Rekenkameronderzoek informatiebeveiliging

Gemeente Zevenaar



DMC GROUP
SECURITY MANAGEMENT

Documentbeheer

Opdrachtgever

REKENKAMER ZEVENAAR

Versie
v1.0

Datum
22 september 2026

Auteur(s)
drs. Chris Deben MBA CISM
Youri Lammerts MSc. CISM CISA CISSP CIPM CIPP/e
Mick Deben MSc. CISSP CRISC CGEIT CCSP SSCP AAISM

Classificatie
DMC Openbaar. De informatie in dit document is openbaar en mag vrij gedeeld worden.

DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

DMC GROUP
SECURITY MANAGEMENT

Managementsamenvatting

In opdracht van de Rekenkamer Zevenaar heeft DMC Group een onderzoek naar de informatiebeveiliging bij de gemeente de gemeente Zevenaar uitgevoerd. Het onderzoek heeft plaatsgevonden in de periode december 2025 - april 2026. In dit rapport zijn de feitelijke bevindingen verwerkt voor zowel de gemeente Zevenaar als het Regionale Inkoopdienstcentrum (RID) en zijn er aanbevelingen gedaan ter verbetering van de algehele informatiebeveiliging. De rekenkamer trekt op basis van dit rapport haar eigen conclusies.

Gemeenten spelen een cruciale rol in de (digitale) samenleving. Zij beheren en verwerken grote hoeveelheden privacygevoelige informatie, zijn sterk afhankelijk van digitale systemen voor hun dienstverlening en werken intensief samen met ketenpartners en leveranciers. De continuïteit, betrouwbaarheid en veiligheid van de informatievoorziening zijn daarmee essentieel voor het vertrouwen van burgers en bedrijven in de gemeente en de kwaliteit van de publieke taken. Tegelijkertijd worden gemeenten geconfronteerd met een groeiend en complexer wordend cyberdreigingslandschap en strengere wet- en regelgeving, zoals de Cyberbeveiligingswet (Cbw).

Belangrijkste bevindingen en aanbevelingen

De belangrijkste bevindingen en aanbevelingen zijn onderverdeeld in de vier domeinen van de Baseline Informatiebeveiliging Overheid (BIO)2: Organisatorisch, Mensgericht, Fysiek en Technologisch. Het is de vernieuwde basisnorm voor informatiebeveiliging binnen de Nederlandse overheid. De BIO2 biedt een uniforme aanpak en een gemeenschappelijk normenkader voor informatiebeveiliging binnen de overheid, waarbij risicomanagement centraal staat. De vier domeinen zijn complementair en zorgen samen voor een integrale beheersing van informatiebeveiligingsrisico's.

Organisatorisch

Het organisatorische domein gaat over governance (bestuur), verantwoordelijkheid en sturing op informatiebeveiliging, bijvoorbeeld risicomanagementproces, inkoopproces, leveranciersketen en projectmanagement. Het borgt dat bestuur en management duidelijke keuzes maken, risico's afwegen en verantwoording afleggen. Dit is essentieel omdat informatiebeveiliging alleen effectief is als het bestuurlijk is verankerd en actief wordt aangestuurd.

Het managementsysteem voor informatiebeveiliging is niet ingericht volgens de ISO 27001 waardoor de beheerprocessen ten aanzien van informatiebeveiliging beperkt (aantoonbaar) zijn. Aanvullend zijn het informatiebeveiligingsbeleid en de processen daaromtrent beperkt vertaald naar tactisch en operationeel niveau waardoor niet (goed) vastgesteld kan worden in hoeverre processen worden nageleefd. Veel afspraken worden mondeling gemaakt en niet (centraal) vastgelegd. Het is daarom uitdagend voor zowel de gemeente als het het RID om aan te tonen wat de gemaakte afspraken zijn, welke afwegingen er gemaakt zijn en wat stand van zaken zijn.

DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

Mensgericht

Dit domein richt zich op het gedrag, bewustzijn en de competenties van medewerkers en bestuurders, inclusief screening, opleiding en duidelijke verantwoordelijkheden. Het is cruciaal omdat mensen vaak de doorslaggevende factor zijn in het voorkomen, veroorzaken, detecteren en reageren op beveiligingsincidenten; goed geïnformeerde en handelingsbekwame medewerkers verkleinen risico's aanzienlijk.

