Handreiking voor waterschap-bestuurders

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

Auteur: Programma Informatieveiligheid en Privacy van Het Waterschapshuis

Voorwoord

Met onderstaand schrijven bieden wij u een praktische verdieping op het document '10 bestuurlijke principes voor informatiebeveiliging' van de VNG[1], maar dan geënt op de specifieke situatie van waterschappen. Het document van de VNG is een uitstekende handreiking voor bestuurders voor zowel gemeentes, als ook waterschappen. Daar waar "Gemeentelijke bestuurders" staat is dat inwisselbaar voor directieleden en/of leden van een DB of AB van een waterschap.

Aanvulling op het hoofdstuk 'Informatiebeveiliging en de gemeentelijke bestuurder"

Net als gemeentes 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 gemeentes is dit doorgaans van ondergeschikt belang. Bij waterschappen is deze procesautomatisering randvoorwaardelijk om hun werk te kunnen doen. Neem het aansturen van afwaterzuiveringen, gemalen, stuwen en sluizen of neem het verkrijgen van stuurinformatie uit een netwerk van digitale watermeters: zonder procesautomatisering is dit niet meer mogelijk. Tegelijkertijd maakt dit de waterschappen ook extra kwetsbaar.

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

Kaders en verantwoording

Als kader voor informatieveiligheid hanteren de waterschappen de BIO. De BIO is een norm die overheidsbreed wordt gehanteerd en gebaseerd is op de internationale standaard ISO 27001. Voor specifiek procesautomatisering gebruiken de waterschappen de CSIR als richtlijn. Tenslotte, voor privacy geldt de AVG. Binnen de EU is sinds 25 mei 2018 één privacywet geldig, namelijk de Algemene verordening gegevensbescherming.

De wijze van verantwoorden gebeurt verschillend per overheidslaag. Zo gebruiken de gemeentes 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 hWh.

Aanvulling op het hoofdstuk 1 'Bestuurders bevorderen een veilige cultuur'

ICT-systemen zijn niet alleen kwetsbaar geworden voor digitale aanvallen van buitenaf, maar des te meer voor ontwrichtende zaken van binnenuit. Uit onderzoeken blijkt dat meer dan de helft van de

[1] https://www.informatiebeveiligingsdienst.nl/product/de-10-bestuurlijke-principes-voor-informatiebeveiliging

beveiligingsincidenten van binnenuit op treden, vanuit onwetendheid of vanuit kwaadwillendheid. Denk aan zaken als datalekken tot aan ex-werknemers die nog beschikt over autorisaties die zaken kunnen saboteren. Kortom, nog een waarom een veilige cultuur van zo'n belang is

> In hoeverre is er een veilige cultuur binnen uw waterschap?

Aanvulling op het hoofdstuk 3 'Informatiebeveiliging is risicomanagement'

Binnen de waterschappen is al vroeg onderkend dat risicomanagement van evident belang is om de juiste beslissingen te kunnen nemen. Immers, zonder risicomanagement is niet te bepalen of informatie en informatiesystemen te licht of te zwaar worden beveiligd. Daarom de waterschappen binnen Unie van Waterschappenverband in mei 2014 met elkaar afgesproken[2] dat de informatieveiligheid van alle waterschappen binnen enkele jaren aan volwassenheidsniveau 4 (op schaal van 5) voldoet, omdat vanaf dit niveau de continu borging het uitgangspunt is en risicomanagement expliciet aandacht krijgt. In 2020 is besloten ook voor privacybescherming (AVG) volwassenheidsniveau 4 als ambitieniveau te nemen.

In volwassenheidsniveau 4 wordt uitgegaan van een kwaliteitsbenadering. De PDCA (Plan Do Check Act) is hierbij volledig in de lijn geïmplementeerd en informatiebeveiliging wordt risico-gebaseerd en proactief opgepakt. Dat sluit perfect aan op de BIO en AVG waarin risicomanagement een centraal uitgangspunt is. Om risicomanagement te laten slagen dient het denken vanuit risico's een plek te krijgen in de haarvaten van de organisatie. Volwassenheidsniveau 4 impliceert dat.

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

Aanvulling op het hoofdstuk 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?

Aanvulling op het hoofdstuk 5 'Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking

In 2018 hebben de waterschappers, samen met andere overheidslagen, het addendum op het Bestuursakkoord Water ondertekent. Cybersecurity maakt een integraal onderdeel hiervan. Hiermee is de opgave van een informatieveilig waterschap verbreed tot ketenniveau. Immers, een uitval van een gemaal kan misschien kleine impact hebben op de processen van het waterschap, maar een grote impact hebben in de gehele waterketen.

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

De afspraken uit het addendum zijn geconcretiseerd in een samenwerkingsprogramma Cybersecurity. De waterschappen nemen actief deel aan dit programma en de activiteiten die daaruit gevolgd zijn.

Aanvulling op hoofdstuk 7 'Informatiebeveiliging kost geld'

Het advies van Cyber Security Raad[3] al om 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 hoofdstuk 8 'Onzekerheid dient te worden ingecalculeerd'

> Hoe goed lopen de informatielijnen binnen uw waterschap?
>
> Wordt u geïnformeerd over de uitslagen van pentesten[4]?
>
> Wordt u geïnformeerd over de lessons-learned uit de crisisoefeningen met een cyber-component?

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

> Worden in de oefeningen die binnen crisisorganisatie worden gedaan ook cyberincidenten meegenomen?
>
> Weet u of er regelmatig middels testen de risico's en kwetsbaarheden van de systemen van het waterschap worden onderzocht? Wordt de samenvatting hiervan op bestuurlijk niveau besproken?

Aanvulling op hoofdstuk 10 'Het bestuur controleert en evalueert'

Bij de waterschappen wordt er op de geregelde tijden een landelijke audit uitgevoerd onder regie van het programma Informatieveiligheid en privacy van hWh. Deze audit wordt bij alle waterschappen en 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:

---

[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.

[4] Pentest is een afkorting van 'penetration testing'. Bij een pentest kruipen pentesters in de huid van een hacker. Ze proberen op allerlei manieren en met alle mogelijke middelen toegang te krijgen tot de geteste IT-omgeving. Op die manier leggen ze de zwakke plekken van je website, applicatie of zelfs gehele IT-infrastructuur bloot. Na afloop van een pentest kun je met gerichte maatregelen deze kwetsbaarheden zo goed mogelijk verhelpen.

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

In de planning:

- 2023/2024: 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?

Over eindverantwoordelijkheid van het bestuur doet de AVG een uitspraak. Wettelijk is in de AVG 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.