).

Netwerkbeheerders en software leveranciers

Voor het beheer en onderhoud van het ICS-netwerk is een beheerkwaliteitsplan opgesteld en in een dossier afspraken en procedures (DAP) is de werkwijze voor dagelijkse monitoring en netwerkbeheer vastgelegd.

DBI is gecertificeerd voor Assetmanagement. Vanuit die werkprocedures wordt er driemaandelijks een risicosessie gehouden. De beschikbaarheid van systemen is één van de meest kritische parameters. Cyber security is één van de te beheersen risico's. Door het treffen van voldoende maatregelen worden de risico's beperkt tot een aanvaardbaar niveau.

Voor het ICS-netwerk zijn maatregelpakketten voor de beveiliging van het ICS-netwerk geformuleerd. Deze maken onderdeel uit van de contracten met leveranciers en netwerkbeheerders. Hierin zijn de beveiligingseisen geformuleerd die aan de leveranciers en beheerders worden gesteld.

Documenten

Het volgende document maken wij (gedeeltelijk) openbaar:

- *Samenwerkingsovereenkomst standaard 2.0.* Zie bijlage
  Dit betreft het model van de samenwerkingsovereenkomsten met aangesloten gemeenten. In Bijlage 3 van deze overeenkomst maken wij het onderdeel 'Maatregelen' niet openbaar. Voor de weigeringsgrond verwijzen wij u naar de onderaan deze brief opgenomen motivering van ons beroep op de uitzonderingsgronden van de Wob

De volgende documenten maken wij niet openbaar, op grond van veiligheidsoverwegingen. Deze documenten bevatten de concrete beveiligingsmaatregelen en beheerafspraken die de provincie vraagt van haar leveranciers en van de samenwerkende partijen die toegang krijgen op het provinciale ICS netwerk:

- Uitgevoerde Business Impact analyses:
  - *BIA Verkeerscentrale (januari 2013)*
  - *BIA VMS-systemen (januari 2016) v1.0*
- *Beveiligingseisen PZH-VMS-netwerk Provincie Zuid Holland,* december 2015
- Audit- en toetsingsdocumenten:
  - *20160325 Eindrapportage informatieveiligheid DVM-wegen v1.01,* 2016
  - *Rapport Cyber Security Audit PZH-VMS-netwerk,* 2018
  - *Cyber Security audit PZH ketenpartners Verkeersmanagement netwerk*, 2018
- Het beheerplan en het dossier afspraken en procedures voor het beveiligde netwerk voor de verkeerssystemen:
  - *Beheerkwaliteitsplan 21012015*, 21 jan 2015.
  - *DAP Beveiligd netwerk definitief v1 4*, 14 aug 2015
- Diverse documenten ten aanzien van de risicobeheersing van het assetmanagement. Sinds september 2017 wordt een risicodossier bijgehouden voor assetmanagement, waarin informatiebeveiliging een onderdeel is

Voor de weigeringsgrond verwijzen wij u naar de onderaan deze brief opgenomen motivering van ons beroep op de uitzonderingsgronden van de Wob.

**4. Centraal Objectbedieningssysteem**

De afgelopen tien jaar worden steeds meer bruggen niet meer lokaal maar op afstand bediend vanuit centrales. De bruggen zijn met dedicated glasvezelkabels verbonden met de bediencentrales. De centrales zijn ook onderling met elkaar verbonden.

Aan de hand van gedetailleerde risicoanalyses en de eisen voortvloeiend uit de ISO-norm, zijn maatregelen getroffen op organisatorisch, technisch en procedureel vlak. Zodanig dat de geïdentificeerde risico's zijn gereduceerd tot een acceptabel niveau.

Een adviesbureau heeft de provincie geadviseerd om de grote hoeveelheid policies (werkafspraken) en procedures te borgen in een Cyber Security Management Systeem.

Documenten
De volgende documenten maken wij niet openbaar op grond van veiligheidsoverwegingen. Deze documenten bevatten de concrete beveiligingsmaatregelen en beheerafspraken in relatie tot centrale objectbediening:

- *PZH Cyber Security Management Systeem– B03*, 2018
- Documenten ten aanzien van risicobeheersing objectbediening:
    - *Toegangsverlening Objecten DBI 20151009*, 2015
    - *Quick Scan informatiebeveiliging COB*, 2018

Voor de weigeringsgrond verwijzen wij u naar de onderaan deze brief opgenomen motivering van ons beroep op de uitzonderingsgronden van de Wob.

**5. De aansturing van pompen en gemalen**
Het beheer en onderhoud van het ICS-systeem voor de bediening op afstand van pompen en gemalen is opgedragen aan een gespecialiseerd bedrijf. In een document dat is getoetst door een andere marktpartij is aangegeven op welke wijze invulling is gegeven aan de Interprovinciale Baseline Informatieveiligheid. Via een applicatie kan de provincie toegang verkrijgen tot het systeem.

Documenten
Het volgende document maken we niet openbaar op grond van veiligheidsoverwegingen. Dit document bevat de concrete beveiligingsmaatregelen en beheerafspraken in relatie tot de aansturing van pompen en gemalen:

- *2016-03-08 Implementatie beveiligingsmaatregelen leverancier Pomptechniek*, 8 maart 2016.

