Hilversum Mediastad



Rekenkameronderzoek Informatiebeveiliging

Eindrapport

1 juni 2026

Inhoud

Bestuurlijke Nota 2

Inleiding 3

Samenvatting van de bevindingen 4

Conclusies 7

Aanbevelingen 10

Aanbevelingen aan het college 10

Aanbevelingen aan de raad 12

Nota van Bevindingen 13

Bestuurlijke Nota



Inleiding

De Rekenkamer Hilversum heeft onderzoek gedaan naar de informatiebeveiliging van de gemeente Hilversum. De rekenkamer vroeg zich af hoe weerbaar de gemeente is tegen actuele dreigingen als cybercriminaliteit en hoe het is gesteld met de informatieveiligheid van de gemeente Hilversum. Het onderzoek is uitgevoerd door onderzoeksbureau Hoffmann.

In dit onderzoek zijn de volgende onderzoeksvragen beantwoord:

Hoofdvraag

- In hoeverre is de informatieveiligheid van de gemeente Hilversum gewaarborgd?

Onderzoeksvragen 'Opzet'

- Welk beleid heeft de gemeente vastgesteld op het gebied van informatieveiligheid en hoe is dit beleid uitgewerkt in regels, procedures en werkprocessen?
- Heeft de gemeente de beleidsstukken die de Baseline Informatiebeveiliging Overheid (BIO[1]) voorschrijft?
- Wat heeft de gemeente Hilversum tot nu toe ondernomen om aan de zorgplicht van de nieuwe EU-richtlijn (de NIS 2[2]) te voldoen?
- Welke risico's kent de gemeente op het vlak van informatiebeveiliging?

Onderzoeksvragen 'Bestaan'

- In hoeverre worden deze regels, procedures en werkprocessen in de dagelijkse uitvoeringspraktijk ook daadwerkelijk gehanteerd?
- In hoeverre zijn er adequate middelen (budget en capaciteit) beschikbaar gesteld om de informatiebeveiliging te waarborgen?
- Hoe informeert de gemeente Hilversum haar inwoners over de maatregelen die worden getroffen inzake informatiebeveiliging?

Onderzoeksvragen 'Werking'

- Voert de gemeente Hilversum steekproeven en/of pentesten uit en, zo ja, met welk resultaat/effect?
- Zijn de systemen en informatie van de gemeente Hilversum toegankelijk voor onbevoegden?
- Op welke onderdelen is er ruimte voor verbetering op het vlak van informatiebeveiliging?
- Zijn raadsleden, B&W en ambtenaren zich bewust van de risico's en regels op het gebied van informatieveiligheid en weten zij wat ze moeten doen wanneer zij met een verdachte situatie te maken krijgen?

Onderzoeksvraag 'Rol van de Raad'

- Op welke manier wordt de gemeenteraad geïnformeerd over de uitvoering van het beleid rondom de informatiebeveiliging? Welke mogelijkheden heeft de raad om te sturen en te controleren?

---

[1] Baseline Informatiebeveiliging Overheid, het basis normenkader voor informatiebeveiliging binnen de overheid. Ten tijde van het onderzoek was de BIO2 nog niet van kracht. De toetsing heeft daarom plaatsgevonden aan de op dat moment geldende wet- en regelgeving (de BIO). Bij de uitvoering en duiding van het onderzoek is echter nadrukkelijk rekening gehouden met de uitgangspunten en de beoogde richting van de BIO2.

[2] De Europese Network and Information Security directive, of NIS2-richtlijn, is gericht op het verbeteren van de cyberbeveiliging en de weerbaarheid van essentiële diensten in EU-lidstaten. Deze richtlijn is van kracht sinds 16 januari 2023 voor lidstaten van de Europese Unie. De Cyberbeveiligingswet (Cbw) vertaalt deze richtlijn voor Nederland naar nationale wetgeving en vervangt, zo gauw deze wordt aangenomen, de huidige Wet beveiliging netwerk- en informatiesystemen (Wbni).

Samenvatting van de bevindingen

Dit onderzoek heeft als doel inzicht te verkrijgen in de mate waarin de informatiebeveiliging van de gemeente Hilversum is gewaarborgd, mede in het licht van geldende en aankomende wet- en regelgeving. Daartoe is gekeken naar de informatiebeveiliging vanuit drie samenhangende perspectieven: opzet, bestaan en werking van maatregelen; bezien vanuit mens, proces en techniek.

Op basis van interviews, documentanalyse en uitgevoerde operationele testen ontstaat het beeld dat de gemeente Hilversum in de afgelopen jaren actief heeft geïnvesteerd in informatiebeveiliging en zich bewust is van het toenemende belang hiervan voor de continuïteit van de dienstverlening, de bescherming van persoonsgegevens en het vertrouwen van burgers. Het onderzoek laat zien dat de informatiebeveiliging een duidelijke basis kent, maar ook concrete ontwikkelkansen om het volwassenheidsniveau te verhogen en de aantoonbaarheid van maatregelen verder te versterken, conform BIO(2)- en aankomende NIS2-vereisten.

Beantwoording van de hoofdvraag

De hoofdvraag van het onderzoek luidt: "*In hoeverre is de informatieveiligheid van de gemeente Hilversum gewaarborgd?*" Op basis van het uitgevoerde onderzoek luidt de conclusie dat de informatieveiligheid van de gemeente Hilversum gedeeltelijk is gewaarborgd, maar nog onvoldoende aantoonbaar en structureel om te kunnen spreken van een robuuste en toekomstbestendige invulling van de wettelijke zorgplicht. De gemeente Hilversum heeft stappen gezet om informatiebeveiliging te organiseren en te verbeteren. Maar deze zijn niet overal volledig uitgewerkt, niet consistent vastgelegd, niet systematisch getoetst op effectiviteit en niet anticiperend op (toekomstige) beleidsontwikkelingen. Dit blijkt onder meer uit het ontbreken van actueel en vastgesteld beleid en bijbehorende procedures voor alle BIO onderwerpen, waardoor keuzes en verantwoordelijkheden niet altijd eenduidig zijn vastgelegd. Daarnaast laten praktijktoetsen en observaties zien dat maatregelen in de dagelijkse uitvoering niet altijd de beoogde werking hebben, bijvoorbeeld ten aanzien van het bewustzijn van medewerkers over veilig omgaan met informatie en digitale dreigingen. Tot slot zijn binnen het Information Security Management Systeem (ISMS)[3] weliswaar onderdelen zoals *scoping (*het vaststellen van de grenzen van de te beveiligen IT-omgeving), verantwoordelijkheden van managementposities, PIT-rapportages en een gap-analyse uitgewerkt, maar ontbreekt een volledig en risicogestuurd ingericht ISMS. Hierdoor zijn periodieke controle, samenhangende prioritering en aantoonbare borging van maatregelen slechts beperkt mogelijk. Dit leidt tot een situatie waarin maatregelen in de praktijk soms wel worden uitgevoerd, maar niet of onvoldoende aantoonbaar zijn vastgelegd in beleid, procedures en periodieke controles, zoals vereist onder de BIO(2) in samenhang met de Cyberbeveiligingswet (Cbw).

Opzet van informatiebeveiliging

Kijkend naar de opzet van informatiebeveiliging beschikt de gemeente Hilversum over een vastgesteld Strategisch Gegevensbescherming en Informatiebeveiligingsbeleid (2025-2029). In dit beleid spreekt de organisatie de ambitie uit om te voldoen aan geldende wet- en regelgeving, waaronder de BIO, en om risicogestuurd te werken. Ook zijn rollen en verantwoordelijkheden op

[3] Het Information Security Management System is de verzameling van alle onderling samenhangende elementen op het vlak van informatiebeveiliging. Helpt beleid, procedures en doelstellingen te formuleren, implementeren, communiceren en evalueren om de algehele informatiebeveiliging te verbeteren/garanderen.

hoofdlijnen belegd, onder andere via het '*three lines of defense*'-model[4]. Tegelijkertijd blijkt uit de documentanalyse dat de verdere uitwerking van het strategisch beleid onvoldoende concreet en onvolledig is. Een groot deel van de door de BIO voorgeschreven beleidsdocumenten ontbreekt, is vier jaar of ouder zonder dat deze documenten tussentijds zijn herzien, of heeft nog de status 'concept'. Slechts een beperkt aantal van de 25 door de BIO benoemde beleidsonderwerpen is uitgewerkt in vastgesteld en actueel beleid. Hierdoor ontbreken op meerdere thema's duidelijke normstelling en richtinggevende kaders voor de organisatie. Daarnaast is vastgesteld dat het strategisch beleid grotendeels is gebaseerd op de BIO, terwijl de BIO2 inmiddels is vastgesteld en de aankomende Cyberbeveiligingswet voorziet in een wettelijk verplichte en aangescherpte invulling van informatiebeveiliging. Met het vaststellen van het huidige strategisch beleid is daarmee onvoldoende voorgesorteerd op deze ontwikkelingen. De impact van de BIO2 en de Cyberbeveiligingswet is nog niet aantoonbaar vertaald naar beleid, governance en samenhangende prioritering binnen de organisatie.

Bestaan en inrichting van informatiebeveiliging in de praktijk

Ten aanzien van het bestaan van maatregelen in de dagelijkse praktijk bestaat een gemengd beeld. Uit interviews en operationele testen blijkt dat medewerkers, afdelingen en ondersteunende teams zich bewust zijn van risico's en in de praktijk diverse maatregelen toepassen. Tegelijkertijd ontbreekt het vaak aan formele vastlegging, uniforme werkwijzen en periodieke controlemechanismen. De door de gemeente Hilversum zelf uitgevoerde BIO gap-analyse laat zien dat de organisatie stelt aan circa 71% van de maatregelen te voldoen. Deze zelfbeoordeling laat groei zien ten opzichte van eerdere jaren, maar maakt ook duidelijk dat de gemeente Hilversum op basis van de eigen analyse nog niet BIO compliant is. Daarbij is vastgesteld dat de wijze waarop maatregelen als "compliant", "gedeeltelijk" of "niet van toepassing" worden beoordeeld, niet altijd eenduidig of herleidbaar is. Een belangrijk aandachtspunt is dat maatregelen regelmatig als aanwezig worden beschouwd op basis van feitelijke uitvoering ("we doen het wel"), terwijl procedures, werkinstructies of controleafspraken ontbreken. Onder de BIO en zeker onder de BIO2 is deze werkwijze onvoldoende, omdat informatiebeveiliging aantoonbaar moet zijn ingericht, onderhouden en geëvalueerd.

Werking en effectiviteit van maatregelen

De werking van maatregelen is in dit onderzoek getoetst door middel van operationele testen, waaronder een technische penetratietest, een phishingtest en een fysieke inlooptest. Deze testen geven inzicht in de daadwerkelijke weerbaarheid van de organisatie in de praktijk.

Uit de technische penetratietest blijkt dat de externe digitale weerbaarheid van de gemeente Hilversum op orde is: het netwerk bleek van buitenaf niet direct toegankelijk voor onbevoegden. De interne digitale weerbaarheid daarentegen laat verbeterpunten zien. Vanuit een interne positie was het mogelijk om kwetsbaarheden te benutten die uiteindelijk leidden tot het verkrijgen van verhoogde rechten en toegang tot systemen. Dit wijst op risico's in onder meer (onvoldoende) netwerksegmentatie (het opdelen van een computernetwerk in kleinere, afzonderlijke netwerken die beter te beveiligen zijn), toegangsbeheer en interne beveiligingsmaatregelen. De resultaten van de phishingtest laten zien dat het bewustzijn van medewerkers rondom digitale dreigingen onvoldoende is. Met een klikpercentage van 36% en het achterlaten van inloggegevens door een substantieel deel

[4] Het 'three lines of defense'-model is een model waarin 1) lijnmanagement verantwoordelijk is "voor het realiseren van gegevensbescherming en IB-maatregelen in eigen processen.", 2) de Information Security Officer (ISO) en Privacy Officers (PO) hierbij adviseren en ondersteunen, en 3) de interne auditor, Chief Information Security Officer (CISO) en de Functionaris Gegevensbescherming (FG) de organisatie van een objectief oordeel voorzien en het toezicht vormgeven.

van de medewerkers, ligt dit ruim boven het gemiddelde van vergelijkbare organisaties. Hoewel technische maatregelen zoals tweefactorauthenticatie directe schade hebben beperkt, blijft het risico bestaan dat menselijk handelen kan leiden tot ernstige incidenten. De fysieke inlooptesten tonen aan dat ook de fysieke informatiebeveiliging kwetsbaar is. Op meerdere locaties was het mogelijk om ongeautoriseerd toegang te krijgen tot gebouwen en gevoelige informatie, onder meer door *tailgating* (het onbevoegd meelopen met iemand met autorisatie, bijvoorbeeld door een toegangspoortje of beveiligde deur), beperkte toegangscontrole en onvoldoende afgesloten documentopslag.

Governance, middelen en toezicht

Wat betreft governance en middelen beschikt de gemeente Hilversum over een gemotiveerd informatiebeveiligings- en privacyteam, met duidelijke rollen in de tweede lijn. De samenwerking met ICT, Facilitair en Informatiemanagement draagt bij aan de uitvoering van maatregelen.

Tegelijkertijd is vastgesteld dat structurele evaluatie, monitoring en borging nog onvoldoende ingericht of mogelijk van onvoldoende niveau zijn om het toezicht effectief in te vullen. Vanuit haar toezichtrol heeft de derde lijn de verantwoordelijkheid om het college en de gemeenteraad via onder meer ENSIA-rapportages[5] en raadsinformatiebrieven te informeren over de status en naleving van het informatiebeveiligingsbeleid. De bevindingen uit dit onderzoek wijken echter af van de “compliant”-beoordeling zoals die in de ENSIA-rapportages worden gepresenteerd. Dit roept de vraag op of het huidige toezichtsmodel van de derde lijn voldoende scherp is ingericht om tijdig en zelfstandig kwetsbaarheden in opzet, bestaan en werking van het informatiebeveiligingsbeleid te signaleren.

Daarnaast is er geen integraal en risicogebaseerd overzicht van benodigde middelen. Budgetten voor informatiebeveiliging zijn niet expliciet gekoppeld aan risico’s en prioriteiten, waardoor het lastig is om de proportionaliteit en effectiviteit van investeringen te beoordelen.

Rol van de Raad

De gemeenteraad wordt via verschillende kanalen geïnformeerd over informatiebeveiliging, waaronder ENSIA-rapportages en incidentele raadsinformatiebrieven. Deze informatievoorziening is echter niet structureel en niet integraal. De raad ontvangt op dit moment nog geen compleet en samenhangend overzicht van risico’s, dreigingen, maatregelen, rollen en verantwoordelijkheden. De informatie wordt nu verspreid en gefragmenteerd aangeboden (zoals via ENSIA, losse brieven en bijeenkomsten), waardoor een eenduidig en begrijpelijk totaalbeeld van risico’s en dreigingen ontbreekt. Hierdoor is het voor de raad lastig om consistent te sturen op risico’s, prioriteiten en de mate waarin de zorgplicht daadwerkelijk wordt ingevuld.

[5] De jaarlijkse ENSIA-rapportage is een zelfevaluatie die door de CISO van de gemeente wordt uitgevoerd, wordt gecontroleerd door middel van een externe Auditor en goedgekeurd door het College van Burgemeesters en Wethouders. Daarna worden de stukken aan de raad beschikbaar gesteld middels een raadsinformatiebrief met de (geheime) stukken via de procedure van de griffie met het geheime kastje.

Conclusies

Uit dit onderzoek is gebleken dat de gemeente Hilversum zich in een ontwikkelfase bevindt op het gebied van informatiebeveiliging. Er is sprake van betrokkenheid, bewustzijn over het belang van informatieveiligheid en er zijn concrete initiatieven om dit te versterken, maar de informatiebeveiliging is nog onvoldoende volwassen, risicogestuurd en aantoonbaar ingericht om te voldoen aan de eisen die voortvloeien uit de BIO, de BIO2 en de aankomende Cyberbeveiligingswet. Zonder verdere professionalisering van het Information Security Management Systeem, expliciete risicosturing, structurele toetsing van maatregelen en het vergroten van het bewustzijn over informatieveiligheid bij medewerkers, blijft de organisatie kwetsbaar voor incidenten die impact kunnen hebben op de continuïteit van dienstverlening, de privacy van burgers en het vertrouwen in het bestuur.

