Hoogheemraadschap van Rijnland

Notulen
Beeld-VV Informatieveiligheid

Datum: 3 april 2024 uur, 19:05 - 20:30 uur
Plaats: VV-zaal Leiden
Verslag: Mevr. R. Lubbers, Vi.a.Vi Office Management

Aanwezigen:
Dhr. R.A.M. van de Sande (dijkgraaf)
Dhr. J.B. Knapp (hoogheemraad)
Dhr. J.G.M. Schouffoer (hoogheemraad)
Dhr. A.G. Straathof (hoogheemraad)
Mevr. M.R. Verkleij-Lemmers (hoogheemraad)
Dhr. J.P. de Vries (hoogheemraad)
Dhr. H.J. van Egmond (BBB)
Dhr. H. Hazenoot (BBB)
Dhr. J. van Pareren (BBB)
Dhr. H.C.M. Kortman (VVD)
Dhr. J.L. van Oeveren (VVD)
Mevr. S.F. Jahan (VVD)
Dhr. W.H.B. van Dunné (PvdA)
Dhr. J.A. de Ridder (PvdA)
Mevr. A.V. Baerveldt (Water Natuurlijk)
Dhr. K. Buskermolen (Water Natuurlijk)
Dhr. E. van Dijk (Water Natuurlijk)
Dhr. M.J. Minnee (Water Natuurlijk)
Dhr. H. van der Kaap (PvdD)
Dhr. H.A.M. Koenders (PvdD)
Dhr. J.A. Stenfert Kroese (PvdD)
Dhr. R.A. Roorda (CU-SGP)
Dhr. A.H.J. van Strien (50PLUS)
Dhr. A.J.G. Burger (CDA)
Dhr. J.W.C. de Mooij (CDA)
Dhr. J.A.M. van der Slot (Agrarisch)

Aanwezigen Rijnland:
Mevr. I.C. Gerrits
Mevr. S. Chaouat
Dhr. R. van der Voort
Dhr. S. Hoeksma
Mevr. I. Wetzer (Secura)

Opening
De dijkgraaf heet de aanwezigen van harte welkom. Omdat het beoogde afscheid van de Rekenkamercommissie geen doorgang kan vinden, geeft hij het woord meteen aan hoogheemraad mevrouw Verkleij voor de aftrap van het avondprogramma.

Hoogheemraad Verkleij memoreert dat de VV op 27 september 2023 het rapport van de Rekenkamer 'Grip op Informatieveiligheid' heeft behandeld. Hierin werd onder andere geadviseerd de inhoudelijke kennis van de VV op het gebied van informatieveiligheid en cybersecurity te vergroten. Daartoe is deze Beeld-VV belegd. Centrale thema's zijn onder andere: 'awareness' en bovenal ook 'het gedrag' van de aanwezigen in hun rol als bestuurder maar ook als persoon. Voor het maken van noodzakelijk geachte stappen wordt een aantal adviezen aanreikt.
Tevens wordt in deze Beeld-VV aandacht besteed aan de aanstaande wet- en regelgeving van de 'Network and Information Security (NIS2) directive.' Deze richtlijn is gericht op een verbetering van de digitale en economische weerbaarheid van Europese lidstaten. Ook Rijnland moet aan deze Europese vereisten voldoen.

Programma
Presentatie door mevrouw dr. Inge Wetzer (Hoofdpsycholoog Cybersecurity & Compliance bij Secura).
Presentatie door mevrouw Sophie Chaouat, Sierk Hoeksma en Anne van der Voort.

Awareness en cybersecurity
Als eerste stelt mevrouw Wetzer dat de mens niet het grootste risico *hoeft* te vormen met betrekking tot cybersecurity *mits* deze maar op de juiste wijze wordt ondersteund. Als psycholoog is zij gespecialiseerd in de 'menskant van cybersecurity'. Ook al beschikt een bedrijf over optimale beveiliging, dan nog speelt de mens een doorslaggevende rol. Beveiliging is niet opgewassen tegen het telefonisch weggeven van wachtwoorden dan wel het verlenen van toegang tot het waterschap aan onbevoegden.
Aandacht voor cybersecurity is om meerdere redenen noodzakelijk: het is zeer schadelijk voor een instantie/bedrijf als in de media berichten verschijnen over de gevolgen van een (mogelijk) lek. Ook zal een ransomware-aanval tot forse financiële schade leiden (ook indirect doordat het getroffen bedrijf plat komt te liggen) en kan het een behoorlijke negatieve persoonlijke impact hebben. Deze vorm van georganiseerde criminaliteit gaat zeer gewiekst te werk en eist veelal een weloverwogen bedrag om daarmee de 'gestolen gegevens' weer toegankelijk te maken voor het getroffen bedrijf.

