Bezoekadres
Mien Ruysweg 1
9408 KA Assen

Postadres
Postbus 144
9400 AC Assen

T 0592 - 30 63 00
F 0592 - 31 42 48
E info@ggddrenthe.nl
I www.ggddrenthe.nl

Aan de raden van de Drentse gemeenten
t.a.v. de Raadsgriffier

Datum	14 april 2022
Ons kenmerk	U220063/GM/RW
uw kenmerk	
Behandeld door	G. Meijer
Onderwerp	Begrotingswijziging voor beleidsimpuls GGD

Geachte gemeenteraad,

Tijdens haar vergadering van 11 april 2022 heeft het algemeen bestuur van GGD Drenthe voorlopig ingestemd met de inhoudelijke en financiële bijdrage van de GGD aan een verbeterplan informatieveiligheid & privacy.
De structurele kosten gelden vanaf 2022 en zijn verwerkt in de concept-begroting 2023. Middels de voorliggende brief vragen wij uw zienswijze in te dienen over de wijziging van de begroting 2022 voor de eenmalige bijdrage van € 75.000,- en de structurele bijdrage van € 240.000,-. Graag ontvangen wij uw zienswijze tegelijkertijd met uw zienswijze op de separaat verzonden ontwerpbegroting 2023, uiterlijk 10 juni a.s.

Gezamenlijke invulling VRD en GGD

De Veiligheidsregio Drenthe en de GGD Drenthe kiezen voor een gezamenlijke invulling van de informatievoorziening binnen de beide organisaties. VRD en GGD delen expertise, infrastructuur en andere middelen om een goede informatievoorziening mogelijk te maken.

Informatievoorziening heeft uiteraard betrekking op de eigen bedrijfsvoering van de beide organisaties, maar beide organisaties hebben ook een belangrijke plaats voor informatievoorziening in hun strategische agenda ingeruimd. Kennisintensief, data-gestuurd en met een lerende organisatie geven beide organisaties invulling aan hun maatschappelijke taken.

Hoewel de taken voor de VRD en GGD verschillend zijn, is er wel een belangrijke overeenkomst in de maatschappelijke opgave waar beide organisaties voor staan. In de afgelopen periode is meer duidelijk geworden dat het streven naar een gezond en veilig Drenthe voor de VRD en GGD leidt tot meer samenwerking en afstemming. Het samenvoegen en gezamenlijk inzetten van elkaars faciliteiten is in dat verband niet alleen logisch, maar ook noodzakelijk geworden. Een gezamenlijke informatievoorziening maakt daar onderdeel van uit.

Om de maatschappelijke taken van de VRD en GGD met behulp van informatievoorziening uit te kunnen voeren is een goede beveiliging van deze informatievoorziening nodig. In dit voorstel wordt op de beveiliging van de informatievoorziening binnen de VRD en GGD ingegaan. Daarnaast zal bijzondere aandacht worden gegeven aan de bescherming van privacy, wat voor de GGD belangrijk is gelet op de verwerking van grote persoonsgerichte informatie in het zorgdomein.

Vertrekpunt

Net als alle andere organisaties heeft de VRD/GGD uiteraard al lange tijd maatregelen getroffen voor het beveiligen van onze informatiesystemen en informatie. Gebruikersidentificatie, autorisatie, virusscanning, netwerkmonitoring, toegangsbeveiliging zijn allemaal maatregelen die in de afgelopen jaren gemeengoed zijn geworden en zijn ook gedurende de afgelopen periode effectief geweest.

Het is echter duidelijk merkbaar dat de situaties van misbruik of oneigenlijk gebruik van onze informatie en informatiesystemen, of de poging daartoe, toenemen. Daarbij gaat het om het aantal situaties, maar ook over het raffinement van het misbruik of oneigenlijk gebruik. Diefstal van data uit onze informatiesystemen door medewerkers, geautomatiseerde pogingen om toegang te krijgen tot onze netwerken en systemen, nepmails of nepsites bedoeld om de digitale identiteit van medewerker te verkrijgen, en het plaatsen van software om schade om systemen te kunnen ‘gijzelen’ zijn zeer realistische dreigingen geworden. Dreigingen waar overigens niet alleen de VRD/GGD mee te maken heeft, maar vrijwel iedere organisatie of persoon die gebruik maakt van computers of informatie. Digitale criminaliteit is onderdeel geworden van onze maatschappij en leidt tot bijzonder grote risico's op het gebied van continuïteit en hoge kosten om de gevolgen van verstoring op te kunnen heffen.