Het bevorderen van veilig gedrag onder alle medewerkers is beperkt, heeft een vrijblijvend karakter en is ad-hoc gedreven, dit geldt voor zowel de gemeente Zevenaar als het RID. Activiteiten die hebben plaatsgevonden zijn onder andere: e-learning bij indiensttreding, mystery guest onderzoek en kennisdeling via intranet.

Fysiek

Dit domein richt zich op de beveiliging van gebouwen, werkplekken, datacenters en fysieke toegang tot systemen en informatie. Dit domein is belangrijk omdat digitale beveiliging niet losstaat van fysieke bescherming: onbevoegde fysieke toegang kan technische maatregelen direct ondermijnen.

Op fysiek vlak heeft de gemeente Zevenaar verschillende maatregelen getroffen. Desondanks is het verkrijgen van ongeautoriseerde toegang vrij eenvoudig en zijn adviezen uit voorgaande onderzoeken en van eigen personeel niet (allemaal) opgevolgd. Dit gecombineerd met het open karakter van de Cultuurfabriek, het niet zichtbaar hoeven dragen van een identificatiemiddel en ongestructureerde aandacht voor veilig gedrag zijn risicoverhogend.

Technologisch

Dit domein omvat de technische beveiliging van systemen en netwerken, zoals toegangsbeheer, logging, monitoring, patching en back-ups. Het is essentieel omdat digitale dienstverlening en gegevensbescherming direct afhankelijk zijn van robuuste en actuele Informatietechnologie[1] *(IT-) en Operationele Technologie*[2] *(OT-)beveiliging.*

De gemeente Zevenaar is in sterke mate afhankelijk van het RID voor de inrichting en borging van de beveiliging van haar IT-infrastructuur. Deze afhankelijkheid brengt risico's met zich mee doordat een integrale en gestandaardiseerde aanpak voor informatiebeveiliging ontbreekt. Er is geen sprake van periodieke objectieve en onafhankelijke toetsing van de technische beveiligingsmaatregelen, waardoor de effectiviteit en volwassenheid van de huidige beveiligingsinrichting onvoldoende inzichtelijk zijn.

De uitgevoerde penetratietest toont aan dat de IT-infrastructuur geen robuuste weerbaarheid biedt zodra de eerste beveiligingslaag is doorbroken. Hierdoor was een kettingreactie mogelijk die leidde tot een overname van de gehele gedeelde infrastructuur. De gevolgen hiervan zijn toegang tot alle apparaten van de werknemers, de gegevens op het interne netwerk en het gedeelde netwerk met andere organisaties.

De belangrijkste risico's hebben betrekking op onvoldoende beperking van de toegang, kwetsbare configuraties en opvolgingsmogelijkheden en afhankelijkheden binnen de gedeelde infrastructuur van een Shared Service Center (SSC).

DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

Tijdens het onderzoek heeft het uitbestede detectie- en responsteam afwijkende activiteiten waargenomen en gemeld. Deze signalen zijn in het kader van de vooraf afgestemde pentest niet als regulier incident opgevolgd. Dit laat zien dat detectiemaatregelen aanwezig zijn, maar neemt de onderliggende kwetsbaarheden niet weg. In een realistisch aanvalsscenario kunnen detectie en respons de aanval bemoeilijken, maar dit is geen vervanging voor preventieve maatregelen, veilige configuraties en effectieve segmentatie. De aanbevelingen richten zich op het oplossen van afzonderlijke technische bevindingen.

De slagkracht op het gebied van informatiebeveiliging wordt beperkt door een tekort aan capaciteit binnen de operationele IT-teams. Hoewel er monitoring plaatsvindt binnen het Microsoft ecosysteem, ontbreekt het aan een bredere, proactieve security monitoring in de vorm van een SIEM- en/of SOC-oplossing[3]. Hierdoor is het detectievermogen ten aanzien van dreigingen en afwijkend gedrag beperkt.

Ten slotte zijn de processen rondom incident response en disaster recovery ontoereikend ingericht. Dit vergroot de kans op vertraging in de respons bij beveiligingsincidenten en belemmert een effectief herstel na verstoringen. Gezien de bovenstaande factoren is het voor de gemeente Zevenaar uitdagend om zich adequaat voor te bereiden op en te beschermen tegen (toekomstige) cyberdreigingen.