Een geslaagde aanval is meestal terug te voeren tot het handelen van één persoon (downloaden muziekbestanden van website/klikken op phishing-link en daarmee op foute website is ingelogd/weggeven wachtwoord/gebruik van onveilig wachtwoord). Kortom: de mens is cruciaal, naast processen en techniek. Tijdens deze presentatie staat de 'menskant van cybersecurity' dan ook centraal.

Zie hiervoor de presentatie op de website van Rijnland: https://rijnland.waterschapsinformatie.nl/vergadering/1192329
Onderstaand enkele kernpunten:

- Medewerkers krijgen instructies over wat te doen. En er wordt vervolgens verwacht dat men die ook daadwerkelijk toepast. Maar in de praktijk blijkt, dat mensen zich niet altijd aan de regels houden. Dus waarom zou het ten aanzien van cybersecurity afdoende zijn als de regels zijn gecommuniceerd?
  Weten wat je moet doen houdt dus niet in dat je het ook doet.
- Onderzoek heeft aangetoond, dat er ten aanzien van cybersecurity een kloof is tussen 'awareness' en gedrag.
- Zie de praktijk waarin wachtwoorden op slinkse wijze door onbekende bellers succesvol worden ontfutseld, ook aan diegenen die denken dat zij ongevoelig zijn voor deze benadering.
- Of misleidende adviezen om bepaalde louche websites te bezoeken om zogenaamd 'zelf' een accountcontrole uit te voeren waarmee men dus onbevoegden toegang geeft (die sites zijn -om vertrouwen te wekken- zelfs voorzien van het logo van het eigen bedrijf).
- 35% personen deelt desgevraagd zijn wachtwoord (er is geen verschil of dit via een website of persoonlijk wordt gevraagd). Dus: weten wat je moet doen, is niet voldoende om het ook daadwerkelijk te gaan doen.
- Als einddoel van het programma voor Rijnland is de focus niet gelegd op 'awareness' maar op 'veilig gedrag'.
- Volgens psychologie bestaat gedrag uit drie factoren:
  - capaciteit (weten en kunnen wat te doen, dus inclusief awareness)
  - willen: zijn mensen wel gemotiveerd, overtuigd van de noodzaak om computers af te sluiten e.d.
  - gelegenheid: worden mensen in staat gesteld te doen wat er van hen wordt verwacht (men dient in te loggen op de VPN, maar als die hapert, laat men het zitten): dus zorg er als bedrijf voor dat dingen goed werken.
- Hierin moet zijn voorzien voordat mensen bepaald gedrag gaan vertonen. Willen we gedrag wijzigen, dan moet *eerst* in kaart worden gebracht welke van de genoemde factoren ontbreekt/ontbreken.
- Als mensen iets niet weten, is het tijd om hen te instrueren (vertellen en herhalen van regels, bijvoorbeeld). Kennis die wordt aangeboden, moet gericht worden aangeboden.
  Voorbeeld: de noodzaak van sterke wachtwoorden (zie hieronder).
- Maar als zij wel geïnformeerd zijn, is het herhalen van regels zinloos. Dan moeten zij worden gemotiveerd.
- Als de gelegenheid ontbreekt, moeten mensen worden geholpen/gefaciliteerd om het gewenste te kunnen doen.

Wachtwoorden
Door de snel voortschrijdende techniek, worden sterke wachtwoorden steeds belangrijker.
Hackers maken gebruik van een gigantische en steeds geüpdatete database (met alle woorden uit het woordenboek, ondertiteling van films, nieuws, nieuwe woorden e.d.). Hierin staan 5,1 miljard woorden. Versleutelde wachtwoorden worden hiermee (al dan niet aangevuld met speciale tekens e.d.) razendsnel vergeleken. Al met al: met 1 triljoen opties (ook gecombineerde woorden).
Een goed wachtwoord mag dus niet in deze 'hackers-bibliotheek' voorkomen.
Hoe langer het wachtwoord, samengesteld uit onwaarschijnlijke -niet te raden- woorden en combinatie met karakters e.d., hoe beter!
Uit het voorbeeld blijkt dat een wachtwoord bestaande uit 18 tekens (combinatie hoofdletters/kleine letters-cijfers en speciale tekens) *momenteel* nog jaren vergt om te kraken. *Advies Secura*: kies een niet te raden wachtwoord (dat niet voorkomt in de 'hackers-database') van minimaal 12 tekens. Naarmate de techniek voortschrijdt, moet er een steeds langer wachtwoord worden gekozen en zullen 12 tekens niet meer afdoende zijn.