Meer specifiek komen uit dit onderzoek de volgende conclusies naar voren:

1. De informatieveiligheid van de gemeente Hilversum is gedeeltelijk gewaarborgd, maar er zijn verbeteringen mogelijk, zowel op het gebied van technische, organisatorische als menselijke factoren (Hoofdconclusie).

De gemeente heeft de afgelopen jaren aantoonbaar stappen gezet om de informatiebeveiliging te verbeteren en beschikt over betrokken medewerkers, een gemotiveerd informatiebeveiligings- en privacyteam en diverse ingezette maatregelen. Tegelijkertijd laat het onderzoek zien dat deze maatregelen nog onvoldoende aantoonbaar, structureel en risicogestuurd ingericht zijn om volledig te voldoen aan de huidige en toekomstige wetgeving (BIO2 en de Cyberbeveiligingswet). Uit de tijdens dit onderzoek uitgevoerde operationele testen is gebleken dat de organisatie niet altijd weerbaar is in de praktijk als het gaat om technische (digitale) weerbaarheid, menselijke factoren en fysieke beveiliging van vertrouwelijke gegevens.

2. Het gemeentelijk informatiebeveiligingsbeleid voldoet niet aan alle geldende wettelijke normen en is nog niet voldoende voorbereid op nieuwe wetgeving.

Gemeenten moeten voldoen aan de Baseline Informatieveiligheid Overheid (BIO). Deze BIO gaat ervan uit dat maatregelen kunnen worden aangetoond in opzet, bestaan en werking. Het Informatiebeveiligingsbeleid van de gemeente Hilversum voldoet niet volledig aan de norm die de BIO voorschrijft. Uit het onderzoek blijkt dat een deel van het beleid en de procedures van de gemeente Hilversum niet compleet of verouderd is.

Het Strategisch Informatiebeveiligingsbeleid en het onderliggende tactisch beleid van de gemeente zijn daarnaast nog niet aangepast aan nieuwe wetgeving: de BIO2 en Cyberbeveiligingswet (Cbw). De impact van de wijzigingen van de BIO naar de BIO2 is nog onvoldoende bepaald en tevens is de Wet weerbaarheid kritieke entiteiten (Wwke) geen onderdeel van het beleid. Daarmee is de gemeente nog niet voldoende voorbereid op de nieuwe wetgeving die binnenkort, zo gauw deze wetgeving aangenomen wordt (naar verwachting medio 2026), leidend zal worden.

3. Het Information Security Management Systeem (ISMS) is niet volledig en sluit nog onvoldoende aan op de uitgangspunten van de BIO(2).

Met de komst van de BIO2 en de Cyberbeveiligingswet (Cbw) wordt een samenhangend en aantoonbaar ingericht ISMS verplicht gesteld. Het huidige ISMS van de gemeente Hilversum is nog

niet voldoende en samenhangend ingericht. Het gaat hier bijvoorbeeld om de samenhang tussen beleid, uitvoering en sturing en de vertaling van beleid naar concrete procedures en werkinstructies. Ook is het risicogestuurd werken nog niet overal consequent uitgewerkt. Hoewel dit als uitgangspunt is opgenomen in het strategisch beleid, ontbreekt een integraal en organisatiebreed uitgewerkt risicomanagement. Hierdoor worden maatregelen nog niet altijd aantoonbaar gebaseerd op een systematische risico-afweging.

Dit komt onder andere tot uiting in het ontbreken van een integraal, risicogestuurd overzicht van benodigde middelen. Budgetten zijn nog beperkt expliciet gekoppeld aan risico's en prioriteiten, waardoor er kansen liggen om de proportionaliteit en effectiviteit van investeringen beter inzichtelijk te maken.

4. Medewerkers en afdelingen onderschrijven het belang van informatiebeveiliging, maar in de praktijk wordt hier niet altijd naar gehandeld.

Uit interviews en observaties blijkt dat medewerkers en afdelingen zich bewust zijn van het belang van informatiebeveiliging en dat maatregelen in veel gevallen daadwerkelijk worden toegepast. Tegelijkertijd ontbreekt het vaak aan formele procedures, uniforme werkwijzen en controlemechanismen. Er is een operationeel meldingsloket voor incidenten, maar er is geen duidelijk incidentmanagementproces vastgelegd waarbij incidenten snel kunnen worden gemeld en opgevolgd. Er wordt niet aantoonbaar periodiek geoefend op incidentscenario's.

Uit de uitgevoerde testen bleek dat het bewustzijn van medewerkers rondom digitale dreigingen zoals insluiping en mailphishing onvoldoende is. Hoewel tweefactorauthenticatie directe schade beperkt, toont de mailphishingtest aan dat het bewustzijn rondom digitale dreigingen verder kan worden versterkt en dat menselijk handelen een reëel risico vormt. De bevindingen en concrete verbetersuggesties zijn opgenomen in het vertrouwelijke rapport 'Bijlage 5.2 Verloop Mailphishing Gemeente Hilversum' dat is gedeeld met de organisatie.

5. De fysieke beveiliging van vertrouwelijke gegevens behoeft aandacht.

De fysieke inlooptesten laten zien dat op meerdere locaties ongeautoriseerde toegang mogelijk was door onder meer *tailgating*, beperkte toegangscontrole en onvoldoende afgesloten documentopslag. Hierdoor konden vertrouwelijke documenten worden ingezien of meegenomen. De technische bevindingen en concrete verbetersuggesties zijn opgenomen in het vertrouwelijke rapport 'Bijlage 5.3 Verloop Fysieke Inlooptest Gemeente Hilversum' dat is gedeeld met de organisatie.

6. De technische digitale weerbaarheid is extern gezien op orde; intern gezien zijn verbeteringen mogelijk.

De externe digitale weerbaarheid bleek in dit onderzoek op orde: het netwerk was van buitenaf niet direct toegankelijk voor onbevoegden. De interne digitale weerbaarheid laat echter verbeterpunten zien. Vanuit een interne positie konden kwetsbaarheden worden benut die uiteindelijk leidden tot verhoogde rechten en toegang tot systemen. Dit wijst op risico's in netwerksegmentatie, toegangsbeheer en interne beveiligingsmaatregelen. De technische bevindingen en concrete verbetersuggesties zijn opgenomen in het vertrouwelijke rapport 'Bijlage 5.4 Verloop Digitale Pentest Gemeente Hilversum' dat is gedeeld met de organisatie.

7. Het toezicht van de derde lijn moet verder worden verdiept en versterkt.

De gemeente hanteert een '*three lines of defense*'-model, wat een goede basis vormt voor sturing en toezicht. Tegelijkertijd blijkt uit het onderzoek dat de invulling van de derde lijn op onderdelen verder kan worden versterkt, met name in diepgang, structurele monitoring en het tijdig signaleren van kwetsbaarheden in opzet, bestaan en werking van maatregelen.

De samenwerking met afdelingsmanagers is hierbij een belangrijke succesfactor, evenals het verder verduidelijken van taken, verantwoordelijkheden en bevoegdheden. Door het toezichtsmodel op deze punten door te ontwikkelen, kan het nog beter bijdragen aan een volledig en betrouwbaar beeld van de informatiebeveiliging en de sturing daarop.

8. De informatievoorziening aan de raad als het gaat om informatiebeveiliging is niet structureel noch integraal, waardoor het voor de raad beperkt mogelijk is te sturen op risico's, prioriteiten en de invulling van de zorgplicht.

Uit het onderzoek blijkt dat raadsleden, B&W en ambtenaren niet structureel geïnformeerd worden over de risico's en regels op het gebied van informatieveiligheid. Structurele informatievoorziening aan de raad vindt wel plaats via de verplichte jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA)-rapportage en met (niet periodieke) raadsinformatiebrieven, themabijeenkomsten en andersoortige rapportages. Echter er wordt geen structureel eenduidig, begrijpelijk risico- en dreigingsbeeld voor de gemeente gedeeld waardoor een totaalbeeld van risico's en dreigingen ontbreekt. De raad ontvangt op dit moment nog geen compleet en samenhangend overzicht van risico's, dreigingen, maatregelen, rollen en verantwoordelijkheden. Ook worden raadsleden, B&W en ambtenaren onvoldoende gewezen op hun specifieke rollen, rechten en plichten rondom deze risico's. Hierdoor is het voor de raad beperkt mogelijk om consistent te sturen op risico's, prioriteiten en de invulling van de zorgplicht als het gaat om informatieveiligheid. College en raad zijn te weinig onderling in gesprek over de risico's, ambities en de werking van het beleid op het gebied van informatieveiligheid.

Aanbevelingen

De hierboven geformuleerde conclusies leiden tot onderstaande aanbevelingen aan het college en de raad, met het doel concrete handvatten te bieden om de informatiebeveiliging van de gemeente Hilversum te verbeteren.

Aanbevelingen aan het college

1. **Zorg voor een volledig informatiebeveiligingsbeleid, dat aan de geldende wettelijke normen voldoet en is uitgewerkt in werkprocessen.**

Zorg voor een volledig Informatiebeveiligingsbeleid dat in lijn is met de vereisten uit de BIO, Cbw en Wwke. Zorg dat het (strategische) informatiebeveiligingsbeleid op tactisch en operationeel niveau kan worden uitgevoerd door het te vertalen in concrete richtlijnen, procedures en werkinstructies. Evalueer welke uitwerkingen nog ontbreken en vul aan.

2. **Zorg dat het informatiebeveiligingsbeleid is toegerust voor de overgang naar toekomstige wetgeving.**

Zorg voor een Informatiebeveiligingsbeleid dat rekening houdt met nieuwe wetgeving en maak de overgang naar de BIO2 en de Cyberbeveiligingswet expliciet via een impact- en gap-analyse. Richt daarnaast een structurele werkwijze in om wijzigingen in wet- en regelgeving tijdig te signaleren, te beoordelen en door te vertalen naar beleid en maatregelen.

In deze analyses en uitwerking kan de impact van de fusie met Wijdemeren meteen worden meegenomen. Maak inzichtelijk welke stappen worden gezet en welke keuzes zijn gemaakt, zodat de voortgang en naleving aantoonbaar zijn.

3. **Versterk de fundamenten van informatiebeveiliging door een volledig en risicogestuurd ISMS in te richten conform de BIO(2), in samenhang met het bredere risicomanagement binnen de organisatie.**

Richt het ISMS zodanig in dat beleid, risico's, maatregelen, middelen en periodieke controles aantoonbaar samenhangen. Richt in samenhang met concern control structureel risicomanagement in, inclusief een centraal risicoregister als basis voor sturing, en kom tot een gedeeld beeld van de belangrijkste risico's. Gebruik risicoanalyses als basis voor prioritering, besluitvorming en de invulling van jaarplannen en inzet van middelen. Werk het principe van risicogestuurd werken concreet uit in beleid en processen, zodat duidelijk is op basis van welke risico's keuzes worden gemaakt en hoe deze worden vertaald naar maatregelen, procedures en werkinstructies.

Borg daarnaast een effectieve beleidscyclus (PDCA), waarin maatregelen en verbeterpunten structureel worden opgevolgd, geïmplementeerd en periodiek geëvalueerd en getoetst. Neem hierbij ook structureel testen van de digitale en fysieke beveiliging op, op basis van vastgesteld beleid en planning.

4. **Intensiveer activiteiten om kennis van en bewustzijn over informatiebeveiliging en -risico's onder medewerkers te bevorderen.**

Investeer structureel in informatieveiligheidsbewustzijn van medewerkers, (lijn)management, college en raad, waarbij menselijk handelen expliciet wordt meegenomen als kritieke risicofactor. Zorg dat het risicobewustzijn, de taakvolwassenheid en het eigenaarschap verder wordt versterkt om (vertrouwelijke) informatie bij de gemeente beter te beschermen. Bijvoorbeeld met een programma

met bewustwordingsactiviteiten, dat kan worden geëvalueerd door de raad, met duidelijke, praktische uitleg gebaseerd op de belangrijkste risico's. Evalueer welke testen (zoals phishing-mails of incidentscenario's) kunnen bijdragen aan het verhogen van het bewustzijn van medewerkers en voer deze regelmatig uit.

Zorg dat taken, verantwoordelijkheden en bevoegdheden duidelijk belegd zijn bij alle functionarissen en dat deze nageleefd worden. Maak hierbij gebruik van de concrete verbetersuggesties in het vertrouwelijke rapport 'Bijlage 5.2 Verloop Mailphishing Gemeente Hilversum'.

5. Versterk de fysieke beveiliging van vertrouwelijke gegevens van de gemeente.

Maak hierbij gebruik van de concrete, technische verbetersuggesties in het vertrouwelijke rapport 'Bijlage 5.3 Verloop Fysieke Inlooptest Gemeente Hilversum'. Deze verbetersuggesties zijn, met het oog op de veiligheid, vooralsnog enkel gedeeld met de organisatie.

6. Vergroot de interne digitale weerbaarheid van de gemeente.

Maak hierbij gebruik van de concrete, technische verbetersuggesties in het vertrouwelijke rapport 'Bijlage 5.4 Verloop Digitale Pentest Gemeente Hilversum'. Deze verbetersuggesties zijn, met het oog op de veiligheid, vooralsnog enkel gedeeld met de organisatie.

7. Toets periodiek of het toezicht van de derde lijn voldoende aansluit bij de gewenste diepgang en effectiviteit, en voer waar nodig gerichte verbeteringen door.

Breng in kaart in hoeverre de taken, verantwoordelijkheden en bevoegdheden binnen het '*three lines of defense*'-model helder zijn belegd en in de praktijk ook daadwerkelijk worden uitgevoerd. Dit draagt bij aan een meer realistisch en integraal beeld van de informatiebeveiliging en maakt het mogelijk om risico's en verbeterpunten eerder te signaleren.

Voer waar nodig aanpassingen door, bijvoorbeeld door rollen te verduidelijken, taken scherper af te bakenen of de samenwerking tussen de drie lijnen te versterken. Zo kan vanuit gedeelde verantwoordelijkheden en voldoende taakvolwassenheid effectiever worden gestuurd op informatiebeveiliging. Borg daarbij dat de onafhankelijkheid van de CISO, FG en interne auditfunctie behouden blijft, en dat deze rollen hun toezichthoudende taken onafhankelijk kunnen blijven uitvoeren.

8. Verbeter de periodieke informatievoorziening.

Zorg voor een informatievoorziening (bijvoorbeeld via een vast bestuurlijk dashboard, kwartaalrapportage of jaarlijkse themasessie) waarin raadsleden, B&W en ambtenaren actief en consistent worden geïnformeerd over actuele risico's, relevante regels, incidenten en ontwikkelingen op het gebied van informatieveiligheid. Dit voert verder dan de huidige ENSIA-rapportages. Zorg dat college en raad op basis van deze informatievoorziening structureel en consistent kunnen sturen en controleren op risico's, voortgang en naleving van de wettelijke zorgplicht op het gebied van informatiebeveiliging.

Zorg dat structureel en consistent een eenduidig, begrijpelijk risico- en dreigingsbeeld voor de gemeente wordt gedeeld. Zorg daarnaast dat raadsleden, B&W en ambtenaren gewezen worden op hun specifieke rollen, rechten en plichten rondom deze risico's in informatieveiligheid.

Aanbevelingen aan de raad

9. Maak afspraken over hoe en wanneer de raad geïnformeerd wordt over informatieveiligheid.

Bespreek in commissieverband op welke wijze de raad geïnformeerd wordt over informatieveiligheid en met welke frequentie. Leg deze afspraken vast.

Organiseer bijvoorbeeld halfjaarlijks een extra verdiepend (commissie)overleg naar aanleiding van de ENSIA-rapportages en de rapportages van de FG. En maak bijvoorbeeld afspraken over een structurele informatievoorziening aan de raad, opgesteld vanuit risicomanagementperspectief (m.b.v. een dashboard of rapportage). Door de focus te leggen op kritieke processen, en door te rapporteren op strategisch niveau, kan deze informatiestroom overzichtelijk worden gehouden voor de raad.

10. Intensiveer activiteiten voor de raad om kennis van en bewustzijn over informatiebeveiliging(srisico's) onder raads- en commissieleden te bevorderen.

