Rekenkameronderzoek informatiebeveiliging

Gemeente Steenwijkerland

DMC GROUP
SECURITY MANAGEMENT

Documentbeheer

Opdrachtgever
Rekenkamer Steenwijkerland

Versie
v1.0

Datum
21 juni 2026

Auteur(s)
ir. Stijn Hoogervorst CISSP CISM
mr. Alexander Garrelfs CCSP CISSP CISM CIPP/e OTPM/A
Timothy Siebes MSc. GCIH GSEC CISSP
drs. Chris Deben MBA CISM
Mick Deben MSc. CISSP CRISC CGEIT CCSP SSCP AAISM

Distributie
DMC Group distribueert alle versies beveiligd (end-to-end versleuteld) via Tresorit

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 personele unie van de rekenkamers van de gemeenten Meppel, Staphorst, Steenwijkerland en Westerveld (MSSW) heeft DMC een onderzoek naar de informatiebeveiliging bij de vier gemeenten uitgevoerd. Voor elke gemeente is een afzonderlijk en zelfstandig onderzoek uitgevoerd. De onderzoeken hebben plaatsgevonden in de periode augustus 2025 - december 2025. In dit rapport zijn uitsluitend de bevindingen van de gemeente Steenwijkerland verwerkt en zijn aanbevelingen gedaan ter verbetering van de algehele informatiebeveiliging. De rekenkamer trekt op basis van dit rapport 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 BIO2: Organisatorisch, Mensgericht, Fysiek en Technologisch. De vier domeinen zijn complementair en zorgen samen voor een integrale beheersing van informatiebeveiligingsrisico's: bestuurlijk geborgd, menselijk gedragen, fysiek beschermd en technisch afgedwongen.

Organisatorisch

Het organisatorische domein gaat over governance, verantwoordelijkheid en sturing op informatiebeveiliging. 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.

Steenwijkerland beschikt over een goed doordachte en verankerde strategie ten aanzien van informatiebeveiliging die breed wordt ondersteund door medewerkers en management. Informatiebeveiliging leeft en staat structureel op de agenda's. De belangrijkste aandachtspunten hebben betrekking op het aanscherpen en aantoonbaar maken van risicobeheer, het goed voorbereid zijn op cyberincidenten en -crises, het gelijktrekken van het beveiligingsniveau in hybride omgevingen en het verder uitwerken en formaliseren van informatiebeveiligingsbeleid.

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

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 reageren op beveiligingsincidenten; goed geïnformeerde en handelingsbekwame medewerkers verkleinen risico's aanzienlijk.

Er is sprake van een hoog bewustzijnsniveau op het gebied van informatieveiligheid, waarbij medewerkers zich verantwoordelijk tonen en openstaan voor feedback en verbetering. De belangrijkste aandachtspunten hebben betrekking op transparantie over de verwerking van gegevens van medewerkers en de wijze waarop Steenwijkerland handelingen van medewerkers monitort.

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.

Steenwijkerland heeft compartimentering toegepast en de rechten tot verschillende compartimenten gescheiden op basis van het 'need-to-be' principe. Het belangrijkste aandachtspunt heeft betrekking op het vergroten van de herkenbaarheid van bezoekers en medewerkers.

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.

Steenwijkerland heeft op technisch vlak diverse maatregelen geïmplementeerd die de weerbaarheid versterken. De belangrijkste aandachtspunten hebben betrekking op de mate waarin Steenwijkerland afhankelijk is van cloudleveranciers (vendor lock-in), het tijdig detecteren van en reageren op afwijkingen en incidenten en de beveiliging van het lokale- en uitwijk datacenter.

De bevindingen doen geen afbreuk aan de volwassenheid van Steenwijkerland op het gebied van informatiebeveiliging. De aanbevelingen dienen vooral ter verdere versterking en professionalisering van bestaande processen. Zij vormen daarmee geen indicatie van ondermaatse prestaties, maar juist van een organisatie die continu werkt aan verbetering en groei binnen een al hoog volwassenheidsniveau.

[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.

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

Aanbevelingen aan het college van B&W

Bestudeer de bevindingen en aanbevelingen in dit rapport en bepaal of de aanbevelingen worden overgenomen, en zo ja op welke termijn. Ken aan elke actie een actiehouder toe en stuur op opvolging.

Aanbevelingen aan de gemeenteraad

De gemeenteraad heeft een belangrijke rol ten aanzien van de informatieveiligheid binnen Steenwijkerland. De VNG[3] 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 Steenwijkerland risico's beheerst en incidenten aanpakt, is de raad in staat haar kaderstellende en controlerende taak goed te vervullen. Het doel is het structureel versterken van de (digitale) veiligheid van de gemeentelijke dienstverlening en de weerbaarheid van Steenwijkerland en haar inwoners en ondernemers.

Neem kennis van de beschikbare hulpmiddelen[4][5] zodat u (beter) in staat bent om de juiste accenten te leggen en het gesprek inhoudelijk aan kunt gaan met het college.

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.

De Cybersecurity Raad[6] adviseerde in 2018 al om minimaal 10% van het totale IT-budget voor informatiebeveiliging aan te wenden. Sinds 2018 is het cyberdreigingslandschap vergroot 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.

[3] https://vng.nl/artikelen/raadgever-digitale-veiligheid
[4] https://vng.nl/sites/default/files/2025-04/raadsleden-en-informatiebeveiliging.pdf
[5] https://vng.nl/sites/default/files/2023-04/checklist-raadsleden-digitale-veiligheid.pdf
[6] 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

DMC GROUP
SECURITY MANAGEMENT

Inhoudsopgave

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 Steenwijkerland 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 [7] benadrukt dat ransomware[8], datalekken[9] 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[10] 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 de schaal en impact van cyberdreigingen vergroot. Ondanks deze ontwikkelingen benadrukt de AIVD dat veel incidenten te voorkomen zijn met goede basismaatregelen en weerbaarheidstrainingen. Dit onderstreept het belang voor gemeenten om de BIO2 te implementeren en te onderhouden.

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

[8] 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.

[9] 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.

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

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

In dit onderzoek is onder andere onderzocht hoe Steenwijkerland 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 Steenwijkerland inspeelt op opkomende risico's en toekomstige technologische ontwikkelingen. Zo wordt de volwassenheid in context geplaatst van het actuele cyberdreigingsbeeld.

1.2 Cyberbeveiligingswet

De 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. Zij moeten zelf over voldoende kennis beschikken en borgen dat medewerkers structureel worden opgeleid. Daarnaast is Steenwijkerland verantwoordelijk voor het tijdig melden van meldplichtige incidenten. De toezichthouder voor overheidsorganisaties is de Rijksinspectie Digitale Infrastructuur (RDI).[11]

1.3 Onderzoeksvragen en -aanpak

De hoofdvraag van dit onderzoek luidt: *Hoe wordt de informatieveiligheid binnen de gemeenten georganiseerd, welke maatregelen zijn er genomen om de veiligheid van gevoelige gegevens te waarborgen, en in hoeverre zijn de kritische processen van de gemeenten beschermd tegen infiltratie en ongeautoriseerde toegang?* De rekenkamer heeft twintig deelvragen geformuleerd verdeeld over acht categorieën:

1. Algemene informatieveiligheid
2. Beveiliging van kritische systemen
3. Risicoanalyse en dreigingen
4. Testen van infiltratie
5. Opleiding en bewustwording van personeel
6. Beveiliging van gegevens en privacy
7. Incidentmanagement en crisiscommunicatie
8. Kosten beveiligingsmaatregelen

Om de hoofd- en deelvragen te beantwoorden is informatie en zijn documenten opgevraagd, interviews gehouden met verschillende medewerkers en heeft een schouw op locatie plaatsgevonden. De deelvragen zijn in het derde hoofdstuk beantwoord.

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

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

1.4 Disclaimer

Dit rapport vormt een momentopname van de huidige volwassenheid 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.

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 Bevindingen & aanbevelingen

De bevindingen en aanbevelingen zijn onderverdeeld in de vier domeinen die aansluiten op de structuur van de Baseline Informatiebeveiliging Overheid (BIO) 2[12]:

- Organisatorisch als het betrekking heeft op organisatorische aspecten;
- Mensgericht als het betrekking heeft op individuele personen;
- Fysiek als het betrekking heeft op fysieke objecten;
- Technologisch als het betrekking heeft op technologie.