**Motivering weigeringsgronden onder punten 3, 4 en 5**
Voor alle bovengenoemde documenten die wij (gedeeltelijk) niet openbaar maken, geldt het volgende. De inhoud van de documenten heeft betrekking op de wijze waarop wij uitvoering geven aan ons beleid omtrent informatieveiligheid van onze systemen als bedoeld onder de punten 3, 4 en 5. Niet alleen de wijze waarop dit wordt uitgevoerd is van belang, maar ook de mate van gedetailleerdheid, en daarmee de gevoeligheid en kwetsbaarheid, daarvan is voor ons bepalend om andere personen dan die door ons specifiek zijn aangewezen, hierover geen informatie te verstrekken. Informatieveiligheid is voor ons van essentieel belang om onze systemen optimaal te kunnen laten functioneren en het functioneren daarvan is uiteraard ook belang voor onze omgeving, te weten de (weg)gebruikers c.q. inwoners van de provincie. Het betreft documenten die onze bedrijfsvoering rechtstreeks raken en in het geval van openbaarmaking zelfs in gevaar kan brengen. Naast bovenstaande motivering benadrukken wij, dat alle documenten in samenhang met elkaar zelfs een extra risico voor de provinciale bedrijfsvoering oplevert en mogelijk ook voor onze samenwerkingspartners.

Daarnaast kan openbaarmaking van bovengenoemde documenten onze financiële of economische belangen schaden, omdat wij, bij mogelijke oneigenlijke inmenging van buitenaf in onze systemen, genoodzaakt zijn direct maatregelen te treffen om te voorkomen dat onze bedrijfsvoering in gevaar komt. Het nemen van extra maatregelen heeft gevolgen voor onze

financiële positie. Wij achten het financiële of economische belang van de provincie zwaarder wegen dan het belang van openbaarheid voor een ieder. Voorts kunnen derden door het openbaar maken van de informatie hiermee mogelijk hun voordeel doen en kunnen derden bovendien de informatie gebruiken voor andere doeleindenals gevolg waarvan de positie van de provincie mogelijk wordt benadeeld. Ook kunnen door de openbaarmaking van de betreffende documenten de partners waarmee wij een (samenwerkings)overeenkomst hebben gesloten ten behoeve van de uitvoering van ons veiligheidsbeleid, ernstig worden benadeeld. Deze benadeling kan eveneens mede bestaan uit de financiële gevolgen voor de door hen te treffen noodzakelijke maatregelen. Wij achten het belang van onevenredige bevoordeling of benadeling van derden zwaarder wegen dan het belang van openbaarheid voor een ieder.

Gelet op vorenstaande doen wij een beroep op artikel 10, lid 1, onder b van de Wob. Voor zover deze uitzonderingsgrond in rechte geen stand houdt, doen wij tevens een beroep op artikel 10, lid 2, onder b en g van de Wob.

Voorts merken wij voor de goede orde op, dat wij in een enkel document enkele persoonlijke gegevens onleesbaar hebben gemaakt, zoals namen van ambtenaren en derden, parafen en handtekeningen, vanwege de bescherming van de persoonlijke levenssfeerals bedoeld in artikel 10, lid 2, onder e van de Wob. Dit doet overigens niets af aan de inhoud van de door u gevraagde informatie.

**Tot slot**
Graag vernemen wij van u of bovenstaande voldoende tegemoet komt aan uw vraag om informatie zoals door u tijdens het gesprek van 11 maart jl. is toegelicht. Mocht u nog vragen hebben dan geven wij u in overweging deze nader te stellen. Dit kunt u doen doorcontact op te nemen met de personen rechts bovenaan in deze brief.
Mocht bovenstaande nadere toelichting met de daarbij behorende documenten die wij hierbij openbaar maken, voor u aanleiding zijn uw bezwaarschrift in te trekken dan vernemen wij dit eveneens graag van u.

Wij verzoeken u in uw correspondentie altijd het DOS-nummer te vermelden dat wij rechts bovenaan in deze brief hebben opgenomen.

Hoogachtend,

Gedeputeerde Staten van Zuid-Holland,
voor dezen,

Hoofd Beleidscoördinatie en Advies
*Deze brief is digitaal vastgesteld, hierdoor staat er geen fysieke handtekening in de brief.*

Tegen dit besluit kunnen belanghebbenden ingevolge artikel 7:1 van de Algemene wet bestuursrecht bij ons een gemotiveerd bezwaarschrift indienen. Dit bezwaarschrift dient binnen zes weken na de dag van verzending of uitreiking van het besluit te worden toegezonden, onder vermelding van “Awb-bezwaar” in de linkerbovenhoek van enveloppe en bezwaarschrift. Het bezwaar moet worden gericht aan: Gedeputeerde Staten van Zuid-Holland, t.a.v. het Awb-secretariaat, Postbus 90602, 2509 LP Den Haag.

Bijlagen:

- Convenant Interprovinciale Regulering Informatieveiligheid, september 2014.
- Het document Beleid informatieveiligheid Provincie Zuid-Holland 2014-2018.
- Interprovinciale Baseline Informatieveiligheid 2.0, 3 mei 2016.
- De samenwerkingsovereenkomsten met aangesloten gemeenten; bijgaand de template die gebruikt is voor alle aangesloten gemeenten.