Bevorder het kennisniveau en bewustzijn van veiligheidsrisico's onder raads- en commissieleden, bijvoorbeeld door periodiek een awareness-sessie te organiseren. Organiseer bewustwordingsactiviteiten met duidelijke, praktische uitleg, gebaseerd op de belangrijkste risico's specifiek voor raads- en commissieleden. Sluit hierbij waar mogelijk aan bij de activiteiten en trainingen die door de griffie en/of de organisatie worden georganiseerd. Vraag het college om de raad structureel mee te nemen in testen die bijdragen aan het verhogen van het bewustzijn.

Nota van Bevindingen





Nota van Bevindingen Informatiebeveiliging Gemeente Hilversum

Dossiernummer 22507030

Onderzoek in opdracht van

Rekenkamer Hilversum

OPENBAAR

Hoffmann
Luidsprekerstraat 10
1322 AX Almere

T 088 - 298 66 00
E info@hoffmann.nl
W www.hoffmann.nl

IBAN NL87ABNA0861616820
KvK 33170622
BTW NL006275199B01

INHOUDSOPGAVE

1.	Inleiding	3
2.	Belang van informatiebeveiliging	6
3.	Beantwoording hoofdvraag en deelvragen (bevindingen)	9
4.	Conclusie en praktische oplossingsrichtingen	2525
5.	Bijlagen	31

1. Inleiding

De Rekenkamer van de gemeente Hilversum (hierna genoemd: 'de Rekenkamer') heeft Hoffmann gevraagd een onderzoek uit te voeren naar de informatiebeveiliging (IB) bij de gemeente Hilversum (hierna genoemd: 'de gemeente'). Informatiebeveiliging beschermt de informatie binnen de gemeente tegen een breed scala aan bedreigingen door middel van organisatorische, technische en beleidsmatige maatregelen. Deze maatregelen vallen of staan echter bij het gebruik en de opvolging van de medewerker in de dagelijkse praktijk. Andersom: de mens kan welwillend en bekwaam zijn, maar wanneer deze niet wordt gefaciliteerd door techniek of de organisatie, brengt dat eveneens kwetsbaarheden met zich mee. Dit onderzoek richt zich daarom op de informatiebeveiliging binnen de gemeente, vanuit een menselijk, proces én technisch perspectief. Op basis van de bevindingen zijn de aanbevelingen in kaart gebracht welke gebruikt kunnen worden om de informatiebeveiliging naar een hoger niveau te tillen. Dit onderzoek heeft plaatsgevonden in de periode september t/m december 2025.

1.1 Doelstellingen en scope

1.1.1 Doelstellingen en onderzoeksvragen

Door een onderzoek uit te voeren naar de informatiebeveiliging wil de Rekenkamer met haar onderzoek aanbevelingen doen die bijdragen aan een verbetering van de informatieveiligheid van de gemeente. De onderzoeksvragen zijn opgesteld in overleg met de Rekenkamer Hilversum. De beantwoording van deze vragen geeft inzicht in de risico's voor de gemeente en wat eraan gedaan wordt (en kan worden) om deze tot een aanvaardbaar niveau te brengen. De genomen maatregelen dienen in verhouding te staan tot de grootte van het risico.

De hoofdvraag van dit onderzoek luidt: "In hoeverre is de informatieveiligheid van de gemeente Hilversum gewaarborgd?".

De beantwoording van de hoofdvraag wordt ondersteund door deelvragen. Per deelgebied zijn de volgende deelvragen geformuleerd waar in hoofdstuk 3 antwoord op wordt gegeven:

Onderzoeksvragen 'Opzet'

- Welk beleid heeft de gemeente vastgesteld op het gebied van informatieveiligheid en hoe is dit beleid uitgewerkt in regels, procedures en werkprocessen?
- Heeft de gemeente de beleidsstukken die de Baseline Informatiebeveiliging Overheid (BIO)[1] voorschrijft?

[1] Ten tijde van het onderzoek was de BIO2 nog niet van kracht. De toetsing heeft daarom plaatsgevonden aan de op dat moment geldende wet- en regelgeving. Bij de uitvoering en duiding van het onderzoek is echter nadrukkelijk rekening gehouden met de uitgangspunten en de beoogde richting van de BIO2.

- Wat heeft de gemeente Hilversum tot nu toe ondernomen om aan de zorgplicht van de nieuwe EU-richtlijn (de NIS2[2]) te voldoen?
- Welke risico's kent de gemeente op het vlak van informatiebeveiliging?

Onderzoeksvragen 'Bestaan'

- In hoeverre worden deze regels, procedures en werkprocessen in de dagelijkse uitvoeringspraktijk ook daadwerkelijk gehanteerd?
- In hoeverre zijn er adequate middelen (budget en capaciteit) beschikbaar gesteld om de informatiebeveiliging te waarborgen?
- Hoe informeert de gemeente Hilversum haar inwoners over de maatregelen die worden getroffen inzake informatiebeveiliging?

Onderzoeksvragen 'Werking'

- Voert de gemeente Hilversum steekproeven en/of pentesten uit en, zo ja, met welk resultaat/effect?
- Zijn de systemen en informatie van de gemeente Hilversum toegankelijk voor onbevoegden?
- Op welke onderdelen is er ruimte voor verbetering op het vlak van informatiebeveiliging?
- Zijn raadsleden, B&W en ambtenaren zich bewust van de risico's en regels op het gebied van informatieveiligheid en weten zij wat ze moeten doen wanneer zij met een verdachte situatie te maken krijgen?

Deelvragen Rol van de Raad

- Op welke manier wordt de gemeenteraad geïnformeerd over de uitvoering van het beleid rondom de informatiebeveiliging? Welke mogelijkheden heeft de raad om te sturen en te controleren?

1.1.2 Aanpak en scope

De aanpak van dit onderzoek bestond uit drie fasen:

1. Afname Interviews & Documentanalyse (zie bijlage 5.8 en de vertrouwelijke bijlage 5.9 voor meer inzicht in de geïnterviewden en welke documenten zijn geraadpleegd door de onderzoekers van Hoffmann);
2. Uitvoering van Operationele Testen, te weten:
    a. Phishingtest: het uitvoeren van een digitale test waarin het menselijk handelen wordt getoetst door te meten en analyseren of ambtenaren gevoelig zijn voor het ontvangen van malafide e-mails van waaruit toegang tot het gemeentelijk netwerk kan worden verschaft door kwaadwillenden.

[2] NIS2 (Network and Information Security 2 Directive) is de Europese richtlijn voor cyberbeveiliging die geldt voor organisaties in vitale en belangrijke sectoren (zoals energie, zorg en overheid) en hen verplicht passende beveiligingsmaatregelen te nemen en incidenten te melden.

b. Inlooptest: het uitvoeren van een fysieke test waarin fysieke beveiligingsmaatregelen op de gemeentelijke locaties worden getoetst en wordt gekeken naar het gedrag van ambtenaren om fysieke toegang tot informatie te belemmeren voor kwaadwillenden.
c. Penetratietest: het uitvoeren van een digitale test waarin de opzet van digitale maatregelen wordt getoetst door actief te proberen toegang te verschaffen tot de digitale omgeving en systemen van de gemeente.

3. Rapportage & toepassing van 'hoor en wederhoor'.

In de gehele aanpak is er voortdurend gekeken naar de volgende elementen:

- Opzet: in hoeverre is de genomen maatregel vooraf ontworpen om haar doel te behalen?
- Bestaan: in hoeverre is deze maatregel ook ingericht in de praktijk?
- Werking: in hoeverre is de genomen maatregel in de praktijk ook daadwerkelijk effectief?

In algemene zin geldt, dat zowel 'opzet' als 'bestaan' op basis van een analyse (interviews en documentatie) kunnen worden beoordeeld. Waar het de 'werking' betreft, zijn de bevindingen uit de Operationele Testen leidend. Het onderzoek is een kwalitatief onderzoek en is een momentopname van de situatie zoals deze ten tijde van het onderzoek wordt gezien en ervaren. Hoffmann is afhankelijk van de ten tijde van het onderzoek beschikbaar gestelde relevante documentatie en informatie uit de interviews. Waar mogelijk probeert Hoffmann recht te doen aan 'lopende initiatieven', echter: wat nog in wording is, levert vandaag de dag nog geen verhoogde weerbaarheid op. Aanbevelingen kunnen op deze wijze uiteraard wel een bevestiging zijn van een reeds ingezette beweging of opgezet project binnen de gemeente.

De scope van het gehele onderzoek betreft:

- De bestuurlijke en ambtelijke organisatie van de gemeente Hilversum;
- De gemeentelijke processen zoals centraal vormgegeven binnen de gemeente Hilversum;
- De (beschreven) digitale omgeving van de gemeente Hilversum;
- Afhankelijk van het ingezette middel alle medewerkers, dan wel een gericht aantal medewerkers van de gemeente Hilversum;
- Het Raadhuis, Stadskantoor, Sociaal Plein en de Gemeentewerf van de gemeente Hilversum (voor de fysieke inlooptesten).

Buiten scope vallen:

- Alle activiteiten die onder burgers van de gemeente plaatsvinden in het 'Openbare Domein';
- Alle Operationele Techniek (OT) welke beheerd wordt door de gemeente Hilversum;
- Alle overige locaties welke worden gebruikt door of in het beheer zijn van de gemeente Hilversum buiten de voor de fysieke inlooptest benoemde locaties.

In bijlage 5.7 is een verklarende woordenlijst opgenomen met informatiebeveiligingstermen ter bevordering van de leesbaarheid van het rapport.

1.1.3 Leeswijzer

In het opvolgende hoofdstuk 2 wordt verder ingegaan op het belang van informatiebeveiliging voor de gemeente in algemene zin. In hoofdstuk 3 worden de hoofdvraag en onderliggende deelvragen per thema behandeld. In paragraaf 3.6 wordt vervolgens afgesloten met een weergave van de belangrijkste bevindingen uit de uitgevoerde operationele testen. Hoofdstuk 4 bevat de hoofdconclusie en biedt praktische oplossingsrichtingen voor de aanbevelingen uit de bestuurlijke nota.

1.2 Versiebeheer

Versie	Datum	Status
0.4	15 december 2025	Rapportage voor Feitelijk Hoor en Wederhoor
0.9	4 maart 2026	Verwerking Feitelijk Hoor en wederhoor
1.0	1 juni 2026	Definitieve rapportage

2. Belang van informatiebeveiliging

In de Nederlandse samenleving[3] worden steeds meer diensten en processen ondersteund middels Informatie Technologie (IT) en Operationele Technologie (OT). Deze inzet van digitale middelen leidt tot een toename van de effectiviteit en efficiëntie van bijvoorbeeld gemeentelijke processen, maar leidt ook tot een toenemende afhankelijkheid van informatie en benodigde digitale systemen. Deze ontwikkeling leidt ertoe dat informatiebeveiliging (IB) steeds belangrijker wordt voor Nederlandse gemeenten en niet alleen als technisch vraagstuk moet worden benaderd, maar als continuïteitsvraagstuk voor gemeentelijke processen en dienstverlening.

2.1 Zorgplicht richting burgers

Gemeenten zijn verantwoordelijk voor de bescherming van persoonsgegevens en andere vertrouwelijke informatie van hun inwoners. Deze zorgplicht vloeit voort uit verschillende wettelijke kaders[4], zoals:

- Algemene Verordening Gegevensbescherming (AVG);
- Wet Digitale Overheid;
- BIO (Baseline Informatiebeveiliging Overheid) versie 1.04zv en daaropvolgende BIO2;
- Grondwet Artikel 10 (recht op privacy);
- En de aankomende Cyberbeveiligingswet (gebaseerd op de NIS2).

[3] Dit geldt, uiteraard, niet alleen voor de Nederlandse samenleving, maar is een fenomeen wat zich wereldwijd voltrekt.
[4] Zowel voor de BIO2 als de Cyberbeveiligingswet geldt voor gemeenten om zich hier actief op voor te bereiden en te starten met de implementatie.

Deze wetten verplichten gemeenten om passende maatregelen te nemen op organisatorisch, menselijk en technisch vlak om informatie(systemen) te beveiligen. Een gemeente handelt dus niet alleen uit juridische noodzaak, maar ook uit een maatschappelijke verantwoordelijkheid om haar zorgplicht in te kunnen vullen.

2.2 Gevoelige informatie

Gemeenten verwerken informatie die gevoelig kan zijn. Hierbij valt te denken aan persoonsgegevens van burgers:

- Burgerservicenummers (BSN);
- Informatie over uitkeringen, schulden of jeugdzorg;
- Gezondheidsgegevens (bijvoorbeeld via Wmo of Jeugdwet);
- Informatie over verblijfsstatus of huiselijk geweld.

Het uitlekken of verkeerd gebruiken van deze gegevens kan grote persoonlijke gevolgen hebben voor burgers (denk bijvoorbeeld aan identiteitsfraude) of leiden tot maatschappelijke schade.

Daarnaast verwerken gemeenten ook informatie die gevoelig kan zijn in politiek bestuurlijke zin. Denk hierbij aan bestemmingsplannen, projecten die gaan over de inrichting van de publieke ruimte of casuistiek die de openbare orde en veiligheid binnen de gemeente adresseren.

2.3 Toename van cyberdreigingen

Gemeenten zijn steeds vaker doelwit van:

- Ransomware-aanvallen (zoals bv. bij Hof van Twente en de gemeente Buren[5]), waarbij de digitale infrastructuur gegijzeld wordt en enkel tegen losgeld weer wordt vrijgegeven door hackers[6];
- Phishing en social engineering, waarbij hackers misbruik maken van menselijke tekortkomingen of onoplettendheid om daaropvolgend toegang te krijgen tot (gevoelige) informatie van de gemeente;
- Datalekken door menselijke fouten of verouderde systemen, waardoor (gevoelige) data onbedoeld in handen komt van mensen die hiervoor niet geautoriseerd zijn.

Zonder een goede informatiebeveiliging kunnen deze dreigingen leiden tot verstoring van gemeentelijke dienstverlening en verlies van publieke middelen.

---

[5] Zie voor meer context over deze cases: https://nos.nl/artikel/2557248-gemeente-hof-van-twente-moet-miljoenenschade-hack-echt-zelf-betalen of https://www.gld.nl/nieuws/7711385/zo-konden-hackers-toeslaan-bij-de-gemeente-buren

[6] De term ‘hackers’ wordt hier gebruikt om te verwijzen naar een brede typologie van kwaadwillenden die vanwege verschillende overtuigingen overgaan tot het inzetten van digitale middelen om zich toegang te verschaffen tot de informatiesystemen van organisaties.

2.4 Continuïteit van dienstverlening

Veel gemeentelijke processen zijn digitaal en afhankelijk van informatiesystemen. Denk aan:

- Vergunningaanvragen;
- Veiligheid in de stad;
- Paspoort- of rijbewijsaanvragen;
- Sociaal domein (zorg, werk, inkomen).

Een verstoring door bijvoorbeeld een cyberaanval kan ertoe leiden dat burgers (tijdelijk) geen toegang meer hebben tot deze essentiële diensten.

2.5 Verstoringen in het Openbare Domein

Naast gemeentelijke processen kan (vitale) infrastructuur in het Openbare Domein, zoals watervoorziening, elektriciteitsnetwerk, internetverbinding en bijvoorbeeld verkeerssystemen ook geraakt worden bij cyberdreigingen of incidenten gerelateerd aan informatiesystemen en -verwerking. De Operationele Techniek (OT) vergt in de meeste gevallen een separate aanpak en focus naast IT-gerelateerde processen binnen de fysieke locaties van de gemeente zelf.

2.6 Verlies van vertrouwen en reputatieschade

Burgers moeten erop kunnen vertrouwen dat de gemeente zorgvuldig met hun gegevens omgaat. Een incident kan leiden tot:

- Politieke en bestuurlijke gevolgen;
- Vertrouwensbreuk met burgers en bedrijven binnen de gemeente;
- Verhoogde druk op gemeentelijke medewerkers en de inzet van publieke middelen.

2.7 Toezicht en handhaving

De Autoriteit Persoonsgegevens (AP) en andere toezichthouders kunnen ingrijpen bij nalatigheid. Gemeenten kunnen sancties opgelegd krijgen, zoals:

- Boetes bij AVG-overtredingen;
- Aanwijzingen of dwangsommen;
- Verscherpt toezicht.

