Gemeente Hardenberg

Rekenkamercommissie

PBLQ

De bescherming en weerbaarheid van de digitale systemen van de gemeente Hardenberg

onderzoeksrapportage inclusief conclusies en aanbevelingen

13 januari 2022

PBLQ
verbinders in de informatiesamenleving

Inhoudsopgave

1. Inleiding

1.1 Aanleiding

Naar aanleiding van berichten in de media heeft de Rekenkamercommissie van de gemeente Hardenberg besloten een onderzoek te doen naar de digitale veiligheid. Gemeenten, onderwijsinstellingen en andere organisaties in het publiek domein zijn (steeds) meer doelwit van cybercriminaliteit. Zo zijn recentelijk een aantal gemeenten, maar bijvoorbeeld ook de Universiteit van Maastricht, getroffen door gijzelsoftware. Dit kan organisaties veel geld kosten; de dienstverlening loopt gevaar, het is slecht voor het imago en het kan ten koste gaan van het vertrouwen van bijvoorbeeld inwoners in de organisatie. Er is organisaties daarom veel aan gelegen de informatieveiligheid in het algemeen, maar zeker voor persoonsgegevens, goed op orde te hebben.

Ook bij gemeenten is de aandacht voor de beveiliging van informatie de laatste jaren sterk toegenomen. Gemeenten werken steeds ‘digitaler’ en wisselen intern, met andere organisaties (in een keten) en met burgers en ondernemingen gegevens uit. Het is belangrijk dat gemeenten zichzelf beschermen, omdat zij met persoonsgegevens en andere gevoelige informatie werken. Kortom, ambtelijke en bestuurlijke aandacht voor de informatiebeveiliging is noodzakelijk.

Maar 100% veilig bestaat niet. Cybercriminelen worden steeds slimmer en de techniek geavanceerder. Er moet dus rekening worden gehouden met cybercriminaliteit en beveiligingsincidenten. Gemeenten moeten weerbaarder worden. Een digitaal weerbare gemeente kan potentiële incidenten vroegtijdig signaleren en de gevolgen ervan beperken, omdat de juiste maatregelen zijn getroffen (Bron: Website Informatiebeveiligingsdienst Gemeenten).

De Rekenkamercommissie van Hardenberg heeft daarom onderzoek gedaan naar de bescherming en weerbaarheid van de digitale systemen van de gemeente Hardenberg en het beveiligingsbewustzijn van de medewerkers, om zo mogelijk cyberaanvallen buiten de deur te kunnen houden.

1.2 Opdrachtformulering

Aan de basis van het onderzoek staat de volgende centrale onderzoeksvraag:

Centrale onderzoeksvraag

Hoe goed zijn de persoonsgegevens en andere informatie van de gemeente Hardenberg beschermd tegen cybercriminaliteit én hoe is de gemeente voorbereid op een mogelijk beveiligingsincident?

Deze centrale onderzoeksvraag is uitgewerkt in de volgende deelvragen.

Deelvragen

1. Hoe weerbaar zijn de digitale systemen van de gemeente Hardenberg tegen cybercriminaliteit?
2. Hoe beveiligingsbewust zijn de medewerkers van de gemeente Hardenberg als het gaat om persoonsgegevens en andere informatie?
3. Hoe is de gemeente voorbereid in het geval van mogelijke incidenten?
4. Waar liggen de grootste risico’s en hoe kan de gemeente Hardenberg hierin verbeteringen aanbrengen?

5. Welke controle- en sturingsmogelijkheden heeft de gemeenteraad bij informatiebeveiliging en worden deze ook gebruikt?

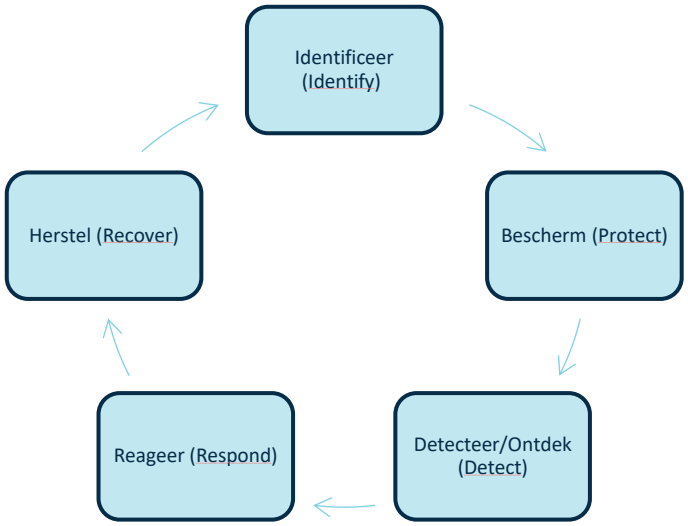
1.3 Referentiekader

Allereerst staan we stil bij het begrip ‘cybercriminaliteit’ dat in de hoofdvraag wordt gebruikt. Onder cybercriminaliteit wordt verstaan dat doelbewust – van buiten of binnenuit de organisatie – inbreuk wordt gemaakt op de ICT en op data met als doel om te verstoren, op te lichten, losgeld te verkrijgen of data te stelen. Denk hierbij aan hacks, phishing, DDoS-aanvallen, whatsapp fraude of ransomware.

Wij plaatsen dit begrip in een bredere context, waarbij we in het onderzoek kijken naar informatiebeveiliging. Informatiebeveiliging gaat over de maatregelen en procedures om beschikbaarheid, integriteit en vertrouwelijkheid van informatie te garanderen en in het bijzonder om de continuïteit van de informatie en informatievoorziening te waarborgen en de gevolgen van incidenten tot een acceptabel niveau te beperken. De maatregelen die in het kader van informatiebeveiliging worden genomen zijn bedoeld om te beschermen tegen cybercriminaliteit, maar ook tegen andere bedreigingen zoals menselijke fouten of technisch falen.

Bescherming tegen beveiligingsincidenten gaat niet alleen over de betrouwbaarheid en beveiliging van de informatiesystemen van de gemeente en de (persoons-) gegevens die erin zijn opgeslagen. Digitale weerbaarheid gaat ook over de betrouwbaarheid en continuïteit van de belangrijkste processen van de gemeente, zoals de dienstverlening aan burgers, de interne bedrijfsvoering en het democratische proces. In dit onderzoek wordt gekeken naar de bescherming van persoonsgegevens in de context van de algemene digitale weerbaarheid tegen cybercriminaliteit. Daarbij staan de verschillende activiteiten centraal die de gemeente moet uitvoeren om gegevens te beschermen, maar ook om adequaat te reageren bij een grootschalig incident. Dit is een integrale insteek, juist omdat het niet alleen gaat om het detecteren en het voorkomen van mogelijke incidenten, maar ook over de respons van de gemeente Hardenberg als een incident zich voordoet en hoe je als organisatie daarvan leert.

Dit onderzoek laat zich inspireren door het NIST Framework for Improving Critical Infrastructure Cybersecurity. Dit framework benoemt verschillende functies of kernactiviteiten die cybersecurityrisico’s adresseren.



Het biedt een kader, waarmee de verschillende activiteiten ten behoeve van de weerbaarheid tegen cybercriminaliteit geanalyseerd kunnen worden. Door de kernactiviteiten uit het kader centraal te stellen, wordt inzicht verkregen in de voorbereiding van de gemeente op een incident, hoe het deze kan detecteren en hoe de gemeente erop kan reageren en ervan kan herstellen. Deze benadering sluit daarmee ook aan op de definitie van een digitaal weerbare gemeente, zoals geformuleerd door de Informatiebeveiligingsdienst gemeenten (IBD). Deze insteek heeft als voordeel ten opzichte van een algemeen onderzoek naar informatiebeveiliging, dat het een beeld geeft van de samenhangende maatregelen die de gemeente heeft genomen. Daarnaast wordt er specifiek aandacht geschonken aan het reageren en herstellen, stappen die voor digitale weerbaarheid essentieel zijn.

De gemeenteraad heeft ook een belangrijke rol bij digitale weerbaarheid, deze wordt expliciet meegenomen in dit onderzoek. Door het gemeentelijke beleid voor de bescherming van persoonsgegevens en andere informatie te toetsen op doeltreffendheid, doelmatigheid en rechtmatigheid, geeft de raad invulling aan haar controlerende rol. Vanuit de volksvertegenwoordigende rol is het voor de raad van belang de weerbaarheid tegen cybercriminaliteit te toetsen en daarbij het belang en perspectief van de inwoner mee te nemen en op basis hiervan eventueel nadere kaders te stellen.

1.3.1 Relatie met andere kaders en onderzoeken

De gemeente Hardenberg moet – net als andere Nederlandse gemeenten – aan een aantal kaders voor informatiebeveiliging voldoen. Eén van deze kaders is de Baseline Informatiebeveiliging Overheid (BIO). Ook worden er regelmatig onderzoeken uitgevoerd naar informatiebeveiliging, zoals de jaarlijkse ENSIA (Eenduidige Normatiek Single Information Audit) met betrekking tot basisadministraties, Suwinet en DigiD.[1] Daarnaast kan de gemeente zelf ook opdracht geven voor onderzoek naar informatiebeveiliging, bijvoorbeeld in de vorm van een penetratietest of een volwassenheidsonderzoek. De gemeente heeft een verantwoordelijkheid om te voldoen aan deze kaders en verplichte of eigen onderzoeken uit te voeren om aan te tonen dat er aan deze kaders wordt voldaan.

Dit rekenkameronderzoek heeft niet tot doel om de rol van andere onderzoeken over te nemen of op detailniveau aan te tonen in welke mate de gemeente voldoet aan verplichte kaders. Met behulp van het onderzoek wordt een oordeel gegeven over de digitale weerbaarheid van de gemeente, waarbij de genoemde kaders en onderzoeken een belangrijke rol spelen maar niet op detailniveau getoetst worden of over worden gedaan. Als het gaat om de BIO, richt dit onderzoek zich op de beheersing van informatiebeveiliging door de gemeente op basis van de BIO. Als het gaat om specifieke onderzoeken of audits, richt dit onderzoek zich op welke onderzoeken de gemeente uitvoert, hoe bevindingen worden opgevolgd en welke blinde vlekken er mogelijk zijn ten aanzien van digitale weerbaarheid.

1.4 Normenkader

In onderzoeken van gemeentelijke rekenkamers is het gebruikelijk om vooraf een normenkader in te richten, dat als basis dient voor de beoordeling van de bevindingen. Een dergelijk normenkader is gebaseerd op inzichten uit de relevante literatuur en op ervaringen in andere gemeenten. Het normenkader beschrijft daarmee de ‘ideale situatie’, ofwel wat we verwachten aan te treffen tijdens het onderzoek. Door de bevindingen daaraan te relateren wordt duidelijk welke verschillen er zijn tussen de

[1] De termen BIO en ENSIA worden later in dit rapport in relatie tot het gemeentelijk beleid nog verder toegelicht.

- in dit geval - concrete bevindingen in Hardenberg en de geschetste ideale situatie. Bij dit onderzoek hoort het onderstaande normenkader.

Normenkader

Identificeer (Identify)
De gemeente heeft een duidelijk beleid en uitvoeringskader bij hoe zij omgaat met cybersecurity risico's van/aan systemen, mensen, gegevens, informatie en middelen.
De gemeente heeft de belangrijkste processen, systemen en risico's in beeld.
De gemeente stelt dit risicobeeld periodiek bij op basis van (onder andere) informatie over dreigingen en veranderingen in processen en systemen.
Bescherm (Protect)
De gemeente heeft maatregelen ontwikkeld en geïmplementeerd om te zorgen voor de continuïteit en bescherming van kritische processen en dienstverlening.
Medewerkers werken volgens de maatregelen en zijn bewust van eigen handelen en verantwoordelijkheid.
Detecteer/ Ontdek (Detect)
De gemeente heeft maatregelen ontwikkeld en geïmplementeerd om cybersecurity incidenten te detecteren.
Er is een procedure voor het melden van incidenten en medewerkers kennen en gebruiken deze procedure.
Er is een escalatieprocedure richting de directie, college en gemeenteraad.
Reageer (Respond)
De gemeente heeft maatregelen/acties/processen geïmplementeerd om actie te (kunnen) ondernemen tegen/na potentiële cybersecurity incidenten. Het gaat bijvoorbeeld om een incidentrespons procedure en nood/continuïteitsplannen.
De gemeente toetst, oefent en evalueert deze maatregelen/acties/processen periodiek (zoals het oefenen van een cyberaanval).
De rollen en verantwoordelijkheden van functionarissen, directie en raad zijn vastgelegd en in de praktijk bekend.
Herstel (Recover)
De gemeente werkt planmatig aan weerbaarheid en is voorbereid op activiteiten ten behoeve van herstellen van processen en dienstverlening.
Incidenten op het gebied van informatiebeveiliging of cybersecurity worden geëvalueerd en leiden tot structurele verbetermaatregelen.
Algemeen
De raad wordt periodiek geïnformeerd over de digitale weerbaarheid van de gemeente en de ontwikkelingen op dat vlak.
De informatieverstrekking aan de raad biedt de raad voldoende mogelijkheden om de sturende en controlerende verantwoordelijkheden waar te maken.
De maatregelen, die de gemeente neemt, worden periodiek getoetst, geoefend en/of geëvalueerd.

1.5 Werkwijze

De Rekenkamercommissie laat zich in de uitvoering van het onderzoek ondersteunen door een extern bureau (PBLQ). Zowel de organisatie, het college als de gemeenteraad worden intensief betrokken bij de uitvoering, waarbij de nadruk ligt op de rolneming van de raad.

