provinciehuis Westerbrink 1, Assen
postadres Postbus 122, 9400 AC Assen

www.drenthe.nl
0592 - 36 55 55

provincie Drenthe

Aan:
de Volkskrant
[redacted]
Postbus 1002
1000 BA AMSTERDAM

Assen,13 februari 2019
Ons kenmerk 7/5.2/2019000432
Behandeld door [redacted] (0592) 36 55 55
Onderwerp: Besluit Wob-verzoek

Geachte [redacted],

In uw brief van 20 december 2018, door ons ontvangen op 21 december 2018, hebt u met een beroep op de Wet openbaarheid van bestuur (Wob) een verzoek om informatie ingediend over het beleid ten aanzien van malware als Black Energy en een overzicht van de gevallen waar malware als Black Energy in systemen werd vastgesteld.

Procedure
De ontvangst van uw verzoek is schriftelijk bevestigd bij brief van 8 januari 2019. Tevens is de beslistermijn in deze brief met vier weken verdaagd.

Besluit
Op uw verzoek hebben wij als volgt besloten. Hierbij vindt u de documenten die onder de reikwijdte van uw verzoek vallen. Dit met inachtneming van artikel 10, tweede lid, aanhef en onder e, van de Wob. Op grond van artikel 10, tweede lid, aanhef en onder e, van de Wob blijft verstrekking van informatie achterwege voor zover het belang daarvan niet opweegt tegen het belang van eerbiediging van de persoonlijke levenssfeer. Ambtenaren en andere bij de besluitvorming betrokken personen kunnen in hun beroepshalve functioneren niet altijd ten volle een beroep doen op de persoonlijke levenssfeer.

Volgens vaste jurisprudentie kan wel een beroep op de persoonlijke levenssfeer worden gedaan als het gaat om gegevens als namen, telefoonnummers en e-mailadressen van ambtenaren of personen van andere organisaties. Namen en andere naar een persoon herleidbare gegevens zijn immers persoonsgegevens en het belang van eerbiediging van de persoonlijke levenssfeer kan zich tegen het openbaar maken van deze informatie verzetten. Uitgangspunt hierbij is dat van openbaarmaking wordt

afgezien voor zover het gaat om ambtenaren en derden die niet uit hoofde van hun functie in de openbaarheid treden.

Leidinggevenden en bestuurders treden volgens ons uit hoofde van hun functie in de openbaarheid. De namen van deze functionarissen zijn derhalve zichtbaar. Volgens ons weegt de persoonlijke levenssfeer van de andere betrokkenen zwaarder dan het publieke belang van openbaarmaking van deze informatie. In alle documenten zijn de persoonsgegevens, te weten namen, tot personen herleidbare functienamen, telefoonnummers en e-mailadressen van deze personen daarom onleesbaar gemaakt.

Het weglakken van gegevens die de persoonlijke levenssfeer raken is voor zover mogelijk op een dusdanige manier gebeurd dat herleidbaar is om welk type gegevens het gaat.

Afbakening en relevantie voor de provincie Drenthe
De provincie Drenthe gebruikt ICS/Scada-systemen voor de bediening van objecten zoals bruggen, sluizen. De vaarwegen worden hoofdzakelijk recreatief gebruikt, de beroepsvaart is gering in omvang. De provincie Drenthe werkt nauw samen met de provincie Groningen. De afspraken zijn vastgelegd in bijgaande samenwerkingsovereenkomst. De provincie Groningen geeft op basis hiervan uitvoering aan het beheer van de ICS/Scada-systemen van de provincie Drenthe. Zodoende hebben wij verder hierover geen informatie beschikbaar.

Om uw vragen te beantwoorden is hieronder aangeven op welke wijze de provincie Drenthe risico's, zoals malware mitigeert.

Risico's en Beveiligingsvuistregels
De provincie Drenthe hanteert informatiebeveiligingsbeleid, gebaseerd op de ISO 27002 norm, in de periode 2014-2018 in de vorm van de IBI (internetverwijzing) hetgeen verder verankerd is in provinciaal informatiebeveiligingsbeleid. Dit beleid wordt zo nodig periodiek bijgesteld. Wij doen u hierbij dit beleid toekomen.

De risico's van de objecten door de ICS/Scada-systemen betreffen de continuïteit van de bedrijfsvoering, veiligheid (safety) en informatiebeveiliging. Uw WOB-verzoek betreft met name de informatiebeveiligingsrisico's. De provincie Drenthe hanteert hieromtrent bestendige gedragslijnen om risico's te mitigeren:

Beveiliging door Handbediening
Voor de objecten geldt de vuistregel dat zij altijd handmatig bediend kunnen worden in geval van nood. Zodoende kan een digitale aanval op een object altijd binnen redelijke termijn teniet worden gedaan door middel van een manuele ingreep.