Kortom: de afhankelijkheid van informatiesystemen en het groeiende risico op dit domein leidt ertoe dat informatiebeveiliging (IB) steeds belangrijker wordt voor Nederlandse gemeenten en niet alleen als IT-vraagstuk moet worden benaderd, maar als continuïteitsvraagstuk voor gemeentelijke processen en dienstverlening.

3. Beantwoording hoofdvraag en deelvragen (bevindingen)

In dit hoofdstuk worden de onderzoeksvragen, zoals gesteld door de Rekenkamer beantwoord en de bevindingen uit het onderzoek gepresenteerd. Eerst wordt ingegaan op de algemene hoofdvraag en vervolgens de deelvragen in de onderliggende thema's: Opzet, Bestaan, Werking, Rol van de Raad, Bevindingen van de Operationele Testen. In paragraaf 3.6 wordt een weergave geboden van de belangrijkste bevindingen uit de uitgevoerde operationele testen.

3.1 Beantwoording hoofdvraag

3.1.1 "In hoeverre is de informatieveiligheid van de gemeente Hilversum gewaarborgd?"

De gemeente Hilversum heeft in de afgelopen jaren ingezet op het verhogen van haar weerbaarheid tegen risico's die de informatieveiligheid van systemen, interne en externe processen en (vertrouwelijke) informatie bedreigen. Uit de interviews, verstrekte documentatie en voorbeelden vanuit de dagelijkse praktijk wordt duidelijk dat de gemeente in de afgelopen jaren zich heeft ingezet om de informatieveiligheid op orde te krijgen. De gemeente heeft echter nog ruimte voor verbetering om over de assen 'opzet', 'bestaan' en 'werking' de informatieveiligheid volledig te kunnen waarborgen.

Uit de bevindingen blijkt dat de opzet van maatregelen in het aanwezige beleid en de procedures niet volledig is en dat een tweetal van de documenten nog de status 'concept' hebben (versies 2021 en 2024). De gemeente constateert zelf in haar gap-analyse[7] van 2025 aan 71%[8] van de maatregelen te voldoen en dat voor de overige maatregelen deze niet volledig zijn toegepast, niet te voldoen of niet van toepassing zijn. Een 100% score van de zelf-geselecteerde BIO-normen leidt echter tot het voldoen aan de richtlijn. Daarnaast worden maatregelen nu nog niet vanuit 'risico-denken' vormgegeven of geprioriteerd, wat een eis is van de NIS2. Overigens staat in het Strategisch Gegevensbescherming en Informatiebeveiligingsbeleid 2025 – 2029 versie 1.0 (verder Strategisch IB-beleid) dat risicogestuurd werken wel de ambitie is.

De BIO gaat ervan uit dat maatregelen kunnen worden aangetoond in opzet, bestaan en werking. Daarbij komt een zekere mate van documentatie, vastlegging, periodieke controle en vernieuwing kijken om zodoende aantoonbaar te maken dat maatregelen daadwerkelijk worden genomen. Onder de BIO2 verschuift de semi-vrijblijvende richtlijn van de BIO, naar een wettelijk verankerd kader dat wordt opgehangen aan de Cbw. Hiermee wordt het voeren van een adequaat Information Security Management Systeem (ISMS) wettelijk verplicht.

[7] Een gap-analyse toetst de gewenste status met de daadwerkelijke status. Door dit vergelijk te maken – in dit geval door de gemeente zelf gedaan t.o.v. de BIO – wordt duidelijk welke maatregelen wel en niet genomen zijn.
[8] Zie de uiteenzetting onder 3.3.1.1 voor inzicht in de scores uit de gap-analyse van de gemeente.

In het onderzoek komt naar voren dat het Information Security Management Systeem (ISMS) niet volledig is en dat genomen maatregelen, gemaakte afwegingen en specifieke uitwerkingen in procedures of werkinstructies niet aantoonbaar zijn gemaakt (zie voor verdere duiding de beantwoording van de deelvragen). Het ontbreekt aan vastgelegde periodieke controles en gemaakte afspraken daaromtrent.

Om als organisatie de informatiebeveiliging op orde te brengen kan het maturity model van informatiebeveiliging[9] handvatten bieden. Het model maakt inzichtelijk wat het volwassenheidsniveau van een organisatie is op het vlak van informatiebeveiliging. Zo is de afstemming tussen technische, organisatorische en mensgerichte maatregelen - die zowel in opzet, bestaan als in werking dienen te worden ontworpen op basis van de specifieke risico's die van toepassing zijn op de gemeente - geclassificeerd als 'herhaalbaar' (niveau 2). Een aantal tactische beleidsstukken ontbreken namelijk of hebben de status 'concept' (versies 2021 en 2024; zie bijlage 5.5). Hoffmann constateert overigens dat bepaalde processen en maatregelen richting het niveau 'gedefinieerd' (3) gaan, wat laat zien dat de organisatie in de goede richting beweegt.
De overige 29% van de maatregelen die de gemeente zelf definieert als 'deels' of 'niet' uitgevoerd leiden tot een score 'initieel' (1).

Uit de operationele testen, die de werking van het beleid in de praktijk toetsen, zijn verschillende aandachtspunten naar voren gekomen. De technische pentest laat zien dat het externe netwerk robuust en weerbaar is gebleken tegen een gesimuleerde aanval van buitenaf. Het interne netwerk is daarentegen, vanuit een greybox perspectief[10], niet weerbaar gebleken. Er zijn tekortkomingen vastgesteld waardoor onze ethische hacker uiteindelijk het netwerk en de systemen van de gemeente heeft weten over te nemen. De IT-afdeling van de gemeente is na het doen van deze bevindingen direct hiervan op de hoogte gesteld. De ethische hacker heeft geadviseerd om deze bevindingen direct te mitigeren en na de implementatie ervan een hertest te laten uitvoeren om te na te gaan of deze tekortkomingen zijn verholpen.

De bevindingen uit de inlooptest laten zien dat de mystery guest van Hoffmann is binnengedrongen op drie van de vier locaties waar de test is uitgevoerd. De mystery guest kon vrijelijk bewegen binnen de locaties en kon relatief eenvoudig gevoelige informatie bemachtigen uit open kasten en papier containers die niet op slot zaten[11].

Tot slot blijkt uit de mailphishingtest dat 36% van de medewerkers die deze mail heeft ontvangen, heeft geklikt op de link in de mail en inloggegevens heeft achtergelaten. De gemeente Hilversum zit hiermee

[9] Zie bijlage 5.1: Maturity Model, voor een verdere duiding van deze volwassenheidsniveaus.
[10] Met een greybox pentest wordt in de context van dit rapport een penetratietest bedoeld waarbij de tester vooraf beperkte accountgegevens en toegangsrechten tot de doelomgeving heeft gekregen, zodat realistische aanvalsscenario's met gedeeltelijke voorkennis konden worden gesimuleerd.
[11] De gemeente gebruikt twee papieren containers: een container voor oud papier en karton en een container voor gevoelige informatie en persoonsgegevens. Er is gevoelige informatie aangetroffen in een niet afgesloten papiercontainer.

ruim boven het gemiddelde van 15% dat bij vergelijkbare organisaties wordt vastgesteld. Dit onderbouwt dat het bewustzijn van medewerkers rondom insluiping en mailphishing niet voldoende is.

3.2 Beantwoording Onderzoeksvragen 'Opzet'

3.2.1 Welk beleid heeft de gemeente vastgesteld op het gebied van informatieveiligheid en hoe is dit beleid uitgewerkt in regels, procedures en werkprocessen?

De gemeente Hilversum hanteert haar Strategisch IB-beleid als leidraad voor de inrichting en aanpak van Informatiebeveiliging en Privacy. In dit beleid stelt de gemeente de Baseline Informatiebeveiliging Overheid (BIO) na te leven en geldende wetgeving[12] te volgen. Het Strategisch IB-beleid geldt als abstract document. Verdere uitwerking dient te worden gevonden in "... werkplannen, procedures en werkinstructies." (pg. 7).

Het Strategisch IB-beleid van de gemeente heeft als doel om het volgende te realiseren (pg. 9):

- Garanderen van correcte en veilige informatievoorzieningen en -systemen.
- Adequate bescherming van (persoons)gegevens en het toepassen van dataminimalisatie.
- Managen van de informatiebeveiliging en het beschermen van (kritieke) bedrijfsprocessen.
- Minimaliseren van risico's van menselijk handelen.
- Voorkomen van ongeautoriseerde toegang tot informatievoorzieningen en -systemen.
- Adequaat reageren op incidenten en bewaken van de rechten van betrokkenen.
- Voldoen aan de wettelijke verplichtingen.

Aanvullend beschrijft de gemeente in te zetten op een *'three lines of defense'*-model waarin 1) lijnmanagement verantwoordelijk is "voor het realiseren van gegevensbescherming en IB-maatregelen in eigen processen.", 2) de Information Security Officer (ISO) en Privacy Officers (PO) hierbij adviseren en ondersteunen, en 3) de interne auditor, Chief Information Security Officer (CISO) en de Functionaris Gegevensbescherming (FG) de organisatie van een objectief oordeel voorzien en het toezicht vormgeven.

Verder stelt de organisatie dat ze zich laat "… leiden door een objectieve beoordeling van de risico's." (pg. 5), waarbij de focus op processen binnen de organisatie en de samenwerking met de afdelingsmanagers van belang is voor het nemen van effectieve maatregelen.

Het Strategisch IB-beleid is van toepassing op "… alle gemeentelijke processen, onderliggende informatiesystemen, procesautomatisering, informatie en gegevens van de gemeente en externe partijen… Ook de fysieke toegangsbeveiliging is onderdeel van (red.) dit beleid. … Alle procesautomatiseringssystemen die binnen de gemeentelijke gebouwen en in de publieke ruimte van de gemeente worden

[12] Opsomming die wordt gegeven in het Strategisch IB-beleid: AVG, UAVG, Wpg, Bpg, AI Act, Cbw, BRP, PNIK/PUN, DigiD en Suwi.

gebruikt, die van de gemeente zijn, zoals gebouwbeheersystemen en bijvoorbeeld cameratechnologie of verkeersregelinstallaties en gemalen maken ook onderdeel uit van dit beleid." (pg. 7).

Naast het Strategisch IB-beleid, hanteert de organisatie een tweejaarlijkse cyclus voor het Tactisch Informatiebeveiligingsplan[13]. In dit onderliggende plan worden de onderwerpen benoemd waar de gemeente in de desbetreffende twee jaar haar focus op wil leggen. Hierin worden met name de gaten uit de conceptversie van de tweejaarlijkse 'gap analyse' op de BIO geadresseerd[14]. Oftewel: welke maatregelen die worden genoemd in de BIO zijn nog niet genomen door de organisatie?

Uit de documentanalyse en interviews ontstaat het beeld dat de verdere uitwerking van beide relatief abstracte beleidsstukken in verdere procedures of werkinstructies (ten dele) wordt uitgevoerd vanuit de afdelingen die verantwoordelijk zijn voor deze processen. Zie 3.2.2. voor een verdere analyse.

3.2.2 Heeft de gemeente de beleidsstukken die de Baseline Informatiebeveiliging Overheid (BIO) voorschrijft?

In Bijlage 5.6 is een overzicht opgenomen van 25 onderwerpen die de BIO voorschrijft waarop overheidsorganisaties geacht worden om beleid te ontwikkelen, dit uit te werken voor specifieke processen en om te zetten in concrete uitwerkingen zodat deze maatregelen kunnen worden geïmplementeerd in de organisatie.

Kijkende naar de aangeleverde beleidsstukken in relatie tot de geïdentificeerde onderwerpen binnen de BIO (zie bijlage 5.5 en 5.6) komt Hoffmann tot het volgende inzicht:

- 9 van de 25 onderwerpen worden geadresseerd (36%). Waarvan 4 van deze beleidsstukken 4 jaar of ouder zijn en niet periodiek worden herzien.
- 2 van de 25 onderwerpen worden geadresseerd in concept-stukken (8%). Het is onduidelijk of deze stukken ook gelden in de organisatie als geaccepteerd beleid.
- 14 van de 25 onderwerpen worden niet geadresseerd in beleidsstukken (56%). Op basis van de afgenomen interviews en de uitgevoerde operationele testen wordt operationele uitvoer (ten dele) aannemelijk geacht, maar niet of verminderd aantoonbaar.

3.2.3 Wat heeft de gemeente Hilversum tot nu toe ondernomen om aan de zorgplicht van de nieuwe EU-richtlijn (NIS2) te voldoen?

Uit de interviews blijkt dat de gemeente zich bewust is van de NIS2 en de doorvertaling hiervan naar de Cyberbeveiligingswet (Cbw) en dat dit invloed gaat hebben op de vernieuwing van de BIO naar de BIO2. In de aangeleverde stukken blijkt dit ook uit een informatieve flyer: "Wat betekent de NIS2 voor gemeente Hilversum?". Ook geeft men aan dit besproken te hebben en in de gaten te houden.

[13] Het huidig geldende Tactisch Beleid is dat van 2024-2025.
[14] De gemeente heeft hiervoor het document 'Hilversum GAP Analyse BIO 2025 Normen-Controls-Controlepunten CONCEPT.pdf' gedeeld met de onderzoekers. Aangezien dit document een 'concept' is, adviseert Hoffmann om rekening te houden met eventuele afwijkingen van de definitieve versie. Het stuk was echter dusdanig volledig en verschillend van de gap-analyse uit 2023 dat het document is gebruikt voor een onderbouwing van de bevindingen.

Het is echter niet aantoonbaar welke stappen er zijn genomen om te voldoen aan de zorgplicht[15]. Er is geen analyse aanwezig van waaruit blijkt dat het duidelijk is voor de gemeente wat er precies verandert en wat dit specifiek betekent voor de gemeente. Bijvoorbeeld als het gaat om het nieuwe IB-beleid, dat is vastgesteld voor de periode 2025-2029. Dit beleid gaat uit van de BIO, terwijl de BIO2 op 23 september 2025 is vastgesteld. Op moment van schrijven van het strategische beleid had meer rekening gehouden kunnen worden met toekomstige wetgeving. Er waren op dat moment al meerdere aankondigingen en voorpublicaties over de BIO2 geweest. Er had bijvoorbeeld ook voor gekozen kunnen worden om het bestaande beleid met een jaar te verlengen, in afwachting van de wettelijke verankering van Europese wetgeving in de Cbw (en een mogelijke verplichtstelling van de BIO2)[16].

Daarnaast heeft de NIS2 niet alleen impact op de Cbw en daarmee op de BIO, maar ook op de Wet weerbaarheid kritieke entiteiten (Wwke). Deze wetgeving is specifiek opgesteld ter bescherming van kritieke entiteiten, waaronder gebouwen en systemen in de openbare ruimte – volgens de gemeente valt ook dit binnen de reikwijdte van haar Strategisch IB-beleid. De impact van deze wetgeving is niet verder uitgewerkt door de gemeente.

3.2.4 Welke risico's kent de gemeente op het vlak van informatiebeveiliging?

De gemeente heeft geen overzicht aangeleverd van de risico's op het vlak van informatiebeveiliging of een beleid omtrent risicomanagement[17]. Wel blijkt uit de gesprekken en uit aangeleverde stukken[18] dat men zich bewust is van risico's in de algemene zin voor de organisatie. Hoewel het strategisch IB-beleid stelt uit te gaan van 'risico gebaseerd' denken en het objectief beoordelen van risico's binnen processen, is dit niet aantoonbaar in de praktijk gebracht.

In hoofdstuk 2 van dit rapport is door Hoffmann een korte omschrijving van verschillende risicogebieden opgenomen om het belang van Informatiebeveiliging voor gemeenten te duiden.

[15] Aantoonbare elementen zouden bijvoorbeeld een uitgevoerde impactanalyse kunnen zijn, het adresseren van de BIO2 in het Strategische IB-beleid, het overleggen van notulen van een vergadering waarin dit besproken is en keuzes zijn gemaakt of dat de inhoudelijke onderwerpen vanuit de BIO2 (en vooral de gewijzigde elementen) expliciet aandacht krijgen in beschikbaar beleid of in gesprekken met functionarissen. Deze elementen zijn niet aangetroffen door Hoffmann tijdens het onderzoek.