De aanbevelingen in paragrafen 2.1 tot en met 2.4 zijn gericht aan het college van B&W. De aanbevelingen in paragraaf 2.5 zijn gericht aan de gemeenteraad.

2.1 Organisatorisch

Het organisatorische domein gaat over governance, verantwoordelijkheid en sturing op informatiebeveiliging. 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 (Information Security Management Systeem, ook wel ISMS) is een werkwijze om informatiebeveiliging op een gestructureerde manier toe te passen in de gemeente. Zo wordt de gemeente, en een bestuurder in het bijzonder, in staat gesteld om de juiste afwegingen te maken.

Om een veelvoorkomend misverstand te voorkomen: een managementsysteem is géén applicatie. Een applicatie kan wel ondersteunen bij het toepassen van een managementsysteem.

De BIO schrijft voor dat het managementsysteem van een organisatie voldoet aan NEN-EN-ISO/IEC 27001. Bij het bepalen van de reikwijdte van het managementsysteem moet een organisatie minimaal de bedrijfsprocessen en informatiesystemen opnemen die kritisch zijn voor haar dienstverlening, waarbij aantasting van de beschikbaarheid, integriteit of vertrouwelijkheid zou leiden tot onacceptabele impact.

Het managementsysteem voor informatiebeveiliging borgt de beschikbaarheid, integriteit en vertrouwelijkheid van informatie door een risicomanagementproces toe te passen. Dit geeft belanghebbenden het vertrouwen dat risico's adequaat worden beheerd.

Het is belangrijk dat het managementsysteem voor informatiebeveiliging deel uitmaakt van en geïntegreerd is met de procedures van de gemeente en met de algehele managementstructuur, en dat informatiebeveiliging in aanmerking wordt genomen bij het ontwerpen van processen, informatiesystemen en beheersmaatregelen.

[12] https://www.bio-overheid.nl/nieuws/bio2-vernieuwde-baseline-informatiebeveiliging-overheid-gepubliceerd

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

2.1.1 Bevindingen

1. Binnen Steenwijkerland wordt actief gestuurd op een open meldcultuur. Medewerkers worden aangemoedigd om incidenten en problemen te melden en verantwoordelijkheid te nemen, waarbij er geen sprake is van schaamte of terughoudendheid om fouten te delen.
2. Er is in 2024 een cybercrisisoefening gehouden om de weerbaarheid van Steenwijkerland te testen, met het voornemen deze oefening in de toekomst opnieuw te organiseren.
3. Informatiebeveiliging wordt structureel geagendeerd binnen Steenwijkerland; tweemaal per jaar vindt overleg plaats met het Security Board, waarbij vanuit verschillende invalshoeken wordt bijgedragen aan dit onderwerp.
4. Beleidsdocumenten op het gebied van informatiebeveiliging en aanverwante thema's worden formeel vastgesteld door de directie of bekrachtigd door het college. In 2025 is beleid ten aanzien van Artificial Intelligence vastgesteld, waarmee Steenwijkerland laat zien een verstandige en zorgvuldige voorloper te willen zijn op dit terrein.
5. Een formele retainer[13] ten behoeve van Digital Forensics & Incident Response (DFIR) met een gespecialiseerde partij is niet afgesloten; dit wordt meegenomen in de lopende SOC/SIEM-aanbesteding.[14] Er is binnen Steenwijkerland overeenstemming bereikt dat bij een ernstige cybercrisis een externe, gespecialiseerde partij zal worden ingeschakeld voor ondersteuning bij besluitvorming, schade afhandeling en herstel. Steenwijkerland kan te allen tijde contact opnemen met de Informatiebeveiligingsdienst (IBD) voor ondersteuning tijdens een cyberincident, maar de IBD ondersteunt gemeenten niet op locatie.
6. Bijlage 12 van de openbare SIEM/SOC aanbesteding bevat gevoelige en waardevolle informatie voor kwaadwillenden. Hierin is opgenomen welke hard- en software Steenwijkerland gebruikt inclusief de versienummers. Kwaadwillenden kunnen hier kennis van nemen en gericht aanvallen uitvoeren.
7. Er is binnen Steenwijkerland geen actueel risicoregister beschikbaar waarin risico's op het gebied van informatiebeveiliging en privacy systematisch worden vastgelegd, gerapporteerd, beoordeeld en opgevolgd.
8. Binnen Steenwijkerland heerst een behulpzame cultuur die verder reikt dan alleen de IT-afdeling. Deze houding draagt positief bij aan samenwerking en het snel oplossen van informatiebeveiligings- en IT-vraagstukken.
9. De CISO[15] draagt actief de onderliggende filosofie van informatieveiligheid uit en is voor medewerkers en management goed benaderbaar. Tegelijkertijd is zichtbaar dat Steenwijkerland in belangrijke mate leunt op zijn kennis en aanwezigheid, waardoor afhankelijkheid van één persoon ontstaat.

[13] Een contractuele overeenkomst waarbij garanties worden afgegeven door de gespecialiseerde partij over het bieden van ondersteuning bij cyberincidenten
[14] https://www.tenderned.nl/aankondigingen/overzicht/405225
[15] Chief Information Security Officer

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

10. Binnen Steenwijkerland zijn de taken, verantwoordelijkheden en bevoegdheden van de CISO formeel vastgelegd, voor de ISO en TISO rollen is dit niet het geval.[16] Desondanks is sprake van een hoge mate van betrokkenheid en verantwoordelijkheid bij de uitvoering van werkzaamheden op het gebied van informatiebeveiliging. De CISO is zich duidelijk bewust van zijn rol en vervult deze met overtuiging en professionaliteit. Hij is toegankelijk voor medewerkers en management, communiceert open en transparant, en schroomt niet om waar nodig kritisch te zijn en knelpunten bespreekbaar te maken.
11. De implementatie van de Baseline Informatiebeveiliging Overheid (BIO) maatregelen binnen de Microsoft Azure-omgeving loopt asynchroon vergeleken met de lokale IT-omgeving.
12. De privacy organisatie binnen Steenwijkerland is gedegen ingericht en functioneert conform het drie-lijnenmodel[17]. De i-adviseurs vervullen in de eerste lijn een signalerende rol als 'voelsprieten' binnen Steenwijkerland, terwijl de privacy officers in de tweede lijn zorgen voor de uitvoering van privacytaken en de afstemming met relevante stakeholders. De FG[18] houdt vanuit de derde lijn toezicht en wordt actief betrokken bij incidenten en DPIA's[19]. De samenwerking tussen de FG, de lijnorganisatie, de CISO en andere betrokken partijen verloopt constructief. Het verwerkingsregister is volledig en wordt actueel gehouden door wijzigingen in processen en verwerkingen tijdig te verwerken.
13. De registratie en opvolging van privacy-incidenten vindt plaats in het datalekkenregister van de gemeente. Hierin wordt naast registratie ook de verdere afhandeling vastgelegd. Ieder boekjaar wordt het register opgeslagen in het zaaksysteem. Dit proces is echter niet (goed) gedocumenteerd en daardoor niet structureel geborgd. De continuïteit bij personele wisselingen is daardoor in het geding.
14. De onafhankelijkheid en positionering van de FG is niet formeel vastgelegd in een handvest of mandaatdocument, hetgeen risico's kan opleveren voor de structurele borging van diens toezichtrol.
15. Documentatie gerelateerd aan informatiebeveiliging is overwegend verouderd en informeel. Aspecten zoals versiebeheer, classificatie, eigenaarschap, geldigheid, etc. ontbreken.
16. Steenwijkerland heeft beperkt tactisch en operationeel (vastgesteld) beleid ten aanzien van informatiebeveiliging.

2.1.2 Aanbevelingen

1. Leg de afspraken met betrekking tot externe crisisondersteuning vooraf formeel vast, bijvoorbeeld via een retainercontract, zodat bij een daadwerkelijke cyberaanval direct duidelijk is welke partij en welke procedures worden ingezet voor besluitvorming en ondersteuning.

