Hoogheemraadschap van Rijnland

Memo – Ter kennisname

Registratienummer:
20.014159

Aan:	VV
Van:	D&H
Onderwerp:	Informatieveiligheid
Datum:	3-3-2020

Waarom moet u dit weten

Er is geregeld aandacht geweest voor het thema informatieveiligheid. Met name de relatief grote incidenten, zoals de Citrix-calamiteit van januari 2020 en de calamiteit met 'ransomware' bij de Universiteit Maastricht van eind 2019 maken de kwetsbaarheid van digitale systemen duidelijk; een goed niveau van informatiebeveiliging is een randvoorwaarde voor een ongestoorde bedrijfsvoering. Bij de behandeling van de najaars-burap 2019 in de VV-cie van 6 november is door de heer Roorda de vraag gesteld wat de impact is van de in de burap gemelde achterstanden met het op orde krijgen van de informatieveiligheid.

In de beeldvormende sessie van de VV van 25 maart 2020 over digitale transformatie zal ook aandacht bestaan voor informatieveiligheid, maar gezien het specifieke karakter van dit onderwerp, lijkt het tevens goed u daar apart over te informeren met dit memo.

Regulier zal de vv geïnformeerd blijven via de gebruikelijke systematiek van bestuurs-rapportages in de planning en control-cyclus. Als zaken tussendoor bestuurlijk relevant zijn, wordt de vv geïnformeerd, zoals ook standaard al bij opgeschaalde calamiteiten geschiedt.

Kernboodschap n.a.v. vv-vraag

In antwoord op de vraag van de heer Roorda kan aangegeven worden dat met de achterstand bedoeld is dat de planmatig ingezette risico-analyses ook in het jaar 2020 nog zullen doorlopen. Het gaat daarbij om het project om alle Rijnlandse informatie-verwerkende systemen aan een zogenaamde business impact analyse, diepgaande risico-analyse en/of privacy impact analyse te onderwerpen. De stand is dat inmiddels alle systemen die eerder een hoger risico was toegedicht, onderzocht zijn en maatregelen worden geïmplementeerd. De systemen met een lager risico worden in 2020 onderzocht. In die zin wordt ook hier risico-gebaseerd gepland (grootste risico's eerst).

Algemeen

Rijnland is in nauwe samenwerking met het Hoogheemraadschap van Schieland en de Krimpenerwaard (HHSK) grondig aan de slag om de informatieveiligheid op niveau te brengen. De baseline informatieveiligheid overheden (BIO) stelt de eisen waaraan ook Rijnland dient te voldoen en is een basis om informatieveilig te zijn.

In de Uniecommissie CBCF is reeds in 2014 afgesproken dat de waterschapsector als geheel naar een volwassenheidniveau 4 zal groeien in een aantal jaren. In het bijbehorende stuk (bijlage WIV 14-32) staat wat niveau 4 inhoudt. Op 12 oktober 2018 is die afspraak in de Ledenvergadering van de Unie van Waterschappen nog eens herbevestigd en afgesproken dat eind

2020 volwassenheidsniveau 3 bereikt zal zijn en eind 2021 volwassenheidsniveau 4 (zie bijlage LV 18-26a). In 2021 zal ook een waterschapsector-brede audit worden gehouden.

Voor Rijnland is het bereiken van niveau 3, eind 2020 en niveau 4, eind 2021 wel reëel. Er is nog wel een forse inspanning nodig, maar de verwachting is niet dat daar een omvangrijke financiële investering voor nodig zal zijn.

De PA-nulmeting vanuit Het Waterschapshuis is een audit, specifiek op de procesautomatisering van de waterschappen en geeft in meer detail een beeld van een deel van de informatiebeveiligings-inspanningen (zie bijlagen 'nulmeting PA Rijnland' en 'nulmeting PA landelijk'). De niveau's van volwassenheid, zoals geformuleerd in de PA-nulmeting zijn niet direct te relateren aan de niveau's, zoals geformuleerd in de Unie-besluiten. Ze zijn specifieker, maar wel in lijn met wat regulier gevraagd wordt bij een professionele informatiebeveiliging in lijn met de baseline informatieveiligheid overheden (BIO). Met de score van 2,2 voor Rijnland wordt feitelijk bevestigd dat Rijnland op de goede weg is en maakt, zoals hierboven gesteld, niveau 3, eind 2020 realiseerbaar.