Mensen willen wachtwoorden kunnen onthouden. Het gebruik van namen van kinderen e.d. is uiteraard uit den boze.
Voorbeelden van sterke wachtwoorden (het kleine beetje extra moeite levert een enorme winst qua veiligheid op):
a. *Maak een zin waarvan de eerste letters achter elkaar worden geplakt, met een cijfer.*
Voorbeeld: 'Mijn kinderen heten Jip en Janneke en zijn 6 en 8 jaar oud'. Dit wordt dus: MkhJ&J&z6&8jo
b. *Of plak drie random woorden aan elkaar waarvan één niet-bestaand woord.*
Voorbeeld: 'PannekoekTenerifeWappewaaier' of nog beter: 'Pannekoek,Tenerife&Wappewaaier'.
Non-woorden (zelf verzonnen) bemoeilijken het kraken, zeker als hier nog een komma of speciaal teken aan wordt toegevoegd.
Nota bene: in de 'hackers-database' staan ook verkeerd gespelde woorden zoals 'pannekoek' (in plaats van 'pannenkoek').

Vraag: Secura gaat ervan uit, dat iemand bij elke inlog zijn/haar wachtwoord invult maar in de praktijk worden wachtwoorden door bepaalde sites onthouden (zoals Facebook).
Antwoord: In het voorbeeld wordt gedoeld op een sterk wachtwoord voor het eigen account van medewerkers van Rijnland, de bank, de laptop van Rijnland: dat *moet* sterk zijn. Voor de diverse sites, moet idealiter gebruik worden gemaakt van een

uniek wachtwoord per site: daarvoor kan men gebruik maken van 'wachtwoordmanagers' (dan is één sterk wachtwoord voor de toegang tot die 'kluis' voldoende: de wachtwoordmanagers maakt de wachtwoorden voor de sites aan).
Nota bene: als een computer openstaat, kan die worden gebruikt door iemand anders en zodoende kan deze niet-geautoriseerde persoon ook alle websites die daarmee verbonden zijn benaderen: dan kan niet als gebruik wordt gemaakt van een wachtwoordmanager (dan moet via die wachtwoordmanager immers nog worden ingelogd)

(vervolg presentatie)
Wat te doen als mensen het gewenste gedrag niet vertonen omdat ze niet gemotiveerd zijn? Zaken niet belangrijk vinden? In dit geval moeten zij worden gemotiveerd worden waarbij de rol van management en bestuur doorslaggevend zijn. Voorbeeldgedrag is essentieel: dit sijpelt door naar de rest van de organisatie.
Dus:

- Vertoon voorbeeldgedrag
- Spreek anderen erop aan als je 'onveilig' gedrag waarneemt (zoals het laten rondslingeren van stukken; het verzenden van stukken via hotmail.com of gmail.com, het laten openstaan van een onbewaakte computer). Vraag: durven mensen elkaar op onveilig gedrag aan te spreken?
- Is cybersecurity wel een vast onderdeel van de agenda?
- Stel vragen! Houd het onderwerp levend. Is er bij nieuwe plannen aandacht besteed aan cybersecurity? Zijn systemen getest? Zijn de leveranciers bewezen betrouwbaar?

Gelegenheid
Het bedrijf moet erop toezien dat de materialen in de praktijk functioneren en vindbaar zijn in het eigen werk-account. Als dat niet het geval is, worden wachtwoorden veelal uitgewisseld en wordt in het account van een collega gewerkt.

Cultuur
Mensen moeten elkaar durven aanspreken, bijvoorbeeld op het zichtbaar dragen van de werkpas.
In de praktijk zijn mensen terughoudend: men is bevreesd voor de gevolgen als men (onwetend) een 'hotemetoot' aanspreekt. Zodoende doen medewerkers dus niet wat er eigenlijk van hen wordt verlangd!
Dus zorg van bovenaf voor een cultuur, waarin iedereen elkaar kan aanspreken en dat ook doet. Draag als leidinggevenden uit, dat dit een belangrijk thema is (bottom-up en vice versa).

Dus Secura gaat Rijnlanders opleiden én motiveren zodat het gedrag wordt aangepast. Tevens wordt er door Secura gefaciliteerd, zowel in cultuur als in context.