De VRD en GGD realiseren zich goed dat onze informatiesystemen en informatie van waarde kunnen zijn voor criminaliteit. Dagelijks zijn wij succesvol in het pareren van pogingen tot misbruik, we delen in de ervaringen die collega-veiligheidsregio’s en GGD-en, hebben opgedaan met misbruik en uiteraard hebben de situaties van datadiefstallen uit de landelijke informatiesystemen die gebruikt worden voor de werkzaamheden ten behoeve van Covid onze organisatie op scherp gezet.

Om een goed beeld te krijgen van het huidige niveau van onze beveiliging hebben wij met behulp van ons framework, audit en self-assessments de huidige situatie geïnventariseerd. Dit beeld leidt direct tot de conclusie dat de informatiebeveiliging van de VRD en GGD niet op orde is in relatie tot de landelijke normen, maar ook in relatie tot juist toepassen van interne procedures. Het juiste gebruik van privacygevoelige gegevens is onvoldoende gewaarborgd. Bovendien werd duidelijk dat de trend om steeds meer informatiesystemen als een internetdienst af te nemen in plaats van zelf in eigendom te hebben nieuwe

complicaties oplevert. Aanvullende maatregelen zijn nodig, die wij hierbij presenteren onder de noemer ‘Verbeterplan informatieveiligheid en privacy’.

Framework

Voor de inrichting van de beveiliging van informatie en informatiesystemen hebben we een framework opgesteld, dat wij hanteren als normenkader voor de beveiliging van onze informatievoorziening. Dit framework bestaat uit de volgende onderdelen:

- We maken gebruik van het kwadrantenmodel (zie bijlage 1 voor toelichting).
- We sluiten aan bij initiatieven op landelijk niveau van de veiligheidsregio’s en GGD/ GHOR zoals vastgesteld in het Veiligheidsberaad en de DPG-raad.
- We worden compliant aan BIO en NEN7510.
- We voldoen aan de privacybescherming van burgers en personeel op grond van de AVG.
- We verhogen onze weerbaarheid.
- We gaan van ad hoc en eenmalig naar gestructureerd en geprioriteerd werken aan informatieveiligheid en richten daar onze organisatie op in.

In bijlage 1 is een toelichting opgenomen van de verschillende onderdelen van het framework dat wij hanteren.

Situatieschets: uitkomsten audits en self-assessment

Voor een analyse van de huidige staat van onze informatiebeveiliging maken wij gebruik van audits en self-assessment die wij in de afgelopen periode hebben laten uitvoeren. Dit zijn de volgende:

- Collegiale audit veiligheidsregio’s Nederland (M&I Partner, april 2019);
- Audit Informatiesystemen GGD (We do trust, juni 2021);
- Self-assessment implementatie BIO (september 2021).

Elk van deze onderzoeken had een eigen onderzoeksvraag en daarmee ook een afzonderlijke en specifieke uitkomsten die in rapportages zijn vastgelegd. Duidelijk daarbij is ook dat een aantal bevindingen in vrijwel elk onderzoek terugkomt, we kiezen ervoor om deze bevindingen prioriteit te geven in ons verbeterplan. Sterk samengevat gaat het om de bevindingen op de volgende onderwerpen:

- risicoanalyse en classificatie;
- bewustzijnsniveau;
- authenticatie;
- autorisatie;
- logging;
- back-end systemen;
- koppelingen en gegevensuitwisseling.

Verbeterplan: de maatregelen

Voor het realiseren van de verbetering van de beveiliging van onze informatie en informatiesystemen richten wij ons op vier onderdelen:

- implementatie van BIO en NEN 7510;
- inrichting organisatie;
- technische voorzieningen;
- evalueren en leren.

Ad 1 Implementatie van BIO en NEN 7510
Gelet op de tekortkomingen binnen de VRD en GGD op het gebied van informatievoorziening is het voor de hand liggend de verbetermaatregelen te baseren op de BIO en de NEN 7510. Aan de hand van het self-assessment leidt dit ertoe dat er in totaal 109 acties uitgevoerd moeten worden om uiteindelijk compliant te worden aan de BIO.

In bijlage 2 is een samenvatting opgenomen van de acties die wij benoemd hebben. Voor de uitvoering maken wij gebruik van de organisatie die wij nu beschikbaar hebben. Concreet betekent dit dat wij de acties kunnen verdelen over verschillende actiehouders en een verdeling van de acties over de kwartalen hebben gemaakt. Ons doel is de implementatie van de BIO aan het eind van 2022 af te ronden.
Gelet op de verwerking van privacygevoelige data binnen met name de GGD hechten wij zeer aan waarborgen voor een juiste omgang met deze data. Daarom hebben wij de eisen van de BIO waar nodig aangevuld met de normen uit de NEN 7510. Onze acties voorzien er in dat wij eind 2022 ook voldoen aan deze normen.

