REKENKAMERONDERZOEK

NAAR DE INFORMATIEBEVEILIGING IN DE GEMEENTE WESTLAND

JUNI 2019

Rekenkamercommissie Westland

Colofon

De Rekenkamercommissie Westland

De Rekenkamercommissie van de gemeente Westland (hierna: RKC Westland) is eind 2005 op grond van de Gemeentewet ingesteld. De RKC Westland bestaat uit drie externe leden (w.o. de voorzitter), dat wil zeggen leden die afkomstig zijn van buiten de gemeenteraad en twee interne leden. Zowel de externe als de interne leden zijn door de gemeenteraad benoemd. Daarnaast wordt de commissie ondersteund door een ambtelijk secretaris.

De RKC onderzoekt de doelmatigheid en de doeltreffendheid van het beheer van de organisatie en van het gevoerde beleid van het college. Bij doelmatigheid wordt met name onderzocht of het beleid tegen zo laag mogelijke kosten is uitgevoerd en bij doeltreffendheid of het gewenste effect is bereikt. Het werkterrein van de RKC Westland strekt zich uit over alle gemeentelijke organen en gelieerde instellingen. De leden van het college van B&W en de ambtenaren van de gemeente zijn verplicht informatie te verstrekken als de RKC Westland daarom vraagt. De RKC Westland formuleert op basis van de feiten die zij in haar onderzoeken heeft geconstateerd, conclusies en aanbevelingen. Zij legt dit alles, inclusief een eventuele reactie van het College van B&W en nawoord van de RKC hierop, vast in de vorm van onder meer rapporten of brieven, gericht aan de gemeenteraad. Het is aan de raad te besluiten al dan niet actie te ondernemen naar aanleiding van de uitkomsten van het onderzoek.

De RKC Westland is derhalve een 'instrument' van de raad dat erop gericht is de raadsleden te ondersteunen bij hun controlerende taak. De RKC heeft een onafhankelijke positie binnen de gemeente. De RKC bepaalt zelf welke onderzoeken zij zal instellen. Eventuele verzoeken voor het doen van onderzoek van (leden van) de gemeenteraad en/of burgers van de gemeente Westland, zal de RKC Westland beoordelen en indien passend binnen haar taken en bevoegdheden in het onderzoeksprogramma opnemen.

Samenstelling Rekenkamercommissie

De commissie bestaat uit de volgende leden:

Voorzitter	mevrouw drs. F.C. Buruma
Externe leden	de heer mr. N. Nijdam
	de heer A.W. Timmerman
Raadsleden	mevrouw P. Scheffers-van der Lelij
	de heer mr. P.J.L.J. Duijsens
Ambtelijk secretaris	de heer D. van Vliet

REKENKAMERCOMMISSIE
WESTLAND

Postadres:
Postbus 150
2670 AD Naaldwijk
Bezoekadres:
Laan van de Glazen Stad 1
2672 TA Naaldwijk
T 14 0174
F (0174) 673 600
E info@gemeentewestland.nl
I www.gemeentewestland.nl

Aan de Raad van de gemeente Westland
Postbus 150
2670 AD NAALDWIJK

UW BRIEF	UW KENMERK	ZAAK-/PROJECTNR.	DOCUMENTNR.	BIJLAGE(N)
			G19-001374	1

CONTACTPERSOON	CLUSTER	TELEFOONNUMMER	DATUM VERZONDEN
D. van Vliet	RKC	(0174) 673 038	05-06-2019

ONDERWERP
RKC-onderzoek informatiebeveiliging gemeente Westland

Geachte leden van de Raad,

De Rekenkamercommissie Westland (RKC) heeft het onderzoek naar de informatiebeveiliging in de gemeente Westland afgerond. Voor u ligt het eindrapport van dit onderzoek.

Het onderzoek
Het onderzoek is in de periode 6 februari 2019 t/m 19 februari 2019 uitgevoerd door onderzoeksbureau Hoffmann Cybersecurity uit Almere. Het onderzoeksteam bestond uit de heer Leander van Hoesel, de heer Michael Wessels en mevrouw Suzanne de Wilde. De werkgroep van de RKC bestond uit mevrouw Fiona Buruma (voorzitter RKC en lid-rapporteur van dit onderzoek), de heer André Timmerman (extern lid RKC) en de heer Dick van Vliet (secretaris RKC).

Het doel van het onderzoek is de volgende hoofdvraag te beantwoorden: "Hoe is het gesteld met de informatiebeveiliging van de gemeente Westland?". De conclusie naar aanleiding van dit onderzoek is dat de gemeente Westland een gedegen informatiebeveiligingsbeleid heeft, maar dat desondanks diverse kwetsbaarheden zijn ontdekt op de onderzochte aspecten. Met andere woorden er zijn verschillen geconstateerd tussen het beleid op papier en de implementatie daarvan in de praktijk. Op enkele punten was er sprake van een ernstig risico voor de gemeente, waarover de RKC de organisatie onverwijld heeft geïnformeerd, zodat lopende het onderzoek reeds de nodige maatregelen konden worden getroffen.

Het onderzoek heeft een lijst van concrete aanbevelingen opgeleverd en de RKC verzoekt de raad om deze over te nemen en de uitvoering ervan te volgen. De RKC wil de raad in overweging geven om over 6 tot 12 maanden een vervolgonderzoek ("*quick scan*") uit te voeren om na te gaan of de stand van de informatiebeveiliging van de gemeente Westland is verbeterd. De RKC is de raad hierbij graag van dienst.

Commissie- en raadsbehandeling
In de openbare raadscommissie Bestuur van 6 juni 2019 wordt het rapport officieel aangeboden. Vervolgens is het aan de raadscommissie wanneer het rapport inhoudelijk wordt behandeld.

Het rapport kent een openbare versie en een geheime versie. Artikel 185, lid 5, van de Gemeentewet bepaalt dat rapporten van de rekenkamer(commissie) openbaar zijn. Lid 1 van hetzelfde artikel bepaalt dat in het rapport niet worden opgenomen gegevens en bevindingen, die naar hun aard vertrouwelijk zijn. Om die reden is een openbare versie opgesteld, die geschoond is van vertrouwelijke gegevens en bevindingen. Deze versie zal officieel worden aangeboden aan de voorzitter van de raadscommissie Bestuur.