Aanbevelingen voor het college van B&W

Bestudeer de bevindingen en aanbevelingen uit de bijlagen en bepaal of de aanbevelingen gericht aan het college worden overgenomen en zo ja, op welke termijn. Informeer de gemeenteraad over uw plan om de risico's te mitigeren en houdt de raad regelmatig op de hoogte over de voortgang.

Aanbevelingen voor de gemeenteraad

De gemeenteraad heeft een belangrijke rol ten aanzien van de informatieveiligheid binnen de gemeente. De VNG[4] benadrukt dat digitale veiligheid een bestuurlijke verantwoordelijkheid is die niet alleen de ambtelijke organisatie betreft, maar een integraal onderdeel moet zijn van het bestuurlijke werk van de raad. Door als raad het onderwerp informatiebeveiliging regelmatig te agenderen kan de raad adequaat toezicht houden op hoe de gemeente risico's beheerst en incidenten aanpakt. Het doel is het versterken van de (digitale) veiligheid van de gemeentelijke dienstverlening en de weerbaarheid van de gemeente en haar inwoners en ondernemers. Bepaal of de aanbevelingen gericht aan de gemeenteraad worden overgenomen.

Aanbevelingen voor het RID

Dit rekenkameronderzoek richtte zich primair op de gemeente Zevenaar, maar aangezien het RID een belangrijke rol vervult met betrekking tot de informatieveiligheid van de gemeente Zevenaar, zijn er ook voor het RID aanbevelingen geformuleerd. Het college wordt verzocht om de bevindingen en aanbevelingen die betrekking hebben op het RID aan het RID voor te leggen én daar een formele reactie op verlangen (wat gaan ze doen met de bevindingen).

DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

DMC GROUP
SECURITY MANAGEMENT

Inhoudsopgave

1 Inleiding **7**

1.1 Cyberdreigingsbeeld gemeenten 7

1.2 Cyberbeveiligingswet 7

1.3 Onderzoeksvragen en -aanpak 8

1.4 Disclaimer 8

2 Beantwoording onderzoeksvragen **9**

2.1 Aanbevelingen gemeenteraad 11

Noten **13**

DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

DMC GROUP
SECURITY MANAGEMENT

1 Inleiding

Gemeenten spelen een cruciale rol in de (digitale) samenleving. Zij beheren en verwerken grote hoeveelheden privacygevoelige informatie, zijn sterk afhankelijk van digitale systemen voor hun dienstverlening en werken intensief samen met ketenpartners en leveranciers. De continuïteit, betrouwbaarheid en veiligheid van de informatievoorziening zijn daarmee essentieel voor het vertrouwen van burgers en bedrijven in de gemeente en de kwaliteit van de publieke taken. Tegelijkertijd worden gemeenten geconfronteerd met een groeiend en complexer wordend cyberdreigingslandschap en strengere wet- en regelgeving, zoals de Cyberbeveiligingswet (NIS2).

1.1 Cyberdreigingsbeeld gemeenten

Het cyberdreigingsbeeld van de Informatiebeveiligingsdienst voor gemeenten[5] benadrukt dat ransomware[6], datalekken[7] en uitval van processen door incidenten de grootste bedreigingen vormen voor Nederlandse gemeenten. De Informatiebeveiligingsdienst stelt dat gemeenten hun digitale weerbaarheid moeten versterken door basismaatregelen, leveranciersmanagement en intensievere samenwerking met andere gemeenten. De Informatiebeveiligingsdienst concludeert: ”Digitale veiligheid is geen luxe maar een noodzakelijke voorwaarde voor continuïteit en vertrouwen in gemeentelijke dienstverlening. Gemeenten moeten blijven investeren in bewustwording, technologie en samenwerking om huidige én toekomstige dreigingen effectief het hoofd te kunnen bieden. ”In dit licht is het van belang dat gemeenten inzicht hebben in hun huidige volwassenheid ten aanzien van informatiebeveiliging. Oftewel, in hoeverre processen, maatregelen en verantwoordelijkheden zijn ingericht, geborgd en effectief functioneren.