[16] Information Security Officer, Technical Information Security Officer
[17] https://www.rijksfinancien.nl/sites/default/files/hafir/extra-info/Uiteenzetting-Three-Lines-Model-IAA.pdf
[18] Functionaris Gegevensbescherming
[19] Data Protection Impact Assessment

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

2. Stel een risicoregister op en onderhoud dit, zodat risico's op het gebied van informatiebeveiliging en privacy gestructureerd worden geïdentificeerd, beoordeeld en gemonitord.
3. Borg de continuïteit van de CISO-functie door tijdig een plaatsvervanger of 'backup CISO' op te leiden die vertrouwd is met de beleidskaders, processen en cultuur van informatiebeveiliging binnen Steenwijkerland.
4. Richt een formeel risico-acceptatieproces ('explain-proces') in, waarmee afwijkingen van BIO-maatregelen systematisch worden beoordeeld, vastgelegd en verantwoord richting het management.
5. Richt een structureel en afgeschermd registratiesysteem in voor privacy-incidenten, bijvoorbeeld door gebruik te maken van een ticketsysteem of centraal register.
6. Zorg ervoor dat er geen discrepanties zijn tussen de mate van beveiliging in cloud- en lokale IT-omgevingen.
7. Leg de positionering, onafhankelijkheid en bevoegdheden van de (externe) FG formeel vast in een handvest of mandaatdocument.
8. Werk het informatiebeveiligingsbeleid verder uit in tactisch en operationeel beleid en stel dit formeel vast.
9. Wees terughoudend met het delen van gevoelige informatie in openbare stukken behorend tot aanbestedingen. Deel gevoelige informatie pas in een later stadium of uitsluitend via directe communicatie met belanghebbenden.

2.2 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.

2.2.1 Bevindingen

1. Het is onduidelijk op welke manier medewerkers worden geïnformeerd over de omgang met hun persoonsgegevens gedurende het dienstverband en over eventuele monitoringactiviteiten die plaatsvinden ten behoeve van informatiebeveiliging.
2. Het indiensttredingsproces is goed ingericht. Iedere nieuwe medewerker volgt verplicht een training op het gebied van informatiebeveiliging en er wordt actief gemonitord of deze training daadwerkelijk is afgerond. De training wordt bovendien periodiek geëvalueerd en aangepast waar nodig.

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

3. Er is een duidelijk informatieraamwerk vastgesteld waarin staat waar en hoe medewerkers gegevens dienen op te slaan.

4. Steenwijkerland stimuleert bewustwording via een tool ('het initiatief Sir Askalot'), waarin wekelijks op een laagdrempelige manier aandacht wordt besteed aan informatiebeveiliging, privacybescherming en integriteit. Dit draagt zichtbaar bij aan een positieve en lerende veiligheidscultuur.

5. Er is geen formeel rol-gebaseerde toegang (RBAC)[20] ingericht. Softwaretoegang wordt momenteel via teamleiders aangevraagd, en tweemaal per jaar vindt een controle plaats op de geldigheid van applicatierechten. Er is geen vastgelegde lijst met autorisaties per functie, waardoor toekenning grotendeels op basis van onderlinge bekendheid plaatsvindt. Bij disciplinaire maatregelen wordt het integriteitsproces gevolgd en overige HRM-processen zijn goed op orde.

6. Binnen Steenwijkerland is vastgesteld dat medewerkers goed op de hoogte zijn van wat er van hen wordt verwacht op het gebied van informatieveiligheid. De verplichte trainingen en het bewustwordingsprogramma Sir Askalot worden positief en niet als belastend ervaren. Medewerkers weten waar zij terecht kunnen met vragen over informatiebeveiliging en geven aan dat zij geïnstrueerd zijn om nooit vertrouwelijke gegevens te delen met burgers via de telefoon. Ook is er geen sprake van druk of pogingen van buitenaf om dergelijke informatie te ontfutselen.

7. Medewerkers signaleren incidenteel onbekende personen op de gangen. Bezoekers zijn herkenbaar aan rode keycords, waardoor zij in de meeste gevallen snel worden herkend en aangesproken.

8. Medewerkers ervaren over het algemeen een goede balans tussen werkbaarheid en informatiebeveiliging. Wel is opgemerkt dat het automatische script dat voorheen de downloadmappen van werkstations leegmaakte om datalekken te voorkomen, sinds de overstap naar de cloudomgeving niet langer actief is. Medewerkers moeten nu zelf hun downloads verwijderen.

2.2.2 Aanbevelingen

1. Zorg voor transparante communicatie richting medewerkers over de verwerking van hun persoonsgegevens gedurende het dienstverband en monitoring van digitale handelingen.

2. Blijf investeren in de bestaande bewustwordingsinitiatieven, zoals Sir Askalot, en evalueer periodiek de effectiviteit nadat concrete doelstellingen, eventueel per doelgroep, zijn vastgesteld.

3. Integreer de inhoud van de informatie- en opslagmatrix in de bestaande trainingen ten aanzien van informatiebeveiliging.

[20] Bepalen of een gebruiker bij een digitaal systeem mag komen. Men kijkt daarbij naar de rol die de gebruiker of een groep gebruikers heeft. Voorbeelden van rollen zijn viewer, editor en manager.

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

2.3 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.

2.3.1 Bevindingen

1. Binnen het domein gebouwbeheer is vastgesteld dat het toegangssysteem met druppelregistratie naar behoren functioneert en correct is geïmplementeerd.
2. Tijdens de bezoeken is geconstateerd dat bezoekers zich bij binnenkomst niet hoefden te legitimeren en dat er geen bezoekersbadge werd verstrekt of zichtbaar gedragen. Hierdoor is voor medewerkers niet zichtbaar wie een interne medewerker is en wie een externe bezoeker. Medewerkers dragen niet zichtbaar een toegangspas of ander herkenbaar identificatiemiddel.
3. De deur vanaf de parkeerplaats vormt een verhoogd risico op zogenoemd “meelopen” (tailgating), waarbij onbevoegden ongemerkt het gebouw kunnen betreden.

2.3.2 Aanbevelingen

1. Implementeer een herkenbaar registratie- en badgesysteem voor zowel bezoekers als medewerkers, zodat voor alle medewerkers direct zichtbaar is wie geautoriseerd toegang heeft. Iedereen dient zichtbaar herkenbaar te zijn.
2. Evalueer het risico op meelopers bij de ingang vanaf de parkeerplaats en bepaal een proportionele mitigerende maatregel.

2.4 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 IT- en OT-beveiliging.

2.4.1 Bevindingen

1. Steenwijkerland heeft een duidelijke visie op de inrichting van de ICT binnen de gemeente, gebaseerd op het Microsoft Azure-platform, met als kernwaarden schaalbaarheid, flexibiliteit en security. De uniformiteit en deskundigheid binnen de ICT-afdeling weerspiegelen deze visie. Tegelijkertijd ontstaat hierdoor een afhankelijkheid van één leverancier, hetgeen risico’s met zich meebrengt op het gebied van vendor lock-in en geopolitieke dreigingen.

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

2. Het fysieke datacenter en de uitwijkvoorziening krijgen in de huidige opzet onvoldoende aandacht. De huidige uitwijkconstructie brengt onnodige risico's met zich mee.
3. Er is sprake van gedeelde faciliteiten met de gemeente Meppel, waarbij autorisaties onvoldoende zijn vastgelegd. Zo is er geen sluitende procedure voor toegang en zijn de serverkasten van Meppel in het gemeentehuis van Steenwijkerland toegankelijk voor onbevoegde personen.
4. Er is een intentieverklaring, maar geen formeel contract over de gedeelde faciliteiten tussen de gemeenten Meppel en Steenwijkerland.
5. Steenwijkerland monitort haar systemen en netwerken niet pro-actief (SIEM[21]/SOC[22]). Microsoft meldingen worden incidenteel opgevolgd tijdens kantooruren. Buiten kantoortijd vindt geen structurele monitoring plaats.
6. Steenwijkerland maakt gebruik van Qualys voor kwetsbaarhedenbeheer. Het is onduidelijk of de Azure-omgeving actief in deze controles is opgenomen.
7. De Center for Internet Security (CIS) benchmarking[23] functionaliteit binnen Microsoft Azure is niet geactiveerd.
8. Binnen de netwerkarchitectuur is poortgebaseerde toegangscontrole[24] uitgerold op het draadloze netwerk. Poortconfiguratie vindt handmatig plaats, waardoor risico's ontstaan op ongeautoriseerde aansluiting van apparaten op het draadloze- en bedrade netwerk.
9. Steenwijkerland heeft geen volledige inventarisatie gemaakt van de aanwezige OT-[25] en IoT-apparatuur[26] die wordt gebruikt voor kantoorwerkzaamheden.
10. Netwerkpoorten die niet in gebruik zijn, worden momenteel toegewezen aan een specifiek netwerksegment (dummy-VLAN[27]), maar dit VLAN[28] wordt niet actief gemonitord.
11. Voor het beheren van de firewall worden lokale accounts gebruikt waarvan de wachtwoorden zijn opgeslagen in een KeePass-bestand[29]. Het wachtwoord van dit