De geheime versie, met gedetailleerde bevindingen en aanbevelingen, wordt vervolgens digitaal onder geheimhouding aangeboden aan de raad. De geheime versie van het rapport kan dan vervolgens, zo daar behoefte aan is, worden behandeld in een besloten raadscommissie.

Bestuurlijk wederhoor

Het college heeft ervoor gekozen om de bestuurlijke reactie onder geheimhouding te verstrekken aan de RKC. De RKC respecteert deze beslissing en zal de reactie derhalve voegen bij de geheime versie van het rapport. Aangezien het een geheim stuk betreft kan de RKC in deze aanbiedingsbrief niet nader ingaan op de inhoud van de reactie. Wel wil de RKC aangegeven verheugd te zijn dat het college zich herkent in de bevindingen en aanbevelingen en dat reeds een actieplan is opgesteld en maatregelen zijn afgerond.

Tot slot

Ten slotte zegt de RKC de ambtelijke organisatie dank toe voor de open opstelling en de medewerking aan het onderzoek. Tevens dankt de RKC het college voor het tijdig toesturen van de bestuurlijke reactie, zodat het onderzoek binnen de planning voor het zomerreces van uw raad kan worden afgerond.

Hopende u hiermee te hebben gediend,

Hoogachtend,

F.C. Buruma
Voorzitter Rekenkamercommissie Westland

Openbaar

Informatiebeveiliging Gemeente Westland

Rapportage

Onderzoek Rekenkamercommissie

Classificatie:	*Openbaar*
Opdrachtgever:	Rekenkamercommissie gemeente Westland
Dossiernummer:	21901062
Datum:	05-06-2019
Versie:	1.5

Inhoudsopgave

1 Inleiding

In opdracht van de rekenkamercommissie gemeente Westland heeft Hoffmann Cybersecurity een onderzoek uitgevoerd. Daarbij was de hoofdvraag: "Hoe is het gesteld met de informatiebeveiliging van de gemeente Westland?"

De doelstelling van het onderzoek was om een gedegen beeld te geven van aanwezige kwetsbaarheden, de daarmee samenhangende risico's en om de concreet uitvoerbare verbetermogelijkheden in kaart te brengen. Dit rapport legt de nadruk op de geconstateerde kwetsbaarheden die tijdens het onderzoek naar het beveiligingsniveau van zowel de organisatie, de mens als de techniek (ICT) in kaart zijn gebracht. Doel van het onderzoek is dat dit een lerend effect heeft voor de organisatie.

Het onderzoek is uitgevoerd door Leander van Hoesel, Senior Security Consultant, Michael Wessels, Consultant Risk Management, en Suzanne de Wilde, Operationeel Manager Cybersecurity van Hoffmann. Van de zijde van de rekenkamercommissie Westland waren betrokken Fiona Buruma, André Timmerman en Dick van Vliet. Het onderzoek is uitgevoerd in de periode van 6 februari 2019 tot en met 19 februari 2019. Op 27 maart is het rapport uitgegaan voor ambtelijk wederhoor en vervolgens op 26 april voor bestuurlijk wederhoor. Op 6 juni 2019 is het eindrapport aangeboden aan de voorzitter van de Commissie Bestuur.

In Hoofdstuk 2 zijn de resultaten van het onderzoek samengevat. Vervolgens zijn in Hoofdstuk 3 de conclusies en aanbevelingen opgenomen. De informatie en bevindingen omtrent het onderzoek naar het informatiebeveiligingsbeleid en de uitgevoerde onderzoeksactiviteiten zijn terug te vinden in hoofdstuk 4 en 5. In verband met de vertrouwelijkheid van de uitkomsten rapporteert de rekenkamercommissie in het onderliggende openbare rapport (versie 1.5) op hoofdlijnen over de bevindingen, zodat deze geen houvast bieden voor kwaadwillenden. Het originele rapport (versie 1.4) is beschikbaar gesteld aan raads- en collegeleden.

Tijdens het onderzoek zijn meerdere kritieke kwetsbaarheden geconstateerd die onmiddellijk met ICT Beheer zijn gedeeld. Deze zijn direct voortvarend opgepakt, waarmee het risico door de gemeente is weggenomen. Vanwege de verwachte doorlooptijd die nodig is om de overige geconstateerde kwetsbaarheden in de ICT-omgeving op te kunnen lossen, is direct na het einde van het onderzoek een (vertrouwelijke) bijlage met detailbevindingen van het technische onderzoek gedeeld met de ICT-afdeling na oplevering van de rapportage. Hiermee wordt de organisatie in staat gesteld de prioriteiten en uitvoering voor het oplossen

van de kwetsbaarheden te onderzoeken en te plannen en daarmee het risico voor de gemeente Westland al tijdens het lopende proces van hoor en wederhoor weg te nemen.

Wij danken de ambtelijke organisatie voor de flexibiliteit en medewerking tijdens het onderzoek. Hierdoor konden wij dit volgens planning afronden.

2 Managementsamenvatting

De rekenkamercommissie Westland heeft Hoffmann ('de onderzoeker') gevraagd een onderzoek uit te voeren naar de informatiebeveiliging in de gemeente Westland. Om een gedegen beeld te krijgen van de aanwezige kwetsbaarheden is tijdens het onderzoek het beveiligingsniveau van zowel de organisatie, de mens als de techniek (ICT) onderzocht. Op basis van de bevindingen zijn de daarmee samenhangende risico's en de concreet uitvoerbare verbetermogelijkheden (aanbevelingen) in kaart gebracht.

Het onderzoek naar de organisatie van de informatiebeveiliging had tot doel na te gaan of de gemeente Westland de belangrijkste risico's in beeld heeft, hoe het vigerende informatiebeveiligingsbeleid binnen de organisatie wordt toegepast en of de beveiligingsmaatregelen door de organisatie worden nageleefd. Tijdens het technische onderzoek is getoetst of de informatiesystemen van de gemeente voldoende beveiligd zijn tegen het risico van hacken. Hackers van Hoffmann Cybersecurity hebben de informatiebeveiliging zowel getest vanaf het internet (externe penetratietest) als vanuit het gemeentehuis (interne penetratietest). Het bewustzijn van de medewerkers is getest door middel van *mail phishing*, waarbij er een mail is verstuurd die uitnodigde op een link te klikken en de gebruiker te verleiden om persoonlijke inloggegevens af te geven. Ook is een fysieke inlooptest gedaan. Hierbij heeft een medewerker van Hoffmann geprobeerd om zonder toestemming binnen te komen in het gemeentehuis.