Het Cybersecuritybeeld Nederland[8] onderkent dat het cyberdreigingslandschap divers en onvoorspelbaar is en dat verschillende dreigingsactoren zich richten op Nederlandse doelwitten. Het benoemt dat geopolitieke ontwikkelingen het cyberdreigingslandschap beïnvloeden en dat generatieve AI[9] de schaal en impact van cyberdreigingen vergroot. Ondanks deze ontwikkelingen benadrukt de Algemene Inlichtingen en Veiligheidsdienst (AIVD) dat veel incidenten te voorkomen zijn met goede basismaatregelen en weerbaarheids-trainingen. Dit onderstreept het belang voor gemeenten om de BIO2 te implementeren, te borgen en te onderhouden.

In dit onderzoek is onder andere onderzocht hoe de gemeente Zevenaar zich verhoudt tot deze actuele dreigingen. Daarbij is gelet op de aanwezigheid en borging van basismaatregelen, het beheer van leveranciers- en ketenrisico’s, de voorbereiding op incidenten en calamiteiten en de inrichting van governance en capaciteit. Ook is aandacht besteed aan de manier waarop de gemeente Zevenaar inspeelt op opkomende risico’s en toekomstige technologische ontwikkelingen.

1.2 Cyberbeveiligingswet

De NIS2 (Cyberbeveiligingswet) verplicht alle overheidsorganisaties de BIO2 aantoonbaar na te leven en legt de eindverantwoordelijkheid expliciet bij het bestuur. Bestuurders moeten risicogebaseerd passende en evenredige maatregelen voor informatiebeveiliging vaststellen en goedkeuren, toezien op de kwaliteit van de uitvoering en actief sturen op cyberrisico’s.

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

Zij moeten zelf over voldoende kennis beschikken en borgen dat medewerkers structureel worden opgeleid. Daarnaast is de gemeente Zevenaar verantwoordelijk voor het tijdig melden van meldplichtige incidenten. De toezichthouder voor overheidsorganisaties is de Rijksinspectie Digitale Infrastructuur (RDI).[10] De NIS2 zal naar verwachting medio 2026 omgezet zijn naar nationale wetgeving.

1.3 Onderzoeksvragen en -aanpak

De hoofdvraag van dit onderzoek luidt: *In welke mate is de informatiebeveiliging in de gemeente Zevenaar voldoende geborgd en in hoeverre biedt de aanwezige documentatie de gemeenteraad het benodigde inzicht om effectief te sturen op dit thema?*

De rekenkamer heeft zeven deelvragen geformuleerd. Om deze vragen te kunnen beantwoorden is informatie en documentatie opgevraagd, zijn interviews gehouden met verschillende medewerkers, raads- en commissieleden, heeft er een schouw op locatie plaatsgevonden en is een penetratietrest[11] uitgevoerd. Het onderzoek heeft plaatsgevonden in de periode december 2025 - april 2026.

1.4 Disclaimer

Dit rapport vormt een momentopname ten aanzien van informatiebeveiliging op basis van de beschikbare informatie ten tijde van het onderzoek. De bevindingen zijn gebaseerd op steekproeven, interviews en documentreview binnen de beperkte doorlooptijd en het beschikbare budget. Hierdoor kan niet worden uitgesloten dat er aanvullende risico's, kwetsbaarheden of verbeterpunten bestaan die buiten de reikwijdte van dit onderzoek vallen. De bevindingen en aanbevelingen dienen daarom te worden geïnterpreteerd als een indicatief beeld en niet als een volledige of uitputtende beoordeling van de informatiebeveiliging. Vanwege het vertrouwelijke karakter van dit onderzoek zijn de detailbevindingen en aanbevelingen in afzonderlijke bijlagen verwerkt.

DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

DMC GROUP
SECURITY MANAGEMENT

2 Beantwoording onderzoeksvragen

De onderzoeksvragen zijn beantwoord op basis van de bevindingen uit de separate vertrouwelijke bijlagen.

Deelvragen

1. Komen de vastgestelde beleidsdoelstellingen (bijvoorbeeld conform de BIO2 en NIS2 wetgeving) overeen met de uitvoering in de gemeente Zevenaar?

De beleidskaders en -doelstellingen ten aanzien van informatiebeveiliging zijn beperkt en/of verouderd. Er zijn discrepanties tussen de werkelijkheid en de beleidskaders vastgesteld. Het informatiebeveiligingsbeleid stelt dat het ook van toepassing is op de Operationele Technologie (OT) systemen in de publieke ruimte, maar in de praktijk blijkt dat zowel het RID als de gemeente Zevenaar daar geen tactische en/of operationele rol in spelen en de veiligheidsstatus onbekend is. Daarnaast zijn de beleidskaders voornamelijk strategisch en onvoldoende vertaald naar operationeel niveau waardoor het lastig is om vast te stellen in hoeverre ze worden nageleefd.

