UNIE VAN WATERSCHAPPEN

BEZOEKADRES
Koningskade 40
2596 AA Den Haag
070 351 97 51
Nederland

POSTADRES
Postbus 93218
2509 AE Den Haag
Nederland

Onderzoeksraad voor Veiligheid
t.a.v. de heer ir. J. Dijsselbloem (voorzitter)
Postbus 95404
2509 CK Den Haag

datum	ons kenmerk	contactpersoon
14 april 2022	117886/EG	mw. N. de Keijzer
bijlage(n)	**uw kenmerk**	**e-mail**
-	-	nkeijzer@uvw.nl

betreft
Reactie waterschappen op rapport Kwetsbaar door software

Geachte heer Dijsselbloem,

Op 16 december 2021 heeft u het rapport *"Kwetsbaar door software – Lessen naar aanleiding van beveiligingslekken door software van Citrix"* gepubliceerd. Onlangs hebben wij uw rapport in onze Commissie Bestuurszaken, Communicatie en Financiën (CBCF) met de waterschappen besproken. Hierbij wil ik u graag informeren over de reactie van de waterschappen op uw rapport.

De waterschappen herkennen de toenemende afhankelijkheid van een goed functionerende ICT-infrastructuur en -dienstverlening. Dit maakt de waterschappen in potentie kwetsbaar voor aanvallen van buitenaf (cybercrime). Steeds meer objecten van waterschappen worden geautomatiseerd en op afstand gemonitord en bestuurd, zoals gemalen, rioolwaterzuiveringsinrichtingen, sluizen, stuwen en bruggen. Informatieveiligheid is voor waterschappen van groot belang om de vitale belangen - droge voeten, schoon en voldoende water - te waarborgen. Het onderwerp staat bij de waterschappen dan ook hoog op de (bestuurlijke) agenda en door de huidige ontwikkelingen in de wereld wordt het belang van informatieveiligheid nog eens extra onderstreept.

De waterschappen hebben als sector deze verantwoordelijk opgepakt door sinds 2013 een gezamenlijk programma Informatieveiligheid vorm te geven en uit te voeren. Een belangrijk resultaat van dit programma was het per 1-1-2017 aansluiten van alle waterschappen op het Computer Emergency Response Team Watermanagement (CERT-WM), een team dat samen met Rijkswaterstaat gespecialiseerd is in het ontdekken, onderzoeken en afslaan van cyberaanvallen. Daarnaast zijn de waterschappen aangesloten bij het Information Sharing and Analysis Centre (ISAC) Keren en Beheren, een publiek-private samenwerking waarin informatie en ervaringen over cybersecurity worden uitgewisseld.
Begin 2020 is het CERT-WM officieel aangewezen als essentieel voor het Landelijk Dekkend Stelsel, waardoor intensievere informatie-uitwisseling tussen het CERT-WM en het NCSC mogelijk is geworden. Recent heeft dit zijn meerwaarde weer bewezen bij de kwetsbaarheid in Apache Log4J. Vanuit onze ervaringen met het CERT-WM onderschrijven de waterschappen dan ook de aanbeveling van de Onderzoeksraad om potentiële slachtoffers van cyberaanvallen gevraagd en ongevraagd te waarschuwen voor geconstateerde kwetsbaarheden en maatregelen te delen om de digitale veiligheid te borgen.

De komende maanden onderzoeken de waterschappen de doorontwikkeling van de dienstverlening van het CERT-WM naar een gemeenschappelijk Security Operations Center (SOC). Het doel van een gemeenschappelijke SOC is een centrale en proactieve rol te spelen bij het detecteren van cyberdreigingen en te zorgen dat de aangesloten waterschappen snel gealarmeerd worden.

