Gemeente Wassenaar

Informatiebrief aan de Raad

090

Zaaknummer:	Z - 20/043742
Documentnummer:	20/043742/270398
Datum:	maandag 11 oktober 2021
Onderwerp:	Toezeggingen RKC rapport informatiebeveiliging
Bijlage(n):	

Geachte Raad,

Dinsdag 7 september is tijdens de Commissie Bestuur & Middelen het rapport informatiebeveiliging van de Rekenkamer Commissie besproken. Hierin is toegezegd op een aantal vraagstukken terug te komen middels een informatiebrief. Specifiek gaat het om de volgende onderwerpen:

- Het structureel en frequent uitvoeren van risicoanalyses.
- De afweging tussen ICT 'in eigen huis' of uitbesteed en de waarde hiervan voor informatieveiligheid.
- Mogelijkheden tot cybercrime dekking.
- Het loggen van penetratiepogingen.
- Afleggen van verantwoording in de risicoparagraaf van de jaarrekening.
- Verkennen of de accountant de ICT kan controleren.
- Aandacht voor informatiebeveiliging bij verbonden partijen.

De opbouw van deze informatiebrief is gestructureerd volgens deze punten.

Risicoanalyse

De Rekenkamer Commissie noemde als aanbeveling om minimaal jaarlijks een risicoanalyse uit te voeren. Bij de gemeente Wassenaar wordt dit systematisch tweejaarlijks gedaan: in 2017, in 2019 en in 2021. Wij zien geen meerwaarde in het frequenter uitvoeren van een risicoanalyse. Er is dan namelijk onvoldoende tijd voor de ambtelijke organisatie om de acties die uit de analyse naar voren komen uit te voeren. De nieuwe risicoanalyse zou dan gewoonweg hetzelfde resultaat opleveren als de vorige.

Het is hiermee ook niet zo dat er onvoldoende zicht is op de risico's. Dit zicht is er weldegelijk en vormt de leidraad bij de acties die op het gebied van informatieveiligheid worden uitgevoerd. Een jaarlijkse risicoanalyse zou niet meer inzicht in de risico's opleveren, maar eerder een overvloed aan informatie wat ten koste gaat van de productiviteit.

ICT 'in eigen huis' of uitbesteden

In de Commissie kwam de vraag of het voor informatieveiligheid uitmaakt of ICT in eigen beheer is, of dat dit uitbesteed wordt. Momenteel is het overgrote deel van de ICT-afdeling in eigen beheer. Hier zijn mensen voor in dienst genomen met de juiste kennis en expertise. Wij verwachten dat de kwaliteit van de ICT-huishouding niet significant zal verbeteren wanneer deze uitbesteed wordt aan een derde partij. De gemeente Wassenaar zoekt wel steeds vaker samenwerkingen op met marktpartijen, waarbij de gemeente uiteraard zelf in regie blijft. Deze

samenwerkingen zijn zowel op het vlak van 'traditionele' ICT, als voor informatieveiligheid (bijvoorbeeld in de vorm van GGI-Veilig).

Een andere vraag op dit vlak betrof het uitbesteden van het ICT gedeelte wat toeziet op de informatiebeveiliging. Deze vraag gaat uit van de opvatting dat informatieveiligheid uitsluitend onderdeel is van ICT. Informatieveiligheid is organisatiebreed en behoeft aandacht vanuit alle gemeentelijke domeinen. Voor informatiebeveiliging zou het daarom niet veel uitmaken of ICT wordt uitbesteed of in eigen beheer blijft, aangezien informatieveiligheid bij de overige gemeentelijke domeinen dan nog niet gedekt zou zijn.

Cybercrime dekking

Een cybercrime incident kan voor de gemeente aanzienlijke financiële kosten opleveren. De Commissie stelde de vraag of het mogelijk is hier een verzekering voor af te sluiten. Een dergelijke verzekering verzorgt niet alleen financiële dekking voor eventuele kosten die met een incident gemoeid gaan, maar het stelt ook eisen aan de kwaliteit van de eigen ICT-huishouding. Hiermee wordt een extra controlestap voor de eigen organisatie ingebouwd.