[21] 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.
[22] Afdeling, team of dienst dat digitale systemen en/of -identiteiten controleert en/of bewaakt en soms ook afhandelt.
[23] CIS benchmarks zijn veilige configuraties voor diverse soft- en hardware waarbij het aanvalsoppervlak is gereduceerd door het uitschakelen en blokkeren van onnodige functionaliteiten en accounts.
[24] 802.1X authenticatie RFC 3580 https://www.rfc-editor.org/rfc/rfc3580
[25] Operational Technology is 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.
[26] Een netwerk van slimme apparaten, sensoren en andere objecten die (vaak verbonden met het Internet) gegevens verzamelen over hun omgeving, deze kunnen uitwisselen en op basis daarvan (semi-) autonome beslissingen of acties nemen die van invloed zijn op hun omgeving.
[27] Virtual Local Area Network
[28] Het onderverdelen van een fysiek computernetwerk in verschillende logische onderdelen die van elkaar afgeschermd kunnen worden. Op elk netwerksegment kunnen verschillende beveiligingsmaatregelen worden toegepast. Zo krijgt een aanvaller die in een bepaald netwerksegment is gekomen, niet automatisch toegang tot andere (kwetsbare) delen in het computernetwerk.
[29] KeePass is een wachtwoordmanager, zie https://keepass.info/

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

bestand is eenvoudig te onthouden en daardoor kwetsbaar. Daarnaast is het alleen indirect mogelijk om uitgevoerde acties te herleiden naar individuen.

12. De e-mailbeveiliging bevat een sandboxingmechanisme[30] (Microsoft E5 licentie).
13. Mobile Application Management (MAM) voor Outlook is geïmplementeerd, waardoor bestanden niet buiten de beheerde omgeving gedownload kunnen worden.
14. Er is vastgesteld dat binnen de Azure-omgeving een global administratoraccount aanwezig was waarvan het gebruik niet gemonitord werd. Dit is vervolgens direct gecorrigeerd.
15. De huidige inrichting van de cloudomgeving bevat geen structurele toets op de effectiviteit van uitwijk- en herstelmaatregelen. Hierdoor is niet aantoonbaar in hoeverre Steenwijkerland in staat is om bedrijfscontinuïteit te waarborgen bij een calamiteit in de cloudomgeving.
16. Binnen Steenwijkerland wordt gebruikgemaakt van één of meerdere servers die zich buiten het directe beheer van Steenwijkerland bevinden genaamd RAAS-servers[31], maar wel operationeel zijn binnen het gecontroleerde netwerkdomein. Over het patchniveau en de toegepaste beveiligingsmaatregelen van deze systemen bestaat geen inzicht. Hierdoor is niet aantoonbaar in hoeverre deze servers voldoen aan de geldende beveiligingsnormen en vormt dit een potentieel risico voor de integriteit en veiligheid van het netwerk.
17. Poort 22 Secure Shell[32] staat open naar het internet toe op de subdomeinen (api.)betalen.steenwijkerland.nl met IP-adres: 176.62.195.145.

2.4.2 Aanbevelingen

1. Ontwikkel en implementeer een formeel rol-gebaseerde toegang (RBAC) waarin per functie wordt vastgelegd welke software en toegangsrechten noodzakelijk zijn.
2. Evalueer de huidige technische maatregelen rondom lokale opslag van bestanden en overweeg het herinvoeren van automatische opruimmaatregelen binnen de cloudomgeving.
3. Toets de Azure-omgeving expliciet aan de BIO-maatregelen om inzicht te verkrijgen in de mate van naleving en om eventuele tekortkomingen gericht te kunnen adresseren.

[30] Afgeschermd deel in een digitaal systeem. Software die op deze plek werkt, kan geen andere processen in de computer verstoren. Sandboxen kennen verschillende implementaties: - Gebruik als software om applicaties binnen deze sandbox te beschermen tegen aanvallen (wordt vaak toegepast binnen MDM oplossingen). - Een systeem in het netwerk dat ingezet wordt om te onderzoeken op onbekende content (zoals gedownload vanaf het Internet) ongewenst gedrag vertoont.

[31] Reisdocumenten Aanvraag- en Archiefstation

[32] Computerprogramma waarmee een gebruiker met een commandoregel opdrachten kan geven aan het besturingssysteem van een computer.

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. Herzie op korte termijn de afspraken rondom de uitwijklocatie en richt een sluitende toegangsprocedure in.
5. Richt tijdelijke alarmering buiten kantoortijden in (totdat SOC gerealiseerd is), bijvoorbeeld via een pager- of notificatiesysteem voor meldingen met een hoge prioriteit (severity High).
6. Controleer of de Azure-omgeving volledig is geïntegreerd in kwetsbaarhedenbeheer en activeer de CIS-benchmarking.
7. Breid de dekkingsgraad van 802.1x-authenticatie uit om netwerktoegang te beperken tot geautoriseerde apparaten.
8. Voer een inventarisatie uit van alle OT/IoT-apparaten en stel beleid op voor beheer en segmentatie.
9. Implementeer een sterkere authenticatie- en wachtwoordbeheermethode voor kritieke beheertaken.
10. Controleer maandelijks het aantal en de status van global administrators binnen de Azure-omgeving en verwijder inactieve accounts.
11. Voer periodiek uitwijktesten uit binnen de cloudomgeving om de werking van herstelprocedures, back-ups en toegang te verifiëren.
12. Roteer het wachtwoord van het KeePass bestand bij personele wijzigingen van personen die daar toegang tot hebben gehad. Maak gebruik van een wachtwoordkluis waarbij wachtwoorden in teamverband gedeeld kunnen worden inclusief uitgebreide logging mogelijkheden ten behoeve van het realiseren van onweerlegbaarheid.
13. Zet de open SSH poort dicht of tref compenserende maatregelen, zoals IP-allowlisting, VPN[33], SSH-sleutels, blokkeren van brute kracht aanvallen en additionele monitoring.

[33] Uitbreiding van een computernetwerk over een openbaar netwerk. Via die uitbreiding kunnen gebruikers vanaf elke plek veilig gegevens delen met het computernetwerk. Voor de gebruikers is het alsof ze rechtstreeks op het netwerk zijn aangesloten. De veilige verbinding valt te omschrijven als een tunnel en wordt afgekort VPN genoemd.

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

2.5 Aanbevelingen voor de gemeenteraad

De gemeenteraad heeft een belangrijke rol ten aanzien van de informatieveiligheid binnen Steenwijkerland. De VNG[34] 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 Steenwijkerland 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 Steenwijkerland en haar inwoners en ondernemers.

Neem kennis van de beschikbare hulpmiddelen[35][36] zodat u (beter) in staat bent om de juiste accenten te leggen en het gesprek inhoudelijk aan kunt gaan met het college.

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.

De Cybersecurity Raad[37] 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 toeneemt. Wees uzelf daarvan bewust bij de totstandkoming van de begroting.

[34] https://vng.nl/artikelen/raadgever-digitale-veiligheid
[35] https://vng.nl/sites/default/files/2025-04/raadsleden-en-informatiebeveiliging.pdf
[36] https://vng.nl/sites/default/files/2023-04/checklist-raadsleden-digitale-veiligheid.pdf
[37] 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

3 Beantwoording van de onderzoeksvragen

1. Algemene informatieveiligheid

Heeft de gemeente Steenwijkerland op het gebied van informatieveiligheid de risico's voldoende in kaart gebracht en op basis daarvan beleid geformuleerd?