Ad 2 Inrichting organisatie
Zoals beschreven in ons framework, beschikken wij binnen onze organisatie inmiddels over een aantal functies specifiek voor informatiebeveiliging, waarmee we bovendien de eerste stappen hebben kunnen zetten in de gewenste functiescheiding. In het verlengde hiervan is ook een wijziging aangebracht in de verantwoordelijkheid voor de portefeuille en de wijze van aansturing. De concerncontroller is aangewezen als portefeuillehouder binnen beide MT's, en geeft leiding aan het team en de werkzaamheden.
Een aantal functies hebben wij echter nog niet kunnen realiseren, met name door het ontbreken van budget. Als onderdeel van het verbeterplan wordt nu voorgesteld deze functies alsnog in te gaan vullen, waarbij het gaat om:

- Functionaris Gegevensbescherming (uitbreiding)
- Privacy officer;
- Security officer (uitbreiding);
- Functioneel applicatiebeheer;
- System security specialist.

Voor een deel worden de werkzaamheden uit deze functies nu uitgevoerd door andere medewerkers boven op hun reguliere functie binnen beide organisaties. In praktijk betekent dit dat er onvoldoende prioriteit en capaciteit beschikbaar is.
Daarnaast is ook de belasting van medewerkers te groot, zeker ook omdat de werkzaamheden rond beveiliging van informatie niet gebonden is aan reguliere werktijden.

Ad 3 Technische voorzieningen
Voor de beveiliging van informatievoorziening wordt gebruik gemaakt van technische voorzieningen die binnen de VRD en GGD in de afgelopen jaren in gebruik zijn genomen, als onderdeel van de reguliere exploitatie van ICT-voorzieningen. Hierbij is geprofiteerd van de samenwerking tussen de VRD en GGD, beide organisaties hadden dit nooit afzonderlijk binnen de reguliere exploitatie kunnen realiseren.
Voor de komende periode staat er nog een aantal uitbreidingen van de technische voorzieningen op de planning. Met name het investeren in back-up faciliteiten zal versneld moeten worden vormgegeven, waarvoor de middelen binnen de exploitatie nu ontbreken.

Ad 4 Evalueren en leren
Rond het onderwerp informatiebeveiliging hebben wij ervaren dat het kunnen doen van onderzoek, het uitvoeren van audit en assessments cruciaal is om te kunnen evalueren en leren. Alleen zo kunnen we binnen dit vakgebied invulling geven aan de PDCA-cyclus die zowel in de BIO als bij de NEN 7510 terecht veel aandacht krijgt.
Om jaarlijks onderzoek te kunnen doen zal een budget hiervoor worden ingesteld. De portefeuillehouder zal jaarlijks aan de hand van een onderzoeksplan gericht onderzoek doen naar de kwaliteit van de informatiebeveiliging en de uitkomst daarvan omzetten in aanpassingen en verbeteringen.

Financiën

Voor de uitvoering heeft de GGD meer budget nodig dan nu beschikbaar is. Daarom is het nodig dat het budget van de GGD hiervoor wordt verhoogd door en gemeenten de inwonerbijdrage hiervoor verhogen. Gelet op de urgentie van de start van de werkzaamheden wordt gekozen voor een tussentijdse wijziging van de begroting 2022, bestaande uit een incidentele verhoging en een structurele verhoging. In de begroting 2023 is de structurele doorwerking meegenomen.

De financiële investering die nodig is voor de uitvoering van dit verbeterplan kan als omvangrijk overkomen, en in absolute zin gaat het ook om een forse financiële investering. Afgezet tegen de vervolgschade die kan ontstaan als de beveiliging van informatie of waarborgen voor privacy tekortschieten geeft dit echter een veel genuanceerder beeld. Door de grote omvang van dat informatievoorziening binnen VRD en GGD en de omvang van persoonsgevoelige informatie zullen claims van gedupeerden en continuïteitsschade al gauw een veelvoud bedragen van de investering in dit verbeterplan. Een dergelijke business-case benadering leidt dan ook tot een beter oordeel over de voorliggende investeringsvraag.

Bij het vaststellen van de jaarrekening 2021 heeft het bestuur van de GGD besloten het batig rekeningsresultaat voorlopig te reserveren. Uit deze reservering zouden gemeenten de jaarlast 2022 kunnen dekken, zodat de verhoging van de inwonerbijdrage pas ingaat met ingang van 2023.

De gemeentelijke bijdrage neemt hierdoor met € 240.000,- structureel toe. De eenmalige kosten bedragen € 75.000,-. Voor 2022 kunnen deze gedekt worden uit de reservering bij jaarrekening 2021, voor 2023 moet dan rekening worden gehouden met de structurele stijging van € 240.000,-.