Organisatie

In 2018 hebben, mede ingegeven door de inwerkingtreding van de AVG[1], verschillende activiteiten plaatsgevonden gericht op het actualiseren van het informatiebeveiligingsbeleid. Het beleid is volledig en van goede kwaliteit. De medewerkers die de driehoek gegevensbescherming[2] vertegenwoordigen zijn kundig en gedreven om de in het beleid beschreven technische en organisatorische maatregelen te (laten) implementeren binnen de organisatie. De constatering is dat zowel de opzet als het bestaan van procedures en beveiligingsmaatregelen voldoende zijn uitgewerkt, en dat wordt voldaan aan de wettelijke verplichtingen ten aanzien van informatiebeveiliging voor gemeenten. Echter de uitvoerigheid van het beleid vertaalt zich niet door in de daadwerkelijke implementatie van alle maatregelen, een actuele implementatiestatus noch in monitoring op de werking van de beveiligings-maatregelen. Daarmee is de effectiviteit van het beleid onvoldoende.

[1] AVG: Sinds 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat in de hele Europese Unie (EU) dezelfde privacywetgeving geldt. De Wet bescherming persoonsgegevens (Wbp) geldt niet meer.
[2] Driehoek gegevensbescherming: Zie ook §4.2: CISO, Privacy Officer, Functionaris Gegevensbescherming.

Externe penetratietest

Tijdens het testen vanaf het internet bleek het mogelijk om ongeautoriseerde toegang te krijgen tot apparatuur. Er is een verouderd besturingssysteem en verouderde software aangetroffen op netwerkapparatuur. Tot slot bleek de basisbeveiliging en '*hardening*[3]' van enkele met internet verbonden systemen niet op orde, waardoor deze systemen onvoldoende beveiligd zijn tegen aanvallen vanaf het internet.

Interne penetratietest

Om de kwetsbare systemen in kaart te brengen zijn de onderzoekers van Hoffmann gestart met het uitvoeren van een geautomatiseerde scan. Tegelijkertijd is in overleg tussen de beheerders en de onderzoekers van Hoffmann afgestemd om na detectie door te gaan met testen om te waarborgen dat er geen kwetsbaarheden buiten schot zouden blijven. Er zijn besturingssystemen en software aangetroffen die niet meer worden ondersteund door de leverancier en waarvoor geen beveiligingsupdates meer beschikbaar komen. Hierdoor blijven systemen kwetsbaar zolang deze niet worden vervangen of uitgefaseerd.

De penetratietesten die wij uitvoeren voor gemeenten en vergelijkbare organisaties zijn verschillend in die zin dat de scope van de IT-omgeving, de wijze waarop beheer is ingericht en de mate waarin werkzaamheden zijn belegd bij externe partijen niet eenvoudig te vergelijken zijn. Als we de aard van de bevindingen van de gemeente Westland en de bijbehorende risico's en mogelijke impact afzetten tegen bevindingen in andere onderzoeken zijn deze enigszins ernstiger van aard. De technische kwetsbaarheden die onze onderzoekers hebben geconstateerd had de gemeente Westland eerder kunnen constateren wanneer er, conform het beleid, gedegen periodiek onderzoek naar was gedaan. Door beperkte middelen en capaciteit is het uitvoeren van security taken als onderdeel van het ICT-beheer onvoldoende ingeregeld, waar bij andere gemeenten security vaak integraal onderdeel is van, en belegd binnen, de ICT beheertaken.

Fysieke penetratietest (inlooptest)

Een inlooptest is gericht op de fysieke beveiliging van een organisatie door deze binnen te treden met als doel toegang te krijgen tot vertrouwelijke informatie. Het bleek op beide locaties van de gemeente Westland mogelijk om ongeautoriseerde toegang te krijgen.

[3] Hardening is het proces waarbij overbodige functies in besturingssystemen uitgeschakeld worden en/of van het systeem verwijderd worden. En daarnaast door zodanige waarden toekennen aan beveiligingsinstellingen dat hiermee de mogelijkheden om een systeem te compromitteren worden verlaagd en een maximale veiligheid ontstaat.

Social Engineering – mail phishing

Met het versturen van een phishing mail is het bewustzijn van de medewerkers ten aanzien van het herkennen van een nep-mail getoetst. De bevindingen zijn vergelijkbaar met andere gemeenten waar dit scenario is toegepast, maar laten tegelijkertijd zien dat medewerkers gevoelig zijn voor dergelijke aanvallen.

3 Conclusies en aanbevelingen

Het onderzoek dat Hoffmann Cybersecurity in opdracht van de rekenkamercommissie heeft uitgevoerd had als doel de volgende hoofdvraag te beantwoorden: "Hoe is het gesteld met de informatiebeveiliging van de gemeente Westland?"

3.1 Conclusies

De conclusie naar aanleiding van dit onderzoek is dat de gemeente Westland een gedegen informatiebeveiligingsbeleid heeft, de medewerkers die informatiebeveiliging in hun takenpakket hebben, deze taak serieus nemen en zich volledig inspannen om het niveau van informatiebeveiliging binnen de gemeente te verhogen. Desondanks hebben de onderzoekers van Hoffmann op alle onderzochte aspecten kwetsbaarheden ontdekt.

De belangrijkste conclusie ten aanzien van de organisatie van informatiebeveiliging is dat, hoewel er zeer consequent wordt voldaan aan alle wettelijke verplichtingen, de naleving van het eigen informatiebeveiligingsbeleid beter uitgevoerd en gecontroleerd moet worden. Het beleid is niet verankerd in de bedrijfsvoering en niet aantoonbaar effectief. Er is in de praktijk te weinig prioriteit, of wellicht capaciteit, om alle in het beleid beschreven beveiligings-maatregelen, zowel op organisatorisch als technisch vlak, uit te voeren.

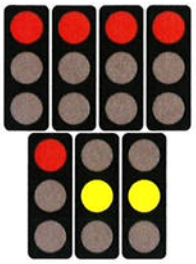
De technische kwetsbaarheden waren eerder aan het licht gekomen wanneer daar eerder, conform het beleid, gedegen periodiek onderzoek naar was gedaan. Door beperkte middelen en capaciteit is het uitvoeren van security taken als onderdeel van het ICT-beheer onvoldoende ingeregeld, waar bij andere gemeenten security vaak integraal onderdeel is van, en belegd binnen, de ICT beheertaken door Security engineers.