Presentatie 'Integraal Risicomanagement - NIS2-Richtlijn - AI Verordening (zie ook de presentatie in iBabs)
Door Sophie Chaouat, Sierk Hoeksma en Anne van der Voort

Kernpunten: de afgelopen jaren is er bij Rijnland veel geïnvesteerd in techniek en beleid en zijn de grootste risico's ('kroonjuwelen') in kaart gebracht samen met de eigenaren en is onderzocht wat moet worden afgedekt.
De 'kroonjuwelen' worden veel gebruikt bij de procesautomatisering en dienen dan ook optimaal beschermd te worden tegen een hackaanval.
De laptops en IPad die Rijnland gebruikt zijn voorzien van adequate beveiliging en het gebruik ervan wordt gemonitord (gebruik buiten Europa wordt bijvoorbeeld vanwege veiligheid geblokkeerd maar het binnendringen via een VPN blijft een risico). De procesautomatisering is het 'hart van het Rijnlandse waterlandschap' en vergt dan ook de best mogelijke beveiliging.
Tevens is onderzoek gedaan naar calamiteiten en werd veel geïnvesteerd in het thema 'awareness' in alle lagen van de organisatie: bestuurders, techneuten die met de kritische systemen werken, medewerkers op de werkvloer e.d.
De komende drie jaar wordt dit nader geconcretiseerd door Secura.

BIO
De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). De Unie van Waterschappen heeft bepaald dat de waterschappen moeten voldoen aan niveau 4. Drie jaar geleden zat Rijnland op niveau 2-2 ½. Anno 2024 op 3,2. De techniek is aardig op orde, maar er moeten nog procedurele stappen worden gezet. Ter ondersteuning is Secura ingehuurd. Al met al kan Rijnland stellen dat het waterschap best 'redelijk in control is op het gebied van security, maar het kan alleen beter'.
E.e.a. hangt samen met PDCA (Plan – Do – Check – Act): een structurele, cyclische aanpak, veelgebruikt in continue verbetertrajecten. Het draagt bij aan het structureel oplossen van problematiek. Deze aanpak sluit aan op het advies van de Rekenkamer: bestuurders van Rijnland hebben nadrukkelijk een rol in dit PDCA-proces. Het kan gezien worden als een belangrijk onderdeel van het bewustzijn -nadrukkelijk ook bij de bestuurders- van risico's bij het aangaan van nieuwe projecten, te nemen beslissingen:

- Wat zijn we aan het doen?
- Doen we de juiste dingen?

- Hebben we de juiste vragen gesteld?

Voorheen was er behoorlijke afstand tussen de digitale en fysieke wereld. Anno 2024 zijn deze onlosmakelijk met elkaar verbonden, zie ook de veranderde wetgeving via richtlijnen en verordeningen.
Richtlijn: stelt een algemeen doel vast.
De EU-lidstaten moeten voor 17 oktober 2024 zelf de richtlijn omzetten in nationale wetgeving teneinde uniformiteit binnen alle EU-landen over de betreffende wet die wordt omgezet.
Verordening: deze is bindend voor alle partijen en werkt rechtstreeks door in de rechtsorde. Voorbeeld: de AVG.

Toegelicht wordt de NIS2-richtlijn én de AI-verordening.
Bij de beoordeling van de digitaliseringswetgeving moeten alle onderstaande rechtsgebieden worden meegewogen:

- De Aanbestedingswet 2012
- Aansprakelijkheid Burgerlijk Wetboek
- Privacy & Ethiek
- AI Act (EU)
- Data Governance Act
- NIS2-richtlijn
- Beleid van andere waterschappen en overheden

Door de AI-verordening zal straks het aansprakelijkheidsregiem maatschappij-breed wijzigen en dus ook voor het waterschap gevolgen hebben.
Voorbeeld: het gevaar is dat de doorvoering van algoritme/technische toepassing leidt tot een probleem voor de burger, en het voor deze betrokkene onmogelijk is om te bewijzen *wat* er mis is gegaan. Het is niet toegestaan dat deze persoon geen inzage heeft in het algoritme, welke data het waterschap hierin heeft verwerkt, wat de resultaten zijn.
Toepassingsgebied van de NIS2-richtlijn

- De NIS2-richtlijn is van toepassing op de waterschappen en sectoren zoals energie, transport, bankwezen, gezondheid, digitale infrastructuur en meer.
- Organisaties met minimaal 50 werknemers of een jaaromzet van minimaal €30 miljoen vallen binnen het toepassingsgebied. Entiteiten die vallen onder de NIS2-richtlijn zijn verplicht zich te registeren.