Er is deels zicht op risico's en Steenwijkerland acteert daarop, maar kan dit onvoldoende aantonen. Dit blijkt onder andere uit de afwezigheid van vastgesteld beleid ten aanzien van risicomanagement, een centraal risicoregister, vastgestelde risicobereidheid, integratie van risicomanagement in processen en periodieke besluitvorming en verantwoording over risico's aangaande informatiebeveiliging.

Hoe wordt de informatieveiligheid binnen de gemeente Steenwijkerland georganiseerd en welke maatregelen zijn er genomen om de veiligheid van gevoelige gegevens te waarborgen?

Steenwijkerland heeft een CISO die zich primair richt op het continu verbeteren van de algehele informatiebeveiliging van Steenwijkerland. De taken, verantwoordelijkheden en bevoegdheden van de CISO zijn formeel vastgelegd, voor de ISO en TISO rollen is dit niet het geval. De CISO werkt nauw samen met de Privacy Officer (PO) en Functionaris Gegevensbescherming (FG).

De portefeuille informatieveiligheid is bestuurlijk belegd, wordt regelmatig besproken en er is een Security board. Teamleiders hebben verantwoordelijkheden voor informatieveiligheid waar ze op gewezen worden.

Steenwijkerland neemt maatregelen om veilig gedrag en bewustzijn bij de verschillende medewerkers te bewerkstelligen. Technische maatregelen worden geïmplementeerd zonder afbreuk aan de gebruiksvriendelijkheid van de IT-dienstverlening. Ontbrekende maatregelen, zoals rond detectie en respons, worden geïdentificeerd en geïmplementeerd. Op organisatorisch vlak zijn ook maatregelen genomen maar kan de aantoonbaarheid verder worden verbeterd.

Op welke wijze wordt de gemeenteraad geïnformeerd over de risico's en maatregelen? En wat is wenselijk in het delen van dergelijke informatie?

De interactie met de gemeenteraad ten aanzien van informatiebeveiliging is reactief en beperkt tot de verplichte jaarlijkse ENSIA-verantwoording waarbij deze ter kennisname worden aangedragen. Het is belangrijk om de raad regelmatig op de hoogte te houden van de status ten aanzien van informatiebeveiliging, zonder daarbij details te delen die een negatief effect op de informatiebeveiliging van Steenwijkerland kunnen hebben.

In hoeverre voldoet de informatieveiligheid van de gemeente Steenwijkerland aan de relevante wet- en regelgeving, zoals de Algemene verordening gegevensbescherming (AVG) en de Wet beveiliging netwerk- en informatiesystemen (Wbni)?

Steenwijkerland voldoet onvoldoende aantoonbaar aan de Baseline Informatiebeveiliging Overheid (BIO) 2 en Cyberbeveiligingswet (NIS2). Er is vastgesteld dat Steenwijkerland de juiste intenties heeft en adequaat handelt, het schort echter aan borging in processen, procedures en onderbouwende documentatie, waardoor het lastig of onmogelijk is om dit aan

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

te kunnen tonen. Met name het risicobeheer binnen Steenwijkerland behoeft aandacht, mede omdat dit naast de BIO een expliciete eis is vanuit de aanstaande Cyberbeveiligingswet.

Welke procedures en beleidsmaatregelen zijn er voor het beheer van gebruiksrechten en toegangscontrole tot kritieke informatiesystemen?

Het uitgangspunt is dat alles achter Single-Sign-On (SSO) moet zitten via Azure. Ook moet alle authenticatie met Multi-Factor plaatsvinden. Op de logins zit conditionele toegang om bijvoorbeeld alleen verkeer vanuit Europa toe te staan. Legacy apps kunnen alleen worden benaderd via de VPN, waarvan de client alleen op beheerde apparaten beschikbaar is.

Het wachtwoordbeleid is geactualiseerd zodat wachtwoorden niet meer verlopen maar gewijzigd moeten worden bij mogelijk uitlekken. Echter is de monitoring op lekken van wachtwoorden onvoldoende ingericht. Beheerders gebruiken aparte admin accounts met Just-In-Time Access waarvan acties gelogd worden.

Het Security dashboard in 365 wordt door beheerders gebruikt om situaties en problemen met accounts en configuraties te detecteren.

De teamleiders zijn de enige die de autorisaties mogen aanvragen, dat gebeurt aantoonbaar en met expliciete ondertekening. Functioneel Beheer stuurt twee keer per jaar voor de kritische applicaties lijsten met gebruikers om te controleren naar de Teamleiders.

Detectie is niet volledig ingericht, maar is een lopend project om dit aan te besteden en te implementeren.

2. Beveiliging van kritische systemen

Welke informatiesystemen worden als ‘kritisch’ beschouwd voor de werking van de gemeente, en hoe wordt de beveiliging van deze systemen gewaarborgd?

Steenwijkerland heeft een beeld van haar kritieke informatiesystemen. Tijdens gesprekken is naar voren gekomen dat Steenwijkerland voor enkele dagen haar werkzaamheden zonder cloud infrastructuur zou kunnen uitvoeren (hoewel ernstige impact op doorlooptijden van individuele acties). Belangrijkste afhankelijkheden zijn Entra ID en de Azure tenant, gezien de uitval van deze diensten ertoe zal leiden dat de werkplekken van Steenwijkerland gedeeltelijk danwel geheel niet meer werken. Deze omgevingen worden beschermd met verschillende monitoringsmaatregelen en strak ingericht identity and access management.

Daarnaast is de RaaS server van belang, gezien uitval van deze omgeving betekent dat veel werkzaamheden, zoals paspoortaanvragen etc., niet meer uitgevoerd kunnen worden. Deze omgeving wordt echter door een derde partij beheerd en kan alleen op infra vlak door Steenwijkerland afgeschermd worden. Het is belangrijk om hier goede afspraken over te maken met de leverancier aangezien deze ook een verouderd besturingssysteem heeft.

Toegang vindt plaats via beheerde werkplekken en -accounts, met MFA. De werkplekken worden actief op compliance gemonitord en anders wordt de toegang afgesloten. Medewerkers worden bewust(er) gemaakt door periodieke e-learning en er vinden regelmatig autorisatiecontroles en penetratietesten plaats.

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

Welke risico's worden er gelopen als de kritische systemen door ongeautoriseerde beïnvloeding van buitenaf uitvallen?

Steenwijkerland heeft dit niet expliciet gemaakt aan de hand van risico-analyses. Dit is wel geoefend in de vorige crisis-simulatie, waarbij de uitkomst was dat erg naar de Teamleider I&A werd gekeken om de systemen te herstellen. Binnen de IT zijn er uitwijkplannen voor de lokale applicaties die jaarlijks getest worden, bij de cloud-applicaties wordt daarbij geleund op de door de leveranciers genomen maatregelen. Bij de oefening bleek dat er binnen Steenwijkerland beperkt plannen op procesniveau zijn om de kritische processen doorgang te laten vinden.

Onderling met andere gemeentes wordt momenteel gekeken naar welke processen als kritisch aangemerkt zouden moeten worden (daar zou nagenoeg volledige overeenkomst in moeten zijn). Op basis hiervan kunnen dan bedrijfscontinuïteitsplannen opgesteld gaan worden.

Er is contractueel met Microsoft afgesproken dat bij uitval van het primaire datacenter er ook een achtervang is geregeld. Alle kernonderdelen waaronder Exchange en Entra ID zijn geo-redundant ingericht: data en directory-informatie worden continu gerepliceerd tussen datacenters binnen de Europese Unie.

Wat zijn de kwetsbaarheden in de bestaande informatiesystemen die het mogelijk maken om in te breken of ongeautoriseerde toegang te verkrijgen?