2. Welke risico's en kwetsbaarheden komen in de onderzochte documenten van de gemeente Zevenaar en het RID de Liemers naar voren?

De gemeente Zevenaar heeft zeer beperkt documentatie beschikbaar waarin risico's en kwetsbaarheden worden behandeld. Er is geen integraal beeld van de risico's en kwetsbaarheden. Het ontbreekt aan een gestructureerd risicomanagementproces volgens de verplichte ISO 27001 standaard en Cyberbeveiligingswet (NIS2): het structureel identificeren en beoordelen van risico's, deze adresseren vanuit de operatie richting MT/bestuur, vanuit daar besluiten nemen en hier actief en aantoonbaar op sturen.

Het RID rapporteerde in 2024 ieder kwartaal over informatiebeveiliging, maar is daar in 2025 mee gestopt. Het RID heeft echter wel zicht op bekende technische kwetsbaarheden en misconfiguraties via bijvoorbeeld het Microsoft dashboard en de kwetsbaarhedenscanner, maar rapporteert daar niet over (zowel intern als extern).

De gemeente Zevenaar en het RID ontvangen maandelijks een rapport over kwetsbaarheden in het externe aanvalsoppervlak. Het sectorale Computer Emergency Response Team (CERT) de Informatiebeveiligingsdienst levert dit aan.

3. Welke risico's en kwetsbaarheden zijn in de praktijk gevonden?

De belangrijkste risico's en kwetsbaarheden die geïdentificeerd zijn:

1. Organisatorisch: de governance ten aanzien van informatiebeveiliging is niet op orde waardoor er onvoldoende mogelijkheden zijn om adequaat te kunnen sturen op dit onderwerp. De risicoperceptie wijkt daardoor af van de werkelijkheid.
2. Mensgericht: informatiebeveiliging is geen integraal onderdeel van de werkzaamheden en de aandacht voor dit onderwerp is ad-hoc gedreven en afhankelijk van individuen.
3. Fysiek: het ongeautoriseerd toegang verkrijgen tot het afgeschermde deel is eenvoudig.
4. Technologisch: beperking van de toegang, kwetsbare configuraties en opvolgingsmogelijkheden

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

en afhankelijkheden binnen de gedeelde infrastructuur van een Shared Service Center (SSC).

4. Welke beheerprocessen kent de gemeente Zevenaar en in hoeverre blijkt dat deze beheersprocessen worden nageleefd?

Het managementsysteem voor informatiebeveiliging is niet ingericht volgens de ISO 27001 waardoor de beheerprocessen ten aanzien van informatiebeveiliging beperkt (aantoonbaar) zijn. Aanvullend zijn het informatiebeveiligingsbeleid en de processen daaromtrent beperkt vertaald naar tactisch en operationeel niveau waardoor niet (goed) vastgesteld kan worden in hoeverre processen worden nageleefd.

5. In hoeverre draagt de gemeente Zevenaar zorg voor bewustwording bij medewerkers en externe partners?

Het bevorderen van veilig gedrag onder alle medewerkers is beperkt, heeft een vrijblijvend karakter en is ad-hoc gedreven, dit geldt voor zowel de gemeente Zevenaar als het RID. Activiteiten die hebben plaatsgevonden zijn onder andere: e-learning bij indiensttreding, mystery guest onderzoek en kennisdeling via intranet.

6. In hoeverre is de informatiebeveiliging van de gemeente Zevenaar voorbereid op verwachte toekomstige dreiging?

De gemeente Zevenaar en het RID zijn momenteel onvoldoende voorbereid op (toekomstige) cyberdreigingen. Deze kwetsbaarheid is het gevolg van een samenloop van factoren, waaronder: (1) een ontoereikende inrichting van het bedrijfscontinuïteitsbeheer, (2) een onvoldoende uitgewerkt en getest incident response proces, (3) beperkte pro-actieve security monitoring, en (4) beperkt inzicht in het feitelijke risicoprofiel.