Het onderzoek is begonnen met een startbijeenkomst waaraan de rekenkamercommissie, de onderzoekers van PBLQ en direct betrokkenen in de gemeentelijke organisatie[2] deel hebben genomen. Vervolgens is kennisgenomen van de relevante documenten. Aansluitend is in gesprekken met ambtenaren en de bestuurlijk portefeuillehouder ingegaan op het gemeentelijk beleid met betrekking tot informatiebeveiliging. Daarnaast is aandacht besteed aan de uitvoering van dit beleid en de ervaringen die daarbij zijn opgedaan.

Om de uitvoering van het beleid te toetsen rondom specifieke processen hebben twee casusbesprekingen plaatsgevonden. Daarbij is onder andere aandacht besteed aan het beveiligingsbewustzijn van de medewerkers van de gemeente Hardenberg en expliciet aan de voorbereiding op mogelijke incidenten. De casusbesprekingen zijn bedoeld als verdieping in het onderzoek en om vast te stellen op welke manier informatiebeveiliging en digitale weerbaarheid in de praktijk vorm krijgt.

De verkenning van de praktijk is afgerond met een convergentiebijeenkomst, waarin inzichten zijn voorgelegd aan de Chief Information Security Officer, voor verdere verdieping en verificatie.

Om een beeld te verkrijgen van de opvattingen van de raadsleden is met hen eveneens een bijeenkomst belegd. In deze bijeenkomst is met de raadsleden gesproken over hun ambities met betrekking tot informatiebeveiliging. Eveneens is aan de orde geweest hoe zij hun sturende en controlerende verantwoordelijkheden rond dit onderwerp invullen.

De gesprekken zijn gevoerd aan de hand van een vragenlijst en waren kwalitatief van aard. In de rapportage worden de verschillende opgedane inzichten en de veelzijdigheid in opvattingen weergegeven.

Het veldwerk voor dit onderzoek van de rekenkamercommissie is in juli 2021 afgerond. Van eventuele ontwikkelingen en aanpassingen in het geldende beleid die nadien hebben plaatsgevonden, kan in deze rapportage niet altijd melding worden gemaakt.

1.6 Leeswijzer

In het volgende hoofdstuk worden de bevindingen beschreven. Allereerst wordt in dat hoofdstuk ingegaan op het gemeentelijk beleid en in het volgende hoofdstuk wordt aandacht besteed aan de uitvoering van het beleid. In het daaropvolgende hoofdstuk worden de ervaringen van de raad beschreven. In het vijfde hoofdstuk worden de deelvragen en de hoofdvraag van het onderzoek beantwoord en vervolgens wordt een beoordeling gedaan aan de hand van het normenkader. Tot slot bevat dit hoofdstuk enkele aanbevelingen voor de gemeenteraad en het College van B&W.

[2] Als in deze rapportage gesproken wordt over ‘de gemeentelijke organisatie’ worden hier zowel de ambtelijke organisatie als het college van B&W bedoeld.

Een overzicht van de geïnterviewde personen en geraadpleegde literatuur is terug te vinden in de bijlagen. Daarnaast worden de bijlagen gebruikt voor informatie en bevindingen van gevoelige aard.In Bijlage D is een lijst met afkortingen en begrippen gerelateerd aan informatiebeveiliging opgenomen.

2. Het gemeentelijk informatiebeveiligingsbeleid

In dit hoofdstuk wordt het gemeentelijk informatiebeveiligingsbeleid van Hardenberg beschreven zoals het op papier is vastgelegd. Daarnaast wordt beschreven hoe rollen en verantwoordelijkheden zijn belegd en wordt het tactisch informatiebeveiligingsbeleid beschreven. Dit tactisch beleid bevat een vertaling van het strategisch beleid naar concretere instrumenten en voor de gemeente Hardenberg relevante aandachtspunten.

2.1 Strategisch beleid

De gemeente Hardenberg heeft een iVisie[3]: 'Informatievoorziening is de basis voor innovatie en verbinding'. De visie is uitgewerkt in een viertal pijlers. In de context van dit onderzoek, is de pijler 'professionele overheid' van belang. Het uitgangspunt is hierbij: 'Inwoners verwachten dat wij een professionele organisatie zijn die slagvaardig, efficiënt en effectief is'. Dit vertaalt zich verder in: 'Inwoners kunnen erop vertrouwen dat hun privacy en gegevensveiligheid wordt gerespecteerd.'

'Inwoners kunnen erop vertrouwen dat hun privacy en gegevensveiligheid wordt gerespecteerd.

Inwoners mogen erop vertrouwen dat wij hun privacy en de veiligheid omtrent hun gegevens bewaken en beschermen. Vanzelfsprekend houden we ons, bij de inrichting van onze informatievoorziening en de uitvoering van onze taken, aan de wet- en de regelgeving rondom privacy en gegevensveiligheid.

Dit belangrijke aspect is geborgd in onze processen en wordt in de alsmaar veranderende digitale wereld periodiek geactualiseerd en waar nodig herijkt.

De gemeente werkt sinds 2015 aan organisatiebrede informatiebeveiliging volgens de Baseline voor Informatiebeveiliging Nederlandse Gemeenten (BIG), voorganger van de BIO. De gemeente heeft een strategisch informatiebeveiligingsbeleid opgesteld (2019-2023).[4] Het beleid bevat uitgangspunten voor de gehele organisatie ten aanzien van de veiligheid van informatie en dekt alle onderliggende deelgebieden af. Dit beleid wordt op tactisch niveau aangevuld (in onder andere het Informatiebeveiligingsplan) met onderwerp-specifieke tactische beleidsregels, die aanvullend zijn op het strategisch beleid.

In het strategisch beleid worden een aantal elementen expliciet benoemd die van invloed zijn op het beleid: de BIO, de '10 principes voor informatiebeveiliging', het Dreigingsbeeld Informatiebeveiliging Nederlands Gemeenten en informatie uit incidenten en inbreuken op de beveiliging. De BIO is (meer dan de BIG) gericht op risicomanagement. Dat betekent dat processen en informatiesystemen beveiligd worden op basis van de risico's die de gemeente (wil) lopen. Het management zal daarbij op voorhand keuzes en afwegingen moeten maken of informatie in nieuwe en bestaande processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid. Het tweede element, de '10 principes voor informatiebeveiliging' (zie kader), wordt genoemd als bestuurlijke aanvulling op het BIO

[3] iVisie Gemeente Hardenberg versie 1.2

[4] Strategisch Gemeentelijk Informatiebeveiligingsbeleid versie 2.01

normenkader. De principes zijn waarden die de bestuurder zichzelf oplegt en gaan over de rol van het bestuur bij het borgen van informatiebeveiliging en ondersteunen de bestuurder bij het uitvoeren van risicomanagement. Ten derde dient het Dreigingsbeeld Informatiebeveiliging Nederlands Gemeenten om focus aan te brengen bij het actualiseren van beleid en plannen voor informatiebeveiliging. Als laatste is het systeem van gemeente Hardenberg voor het vastleggen van incidenten een belangrijke bron om van te leren.

De 10 principes voor informatiebeveiliging

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

Deze principes zijn gelijk met de BIO van kracht, zie besluitvorming Informatiebeveiligingsdienst (IBD) en Verenigde Nederlandse Gemeenten (VNG).

Het strategisch beleid wordt minimaal één keer per drie jaar beoordeeld, maar ook als zich grote wijzigingen voordoen. Het overkoepelend gemeentelijk informatiebeveiligingsbeleid volgt aanvullend beleid per BIO-thema, proces of informatiesysteem. Het huidige beleid is in 2019 opgesteld, waardoor de verwachting is dat het beleid in 2022 wordt herzien.

In haar beleid formuleert de gemeente Hardenberg een aantal uitgangspunten die voor dit onderzoek relevant zijn:

- Alle informatie en informatiesystemen zijn van belang voor de gemeente, waarbij bepaalde informatie van vitaal en kritiek belang is. Het college van B en W is eindverantwoordelijk voor de informatiebeveiliging.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen, die gebruikt worden door de gemeente Hardenberg, hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.

- Informatiebeveiliging is een continu verbeterproces. ‘Plan, do, check en act’ vormen samen het managementsysteem van informatiebeveiliging.

Zoals genoemd, gebruikt de gemeente Hardenberg ENSIA voor de verantwoording van informatiebeveiliging. ENSIA is een initiatief van gemeenten en de ministeries van BZK en SZW. ENSIA streeft naar een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid. Het ondersteunt de gemeente bij de verantwoording over informatiebeveiliging richting de gemeenteraad en de rijksoverheid. ENSIA bestaat onder meer uit het uitvoeren van een zelfevaluatie waarmee de genoemde informatiebeveiligingsnormen worden getoetst onder verantwoordelijkheid van het management. Hierbij gaat het uit van de BIO en informatiebeveiligingsnormen vanuit Basisregistratie Personen (BRP), wet- en regelgeving reisdocumenten, DigiD, Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Gezamenlijke Elektronische Voorzieningen Structuur (GeVS/Suwinet).

Het bestuur van gemeente Hardenberg geeft middels een collegeverklaring ENSIA[5] aan in hoeverre de gemeente voldoet aan de voor DigiD en Suwinet[6] geselecteerde informatiebeveiligingsnormen. Voor het afgeven van de verklaring vraagt het college *assurance* over opzet en bestaan van beheersingsmaatregelen aan een onafhankelijke IT-auditor, in 2019 en 2020 was dit SafeHarbour. Met de collegeverklaring wordt ook de raad geïnformeerd over de verantwoording. In 2019 werd voor DigiD niet aan de normen voor het webapplicatiebeheerproces voldaan en in 2020 werd op het onderwerp contractmanagement niet voldaan aan de normen. Aanvullende beheersmaatregelen zijn volgens de collegeverklaringen in een verbeterplan opgenomen, belegd en gemonitord. Voor de beheersingsmaatregelen (in opzet en bestaan) inzake Suwinet heeft het college verklaard te voldoen aan de geselecteerde normen. Voor 2020 werd eenzelfde verklaring afgegeven.

2.2 Rollen en verantwoordelijkheden

Voor de governance rondom informatiebeveiliging gaat de gemeente Hardenberg uit van het Three Lines of Defence model (3LoD):[7]

Het lijnmanagement (de eerste lijn) is verantwoordelijk voor de eigen processen en gegevenskwaliteit in hun eigen afdeling of team. In de eerste lijn is de directie verantwoordelijk voor de aansturing. Zij zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college geïnformeerd worden en stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. Informatiebeveiliging is onderdeel van risicomanagement in Hardenberg. De afdelingsmanagers en teamleiders zorgen voor de uitvoering en worden hierin ondersteund door de tweede lijn. Voor alle processen, systemen, data en applicaties is het de bedoeling dat er minstens één eigenaar is.

Sinds 2021 zijn de onderwerpen privacy en informatiebeveiliging (weer) onderdeel van de kwartaalrapportage richting de directie en het College. Daarvoor rapporteerde functionarissen apart aan

[5] Collegevoorstel inclusief bijlagen ‘Collegeverklaring ENSIA 2020 inzake Informatiebeveiliging DigiD, Suwinet, BAG, BGT en BRO’, 13 april 2021

[6] Voor Suwinet besteedt de gemeente Hardenberg een deel van diensten uit aan gemeente Ommen. Hardenberg en Ommen hebben een tijdlang een gezamenlijke bestuursdienst gehad, maar zijn inmiddels bezig met een ontvlechting. De splitsing betekent voor Hardenberg een overdracht van dienstverlening die per 1 januari 2025 volledig moet zijn.

[7] Strategisch Gemeentelijk Informatiebeveiligingsbeleid versie 2.01

de directie/gemeentesecretaris via reguliere overleggen. Informatiebeveiliging is ook opgenomen in het jaarverslag van de gemeente.

De tweede lijn (CISO, security officers) ondersteunt, adviseert, coördineert en bewaakt of het lijnmanagement de verantwoordelijkheid neemt. De CISO is een belangrijke spil en coördineert activiteiten op het gebied van informatiebeveiliging vanuit een onafhankelijke positie en rapporteert hierover direct aan het CMT. De rol van CISO heeft geen formele achtervang. In de praktijk vervangen de Functionaris Gegevensbescherming (FG) en CISO elkaar wanneer nodig. Ook zijn er informele afspraken met CISO's van buurgemeenten over vervanging.

De security officers zijn medewerkers in de verschillende afdelingen die naast hun reguliere functie ook taken hebben gekregen op het gebied van informatiebeveiliging. Zij ondersteunen het lijnmanagement met inhoudelijk advies. Deze functie is op dit moment niet bij alle afdelingen ingevuld. Er is geen functiebeschrijving voor de rol van security officer.

De derde lijn, de (interne) auditor, voorziet in een objectief oordeel over het geheel.

2.3 Tactisch informatiebeveiligingsbeleid

Als uitwerking van informatiebeveiligingsbeleid zijn de processen van de gemeente geclassificeerd op basis van beschikbaarheid, integriteit en vertrouwelijkheid en aan die classificatie is een basisbeveiligingsniveau (BBN) toegevoegd.[8] Dit kan gezien worden als een risicoanalyse voor de systemen en processen. Uit deze analyse blijkt dat voor Hardenberg onder andere de volgende systemen en processen de hoogste classificatie hebben: Gezondheidszorg (GGD taak/ ambulancedienst), Basisregistratie personen, Openbare orde en veiligheid (brandweer, preventie, rampbestrijding), Sociale Zaken (Uitvoering/verstrekking voorzieningen).

In het Jaarplan Informatiebeveiliging[9] (dat wordt vastgesteld door het CMT) worden tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de afdelingsmanagers en teamleiders, de CISO, het dreigingsbeeld van de IBD en de uitkomsten van ENSIA. In 2021 is de gemeente voornemens om (tactisch) beleid verder uit te werken, bijvoorbeeld op het gebied van thuiswerken, wachtwoorden en incidentmanagement en response (crisis). Daarnaast werkt de gemeente aan bewustwordingsactiviteiten (zie hieronder).