De 1e begrotingswijziging 2022 ziet er als volgt uit:

	Programma	Primitieve beleids-begroting 2022	Begrotings-wijziging 2022 e.v. structureel	Begrotings-wijziging 2022 incidenteel	Gewijzigde begroting 2022
Baten	Beschermen	3.957	0	0	3.957
	Beschermen - derden	1.991	0	0	1.991
	Bevorderen	386	0	0	386
	Bewaken	483	0	0	483
	Jeugd	11.843	0	0	11.843
	Additioneel	12.147	0	0	12.147
	Bedrijfsvoering en middelen	225	0	0	225
Totaal Baten		**31.031**	**0**	**0**	**31.031**
Lasten	Beschermen	-3.957	0	0	-3.957
	Beschermen - derden	-1.991	0	0	-1.991
	Bevorderen	-386	0	0	-386
	Bewaken	-467	0	0	-467
	Jeugd	-11.902	0	0	-11.902
	Additioneel	-11.823	0	0	-11.823
	Bedrijfsvoering en middelen	-225	-240	-75	-540
Totaal Lasten		**-30.751**	**-240**	**-75**	**-31.066**
Reserveringen	Bewaken	-15	0	0	-15
	Jeugd	59	0	0	59
	Additioneel	-324	0	0	-324
	Bedrijfsvoering en middelen	0	240	75	315
Totaal Reserveringen		**-281**	**240**	**75**	**34**
Eindtotaal		**0**	**0**	**0**	**0**

Deze wijziging leidt niet tot aan aanpassing van de gemeentelijke bijdragen in 2022.

Voor 2023 e.v. zal de begrotingswijziging o.b.v. prijspeil 2022 de volgende verhoging van de gemeentelijke bijdrage met zich mee brengen.

Overige programma's	inwoners	Aanpassing gemeentelijke bijdrage vanaf 2023
	1-1-2021	
Aa en Hunze	25.399	12.320
Assen	68.836	33.390
Borger-Odoorn	25.598	12.417
Coevorden	35.317	17.131
Emmen	107.024	51.914
Hoogeveen	55.603	26.972
Meppel	34.386	16.680
Midden-Drenthe	33.381	16.192
Noordenveld	31.214	15.141
Tynaarlo	33.978	16.482
Westerveld	19.661	9.537
De Wolden	24.374	11.823
Totaal	**494.771**	**240.000**

Tot slot
Ik hoop u door middel van deze brief voldoende geïnformeerd te hebben over dit besluit. Mocht u nog vragen hebben, dan kunt u zich hiervoor wenden tot Sjoerd de Jong, controller bij de GGD.