[16] https://www.bio-overheid.nl/category/producten/bio

[17] Hoffmann is bij het uitvoeren van onderzoek afhankelijk van de door de gemeente beschikbaar gestelde documentatie. De bevindingen worden op de aangeleverde informatie gebaseerd (en compleet verondersteld). Na afronding van de feitenverzameling gaf de gemeente aan over (aanvullende) documentatie c.q. informatie te beschikken met betrekking tot deze risico's. Het betreft het Jaarverslag van de Gemeente, echter dit document is niet aangeleverd of genoemd tijdens de gesprekken over risicomanagement. Dit kon dus niet meer meegenomen worden in het onderzoek.

[18] Zoals bv. Managementletters, PIT-rapportages, Tactisch Beleid, e.a.

3.3 Beantwoording Onderzoeksvragen 'Bestaan'

3.3.1 In hoeverre worden deze regels, procedures en werkprocessen in de dagelijkse uitvoeringspraktijk ook daadwerkelijk gehanteerd?

Om antwoord te geven op deze vraag, heeft Hoffmann gekeken naar twee zaken: de zelfbeoordeling van de gemeente, en het beeld wat naar voren komt vanuit de interviews en de uitgevoerde operationele testen (zie paragraaf 3.6).

3.3.1.1 Zelfbeoordeling BIO-compliancy

Iedere twee jaar voert de gemeente een 'gap-analyse' uit waarbij zij zelf kijkt naar de mate van compliancy (het voldoen aan) aan de BIO-normen. Hierover wordt ook gerapporteerd binnen de gemeente. Uit het concept van 2025 blijkt dat de gemeente zelf stelt:

- Aan 71% van de maatregelen te voldoen,
- Aan 5% van de maatregelen niet te voldoen,
- En aan 18% van de maatregelen gedeeltelijk te hebben voldaan,
- Verder wordt 6% van de maatregelen als 'niet van toepassing' verklaard.

Op basis van deze zelfbeoordeling van de gemeente, is de gemeente niet compliant aan de BIO, maar is zij wel gegroeid ten opzichte van de uitgevoerde analyse in 2023. Uit de documentatie kan niet worden vastgesteld dat de gemeente een toets heeft gedaan of er sprake is van specifieke beveiligingsniveaus (BBN-1, 2 of 3) en op basis daarvan – en andere relevante factoren – specifieke beveiligingsmaatregelen als 'niet van toepassing' heeft verklaard.

Uit de gap-analyse blijkt dat er geen eenduidig proces is op basis waarvan de beoordeling is uitgevoerd. Zo wordt er soms tekstueel beschreven dat "een gedeelte is opgenomen", terwijl de score vervolgens op "Ja, compliant – groen" wordt geplaatst. Ook blijkt dat operationele uitvoer van een maatregel als afdoende wordt geacht, terwijl men zelf aangeeft: "Er is geen procedure, maar we doen het wel." Verder wordt er verwezen naar het Strategisch IB-beleid wanneer er gevraagd wordt om een procedure of werkinstructie of worden maatregelen "niet van toepassing" verklaard, omdat er op dit moment "geen oplossing voor is die wordt gedragen[19]". Hoffmann plaatst hierbij de kanttekening dat de 'gap-analyse' van 2025 in concept is gedeeld met de onderzoekers. Er kunnen mogelijk kleine verschillen zitten in het document met de definitieve versie van de gap-analyse.

3.3.1.2 Beeld vanuit interviews en operationele testen

Hoewel onderwerpen in beleidsstukken worden benoemd, ontbreken uitgewerkte procedures en werkprocessen vaak. Daardoor kan Hoffmann niet vaststellen dat deze processen daadwerkelijk bestaan.

[19] Geparafraseerd door Hoffmann voor de leesbaarheid van het rapport. Zie de beschrijving van maatregelen rondom dataclassificatie in de concept gap-analyse van 2025.

Uit de interviews blijkt echter dat veel onderwerpen niet onbekend zijn en uit de operationele testen blijkt dat veel maatregelen in de praktijk wel (ten dele) worden uitgevoerd.[20]

De BIO gaat er echter wel vanuit dat maatregelen kunnen worden aangetoond in opzet, bestaan en werking. Daarbij komt een zekere mate van documentatie, vastlegging, periodieke controle en vernieuwing kijken om zodoende aantoonbaar te maken dat maatregelen daadwerkelijk worden genomen. Het gaat hierbij niet om de invulling van specifieke audits, maar om de weerbaarheid van de organisatie als geheel. Onder de BIO2 verschuift de semi-vrijblijvende richtlijn van de BIO, naar een wettelijk verankerd kader dat wordt opgehangen aan de Cbw. Hiermee wordt het voeren van een adequaat Information Security Management Systeem (ISMS) wettelijk verplicht.

3.3.2 In hoeverre zijn er adequate middelen (budget en capaciteit) beschikbaar gesteld om de informatiebeveiliging te waarborgen?

De gemeente heeft een Chief Information Security Officer (CISO) aangesteld, daarnaast een CISO met technische affiniteit die zich eveneens begeeft op het vlak van Enterprise Architectuur en aanvullend komt er met de aankomende fusie met de gemeente Wijdemeren nog een technische ISO (TISO) binnen het team. Het team kent de organisatie, is gemotiveerd en werkt gestructureerd in met name de kwartaal Privacy en Informatiebeveiliging-rapportages (PIT) richting de organisatie. Het team is *hands-on* en gericht op het faciliteren en begeleiden van de organisatie en fungeert daarmee met name in de 2e lijn. De toezichthoudende activiteiten die benodigd zijn om invulling te geven aan de 3e-lijnspositie zijn verminderd aanwezig.

Vanuit dit team wordt er nauw samengewerkt met de Privacy Officers en de Functionaris Gegevensbescherming (FG). Hiermee wordt in gezamenlijkheid het Strategisch IB&P-beleid vormgegeven en ieder kwartaal invulling gegeven aan de al genoemde PIT-rapportages waarin de voortgang en uitdagingen rondom IB&P-activiteiten worden benoemd.

Daarnaast wordt er vooral samengewerkt met ICT en Facilitair rondom het vormgeven van concrete maatregelen en Informatiemanagement als het gaat om het opstellen van beleid.

Budgettair gezien is de inzet op IB-maatregelen niet uitgesplitst of inzichtelijk gemaakt. Ook vanwege de afwezigheid van het nemen van maatregelen op basis van risico's en daaraan gekoppelde plannen, incl. budgettaire uiteenzetting, maakt dit dat het niet mogelijk is om een objectieve beoordeling uit te voeren op de adequaatheid van middelen.

[20] Hoffmann is bij het uitvoeren van onderzoek afhankelijk van de door de gemeente beschikbaar gestelde documentatie. De bevindingen worden op de aangeleverde informatie gebaseerd (en compleet verondersteld). Na afronding van de feitenverzameling gaf de gemeente aan over de volgende (aanvullende) documentatie c.q. informatie te beschikken (dit kon echter niet meer meegenomen worden in het onderzoek): er zijn uitgewerkte procedures en/of werkprocedures vastgelegd als Kennisitem in TOPdesk. De BIO vereist dat relevante beleidsstukken aantoonbaar moeten worden vastgelegd. Mogelijk zijn relevante beleidsstukken dus wel (aanvullend) aanwezig maar konden die t.t.v. het onderzoek niet (tijdig) worden aangeleverd.

3.3.3 Hoe informeert de gemeente Hilversum haar inwoners over de maatregelen die worden getroffen inzake informatiebeveiliging?

De gemeente onderneemt geen specifieke activiteiten om haar inwoners te informeren over de getroffen maatregelen inzake informatiebeveiliging. De informatie op dit vlak is beschikbaar via de raadsvergaderingen en de raadsleden die daaraan deelnemen. Gedeelde documentatie en de bespreking daarvan is (in de meeste gevallen[21]) niet openbaar beschikbaar en wordt gepubliceerd in een online omgeving (zie 3.5.1).

3.4 Beantwoording Onderzoeksvragen 'Werking'

3.4.1 Voert de gemeente Hilversum steekproeven en/of pentesten uit en, zo ja, met welk resultaat/effect?

Hoewel de gemeente geen planning heeft voor periodieke steekproeven en/of pentesten, is er geconstateerd dat er:

- Door de gemeente zelf middels 'BITsight' (technische tooling) gekeken wordt naar kwetsbaarheden op het netwerk van buitenaf. Uit de rapportage van augustus 2025 komt het beeld naar voren dat de gemeente hoog in het niveau 'intermediate' (gemiddeld) scoort en dicht bij 'advanced' (gevorderd) zit. Dit beeld kan ook worden onderbouwd met de uitkomsten van de pentest uitgevoerd als onderdeel van dit onderzoek (zie paragraaf 3.6).
- Door de gemeente zelf middels het 'DIP platform' (technische tooling) gekeken wordt naar kwetsbaarheden voor de websites van de gemeente. Hieruit komt naar voren dat "40 van de 62 websites niet voldoen aan beveiligingsstandaarden"[22].
- In 2023 is een 'pentest' uitgevoerd op de infrastructuur, werklaptops en de 'restricted desktop environment'. Hierin werden 2 'high risks' (hoog risico) bevindingen gedaan, 6 'medium risks' en 4 'low risks'.

Het is op basis van het gedane onderzoek niet duidelijk of de bevindingen uit de rapportages ook allemaal zijn opgevolgd. Er heeft geen aantoonbare hertest plaatsgevonden na het eventuele oplossen van de bevindingen.

3.4.2 Zijn de systemen en informatie van de gemeente Hilversum toegankelijk voor onbevoegden?

De gedetailleerde verslagen van de gevonden kwetsbaarheden op fysiek vlak, menselijk gedrag en technische weerbaarheid zijn weergegeven in de vertrouwelijke bijlages van deze rapportage. In algemene zin zijn de volgende bevindingen gedaan:

- Het gemeentelijke netwerk bleek op afstand niet toegankelijk voor onbevoegden. Hoffmann is niet op directe wijze in staat geweest om (extern) toegang te verkrijgen tot het netwerk middels de technische penetratie die is uitgevoerd.

[21] Stukken die als vertrouwelijk worden gezien, worden enkel beschikbaar gesteld voor de Raadsleden.
[22] Status uit het DIP-dashboard op 7 augustus 2025.

- Middels een uitgevoerde phishing-simulatie heeft Hoffmann van 485 medewerkers (36%)[23] de inloggegevens (gebruikersnaam en wachtwoord) ontvangen. Het klikken op de phishinglink kan, afhankelijk van de gebruikte techniek, al leiden tot ongewenste cyberactiviteiten. Een deel van de medewerkers heeft daarnaast ook daadwerkelijk inloggegevens ingevoerd, waardoor de potentiële impact toeneemt. De betreffende inlogsessies waren beveiligd met tweefactorauthenticatie, waardoor niet direct toegang tot het netwerk kon worden verkregen. In de praktijk kan het beschikken over geldige inloggegevens echter op verschillende manieren worden misbruikt en onder omstandigheden alsnog bijdragen aan toegang tot systemen of netwerken. Deze vervolgmogelijkheden zijn door Hoffmann niet uitgevoerd of getest, gezien de afgebakende scope van deze penetratietest. Binnen het cyberdomein blijft gelden dat één menselijke fout kan leiden tot verstrekkende gevolgen voor de organisatie. Het risico wordt in dit geval vergroot doordat een relatief groot aantal medewerkers op de phishinglink heeft geklikt en een substantieel deel inloggegevens heeft achtergelaten.
- Het gemeentelijk netwerk bleek op locatie onvoldoende weerbaar. Door beperkte fysieke toegangsbeveiliging en onvoldoende netwerksegmentatie konden de onderzoekers toegang verkrijgen tot het interne netwerk. Vanuit een onbeveiligd apparaat was het mogelijk om beheerdersrechten te verkrijgen, wat resulteerde in een groot aanvalsoppervlak en een reëel risico op volledige compromittering van het netwerk en onderliggende systemen en accounts[24].
- De bevindingen die het verkrijgen van beheerdersrechten mogelijk maakten, zijn gedurende het onderzoek gedeeld met de IT-afdeling. Hoffmann adviseert deze bevindingen met prioriteit te mitigeren, met aandacht voor netwerktoegangsbeveiliging, netwerksegmentatie, rechtenbeheer en wachtwoordbeleid. Na implementatie wordt geadviseerd een hertest uit te laten voeren.
- Op basis van de interviews en de constatering tijdens de technische penetratietest, is het tevens mogelijk voor interne medewerkers –met brede toegangsrechten – om onbevoegd toegang te krijgen tot systemen en informatie. Dit is gebaseerd op de volgende geconstateerde kwetsbaarheden:
    - De afwezigheid van een sluitend ‘indienst-uitdienst’-proces;
    - De afwezigheid van *risk based*-autorisatiematrices voor alle kritieke informatiesystemen;
    - De afwezigheid van een periodieke check en update van bovenstaande componenten;
    - De mogelijkheid tot exfiltratie van data uit (een deel van de) systemen;
    - De realiteit dat externen decentraal ingehuurd worden en vaak hun eigen laptop gebruiken.

[23] Hoffmann vindt bij de meeste phishing-exercities een score van 15%. De gemeente Hilversum zit met deze score ruim boven het gemiddelde.

[24] De toegang tot het netwerk kon pas worden verkregen nadat de gemeente de door Hoffmann gebruikte apparatuur had vrijgegeven en een account aan de onderzoeker had verstrekt. Dat neemt niet weg dat de geconstateerde kwetsbaarheden ook relevant zijn voor kwaadwillenden die deze toegang niet hebben gekregen. De gemeente geeft aan bekend te zijn geweest met de gevonden kwetsbaarheid. Hiervoor stonden een drietal projecten “aangekondigd” voor 2025, maar deze zijn omwille van de fusie met de gemeente Wijdemeren naar achter geschoven.

3.4.3 Op welke onderdelen is er ruimte voor verbetering op het vlak van informatiebeveiliging?

Hoffmann constateert op basis van het gedane onderzoek, dat er ruimte voor verbetering is voor de gemeente op, o.a., de volgende onderwerpen:

- Het Information Security Management Systeem (ISMS) van de gemeente Hilversum is niet volledig en bemoeilijkt het 'aantoonbaar maken' van afwegingen en keuzes rondom IB-risico's en -maatregelen door de gemeente. Hoewel elementen wel afdoende zijn uitgewerkt (zoals bv. scoping, verantwoordelijkheden van managementposities, de zogenaamde 'PIT-rapportages' en het uitvoeren van een gap-analyse), ontbreken er belangrijke elementen die noodzakelijk zijn om genomen stappen aantoonbaar te maken, periodieke controles uit te zetten, beleid door te vertalen naar procedures of werkinstructies, gezamenlijk tot doelstellingen te komen en om risico-gebaseerd te werken. Bovenal leidt een gebrekkig ISMS in de meeste gevallen tot een moeizame bestuurbaarheid van IB-risico's en het effectief hanteren van de PDCA-cyclus.
- Risico gebaseerd werken wordt in het Strategisch IB-beleid gepositioneerd als kern en basis van de activiteiten op IB-vlak, maar er is geen Risicomanagement beleid, er is geen consensus over wat de belangrijkste IB-risico's zijn voor de gemeente of voor specifieke afdelingen, er zijn geen risicoanalyses uitgewerkt of een methodiek beschreven, er is geen centraal risico register en er zijn geen risico evaluatie criteria afgestemd om IB-risico's te kunnen classificeren of bespreekbaar te maken. Hoewel de samenwerking wordt gezocht met Concern Control, is hier in de praktijk nog geen aantoonbare manier van samenwerken in gevonden die leidt tot 'risico gebaseerd' werken.
- Het IB-bewustzijn van medewerkers van de gemeente Hilversum kan verder worden versterkt. Zowel in algemene zin, als in het toepassen van dat bewustzijn op de processen en systemen waarin en waarmee zij zelf werken. Met name de uitkomsten van de phishingtest door Hoffmann als onderdeel van deze rapportage maken dit inzichtelijk.
- Een sluitend 'Identity- & Access Management'-proces zorgt voor een vertrouwensbasis voor gebruikers en beheerders van informatiesystemen en het netwerk van de gemeente. Wanneer toegewezen 'Identiteiten' niet gecontroleerd en sluitend beheerd kunnen worden, is het veilig houden van informatiesystemen binnen de gemeente een uitdaging. Hiervoor is een samenwerking nodig tussen ICT, HR en de verantwoordelijk manager. Daarbij zijn periodieke controles en onderlinge afstemming tussen de afdelingen cruciaal.
- Middels het vergroten van Logging & Monitoring-capabilities en de analyse van deze data middels een SOC/SIEM-oplossing, kan de gemeente ook reageren op afwijkend gedrag binnen haar informatiesystemen. Zodoende ontstaat er sneller de gelegenheid om in te grijpen bij incidenten, te reageren op afwijkend gedrag en interne controle uit te oefenen rondom informatie met een verhoogd vertrouwelijk karakter.
- Leveranciersmanagement wordt een steeds belangrijker onderwerp – ook aangezet in de BIO2. Dit heeft te maken met de groeiende samenwerking tussen gemeenten en externe leveranciers van informatiesystemen, maar ook met de wettelijke verplichting (o.b.v. de Cbw) om zicht te houden op de risico's binnen 'de keten'. Ook voor de gemeente vraagt dit om beleid te hebben

op dit onderwerp, dit eenduidig uit te dragen, voorwaarden te stellen aan leveranciers, deze samenwerking op te nemen in het incidentmanagementproces en periodieke controles uit te oefenen op gemaakte afspraken.