Bij het opstellen van het jaarplan wordt er getoetst op de verschillen tussen het vastgestelde informatiebeveiligingsbeleid en de situatie in de praktijk. Hiervoor wordt elk kwartaal onder andere een GAP-analyse uitgevoerd[10], waarin de BIO maatregelen worden beoordeeld op bestaan en impact (effectiviteit) om de tussentijdse voortgang te monitoren. De verschillen tussen beleid en praktijk worden vertaald naar een geprioriteerd (jaar-) plan van aanpak, waarin de verbetermaatregelen staan die prioriteit krijgen. In 2019 is men begonnen met een Jaarplan Informatiebeveiliging voor het domein Informatisering, Automatisering en Facilitair (IAF). In het Jaarplan IAF wordt specifiek onderscheid gemaakt tussen ICT, Documentaire Informatie Voorziening (DIV), Intern Service Punt (ISP) en Gegevensbeheer. In 2020 heeft de Publiekdienst (PD) een jaarplan opgesteld met daarin een aantal verbeterambities op hoofdlijnen. Overige domeinen hebben geen eigen jaarplan voor informatiebeveiliging.

[8] Dataclassificatie Q2 2021 versie 2

[9] Jaarplan In Control 2020-2021

[10] GAP BIO 2021 Q1

2.3.1 Jaarplan In Control 2020-2021

De gemeente Hardenberg heeft naast de Informatiebeveiliging jaarplannen ook een 'Jaarplan In Control 2020-2021: Gegevensbescherming, Informatiebeveiliging en Concern control.' Met name projecten voor informatiebeveiliging zijn in de context van dit onderzoek relevant. Deze projecten zijn onder andere gericht op bewustwording van (de noodzaak van) informatiebeveiliging en het opstellen van ontbrekende beleidsstukken voor informatiebeveiliging.

2.3.2 iBewustzijn

In het kader van de bewustwording rondom informatiebeveiliging en privacy is eind 2020 een leercirkel (e-learning) opgenomen in de Hardenberg Academie. In aanvulling daarop is een nulmeting[11] gehouden om het kennisniveau in beeld te brengen en een aanpak daarbij gekozen. De e-learning is verplicht gesteld voor medewerkers en daarnaast is besloten dat teamleiders aantonen in hoeverre de medewerkers de e-learning succesvol hebben afgerond. Met de e-learning iBewustzijn en de monitoring op deelname wordt volgens de gemeente Hardenberg ten eerste de kennis van informatieveiligheid bij medewerkers vergroot. Ten tweede worden medewerkers zich ervan bewust hoe om te gaan met informatieveiligheid in hun dagelijkse werkzaamheden. Ten derde draagt het bij aan het aantoonbaar voldoen aan de BIO en de Algemene Verordening Gegevensbescherming (AVG). Na een jaar wordt vervolgens een zogenoemde 1-meting gehouden. Rondom de e-learning heeft in het kader van iBewustzijn een gemeentebrede communicatiecampagne plaatsgevonden.

2.3.3 Continuïteit en cyberrisico's

Er is een opdracht verstrekt om de bedrijfscontinuïteitcyclus in te richten en om te oefenen met een cybercrisis om ontbrekend beleid op dit gebied te verbeteren.[12] Met een bedrijfscontinuïteitcyclus wil de gemeente de betrouwbaarheid van de dienstverlening verhogen. Een aspect dat direct samenhangt met het imago van de gemeente. Daarnaast wil de gemeente, voor zover dat kan, voorbereid zijn op een cybercrisis en de bewustwording verhogen bij management en bestuur.

Bedrijfscontinuïteitsbeheer is een proces waarbij de gemeente de nodige maatregelen treft om ongeacht de omstandigheden de continuïteit van de meest (kritische) bedrijfsprocessen te garanderen en de impact van verstoringen op de dienstverlening van de gemeente te minimaliseren. Plannen maken en maatregelen nemen zijn belangrijk om bedrijfscontinuïteit te waarborgen en daarmee bijvoorbeeld een cybercrisis te voorkomen. De gemeente stelt dat dit niet 100% uit te sluiten is, daarom houdt zij rekening met scenario's waarbij niet of beperkte beschikbaarheid tot de ICT-omgeving mogelijk is.

Als er een goede bedrijfscontinuïteitcyclus is en deze ook wordt geoefend door periodieke cyberoefeningen, geeft dit vertrouwen door vooraf gemaakte keuzes en prioriteiten bij verstoringen, uitval of andere calamiteiten.

Naast het voornemen om te oefenen met cyberrisico's, heeft de gemeente Hardenberg op algemeen niveau cyberrisico's in kaart gebracht.[13] Daarbij zijn mogelijke aanvallers en hun mogelijkheden onderscheiden evenals actuele risico vectoren, zoals *social engineering* en technische aanvallen. Ook is een aantal maatregelen tegen cyberrisico's benoemd zoals: medewerkers trainen in het gebruik van

[11] Resultaten nulmeting in bijlage C - niet openbaar

[12] Opdrachtbeschrijving Bedrijfscontinuïteitcyclus en Crisisoefening

[13] Cyber risico's gemeente Hardenberg

wachtwoorden en herkennen van phishing, adequaat loggen van events, scannen naar kwetsbaarheden in ict-infrastructuur en het inzetten van encryptie.

2.3.4 Incidenten en calamiteiten

Voor het afhandelen van incidenten is een procesbeschrijving opgesteld waarin is beschreven wie wat doet in het geval van een incident.[14] Daarbij wordt op basis van urgentie en impact een afweging gemaakt wat betreft de actie. Incidenten worden bij de afdeling IAF centraal gemeld en bijgehouden. De gemeente onderscheidt verschillende categorieën, waaronder veiligheidsincidenten in de huisvesting, datalekken, autorisaties, kwetsbaarheden of malware.

Het crisisteam wordt bijeengeroepen als het incident ‘kritiek’ is: wanneer de volledige of essentiële bedrijfsvoering wordt belemmerd en er geen alternatief voorhanden is. De vaste leden van het crisisteam (coördinator ICT, coördinator ISP, Incidentmanager ICT en de medewerker ISP) hebben verschillende verantwoordelijkheden, zoals het voorzitten van het crisisteam en het informeren van de directie tot aan het verslagleggen van de crisis en de overleggen voor evaluatie. De CISO, FG en vertegenwoordigers van de uitvoerende afdelingen zijn optionele leden van het crisisteam en nemen deel wanneer er bijvoorbeeld sprake is van een informatiebeveiligingsincident of een datalek. De crisisorganisatie wordt ook gebruikt voor escalatie van incidenten.

Hardenberg heeft een specifiek uit- en inwijkdraaiboek[15] voor het geval dat de beschikbaarheid en de werking van het systeem is verstoord als gevolg van menselijk of technisch falen, of andere calamiteiten. Applicatiebeheerders brengen een uitwijkadvies aan de CISO uit als het systeem niet binnen één werkdag weer volledig beschikbaar kan zijn. De CISO neemt vervolgens contact op met de gemeentesecretaris en deze neemt het besluit om wel of niet uit te wijken Vanuit de afdeling ICT en CISO is aangegeven dat deze lijn nu niet altijd helder is en dat deze procedure mogelijk gaat wijzigen, waarbij de incidentmanager verantwoordelijk wordt voor het signaal ‘uitwijken’.

De technische uitwijk wordt één keer per jaar gecontroleerd en tijdens de controle worden alle componenten van de uitwijkconfiguratie ook daadwerkelijk aangesloten en in bedrijf gesteld. In 2020 is hiermee gestart. Minimaal jaarlijks beoordelen de technisch- en applicatiebeheerders of de procedure en de uitvoering nog met elkaar in overeenstemming zijn. Als ze niet met elkaar overeenkomen, wordt beoordeeld of de procedure geactualiseerd moet worden of dat medewerkers geïnstrueerd moeten worden op een juiste toepassing van de procedure.

2.4 Externe onderzoeken

De gemeente Hardenberg heeft in 2019 gebruik gemaakt van een mystery guest actie, waarbij de fysieke informatieveiligheid is getoetst. De conclusies uit dit onderzoek zijn gericht op verbeterpunten van het bewustzijn van medewerkers en een aantal technische- en organisatorische beveiligingsmaatregelen.

De gemeente heeft in september 2019 een Security Maturity Assessment (SMA) laten uitvoeren door SecureLink[16]. SecureLink identificeert de vijf activiteiten uit NIST-model, maar heeft zich in dit onderzoek gericht op drie activiteiten: bescherm, detecteer en reageer. Voor het bepalen van een

[14] Incidentmanagement – versie 25 juli 2019

[15] Uitwijk en inwijk draaiboek en Uitwijk en inwijk draaiboek Technisch

[16] SMA Report Gemeente Hardenberg – versie 1.0

volwassenheidsniveau richt het onderzoek zich op drie aspecten: mensen (people), processen (process) en technologieën (technology). Hardenberg scoorde onder het gemiddelde wat betreft volwassenheidsniveau in het algemeen, maar beter dan gemiddeld wat betreft mensen en processen[17].

2.5 Tussenconclusie informatiebeveiligingsbeleid

Strategisch informatiebeveiligingsbeleid

Het valt op dat het informatiebeveiligingsbeleid een vrij algemeen karakter heeft. De gemeente heeft net als vrijwel alle overheidsorganisaties in Nederland de BIO geadopteerd. Ook de tien principes en de speerpunten voor het Hardenbergse beleid zijn heel generiek, terwijl de gemeente wel degelijk richtinggevende keuzes te maken heeft. Dan gaat het bijvoorbeeld over de vraag welke risico's de gemeente bereid is te accepteren ('risk appetite'), hoeveel middelen zij daarvoor over heeft en wanneer het bestuur tevreden is over de informatiebeveiliging. Als het beleid te zeer wordt gericht op het implementeren van de maatregelen zoals de BIO die voorschrijft, dan bestaat het risico dat te veel op 'het zetten van vinkjes' wordt gestuurd.

Tactisch informatiebeveiligingsbeleid

Aanvullend op het strategisch informatiebeveiligingsbeleid heeft de gemeente diverse tactische beleidsplannen, zoals jaarplannen, beleid voor specifieke maatregelen (zoals wachtwoordbeleid) en onderzoeken. Het tactisch informatiebeveiligingsbeleid wordt ook nog verder uitgewerkt op deelonderwerpen, bijvoorbeeld op het gebied van thuiswerken.

Een cruciaal onderwerp binnen het tactisch informatiebeveiligingsbeleid is het kennisniveau over informatiebeveiliging in de organisatie. De rol (en de benoeming) van security officers bij de diverse afdelingen is hierbij belangrijk. Er is nog geen functiebeschrijving voor de security officers opgesteld.Verder valt op dat de gemeente een risicoanalyse heeft uitgevoerd en alle processen en informatiesystemen heeft geclassificeerd, waardoor de gemeente een goed beeld heeft van de belangrijkste beveiligingsrisico's.

[17] Overige resultaten Security Maturity Assessment in bijlage C - niet openbaar

3. Informatiebeveiliging in de praktijk

In de gemeente Hardenberg leidt het beleid tot verschillende beveiligingsmaatregelen. Hoe dit in de praktijk uitpakt, is besproken in een aantal interviews met medewerkers van de gemeente. Daarnaast is aan de hand van twee casussen onderzocht hoe het beveiligingsbeleid in de praktijk vorm krijgt en hoe beveiligingsmaatregelen zorgen voor weerbaarheid van belangrijke processen. Daarbij is niet alleen naar maatregelen gekeken die vooraf (preventief) ter bescherming zijn genomen, maar ook naar maatregelen die de gemeente heeft genomen om in het geval van een incident of een (grote) aanval te handelen, en op welke manier de gemeente voorbereid is op een crisis.

De twee onderzochte casussen zijn ‘opmaken beschikking en aanslag afvalstoffenheffing’ en ‘aanvragen (en mutaties) tot betalen van algemene bijstand uitkeringen.’ Aan de casusbesprekingen hebben medewerkers van de gemeente deelgenomen die kennis hebben van het proces, de risico’s, de gebruikte informatiesystemen en de genomen maatregelen. Met de deelnemers is gekeken naar kritieke stappen in en (be-)dreigingen voor het proces. Tijdens de casusbesprekingen zijn belangrijkste dreigings-/risicoscenario’s verkend en in hoeverre de gemeente ‘weerbaar’ is in het geval zo’n scenario zich daadwerkelijk voordoet. Er is gekeken naar de maatregelen op het gebied van beschermen, detecteren, reageren en herstellen.

De bevindingen zijn beschreven aan de hand van de activiteiten voor informatiebeveiliging volgens het NIST framework, waarbij steeds eerst een korte toelichting op deze activiteiten wordt gegeven.

In dit hoofdstuk worden ook een aantal voorbeelden gegeven die genoemd zijn in interviews of in casusbesprekingen. Deze voorbeelden dienen als toelichting op de bevindingen en gaan bijvoorbeeld op specifieke risico’s of incidenten die zich hebben voorgedaan. De voorbeelden zijn in een apart kader opgenomen.

3.1 Identificeer (Identify)

Onder het *identificeren* van risico’s worden diverse activiteiten geschaard, zoals het hebben van een duidelijk beleid en uitvoeringskader, het in beeld hebben van de belangrijkste processen, systemen en risico’s in beeld, het periodiek bijstellen van het risicobeeld.

In het kader van het informatiebeveiligingsbeleid is voor de processen in Hardenberg het basisbeveiligingsniveau vastgesteld en de processen zijn geclassificeerd op basis van de BIO.[18]

Voorbeeld: Tijdig betalen van uitkeringen

Bij het betalen van bijstandsuitkeringen speelt het aspect tijd een belangrijke rol. Inwoners verwachten op de betaaldatum het bedrag op hun rekening te ontvangen en een vertraging van één of twee dagen kan hen al in financiële problemen brengen. Bovendien levert het te laat uitbetalen schade op in de beeldvorming over de gemeente.