Achtergrondinformatie

Wat is nu, beknopt gesproken, de kern van informatiebeveiliging? Het gaat in hoofdlijnen om veiligheid op drie domeinen:

- Systemen veilig: alle informatie-verwerkende systemen (hard- en software) dienen veilig te zijn. Dat betekent niet alleen dat de systemen permanent een laatste update/patch moeten hebben, maar ook worden gemonitored op beschikbaarheid (op welk moment zijn welke gegevens beschikbaar, hoe lang mag een systeem uitvallen), integriteit (zijn de gegevens juist), vertrouwelijkheid (voor wie zijn welke gegevens zichtbaar of te wijzigen) en privacy (bescherming persoonsgegevens).
- Locaties veilig: wie mag op welke locatie en in welke ruimte. Hier gaat het over de fysieke toegangsbeveiliging en toegangsbeperking voor diegenen die er niks te zoeken hebben;
- Mensen veilig: wie willen we toegang verlenen tot locaties en tot systemen. Screening van medewerkers bij in- door en uitstroom en screening van externe adviseurs, aannemers, leveranciers enz. En hoe willen we de houding en het gedrag van medewerkers en anderen naar een veilige manier van werken krijgen.

Wat wordt er concreet gedaan?
Uitgangspunt is dat de lijnorganisatie zelf verantwoordelijk is om het gewenste niveau van veiligheid te bereiken. Monitoring en rapportage vindt plaats via de Staf Kwaliteit en Veiligheid (vanuit de rol van chief information security officer). Ook daarin wordt samen opgetrokken met HHSK en tevens gerapporteerd aan de gezamenlijke i-Raad en directies.
Op de genoemde domeinen wordt systematisch gewerkt aan het verhogen van de veiligheid. Dat gebeurt:

- risico-gebaseerd: alle systemen en processen worden in 2019 en 2020 aan een risico-analyse en soms diepgaande risico-analyse onderworpen om te bepalen welke beschikbaarheid, integriteit, vertrouwelijkheid en privacy-eisen gesteld dienen te worden en welke maatregelen genomen moeten worden om dat te bereiken;
- om de basis op orde te krijgen: alle benodigde maatregelen vergen veel inspanning. Alle bedrijfsprocessen en ondersteunende systemen dienen een zorgvuldig beheer te kennen, alle contracten gecontroleerd, alle wijzigingen systematisch gedocumenteerd en bij aanschaf of wijziging van systemen dient steeds systematisch te worden onderzocht of en hoe de veiligheid al min of meer standaard kan worden ingebouwd. Dat is werk voor de lijn. Veel maatregelen zitten in de sfeer van kantoor- en procesautomatisering, maar ook vele bij de bedrijfsvoerings-onderdelen (hr, fin-inkoop, facilitair) en de beheerders van locaties;
- via gedragsbeïnvloeding: er is een standaard e-learning module voor alle medewerkers en eerder aandacht aan bewustwording besteed en in 2020 start een grote

bewustwordingscampagne informatieveiligheid en privacy met behulp van een gespecialiseerd bureau, een app op de smartphone en verschillende interventies.
- Via standaard monitoring op incidenten en evaluaties van calamiteiten, zoals de Citrix-calamiteit. Die leren ons hoe de processen zo in te richten dat de kans op incidenten en calamiteiten zo klein mogelijk is;
- Informatiebeveiliging is, zoals voorgeschreven in de BIO, gebaat bij een ISMS (information security management system): hiervoor zetten we een gebruiksvriendelijke applicatie in die zowel de informatieveiligheids-organisatie, maar vooral de business in staat stelt om de benodigde acties te kunnen uitvoeren door beschikbare best practices en door gebruiksvriendelijke rapportage-methodiek waarmee de organisatie uitgevraagd en gemonitored kan worden en gerapporteerd aan directie en bestuur. Dit systeem zal halverwege 2020 in gebruik worden genomen;
- Via Audits, zowel intern (derdelijns controle door Concern control als extern door bijvoorbeeld het Waterschapshuis, waterschapsbreed, zoals bij de PA-nulmeting.