Handreiking voor waterschap-bestuurders

Aanvulling op het document “De 10 bestuurlijke principes voor informatiebeveiliging” voor waterschap bestuurders en directieleden

Auteur: Coenraad Doeser

Programmamanager van het Programma Informatieveiligheid en Privacy van Het Waterschapshuis

Voorwoord

Met onderstaand schrijven bieden wij u een verdieping -geënt op de specifieke situatie van waterschappen- op het document ‘10 bestuurlijke principes voor informatiebeveiliging’ van de VNG. Het document van de VNG is een goede handreiking voor bestuurders. De principes zijn net zo toepasbaar voor de waterschappen. Daar waar de term *gemeentelijke bestuurders* staat is dat inwisselbaar voor directieleden en/of leden van een DB of AB van een waterschap.

Aanvulling op ‘Informatiebeveiliging en de gemeentelijke bestuurder”

Net als gemeenten wisselen waterschappen allerlei informatie uit met inwoners, ondernemers, ketenpartners en medeoverheden. In ICT-termen noemen we dat kantoorautomatisering. Maar bij waterschappen komt nog een ander belangrijk aspect om de hoek kijken. Waterschappen maken namelijk gebruik van digitaal verkeer voor de aansturing van hun primaire processen. Dit wordt ook wel procesautomatisering of industriële automatisering genoemd. Bij gemeenten is dit doorgaans van ondergeschikt belang, bij waterschappen is deze procesautomatisering randvoorwaardelijk om het werk goed te kunnen doen. Neem het aansturen van gemalen, stuwen, sluizen en afwaterzuiveringen of neem het verkrijgen van stuurinformatie uit een netwerk van digitale watermeters: zonder procesautomatisering is dit niet meer mogelijk. Tegelijkertijd brengt verdere automatisering risico’s met zich mee en maakt dit de waterschappen extra kwetsbaar.

- ✓ Weet u in hoeverre uw waterschap kwetsbaar is op dit terrein? En welke maatregelen er worden genoemd om de weerbaarheid hiervan te verhogen?
- ✓ Is er een gedegen ‘fall back’ scenario, mocht de procesautomatisering uitvallen?
- ✓ Is daarmee geoefend?

<u>Normen en regels</u>

De BIO norm is de Baseline Informatiebeveiliging Overheid en geldt overheidsbreed, dus ook voor waterschappen. Bij de wijze van verantwoorden zit een verschil tussen gemeenten en waterschappen. Gemeenten gebruiken daarvoor een zelfevaluatie (ENSIA). Bij de waterschappen wordt er op de geregelde tijden een landelijke audit uitgevoerd onder regie van het programma Informatieveiligheid en privacy van Het Waterschapshuis. Als waterschappen geven we hier de voorkeur aan omdat daarmee de onafhankelijkheid is verzekerd.

Aanvulling op principe 1 'Bestuurders bevorderen een veilige cultuur'

ICT-systemen zijn niet alleen kwetsbaar geworden voor digitale aanvallen van buitenaf, maar ook voor ontwrichtende zaken van binnenuit. Uit onderzoeken blijkt dat meer dan de helft van de beveiligingsincidenten van binnenuit optreden, vanuit onwetendheid of vanuit kwaadwillendheid. Denk aan zaken als het lekken van data vanuit onoplettendheid, tot aan kwaadaardige acties van ex-werknemers die nog geautoriseerd bleken te zijn.

- ✓ In hoeverre is er een veilige cultuur binnen uw waterschap?

Aanvulling op principe 3 'Informatiebeveiliging is risicomanagement'

Zonder risicomanagement is het voor de organisatie moeilijk te bepalen of men de goede dingen doet. De kans is dan groot dat informatie en informatiesystemen te licht of te zwaar beveiligd worden.

Binnen de waterschappen is al vroeg onderkend dat risicomanagement van evident belang is om de juiste beslissing te kunnen nemen. Daarom hebben de waterschappen in de Commissie Bestuurszaken, Communicatie en Financiën (CBCF) in mei 2014 afgesproken[1] dat de informatieveiligheid van alle waterschappen voor 2020 aan volwassenheidsniveau vier (op schaal van vijf) dient te voldoen. Volwassenheidsniveau vier onderscheidt zich van de lagere niveaus door expliciet risicomanagement te benoemen. Een organisatie die voldoet aan dit niveau heeft zijn PDCA (Plan Do Check Act) volledig in de lijn geïmplementeerd en de informatiebeveiliging wordt risico-gebaseerd en proactief opgepakt. Het denken vanuit risico's zit dan in de haarvaten van de organisatie. Volwassenheidsniveau vier sluit perfect aan op de BIO en Algemene verordening gegevensbescherming (AVG) waarin risicomanagement een centraal uitgangspunt is.

In aanvulling op het besluit van 2014 is door de CBCF in 2020 besloten ook voor privacybescherming (AVG) volwassenheidsniveau vier als ambitieniveau te nemen.