De gemeente heeft diverse maatregelen genomen om te zorgen dat uitkeringen op tijd kunnen worden betaald.

[18] Dataclassificatie Q2 2021

Als onderdeel van het beleid heeft de gemeente security officers per team of afdeling die een grote rol spelen in de uitvoering. Security officers, mits aanwezig, voeren taken uit in het kader van het incidentproces, bewustwording en het actueel houden van procesbeschrijvingen. Er is een duidelijke functiescheiding tussen de CISO en de security officers, maar zij hebben wel nauw contact, bijvoorbeeld als het gaat om risico-inschattingen en het vaststellen van beveiligingseisen ten aanzien van de belangrijkste processen en systemen (zoals hoe lang processen maximaal uit mogen vallen). De rol van security officer is (nog) niet binnen elk team (of afdeling) ingevuld.

De security officer van IAF brengt voor de gemeente risico's in kaart aan de hand van gap-analyses[19] en meldingen van de IBD. Daarnaast wordt er gebruik gemaakt van vulnerability scanning en gaat de gemeente een penetratietest laten uitvoeren. In een penetratietest gaat een (ethische) hacker proberen toegang te krijgen tot de systemen en gegevens van de gemeente. Hiermee wordt een beeld gekregen van kwetsbaarheden en risico's in applicaties, netwerk en systemen. Er is budget beschikbaar gesteld om voortaan jaarlijks een penetratietest uit te laten voeren.

De gemeente voert via het wijzigingsproces van IAF technische maatregelen door. Het gaat dan bijvoorbeeld om het verhelpen van een (nieuwe) kwetsbaarheid in de informatiesystemen of infrastructuur van de gemeente. Het initiëren van wijzigingen is belegd bij de security officer van de afdeling. Als onderdeel van het wijzigingsproces wordt door IAF de prioriteit van een wijziging bepaald, onder andere op basis van de onderbouwing van de security officer. Over het algemeen worden wijzigingen in het kader van security (-maatregelen) vaak geïntegreerd met lopende projecten. Het risico daarbij is dat als die projecten uitlopen, ook de informatiebeveiliging risico loopt. Nu loopt de gemeente soms ongewild wellicht langer risico door het verschuiven van projecten.

Voorbeeld: Informatiebeveiliging binnen de afdeling Publieksdienst

De afdeling Publieksdienst heeft een eigen jaarplan voor informatiebeveiliging[20]. In dat jaarplan zijn zaken opgenomen met betrekking tot de BRP, de jaarlijkse audit en te nemen maatregelen. De afdeling is eind 2018, begin 2019 gestart met een project om kritisch naar de processen te kijken (op basis van de lean-methode). De belangrijkste processen, bijvoorbeeld op het gebied van basisregistraties, worden regelmatig doorgelicht behulp van een zelfevaluatie. Jaarlijks worden deze processen ook met de CISO doorgenomen. Daar volgt een verbeterplan uit om risico's weg te nemen en (aanvullende) beveiligingsmaatregelen te nemen.

Er wordt in Hardenberg overwegend op vertrouwd dat de informatiebeveiliging van de systemen goed is geregeld door IAF en de ICT-leveranciers. Vooral het menselijk handelen en gedrag worden als grootste risico gezien. Managers en teamleiders zijn zich bewust dat zij een voorbeeldrol hebben en benadrukken het belang van bijvoorbeeld het anonimiseren van data en het elkaar aanspreken op gedrag. Managers voelen zich daar over het algemeen in gesteund door de CISO en FG, maar ook de security officers spelen een belangrijke rol. Het bewustzijn rondom informatiebeveiliging is erg belangrijk voor de gemeente, zo blijkt ook uit de afgenomen interviews en het bewustwordingsprogramma van de gemeente.

Binnen de gemeente leeft het beeld dat adequate beveiliging van informatie valt of staat met de cultuur in de organisatie en de houding en het gedrag van medewerkers. Leidinggevenden hebben daarin een

[19] GAP BIO 2020 Q1 tot 2021 Q1

[20] Jaarplan Informatiebeveiliging PD 2020 – versie 1.1

belangrijke rol. Ook wordt geconstateerd dat het thuiswerken extra risico's met zich meebrengt. Er zijn weliswaar afspraken over het meenemen van dossiers en over het vergrendelen van het computerscherm, maar men is zich er ook van bewust dat controle op de naleving daarvan lastig is.

Voorbeeld: Thuiswerken

Het thuiswerken maakt informatieveilig gedrag voor de gemeente nog belangrijker, omdat er minder zicht is op medewerkers. Daar waar het risico op het verliezen van vertrouwelijke informatie (te) groot wordt geacht mogen medewerkers geen stukken mee naar huis nemen. Ook de uitval van medewerkers (bijvoorbeeld door ziekte) wordt gezien als risico, omdat het kan bijdragen aan het maken fouten in het doorlopen van het juiste proces.

Voorbeeld: Schaduwadministraties

Een voorbeeld van een risico door menselijk handelen is het bijhouden van schaduwadministraties met bijvoorbeeld persoonsgegevens. De beveiligingsmaatregelen, die voor het beheren van de BRP zijn geïmplementeerd, (met betrekking tot de actualiteit van de registratie, het uitvoeren van controles, etc) werken niet voor de informatie in de schaduwadministratie. Het gevaar is dat er verkeerde informatie in de schaduwadministratie staat met als consequentie dat er bijvoorbeeld brieven gestuurd worden naar personen die overleden zijn.

Voorbeeld: Beveiliging bij ketenpartners

Een risico dat vooral in de casusbesprekingen naar voren kwam, betreft de beveiliging bij ketenpartners van de gemeente. Zij voeren voor of namens de gemeente taken uit en gebruiken daarvoor ook gegevens die afkomstig zijn van de gemeente. Het is bij de verantwoordelijke managers niet altijd bekend in hoeverre daar afspraken over zijn gemaakt en of dit wordt gemonitord.

Tot slot is de behoefte geuit om meer opvolging te geven aan incidenten, deze te evalueren en na fouten te verbeteren om bij te dragen aan de bewustwording bij medewerkers.

3.2 Bescherm (Protect)

Activiteiten om te *beschermen* tegen inbreuken op de beveiliging zijn het ontwikkelen en implementeren van maatregelen om te zorgen voor de continuïteit en bescherming van (kritische) processen en dienstverlening. Medewerkers werken volgens de maatregelen en zijn zich bewust van eigen handelen en voelen de verantwoordelijkheid voor de bescherming van informatie.

De gemeente Hardenberg heeft een verscheidenheid aan (technische) maatregelen geïmplementeerd ten behoeve van informatiebeveiliging.[21] Zo zijn de informatiesystemen in Hardenberg op verschillende manieren afgeschermd met autorisaties en controles op de toegang tot informatie. Leidinggevenden verwachten dat de afdeling IAF en de gemeentelijke ICT-leveranciers voldoende maatregelen hebben getroffen.

[21] GAP BIO 2020 Q1 tot 2021 Q1

De gemeente heeft verschillende maatregelen geïmplementeerd om de continuïteit van processen en dienstverlening te garanderen.[22] De organisatie is er daarnaast van doordrongen dat er continue aandacht moet zijn voor informatiebeveiliging, mede omdat het menselijk handelen als een van de grootste risico's wordt gezien. Binnen Hardenberg loopt een iBewustzijn traject[23] om medewerkers bewust te maken van kwetsbaarheden. Dit traject is niet vrijblijvend, medewerkers moeten deelnemen. Verbetering van het bewustzijn wordt gezien als een kwestie van continue aandacht. Om dat te bewerkstelligen wordt bijvoorbeeld nieuws uit andere gemeenten gebruikt als 'haakje' om informatiebeveiliging onder de aandacht te brengen, maar er wordt ook regelmatig overleg met de CISO georganiseerd en tijdens sommige vergaderingen zijn informatiebeveiliging en privacy een vast agendapunt. Bewustzijn rondom informatiebeveiliging wordt meermaals gezien als een van de belangrijkste elementen voor de weerbaarheid van de gemeente.

De gemeente heeft ook verschillende technische maatregelen genomen om de informatiesystemen en infrastructuur te beschermen, zoals een firewall en maatregelen om DDoS-aanvallen te voorkomen. Aangaande maatregelen tegen DDoS-aanvallen is de gemeente deels afhankelijk van externe leveranciers zoals hosting partijen. De technische en organisatorische maatregelen (specifiek communicatie) is nog niet altijd optimaal bij leveranciers, zo blijkt ook uit een recent incident op het gebied van beschikbaarheid.

Voorbeeld: Beschermingsmaatregelen afdeling Publieksdienst

De afdeling Publieksdienst, waar veel met persoonsgegevens wordt gewerkt, heeft haar processen zoveel mogelijk lean ingericht om risico's op fouten maken weg te nemen. Het klantcontactcentrum (KCC) heeft bijvoorbeeld een raadpleegfunctie in de systemen van belastingen. Daarbij is de afspraak dat medewerkers altijd eerst verifiëren of ze de juiste persoon aan de lijn hebben en geven ze verder nooit gevoelige informatie over de telefoon. Publieksdiensten werkt veel met persoonsgegevens, zoals bij de geboorteaangifte, de processen zijn daarom zodanig ingericht om fouten (zoals informatie naar de verkeerde personen op te sturen na de aangifte).

Er wordt bij burgerzaken gebruikt gemaakt van een camerasysteem dat documenten op echtheid controleert en controleert of de persoon die het document toont ook hoort bij de foto op het document. Dit wordt gedaan om fraude tegen te gaan (in het verleden hebben zich incidenten op dit vlak voorgedaan). Er zijn plannen om de zuil die bij het loket staat te vervangen voor een slimme zuil om documenten direct te kunnen inlezen en zo personen te kunnen identificeren.

Ook in het proces van reisdocumenten zijn er diverse beveiligingsmaatregelen genomen om incidenten te voorkomen, zoals functiescheiding, het inregelen van autorisaties en een vier-ogen principe. Reisdocumenten worden door een specifiek bedrijf verzonden en het komt wel eens voor dat er een document (tijdelijk) kwijt is. Ook worden documenten soms per ongeluk niet vernietigd als dat wel moet. Dergelijke incidenten/datalekken worden gemeld en naar aanleiding van incidenten worden processen ook geëvalueerd en verbeterd.

[22] O.a. GAP BIO 2020 Q1 tot 2021 Q1; Uitwijk en inwijk draaiboek en Uitwijk en inwijk draaiboek Technisch

[23] CMT voorstel Bevorderen iBewustzijn/informatieveiligheid inclusief bijlagen; Wekencampagne iBewustzijn – Informatieveiligheid; Nulmeting iBewustzijnplan informatieveiligheid

3.3 Detecteer/Ontdek (Detect)

De gemeente heeft verschillende maatregelen genomen om beveiligingsincidenten te *detecteren*. Grofweg kunnen deze maatregelen worden opgedeeld in organisatorische maatregelen en technische maatregelen.

De belangrijkste organisatorische maatregelen zijn gericht op het herkennen en melden van beveiligingsincidenten door medewerkers. De verwachting van leidinggevenden is dat medewerkers alert genoeg zijn om kleine incidenten en datalekken te melden. De verschillende activiteiten gericht op bewustwording dragen bij aan de alertheid van medewerkers. Ook organisatorische maatregelen, zoals het toepassen van het 'vier-ogen principe' bij cruciale processen, dragen bij aan hogere veiligheid. Dit is niet altijd 'formeel' beleid, waardoor het lastig is hierop te controleren of te monitoren. Het zal niet altijd worden opgemerkt als het niet wordt toegepast.

Binnen de gemeente worden regelmatig (vermoedens van) incidenten – zoals verdachte e-mails – gemeld bij de security officer van de betreffende afdeling. Daarnaast worden incidenten breder besproken in de teams en afdelingen. Er is een vaste procedure voor het melden en afhandelen van incidenten, maar vanuit de CISO wordt aangegeven dat de bekendheid voor deze procedure kan worden vergroot.[24]

De gemeente ontvangt regelmatig meldingen over nieuwe kwetsbaarheden in informatiesystemen van de Informatiebeveiligingsdienst (VNG Realisatie). De gemeente administreert deze en volgt de kwetsbaarheden op, bijvoorbeeld door beveiligingsupdates te installeren.

Hardenberg heeft een monitoringstool voor de technische omgevingen, die triggers af geeft bij afwijkingen van de beschikbaarheid van systemen. De tool kijkt niet naar 'ongewenste activiteiten'. Daarvoor kan wel teruggekeken worden in de logging, maar daar wordt niet (actief) op gemonitord. Er is nog geen Security Information & Event Management (SIEM) of Security Operations Center (SOC) die correlatie tussen incidenten en dus risico's kan zien. Vanuit de gemeente wordt wel de noodzaak gevoeld om deze functionaliteit in te richten, daarom is Hardenberg betrokken (als afnemer/gebruiker) bij de aanbesteding voor een SIEM/SOC. Echter zal er ook capaciteit moeten komen om de functionaliteit goed in te vullen. Deze betaalt zich op lange termijn wel terug door het proactieve beheer dat er mee bereikt wordt.

Hardenberg heeft ook maatregelen getroffen om een aanval met ransomware tegen te gaan, op basis van een besmetting in het verleden. In de gemeente is ook een incident geweest waarbij er sprake was van besmetting via e-mail, maar de impact van deze besmetting is beperkt geweest.