Met vriendelijke groet,

Namens het algemeen bestuur van GGD Drenthe

H. Vlieg-Kempe
Voorzitter GGD Drenthe

H. Kox
Secretaris

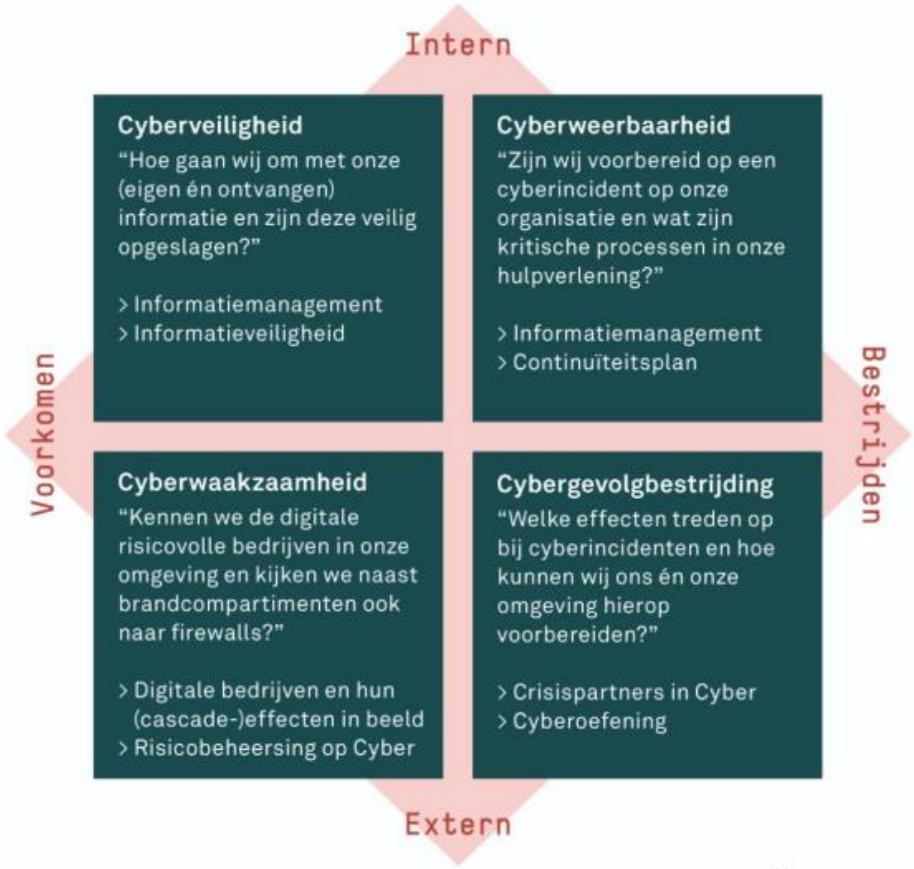
Bijlagen

Bijlage 1: Framework
Framework Veiligheid informatie & privacy

Voor de Informatiebeveiliging en het waarborgen van de privacy in lijn met de AVG werken VRD en GGD samen, in aanvulling op de gedeelde ICT-voorzieningen en informatiesystemen.

Om alle inzet en acties op het gebied van Informatieveiligheid & Privacy (IV&P) te ordenen hebben we een aantal principes besproken en afgesproken deze te gebruiken voor de verdere uitwerking.

I kwadrantenmodel
Digitale verstoringen *(Iedere verstoring van een digitaal systeem, moedwillig of door toeval, bedoeld of door een fout, die de (fysieke) veiligheid of openbare orde in een veiligheidsregio bedreigt)* hebben al snel gevolgen voor ons dagelijks leven. Om deze materie inzichtelijk te maken t.a.v. de verschillende acties die uitgevoerd moeten worden, helpt het kwadranten model.



Een digitale verstoring kan impact hebben op de veiligheidsregio zelf. Er kan bijvoorbeeld essentiële informatie verloren gaan of kantoorautomatiseringsprocessen kunnen uitvallen. Om dit te ondervangen zijn een goede *cyberveiligheid* en *cyberweerbaarheid* essentieel (intern).

Daarnaast kan een digitale verstoring impact hebben op de samenleving; impact waarvan de veiligheidsregio de gevolgen moet bestrijden; cyberwaakzaamheid en cybergevolgbestrijding (extern).
Bij *cyberwaakzaamheid* en *cybergevolgbestrijding* kijken we zowel naar risicobeheersing als naar crisisbeheersing en koppelen dit aan consequenties voor de veiligheidsregio zelf.

De veiligheidsregio staat voor de volgende opgaven:
> een goede informatiepositie verkrijgen; eigen kennis versterken en partners betrekken;
> risico's in beeld krijgen (eigen, maar vooral ook in de regio);
> het interne en externe gedeelte van het cyberkwadrant verbinden;
> zorgen voor aansluiting op het cyber resilience netwerk.

Cyberwaakzaamheid en -gevolgbestrijding aan de ene kant en cyberveiligheid en -weerbaarheid aan de andere kant zijn verschillende en gescheiden disciplines binnen een veiligheidsregio. Voor beiden zijn andere kennis en vaardigheden nodig. Kennis van het digitale domein bij medewerkers in de eigen organisatie op het gebied van cyberveiligheid en cyberweerbaarheid kan van grote waarde zijn bij cyberwaakzaamheid/-gevolgbestrijding (risicobeheersing en crisisbeheersing).

Het is dus van belang een goede koppeling tussen de verschillende onderdelen van het cyberkwadrant te organiseren. Dit helpt zowel als een uitval de eigen organisatie (bedrijfscontinuïteit) raakt als bij een verstoring die de samenleving raakt.

Vanuit de Informatieveiligheid kijken we vooral naar de twee intern kwadranten, namelijk *cyberveiligheid* en *cyberweerbaarheid.*

II Landelijke afspraken
Zowel de samenwerkende veiligheidsregio's als de samenwerkende GGD-en in Nederland ontwikkelen op landelijk niveau een gezamenlijke aanpak om de veiligheid van informatie en privacy te vergroten binnen de organisaties. Het stadium van ontwikkeling en aanpak van de twee lijnen verschilt.

Aangezien de landelijke aanpak van de veiligheidsregio's verder ontwikkeld is kiezen we er voor deze aanpak als uitgangspunt te nemen voor ons framework. De ontwikkelingen binnen GGD/GHOR Nederland blijven we volgen en benutten waar nodig.