3.4.4 Zijn raadsleden, B&W en ambtenaren zich bewust van de risico's en regels op het gebied van informatieveiligheid en weten zij wat ze moeten doen wanneer zij met een verdachte situatie te maken krijgen?

Uit interviews met de portefeuillehouder, ambtenaren en een raadssessie waarin expliciet is nagegaan in hoeverre raadsleden zich bewust zijn van de relevante risico's en bijbehorende regels rondom informatiebeveiliging, komt het beeld naar voren dat men[25] zich bewust is van het belang van informatiebeveiliging voor de gemeente. In algemene zin is het duidelijk dat 'men risico loopt' en dat het onderwerp van 'toenemend belang is'. In alle gesprekken worden voorbeelden gegeven van specifiekere risico's die een impact kunnen hebben op de continuïteit van gemeentelijke processen, de privacy van burgers en mogelijk misbruik van informatie.

Hoewel er een operationeel meldingsloket aanwezig is en meldingen ook direct vanuit de mail gedaan kunnen worden, ontstaat de indruk dat ook informele lijnen van groot belang zijn binnen de gemeente. Men weet elkaar te vinden, de lijnen zijn kort. Tegelijkertijd is er geen uitgewerkt incidentmanagementproces en is ook niet aantoonbaar vastgesteld dat er periodiek geoefend[26] wordt op incidentscenario's.

3.5 Beantwoording Onderzoeksvraag 'Rol van de Raad'

3.5.1 Op welke manier wordt de gemeenteraad geïnformeerd over de uitvoering van het beleid rondom informatiebeveiliging? Welke mogelijkheden heeft de raad om te sturen en te controleren?

In onderstaande tabel staan de mogelijkheden opgenoemd waarop de gemeenteraad geïnformeerd kan worden over de uitvoering van het beleid rondom informatiebeveiliging. Vanuit het gesprek met een afvaardiging van de Raad komt naar voren dat deze uiteenzetting niet volledig is, maar dat er op basis van informele lijnen de ruimte is om door te vragen en aanvullende informatie op te vragen.

[25] De onderzoeksvraag richt zich op het overkoepelende bewustzijn van risico's en regels rond informatiebeveiliging binnen de bestuurlijke context, niet op verschillen tussen afzonderlijke doelgroepen. De kwalitatieve onderzoeksmethoden (interviews en raadssessie) lenen zich bovendien voor een integrale duiding van patronen en rode draden.

[26] Onder periodiek oefenen wordt verstaan: planning van incidentscenario's binnen de organisatie en een vastlegging van de evaluatie en 'lessons learned' vanuit deze oefeningen. Het gaat bijvoorbeeld niet om incidentele (crisis)oefeningen.

Middel	Beschrijving	Uitvoering
ENSIA Rapportage	De jaarlijkse ENSIA-rapportage is een zelfevaluatie die door de CISO van de gemeente wordt uitgevoerd, wordt gecontroleerd door middel van een externe Auditor en goedgekeurd door het College van Burgemeesters en Wethouders. Daarna worden de stukken aan de raad beschikbaar gesteld middels een raadsinformatiebrief met de (geheime) stukken via de procedure van de griffie met het geheime kastje.	Ja
Raadsinformatiebrieven	Raadsinformatiebrieven worden opgesteld bij specifieke onderwerpen om de Raad te informeren. Denk hierbij aan aankomende wetgeving, IB- of privacy-incidenten, wijziging van beleid of concrete dreigingen. Dit is echter geen vast of gepland onderdeel door het jaar heen.	Deels
Themabijeenkomsten	In 2024 is er een themabijeenkomst rondom Informatiebeveiliging georganiseerd om de Raad te informeren over het onderwerp en het belang hiervan voor de gemeente. Dit is geen vast of gepland onderdeel dat periodiek plaatsvindt.	Deels
Planning & Control Rapportages	Rapportages vanuit de Planning & Control-cyclus bevatten elementen van Informatiebeveiliging, maar geven in de praktijk geen volledig beeld van de IB-status en de relevante risico's voor de gemeente.	Deels
Audit Rapportages	Rapportages vanuit audits door externe partijen zorgen voor een objectieve momentopname of 'blik van buiten' over de status van Informatiebeveiliging binnen de gemeente. Er is echter geen structurele planning rondom Informatiebeveiliging specifiek beschikbaar[27].	Ja
Interne Dashboards of vaste rapportage	Dashboards of rapportages vanuit risicomanagement perspectief zijn momenteel niet aanwezig. Vanuit een dergelijk mechanisme worden gemeentelijke doelstellingen voorzien van risico's en daaropvolgend concrete maatregelen geformuleerd. De logica is vergelijkbaar met de P&C-cyclus, maar spitst zich specifiek toe op IB-onderwerpen. Hierbij is het wenselijk zoveel mogelijk aan te sluiten bij (kritieke) processen binnen de gemeente. Om het overzichtelijk te houden kan er op strategisch niveau naar de Raad gecommuniceerd worden, terwijl er op tactisch niveau binnen de afdelingen een verdiepingsslag op de risico's en de maatregelen plaatsvindt.	Nee

[27] De gemeente geeft in ambtelijk wederhoor aan dat er een planning tot uiting komt in het tactische jaarplan en in de ENSIA rapportage. Team concern control geeft geplande opdrachten voor externe audits. Dat is echter niet wat hier wordt aangehaald. Het betreft het feit dat geen structurele planning is aangetroffen specifiek gericht op Informatiebeveiliging. Denk hierbij aan een jaarlijks IB-programma met onder meer periodieke risicoanalyses, actualisatie van beleid, interne controles, awareness-activiteiten, kwetsbaarheidsscans en opvolging van verbeterpunten. Zo'n structurele planning is noodzakelijk om systematisch te sturen op de opzet, het bestaan en de werking van de BIO-maatregelen.

3.6 Bevindingen uit de Operationele testen

Vanwege de gevoeligheid van de bevindingen en om eventueel misbruik te voorkomen, worden de bevindingen in deze paragraaf uitsluitend op hoofdlijnen beschreven. Het specifieke verloop van de testen en de bijbehorende details worden niet openbaar gemaakt, maar zijn op basis van *need-to-know* separaat gedeeld met de gemeente en de Rekenkamer.

3.6.1 Samenvatting 'phishingtest'

Een van de operationele testen binnen dit onderzoek betrof een zogenaamde 'phishingtest' waarbij er een scenario wordt nagebootst waarin medewerkers van de gemeente een malafide e-mail ontvangen. Hierbij is het van belang te beseffen dat in deze test gekeken wordt naar het handelen van medewerkers en niet of het technisch een realistisch scenario is. Deze e-mail bevat in dit geval een link, van waaruit de medewerker wordt verzocht om zijn of haar inloggegevens te delen. Door in te spelen op het vertrouwen van de medewerker in combinatie met een beloningscomponent, kan het verleidelijk zijn voor onoplettende of ongetrainde medewerkers om gegevens te verstrekken. Een bewuste interne medewerker herkent dergelijke pogingen, vertrouwt dergelijke e-mails niet en is zich bewust van de gevaren van onzorgvuldig handelen.

Vanuit de test binnen de gemeente Hilversum blijkt dat 36% van de ontvangers heeft geklikt op de link en haar inloggegevens heeft achtergelaten.

De gemeente Hilversum zit hiermee ruim boven het gemiddelde van 15% dat bij vergelijkbare organisaties wordt vastgesteld. Dit onderbouwt dat het bewustzijn van medewerkers rondom ontvangen *phishing mails* niet voldoende is. Wel blijkt dat de 'tweefactorauthenticatie' van de gemeente haar werk doet en voorkomt dat er direct misbruik gemaakt kan worden van de verkregen inloggegevens.

Tijdens de phishingtest raadpleegden sommige medewerkers collega's, de CISO of de servicedesk om te verifiëren of het om spam ging. Meerdere medewerkers markeerden het bericht als spam en een aantal medewerkers gaf aan dat er een waarschuwing op het intranet geplaatst zou moeten worden.

De phishingcampagne is zorgvuldig voorbereid en afgestemd met de directie, de CISO, de betrokken ICT-medewerker, de servicedesk en de Rekenkamer. Er zijn duidelijke afspraken gemaakt en er is rekening gehouden met mogelijke effecten op medewerkers. Na afloop is er vanuit de Rekenkamer een e-mail verstuurd waarin alle medewerkers zijn geïnformeerd over de gevaren van phishing en hoe zij de e-mail hadden kunnen herkennen. Hiermee is direct aandacht gecreëerd voor het onderwerp en is de bewustwording vergroot.



Fijne Sinterklaas!

DG De geschenkencommissie<geschenkencommissie@feestdagen-geschenken.nl>
Aan:

Beste collega,

Wij wensen je een fijne Sinterklaas toe! Om extra te kunnen genieten van deze feestdag bieden wij alle collega's een geschenk aan. Je kan kiezen uit een verschillende smaken pepernoten of een overheerlijke chocoladeletter.

Via onderstaande pagina kan je jouw voorkeur doorgeven voor het geschenk dat je wilt hebben. Log in met je gemeente Hilversum account zodat wij je voorkeur kunnen verwerken.

hilversum.feestdagen-geschenken.nl

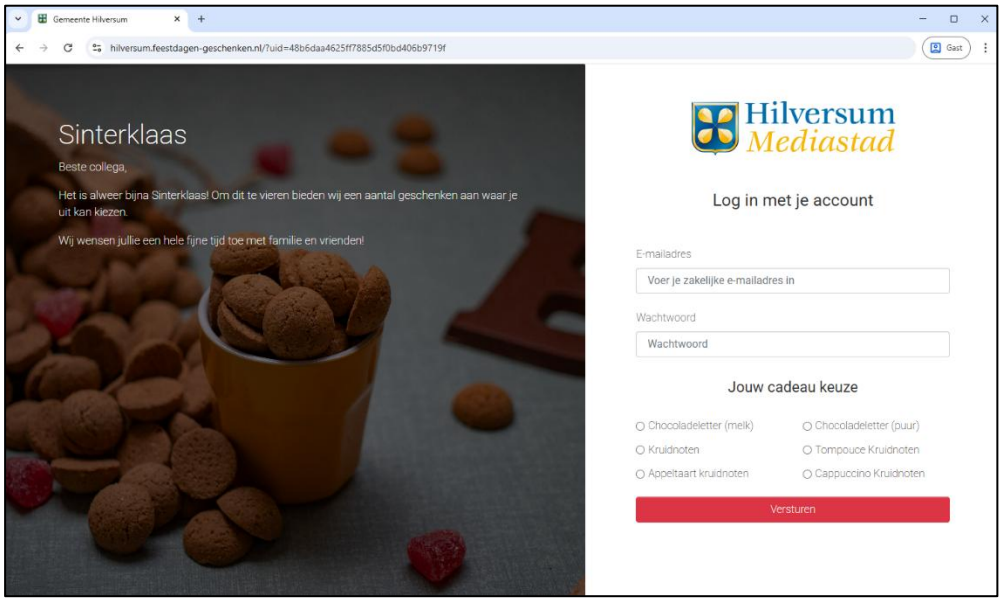
Van een aantal cadeaus is maar een beperkt aantal te bestellen, wees er dus snel bij!

Met vriendelijke groet,

De geschenkencommissie

Dudokpark 1, 1217 JE Hilversum
www.hilversum.nl

Afbeelding 1: De phishingmail



Afbeelding 2: De phishingpagina

De phishingtest benadrukt dat er meer bewustwording nodig is door middel van bijvoorbeeld awareness workshops en periode phishing simulaties.

3.6.2 Samenvatting ‘inlooptest’

Een andere test die inzicht geeft hoe men in de praktijk omgaat met informatiebeveiliging, is de fysieke inlooptest. Hierbij hebben twee Mystery Guests (MG) – met vastgelegde toestemming vanuit de gemeente – pogingen gedaan om zich fysiek toegang te verschaffen tot informatie op het Raadhuis, het Stadskantoor, de Gemeentewerf en het Sociaal Plein van de gemeente.

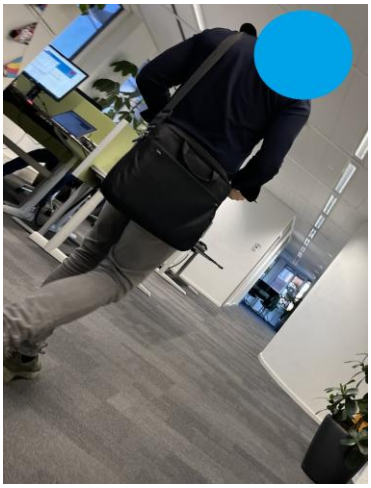
- Op drie van de vier locaties kon er eenvoudig toegang verkregen worden middels ‘tailgating’ (het meelopen met iemand met autorisatie).

- De MG's zijn door een medewerker van het Stadskantoor herhaaldelijk aangesproken op hun aanwezigheid. Andere medewerkers lieten de MG's ongestoord hun gang gaan.
- Op een locatie konden deuren open gemaakt worden door deze te 'flipperen' – daarmee werd het toegangspassysteem omzeild.
- Tijdens de test hadden de MG's toegang tot (vertrouwelijke) documenten en materialen.

De hieronder opgenomen foto's zijn genomen tijdens de inlooptest en dienen ter illustratie van de uitgevoerde activiteiten.



Afbeelding 3: 'Open' deur



Afbeelding 4: Rondlopen op afdeling

Uit de inlooptest is gebleken dat er bijna overal vrijelijk bewogen kan worden met behulp van een fictief verhaal, de identiteit wordt op één geval na niet geverifieerd, deuren bij het Sociaal Plein kunnen door middel van "flipperen" opengebroken worden, er kan relatief eenvoudig achter iemand aangelopen worden door beveiligde deuren, er zijn open kasten en een enkele papier container die niet op slot zit[28]. Deze zaken hebben als gevolg dat er vertrouwelijke documenten bemachtigd kunnen worden door kwaadwillende.

3.6.3 Samenvatting 'penetratietest'

In de digitale 'penetratietest' is er door de onderzoekers van Hoffmann – binnen een specifiek tijdsframe – gezocht naar kwetsbaarheden in 1) de interne infrastructuur, 2) de wifi, 3) de externe infrastructuur, en 4) de cloudomgeving. In totaal zijn er 6 bevindingen als 'hoog' gecategoriseerd, 7 als 'gemiddeld', 1 als 'laag' en 1 als 'informatief'.