De mail-phishing test heeft laten zien dat het bewustzijn van de medewerkers vergelijkbaar is met dat van andere gemeenten. Tijdens de fysieke penetratietest is vastgesteld dat de nieuwe kantoorlocaties en de flexwerkplekken met afsluitbare kasten er toe leiden dat er relatief weinig vertrouwelijk informatie voorhanden is wanneer iemand zich ongeoorloofd toegang verschaft. Het is belangrijk hier voldoende aandacht aan te blijven besteden om de beveiliging van informatie en medewerkers te kunnen waarborgen.

3.2 Aanbevelingen

Om het beveiligingsniveau te vergroten adviseren wij de gemeente de voorgestelde aanbevelingen over te nemen en waar mogelijk uit te voeren. Om de gemeenteraad zoveel mogelijk van dienst te zijn, heeft de rekenkamercommissie een concept raadsbesluit opgesteld, deze is bijgevoegd als bijlage 6.3. De bevindingen en aanbevelingen worden hierna samengevat. Voor inhoudelijke achtergrondinformatie verwijzen wij naar hoofdstuk 4 en 5.

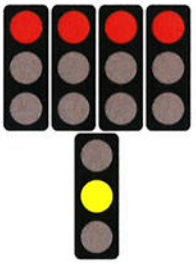
Onderzoek organisatie van informatiebeveiliging



Tijdens dit onderzoek is documentatie ('*evidence*') opgevraagd en is met verschillende medewerkers gesproken voor een toelichting op het opgevraagde materiaal.

Het onderzoek leidde in dit deel van het rapport tot een zevental bevindingen (vijfmaal risico hoog en tweemaal risico gemiddeld).

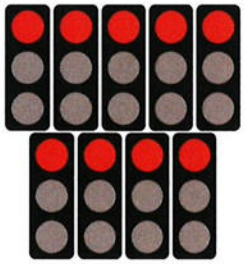
Externe penetratietest



De onderzoekers hebben de externe penetratietest uitgevoerd vanaf het Internet. Hierbij zijn zij zelf op zoek gegaan naar systeemnamen en netwerkcomponenten van de gemeente Westland. De uiteindelijke reikwijdte is in overleg afgestemd met de gemeente.

Het onderzoek leidde in dit deel van het rapport tot een vijftal bevindingen (viermaal risico hoog eenmaal risico gemiddeld).

Interne penetratietest



Tijdens de interne testen hebben de onderzoekers tests uitgevoerd op een flex-werkplek van de gemeente Westland. Vervolgens zijn verschillende kwetsbaarhedenscans uitgevoerd en pogingen ondernomen om de aangetroffen kwetsbaarheden handmatig te misbruiken.

Het onderzoek leidde in dit deel van het rapport tot een negental bevindingen (risico hoog).

Fysieke penetratietest

Een onderzoeker heeft een 'inlooptest' ofwel 'fysieke penetratietest' uitgevoerd als 'mystery guest' met als doet te testen of het mogelijk is om op ongeautoriseerde wijze toegang tot het pand te verkrijgen en gevoelige informatie of systemen te bereiken.

Het onderzoek leidde tot één bevinding (risico hoog).

Social Engineering – Mail phishing

Social engineering is een techniek waarbij een computerkraker een aanval op computersystemen onderneemt door de zwakste schakel in de computerbeveiliging, namelijk de mens, te kraken. Social engineering bestaat uit verschillende aanvalstechnieken om mensen te misleiden om toegang te krijgen tot gevoelige informatie, een methode daarvoor is phishing. Er is een phishing e-mail verstuurd om gebruikers te verleiden in te loggen op een legitiem ogende phishing website. Volgens het beleid van de gemeente Westland moeten medewerkers dergelijke mails melden.

Het onderzoek leidde tot één bevinding (risico hoog).

4 Organisatie van de informatiebeveiliging

Hoffmann Cybersecurity heeft in het onderzoek naar de organisatie van informatiebeveiliging en het informatiebeveiligingsbeleid gekeken naar de volgende drie aspecten:

1. Opzet: zijn beleid, processen en procedures van informatiebeveiliging beschreven?
2. Bestaan: worden processen in de praktijk doorlopen?
3. Werking: werken de processen zoals deze bedoeld zijn?

Waarbij voor een deel in de antwoorden is voorzien door beschikbare "*evidence*" in de vorm van documentatie, rapporten en verklaringen, is daarnaast met verschillende medewerkers gesproken voor een toelichting op het gevraagde materiaal.
Nagenoeg alle gevraagde documentatie is door de gemeente Westland aangeleverd aan de onderzoeker. Een overzicht hiervan is toegevoegd in bijlage 6.1. De ambtelijke organisatie heeft op constructieve wijze haar medewerking verleend aan dit onderzoek.

Onderzoek informatiebeveiligingsbeleid

4.1 Afbakening

Met betrekking tot de afbakening van dit onderzoek is het relevant dat de onderzoeker beoogt na te gaan of de gemeente Westland de belangrijkste risico's (met in potentie de grootste impact) in beeld heeft, hoe het vigerende informatiebeveiligingsbeleid binnen de organisatie wordt toegepast en of de beveiligingsmaatregelen door de organisatie worden nageleefd.

4.2 Aanpak

Tijdens het onderzoek zijn documenten ('*evidence*') opgevraagd, de ontvangen en onderzochte documenten zijn bijgevoegd als bijlage 6.1. Vervolgens is met onderstaande functionarissen, allen werknemer van de gemeente Westland, gesproken voor een toelichting op het opgevraagde materiaal.

Functie	Datum interview
Clusterdirecteur Bedrijfsvoering	7-2-2019
Organisatie ontwikkelaar	7-2-2019
Team manager I&A	5-2-2019
Medewerker CISO	5-2-2019
Medewerker CISO	5-2-2019
Functionaris Gegevensbescherming	5-2-2019
Privacy Officer	5-2-2019

4.3 Bevindingen

Het startpunt voor het onderzoek naar informatiebeveiliging is het beleid. Dit is in 2018 herzien en op 4-2-2019 opnieuw vastgesteld door het College van B&W en verstuurd aan de gemeenteraad.