Risicobeheer en rapportage
Rijnland is verplicht tot het uitvoeren van risicobeoordelingen: die moeten in kaart worden gebracht en er moeten cyberbeveiligingen worden doorgevoerd.
Deze verplichtingen gelden ook voor de toeleverancierssketen: dus waarmee Rijnland op technisch gebied samenwerkt.
Als Rijnland bepaalde beheersmaatregelen neemt, moet Rijnland kunnen controleren of de andere partijen in die keten dezelfde beheersmaatregelen hebben getroffen. Dat vergt awareness bij het waterschap bij de beoordeling van contracten, bekijken van de keten.
Meldingsplicht en bestuurdersaansprakelijkheid
Bij incidenten moet Rijnland die melden (conform geldende termijnen). Bij niet naleving van de NIS2-richtlijn kunnen bestuurders aansprakelijk worden gesteld.
Door het treffen van -bijvoorbeeld- beheersmaatregelen kan de kans op risico's worden beperkt. Er worden alleen in het uiterste geval door de toezichthouder boetes opgelegd. Deze toezichthouder moet nog worden aangesteld.
Toezicht
Rijnland moet rekening en verantwoording afleggen en kunnen bewijzen dat het aantoonbaar voldoet aan de eisen uit de richtlijn. De ambtelijke organisatie dient e.e.a. goed te incorporeren. Bestuurders moeten begrijpen dat het een breed scala wetgeving betreft en dat nieuwsgierigheid wenselijk en zinvol is: zij dienen vragen te stellen ('waarom wordt deze technische oplossing toegepast', 'hoe is het geregeld', 'welke analyses heeft Rijnland gemaakt', e.d.).
Om de bestuurders hierin te ondersteunen, zal een checklist worden ontwikkeld en zullen bestuurders goed worden geïnformeerd.

Vragen:

- Betreft het een direct werkende bepaling? Of is er ook nog lokale wetgeving vereist?
  Antwoord:
  Deze NIS2-richtlijn moet door de wetgever worden omgezet in nationale wetgeving. Bestuursaansprakelijkheid: het is nog niet duidelijk hoe de wetgever deze richtlijn nationaal gaat implementeren.
- Wat is de deadline?
  Antwoord: 17 oktober 2024. De minister veronderstelt dat deze onhaalbaar is en dus zal worden opgeschoven.
- Is de richtlijn automatisch van toepassing?
  Antwoord: zodra deze verbindend is (expliciet, transparant en helder voor iedereen) zal deze meteen voor iedereen gelden. Dat geldt niet voor onderdelen waar mogelijke beleidsruimte voor de wetgevers geldt: waar afwegingen kunnen worden gemaakt. In die gevallen zal worden afgewacht hoe de wetgever de richtlijn omzet in nationale wetgeving.
- Geldt de bestuurlijke aansprakelijkheid het totale bestuur van Rijnland of kunnen ook individuele VV-leden, hoogheemraden aansprakelijk worden gesteld?

Antwoord:
Het kan gaan over de aansprakelijkheid van het bestuur van Rijnland als geheel maar in bepaalde omstandigheden kunnen individuele bestuurders ook aansprakelijk worden gesteld ten aanzien van een genomen besluit. Maar: de impact is nog niet bekend omdat de wetgever de richtlijn nog niet heeft omgezet in nationale wetgeving.
Maar de kans dat een individuele bestuurder aansprakelijk wordt gesteld, is klein mits Rijnland voldoende 'checks and balances' heeft ingebouwd in de processen, de bestuurders optimaal worden geïnformeerd over de richtlijn, dat zij weten welke vragen zij moeten stellen én er intern voldoende beheersmaatregelen zijn getroffen voor specifieke risico's.
Immers: er geldt een gezamenlijke zorgplicht. De NIS-2 gaat over zorgplicht. Dus als kan worden aangetoond dat deze door Rijnland/bestuur goed is ingevuld, zal de discussie over de aansprakelijkheid niet meer zwart/wit zijn. Dan is de wijze waarop in bepaalde omstandigheden is geacteerd bij een specifieke toepassing van een bepaalde technische oplossing essentieel.