Steenwijkerland voert applicatie-patchbeheer grotendeels geautomatiseerd uit met behulp van verschillende tools. Windows en Office applicaties worden automatisch bijgewerkt met Intune en Qualys PM. Overige applicaties worden waar mogelijk via Qualys Patch Management, Intune of Patch my pc geautomatiseerd of, indien dit niet mogelijk is, handmatig bijgewerkt volgens het wijzigingsproces in Topdesk. Applicaties worden wekelijks gepatched en kritieke kwetsbaarheden worden onmiddelijk geadresseerd buiten deze cyclus om, bijvoorbeeld naar aanleiding van berichtgeving van de Informatiebeveiligingsdienst. De patchstatus wordt continu bewaakt via dashboards in Qualys en Intune en de beheerders ontvangen wekelijks rapportages hiervan. De CISO wordt hier maandelijks over geïnformeerd.

Ondanks de uitgebreide awareness-programma's blijft een kwetsbaarheid dat medewerkers van Steenwijkerland inherent erg behulpzaam zijn waardoor ze mogelijk eerder geneigd zijn een deur open te houden of informatie te verstrekken over de telefoon terwijl dat niet de bedoeling is. Document labeling/rubricering (classificatie) kan helpen om medewerkers hier alerter op te laten zijn. Een aanvaller met fysieke toegang zal ook andere kwetsbaarheden moeten uitbuiten om zijn toegang tot informatie te escaleren.

Hoewel er geen concrete indicaties zijn, bestaat ook het risico dat door afhankelijkheid van grote Amerikaanse IT-providers een buitenlandse overheid via gerechtelijke weg toegang tot gegevens en applicaties vereist.

Er is een verbinding (site-to-site) tussen het lokale datacenter in Steenwijk en de Azure tenant. Indien een aanvaller toegang weet te krijgen tot het lokale datacenter dan kan hij ook toegang krijgen tot Azure. Daarnaast zou een kwaadwillende toegang kunnen krijgen tot de Entra ID omgeving met alle consequenties van dien. Ook vindt er reactieve monitoring in de Azure omgeving plaats, waardoor ongeautoriseerde toegang tot de Azure tenant niet direct zichtbaar is.

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

Hoewel de basisbeveiliging goed op orde is ontbreekt het momenteel aan monitoring- en detectiecapaciteiten om onverhoopt succesvolle aanvallen of kwetsbaarheden tijdig te detecteren en op te reageren. Hiervoor loopt reeds een implementatietraject.

Hoe worden de systemen gemonitord op potentiële veiligheidsincidenten en welke mechanismen zijn er voor incidentdetectie en -respons?

Steenwijkerland heeft geen formeel gedocumenteerd proces voor auditlogging. In de praktijk vindt er continu montoring plaats tijdens kantooruren. Steenwijkerland is, zoals eerder genoemd, aan het verkennen hoe zij pro-actieve monitoring kan inrichten met SIEM[38]/SOC[39] oplossingen.

3. Risicoanalyse en dreigingen

Welke interne en externe dreigingen worden momenteel geanalyseerd en beheerd om inbreuken in informatiesystemen te voorkomen?

Steenwijkerland heeft dit niet expliciet inzichtelijk gemaakt. Steenwijkerland voert jaarlijks interne audits en controles uit, waarbij impliciet bepaalde risico's geanalyseerd en beheerst worden. In de jaarplannen komen de activiteiten met de hoogste prioriteit thematisch aan de orde. De directe relatie met risico's ontbreekt.

In hoeverre worden risico's zoals social engineering, phishing-aanvallen, malware-infecties en andere vormen van cyberaanvallen in kaart gebracht en tegengegaan?

Steenwijkerland voert interne audits en controles uit en heeft technische maatregelen getroffen om cyberaanvallen tegen te gaan: firewalls, extended endpoint protection & response (XDR)[40], e-mail beveiligingsstandaarden, beheren van apparaten, Multi-factor authenticatie[41] (MFA), harde schijf versleuteling, applicatie allowlisting[42], geautomatiseerd patchmanagement, enzovoort. Aanvullend daarop wordt Steenwijkerland constant gevoed met actuele dreigingsinformatie door de IBD. Bijvoorbeeld over nieuwe ontwikkelingen en trends in het dreigingslandschap en informatie over risico's in het externe aanvalsoppervlak (Darktrace). Gezamenlijk geeft dit een goed beeld van het daadwerkelijke dreigingsbeeld en stelt dit Steenwijkerland in staat om daar adequaat op te reageren.

[38] 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.
[39] Afdeling, team of dienst dat digitale systemen en/of identiteiten controleert en/of bewaakt en soms ook afhandelt.
[40] Extended Detection and Response. Een detectie- en responsplatform dat verschillende technieken combineert voor een betere verdediging.
[41] Een manier van identiteit vaststellen waarvoor meerdere onafhankelijke bewijzen van identiteit zijn vereist.
[42] Actie waarmee men in een lijst vastlegt welke applicaties, gebruikers en acties men toestaat. Alles wat niet op de lijst staat wordt automatisch geblokkeerd. Het tegenovergestelde is blacklisting.

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. Testen van infiltratie

Is er een periodieke penetratietest of red-teaming uitgevoerd om de kwetsbaarheden van de informatiesystemen te identificeren en de effectiviteit van de beveiliging te testen?

Steenwijkerland heeft de afgelopen jaren door onafhankelijke gespecialiseerde partijen penetratietesten laten uitvoeren. De reikwijdte van deze testen was verschillend en er is aangetoond dat de bevindingen geadresseerd zijn. Het centraal vastleggen van risico's en de behandeling daarvan is een aandachtspunt.

Welke incidenten of beveiligingslekken zijn er in de afgelopen jaren geconstateerd, en hoe zijn deze opgelost? Hoe wordt er bijvoorbeeld bij een datalek gecommuniceerd met de mogelijk betrokkenen binnen en buiten de gemeentehuizen?

In 2024 zijn 19 datalekken geregistreerd waarvan er 3 aan de Autoriteit Persoonsgegevens (AP) zijn gemeld. Voor het afhandelen van datalekken is een procedure vastgesteld waarbij de betrokkenen en eventueel andere stakeholders geïnformeerd worden (indien nodig/wenselijk). De voornaamste oorzaak van de datalekken was menselijk handelen. Het is van belang om op te merken dat dit overzicht onvolledig is omdat het niet de technische incidenten bevat. Incidenten zoals pogingen tot malware-infecties, brute forcing, password spraying, phishing e-mails, etc. komen niet in dit overzicht aan de orde. Deze technische incidenten zijn geregistreerd in Topdesk en het Microsoft portaal.

5. Opleiding en bewustwording van personeel

Hoe worden medewerkers van de gemeenten opgeleid in het herkennen van beveiligingsrisico's, zoals phishing en social engineering-aanvallen?

Alle medewerkers krijgen wekelijks mailtjes van Sir Askalot om de bewustwording ten aanzien van informatiebeveiliging op niveau te krijgen en te houden. Onderwerpen zoals social engineering komen daarin aan de orde. Aanvullend daarop vindt er communicatie via intranet plaats en worden steekproeven gedaan, zoals bijvoorbeeld controles op opgeruimde werkplekken en vergrendelde werkplekken (clear screen & clean desk). Ten aanzien van veilig gedrag zijn geen concrete meetbare doelstellingen geformuleerd (KPI's/KRI's[43]) en de effectiviteit van inspanningen en investeringen wordt niet periodiek vastgesteld.

Wat is de frequentie en effectiviteit van de trainingen die medewerkers ontvangen met betrekking tot informatieveiligheid?

Medewerkers ontvangen buiten de verplichte training bij indiensttreding geen (specifieke) trainingen ten aanzien van informatiebeveiliging.

[43] Key Performance Indicator / Key Risk Indicator

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

6. Beveiliging van gegevens en privacy

Hoe wordt de privacy van persoonsgegevens gewaarborgd binnen de informatiesystemen van de gemeenten?

De privacy organisatie van Steenwijkerland is gedegen ingericht en functioneert conform het drie-lijnenmodel[44]. De i-adviseurs vervullen in de eerste lijn een signalerende rol als 'voelsprieten' binnen Steenwijkerland, terwijl de privacy officers in de tweede lijn zorgen voor de uitvoering van privacytaken en de afstemming met relevante stakeholders. De FG houdt vanuit de derde lijn toezicht en wordt actief betrokken bij incidenten en DPIA's. De samenwerking tussen de FG, de lijnorganisatie, de CISO en andere betrokken partijen verloopt constructief. Het verwerkingsregister is volledig en wordt actueel gehouden door wijzigingen in processen en verwerkingen tijdig te verwerken.