Het informatiebeveiligingsbeleid beschrijft de volgende PDCA-cyclus die jaarlijks doorlopen moet worden om borging van het beleid en daarvan afgeleide plannen te realiseren:

1. ***Informatiebeveiligingsbeleid***
   Bevat het beleid en de visie op informatiebeveiliging. Bijstelling van het informatiebeveiligingsbeleid vindt plaats om de 3 jaar of bij grote wijzigingen.
2. ***Informatiebeveiligingsanalyse***
   a) De risicoanalyse en de GAP-analyse (de toets aan de praktijk) op basis van het informatiebeveiligingsbeleid en de normen die hier in zijn vermeld of de normen waar in het beleid naar wordt gerefereerd.
   b) Jaarlijks wordt een zelfevaluatie uitgevoerd, georganiseerd door de Rijksoverheid. Via deze ENSIA-methode wordt de gemeente bevraagd op getroffen maatregelen ten aanzien van informatiebeveiliging. Een selectie van normen uit de BIG wordt getoetst middels een zelfevaluatie; daarnaast wordt van de gemeente een verantwoording gevraagd over aangewezen normenkaders. Het college legt vervolgens met een collegeverklaring verantwoording af aan het Rijk en de gemeenteraad over de mate van voldoen aan deze aangewezen normenkaders.
3. ***Verbeterplan***
   Het verbeterplan bevat de concrete verbeteracties volgend uit de risicoanalyse, GAP –analyse en de ENSIA-zelfevaluatie. Dit verbeterplan wordt periodiek geëvalueerd en waar nodig bijgesteld. Over de uitvoering van het verbeterplan wordt aan het bestuur en voor wat betreft de verbeteracties voortvloeiend uit ENSIA aan de toezichthoudende instanties gerapporteerd. Tijdens het onderzoek heeft Hoffmann het verbeterplan 2017 ontvangen, maar deze is niet meer actueel. Vervolgens is het verbeterplan 2018 ontvangen, deze moest ten tijde van het onderzoek nog worden vastgesteld door het Directieteam. Het verbeterplan bevat geen maatregelen voor de behandeling van geconstateerde kwetsbaarheden tijdens dit onderzoek.

De verantwoordelijkheid voor informatiebeveiliging is belegd bij de Directeur Bedrijfsvoering (D-BV) die samen met het directieteam (DT) het gewenste niveau van informatiebeveiliging vaststelt voor de gemeente. De beveiligingseisen worden per bedrijfsproces vastgesteld.

De D-BV is verantwoordelijk voor de juiste implementatie van het IB-niveau in de bedrijfsprocessen en wijst daarvoor een verantwoordelijke aan (Procesverantwoordelijke). Ondersteunend aan de processen zijn de in- en externe (informatie)systemen en ook hiervoor wijst de D-BV een verantwoordelijke aan (applicatie- of systeemeigenaar). De Teammanager I&A[4] is verantwoordelijk voor bijv. alle generieke systemen van de kantoorautomatisering. Als uit risicoanalyses blijkt dat voor bepaalde gegevens verwerkingen of omstandigheden meer of andere maatregelen nodig zijn dan de maatregelen die in de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) zijn beschreven moeten door de daarvoor verantwoordelijke proces- of systeemeigenaar aanvullende maatregelen worden getroffen.

Informatiebeveiligingsbeleid

Opzet en bestaan van het informatiebeveiligingsbeleid is goed. De verantwoordingsdocumentatie gaat over 2017 (ENSIA), omdat het proces voor 2018 nog niet is afgerond. Wel is alle IB-documentatie in 2018 herzien. De in het beleid beschreven PDCA-cyclus is gevolgd, er is een RI&E-analyse aanwezig en een verbeterplan voor 2017. Er heeft in 2018 een GAP-analyse plaatsgevonden die in oktober is aangeboden aan het DT ter besluitvorming, echter deze besluitvorming heeft ten tijde van deze rapportage nog niet plaatsgevonden (gepland maart 2019) De eerdere GAP-analyse bevatte 127 maatregelen, maar omdat een groot deel hiervan fysiek was en de 2 nieuwe panden zijn betrokken is hier geen nadere invulling aan gegeven. Na de goedkeuring van de GAP-analyse in het DT wordt er een nieuw verbeterplan opgesteld.

Het is niet inzichtelijk wat de status is van de maatregelen die staan opgesomd in sommige hoofdstukken van het beleid: opzet, bestaan of werking. Van de adequate werking van maatregelen is geen verantwoordingsinformatie aangetroffen. Het beleid is daarmee niet verankerd in de bedrijfsvoering en niet aantoonbaar effectief.

Informatiebeveiligingsanalyse

Het uitvoeren van een gemeente brede risicoanalyse vindt jaarlijks plaats. Deze RIE wordt verzorgd door een extern onafhankelijke partij (met aandacht voor het verplichte BRP en PNIK gedeelte). Daarnaast is er intern een GAP analyse opgesteld van de BIG maatregelen, voor 2018 moet deze nog worden vastgesteld en goedgekeurd in het DT.

[4] I&A: Informatievoorziening en Automatisering

Verder is in het informatiebeveiligingsbeleid bepaald dat als uit risicoanalyses blijkt dat voor bepaalde gegevens verwerkingen of omstandigheden meer of andere maatregelen nodig zijn dan beschreven in de BIG, door de daarvoor verantwoordelijke proces- of systeemeigenaar aanvullende maatregelen moet worden getroffen. Het uitvoeren van risicoanalyses zou volgens de BIG een standaard onderdeel moeten zijn van informatiebeveiliging door gemeenten. Zo zou het lijnmanagement op basis van een expliciete risicoafweging betrouwbaarheidseisen voor zijn informatiesystemen moeten vaststellen. Op basis van deze betrouwbaarheidseisen kunnen de te nemen beveiligingsmaatregelen worden bepaald.
De manier waarop de risicoanalyses moeten worden uitgevoerd is niet beschreven in het informatiebeveiligingsbeleid of aanvullende documenten. Het risico bestaat dat het informatiebeveiligingsbeleid niet als *'risk-based'* (gebaseerd op risico's) maar als *'compliance-based'* (gericht op naleving) wordt omschreven. Het gevaar van deze benadering is dat de capaciteit voor informatieveiligheid ineffectief wordt ingezet, zonder rekening te houden met daadwerkelijke risico's.