De bevindingen zijn niet als 'kritiek' geclassificeerd, gezien de kwetsbaarheden niet direct en eenvoudig kunnen worden misbruikt. Om tot daadwerkelijke exploitatie te komen, zijn meerdere aanvullende

[28] De gemeente gebruikt twee papieren containers: een container voor oud papier en karton en een container voor gevoelige informatie en persoonsgegevens. Er is gevoelige informatie aangetroffen in een niet afgesloten papiercontainer.

stappen en voorwaarden noodzakelijk. Zo is eerst toegang tot het interne netwerk vereist en moeten geldige inloggegevens van een gebruikersaccount worden verkregen, voordat verdere escalatie naar een account met hogere rechten mogelijk is. Daarnaast zijn er meerdere technische handelingen nodig om de kwetsbaarheid daadwerkelijk te kunnen benutten.

Op 3 november 2025 zijn tijdens het uitvoeren van de penetratietest de bevindingen die het mogelijk maakten om verhoogde rechten binnen het netwerk van de gemeente te verkrijgen, zowel per e-mail als telefonisch gedeeld met de ICT-afdeling. Daarnaast zijn deze bevindingen door de uitvoerende ethische hacker mondeling toegelicht aan de CISO tijdens het locatiebezoek. Verdere details zijn uitsluitend op basis van *need-to-know* en vertrouwelijk met de gemeente gedeeld.

Het gemeentelijke netwerk was op afstand niet direct toegankelijk voor onbevoegden. Tijdens de technische penetratietest is geen externe toegang tot het netwerk verkregen, wat erop wijst dat de externe beveiliging op orde is.

4. Hoofdconclusie en praktische oplossingsrichtingen

4.1 Conclusie

De informatieveiligheid van de gemeente Hilversum is gedeeltelijk gewaarborgd, maar nog onvoldoende aantoonbaar, structureel en risicogestuurd ingericht om te kunnen spreken van een robuuste en toekomstbestendige invulling van de wettelijke zorgplicht. De BIO stelt als uitgangspunt dat informatiebeveiligingsmaatregelen aantoonbaar zijn ingericht in opzet, bestaan en werking. Dit vraagt om samenhangende documentatie, expliciete vastlegging, periodieke toetsing en structurele actualisatie van beleid, processen en maatregelen. Met de overgang naar de BIO2 verschuift dit kader van een richtinggevende norm naar een wettelijk verankerde verplichting onder de Cyberbeveiligingswet, waarmee het voeren van een adequaat en risicogestuurd Information Security Management Systeem (ISMS) expliciet verplicht wordt gesteld.

De gemeente heeft de afgelopen jaren aantoonbaar stappen gezet om informatiebeveiliging te verbeteren en beschikt over betrokken medewerkers, een gemotiveerd IB- en privacyteam en diverse ingezette maatregelen. Tegelijkertijd laat het onderzoek zien dat deze maatregelen onvoldoende samenhang vertonen, niet altijd zijn vastgelegd in beleid, procedures en controles, en beperkt worden getoetst op effectiviteit. Hierdoor blijft de organisatie kwetsbaar voor incidenten met potentieel grote impact op dienstverlening, privacy van burgers en bestuurlijk vertrouwen.

Samenvattend wordt geconcludeerd dat de gemeente Hilversum zich in een ontwikkelfase bevindt op het gebied van informatiebeveiliging. Er is sprake van betrokkenheid, bewustzijn over het belang van informatiebeveiliging en er zijn concrete initiatieven om dit te versterken, maar de informatiebeveiliging is nog onvoldoende volwassen, risicogestuurd en aantoonbaar ingericht om te voldoen aan de eisen die voortvloeien uit de BIO, de BIO2 en de aankomende Cyberbeveiligingswet. Zonder verdere professionalisering van het Information Security Management Systeem, expliciete risicosturing en structurele toetsing van maatregelen blijft de organisatie kwetsbaar voor incidenten die impact kunnen hebben op de continuïteit van dienstverlening, de privacy van burgers en het vertrouwen in het bestuur.

Deze hoofdconclusie vormt de basis voor de conclusies en aanbevelingen zoals uitgewerkt in de bestuurlijke nota.

4.2 Praktische oplossingsrichtingen

De in de bestuurlijke nota geformuleerde aanbevelingen zijn gebaseerd op bevindingen die zijn gedaan in de beantwoording van de (deel)vragen in dit onderzoek en bieden concrete handvatten om de volgende stap te zetten en de informatiebeveiliging van de gemeente Hilversum duurzaam naar een hoger volwassenheidsniveau te brengen.

Bij de uitvoering van de in de bestuurlijke nota geformuleerde aanbevelingen kan gebruik worden gemaakt van de volgende verbeterpunten en oplossingsrichtingen:

Nr.	Paragraaf	Verbeterpunten	Oplossingsrichtingen
Thema 1: versterk de fundamenten van informatiebeveiliging			
1	3.2.1	Het Strategisch Gegevensbescherming en Informatiebeveiligingsbeleid geldt van 2025-2029, maar houdt nog onvoldoende rekening met wijzigingen van de BIO naar de BIO2.	• Voer een impactanalyse en gap-analyse uit om beter te begrijpen wat de BIO2 (en haar verankering in de Cyberbeveiligingswet, Cbw) voor impact heeft op het IB-beleid van de gemeente.
2	3.2.2	De gemeente heeft niet voor alle onderwerpen beleid zoals genoemd in de BIO. Ook de onderliggende uitwerking van het beleid in procedures en werkinstructies is niet volledig.	• Stel beleid op in lijn met de vereisten vanuit de BIO2. • Werk deze uit in concrete toegepaste procedures. • Stel werkinstructies op waar nodig om operationele processen specifiek te sturen.
3	3.2.3	De gemeente heeft geen aantoonbare stappen gezet om de impact van de vertaling naar de BIO2 te bepalen[29]. Ook de Wwke vormt geen onderdeel van het beleid, terwijl er wel specifiek wordt verwezen naar 'OT' in het openbare domein.	• Zie Oplossingsrichting 3.2.1 in deze tabel. • Voer een impactanalyse uit rondom de Wet weerbaarheid kritieke entiteiten (Wwke) en de mate van toepassing op 'OT' in het openbare domein voor de gemeente Hilversum – ook met het oog op de fusie met de gemeente Wijdemeren.
4	3.2.4	Er is geen aantoonbaar beleid of uitvoering daarvan rondom 'risicomanagement' binnen de gemeente gericht op IB-risico's.	• Werk uit wat 'risico-gebaseerd werken' betekent voor de gemeente en hoe de gemeente komt tot een 'objectieve beoordeling' – zoals gesteld in het Strategisch IB-beleid. • Volg de verplichting vanuit de BIO2 – wettelijk verankerd in de Cbw – om risico gebaseerd maatregelen te nemen rondom IB-vraagstukken.

[29] De gemeente geeft in ambtelijk wederhoor aan dat er wel degelijk aantoonbare stappen worden gezet in het bepalen van de impact van de vertaling van de BIO naar de BIO2. Elementen die hadden kunnen bijdragen aan deze aantoonbaarheid (maar niet aanwezig waren in de voor het onderzoek aangeleverde informatie), konden bijvoorbeeld zijn: de aanwezigheid van een impactanalyse, het benoemen van de BIO2 en de verhouding daartoe in het Strategisch IB-beleid (2025-2029), het vastleggen van notulen van vergaderingen waarin keuzes hieromtrent zijn gemaakt, inhoudelijke onderwerpen vanuit de BIO2 die naar voren komen in andere beleidsstukken.

5	3.3.1	De gemeente is niet volledig compliant aan de BIO, maar heeft ook voor zichzelf niet bepaald waar het aan zou moeten voldoen.	• Werk vanuit de analyse rondom de BIO2 (zie aanbeveling 1) toe naar een risico gebaseerde selectie van maatregelen op de primaire processen en kritieke informatiesystemen van de gemeente. • Vervang de 'compliant'-mindset voor een 'risk-based'-mindset. Waar een 'compliant'-mindset primair is gericht op het formeel voldoen aan normen en checklists, richt een 'risk-based'-mindset zich op het systematisch identificeren en beheersen van de meest relevante risico's. Door informatiebeveiliging primair te sturen vanuit risico's in plaats van normnaleving, ontstaat meer focus op effectiviteit, prioritering en daadwerkelijke weerbaarheid van de organisatie. • Realiseer dat de BIO2 een wettelijke verankering heeft in de Cbw en niet langer alleen als richtlijn geldt.
6	3.4.3	Uitgelichte verbeterpunten voor de gemeente op het vlak van informatiebeveiliging om de gemeente in verhoogde mate weerbaar te maken (zie tekst onder 3.4.3 voor verdere onderbouwing).	• Stel een ISMS op zoals dit wordt voorgeschreven vanuit de BIO/BIO2 en in lijn met *best practices*. Dicht de 'gaps' die op dit moment geconstateerd zijn in het huidige ISMS. • Zie 3.2.4 rondom 'risico management'. • Zie 3.4.2 rondom 'bewustzijn'. • Zie 3.4.2 rondom 'IAM'. • Verken de mogelijkheden om Logging & Monitoring uit te rollen op basis van risico's voor de organisatie. • Versterk het leveranciersbeleid en bijbehorende procedures in lijn met geldende wet- en regelgeving.
Thema 2: Vergroot de effectiviteit en aantoonbaarheid van maatregelen in de praktijk			
7	3.3.2	De gemeente heeft geen budget ter beschikking specifiek voor informatiebeveiliging.	• Overweeg in hoeverre het wenselijk is om de inzet van middelen inzichtelijk te maken specifiek voor IB-activiteiten en -maatregelen. • Alloceer het nemen van maatregelen bij specifieke verantwoordelijke afdelingen of functionarissen. • Behoud het overzicht hierover vanuit de CISO-positie en geef opvolging aan geconstateerde tekortkomingen en toegezegde plannen om maatregelen te implementeren.

8	3.4.1	Er is geen planning[30] beschikbaar wat voor steekproeven of testen er worden uitgevoerd binnen de gemeente[31].	• Stel een 'testbeleid' vast en voorzie deze van onderliggende operationele planning. • Beleg de uitvoer binnen de organisatie (zowel binnen afdelingen als vanuit een derdelijnsfunctie). • Plan testen in en stuur hierop vanuit een vastgelegde agenda en specifiek toegewezen budget.
9	3.4.2	De gemeente scoort bovengemiddeld in de phishingtest en lijkt hiermee kwetsbaarheden te vertonen rondom het bewustzijn van medewerkers om veilig om te gaan met e-mails.	• Herhaal phishing exercities periodiek. • Onderzoek wat voor andere testen kunnen bijdragen aan het verhogen van het bewustzijn van medewerkers op dit vlak. • Realiseer dat MFA/2FA een werkende maatregel is, maar dat deze met voldoende tijd en kennis ook te omzeilen valt door kwaadwillenden en dat verkregen credentials ook op andere wijze een risico kunnen vormen voor de organisatie en voor individuen.
10	3.4.2	Ongeautoriseerde toegang tot netwerk of informatiesystemen geldt ook van 'binnenuit'.	• Creëer een sluitend In dienst /Uit dienst-proces voor interne en externe medewerkers. • Vergroot de afstemming met en samenwerking tussen ICT, HR en verantwoordelijk management. • Initieer periodieke checks rondom functies met een verhoogd risico. • Initieer periodieke checks rondom kritieke systemen. • Initieer periodieke checks rondom gevoelige informatie. • Beperk de mogelijkheden tot exfiltratie van data op basis van risico's voor de organisatie.

[30] Het gaat in deze bevindingen om het aantoonbare en structurele karakter van de genomen maatregelen. In ambtelijk wederhoor geeft de gemeente aan dat er jaarlijkse uitwijktesten worden gedaan en dat verbetervoorstellen worden geïdentificeerd en geïmplementeerd. Hier is echter geen aantoonbare structurele planning voor aangeleverd.

[31] De gemeente geeft aan dat er jaarlijks een uitwijktest gedaan wordt voor de dienstverlening aan de loketten in het stadskantoor. Hierover wordt gerapporteerd aan de CISO, er worden verbetervoorstellen geïdentificeerd en geïmplementeerd.

Thema 3: Richt de bestuurlijke informatievoorziening structureel in			
11	3.4.4	Raadsleden, B&W en ambtenaren worden niet structureel geïnformeerd over de risico's en regels op het gebied van informatieveiligheid.	• Richt een structurele en periodieke informatievoorziening in (bijvoorbeeld via een vast bestuurlijk dashboard, kwartaalrapportage of jaarlijkse themasessie) van voldoende volwassenheidsniveau, waarin raadsleden, B&W en ambtenaren **actief en consistent** worden geïnformeerd over actuele risico's, relevante regels, incidenten en ontwikkelingen op het gebied van informatieveiligheid. • Communiceer een eenduidig risico- en dreigingsbeeld voor de gemeente op een begrijpelijke wijze met stakeholders. • Wijs de stakeholders op hun specifieke rol, rechten en plichten rondom deze risico's. • Betrek stakeholders op basis van hun toegewezen verantwoordelijkheden bij incidentscenario-besprekingen, table tops en specifieke oefeningen. • Zorg voor een duidelijk incidentmanagementproces, zodat meldingen snel en eenduidig kunnen worden gedaan, efficiënt en effectief kunnen worden opgevolgd. • Leg incidenten vast, evalueer ze en leg 'lessons learned' vast.
12	3.5	Het is niet vastgesteld of de controle- en formele goedkeuringsmechanismen van de jaarlijkse ENSIA-zelfevaluatie van voldoende kwaliteit zijn. Deze mechanismen behoren bij te dragen aan de objectiviteit, zorgvuldigheid en betrouwbaarheid van de rapportage. De beoordeling van deze mechanismen viel echter niet binnen de scope van dit onderzoek.	• Vergelijk de uitkomsten van de zelfevaluatie met de bevindingen uit dit onderzoek om een zorgvuldig en onderbouwd beeld te krijgen van het volwassenheidsniveau van de zelfevaluatie. • Leg vast op welke wijze de externe auditor zijn toetsing uitvoert, zodat helder is welke beoordelingscriteria en werkwijzen worden toegepast. • Maak inzichtelijk in welke mate de uitkomsten van de zelfevaluatie worden getoetst en kritisch bevraagd door de verschillende goedkeuringsgremia, zodat de kwaliteit en betrouwbaarheid van het totale toetsingsproces gewaarborgd blijft.

Disclaimer

De volgende medewerkers van Hoffmann hebben het onderzoek uitgevoerd en deze rapportage opgemaakt[32]:

Onderzoeker 1
Security Risk Management Consultant

Onderzoeker 2
Cyber Security Specialist

Onderzoeker 3
Mystery Guest

Onderzoeker 4
Mystery Guest

Ondergetekende is vanuit haar rol als leidinggevende eindverantwoordelijk voor dit onderzoek.



Elisabeth Huige – Van de Loo
Algemeen Directeur

Dit rapport is geschreven voor de opdrachtgever, zodat hij of zij in staat wordt gesteld om maatregelen te nemen teneinde de cyberweerbaarheid van zijn/haar organisatie te verhogen. Wij kunnen geen aansprakelijkheid aanvaarden voor acties of maatregelen die door opdrachtgever of diens vertegenwoordigers op basis van het rapport worden ondernomen. Tenslotte verwijzen wij naar de van toepassing zijnde dienstverleningsvoorwaarden.

Almere, 1 juni 2026

[32] De onderzoekers zijn met naam en toenaam bekend bij Hoffmann en de opdrachtgever, maar worden hier in het kader van hun privacy niet nader benoemd.