De landelijke aanpak van de veiligheidsregio's is laatstelijk gepresenteerd in de vorm van een versnellingsplan. Dit plan biedt veiligheidsregio's de gelegenheid hun volwassenheid middels een assessment te achterhalen en verder uit te bouwen.

GGD/GHOR faciliteert kennisuitwisseling tussen (C)ISO's en FG-en op het gebied van AVG en NEN7510 middels landelijke overleggen en een gedeelde werkomgeving.

III BIO
Kern van de het versnellingsplan is de implementatie van de Baseline Informatiebeveiliging Overheid (BIO). De BIO is afgeleid van hét normenkader voor informatiebeveiliging, ISO27001 & 27002. Voor de VRD en GGD hebben we een overzicht beschikbaar welke onderdelen we geïmplementeerd hebben en waar het nog aan ontbreekt. De ontbrekende delen worden via een prioriteitsstelling gericht geïmplementeerd.

Het zwakke punt bij onze huidige implementatie van de BIO is de complete regelkring, met name de fase van terugkoppeling ontbreekt vaak.

Voor de implementatie van de BIO is een afzonderlijke planning opgesteld.
Implementatieplan BIO gereed december 2021: Onderdelen zijn Self Assessment en Risicoanalyse. BIO geïmplementeerd 1 januari 2023: Prioritering op basis van risicoanalyse.
IV NEN 7510
In het versnellingsplan ontbreekt specifieke aandacht voor informatieveiligheid & privacy bij zorg specifieke taken. Voor de GGD is het verplicht om te voldoen aan de zorg specifieke normen van NEN7510. Om dit te borgen vullen we het versnellingsplan aan met de implementatie van de NEN 7510. Hiermee nemen we een set van maatregelen op basis van de specifieke vereisten binnen de zorg, waarmee de AVG gewaarborgd wordt.

Met compliance aan BIO en NEN7510 hebben we voor een deel ook de privacy geborgd. Het beschermen van de privacy-rechten van individuen vraagt echter meer specifieke aandacht dan de maatregelen in de BIO en NEN7510 aangeven. Daarom wordt dit punt meegenomen in het jaarplan van de FG wat in samenhang met implementatie BIO en NEN7510 is opgesteld.

V Weerbaarheid
Instellen Proces en werkgroep om (mogelijke) cyberincidenten te beoordelen
Vanuit een pragmatische aanpak is er een werkgroep ontstaan die elkaar inhoudelijk opzoeken wanneer er (mogelijke) cyberincidenten zijn. Deze werkgroep en het proces waarlangs de beoordeling van deze incidenten gaat moet bestendigd worden. Niet alleen in beschikbaarheid en bereikbaarheid van de medewerkers, maar ook in een vastgelegde werkwijze en rapportage.

Continuïteitsplan
Het continuïteitsplan vanuit het oogpunt van cyberincidenten moet opgesteld worden. Hierin kan een tweedeling zitten namelijk

- continuïteitsplan vanuit ICT-techniek;
- continuïteitsplan voor onbekende cyberincidenten.

Onderdeel van het de aanbesteding van de nieuwe ICT beheerder (Switch) is het opstellen van een continuïteitsplan voor ICT. In dit deel van het continuïteitsplan zullen voor bekende incidenttypen plannen worden gemaakt. Denk hierbij aan zaken als stroomuitval, tijdelijk verlies van internetverbinding, uitval van specifieke hardwarecomponenten. In september wordt gestart met de overdracht van de huidige beheerder naar Switch. Switch heeft een groot aandeel m.b.t. de inhoud van het continuïteitsplan. Maar dit moet in lijn gebracht worden met kritische processen van de organisaties. Naar verwachting zal in het eerste half jaar van 2022 het continuïteitsplan opgeleverd worden.

Op basis van best-practices uit onze omgeving zal het tweede deel van het continuïteitsplan een inrichting/beschrijving geven van de processen en rollen die voor de onbekende cyberincidenten noodzakelijk zijn. Kritische processen worden gekoppeld aan praktische werkwijze waarbij de volgende punten centraal staan:

1. beoordelen van cyberincident;
2. betrokken partijen;
3. communicatie;
4. beperking van schade;
5. herstel van functionaliteit/omgeving.

Kennis en samenwerking partners versterken
Onderdeel van de weerbaarheid is het kennis hebben van partners in de omgeving. Bij relatief grote cyberincidenten is hulp van meerdere partijen wenselijk of noodzakelijk. Ook zullen incidenten al snel effect hebben op organisaties/partners om ons heen. Voor cyberincidenten die de gehele regio raken zal vooral vanuit cyberwaakzaamheid en cybergevolgbestrijding plannen en afspraken moeten komen.