Hardenberg doet mee met het traject GGI-Veilig van de Vereniging Nederlandse Gemeenten. Via GGI-Veilig kunnen gemeenten informatiebeveiligingsproducten afnemen waaronder de SIEM/SOC oplossing voor het bewaken van gedrag en acties op het eigen bedrijfsnetwerk en beveiligingsproducten voor de gemeentelijke ICT-infrastructuur. Een laatste voorbeeld van een detectiemaatregel die de gemeente heeft afgenomen binnen GGI-veilig is de penetratietest.

Voorbeeld: Detectie van fouten bij afvalstoffenheffing

[24] Incidentmanagement – versie 25 juli 2019

In het proces van afvalstoffenheffing wordt gebruik gemaakt van testruns voordat beschikkingen en aanslagen naar de productieomgeving worden doorgezet. Ook worden de jaarlijkse aanslaggegevens gecontroleerd op basis van de gegevens van het jaar daarvoor.

Ook wordt er in het proces gewerkt met het vierogen principe bij de invoer van cruciale gegevens. Eén persoon voert de gegevens in en een ander controleert deze, waarbij fouten kunnen worden gedetecteerd.

3.4 Reageer (Respond)

Activiteiten die de gemeente kan uitvoeren om te *reageren* zijn het implementeren van maatregelen om actie te ondernemen tegen/na potentiële cybersecurity incidenten, zoals bijvoorbeeld een incidentrespons-procedure en nood/continuïteitsplannen. Ook het periodiek toetsen, oefenen en evalueren van die maatregelen (processen) en het vastleggen van rollen verantwoordelijkheden hoort daarbij.

In Hardenberg hebben geen grote calamiteiten plaatsgevonden als gevolg van cybercriminaliteit. Vanuit de gemeente wordt wel gesignaleerd dat er steeds meer pogingen gedaan worden. In Hardenberg is wel sprake van kleinere beveiligingsincidenten, zoals ongewenste autorisaties, beschikbaarheidsissues of gevonden kwetsbaarheden in de gebruikte softwarepakketten. De issues worden in het centrale incidentregistratiesysteem (Topdesk) bijgehouden. Met name over de grotere incidenten wordt richting het management gerapporteerd, datalekken worden bijvoorbeeld via de FG bij de gemeentesecretaris gemeld, zo blijkt uit de gesprekken met medewerkers.

Vanuit het management wordt vertrouwen uitgesproken dat Hardenberg adequaat kan reageren op eventuele incidenten. Er is ook een procedure voor incidenten[25], maar wat de procedure inhoudt is niet bij iedereen bekend. Het beeld bestaat dat bij grote incidenten met name de CISO (of FG) en security officer aan zet zijn om het proces te begeleiden. Vanuit de uitvoering is de security officer in de ‘lead’ voor het melden, afhandelen en evalueren van incidenten en datalekken. Het verantwoordelijke management wordt voornamelijk aan het einde van het proces geïnformeerd over incidenten en de afhandeling daarvan.

Bij een groot incident treedt in Hardenberg een crisisorganisatie in werking, waarbij ook de gemeentesecretaris en de burgemeester betrokken worden. Er wordt twee of drie keer per jaar binnen de crisisstructuur geoefend en geëvalueerd. Met de crisisorganisatie is tijdens het onderzoek voor het eerst sinds lange tijd een oefening rondom informatiebeveiliging geweest (de cybergame van de IBD). In de game wordt een hack gesimuleerd waarbij het politiek-bestuurlijke aspect van belang is. De resultaten en leerpunten uit deze oefening zijn niet bekend ten tijde van dit onderzoek.

De gemeente werkt aan een project ten behoeve van de bedrijfscontinuïteit[26], waarbij onder andere de planning en control cyclus verder worden geformaliseerd. In het kader van het project worden alle kritische processen beschreven voor de reguliere situatie. De inventarisatie van de continuïteit van die processen moeten worden opgenomen in een cyclus, zodat periodiek kan worden geëvalueerd.

[25] Incidentmanagement – versie 25 juli 2019

[26] Opdrachtbeschrijving Bedrijfscontinuïteitcyclus

De gemeente werkt ook aan de segmentering van het netwerk. Dit wordt projectmatig uitgevoerd en is nog niet in voldoende mate afgerond. Segmentering van het netwerk zorgt ervoor dat bij een aanval (zoals ransomware) de impact beperkt blijft.

3.5 Herstel (Recover)

Om te *herstellen* na een incident kan planmatig aan weerbaarheid gewerkt worden, om zo voorbereidingen te treffen voor het herstellen van processen en dienstverlening. Activiteiten zijn bijvoorbeeld het evalueren van incidenten op gebied van informatiebeveiliging of cybersecurity en structureel werken aan verbeteringen in maatregelen.

Om te kunnen herstellen in het geval van een incident heeft de gemeente Hardenberg diverse maatregelen getroffen. Zo heeft Hardenberg naast een gespiegelde omgeving en drie back-ups, op twee verschillende locaties waarvan één offline back-up. Ook hier geldt dat leidinggevenden bij de gemeente Hardenberg er op vertrouwen dat deze maatregelen voldoende zijn om na een incident weer snel aan de slag te kunnen.

Hardenberg heeft ook een uitwijkmogelijkheid in Ommen. Er is afstemming tussen de CISO's van Hardenberg en Ommen en een groot deel van de maatregelen zijn ook (nog) relevant voor Ommen. De uitwijk in Ommen is een gespiegelde omgeving en daarvoor is een uit- en inwijkplan opgesteld. De gemeente oefent jaarlijks met deze uitwijk, maar in het kader van de ontvlechting van Ommen verandert de uitwijklocatie (en bijbehorend plan) vanaf uiterlijk 2024.[27]

De back-ups voor Hardenberg worden incrementeel (alleen de wijzigingen) en online gemaakt. Een keer per week wordt er een volledige back-up gemaakt, daarnaast worden er back-ups weggeschreven op tapes. Medewerkers kunnen zelf online ook twee of drie stappen terug, maar technisch beheer kan met de online back-ups tot een week terug. De back-up en restore activiteiten worden jaarlijks getest en gecontroleerd (als onderdeel van ENSIA en IT-Audit).[28]

Voorbeeld: Evaluatie van incidenten

Sommige incidenten worden in de gemeenten gebruikt om van te leren. Een voorbeeld is een incident waarbij medewerkers uit praktische overwegingen gebruik maakten van elkaars autorisaties. Na gesprekken met de betreffende medewerkers is de casus meegenomen naar het werkoverleg, zodat andere medewerkers er ook van konden leren.

De gemeente heeft recentelijk een dashboard aangeschaft, waarmee teamleiders via een stoplichtmethodiek kunnen zien wat de stand van zaken is voor de maatregelen waar ze verantwoordelijk voor zijn. De hoop is dat door betere zichtbaarheid en teamleiders van elkaar gaan leren en dat proceseigenaren zich meer verantwoordelijk voelen voor informatiebeveiliging. Het dashboard wordt op dit moment ingericht en wordt nog niet gebruikt.

[27] Uitwijk en inwijk draaiboek en Uitwijk en inwijk draaiboek Technisch

[28] Zelfevaluatie ENSIA 2020

3.6 Informatiebeveiliging in de organisatie

Naast de activiteiten die gebaseerd zijn op het NIST Framework zijn er ook een aantal andere thema's relevant voor de weerbaarheid. Hierbij kan gedacht worden aan het periodiek informeren van de raad en hen mogelijkheden bieden om te sturen en controleren. Maar ook het periodiek toetsen van maatregelen en het formuleren van een algemene ambitie of afwegingskader geformuleerd op het vlak van informatiebeveiliging.

De gemeente heeft wel een ambitie op specifieke onderwerpen, bijvoorbeeld als het gaat om het tonen van goed werkgeverschap in combinatie met veilig werken (in relatie tot de aanschaf van nieuwe laptops) en de uitspraak om in te zetten op het voorkomen van een crisis zoals in Hof van Twente. Het uitspreken van een expliciete ambitie voor de gemeente wordt wel als een goed idee gezien. Een probleemanalyse met betrekking tot informatiebeveiliging binnen Hardenberg en een vertaling van bestaande regelgeving en landelijke kaders naar de lokale praktijk zijn volgens bestuur belangrijke elementen om tot zo'n ambitie en bijbehorende acties te komen.

3.6.1 De CISO

Voor de invulling van de rol van de CISO wordt uitgegaan van de professionaliteit van de medewerker. Aan dat vertrouwen wordt ook veel waarde gehecht door de gemeentesecretaris. In praktijk is het beeld dat de CISO (samen met de FG) verantwoordelijk is voor de informatiebeveiliging op strategisch niveau en de lijn voor de uitvoering. Ook is het beeld dat de CISO vanuit zijn rol de organisatie motiveert en informeert op het gebied van informatiebeveiliging. Vanuit de CISO zelf wordt juist benadrukt dat informatiebeveiliging de verantwoordelijkheid van de proceseigenaren is, of danwel de concernmanager of eventueel de gemeentesecretaris. De CISO geeft aan niet (eind)verantwoordelijk te zijn, al wordt opgemerkt dat men toch vaak bij de security officers of de CISO uitkomt en die verantwoordelijkheid wel wordt gevoeld. Er is in Hardenberg buiten een functieomschrijving geen kader voor de invulling van de rol van CISO, voor Securiy Officers (SO) is er geen kader of functieomschrijving, daarom is deze afhankelijk van de invulling van degene die deze functie vervult. Momenteel wordt dat gedaan op basis van input van medewerkers en door bij te sturen waar het minder goed gaat wat betreft informatiebeveiliging. Ook wordt gekeken naar ontwikkelingen in de techniek en op basis van de BIO en auditresultaten.

3.6.2 Rapportage

Vanuit het management wordt waardering uitgesproken voor de ambassadeursrol van de CISO. Er wordt echter ook aangegeven dat er meer behoefte is aan reguliere rapportages op het gebied van informatiebeveiliging. De inhoudelijke rapportagecyclus voor informatiebeveiliging is een zaak van de portefeuillehouder. Daarnaast rapporteert de gemeentesecretaris ieder kwartaal aan de burgermeester over de stand van zaken met betrekking tot verschillende onderwerpen, waaronder informatiebeveiliging. De concernmanager bedrijfsvoering is verantwoordelijk voor de invoering van veel (beveiligings-) maatregelen en er wordt gestuurd op basis van rapportages. De sturingsmechanismes zoals rapportage en evaluatie over maatregelen en risico's worden nog verder ingericht. Door informatiebeveiliging als regulier proces in te richten en minder ad hoc op te pakken, landt het thema meer bij de MT's en het CMT, zo is de veronderstelling. Vanuit management wordt aangegeven dat de gemeente nog kan verbeteren wat betreft de rapportage op het gebied van incidenten.

De gemeente werkt naar eigen zeggen nog niet erg risicogestuurd, maar is wel bezig met een professionaliseringslag op dat gebied. Met name het sturen op risico's en afwegingen maken daarop, is

nog in ontwikkeling. Dit is voor Hardenberg van belang, omdat het besef weliswaar leeft dat niet alle risico's kunnen worden gemitigeerd en dat de context continue in beweging is, maar dat hier nog niet actief op wordt gehandeld. Een gehoorde wens is om dit soort risicoafwegingen bij het CMT te beleggen en niet aan medewerkers zelf over te laten. In januari is zo'n risicoafweging gemaakt, toen de gemeentesecretaris signaleerde dat veel medewerkers thuiswerkten met eigen systemen. Toen is besloten dat alle medewerkers een eigen laptop zouden krijgen zowel uit het oogpunt van goed werkgeverschap als om te kunnen zorgen voor een goede en veilige systeeminrichting.

3.6.3 Informatiebeveiliging als bestuurlijke portefeuille

De portefeuille informatiebeveiliging is belegd bij één van de collegeleden. Recent is de verantwoordelijk wethouder vertrokken, waarna de burgemeester de portefeuille tijdelijk heeft waargenomen. In het college is informatiebeveiliging ook onderwerp van gesprek, wethouders en burgemeester interesseren zich voor informatiebeveiliging. Vanuit het bestuur is het besef dat situaties zoals bij de gemeente Hof van Twente nooit helemaal uit te sluiten zijn. Vanuit de organisatie leeft echter het beeld dat het bestuur vooral geruststelling zoekt ten aanzien van informatieveiligheid. Het blijkt niet altijd even gemakkelijk om het bestuur aangehaakt te houden bij een onderwerp als informatiebeveiliging, daarom wordt de link gelegd met financiën. De aanname is dat risicoanalyse daarbij helpt, maar het is voor de gemeente ook lastig om te bepalen welke processen en systemen het belangrijkst zijn. Dit is met name het geval als de (financiële) vertaling gemaakt moet worden naar welk risico de gemeente acceptabel vindt.

In de interviews kwam tot uiting dat beveiliging vaak een onderwerp is voor de uitvoering, terwijl men vindt dat het lijnmanagement nog meer betrokken mag worden. De gemeentesecretaris en de concernmanager bedrijfsvoering zijn weliswaar goed aangehaakt en overleggen geregeld met de CISO, maar ook voor de afdelings- en teammanagers wordt meer betrokkenheid verwacht. Mede door het incident bij Hof van Twente wordt meer bewustwording voor het belang van informatiebeveiliging bij het hogere management waargenomen. Daarbij is de uitdaging om de informatie terug te brengen naar de essentie. Het gaat vaak om technische onderwerpen en die moeten begrijpelijk gemaakt worden voor het bestuur, zodat zij vanuit hun rol belangen kunnen afwegen bij informatiebeveiliging(-smaatregelen). Het beeld is dat het college tot op heden geen risico wil lopen door te weinig geld voor informatiebeveiliging te reserveren, maar dat het college nog geen expliciete afwegingen maakt. Er zijn geen kaders afgesproken, waardoor het voor de organisatie naar eigen zeggen lastig is om in te schatten hoeveel risicoacceptatie en -tolerantie is.