De uitgevoerde penetratietest door Dong-IT heeft waardevolle inzichten opgeleverd in technische kwetsbaarheden en misconfiguraties. Het uitvoeren van dergelijke onafhankelijke technische beoordelingen is echter geen structureel onderdeel van de beveiligingsaanpak. Om de weerbaarheid te vergroten, is het van belang dat informatiebeveiliging met name vanuit technisch perspectief periodiek en onafhankelijk wordt getoetst. Dit draagt bij aan een beter inzicht in risico's, het tijdig identificeren van kwetsbaarheden en het structureel verbeteren van de beveiligingsmaatregelen.

7. Welke knelpunten werken blokkerend voor een optimale informatiebeveiliging en welke verbeteringstrajecten zijn aan te bevelen?

De governance binnen de gemeente Zevenaar en in de Samenwerking de Liemers met het RID ten aanzien van informatiebeveiliging zijn het belangrijkste aandachtspunt. Het is uitermate belangrijk om dit volgens de ISO 27001 structuur in te richten en binnen de Samenwerking de Liemers duidelijke afspraken hieromtrent te maken. Gebleken is dat essentiële informatie blijft steken op operationeel en tactisch niveau, ten nadele van het risicoprofiel, de urgentie en bestuurlijk draagvlak en ondersteuning.

DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

Hoofdvraag

In welke mate is de informatiebeveiliging in de gemeente Zevenaar voldoende geborgd en in hoeverre biedt de aanwezige documentatie de gemeenteraad het benodigde inzicht om effectief te sturen op dit thema?

Informatiebeveiliging heeft de aandacht binnen zowel de gemeente Zevenaar als het RID. Desondanks is dit thema onvoldoende verankerd in een gestructureerd en cyclisch managementsysteem. Hierdoor ontbreekt het aan consistent en integraal inzicht, wat het vermogen om effectief te sturen en bij te sturen belemmerd.

Daarnaast is de beschikbare documentatie beperkt en worden belangrijke afspraken veelal mondeling gemaakt, zonder centrale en formele vastlegging. Dit leidt tot een gebrek aan transparantie en herleidbaarheid. Voor zowel de gemeente Zevenaar als het RID is het daardoor lastig om inzichtelijk te maken welke afspraken zijn gemaakt, welke afwegingen daaraan ten grondslag liggen en wat de actuele stand van zaken is. Deze situatie bemoeilijkt niet alleen de interne sturing, maar vormt ook een belemmering voor verantwoording en toetsbaarheid richting externe stakeholders, zoals een toezichthouder.

2.1 Aanbevelingen gemeenteraad

De gemeenteraad heeft een belangrijke rol ten aanzien van de informatieveiligheid binnen de gemeente Zevenaar. De VNG[12] benadrukt dat digitale veiligheid een bestuurlijke verantwoordelijkheid is die niet alleen de ambtelijke organisatie betreft, maar een integraal onderdeel moet zijn van het bestuurlijke werk van de raad. Door als raad het onderwerp regelmatig te agenderen, kaders te stellen, prioriteiten te bepalen, voldoende middelen beschikbaar te stellen en toezicht te houden op hoe de gemeente Zevenaar risico's beheerst en incidenten aanpakt, is de raad in staat haar kaderstellende en controlerende taak goed te vervullen. Het doel is het versterken van de (digitale) veiligheid van de gemeentelijke dienstverlening en de weerbaarheid van de gemeente Zevenaar en haar inwoners en ondernemers.

1. Neem kennis van de beschikbare hulpmiddelen[13][14] zodat u (beter) in staat bent om de juiste accenten te leggen en het gesprek inhoudelijk aan kunt gaan met het college.
2. Realiseer u dat de ENSIA-verantwoording een beperkt beeld van de realiteit schetst vanwege zelfevaluaties en beperkte onafhankelijke toetsing. Daarnaast richt ENSIA zich vooralsnog uitsluitend op het voldoen in opzet en bestaan aan de BIO-beheersmaatregelen, en niet op de effectieve werking over een langere periode. Zet het onderwerp informatiebeveiliging daarom regelmatig op de agenda en nodig bijvoorbeeld de CISO uit om de raad hierover bij te praten. Dit biedt de raad tevens ook de mogelijkheid om (technische) vragen te stellen.
3. De Cybersecurity Raad[15] adviseerde in 2018 al om minimaal 10% van het totale IT-budget voor informatiebeveiliging aan te wenden. Sinds 2018 is het cyberdreigingslandschap verergerd en zijn er meer wettelijke eisen in werking getreden. Het is dan ook niet meer dan logisch dat de kosten voor het onderhouden en aanscherpen van de algehele informatiebeveiliging ook toenemen. Wees uzelf daarvan bewust bij de totstandkoming van de begroting.