AI-Verordening (Act)
Er is een samenhang tussen deze verordening en de NIS-2-richtlijn. Beide betreffen digitaliseringswetgeving.
De AI ziet specifiek op de toepassing van AI en is risico-gericht.
Het is de bedoeling van deze AI-Verordening, dat binnen de EU alle landen een bepaalde mate van 'awareness' creëren en zij met elkaar bepaalde risico's niet willen nemen. Denk aan de onacceptabele en hoge risico's.
Er bestaan:

- Onacceptabele risico's: het toepassen van AI is dan verboden (voorbeeld: biometrische identificatie/social scoring, dus op basis van sociaal wenselijk gedrag).
- Hoge risico's: AI is weliswaar niet verboden, maar hoe hoger het risico, hoe meer eisen worden gesteld aan de transparantie van de werking, informatie én besluitvorming.
- Beperkte risico's
- Minimale risico's

De AI-Verordening vergt nieuwe compliance- en beveiligingsverplichtingen. Er zullen meer controles worden toegepast.
Risico's zullen integraal worden beoordeeld (wat zijn de effecten voor IT, de juridische effecten, voor andere organisaties, watersystemen e.d.). De brede toepassingen moeten met elkaar in kaart worden gebracht.
Belangrijk: een AI-systeem mag geen 'black box' zijn. Dat houdt in dat onbekend is wat de uitkomsten zijn van het invoeren van data (zicht op wat er precies is gebeurt in dit proces ontbreekt) en men kan de output van de AI ook niet begrijpen: niet herleiden tot de data die worden aangeleverd na de bewerking.
De wetgever bepaalt: het is verplicht dat de data na de AI-bewerking kunnen worden gematcht (en uitgelegd) met de ingevoerde data.
De bewijslast voor wat betreft aansprakelijkheid gaat verschuiven.
Doel van de AI-Verordening
Het stimuleren van innovatie.
De veiligheid voor toepassing van AI en grondrechten waarborgen.
Het beschermen van de democratische rechtstaat binnen de EU.
Overige aandachtspunten:

- De AI Act is aangenomen.
- Rijnland moet rekening houden met bepaalde termijnen (afhankelijk van het type risico's dat wordt gelopen op basis van de AI Verordening)
- Basismodellen (Bing Chat en ChatCPT): ontwikkelaars van deze basismodellen moeten 12 maanden na invoering van de AI Verordening (begin 2025) aan deze Verordening voldoen bij de toepassingen.
- In het geval van verboden systemen, moet elke lidstaat binnen 6 maanden na inwerkingtreding van de AI Verordening, hier hard tegen optreden.
- De hoogte van de boetes is afhankelijk van de mate van de schending e.d.
- De beoordeling van risico's moet op basis van de AI Verordening én de NIS2-richtlijn (gezien hun samenhang).

Vragen:

- Wat kan er misgaan?
  Antwoord: zie een uitspraak van de Raad van State (AERIUS). De berekeningen waren niet inzichtelijk voor de gedupeerden die de zaak hadden aangespannen. De RvS stelde dat als men een bepaalde berekeningsmethodiek toepast (dat was een bepaald algoritme) dan moet men kunnen begrijpen hoe die berekening tot stand is gekomen én waarom is gekozen voor die toepassing. Er moet dus worden voldaan aan het transparantie-vereiste zodat burgers/gedupeerden kunnen reageren op een genomen besluit.
- Wordt een dergelijke toepassing/model verboden (en mag dus niet meer worden gebruikt?) of kan het worden gebruikt totdat een andere gedupeerde een zaak aanspant?
  Antwoord:
  Neen: het model mag dan niet meer worden toegepast. Er moet worden voldaan aan een transparantie-verplichting, er moeten 'checks and balances' en eisen worden ingebouwd.
  Een verbod is niet per se noodzakelijk maar een uitspraak moet wel leiden tot aanpassingen.

In de AI Verordening wordt overigens nauwkeurig omschreven wat onder verboden systemen wordt verstaan.
Verschuiving aansprakelijkheid: op basis van de AI Verordening moeten bedrijven aantonen dat zij AI correct hebben toegepast. Zij moeten hun systemen dus kunnen uitleggen. Als de burger kan aantonen dat een bedrijf een fout heeft gemaakt (door toepassing van een systeem) dan moet dit bedrijf kunnen aantonen dat deze fout het bedrijf niet kan worden aangerekend. Het bedrijf moet dus weten wat er in de keten van besluitvorming is gebeurd (dus: 'comply or explain').