3.6.4 De gemeenteraad

De gemeenteraad zou, wat de organisatie betreft, weloverwogen keuzes moeten maken (kaders stellen) en het college bevragen over risico's, financiën en mogelijke impact op dienstverlening in die gevallen dat een groot incident zich voordoet. Nu ziet men dat de raad vooral gerustgesteld wil worden en kennisneemt van de globale informatie die zij krijgt. De raad wordt op basis van de planning en control cyclus geïnformeerd: informatiebeveiliging is onderdeel van het jaarverslag. Er wordt gesignaleerd dat afstand van de raadsleden tot de dagelijkse praktijk groot is. Een van de wensen vanuit de organisatie is, dat de gemeenteraad meer doorvraagt danwel positie inneemt wat betreft informatiebeveiliging. Op dit moment zien raadsleden de verantwoording achteraf, maar is zij niet op de hoogte van bijvoorbeeld jaarplannen. Er wordt ook erkend dat het onderwerp voor de raad wellicht wat abstract is.

In het algemeen is verder geconstateerd dat er weinig tot geen vragen door de raad worden gesteld over het onderwerp informatiebeveiliging of digitale weerbaarheid.

4. Ervaringen en opvattingen vanuit de raad

In het kader van dit onderzoek is met een vertegenwoordiging van verschillende fracties uit de gemeenteraad van gedachten gewisseld over informatiebeveiliging. Hierbij zijn diverse onderwerpen aan de orde gekomen, zoals de kennis die raadsleden hebben van informatiebeveiliging, ervaringen die zij als raadslid hebben met dit onderwerp en hoe zij informatiebeveiliging tot een onderwerp in de raad kunnen maken. Een (fictieve) casus was de leidraad in deze bijeenkomst, waarbij in de bespreking ervan de relatie is gelegd met informatiebeveiliging in de gemeente Hardenberg.

Het karakter van de bijeenkomst was informerend en inventariserend en niet gericht op het innemen van standpunten. De bevindingen in dit hoofdstuk moeten niet gelezen worden niet als ‘opvattingen van de gemeenteraad’, maar wel als opvattingen van raadsleden.

Fictieve casus

In de casus (die geen relatie had met de gemeente Hardenberg) stond een gemeenteraadslid uit een andere gemeente centraal. Dit raadslid werd geconfronteerd met een mogelijke inbreuk op de informatiebeveiliging van de gemeente. Het raadslid realiseerde zich dat ondanks dat informatiebeveiliging steeds belangrijker is en de risico’s voor de gemeente groot, er toch is bezuinigd op het ICT-budget. Daarnaast herinnerde hij zich dat de raad wel geregeld is geïnformeerd over de stand van zaken, maar dat de stukken veel specifieke termen bevatten. Het had niet geleid tot discussie in de gemeenteraad.

In het algemeen zouden raadsleden meer kennis van het onderwerp willen hebben. Een informele informatieve raadsbijeenkomst, waarin medewerkers van de gemeente informatie geven over informatiebeveiliging zou men zeer op prijs stellen. Raadsleden hebben vragen over hoe de gemeente omgaat met risico’s, afwegingen die daarbij gemaakt worden en getroffen maatregelen. Ook willen zij informatie over bijvoorbeeld de fysieke toegangsbeveiliging en over de beveiliging van de ICT-hulpmiddelen die gemeenteraadleden hebben gekregen.

Het onderwerp informatiebeveiliging of digitale weerbaarheid staat verder niet op het netvlies van de raad. Er worden weinig tot geen vragen gesteld over het onderwerp. Het onderwerp komt wel onder de aandacht in het geval van een incident: dat is een duidelijke aanleiding om informatiebeveiliging te agenderen maar roept tegelijkertijd ook vragen op over de impact op de gemeente en inwoners bij raadsleden.

Voor raadsleden is in eerste instantie belangrijk dat de inwoners van Hardenberg erop moeten kunnen vertrouwen dat hun gegevens goed beschermd zijn bij de gemeente. Het is echter voor de gemeenteraad lastig om na te gaan of dat werkelijk het geval is. Actieve transparantie voor dit onderwerp vinden zij belangrijk, ook in het geval er een incident is geweest. Dan is het heel belangrijk om direct duidelijk te maken of er gegevens gelekt zijn, of dat dat door adequaat handelen van de gemeente is voorkomen.

Raadsleden zouden graag twee keer per jaar over de status geïnformeerd willen worden. In de normale raadsvergadering willen zij graag kennisnemen van de algemene status van informatiebeveiliging en welke stappen zijn gezet om de kwaliteit te verbeteren. Het gaat ze niet om heel technische of specifieke informatie, omdat zij zich ook realiseren dat dit gevoelige informatie is die niet openbaar moet worden. Deze momenten zouden bijvoorbeeld gekoppeld kunnen worden aan het overleg over de begroting of

de behandeling van de jaarrekening. Raadsleden zien voor de informatieverstrekking over concrete risico's of incidenten dan ook een vertrouwelijk overleg in het presidium of een besloten (commissie)vergadering voor zich. Hier kan specifieker en in meer detail over bepaalde zaken worden gesproken. Zij vinden het belangrijk dat er een protocol is, waarin duidelijkheid wordt gegeven over welke risico's en incidenten de raad geïnformeerd moet worden, op welke manier en wat de raadsleden met de verstrekte informatie mogen doen. Voor zover zij weten is er geen 'escalatieladder' die hier duidelijkheid over geeft. Als voorbeeld geven zijn aan dat onlangs in het presidium gesproken over een DDOS-aanval en raadsleden misten daarbij duidelijkheid over hoe zij met deze informatie moeten omgaan.

5. Conclusies en aanbevelingen

In dit hoofdstuk staan de conclusies en aanbevelingen van het onderzoek. Allereerst wordt per norm uit het normenkader een beoordeling gegeven. Daarna wordt de hoofdvraag aan de hand van de deelvragen beoordeeld. Als laatste worden aanbevelingen gegeven voor de verbetering van de digitale weerbaarheid van de gemeente.

5.1 Normenkader

Hieronder staat de beoordeling van de normen uit het normenkader. Normen worden positief (+), negatief (-) of neutraal (+/-) beoordeeld. Een neutrale beoordeling betekent dat de gemeente (groten)deels aan de norm voldoet, maar dat er één of enkele duidelijke verbeterpunten zijn. De beoordeling van de normen is onderbouwd per categorie (identificeer, bescherm, detecteer/ontdek, reageer en herstel). De onderbouwing wordt gedaan op basis van bevindingen uit het onderzoek, waarbij de belangrijkste of doorslaggevende bevindingen als onderbouwing worden meegegeven.

Identificeer (Identify)	Beoordeling
De gemeente heeft een duidelijk beleid en uitvoeringskader bij hoe zij omgaat met cybersecurity risico's van/aan systemen, mensen, gegevens, informatie en middelen.	+/-
De gemeente heeft de belangrijkste processen, systemen en risico's in beeld.	-
De gemeente stelt dit risicobeeld periodiek bij op basis van (onder andere) informatie over dreigingen en veranderingen in processen en systemen.	+/-

De gemeente heeft strategisch en onderliggend (tactisch) beleid voor informatiebeveiliging. In dit beleid staan de belangrijkste zaken om informatiebeveiligingsrisico's te kunnen beheersen. Het strategisch informatiebeveiligingsbeleid heeft wel een vrij algemeen karakter. Er zijn mogelijkheden voor aanvulling en verduidelijking, bijvoorbeeld op het vlak van de taken en verantwoordelijkheden van de security officers en formele verantwoordings- en rapportagelijnen. De gemeente heeft geen expliciete ambitie op het gebied van informatiebeveiliging, risicobereidheid of beleidsdoelen vastgesteld. Ook zijn er geen expliciete afwegingen gemaakt door het College of management over risicobereidheid.

De belangrijkste processen, systemen en risico's zijn in beeld. Voorbeelden van actuele risico's die tijdens het onderzoek naar voren zijn gekomen liggen op het gebied van thuiswerken, schaduwadministraties en de beveiliging bij ketenpartners/leveranciers.

De gemeente heeft ook in beeld welke maatregelen uit de BIO al zijn geïmplementeerd en welke nog moeten worden geïmplementeerd. Dit wordt periodiek bijgehouden. Nog te implementeren maatregelen zijn samen met andere beveiligingsactiviteiten onderdeel van jaar- en verbeterplannen. De gemeente heeft haar informatiesystemen en de bijbehorende informatie ook geclassificeerd en het basisbeveiligingsniveau bepaald.

De gemeente heeft geen aanvullende risicoanalyses uitgevoerd op belangrijke processen of systemen om voor kritische processen en dienstverlening de te nemen maatregelen in detail te onderbouwen.

Daarnaast is niet vastgesteld dat de gemeente zicht heeft op of alle leveranciers en ketenpartners adequate maatregelen geïmplementeerd hebben.

Periodieke penetratietesten moeten zicht geven op kwetsbaarheden in de ICT. De gemeente voert niet periodiek een penetratietest uit om de werking van technische maatregelen te toetsen, maar is wel voornemens om dit te doen. Pentesten zijn essentieel om inzicht te hebben in de belangrijkste risico's in de informatiesystemen.

Bescherm (Protect)	Beoordeling
De gemeente heeft maatregelen ontwikkeld en geïmplementeerd om te zorgen voor de continuïteit en bescherming van kritische processen en dienstverlening.	+/-

De gemeente heeft diverse technische en organisatorische maatregelen genomen om de belangrijkste systemen en de IT-infrastructuur te beschermen tegen verschillende bedreigingen. De gemeente heeft in beeld welke maatregelen uit de BIO al zijn geïmplementeerd en welke nog moeten worden geïmplementeerd en werkt dit ook periodiek bij.

Uit de onderzochte processen blijkt dat er bij de uitvoering van sommige maatregelen (zoals een vier-ogen principe) wordt uitgegaan van vertrouwen in de medewerker (ten opzichte van technisch afdwingen). Op dit punt zou de implementatie van beschermingsmaatregelen nog beter kunnen.

Detecteer/ Ontdek (Detect)	Beoordeling
Medewerkers werken volgens de maatregelen en zijn bewust van eigen handelen en verantwoordelijkheid.	+/-
De gemeente heeft maatregelen ontwikkeld en geïmplementeerd om cybersecurity incidenten te detecteren.	+/-
Er is een procedure voor het melden van incidenten en medewerkers kennen en gebruiken deze procedure.	+
Er is een escalatieprocedure richting de directie, college en gemeenteraad.	+

Er is veel aandacht voor veilig gedrag en bewustzijn van medewerkers zowel door team- en afdelingsmanagers als met behulp van een e-learning programma dat in 2021 is gestart en tijdens de onderzoeksperiode nog uitgevoerd werd. Tijdens de onderzoeksperiode hadden nog lang niet alle medewerkers de e-learning afgerond.

Incidenten worden wel herkend, gemeld en opgevolgd. Bij escalatie wordt gebruik gemaakt van de bestaande crisisstructuur.

De gemeente ontvangt ook meldingen over nieuwe kwetsbaarheden in informatiesystemen van de Informatiebeveiligingsdienst (en volgt deze ook op). Verder is er monitoring van de IT-infrastructuur op het vlak van beschikbaarheid, om verstoringen in de dienstverlening te kunnen detecteren. Als het gaat om andere vormen van monitoring, zoals het detecteren van ongeautoriseerde toegang, zijn er nog verbeteringen mogelijk. De gemeente is hiervoor aangesloten bij GGI-veilig.

Reageer (Respond)	Beoordeling
De gemeente heeft maatregelen/acties/processen geïmplementeerd om actie te (kunnen) ondernemen tegen/na potentiële cybersecurity incidenten. Het gaat bijvoorbeeld om een incidentrespons procedure en nood/continuïteitsplannen.	+/-
De gemeente toetst, oefent en evalueert deze maatregelen/acties/processen periodiek (zoals het oefenen van een cyberaanval).	+/-
De rollen en verantwoordelijkheden van functionarissen, directie en raad zijn vastgelegd en in de praktijk bekend.	+/-

De gemeente heeft verschillende procedures ingericht om te kunnen acteren bij een incident, zoals een uitwijkprocedure en een incidentenprocedure. Daarnaast heeft de gemeente een crisisplan en -organisatie die regelmatig oefeningen uitvoert. Tijdens de onderzoeksperiode is een oefening met een informatiebeveiligingsincident uitgevoerd.

De gemeente heeft geen actueel continuïteitsplan, wat een risico oplevert voor de reactie op incidenten. Er worden wel acties ondernomen om een nieuw continuïteitsplan op te stellen, mede gebaseerd op het continuïteitsplan dat voor Covid-19 is gemaakt.

Meldingen over kwetsbaarheden worden geregistreerd en opgevolgd, bijvoorbeeld met een beveiligingsupdate.

De beschrijving van rollen en verantwoordelijkheden van functionarissen is niet altijd expliciet aanwezig en kan nog duidelijker, bijvoorbeeld als het gaat om de rol van security officer bij de afdelingen. De afspraken over de rol van de raad en de informatievoorziening aan de raad over informatiebeveiliging en digitale weerbaarheid zijn niet duidelijk.

Herstel (Recover)	Beoordeling
De gemeente werkt planmatig aan weerbaarheid en is voorbereid op activiteiten ten behoeve van herstellen van processen en dienstverlening.	+/-
Incidenten op het gebied van informatiebeveiliging of cybersecurity worden geëvalueerd en leiden tot structurele verbetermaatregelen.	+

De gemeente heeft een goed werkend proces om risico's op het gebied van informatiebeveiliging te beheersen en te verbeteren. De gemeente werkt systematisch en gestructureerd aan de implementatie van beleid en maatregelen en daarmee aan de weerbaarheid van haar informatiesystemen.