Een cyberrisicoverzekering is een relatief nieuwe productcategorie van verzekeraars en het nut van een dergelijke verzekering is al een tijd een veelbesproken onderwerp in het veld van informatiebeveiliging.

Over het algemeen komt men echter altijd uit op de volgende conclusie: het verhalen van de geleden schade brengt te veel onevenredigheden met zich mee in het kader van de voorwaarden die gesteld worden in een dergelijke polis. Energie en budget steken in risicobeheersing en de implementatie van de BIO is waar de voorkeur naar uitgaat.

Daarnaast zijn de premies voor degelijke cyberrisicoverzekeringen dusdanig hoog dat deze over het algemeen niet opwegen tegen het investeren in de eigen informatiebeveiliging.

Loggen van penetratiepogingen

In de Commissie werd de vraag gesteld of er inzicht is in hoe vaak er wordt geprobeerd in te breken in de gemeentelijke netwerken.

Bij de gemeente Wassenaar zijn er verschillende mechanismen ingericht waarmee penetratiepogingen gedetecteerd, gestopt en gelogd worden. Een voorbeeld van een dergelijk mechanisme is de Firewall. De Firewall is een beschermingstechnologie die inkomend en uitgaand dataverkeer blokkeert en controleert. Wekelijks genereert de Firewall een rapport waarin al het dataverkeer van die week is gelogd.

Naast de informatie die de Firewall genereert wordt er bij de gemeente een incidentenregister bijgehouden. Hierin worden o.a. penetratiepogingen met een hoog dreigingsniveau geregistreerd, alsook datalekken en overige informatiebeveiligingsincidenten.

Ten slotte is de gemeente Wassenaar momenteel bezig met de implementatie van de percelen van GGI-Veilig. Een van deze percelen betreft een Siem/SOC, een actief monitoring & response systeem voor het bewaken van gedrag en acties op het eigen netwerk. De verwachting is dat deze implementatie in de eerste helft van 2022 is afgerond.

Afleggen van verantwoordelijkheid in risicoparagraaf jaarrekening

Jaarlijks werd in de jaarrekening van de WODV een paragraaf Informatieveiligheid & Privacy opgenomen. Hierin wordt onder andere aandacht besteed aan het informatieveiligheidsbeleid, eventuele incidenten van het afgelopen jaar, vorderingen op technisch vlak en de stappen die zijn gemaakt op het gebied van bewustwording. Vanaf dit jaar zal dit worden opgenomen in de gemeentelijke jaarrekening van Wassenaar.

ICT-controle door accountant

Uit de Commissie kwam een vraag betreffende de mogelijkheid tot het aanleveren van informatie, zodat een ICT-controle aan de accountant zou kunnen worden overgedragen. Deze informatie zou in principe aangeleverd kunnen worden.

Daarbij is het wel goed om te beseffen dat er jaarlijks al een onafhankelijke ICT-controle wordt uitgevoerd tijdens de IT-audit van de Jaarrekening, de ENSIA zelfevaluatie en de DigiD-audit voor de nieuwe aansluitingen.

Bij beide audits wordt de ICT-huishouding van de gemeente gecontroleerd door een onafhankelijke auditor. Hier wordt vervolgens een rapport over uitgebracht. Informatie voor een extra ICT-controle door de accountant kan uiteraard aangeleverd worden, maar de meerwaarde hiervan moet in overweging genomen worden.

Informatiebeveiliging bij verbonden partijen

In alle overeenkomsten die de gemeente Wassenaar met verbonden partijen aangaat wordt aandacht besteed aan informatiebeveiliging. De verbonden partij moet aan kunnen tonen 'in control' te zijn over hun eigen ICT-huishouding.

Hiervoor leveren leveranciers van kritieke applicaties jaarlijks een Third Party Memorandum (TPM) over de kwaliteit van de ICT-dienstverlening en –beheersing van de organisatie.

Met vriendelijke groet,
het college van burgemeester en wethouders,

drs. H.I.P. Oppatja,
gemeentesecretaris

drs. L.A. de Lange,
burgemeester

Deze brief is digitaal vastgesteld. Hierdoor staat er geen fysieke handtekening in de brief.