Voor de cyberincidenten die vooral onze eigen organisatie raken moeten we samenwerking met partijen afspreken. Hiertoe is noodzakelijk dat actief partners maar ook marktpartijen benaderd worden.
Planning: doorlopend proces en vraagt gedurende het jaar regelmatig inzet.

Bijlage 2: Overzicht acties

Inleiding

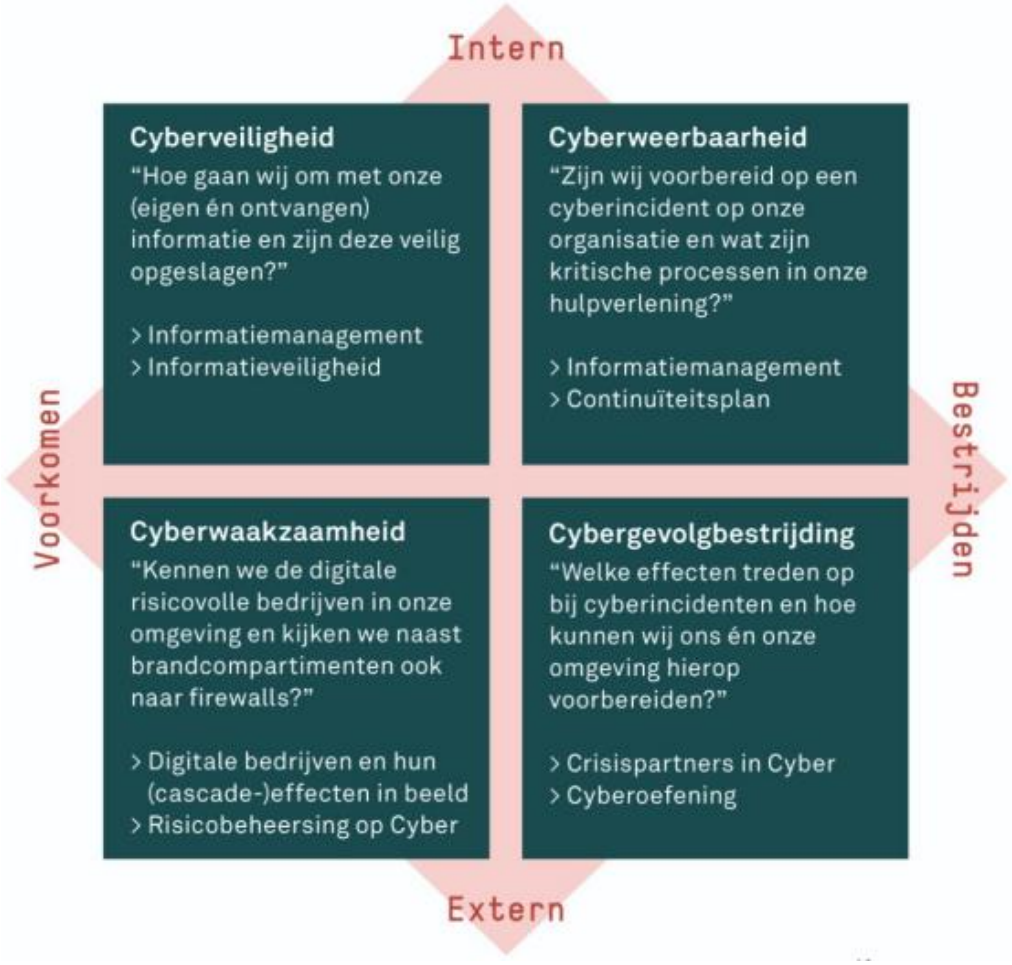
Met de groei aan digitale systemen en processen groeit ook het potentiële aanvalsoppervlak voor cyberaanvallen en de risico's op datalekken. De drempel om via de digitale weg te verstoren of te saboteren ligt lager dan de fysieke weg. De gevolgen van digitale verstoringen en privacy schendingen worden steeds groter. De eisen die intern en extern gesteld worden aan de bescherming van de ICT-omgeving en informatie van GGD-VRD nemen toe. Dit alles betekent dat het belang van informatieveiligheid toeneemt en VRD en GGD Drenthe nog beter moeten kunnen inspelen op digitale kwetsbaarheden en dreigingen. Om de informatieveiligheid te verhogen moeten inspanningen geleverd worden in het totale spectrum van mens, techniek en organisatie.

Zowel de samenwerkende veiligheidsregio's als de samenwerkende GGD-en in Nederland ontwikkelen op landelijk niveau een gezamenlijke aanpak om de veiligheid van informatie en privacy te vergroten binnen de organisaties. Het stadium van ontwikkeling en aanpak van de twee lijnen verschilt. Vanuit GGD-VRD is ervoor gekozen om aan te sluiten bij het versnellingsplan van IFV als aanpak voor het vergroten van de informatieveiligheid aangezien deze aanpak verder ontwikkeld is.