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

4. Verzoek het college om minimaal jaarlijks een rapport aan de raad op te leveren waarin uitgebreid stilgestaan wordt bij informatiebeveiliging. De I&A-visie bevat een mooie opzet en ambitie voor informatiebeveiliging, maar het ontbreekt aan een uitvoeringsplan waaruit blijkt wat gerealiseerd is, hoe middelen zijn besteed en hoe de opvolging plaatsvindt. Zorg dat er concrete afspraken hieromtrent gemaakt worden zodat de raad haar controlerende taak adequaat kan vervullen.

Einde van het openbare rapport

DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

DMC GROUP
SECURITY MANAGEMENT

Noten

[1] Informatietechnologie is een term binnen de informatica en behandelt een groot werkveld in de computertechnologie van hardware, software en computernetwerken.

[2] Een verzamelnaam voor verschillende systemen die worden gebruikt voor het beheer van operationele processen in de fysieke wereld zoals het aansturen en monitoren van (industriële) apparatuur. Voorbeelden zijn sluizen en medische apparatuur.

[3] Security Information and Event Management, systeem waarin men informatie uit computersystemen verzamelt en analyseert. Het doel is om verdacht gedrag te ontdekken of zien dat iemand dingen in het systeem heeft veranderd, terwijl hij dat niet mocht. Security Operations Center, afdeling, team of dienst dat digitale systemen en/of indentity's controleert en/of bewaakt en soms ook afhandelt.

[4] https://vng.nl/artikelen/raadgever-digitale-veiligheid

[5] https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2025/06/IBD-Dreigingsbeeld-informatiebeveiliging-2025-2026.pdf

[6] Kwaadaardige software waarbij een slachtoffer afgeperst wordt, nadat zijn digitale systeem of de bestanden erop met een code op slot zijn gezet. De aanvaller biedt de code tegen betaling aan, zodat hij er weer bij kan. Maar zelfs dat is niet zeker. Ransomware is een samenvoeging van de woorden ransom (losgeld) en software. Tegenwoordig is de daadwerkelijke software maar een kleine stap in de totale aanval die plaatsvindt. Alle stappen samen vormen de Ransomware Killchain.

[7] Een gangbare term voor een cyberincident, veelal gebruikt in relatie tot persoonsgegevens. In de context van de Algemene Verordening Gegevensbescherming is een datalek een leken-term voor 'inbreuk in verband met persoonsgegevens', inhoudende een incident waardoor de integriteit, beschikbaarheid en/of vertrouwelijkheid van persoonsgegevens worden aangetast. Voorbeelden zijn ransomware aanvallen, of een e-mail met alle geadresseerden in het "To" – veld.

[8] https://www.aivd.nl/documenten/publicaties/2025/11/26/cybersecuritybeeld-nederland-2025

[9] Generatieve AI gaat over vormen van kunstmatige intelligentie (AI) die nieuwe content creëren of genereren. Zoals teksten en afbeeldingen die net echt lijken.

[10] https://www.rdi.nl/

[11] Handmatige controle waarbij men zo diep mogelijk wil binnendringen in een digitaal systeem om zwakke plekken te vinden en de gevolgen hiervan te kennen. Men gebruikt de zwakke plekken om nog wat dieper in het systeem te komen. Doel van de test is niet om zoveel mogelijk zwakke plekken te vinden, maar om te onderzoeken of een systeem zwakke plekken kent. Het zoeken naar zoveel mogelijk zwakke plekken gebeurt wel bij een vulnerability scan.

[12] https://vng.nl/artikelen/raadgever-digitale-veiligheid

[13] https://vng.nl/sites/default/files/2025-04/raadsleden-en-informatiebeveiliging.pdf

[14] https://vng.nl/sites/default/files/2023-04/checklist-raadsleden-digitale-veiligheid.pdf

[15] https://www.cybersecurityraad.nl/documenten/2018/04/01/csr-meerjarenstrategie-2018-2021

DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group