Ter informatie: de uitkomst van de drie landelijke audits -gehouden tussen 2017 en 2020- was dat de waterschappen qua volwassenheid zich tussen de twee (**Herhaalbaar**: verbetering verloopt projectmatig) en drie (**Gedefinieerd:** vastgelegde processen) bevinden. Waterschappen zitten niet meer op het ad-hoc niveau (niveau 1). Hierbij is getoetst op 'opzet' en 'bestaan' en (nog) niet op 'werking'.

- ✓ Weet u met welk volwassenheidsniveau uw waterschap volgens het laatste audit rapport is beoordeeld?

Aanvulling op principe 4 'Risicomanagement is onderdeel van de besluitvorming'

- ✓ Ziet u risicomanagement is chefsache?
- ✓ Worden risico overwegingen, al dan niet geaggregeerd, besproken op bestuurlijk niveau binnen uw waterschap?

[1] zie vergaderstuk CBCF, bijlage WIV 14-32

Aanvulling op principe 5 'Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking'
Een uitval van een object, bijvoorbeeld een gemaal of van een netwerk van watermeters, kan een kleine impact kan hebben op de processen van het waterschap, maar een grote impact hebben in de gehele waterketen. Dit wetende, plus het feit dat kennis van informatieveiligheid schaars is en daarom tot samenwerking dwingt, heeft er voor gezorgd dat de handen in de waterketen ineen zijn geslagen. In 2018 hebben de waterschappen, samen met andere overheidslagen, het addendum op het Bestuursakkoord Water ondertekend. Cybersecurity is hier een integraal onderdeel van. De afspraken uit het addendum zijn geconcretiseerd in een samenwerkingsprogramma *Versterken Cyberweerbaarheid in de Watersector* onder regie van het ministerie van IenW. De waterschappen nemen actief deel aan dit programma. In debatten in de Tweede kamer[2] wordt menigmaal verwezen naar dit programma.

Aanvulling op principe 7 'Informatiebeveiliging kost geld'
De Cyber Security Raad[3] adviseert de uitgaven aan IT-beveiliging op te schroeven naar 10 procent van het IT-budget. Bij banken is dit zelfs 20%.

- ✓ Weet u welk deel van het ICT-budget aan informatieveiligheid opgaat?

Aanvulling op principe 8 'Onzekerheid dient te worden ingecalculeerd'

- ✓ Hoe goed lopen de informatielijnen binnen uw waterschap?
- ✓ Wordt u geïnformeerd over de uitslagen van pentesten ?
- ✓ Wordt u geïnformeerd over de lessons-learned uit de crisisoefeningen met een cyber-component?

Aanvulling op principe 9 'Verbetering komt voort uit leren en ervaring'

- ✓ Zijn cyberincidenten een onderdeel van de oefeningen die binnen de crisisorganisatie worden gedaan?
- ✓ Weet u of de risico's en kwetsbaarheden van de systemen middels testen worden onderzocht? Wordt de samenvatting hiervan op bestuurlijk niveau besproken?

Aanvulling op principe 10 'Het bestuur controleert en evalueert'
Bij de waterschappen wordt er geregeld een landelijke audit uitgevoerd onder regie van het programma Informatieveiligheid en privacy van Het Waterschapshuis. Deze audit wordt bij alle

[2] Bijvoorbeeld Kamerbrief Versterken Cyberweerbaarheid in de Watersector van 4 november 2020
[3] De Cyber Security Raad (CSR) is een nationaal en onafhankelijk adviesorgaan van het kabinet en bedrijfsleven (via het kabinet) en is samengesteld uit hooggeplaatste vertegenwoordigers van publieke en private organisaties en de wetenschap. De CSR zet zich op strategisch niveau in om de cybersecurity in Nederland te verhogen.

waterschappen door een onafhankelijk audit instantie uitgevoerd. Waterschappen krijgen een individueel rapport met de uitkomsten. De volgende audits hebben plaats gevonden of staan in de planning:

Uitgevoerd:

- 2017 audit op BIWA (voorganger van BIO) in opzet en bestaan
- 2018 audit op privacy / AVG in opzet en bestaan
- 2020 audit specifiek op procesautomatisering in opzet en bestaan. Toetsingskader is de BIO

In de planning:

- 2021/2022: integraal audit op BIO en AVG op opzet en bestaan, uitgaande van volwassenheidsniveau 3
- 2022/2023: integraal audit op BIO en AVG op opzet, bestaan en werking, uitgaande van volwassenheidsniveau 4

- ✓ Heeft u kennis genomen van de uitslagen van de audit-rapporten van uw waterschap?
- ✓ Weet u of het audit rapport tot acties heeft geleid?

In de AVG is wettelijk vastgelegd dat bestuurders een verantwoordelijkheid hebben in het nemen om passende maatregelen te treffen om persoonsgegevens te beveiligen en af te schermen van onbevoegden. De Autoriteit Persoonsgegevens (AP) heeft ruime sanctiebevoegdheden toegekend gekregen in de AVG. Een boete kan oplopen tot maximaal € 20 miljoen of 4% van de wereldwijde jaarlijkse omzet van een organisatie. Hier bovenop kan ook een persoonlijke boete opgelegd worden aan bestuurders van de organisatie.

Los van wel of geen boete, elk incident kan reputatie en imago schade opleveren voor het individuele waterschap of de waterschapsector als geheel.