- Rijnland is een besluitvormend orgaan. Heeft de Wetenschappelijke Raad voor het Regeringsbeleid (of ander belangrijk orgaan) al een uitspraak gedaan over de (on)wenselijkheid van het gebruik van ChatGPT bij besluitvormingsprocedures (bijvoorbeeld binnen de VV)?
  Antwoord:
  De Unie van Waterschappen buigt zich momenteel over de richtlijnen als basis om te gaan toepassen binnen diverse gradaties. ChatGPT is een publiekelijke applicatie die de waterschappen eigenlijk niet willen gebruiken. De waterschappen willen de zakelijke variant gebruiken: die is beter controleer- en uitlegbaar vanuit een zakelijk perspectief. E.e.a. in het verlengde van de risicoafwegingen (welke bronnen zijn gebruikt, wat kan wel/niet worden uitgelegd). Elke toepassing moet apart worden beoordeeld.
  Alle moderne mobiele telefoons zijn al voorzien van een behoorlijke dosis AI.
  Rijnland gaat een pilot doen met 80 medewerkers: er wordt geëxperimenteerd met Microsoft CoPilot. De zakelijke variant van ChatGPT. Er wordt onderzocht hoe binnen de organisatie veilig gebruik kan worden gemaakt van AI. Hiervoor zijn richtlijnen opgesteld: er mag geen persoonlijke informatie worden opgevraagd en de bronvermelding moet inzichtelijk worden gemaakt zodat men 'kan terugkijken'.
  Bij het gebruik van AI moet rekening worden gehouden met de privacy: de richtlijnen zullen daarop worden afgestemd.
- Er zijn/komen richtlijnen en kaders. Maar hoe kan worden afgestemd dat deze goed worden toegepast?
  Antwoord:
  Kaders zijn een keuze van de organisatie die daarbij moet handelen op basis van de wetgeving (dus: geen social scoring). In de risico-categorieën tussen hoog en midden, zal de organisatie zelf keuzes moeten maken.
  In de nieuwe waterzuivering van Haarlem-Waarderpolder wordt AI ingezet ten behoeve van optimalisatie van het zuiveringsproces. Dus naast de fysieke omgeving moet ook de digitale omgeving worden meegewogen in de integrale risico-afweging.
  Het overheidsorgaan moet er zelf op toezien dat het binnen de lijnen blijft opereren en zorgt voor een kader dat past bij het risico dat wordt toegepast (bij de technische oplossing). Maar er moet uiteraard worden voldaan aan de bestaande wetgeving/richtlijnen (de genoemde integrale wetten/regels). Het kader moet daarbij aansluiten. Binnen de beleidsruimte, moeten bedrijven transparant handelen en voldoen aan de algemene beginselen van behoorlijk bestuur.
- Betekent dit dat organisaties e.e.a. zelf moeten 'uitvogelen'?
  Antwoord:
  Neen: er wordt immers samengewerkt met andere overheden, zoals het Rijk en de Unie van Waterschappen. De waterschappen trekken gezamenlijk op. Na de ingang van nieuwe wetgeving, moet er altijd wat worden gepionierd maar op basis van het scala wetgeving/regels, zal er weinig verschil optreden qua keuzes. Iedereen moet zich immers aan de wet houden, en de AI Verordening werkt rechtstreeks én is duidelijk.
- Stel Rijnland gaat AI op een installatie toepassen en is dan leidend voor aantal beslissingen. Hoe worden calamiteiten voorkomen als AI verkeerde keuzes maakt?
  Antwoord:
  Rijnland zal nimmer een inbreuk toestaan van AI op de veilige procesautomatisering. Er zijn altijd 'check and balances' die voorkomen dat er risico's worden gelopen. Maar mensen reageren langzamer op de ontwikkelingen van de waterkwaliteit dan AI. Door de inzet van AI kunnen de door mensen opgestelde bandbreedtes dichter worden gevolgd dan handmatig het geval is.
- Rijnland heeft geen hoogrisico-categorie. Voldoet Rijnland al aan de governance van de AI Act?
  Antwoord:
  De AI Act is op 14 maart 2024 door het EU Parlement aangenomen. Rijnland gaat AI vooralsnog alleen experimenteel toepassen binnen de kaders van de wet. Het vergt nog tijd om te bepalen wat de impact van de AI Act zal zijn voor Rijnland (welke kaders/richtlijnen moeten worden opgesteld, wat de gevolgen zijn voor risicobewustzijn en beoordeling, hoe Rijnland aankijkt tegen de keten en wat de risico's zijn voor Rijnland én de cybersecurity-risico's e.d.). Dit wordt meegenomen in het kader van de integrale risicomanagementbeoordeling.
- Data moeten veilig zijn. Is er een compleet zicht op de databronnen? Wordt er beschikt over een datacatalogus? Hoe zijn de verantwoordelijkheden vastgelegd?
  Antwoord:
  Binnen Rijnland wordt gesproken over systeemeigenaren. Deze zijn ook verantwoordelijk voor de data in het systeem. Voor wat betreft de 'kroonjuwelen' (primaire Rijnlandse systemen) zijn de eigenaren verantwoordelijk voor de data. Los daarvan bestaan er systemen die de data van Rijnland hergebruiken en het eigenaarschap elders is belegd.