De gemeente heeft een overkoepelend jaarplan voor informatiebeveiliging waar de belangrijkste activiteiten die (gemeentebreed) moeten worden uitgevoerd genoemd staan. Voor zover is vastgesteld liggen er geen specifieke risicobeoordelingen aan het jaarplan ten grondslag. Pas recent is besloten om hierover periodiek te rapporteren aan het management. Twee afdelingen binnen de gemeente hebben een eigen jaarplan voor informatiebeveiliging (de overige afdelingen hebben dit niet).

De gemeente heeft in beeld welke maatregelen uit de BIO al zijn geïmplementeerd en welke nog moeten worden geïmplementeerd en werkt dit ook periodiek bij. Te implementeren maatregelen of

beveiligingsactiviteiten zijn onderdeel van een jaar- of verbeterplan. De afdeling IAF heeft een standaard wijzigingsproces om verbetermaatregelen (vaak projectmatig) door te voeren.

Informatiebeveiligingsincidenten worden regelmatig binnen afdelingen besproken en geëvalueerd, met als doel deze in de toekomst te voorkomen.

Algemeen	Beoordeling
De raad wordt periodiek geïnformeerd over de digitale weerbaarheid van de gemeente en de ontwikkelingen op dat vlak.	-
De informatieverstrekking aan de raad biedt de raad voldoende mogelijkheden om de sturende en controlerende verantwoordelijkheden waar te maken.	-

De informatievoorziening aan de raad is over het algemeen beperkt tot het jaarverslag van de gemeente. In het jaarverslag is een paragraaf over informatiebeveiliging opgenomen. Ook de collegeverklaring (op basis van de ENSIA-audit) wordt aan de raad gestuurd.

Het onderwerp digitale weerbaarheid of informatiebeveiliging staat zeer beperkt op het netvlies van de raad. Er worden weinig tot geen vragen gesteld over het onderwerp (zowel naar aanleiding van de collegeverklaring of vanwege een losstaande aanleiding). Incidenten op het gebied van informatiebeveiliging is voor de raad wel aanleiding om het onderwerp te agenderen.

Er is geen protocol aanwezig dat aangeeft wanneer en op welke wijze de gemeenteraad geïnformeerd wordt over incidenten.

De raad heeft de behoefte geuit om vaker geïnformeerd te willen worden over het onderwerp door middel van bijvoorbeeld informatieve raadsbijeenkomsten.

Algemeen	Beoordeling
De maatregelen die de gemeente neemt worden periodiek getoetst, geoefend en/of geëvalueerd.	+/-

De gemeente toetst de aanwezigheid en effectieve werking van maatregelen op verschillende manieren. Jaarlijks wordt de ENSIA-audit uitgevoerd. De crisisorganisatie van de gemeente voert regelmatig oefeningen uit en heeft tijdens de onderzoeksperiode een oefening met een informatiebeveiligingsincident uitgevoerd. IAF test de uitwijkprocedure jaarlijks en is voornemens om periodiek een penetratietest uit te voeren.

5.2 Conclusies

5.2.1 Beantwoording onderzoeksvragen

Op basis van de beoordeling van het normenkader en de bevindingen van het onderzoek worden hieronder de onderzoeksvragen beantwoord. Eerst worden de deelvragen beantwoord, daarna wordt de hoofdvraag beantwoord.

Deelvraag 1: Hoe weerbaar zijn de digitale systemen van de gemeente Hardenberg tegen cybercriminaliteit?

De gemeente heeft een goed werkend proces om risico's op het gebied van informatiebeveiliging te beheersen en te verbeteren. Dat betekent niet dat alle benodigde maatregelen (uit de BIO) geïmplementeerd zijn, maar wel dat de gemeente systematisch en gestructureerd werkt aan de implementatie van maatregelen en daarmee aan de weerbaarheid van haar informatiesystemen. In het algemeen kan worden gesteld dat de gemeente processen en informatiesystemen beveiligd heeft conform de geldende normenkaders (specifiek de BIO), en dat daar waar nog niet aan het normenkader wordt voldaan er inzichtelijk is welke verbeteringen er nodig zijn. Via jaar- en verbeterplannen worden deze maatregelen geïmplementeerd.

De gemeente werkt aan een aantal technische maatregelen en beveiligingsactiviteiten die van belang zijn voor een digitale weerbaarheid die past bij de dreigingen van bijvoorbeeld cybercriminaliteit. Enkele voorbeelden hiervan zijn de verdere segmentering van het netwerk (wat de impact van aanvallen kan verkleinen) en monitoring van de systemen van de gemeente (om aanvallen te detecteren). De gemeente heeft nog geen penetratietest uitgevoerd op haar systemen. Dit betekent dat de informatiesystemen van de gemeente op dit moment niet voldoende getoetst zijn op eventuele kwetsbaarheden van buitenaf. Zonder een penetratietest uit te voeren is niet volledig vast te stellen hoe weerbaar de systemen van de gemeente zijn tegen aanvallen van buitenaf. De gemeente is wel voornemens om periodiek een penetratietest uit te voeren.

Als het gaat om organisatorische maatregelen ten behoeve van de weerbaarheid van de processen en systemen, kan op basis van het onderzoek worden geconcludeerd dat – ten minste in de twee onderzochte processen – er diverse maatregelen aanwezig zijn om de betrouwbaarheid van informatie te garanderen. Daarbij is wel een kanttekening te plaatsen: de onderzochte processen zijn zo ingericht dat er sterk geleund lijkt te worden op het vertrouwen in medewerkers (ten opzichte van een formelere inrichting van processen). Er zijn op dit vlak geen expliciete risico-afwegingen gemaakt. Ook zijn er voor de belangrijkste processen geen specifieke risicoanalyses uitgevoerd om in detail risico's en te nemen maatregelen in kaart te brengen.

Deelvraag 2: Hoe beveiligingsbewust zijn de medewerkers van de gemeente Hardenberg als het gaat om persoonsgegevens en andere informatie?

De gemeente investeert veel in het beveiligingsbewustzijn van de medewerkers. Van hoog tot laag in de organisatie moeten medewerkers deelnemen aan trainingen iBewustzijn. Tijdens het onderzoek kwam naar voren dat afdelings- en teammanagers in de werkoverleggen regelmatig het onderwerp informatiebeveiliging aan de orde stellen. Dat kan in algemene zin zijn, of vanwege nieuwsberichten of kleine incidenten die zich hebben voorgedaan.

In het algemeen concluderen wij dat het informatiebewustzijn hoog is. Daarbij is ook sprake van een groot vertrouwen in de medewerkers van de gemeente. Wel kan er nog meer aandacht aan het onderwerp gegeven worden in relatie tot thuiswerken. Het meenemen van dossiers naar huis en de toegang tot de systemen van de gemeente is een risico.

Deelvraag 3: Hoe is de gemeente voorbereid in het geval van mogelijke incidenten?

De gemeente heeft verschillende maatregelen en procedures ingericht om voorbereid te zijn op mogelijke (grote) beveiligingsincidenten. Ook worden deze regelmatig getoetst of geoefend. Zo heeft de gemeente een incidentenprocedure en melden medewerkers ook met regelmatig incidenten die opgevolgd en wanneer nodig besproken worden. De gemeente heeft daarnaast een uitwijkplan welke periodiek (voor het eerst in 2020) getest wordt. Ook heeft de gemeente een crisisorganisatie die regelmatig een oefening uitvoert. Tijdens de onderzoeksperiode is geoefend met een beveiligingsincident.

Een hiaat in de voorbereiding van de gemeente is de aanwezigheid van een actueel continuïteitsplan (en het oefenen daarvan). Tijdens de onderzoeksperiode werd nog aan een (nieuw) continuïteitsplan gewerkt.

Al met al kan geconcludeerd worden, dat de gemeente de belangrijkste voorbereidingen heeft genomen en werkt aan verbeteringen waar dat nodig is.

Deelvraag 4: Waar liggen de grootste risico's en hoe kan de gemeente Hardenberg hierin verbeteringen aanbrengen?

In het onderzoek zijn een aantal risico's op het vlak van informatiebeveiliging naar voren gekomen die breed in de gemeente van toepassing zijn.

Een belangrijk risico ligt op het vlak van veilig gedrag door medewerkers (bewust of onbewust foutief handelen). Processen zijn soms zodanig ingericht dat er meer ruimte voor fouten is dan nodig. De gemeente hanteert veelal het uitgangspunt van vertrouwen in de medewerkers. Hoewel het beveiligingsbewustzijn in de gemeente op peil is (zie deelvraag 2), is het altijd mogelijk dat een menselijke fout of bewust handelen van een medewerker zorgt voor verstoring van de dienstverlening of aantasting van de betrouwbaarheid van processen en informatie. De gemeente heeft verder geen risicoanalyses uitgevoerd voor de belangrijkste processen om zo op detailniveau te onderbouwen welke maatregelen er nodig zijn om het gewenste betrouwbaarheidsniveau te garanderen.

Een tweede risico betreft de technische maatregelen die de gemeente heeft genomen ten behoeve van de weerbaarheid van systemen (zie ook deelvraag 1). Op dit vlak zijn er nog verschillende verbeteringen mogelijk die vaak al in gang zijn gezet, maar nog niet zijn ingericht. Specifiek het periodiek uitvoeren van penetratietesten op de systemen en infrastructuur van de gemeente is van belang om inzicht te krijgen in de kwetsbaarheden.

Een derde risico betreft het inzicht in de maatregelen die leveranciers en ketenpartners van de gemeente op het gebied van informatiebeveiliging hebben genomen. De gemeente heeft nog niet op alle vlakken dit inzicht en het is niet zeker of er bij leveranciers kwetsbaarheden bestaan die de dienstverlening van de gemeente kunnen schaden in het geval van een aanval of een verstoring.

Andere risico's die naar voren gekomen zijn, bevinden zich op het vlak van thuiswerken (in combinatie met gevoelige/vertrouwelijke informatie, bijvoorbeeld over burgers), schaduwadministraties en de afwezigheid van een continuïteitsplan.

Deelvraag 5: Welke controle- en sturingsmogelijkheden heeft de gemeente(raad) bij informatiebeveiliging en worden deze ook gebruikt?

Het jaarverslag met de collegeverklaring over informatiebeveiliging is het belangrijkste controle- en sturingsinstrument van de gemeenteraad. Deze wordt jaarlijks aan de gemeenteraad gestuurd, maar in het onderzoek is niet gebleken dat dit tot vragen of discussie is gekomen. De gemeenteraad stelt weinig tot geen vragen over het onderwerp. Een beveiligingsincident binnen de gemeente wordt daarbij genoemd als de belangrijkste aanleiding om het onderwerp te agenderen. Daarbij is het wel van belang dat de informatievoorziening over incidenten aansluit bij de vertrouwelijkheid die dat vereist, met een rol voor het presidium of een besloten commissievergadering. Er is op dit moment geen protocol dat beschrijft wanneer en op welke wijze de raad over incidenten geïnformeerd wordt.

Tijdens de raadsledenbijeenkomst is een behoefte aan meer kennis en informatie over het onderwerp geuit tijdens het onderzoek. Dit zou kunnen via een informatieve raadsbijeenkomst. Van deze mogelijkheid is recentelijk geen gebruik gemaakt.

5.2.2 Hoofdconclusie

Met de beantwoording van de deelvragen kan ook de centrale onderzoeksvraag worden beantwoord:

Hoe goed zijn de persoonsgegevens en andere informatie van de gemeente Hardenberg beschermd tegen cybercriminaliteit én hoe is de gemeente voorbereid op een mogelijk beveiligingsincident?

De gemeente heeft een vrij goed werkend proces om persoonsgegevens en andere informatie te beschermen tegen bedreigingen zoals cybercriminaliteit. In dit proces is aandacht informatiebeveiligingsbeleid, specifieke risico's, veilig gedrag van medewerkers, technische beveiliging en audits en externe onderzoeken. Daar waar verbeteringen mogelijk zijn in het nemen van beveiligingsmaatregelen, heeft de gemeente deze over het algemeen geborgd in jaar- en verbeterplannen, in lopende acties of in concrete voornemens. De algemene conclusie van dit onderzoek is dan ook dat de gemeente op hoofdlijnen haar informatiebeveiliging op orde heeft.

Wel zijn er tijdens het onderzoek een aantal aandachtspunten naar voren gekomen die een risico kunnen vormen voor de digitale weerbaarheid van de gemeente.

- **Er is geen ambitieniveau op bestuurlijk niveau vastgesteld.** Een ambitie geeft richting voor de verbeteringen en ontwikkelingen op het gebied van informatiebeveiliging, maakt duidelijk wat de risicobereidheid van de gemeente is en geeft aan welke speerpunten aan gewerkt moet worden. In bredere zin zijn er op bestuurlijk niveau binnen de gemeente geen expliciete afwegingen gemaakt met betrekking tot digitale weerbaarheid en risicobereidheid.

  Gerelateerd hieraan is de beperkte formele verantwoording en rapportage richting het management, het college en de gemeenteraad. In 2021 is het onderwerp informatiebeveiliging onderdeel geworden van de kwartaalrapportage aan de directie, maar daarvoor was deze rapportage er niet. Dit maakt het voor directie, college en gemeenteraad moeilijk om te sturen op de risico's op het gebied van informatiebeveiliging. De gemeente heeft met het in te voeren dashboard voor informatiebeveiliging wel ambities op dit vlak.

