Bezoekadres De Blomboogerd 1, 4003 BX Tiel
Postadres Postbus 599, 4000 AN Tiel
T (0344) 64 90 90 **F** (0344) 64 90 99
E info@wsrl.nl **I** www.waterschaprivierenland.nl
Bank IBAN NL93NWAB0636757269
BIC NWABNL2G

Waterschap Rivierenland

Fractie 50PLUS Waterschap Rivierenland
t.a.v. de heer J. Opschoor

Datum:	Uw kenmerk:	Ons kenmerk:	Behandeld door:
27 juni 2019		2019069709/2019081205	H.T.M. Peterse

Onderwerp:
Antwoord vragen ex artikel 4.5. RvO over cybercriminaliteit

Doorkiesnummer / e-mail:
(0344) 64 91 50
h.peterse@wsrl.nl

Geachte heer Opschoor,

In uw brief d.d. 20 mei stelt u vragen over cybercriminaliteit.
In onderstaande beantwoording zijn de vragen opgenomen en voorzien van een antwoord.

1) Wat zijn de stappen die het Waterschap onderneemt om voorbereid te zijn op deze aanvallen.
Antwoord: Waterschap Rivierenland is zich bewust van de verschillende dreigingen door digitale criminaliteit. Wij zijn constant bezig om onze beveiliging te verbeteren. Hiervoor is een programmatische aanpak gestart voor het verbeteren van de digitale weerbaarheid van het waterschap. Binnen dit programma worden de onderwerpen fysieke beveiliging, informatiebeveiliging en privacy in onderlinge samenhang opgepakt.

2) Is het Waterschap opgewassen tegen aanvallen van buitenaf.
Antwoord: De geavanceerde beveiligingsmiddelen die ingezet zijn, voorkomen dat aanvallen van buitenaf effect hebben op de uitvoering van ons werk. Echter 100% zekerheid is niet te geven omdat de ontwikkelingen op dit gebied elkaar snel opvolgen.

3) Zijn er al cyberaanvallen geweest op het netwerk van het Waterschap.
Antwoord: Uit de rapportages is op te maken dat er in het verleden pogingen zijn gedaan om ons netwerk aan te vallen. Alle aanvallen van buitenaf zijn door onze firewall onderschept. Wekelijks worden er meer dan 50.000 pogingen gedaan om digitaal binnen te komen. Geen van deze pogingen om binnen te komen zijn gelukt of hebben schade kunnen aanbrengen.

4) Hoe is de staat op dit moment van het digitale netwerk waar onderdelen van het watersysteem en keten mee worden bestuurd en zijn er back-up systemen?
Antwoord: Het netwerk waar onderdelen van watersysteem en waterketen mee worden bestuurd is gescheiden van het kantoornetwerk en objecten zijn niet aan het internet verbonden. Momenteel wordt er hard gewerkt om het netwerk op te knippen in kleine clusters zodat bij een eventuele inbraak of storing de impact tot één cluster beperkt blijft. De systemen voor de bediening van het watersysteem zijn redundant uitgevoerd en watersysteemobjecten kunnen in geval van nood met het lokale systeem of eventueel nog met de hand worden bediend. Voor de systemen van de zuiveringen zijn reservesystemen op voorraad. Ook hier kan bij een eventuele verstoring van de centrale aansturing vanuit de CRK, lokaal op een zuivering de installatie bediend worden.

Wij verzoeken u vriendelijk bij verdere correspondentie ons kenmerk te vermelden, zodat wij uw brief sneller kunnen beantwoorden.

5) Zijn er in de afgelopen periode kwetsbaarheidstesten uitgevoerd, en wat was hiervan het resultaat.
Antwoord: Er zijn in het verleden meerdere kwetsbaarheidstesten uitgevoerd. Na elke test zijn leer- en verbeterpunten opgemaakt en zijn verbeteringen projectmatig doorgevoerd dan wel opgenomen in het eerdergenoemde verbeterprogramma. Bij de laatste test is met name opgevallen dat houding en gedrag van medewerkers ten aanzien van beveiliging een aandachtspunt is Hiervoor zal een awareness-programma worden gestart. Daarnaast is uit de kwetsbaarheidstesten naar voren gekomen dat de fysieke beveiliging een aandachtspunt is. Ook hiervoor worden een aantal maatregelen getroffen.

6) Hoe vaak wordt de beveiliging software van de digitale systemen geüpdatet.
Antwoord: De beveiligingssoftware wordt continu geüpdatet. Ook het updaten van het operating system op onze servers gebeurt automatisch. De meeste mobiele apparaten worden op afstand beheerd. Systemen die van de buitenwereld zijn afgeschermd worden minder periodiek geüpdatet.

7) Hoe is de samenwerking tussen de verschillende Waterschappen en Gemeenten is er sprake van een uniform beleid, en is er contact met de veiligheidsdiensten.
Antwoord: Waterschap Rivierenland werkt met de andere waterschappen samen binnen Het Waterschapshuis en is aangesloten op het CERT-WM (Computer Emergency Response Team WaterManagement). Ook werken we samen met andere waterschappen, Rijkswaterstaat en het Nationaal Cyber Security Centrum van het Ministerie van Justitie en Veiligheid via de ISAC Keren & Beheren (Information Sharing and Analysis Center).

Voor alle overheden is de BIO (Baseline Informatiebeveiliging Overheden) in december 2018 vastgesteld. Deze moet eind 2020 zijn geïmplementeerd. Op grond van eerder genoemd verbeterprogramma verwacht Waterschap Rivierenland deze termijn niet te halen. Op dit moment wordt geïnventariseerd welke extra inspanning nodig is om deze termijn wel te halen. Hierover zult u separaat worden geïnformeerd.

Wij hopen u hiermee voldoende inzicht te hebben gegeven in de getroffen en nog te treffen maatregelen ter voorkoming van verstoring van vitale bedrijfsonderdelen.

Hoogachtend,
het college van dijkgraaf en heemraden
van Waterschap Rivierenland,
de secretaris-directeur,

ir. Z.C. Vonk

de dijkgraaf,

prof. dr. J.C. Verdaas

Bijlagen:
Afschrift: Archief (inclusief bijlagen)