Verbeterplan

De onderzoeker constateert dat het uitvoeren van risicoanalyses geen wezenlijk onderdeel is van de informatiebeveiligingsplannen, omdat er niet aantoonbaar risicoanalyses per applicatie of proces zijn uitgevoerd. Wel zijn alle applicaties geclassificeerd, zodat inzichtelijk is welke applicaties kritiek zijn voor de bedrijfsvoering en welke minder kritiek. Voor deze applicaties is niet aantoonbaar ingeschat of het beveiligingsniveau van de BIG volstaat, of dat extra beveiligingsmaatregelen moeten worden getroffen. In de praktijk lijkt de gemeente voorrang te geven aan de invoering van de minimummaatregelen uit de BIG.
Het verbeterplan 2018 is gebaseerd op de activiteiten die in 2018 zijn uitgevoerd naar aanleiding van de wettelijke verplichtingen t.a.v. de BIG/ENSIA en staat geagendeerd ter goedkeuring in een DT-overleg in maart 2019.

Sturing

De D-BV herkent haar verantwoordelijkheid ten aanzien van de IB en is zich bewust van het feit dat het informatiebeveiligingsbeleid nog niet volledig is geïmplementeerd in de processen. De organisatie is onderhevig aan veranderingen en groeit hard. Om een toekomstvaste informatiebeveiliging in te regelen is het voornemen om de organisatie uit te breiden met aanvullende Information Security Officers (ISO) per cluster. Deze ISO's moeten het lijnmanagement gaan ondersteunen met de implementatie van en controle op de in het IB-beleid voorgeschreven beveiligingsmaatregelen. Cruciaal is dat deze medewerkers een

gedegen kennis hebben van informatiebeveiliging om hier invulling aan te kunnen geven. Onderdeel daarvan is ook de start van een bewustwordingscampagne.
Er vindt maandelijks overleg plaats tussen de CISO's en de Team(manager) I&A. Dit om een betere aansluiting van de informatiebeveiligingsmaatregelen te bewerkstelligen in het IT-domein. Vooralsnog is de samenwerking gebaseerd op advies en controle, maar ontbreekt het aan de juiste handvatten en afspraken om prioriteiten te stellen, en de IB op een adequate manier te kunnen inrichten. Er is in de praktijk te weinig prioriteit, of wellicht capaciteit, voor de implementatie van het vigerende IB-beleid en de controle op de naleving.

Naleving

Controle op naleving van het beleid ontbreekt, maar zou volgens het informatiebeveiligingsbeleid moeten plaatsvinden o.b.v. het *3 Lines of Defense model* (3LoD): lijnmanagement, (systeem)beheer en de security officers.
Volgens de procesbeschrijving "DEF 15 Naleving 12-10-18 14-13" uit het IB-beleid zou rapportage over de naleving moeten plaatsvinden over de volgende onderwerpen:

- HRM
- Fysieke Beveiliging
- Processen
- ICT
- Wettelijke verplichtingen

In de laatste kwartaalrapportages aan B&W worden deze onderwerpen, met uitzondering van alle activiteiten ten aanzien van de wettelijke verplichtingen niet benoemd.
Belangrijk in het kader van aanmerken hoe kwetsbaar de organisatie is om te rapporteren over de feitelijke stand van zaken en niet op basis van informatie die generiek beschikbaar is en onvoldoende weergeeft hoe de gemeente Westland er als organisatie voor staat.

HRM

Volgens het informatiebeveiligingsbeleid moeten controles ten aanzien van HR controles plaatsvinden op de volgende aspecten:

- Het werving- en selectieproces van nieuwe medewerkers waarin geborgd moet zijn dat nieuwe medewerkers niet zonder enige controle op betrouwbaarheid worden aangenomen.
- Personeelsmutaties leiden tot handelingen. Deze kunnen betrekking hebben op het uitreiken of innemen van verstrekte items en bevoegdheden. Het HRM proces is de trigger voor het proces en de procedures dienen zodanig te zijn dat op het gebied van facilitaire zaken en ICT de activiteiten worden uitgevoerd. Op dit gebied is het van

belang dat periodiek de rechten op het netwerk en binnen de systemen worden gecontroleerd.
- De verstrekking en vastlegging van middelen (telefoons, tablets, laptops etc.) en de gedrags- en gebruikersprotocollen hieromtrent.
- Het meten van het beveiligingsbewustzijn van de medewerkers.

Periodiek dient er gecontroleerd te worden op in- en uitstroom van medewerkers ten behoeve van de autorisaties op applicaties. Hiervoor is een uitvraagprocedure beschikbaar. Er vindt niet aantoonbaar door iedere applicatie- en proceseigenaar een controle op de autorisaties plaats. Manager I&A geeft aan dit wel te doen voor de generieke applicaties.
Er zijn ten tijde van de AVG-implementatie verschillende berichten geplaatst op het Intranet om de medewerkers te informeren. Er vindt een registratie plaats van incidenten en hier is naar aanleiding van de communicatie over de AVG-verplichting een toename in het aantal meldingen geconstateerd. Het aantal datalekken wat de gemeente heeft moeten melden is echter beperkt.

Fysieke Beveiliging

Onder de fysieke beveiliging valt uiteraard het gebouw en de aangebrachte veiligheidsvoorzieningen maar daarnaast ook een controle op de houding en gedrag van de medewerkers in deze. Zo zijn er gedragsregels en moet er volgens het beleid periodiek gecontroleerd worden op de '*clear screen*' en de '*clean desk*' afspraken. Zou er tweejaarlijks een fysieke inspectie van het gebouw moeten plaatsvinden en een controle op openstaande risico's, deze controle moet vanwege de verhuizing naar de nieuwbouw locaties opnieuw ingericht worden. De verantwoordelijkheid is grotendeels belegd bij "de Groene Schakel". Er zijn aantoonbaar groepen ten behoeve van de fysieke toegangsbeveiliging vastgelegd.
In het beleid is bijvoorbeeld opgenomen dat bezoekers na aanmelding bij de receptie een bezoekersbadge krijgen en dat de bezoekers te allen tijde door een medewerker van de gemeente onder begeleiding staan. Tijdens het bezoek van de onderzoeker van Hoffmann werd dit beleid niet gehandhaafd.

Processen

Een ISMS (Information Security Management Systeem) is noodzakelijk om de verschillende activiteiten te kunnen beheren en onderhouden. De gemeente Westland gebruikt hiervoor een Excel, dit is toereikend. In overleg met andere gemeente wordt al enkele jaren onderzoek gedaan naar een geschikte tool maar die is nog niet gevonden.