Tegelijk met het sectorbrede programma Informatieveiligheid hebben de waterschappen in 2013 de Baseline informatiebeveiliging waterschappen (BIWA) vastgesteld. Hierin staan maatregelen die algemeen voorkomende informatiebeveiligingsrisico's bij de waterschappen afdekken. In 2018 is de sectorspecifieke BIWA vervangen door de Baseline Informatiebeveiliging Overheid (BIO), het overheidsbrede, uniforme en eenduidige kader voor informatieveiligheid. De waterschappen hebben gezamenlijk afgesproken om aan de BIO te voldoen op volwassenheidsniveau 4, wat betekent dat op basis van risicoanalyse aanvullende maatregelen zijn genomen in een cyclus van voortdurende verbetering. De waterschappen worden regelmatig door een gecertificeerd extern bureau geaudit op de mate waarin de BIO en Algemene Verordening Gegevensbescherming (AVG) is geïmplementeerd en op de werking van de PDCA-cyclus (Plan-Do-Check-Act). De verbeterpunten die hieruit naar voren komen, worden door de waterschappen als zeer waardevol ervaren. Daarnaast toetsen de waterschappen hun digitale weerbaarheid door regelmatig cyberoefeningen te houden.

De waterschappen werken dus ieder voor zich en gezamenlijk als sector al hard aan hun digitale weerbaarheid. Ze beseffen echter goed dat ze het niet meer alleen kunnen. Grote softwareleveranciers zoals Microsoft voor de kantoorautomatisering en leveranciers van de industriële computers (PLC's), bedieningssystemen, besturingssoftware (SCADA/ICS) en communicatienetwerken zijn lastig door de waterschappen te beïnvloeden. Cyberoefeningen worden steeds vaker samen met andere overheden gehouden, denk aan ISIDOOR van het NCSC en de overheidsbrede cyberoefening van het ministerie van BZK. Bovendien merken de waterschappen dat alle maatregelen op het gebied van informatieveiligheid steeds meer geld en schaarse capaciteit kosten. Ze zijn dan ook verheugd over de aanbeveling van de Onderzoeksraad om het onderwerp gezamenlijk op te pakken, in Nederland en in Europa.

De waterschappen constateren wel dat de samenwerking met andere overheden nog heel versnipperd plaatsvindt. De minister van Justitie en Veiligheid is coördinerend bewindspersoon voor cybersecurity, verantwoordelijk voor het NCSC en voert regie op de uitvoering van de Nationale Cybersecurity Agenda.
Het ministerie van IenW is verantwoordelijk voor de informatieveiligheid binnen de watersector. Bij cyberincidenten en -crises is er contact met het Departementaal Coördinatiecentrum Crisisbeheersing (DCC) en bij het ministerie van IenW loopt het programma Versterken Cyberweerbaarheid in de watersector waarbij we als waterschappen samen met onze ketenpartners (o.a. Rijkswaterstaat) aan onze digitale weerbaarheid werken.
Het ministerie van BZK richt zich op de overheidsbrede digitale weerbaarheid. De Baseline Informatiebeveiliging Overheid (BIO) wordt daar beheerd, er is een overheidsbrede werkgroep Informatiebeveiliging Overheid voor het delen van kennis en bij cyberincidenten en -crises legt het ministerie van BZK verantwoording af namens de gehele overheid. Daarnaast is cybersecurity een speerpunt van het ministerie van EZK in de zin van digitale weerbaarheid van ondernemers en informatieveiligheidseisen richting marktpartijen. Onze verwachting is dat we meer met het ministerie van EZK zullen gaan samenwerken bijvoorbeeld in het kader van het formuleren en afdwingen van veiligheidseisen bij fabrikanten.
Het kost de waterschappen veel tijd en energie om met de vier verschillende ministeries goed samen te werken. Zodoende willen we hierbij graag een oproep doen voor meer coördinatie op Informatieveiligheid binnen de Nederlandse overheid zodat we onderwerpen als ketenaansprakelijkheid gezamenlijk het hoofd kunnen gaan bieden.

Tot slot constateren we dat het ministerie van BZK al de eerste stappen aan het zetten is met betrekking tot uw advies om een wettelijke basis te creëren voor de beheersing van digitale veiligheid en het op eenduidige wijze afleggen van verantwoording over de manier waarop digitale veiligheidsrisico's worden beheerst. De waterschappen steunen deze ontwikkeling en zijn hierbij goed aangehaakt.

Mocht u naar aanleiding van bovenstaande reactie van de waterschappen op uw rapport *Kwetsbaar door software* nog vragen of opmerkingen hebben, dan kunt u contact opnemen met Nicole de Keijzer (nkeijzer@uvw.nl / 06-82013186).

Met vriendelijke groet,

Rogier van der Sande,
voorzitter Unie van Waterschappen.