Hoewel de inrichting en samenwerking goed op orde zijn, zijn er enkele punten die verdere professionalisering kunnen bevorderen. De registratie en opvolging van privacy-incidenten verlopen ad-hoc, waardoor de traceerbaarheid en audit trail beperkt zijn. Daarnaast is de onafhankelijkheid en positionering van de FG niet formeel vastgelegd in een charter of mandaatdocument, hetgeen risico's kan opleveren voor de structurele borging van diens toezichtsrol. Tot slot is tijdens het onderzoek niet duidelijk geworden op welke manier medewerkers worden geïnformeerd over de omgang met hun persoonsgegevens gedurende het dienstverband en over eventuele monitoringactiviteiten die plaatsvinden ten behoeve van informatiebeveiliging.

Zijn er gegevensversleuteling en veilige communicatiekanalen voor het uitwisselen van gevoelige informatie?

De opslag van de beheerde apparatuur is versleuteld en het technisch beheer verloopt via versleutelde verbindingen. VPN wordt gebruikt voor toegang tot legacy systemen en bestanden mogen niet gedownload worden buiten de beheerde omgeving/werkplek. Medewerkers hebben een oplossing voor veilig mailen voorhanden om veilig met derden informatie uit te kunnen wisselen.

7. Incidentmanagement en crisiscommunicatie

Hoe is het incident-managementsproces ingericht voor het geval van een datalek of cyberaanval?

Steenwijkerland heeft een generiek proces ingericht voor het afhandelen van incidenten en datalekken. Er zijn geen incident response plannen voor specifieke cyberdreigingen, zoals bijvoorbeeld ransomware of Distributed Denial of Service (DDoS) aanvallen. Steenwijkerland heeft geen 24x7 beschikbaarheid georganiseerd voor het afhandelen van incidenten en geen retainer met een gespecialiseerde partij afgesloten. Er is echter overeenstemming over het benaderen van een dergelijke partij ten tijde van een cybercrisis. Steenwijkerland kan 24x7 contact opnemen met de Informatiebeveiligingsdienst (IBD), maar die rukken niet uit om op locatie Steenwijkerland te ondersteunen bij de afhandeling van incidenten of het herstel

[44] https://www.rijksfinancien.nl/sites/default/files/hafir/extra-info/Uiteenzetting-Three-Lines-Model-IAA.pdf

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

daarvan. Technisch heeft Steenwijkerland uitwijk ingericht in het gemeentehuis van Meppel en test dit regelmatig. Het aangeleverde uitwijkplan is informeel en sterk verouderd.

Welke procedures zijn er voor crisiscommunicatie en hoe snel kunnen kwetsbaarheden door de gemeente worden geadresseerd?

Er zijn geen crisisplan en/of -procedures aangeleverd. In 2024 heeft er een crisisoefening met een cyber component plaatsgevonden. De bevindingen en opvolging daarvan zijn onbekend.

Het adresseren van kwetsbaarheden waarvoor Steenwijkerland zelf verantwoordelijk is, vindt in de basis uitsluitend tijdens kantooruren plaats. Indien daar aanleiding voor is kan Steenwijkerland dit buiten kantoortijden oppakken, bijvoorbeeld wanneer een ernstige kwetsbaarheid is ontdekt. Voor kwetsbaarheden waarvoor externe partijen verantwoordelijk zijn voor het oplossen daarvan gelden de overeengekomen contractuele afspraken.

8. Kosten beveiligingsmaatregelen

Welke eenmalige en structurele kosten worden er gemaakt voor het beheren van risico's op gebied van informatieveiligheid en bescherming kritische processen en hoe verhouden zich die onderling en tot soortgelijke gemeenten?

Dit is op basis van de aangeleverde informatie en gesprekken niet vast te stellen. De Cybersecurity Raad[45] 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 meer wettelijke eisen in werking getreden.

Hoofdvraag

Hoe wordt de informatieveiligheid binnen de gemeenten georganiseerd, welke maatregelen zijn er genomen om de veiligheid van gevoelige gegevens te waarborgen, en in hoeverre zijn de kritische processen van de gemeenten beschermd tegen infiltratie en ongeautoriseerde toegang?

Steenwijkerland beschikt over een goed doordachte en verankerde strategie ten aanzien van informatiebeveiliging die breed wordt ondersteund door medewerkers en management. Er is sprake van een volwassen bewustzijnsniveau op het gebied van informatieveiligheid, waarbij medewerkers zich verantwoordelijk opstellen en open staan voor feedback en verbetering.

De belangrijkste risico's bevinden zich op het terrein van de cloudafhankelijkheid (vendor lock-in), het beheer van het lokale datacenter en de uitwijklocatie in Meppel, waar aanvullende borging en afspraken gewenst zijn. Deze risico's doen echter geen afbreuk aan de algemene volwassenheid van Steenwijkerland op het gebied van informatiebeveiliging.

De geïdentificeerde aanbevelingen dienen vooral ter verdere versterking en professionalisering van bestaande processen. Zij vormen daarmee geen indicatie van ondermaatse prestaties, maar juist van een organisatie die continu werkt aan verbetering en groei binnen een al hoog volwassenheidsniveau van informatieveiligheid.

[45] 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

DMC GROUP
SECURITY MANAGEMENT

A Aangeleverde informatie

0 CIS_Controls met verdeling per collega.xlsx
06a Vastgesteld_Besluitenlijst_Concern_Managementteam_15_november_2018.pdf
1.1a Intune devices.png
1.1b Nutanix VM Steenwijk.png
1.1c Nutanis VM Meppel.png
1.2a Laptop Compliancy.png
1.2b Mobile Compliancy.png
10.1 toelichting + screenshots.docx
10.1 Windows EDR.png
10.2 toelichting + screenshots.docx
10.3 Removable disk access.png
12.1.docx
14.1 -14.8.pdf
14.1 Memo DT 19 januari 2023 - bewustwordingsprogramma informatiebeveiliging en privacy.pdf
14.1 Memo DT 21 juli 2025 (Sir Askalot).pdf
14.1 memo TLO 23 april 2024 (Sir Askalot) .pdf
14.1 Memo TLO 31 oktober 2023 (Sir Askalot)1.pdf
14.2 Memo phisingtest 2024.pdf
14.3 wachtwoordbeleid 2025.pdf
14.4 clean-desk 23 juni 2025.pdf
14.4 Clean-desk ronde 6 mei 2024.pdf
14.6 hetkennen beveiligingsincidenten.pdf
17.1 incidentafhandelingsproces.pdf
17.1 Processchema datalekken (1).pdf
17.2 shortlist contactinformatie beveiligingsincidenten .pdf
17.3 melden datalek en beveiligingsincident op intranetpagina Spin.pdf
17.3 Memo overzicht datalekken 2023.pdf
17.3 Memo overzicht datalekken jaar 2024 TL-DT .pdf
17.3 Processchema datalekken.pdf
2.2 toelichting + screenshots.docx
2.2a Windows apps intune.png
2.2b Patch-My-PC.png
2.3 Blocked Sofware Executable.png
2.3 toelichting + screenshots.docx
20250108_Formulier voor controle autorisatie.docx
20250708 Formulier voor autorisatie controle Motion Pro.pdf
23-772 - Rapport Gemeente Steenwijkerland - Pentest rapport - d.d. 07.12.2023.pdf
24-167- Rapport Gemeente Steenwijkerland - Penetratietest - d.d. 13.03.2024.pdf
24198 - Montanaro - Management Samenvatting - 2025-01-16.pdf
24198 - Montanaro - Rapportage - 2025-01-16.pdf
3.6a disk-encryption.png
3.6b disk-encryption.png