- **De rol van de gemeenteraad is in de praktijk beperkt en er is geen protocol voor het informeren van de raad bij incidenten.** Het risico is dat de gemeenteraad haar controlerende en kaderstellende taak niet goed kan uitoefenen als het gaat om informatiebeveiliging. Er is ook een kennisbehoefte bij de raad geconstateerd.
- **Het strategisch informatiebeveiligingsbeleid heeft een vrij algemeen karakter,** met het risico dat het beleid, de verschillende rollen en verantwoordelijkheden en de verantwoording- en rapportagecyclus onduidelijk is.
- **Er is relatief weinig aandacht voor organisatorische maatregelen met betrekking tot uitvoerende processen**. De aandacht van uitvoerende afdelingen richt zich in belangrijke mate op het veilig gedrag van medewerkers. Dit is belangrijk en de gemeente investeert hier duidelijk in. Het is echter ook van belang dat er daarnaast in de uitvoerende processen aandacht wordt besteed aan organisatorische maatregelen om te zorgen dat de dienstverlening van de gemeente betrouwbaar is. De security officers van de afdelingen hebben een belangrijk rol om het lijnmanagement ,dat de aandacht over veel verschillende onderwerpen moet verdelen, hierin te ondersteunen en adviseren.
- **De gemeente heeft nog geen penetratietest uitgevoerd.** Een penetratietest is onontbeerlijk om inzicht te krijgen in de kwetsbaarheden in de systemen van de gemeente. Een finale uitspraak over de digitale weerbaarheid van de gemeente kan enkel gedaan worden na een gedegen penetratietest en de gemeente heeft deze nog niet laten uitvoeren. Er is wel een concreet voornemen om dit te gaan doen, wat het risico (in afwachting van de resultaten en opvolging van de penetratietest) beperkt.

5.2.3 Conclusies in bredere context

Voordat wordt overgegaan tot de aanbevelingen vinden wij het nuttig om kort stil te staan bij de bredere context waarin de beantwoording van de onderzoeksvragen en de beoordeling van de normen geplaatst kunnen worden.

De conclusies van dit onderzoek zijn, op de hierboven genoemde kanttekeningen na, positief. Dit onderzoek schetst het beeld dat de gemeente Hardenberg de beveiliging van informatie op orde heeft en daar waar verbeteringen mogelijk zijn deze in beeld heeft en veelal al in gang heeft gezet.

De bedreigingen op het gebied van informatiebeveiliging worden echter steeds groter. Het Cybersecuritybeeld Nederland 2021 van het Nationaal Cyber Security Centrum (NCSC) stelt dat digitale risico's onverminderd groot zijn en steeds zullen toenemen. Dit zal in de toekomst steeds meer van gemeenten vragen op het gebied van informatiebeveiliging. Daar waar de beheersing van informatiebeveiliging nu op orde is, kan dat ook snel veranderen. Daarnaast laten incidenten zoals die in de gemeente Hof van Twente zien dat grote incidenten altijd kunnen voorkomen.

5.3 Aanbevelingen

Uit het onderzoek is gebleken dat de gemeente als een aantal zaken ter verbetering van de digitale weerbaarheid in gang heeft gezet, maar nog niet heeft afgerond. Bovenop de lopende verbeteracties geven we in deze paragraaf een aantal aanbevelingen om de digitale weerbaarheid nog verder te verbeteren.

In lijn met de conclusie in bredere context is het belangrijk om blijvend te investeren in informatiebeveiliging en het verbeteren van digitale weerbaarheid. In lijn met de bevindingen en conclusies formuleren we de volgende aanbevelingen, waarbij we een aantal aandachtspunten meegeven die uit het onderzoek voortkomen:

1. Werk het informatiebeveiligingsbeleid verder uit en spits dit meer toe op de gemeente Hardenberg

Het informatiebeveiligingsbeleid is nu algemeen opgesteld en vooral gebaseerd op de BIO. Aanbevolen wordt om het specifieker te maken op de gemeente Hardenberg, bijvoorbeeld op de volgende punten:.

- Formuleer een ambitie op het gebied van informatiebeveiliging en koppel de risicobereidheid van de gemeente aan deze ambitie.
- Onderdeel van het informatiebeveiligingsbeleid is tenminste een risico-gestuurde aanpak. Een flexibele en dienstverlenende gemeentelijke organisatie brengt ook risico's met zich mee op het gebied van informatiebeveiliging. Risico's moeten voldoende beheerst worden, wat betekent dat een risico-gestuurde aanpak essentieel is. Dat houdt in dat de gemeente voor de lopende processen en huidige systemen, maar ook bij veranderingen een expliciete risico-afweging maakt en aangeeft welke risico's het bereid is te accepteren.
- Daarnaast adviseren we om goede afspraken te maken over het periodiek en incidenteel rapporteren aan het CMT, het college van B&W en de gemeenteraad. Periodieke rapportages bevatten tenminste een terugblik op de afgelopen periode (incidenten, verbeteracties) en een vooruitblik naar de komende periode. Incidentele rapportages zijn vooral van belang bij beveiligingsincidenten, waarbij niet alleen rapportage achteraf (hoe is het opgelost, wat waren de gevolgen?), maar ook snel na het ontdekken van een beveiligingsprobleem belangrijk is. We adviseren een communicatieplan met een escalatieladder op te stellen.
- Tot slot bevelen we aan om de taken en verantwoordelijkheden van de security officers bij de verschillende afdelingen te beschrijven en waar deze nog vacant zijn in te vullen.

Het beleid kan opgesteld worden aan de hand van de ervaringen van de laatste paar jaar. Een update van het volwassenheidsonderzoek kan bijdragen aan het komen tot een nieuwe baseline en een expliciete ambitie.

2. Richt de rol van de gemeenteraad op het gebied van informatiebeveiliging in

De rol van de gemeenteraad op het gebied van informatiebeveiliging blijkt in de praktijk niet helder. Zowel ten aanzien van kaderstelling, controle als ten aanzien van de informatievoorziening kan de positie van de raad worden verbeterd.

Ten eerste adviseren we om wellicht nog met de huidige raad, maar zeker met de nieuwe gemeenteraad een informele, informatieve bijeenkomst te organiseren, waarin de raadsleden worden geïnformeerd over de actuele stand van zaken met betrekking tot informatiebeveiliging en digitale weerbaarheid. Daarbij kan aanvullend aandacht worden besteed aan het veilig werken door raadsleden.

Ten tweede adviseren we een protocol vast te stellen waarin helder is aangegeven wanneer de gemeenteraad wordt geïnformeerd over beveiligingsincidenten. Onderdeel van het protocol is tenminste een beschrijving over het moment waarop de raad wordt geïnformeerd, of de informatie aan de commissie, de gehele raad of het presidium wordt verstrekt en over welke incidenten de raad wordt geïnformeerd.

Tot slot adviseren we om het onderwerp "informatiebeveiliging en digitale weerbaarheid" tenminste twee keer per jaar te agenderen op de agenda van de gemeenteraad. We stellen voor om in aansluiting op het overleg over de begroting te spreken over ambitie, kaders en jaarplan. En in het voorjaar een

terugblik te geven op ervaren problemen en incidenten, de reactie en het herstelvermogen van de gemeente.

3. Neem aanvullende risico-mitigerende maatregelen

Op basis van de bevindingen uit dit onderzoek adviseren we om invulling te geven aan een aantal specifieke risico-mitigerende maatregelen:

- Het periodiek laten uitvoeren van penetratietesten.
- Het met ketenpartners, die gegevens uit de gemeentelijke registratie gebruiken, maken van afspraken over informatiebeveiliging en de controle daarop.
- Het uitvoeren van uitgebreide risicoanalyses voor het thuiswerken en de belangrijkste processen en systemen van de gemeente, om zo te komen tot het treffen van specifieke maatregelen per proces of afdeling.
- Het blijvend onder de aandacht brengen van het (beveiligings-) incidentmanagement proces en het stimuleren dat incidenten ook worden gemeld.

4. Blijf informatiebeveiliging onder de aandacht van medewerkers en management brengen

Het is belangrijk om medewerkers, het college en de gemeenteraad voortdurend bewust te maken en en alert te houden ten aanzien van informatiebeveiliging en de risico's. We bevelen dan ook aan het bewustzijnsprogramma voort te zetten en te sturen op actieve deelname van iedereen. Het opstellen van specifiek beleid voor de gemeente Hardenberg (aanbeveling 1) kan een aanleiding zijn om vanuit het CMT de (hernieuwde) ambitie uit te dragen. We adviseren daarnaast om tenminste één keer per jaar, bijvoorbeeld in het kader van Alert Online / Cyber security month intensief aandacht te besteden aan veilig gedrag met verschillende activiteiten en communicatiemiddelen.

Bijlage A Geïnterviewde personen

Datum	Naam	Functie
17 mei 2021	Leon Post	CISO
17 mei 2021	Ida Oostmeijer	Gemeentesecretaris
17 mei 2021	Conrad Joren	Teamleider Finance & Control
17 mei 2021	Wilma van den Brink - Hendriks	Concernmanager bedrijfsvoering
18 mei 2021	Lambert van den Berg	Coördinator ICT
18 mei 2021	Albert Knol	Teamleider Werk en Inkomen
18 mei 2021	Sandra de Weerd - Bredenhoff	Teamleider Burgerzaken
18 mei 2021	Maarten Offinga	Burgemeester/Portefeuillehouder Informatiebeveiliging
25 mei 2021	Jolly Lucardie	Teamleider IAF
27 mei 2021	Fred Bouma	Teamleider Vergunningen, Toezicht en Handhaving

Bijlage B Bestudeerde documentatie

Documentnaam	Toelichting	Datum
Collegeverklaring ENSIA 2020 inzake Informatiebeveiliging DigiD en Suwinet Hardenberg	Bijlage	April 2021
iBewustzijn Communicatie		
Campagne iBewustzijn - Informatieveiligheid		
Assuranceverklaring ENSIA 2019 - Hardenberg		April 2020
Assuranceverklaring ENSIA 2020 - Hardenberg		April 2021
BBV Collegevoorstel: Verklaring ENSIA 2020 Hardenberg (vergaderversie)		April 2021
Collegeverklaring ENSIA 2020 Hardenberg	Bijlage	April 2021
Collegeverklaring ENSIA 2019 inzake Informatiebeveiliging Suwinet Hardenberg	Bijlage	April 2020
Collegeverklaring ENSIA 2020 Hardenberg	Bijlage	April 2021
CMT voorstel: Bevorderen iBewustzijn/ informatie-veiligheid (vergaderversie)		Januari 2021

Collegeverklaring ENSIA 2019 Hardenberg		April 2020
Contactlijst met instellingen en beroepsverenigingen		
Cyber risico's		
Dataclassificatie		Q2 2021
Informatiebeveiliging Hardenberg ENSIA zelfevaluatie		September 2019
GAP BIO 2020 Q1		Q1 2020
GAP BIO 2020 Q2		Q2 2020
GAP BIO 2020 Q4		Q4 2020
GAP BIO 2021 Q1		Q1 2021
Incidentmanagement procesbeschrijving		September 2019
Infographic Hardenberg resultaten nulmeting		
Jaarplan Informatiebeveiliging IAF 2019	Versie 1.1	September 2019
Jaarplan Informatiebeveiliging IAF 2020	Versie 1.1	April 2020
Jaarplan Informatiebeveiliging PD 2020	Versie 1.1	Februari 2020
CMT: Opdrachtbeschrijving Bedrijfscontinuïteitcyclus en crisisoefening		
Presentatie Incidentmanagement		
Rapportage mystery guest Hardenberg		April 2019
Rapport BIO Informatiebeveiliging 2020 Hardenberg: ENSIA zelfevaluatie		
Security Maturity Assessment Report Gemeente Hardenberg		September 2019
Strategisch Gemeentelijk Informatiebeveiligingsbeleid (GIBB)		Oktober 2019
Uitwerking i-Visie		
Uitwijk en inwijk draaiboek		
Jaarplan In Control 2020-2021: Gegevensbescherming, Informatiebeveiliging en Concern control		
Meldingen register		

Bijlage C Niet openbaar

C. 1 Resultaten nulmeting iBewustzijn

C. 2 Resultaten Security Maturity Assessment door SecureLink

C. 3 Casusbesprekingen

Bijlage D Lijst met afkortingen en begrippen

Afkorting	Betekenis
AVG	Algemene Verordening Gegevensbescherming
BBN	Basisbeveiligingsniveau (1 – 3)
BIG	Baseline Informatiebeveiliging Gemeenten
BIO	Baseline Informatiebeveiliging Overheid
CISO	Chief Informatie Security Officer
ENSIA	Eenduidige Normatiek Single Information Audit
GeVS	Gezamenlijke Elektronische Voorzieningen Structuur
GGI	Gemeentelijke Gemeenschappelijke Infrastructuur
IBD	Informatiebeveiligingsdienst Gemeenten (VNG Realisatie)
ICT	Informatie- en Communicatie Technologie
FG	Functionaris Gegevensbescherming
ISMS	Information Security Management System
PDCA	Plan-Do-Check-Act
SIEM	Security Information & Event Management
SO	Security Officer
SOC	Security Operations Center

Begrip	Betekenis
Cybercriminaliteit	Doelbewust van binnenuit of buitenaf inbreuk maken op informatiesystemen van een organisatie met als doel financieel gewin of verstoren.
DDoS aanval	Een Distributed Denial of Service (DDoS) aanval is een aanval gericht op sabotage of verstoring van informatiesystemen waardoor deze (tijdelijk) niet meer beschikbaar zijn.
Informatiebeveiliging	Het proces van vaststellen van de vereiste beveiliging van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.
Malware	Kwaadwillende software dat informatiesystemen probeert te verstoren.
Phishing aanval	Een aanval waarbij de aanvaller zich voordoet als iemand anders (een persoon of organisatie) met als doel persoonsgegevens of inloggegevens te vergaren.

Ransomware	Ook wel gijzelsoftware genoemd. Blokkeert het gebruik van een systeem of data via versleuteling met als doel losgeld te ontvangen.