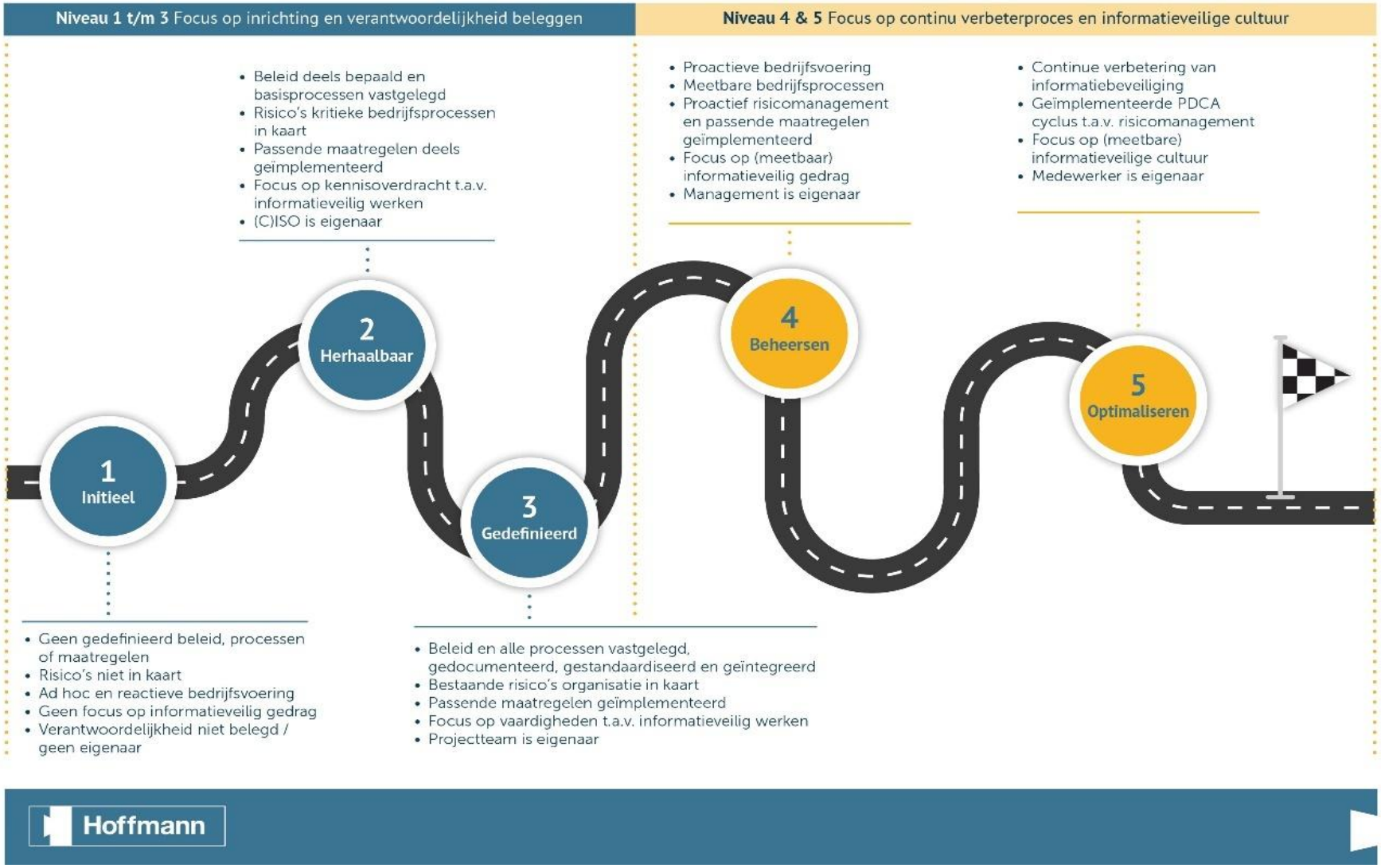
5. Bijlagen

5.1 Maturity model informatiebeveiliging

Om als organisatie de informatiebeveiliging op orde te brengen kan het maturity model informatiebeveiliging handvatten bieden. Het model maakt inzichtelijk wat het volwassenheidsniveau van een organisatie is informatiebeveiliging. Het kan eveneens worden gebruikt als richtlijn welke stappen ondernomen dienen worden om de informatiebeveiliging (verder) te optimaliseren.

Het model op de volgende pagina gaat uit van fasen in de ontwikkeling van organisaties. Hierbij wordt vastgesteld op welk niveau een organisatie zich bevindt, zodat passende acties ondernomen kunnen worden om het volgende niveau te behalen. Dit model is uiteraard een richtlijn en kent haar beperkingen. Het is meer gericht op het ‘hoe’ en minder op het ‘wat’ en ‘wie’ in de ontwikkeling van het volwassenheidsniveau. Daarnaast kan het zo zijn dat een organisatie een 2 scoort op het volwassenheidsniveau en daarnaast ook al aan een aantal kenmerken van niveau 3 voldoet. Een organisatie krijgt de score van het niveau, indien het aan alle bijbehorende kenmerken van het niveau voldoet. Op de volgende pagina wordt het maturity model weergegeven.

Maturity Model Informatiebeveiliging



5.2 Verloop mail-phishingtest

De operationele details van de uitgevoerde test zijn gedeeld met de uitvoerend verantwoordelijken. De conclusies en bevindingen zijn opgenomen in de openbare rapportage.

5.3 Verloop fysieke inlooptest

De operationele details van de uitgevoerde test zijn gedeeld met de uitvoerend verantwoordelijken. De conclusies en bevindingen zijn opgenomen in de openbare rapportage.

5.4 Verloop digitale penetratietest

De operationele details van de uitgevoerde test zijn gedeeld met de uitvoerend verantwoordelijken. De conclusies en bevindingen zijn opgenomen in de openbare rapportage.

5.5 Aanwezige beleidsstukken in relatie tot de BIO

Onderstaande tabel geeft een overzicht van de onderwerpen die in lijn met de BIO-richtlijn verwacht worden bij een gemeentelijke organisatie. De term 'beleid' is in dezen een brede term waarin het gaat om een vorm van beschrijving van het doel, de opzet, de verantwoordelijkheden rondom en de beschrijving van processen rondom genomen maatregelen.

#	Onderwerp	Aanwezig?	Datum
1	Strategisch Informatiebeveiligingsbeleid	Ja	2025-2029
2	Risicomanagementbeleid	Nee	
3	Rollen en verantwoordelijkheden	Ja	Onderdeel strategisch beleid
4	Classificatiebeleid	Nee	
5	Bewustwording & training	Deels	2024 – concept 0.3
6	Incidentmanagement	Nee	Protocol uit 2021 – concept 0.1
7	Logging & monitoring	Ja	2022
8	Audit- & compliance	Deels[33]	Onderdeel strategisch beleid, zichtbare uitvoering, geen planning
9	Bedrijfscontinuïteit	Ja	2025
10	Gegevensbescherming (AVG)	Ja	2024
11	Toegangs- & autorisatiebeleid	Nee	
12	Netwerk- & segmentatiebeleid	Nee	

[33] Tijdens ambtelijk wederhoor geeft de gemeente aan dat Team concern control en audit ook generieke (ITGC) en applicatieve audits laat uitvoeren (inclusief planning). Echter was deze informatie t.t.v. het onderzoek niet voorhanden. De reactie vanuit de gemeente onderschrijft bovendien de classificatie dat dit 'deels' aanwezig is: in algemene zin, niet gespecificeerd op IV-onderwerpen en niet inzichtelijk of (mede-)gecoördineerd vanuit het ISMS van de CISO. Die constatering komt ook naar voren vanuit de gevoerde interviews met zowel de CISO als concern control.

#	Onderwerp	Aanwezig?	Datum
13	Patchmanagement	Nee	
14	Change management	Nee	
15	Werkplek en veilige verbinding op afstand	Ja	2021
16	Encryptie	Nee	
17	Mobiele apparaten	Ja	2021
18	Configuratie	Nee	
19	Opslag- & back-up	Nee	Wel operationele uitvoer
20	Leveranciersmanagement	Nee	
21	Technisch incidentbeheer	Nee	
22	Cloud- en SaaS-gebruik	Nee	
23	Fysieke beveiliging	Ja	2024
24	Screeningsbeleid	Nee	Wel operationele uitvoer
25	Wachtwoordbeleid	Ja	2019

5.6 Overzicht onderwerpen in de Baseline Informatiebeveiliging Overheid (BIO)

#	Onderwerp	Korte beschrijving
1	Beleidslijnen voor informatie-beveiliging	Richtlijnen en kaders voor het opstellen en onderhouden van informatiebeveiligingsbeleid.
2	Organiseren van informatiebeveiliging	Rollen, verantwoordelijkheden en structuur van informatiebeveiliging binnen de organisatie.
3	Beheer van bedrijfsmiddelen	Inventariseren en beschermen van informatie-assets (zoals systemen, data en apparatuur).
4	Personeelsbeveiliging	Beveiligingsmaatregelen rond medewerkers: screening, bewustwording, exitprocedures.
5	Fysieke beveiliging	Beveiliging van gebouwen, serverruimtes en werkplekken tegen onbevoegde toegang of schade.
6	Beheer van communicatie-technologie	Correct gebruik van netwerken, e-mail, internet en andere communicatiemiddelen.
7	Toegangsbeveiliging	Regelen van toegangsrechten en autorisaties voor systemen en informatie.
8	Cryptografie	Gebruik van versleuteling (encryptie) voor vertrouwelijkheid en integriteit van data.

#	Onderwerp	Korte beschrijving
9	Fysieke en logische beveiliging van systemen	Beveiliging van besturingssystemen, applicaties, back-ups, malwarebescherming.
10	Beheer van leveranciers	Beveiliging bij uitbesteding, inclusief contractafspraken over beveiliging met derden.
11	Informatiebeveiligingsincidenten	Detectie, melding, registratie en afhandeling van beveiligingsincidenten.
12	Continuïteitsbeheer	Voorbereiding op calamiteiten en voortzetting van kritieke processen (BCM/DRP).
13	Naleving (compliance)	Voldoen aan wettelijke verplichtingen, normen en interne beleidsregels.
14	Risicomanagement	Identificeren, beoordelen en beheersen van risico's voor informatiebeveiliging.

5.7 Verklarende woordenlijst

Onder leiding van Cyberveilig Nederland (https://www.cyberveilignederland.nl/) hebben ruim 60 organisaties, overheidspartijen en private partijen meegewerkt aan de samenstelling van het cybersecurity woordenboek. Er is een verklarende woordenlijst opgesteld met bijna 600 cybersecuritytermen om bijvoorbeeld rapporten, adviezen of offertes beter te begrijpen.

Voor het complete woordenboek verwijzen wij graag naar: www.cyberveilignederland.nl/woordenboek

Hieronder een opsomming van cybersecuritytermen die voorkomen in deze rapportage.

BEGRIP	BETEKENIS
BIO	Baseline Informatiebeveiliging Overheid, het basis normenkader voor informatiebeveiliging binnen de overheid.
CISO	Chief Information Security Officer. De medewerker die aangewezen verantwoordelijk is voor informatiebeveiliging. Rol op strategisch niveau. Bestuur blijft altijd eindverantwoordelijke.
ENSIA	Eenduidige Normatiek Single Information Audit. Het is een in 2017 geïntroduceerd, uniform verantwoordingsstelsel waarmee Nederlandse gemeenten, provincies en waterschappen jaarlijks verantwoording afleggen over hun informatieveiligheid. Dit proces, gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO), integreert toezicht en toetst de opzet, het bestaan en de werking van beveiligingsmaatregelen.
FG	Functionaris Gegevensbescherming. Verantwoordelijk voor toezicht op toepassing en naleving van de AVG.

BEGRIP	BETEKENIS
Exfiltratie	Het kunnen onttrekken van informatie uit systemen en het daarmee in een onbevoegde, ongecontroleerde omgeving te brengen en ongeautoriseerd toegang tot deze data mogelijk te maken – met als gevolg een datalek of mogelijk misbruik tot gevolg.
Gebruikersnaam	Naam waarmee een gebruiker in een computersysteem kan inloggen.
IAM	Identity & Access Management is een combinatie van een technische maatregel en een organisatorisch proces dat wordt ingezet om gebruikers een unieke en tot de persoon herleidbare identiteit toe te wijzen en passende toegangsmiddelen, -rechten en -rollen daaraan te koppelen. Dit wordt gedaan op basis van de rol of functie die de gebruiker binnen de organisatie vervult. Dat wordt ook wel *role-based access* (RBAC) genoemd.
Informatiebeveiligings-organisatie	Het team wat zich binnen een bedrijf bezighoudt met het beschermen van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie.
ISMS	Information Security Management Systeem. Verzameling van alle onderling samenhangende elementen op het vlak van informatiebeveiliging. Helpt beleid, procedures en doelstellingen te formuleren, implementeren, communiceren en evalueren om de algehele informatiebeveiliging te verbeteren/garanderen.
ISO	Information Security Officer. Verantwoordelijk voor informatiebeveiligingsbeleid evenals de implementatie en toezicht op uitvoering. Tevens verantwoordelijk voor strategie op het gebied van informatiebeveiliging.
Inloggegevens	Gebruikersnaam en wachtwoord waarmee in een computersysteem kan inloggen.
Incident	Gebeurtenis of actie waarbij de beveiliging van hardware, software, informatie, een proces of organisatie mogelijk is gevaar is gebracht of geheel of gedeeltelijk is doorbroken.
Logging	Het automatisch bijhouden van veranderingen en gebeurtenissen binnen een systeem.
Malware	Kwaadaardige software die aanvallers op een digitaal systeem zetten om er op afstand bij te kunnen, het te vernielen of informatie te stelen. Malware is een samentrekking van het Engelse malicious software.
MFA	Multi Factor Authentication is een technische maatregel die ervoor zorgt dat een gebruiker altijd middels het toepassen van (minimaal) twee gescheiden elementen toegang kan krijgen tot informatie(systemen) of fysieke omgevingen.
Mitigerende maatregel	Een activiteit met als doel om de oorzaak of het gevolg van een ongewenste gebeurtenis weg te nemen, of te verkleinen.

BEGRIP	BETEKENIS
Mystery guest bezoek	Beveiligingstest waarbij een daartoe aangewezen persoon op bezoek gaat bij een organisatie. Daar probeert hij in ruimtes te komen waar hij niet mag komen. En hij probeert bij informatie te komen waar hij niet bij mag komen. Zo test de persoon deze organisatie. Men kan deze test combineren met een penetratietest. In dat geval gaat de mystery guest een beveiligde ruimte in. Daar probeert hij in te breken op het lokale computernetwerk.
PDCA	Plan-Do-Check-Act (cyclus). Stappen ter verbetering van bijvoorbeeld een proces of beleid.
Phishing/Mail-phishing	Aanval waarbij de aanvaller iemand verleidt om belangrijke informatie te geven, zoals bijvoorbeeld inloggegevens of creditcardgegevens. Phishing gebeurt vaak via e-mails. Maar aanvallers proberen het ook via de telefoon, een sms of een appbericht
PO	Privacy Officer. Verantwoordelijk voor het ontwikkelen en bewaken van het privacybeleid en ondersteuning bieden bij uitvoering van het beleid.
Ransomware	Ransomware is malware die de databestanden van gebruikers versleutelt, met als doel om deze later te ontsleutelen in ruil voor losgeld.
Security by design	Een product, dienst of systeem ontwerpen en vanaf het begin ook de beveiliging mee ontwikkelen en testen.
SER	Satellite Equipment Room, een satelliet van het technische hart van een bedrijf. Ruimte waarin serverapparatuur, netwerkapparatuur en IT-infrastructuur aanwezig zijn.
SOC/SIEM-oplossing	Staat voor Security Operations Center/Security Incident and Event Monitoring van waaruit bewegingen binnen een netwerk actief of passief bekeken worden en geanalyseerd op afwijkend gedrag om zodoende tijdig in te kunnen grijpen bij (potentiële) incidenten.
Toon aan de top	De houding en gedrag van het hogere management en de invloed hiervan op de cultuur en normen binnen de gehele organisatie.
Wachtwoord	Reeks van letters, cijfers en of andere karakters waarmee een gebruiker in een computersysteem kan komen. Het is de bedoeling dat een gebruiker dit wachtwoord niet aan anderen geeft en een sterk wachtwoord kiest zodat dit moeilijk te kraken is door aanvallers

5.8 Overzicht geïnterviewden

Functie	Datum interview
Chief Information Security Officer	12 september, 15 oktober
Enterprise Architect	15 oktober
Portefeuillehouder	19 november
Concerncontroller	15 oktober
Concerndirecteur	15 oktober
Contract-/Servicemanager	15 oktober
Afdelingshoofd Publiekszaken	24 oktober
IT-/ ICT-team manager	24 oktober
Raads- en commissieleden	17 november

5.9 Overzicht bestudeerde documenten

Ten behoeve van het onderzoek zijn diverse documenten van de gemeente Hilversum ontvangen en bestudeerd. Het overzicht van de geraadpleegde documenten is gedeeld met de uitvoerend verantwoordelijken.


Hoffmann
VERTROUWEN IS GOED,
HOFFMANN IS BETER
www.hoffmann.nl