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

3.6c Bitlocker-key lookup.png
312024020.25.035. ENSIA Steenwijkerland v3.pdf
4.1a Enrollment (Status Page) Windows.png
4.1b Enrollment iOS.png
4.1c Enrollment Android.png
4.2 toelichting + screenshots.docx
4.3a Windows Lock.png
4.4 toelichting + screenshots.docx
4.4 Windows Server Firewall.png
4.5a Firewall and encryption.png
4.5b Firewall and encryption.png
4.6 Intune HTTPS.png
4.6 toelichting + screenshots.docx
4.7 toelichting + screenshots.docx
4.7 Windows LAPS Policy.png
4a. Wachtwoordbeleid DT voorstel.pdf
5.1a AD users.png
5.1b Azure users.png
5.2 Toelichting + screenshots.docx
5.3a Disabled users Active Directory.png
5.3b Deleted users Azure.png
5.4 toelichting + screenshots.docx
5.4a PIMS (JIT).png
5.4b MFA Admin.png
6.3 MFA.png
6.4 VPN config.png
6.5a PIMS (JIT).png
6.5b MFA Admin.png
7.1 toelichting + screenshots.docx
7.2 toelichting + screenshots.docx
7.3 toelichting + screenshots.docx
7.4 toelichting + screenshots.docx
8.2 toelichting + screenshots.docx
8.2a Audit Logs Entra.png
8.3 toelichting + screenshots.docx
9.1a Chrome Browser.png
9.1b Firefox Browser.png
9.2 Microsoft Indicators.png
9.2 toelichting + screenshots.docx
advies Uitkomst hercontrole WPG .pdf
advies addendum privacy en informtiebeveiligingsbeleid B.01 DigiD.pdf
Advies CMT DSP - i-Navigator.docx
advies concept collegeverklaring 2022.pdf
advies ENSIA verantwoording 2023.pdf
advies Implementatieplan NIS2 (2).pdf

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

advies Procdure rechten van betrokkenen (1).pdf
Agenda Security-board 11 april 2024 (2).pdf
Agenda Security-board 30 oktober 2024.pdf
Agenda Security-board 7 december 2023 - Kopie.pdf
Agenda Security-board 8 mei 2023.pdf
AI en Algoritmebeleid Steenwijkerland. (1).pdf
All-Intune-Apps.xlsx
alle leveranciers ict.xlsx
Applicatielijst 18-09-2025.xlsx
assurance.pdf
Audit- en controleplan 2024 (1).pdf
Audit- en controleplan 2025.pdf
Auditplan 2023.pdf
Autorisatiecontrole Key2Burgerzaken 20250724 verwerkt.pdf
Autorisatiecontrole Key2GBA-V 20250724 verwerkt.pdf
Autorisatiematrix en Toegangsbeleid.pdf
Autorisaties Centric Betalen 08-07-2025.docx
Autorisaties Motion 10-07-2025 MW.xlsx
Autorisaties Motion Pro 08-07-2025 MW.docx
Back-up en recovery Beleid V1.0.pdf
BackupDoc.docx
Beheerplan DSP i-Navigator gemeente Steenwijkerland versie 1.0.pdf
Beknopt verslag security board 11 april 2024.pdf
Beknopt verslag security board 17 okt 2022.pdf
Beknopt verslag security board 7 december 2023.pdf
Beknopt verslag security board 8 mei 2023.pdf
Beleid logische toegangsbeveiliging.pdf
Beleid Privacy, informatiebeveiliging en -beheer 2025-2028.pdf
Beleid privacy, informatiebeveiliging en informatiebeheer 2021-2024.pdf
Besluit beleid Privacy, informatiebeveiliging en beheer 2021-20241.pdf
Besluit beleid Privacy, informatiebeveiliging en beheer 2025-2028.pdf
bevindingen_en_opvolging.docx
Bijlage 1 DigiD Belastingloket.pdf
Bijlage 1 DigiD burgerzaken.pdf
Bijlage 1 DigiD zaaksysteem.pdf
bijlage 1 eDiensten burgerzaken.pdf
bijlage 1 Frontoffice.pdf
bijlage 1 Zaaksysteem.pdf
bijlage 2 Suwinet.pdf
BIO2-Gap-analyse-versie-1.2 (1).xlsx
Clean-desk ronde 6 mei 2024 - Kopie.pdf
Collegeverklaring Ensia 2024.pdf
Collegeverklaring.pdf
Controle autorisatie K2Betalen Q2 2025-ondertekend.pdf
darktrace.png

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

Digitale vernietigingsprocedure.pdf
Document.docx
DT advies concept- Collegeverklaring Ensia 2024.pdf
DT advies jaarverslag 2024, beleid 2025-2028, jaarplan 2025 (1).pdf
DT advies OT bij de gemeente Steenwijkerland..pdf
DT advies PVA ENSIA 2023.pdf
DT advies PVA ENSIA 2024.pdf
DT Advies SIEM SOC en IR.pdf
DT pva ENSIA 2025.pdf
DT-advies gebruik apps op mobiele devices (tiktok) - Kopie.pdf
DT-advies gebruik data t.b.v. Monitor Sociaal Domein.pdf
DT-advies jaarverslag-auditrapportage 2022 en jaarplan 2023.pdf
DT-advies jaarverslag-auditrapportage 2023 en jaarplan 2024.pdf
DT-advies opslag informatie bij de Huisvesting Oekraine.pdf
Encryptiebeleid gemeente Steenwijkerland 1.0.pdf
Formulier voor controle autorisatie Motion getekend.pdf
Gebruikers Key2Financien 20250710.pdf
GemeenteSteenwijkerland_backup_health_weekly_2025-09-15-06-09-26.pdf
GemeenteSteenwijkerland_exchange_backup_health_weekly_2025-09-15-06-08-04.pdf
GemeenteSteenwijkerland_sharepoint_backup_health_weekly_2025-09-15-06-10-18.pdf
Jaarplan 2025.pdf
Jaarplan privacy informatiebeveiliging en informatiebeheer 2023.pdf
Jaarverslag en auditrapportage privacy informatiebeveiliging en informatiebeheer 2023.pdf
Jaarverslag en auditrapportage privacy informatiebeveiliging en informatiebeheer 2024.pdf
Maatregelen_nieuw.docx
Maatregelen.docx
Mail RDW Station.png
Marjanne van den Berg_202508121047.pdf
Memo advies invoering NIS2.pdf
Memo DT 11 november 2024 (Sir Askalot).pdf
Memo DT 19 januari 2023 - bewustwordingsprogramma informatiebeveiliging en privacy.pdf
Memo DT 21 juli 2025 (Sir Askalot).pdf
Memo DT 23 maart 2023 - bewustwordingsprogramma informatiebeveiliging en privacy.pdf
Memo DT 5 juni 2024.pdf
Memo overzicht datalekken jaar 2024 TL-DT (2).pdf
Ondertekend voorstel.pdf
Oracle_Rman_backup_dagelijks_verslag.pdf
OV10 (pdca).pdf
Overige vragen uit mail DMC met verdeling.docx
Patchmanagementbeleid V1.0.pdf
Procedure bijhouden logging.pdf
Procedure indienst functiewijziging en uitdienst.pdf
programma studiedag 11 oktober 2024.pdf
Required-Intune-Apps.xlsx
Restore van VM uit Rubrik_032024.docx

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

Rubrik_backup_dagelijks_verslag.pdf
Steenwijkerland_Rapportage over BAG, BGT en BRO 2024_2024 ENSIA.pdf
Uittreksel BRP ENSIA 2024.pdf
uittreksel BRP.pdf
Uittreksel Reisdocumenten ENSIA 2024.pdf
uittreksel Reisdocumenten.pdf
Uitwijkplan.pdf
Uitwijkverslag ondertekend CISO.pdf
Verantwoordingsrapportage basisregistraties (1).pdf
Verklaring inzake Bijlagen DigiD.pdf
VIC _ All users.xlsx
VIC _ Groepen en functionaliteit.xlsx
VIC _ Groepen en gebruikers.xlsx
Wachtwoordbeleid 2025 V21.docx
Whitepaper_DSP_als_risicoclassificatie_V3._DEF.pdf
ww.docx

—

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

B Interviews

- Beheerder BGT
- Gebouwbeheer
- Gebouwbeheer
- Netwerkbeheer
- Technisch beheer security
- M365, Entra
- Medewerker
- Coördinator technisch beheer
- Senior I-adviseur
- Adviseur facilitaire dienstverlening
- Privacy Officer
- CISO
- Teamleider I&A
- Gemeentesecretaris
- Coördinator HR
- BRP-specialist
- Wethouder bedrijfsvoering

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