Beveiliging door 'los gekoppelde autonome systemen'
De objecten dienen standaard voorzien te zijn van diverse elektrotechnische en mechanische veiligheidsmaatregelen die onafhankelijk van elkaar en autonoom functioneren. Hierdoor wordt impliciet voorkomen dat bijvoorbeeld slagbomen te vroeg of juist te laat openen en dat bruggen automatisch sluiten als andere systemen niet functioneren etc. Het compartimenteren van de systemen bevordert de veilige werking van het geheel en beperkt eveneens de impact van een digitale aanval op andere systemen.

Beveiliging door dedicated lines/dark fiber
Voor alle (digitale) verbindingen met de objecten geldt de vuistregel dat verbindingen alleen gerealiseerd worden middels een gesloten netwerk. Dat betekent dat er alleen gebruik gemaakt wordt van dedicated lines dan wel in het geval van glasvezel 'dark fiber'.

Beveiliging door ontkoppeling van 'het internet' en 'stepping stone toegang'
De besturingssystemen van de bruggen en sluizen zijn niet aangesloten op het internet, er is geen standaard koppeling met het reguliere kantoor-netwerk van de provincie. Daarmee is het aanvalsvlak voor een hack op afstand zeer gering. Alleen voor het beheren van systemen op afstand in het kader van onderhoud kan alleen na toestemming een verbinding tijdelijk 'open gezet' worden door de provincie. Hiervoor gelden procedures omtrent autorisatie vooraf alsmede de controle van de verrichting achteraf.

Beveiliging door proven 'technology'
De provincie Drenthe plaatst objecten met een lange levensduur, waarbij uitgegaan wordt van minimaal vijftig jaar. Dat betekent dat het functioneren van het object in dat tijdsperspectief wordt beoordeeld hetgeen de facto inhoudt dat er gebruik gemaakt wordt van bewezen robuuste technologie ('proven technology'). Daarmee worden risicovolle implementaties voorkomen.

Beveiliging door verankering/'hardening'
De systemen worden zodanig ingericht dat alleen die functies die nodig zijn beschikbaar zijn en alle andere niet relevante functies worden afgesloten. Een voorbeeld hiervan is het sluiten van niet gebruikte poorten in een firewall.

Beveiliging door segmentering
Het is de vuistregel om berichtenverkeer met verschillende functies van elkaar te scheiden. Derhalve wordt het netwerkverkeer ten behoeve van ICS/Scada door middel van segmentering gescheiden van het andere netwerkverkeer.

Beveiliging door autorisaties in combinatie met tussentijdse authenticatie
Naast de reguliere autorisaties vooraf en controle hierop hanteert de provincie Drenthe de lijn dat bij structurele wijziging van de object-programmering (verankerd in de PLC's) stelselmatig de gebruiker zich dient te authentiseren. Het authenticatieregime sluit aan op de hoogte van het gepercipieerde risico.

Risico Analyses en Samenwerking
De provincie Groningen voert in opdracht van de provincie Drenthe werkzaamheden uit aan de ICS/Scada-systemen. De provincie Groningen heeft, in samenwerking met Rijkswaterstaat, in de genoemde periode een risicoanalyse uitgevoerd op de ICS/Scada-systemen. In de daarop volgende verbetercyclus zijn de toepasselijke maatregelen ook getroffen voor de configuratie van de provincie Drenthe. Wij zien dit als uitvoering en deze documenten berusten daarom niet bij ons. Omdat u ook een gelijkluidend verzoek heeft gedaan bij de provincie Groningen, verwijzen wij kortheidshalve naar de besluitvorming aldaar.

ICS/ Malware Black Energy incidenten
De provincie Drenthe registreert alle incidenten ten aanzien van de dienstverlening conform de ITIL-proces methode, zodat zij ook een volledig beeld heeft van incidenten zoals malware. Uit analyse van onze data blijkt dat de provincie Drenthe niet is aangevallen door malware zoals Black energy etc.

Toezending documenten
Het document 'Samenwerkingsovereenkomst Groningen-Drenthe en ons informatiebeveiligingsbeleid treft u als bijlage aan. Een dag na bekendmaking van dit besluit aan u zullen de documenten op de provinciale website voor een ieder openbaar worden gemaakt.

Mocht u naar aanleiding hiervan verdere vragen hebben dan kunt u contact opnemen met [redacted] telefoonnummer (0592) 36 55 55.

Hoogachtend,

Gedeputeerde Staten van Drenthe,

, secretaris

, voorzitter

Bijlagen:
- Samenwerkingsovereenkomst Groningen-Drenthe
- Informatiebeveiligingsbeleid

km/coll.

Bezwaar
Bent u het niet eens met dit besluit, dan kunt u binnen zes weken na de dag van verzending ervan hiertegen een bezwaarschrift indienen bij het college van Gedeputeerde Staten van Drenthe. De dag van verzending is de dagtekening van het besluit. Voor meer informatie over het indienen van een bezwaarschrift verwijzen wij u naar http://www.provincie.drenthe.nl/loket/bezwaarschriften.