Rijnland kopieert een deel van de data naar een data-warehouse ten behoeve van het opstellen van rapportages. Maar het eigenaarschap verhuist niet mee.

- AI 'slurpt energie'. Is dit onderdeel van de risicoanalyse?
  Antwoord:
  Het trainen van een AI-model vergt veel energie, maar het gebruik ervan kan zelfs via een mobiele telefoon. Microsoft ChatGPT traint het universele model en als Rijnland dit wil aanpassen aan eigen waterdata, traint Rijnland dus slechts een minuscuul deel daarvan. Dit kost aanmerkelijk minder energie. Door de snel voortschrijdende technologische ontwikkelingen, is AI al in het merendeel van de huidige telefoons verwerkt. Afhankelijk van de inzet van ChatGPT kan ook gesteld worden dat AI soms ook energie oplevert.
- Het is denkbaar dat de medewerkers van Rijnland hoorndol worden van steeds wijzigende regels ten aanzien van security e.d. waardoor zaken verloren kunnen gaan.
  Is er sprake van samenwerking tussen de waterschappen, gelet op de complexiteit en benodigde kennis?
  Antwoord:
  Rijnland werkt samen met de UvW in het kader van de richtlijn. Ook worden er met aantal waterschappen co-pilots opgezet (met het Waterschapshuis). Aanvankelijk met een viertal waterschappen. Later met meerdere.
  Er wordt de laatste jaren structureel samengewerkt op het gebied van cybersecurity. Er wordt gebruik gemaakt van 'IT exception management'. Dat houdt in dat in de hele keten alleen diegene toegang krijgt tot bepaalde data waarvoor deze is geautoriseerd.
  Nog niet alle systemen zijn overigens hierop al ingericht (afhankelijk van de levensduur). Deze worden dan ook niet automatisch aangesloten op een AI-omgeving.
  Binnen de Unie van Waterschappen wordt samengewerkt met diverse juristen. Er wordt een AI Werkgroep opgezet die ook de kaders gaat opstellen (gericht op uniformiteit).
- NIS-2: beschikt Rijnland over een 'Incident Response Plan'?
  Antwoord: Rijnland en Schieland hebben gezamenlijk een calamiteitenplan dat verder reikt dan alleen de IT. 4 april start een uitgebreide training om te borgen dat IT en de calamiteiten met elkaar verbonden zijn/worden.

Checklist
Er wordt gewerkt aan een concrete checklist. Zie dia 11 en 12. Hierin worden vragen die gesteld kunnen worden opgenomen over:

- risicobeoordeling
- beveiligingsmaatregelen
- transparantie/uitlegbaarheid
- verantwoordelijkheid
- identificatie en classificatie
- opleiding en bewustwording
- privacy en ethiek

Het stellen van deze vragen zijn een belangrijk onderdeel van de zorgplicht, en wordt de kans dat Rijnland aansprakelijk wordt gesteld, voorkomen. Het risico wordt dus verkleind.
Tot slot:
De VV-leden krijgen de kans om in kleine groepjes (6-7 personen) fysiek een test te doen/te oefenen. Hierin wordt aandacht besteed aan onder andere privacy en ethiek.

Vraag:

- Staat er een 'Responsible disclosure procedure' op de website? Waarmee hackers wordt uitgenodigd om lekken op te sporen?
  Antwoord:
  Sinds kort is dit het geval. Maar Rijnland nodigt zelf ook georganiseerd hackers uit om op het hoofdkantoor testen uit te voeren.

Afsluiting
Hoogheemraad Verkleij-Lemmers dankt betrokkenen voor de duidelijke uitleg bij de presentatie. Zij roept de VV op zich aan te melden voor de cursus en toets mede gezien het belang van voorbeeldgedrag richting anderen. Aanvullende vragen kunnen ook na deze bijeenkomst worden gesteld.