ICT

Het Taakveld I&A van de gemeente Westland, waarvan systeembeheer deel uitmaakt, beheert de werkplekken, serverplatformen, lokale netwerken, wifi -verbindingen, externe netwerkverbindingen en verzorgt het technische en functionele (wijziging)beheer van databases, bedrijfsapplicaties en kantoorautomatiseringshulpmiddelen. Verder is de afdeling medeverantwoordelijk voor alle technische aansluitingen op andere ketenpartners en landelijke voorzieningen. De Taakveldverantwoordelijke I&A is tevens verantwoordelijk voor de implementatie van ICT - technische beveiligingsmaatregelen. Door I&A wordt verantwoording over de getroffen beveiligingsmaatregelen aan de procesverantwoordelijken en systeemeigenaren afgelegd.

De applicaties zijn, conform beleid, allemaal geregistreerd en toegewezen en gekoppeld aan een verantwoordelijk cluster. De betreffende directeur van het cluster is dus eindverantwoordelijk. De applicaties zijn gewaardeerd en geclassificeerd op BIV (Beschikbaarheid, Integriteit en Vertrouwelijkheid) van de informatie in de applicaties.

Slechts op de applicaties waarvoor dit wettelijk is verplicht voert de IT-afdeling maandelijks een beperkte kwetsbaarhedenscan uit, voor deze applicaties is tegelijkertijd patch management ingericht. Het blijkt uit de rapportage niet of dit adequaat en structureel gebeurt, waardoor het niet mogelijk is vast te stellen hoe kwetsbaar de ICT-omgeving van de gemeente Westland is op basis van een continu proces.

Conform het beleid zou er jaarlijks een penetratietest op de ICT omgeving moeten worden uitgevoerd en daarnaast een onderzoek plaatsvinden naar de implementatie van de security baselines. Deze controles vinden niet aantoonbaar plaats, waardoor het niet mogelijk is aan te geven hoe kwetsbaar de ICT-omgeving is voor dreigingen van buitenaf.

Om de ICT omgeving te beschermen tegen dreigingen van buitenaf schrijft het beleid voor dat er maatregelen getroffen moeten zijn om deze te detecteren en vervolgens hiervoor *logging* en *monitoring* in te richten zodat deze gegevens gebruikt kunnen worden voor nader onderzoek naar misbruik. Er vindt *logging* plaats op sommige kritieke applicaties en op de logische toegangsbeveiliging van de KA, maar dit is niet voor alle systemen ingericht.

De gemeente maakt gebruik van systemen die het mogelijk maken op beveiligde wijze (grote) bestanden uit te wisselen.

Er is beleid opgesteld ten aanzien van afspraken met leveranciers over de informatiebeveiliging, en hoe proces- en applicatie eigenaren moeten toezien op de naleving van deze afspraken. In de praktijk blijkt dit discussie op te leveren, vooral wanneer bepaalde (ICT)middelen door meerdere afdelingen worden gebruikt.

Sinds het ingaan van de AVG (28 mei 2018) zijn in de nieuwe afgesloten contracten afspraken gemaakt met leveranciers door middel van het afsluiten van bewerkersovereenkomsten (format VNG). Vastgelegd is waar dit nog niet het geval is en hier vindt controle en bewaking op plaats. Met verschillende leveranciers lopen contracten al tientallen jaren, deze zijn allemaal in beeld en wanneer daar persoonsgegevens mee worden uitgewisseld is dat vastgelegd inclusief de status van de overeenkomst.

Er worden aansluitvoorwaarden opgesteld bijv. voor het door leveranciers uitvoeren van onderhoud op ICT-systemen, zodat er veilige verbindingen kunnen worden afgedwongen. Centric en SIM zijn cruciale leveranciers en leveren een groot deel van de applicaties (Centric) of spelen een rol in de uitwisseling van informatie tussen bijvoorbeeld de websites waar burgers aanvragen kunnen doen en de systemen van de gemeente. Zij voeren generiek voor haar klanten controles uit t.b.v. de wettelijke audits en behandeling van kwetsbaarheden en geven hier ook Assurance over. Tevens zijn er met Centric afspraken gemaakt en werkprocedures opgesteld voor uitwijkvoorzieningen mocht dit onverhoopt nodig zijn.

Wettelijke verplichtingen

Voor zover inzichtelijk worden alle wettelijke verplichtingen ten aanzien van ENSIA, BIG en DigiD nagekomen. Waarbij aangetekend dat de onafhankelijke auditor hier ook heeft aangemerkt dat opzet en bestaan voldoende zijn en er geen nader onderzoek heeft plaatsgevonden naar de daadwerkelijke werking van de controles en de effectiviteit van alle beveiligingsmaatregelen.

5 Penetratietesten

De (werking van) de informatiebeveiliging is onderzocht met behulp van penetratietesten:

- ✓ Een externe penetratietest gericht op de vanaf internet benaderbare systemen
- ✓ Een interne penetratietest gericht op de interne bekabelde/draadloze netwerken
- ✓ Een fysieke penetratietest (inlooptest)
- ✓ Social Engineering (phishing e-mail en website)

De penetratietesten hebben plaatsgevonden in de periode van 6 februari tot en met 19 februari 2019.

Tijdens de penetratietesten zijn diverse kwetsbaarheden gevonden. De detailbevindingen en specifieke aanbevolen maatregelen van de externe penetratietest, de interne penetratietest en de fysieke penetratietest zijn beschreven in een separaat ter beschikking gesteld document. Om te voorkomen dat kwaadwillenden de geconstateerde kwetsbaarheden kunnen misbruiken is dit document als geheim aangemerkt en alleen gedeeld met de ICT-afdeling. Dit geldt tevens voor de onder Bijlage 6.2 genoemde documenten.

Wij adviseren om de aanbevolen maatregelen te implementeren.

6 Bijlagen

6.1 Overzicht bestudeerde documenten

Ontvangen documenten	
IB-Beleid	
1	Informatiebeveiligingsbeleid 2018-2021 18-0251091_S_18-0251091_14
2	Informatiebeveiligingsorganisatie 2018-2021 18-0252872_S_18-0252872_2
3	Getekende stukken inzake voorstel tot vaststelling van de Kadernota
4	gedragslijnen matrix_S_18-0273160_3[1]
5	Kadernota Uitgangspunten Privacy beleid V1.0 PvT_S_18-0077745_3[1]
6	Privacyreglement en gedragslijnen_S_18-0077764_1[1]
7	Beleid PIA 18-0148334 V3_S_18-0148334_2[1]
8	Beleidsnota informatiebeveiligingsbeleid 2018-2021
9	collegebrief d.d. 4-2-19 inzake informatiebeveiligingsbeleid 2018-2021
10	DEF 7 Beheer van bedrijfsmiddelen
11	DEF 8 Personele beveiliging
12	DEF 9 Fysieke beveiliging en beveiliging van de omgeving
13	DEF 10 Beheer van communicatie en bedieningsprocessen
14	DEF 11 Toegangsbeveiliging
15	DEF 12 Verwerving, ontwikkeling en onderhoud van informatiesystemen
16	DEF 13 Beheer van informatiebeveiligingsincidenten
17	DEF 14 Bedrijfscontinuiteitsbeheer
18	DEF 15 Naleving
IB-Rapportages	
19	KGB 2018-Q3 18-0253676_add_S_18-0253676_8
20	KRIB 1e kwartaal 2018_S_18-0089598_6
21	KRIB 2e kwartaal 2018 18-0178466_3_S_18-0178466_7
22	Rapportage-Zelfevaluatie-Informatieveiligheid--Westland-20180426132541
23	Verantwoordingsrapportage BAG ENSIA 2017_S_18-0051317_8
24	Verantwoordingsrapportage BGT ENSIA 2017_S_18-0051330_5
25	RIE 2017 WL_S_18-0051346_1
26	Uittreksel B&W besluit
27	Verbeterplan GW 2017
28	Verbeterplan GW
29	Verbeterplan
30	Rapportage-Zelfevaluatie-Informatieveiligheid--Westland-20180426132541
31	Overzicht security incidenten (benoemd in Q-rappportages; geen overzicht ontvangen)
32	Overzicht datalekken (benoemd in Q-rapportage; geen overzicht ontvangen)
Audits	
33	20180712 DBA GEM-WL Her-audit DigiD Centric [LOGIUS] TV01, WA02 411738,
34	20180712 DBA GEM-WL Her-audit DigiD SIM [LOGIUS] TV01, WA02, PW03 1002033,
35	20180918 DBA GEM-WL Her-audit DigiD Centric [LOGIUS] NW06 411738,
36	20180918 DBA GEM-WL Her-audit DigiD SIM [LOGIUS] NW06 1002033,
37	i984.100023_6224 collegeverklaring 2017

38	i984.100024_6224_assurancerapport_it_auditor
39	i984.100032_6224_digid1tpm1
40	i984.100036_6224_digid2tpm1
41	i984.101870_6224_ensia_zelfevaluatie_digid_assessment_2017_bijlage_b_c
42	i984.102354_6224_aansluiting_2_ensia_zelfevaluatie_digid_assessment_2017_bijlage_b_c
Fysiek	
43	Overzicht van de toegangsgroepen Verdilaan en Laan vd Glazenstad
I&A	
44	Data Classificatie
45	FW Actuele (uitgebreide) lijst Domeinen en subdomeinen
46	overzicht applicaties
47	Uitwijk draaiboek WL - AUG2018.pdf
48	uitwijkregeling Centric (Factuur)
49	uitwijkregeling Centric (Offerte)
Niet ontvangen documenten	
50	Auditrapportage, Logische toegang (risicovolle applicaties die persoonsgegevens opslaan en bewerken)
51	(Audit)rapportage t.a.v. Fysieke beveiliging van de gebouwen

6.2 Overzicht geheime bijlagen

De volgende documenten vormen input voor de ICT-afdeling om de aangetroffen kwetsbaarheden te verhelpen.

- ✓ *1901062 technische bevindingen en aanbevelingen penetratietest*
- ✓ *2190162_extern.xlsx* (resultaten externe kwetsbaarhedenscan)
- ✓ *2190162_intern.xlsx* (resultaten interne kwetsbaarhedenscan)

Deze documenten zijn op veilige wijze overhandigd aan de relevante ambtenaren. Gezien de aard van de informatie dienen deze documenten als geheim te worden behandeld.

6.3 Concept raadsbesluit RKC-onderzoek informatiebeveiliging

GEMEENTE WESTLAND

RAADSBESLUIT

De raad van de gemeente Westland;

gelezen het rapport van de Rekenkamercommissie naar de informatiebeveiliging in de gemeente Westland;

gehoord het advies van de commissie EFO van 26 juni 2019 en gehoord de beraadslagingen van onderhavige vergadering;

besluit:

1. Kennis te nemen van het rapport van de Rekenkamercommissie naar de informatiebeveiliging in de gemeente Westland van mei 2019;
2. De aanbevelingen zoals verwoord in het onder 1 genoemde rapport over te nemen;
3. Het college te verzoeken om uitvoering te geven aan de aanbevelingen;
4. Gelet op beslispunt 4 het college verzoeken om binnen 2 maanden aan de raad een actieplan van maatregelen voor te leggen met daarbij een tijdsplanning op elk van de kwetsbaarheden en
5. Over 6 maanden weer een scan door te RKC te laten uitvoeren naar de uitvoering van de maatregelen, zoals genoemd in het actieplan en de bijbehorende tijdsplanning.

Aldus besloten door de raad in zijn openbare vergadering van 9 juli 2019,

de griffier, de voorzitter,

A.P.M.A.F. Bergmans B.R. Arends

6.4 Voorwaardelijkheidsverklaring

Hoewel onze onderzoekers zeer zorgvuldig onderzoek hebben verricht, is het mogelijk dat zij niet iedere kwetsbaarheid gedetecteerd hebben. Dit komt mede doordat onze medewerkers gebonden zijn aan een budget- en tijdslimiet. Daarnaast worden regelmatig nieuwe kwetsbaarheden ontdekt. In veel gevallen worden deze gepubliceerd, inclusief mogelijkheden deze kwetsbaarheden te misbruiken. Wanneer er niet gepubliceerd wordt over een kwetsbaarheid, dan wordt dit een *'zero-day'* genoemd. Deze kwetsbaarheden kunnen voor lange tijd ongemerkt blijven bestaan doordat de leverancier van de getroffen software hier geen updates voor uitbrengt.

Hoffmann Bedrijfsrecherche B.V. kan geen aansprakelijkheid aanvaarden voor acties of maatregelen die op basis van het rapport worden ondernomen.