Kern van de het versnellingsplan is de implementatie van de BIO, het normenkader voor informatieveiligheid bij overheidsorganisaties. Voor de VRD en GGD is een overzicht beschikbaar welke onderdelen geïmplementeerd zijn en waar het nog aan ontbreekt. Aan dit versnellingsplan worden de specifieke eisen voor de zorg, normenkader NEN 7510 toegevoegd. Tot slot zijn de resultaten van de risicoanalyse die GGD liet uitvoeren door WeDoTrust ook meegenomen.

Doel en resultaat

Het doel van het implementeren van de BIO en NEN 7510 is het vergroten van de informatieveiligheid en weerbaarheid waarmee invulling gegeven wordt aan de bovenste helft van het kwadrantenmodel (Figuur 1).



Figuur 1

Het resultaat van deze implementatie moet zijn dat GGD en VRD aantoonbaar compliant zijn aan de normen inclusief borging in een PDCA-cyclus. Certificeerbaarheid op deze normen is niet het doel van deze implementatie. Het wordt echter niet uitgesloten dat dit op termijn wenselijk is.

Bij het beoordelen en invoeren van de onderliggende normen moet het te bereiken doel voor ogen gehouden worden, te weten het vergroten van onze informatieveiligheid. Voorkomen moet worden dat implementatie van de BIO en NEN 7510 gezien wordt als een afvink-lijstje.
Met de implementatie van BIO en NEN 7510 wordt er focus aangebracht aan de activiteiten op het gebied van informatieveiligheid. Hiermee kan op gestructureerde wijze een hoger volwassenheidsniveau gehaald worden in tegenstelling tot ad hoc reactie op signalen en incidenten.

Aanpak

- Uitvoeren Self Assessment
- Te realiseren doelstellingen verzamelen
- Per hoofdonderwerp actiehouder bepalen
- Prioriteitstelling

Om te komen tot een implementatieplan voor het compliant worden aan BIO en NEN7510 is gestart met een self-assessment. In workshops over de 16 hoofdonderwerpen uit de BIO is met inhoudelijk deskundigen gekeken naar ons volwassenheidsniveau op dit onderwerp. Het daarvoor gebruikte self-assessment tool van CIP geeft een weergave van het totale volwassenheidsniveau van GGD-VRD. Dit wordt in figuur 2 weergegeven. In detail kunnen de resultaten van VRD en GGD bij de primaire processen verschillen, echter op hoofdlijnen is het beeld nagenoeg gelijk.

Figuur 2

Om compliant te zijn aan de BIO wordt een volwassenheidspercentage van minstens 80% op alle onderdelen verwacht. Welke doelstellingen nog gehaald moeten worden om dit te bereiken wordt aangegeven in het self-assessment tool. De te realiseren doelstellingen zijn

per hoofdonderwerp gekoppeld aan de onderliggende normen uit de BIO en NEN 7510. Bij implementatie kan daarmee op hoofdlijnen de voortgang gerapporteerd worden terwijl de actiehouders in detail weten wat er gerealiseerd moet worden.

Fasering

We implementeren de BIO risicogestuurd en met focus, zodat we niet op elk incident of elke vraag ad hoc reageren, maar de te realiseren doelstellingen gestructureerd en volledig doorgevoerd worden.

Op basis van de uitgevoerde self-assessment en de daaruit voortvloeiende nog te realiseren doelstellingen is de fasering voor de implementatie uitgewerkt. Naast de self-assessment zijn de aanvullende vereisten uit NEN7510 meegenomen. NEN 7510 is een nadere specificering van de normen. Deze hebben niet geleid tot een aanpassing in de prioritering. Uit het rapport van WeDoTrust zijn de aanbevelingen meegenomen. Dat heeft tot gevolg dat de onderwerpen Veilig personeel, Beleid en Toegangsbeveiliging met prioriteit opgepakt worden. Tot slot is gekeken naar vereisten die GGD/GHOR stelt in het kader van aansluiting bij GT Connect. Dit heeft niet geleid tot een aanpassing van de prioritering.

Parallel aan de uitvoer van dit plan, worden ook verbeteracties ondernomen op het gebied van privacybescherming. De maatregelen uit de BIO en NEN7510 dragen bij aan een betere bescherming van persoonsgegevens. Voor de volledigheid is de jaarplanning voor 2022 zoals deze wordt gehanteerd door de FG bijgevoegd in de bijlage. Acties zullen zoveel mogelijk complementair worden uitgevoerd.

Om te komen tot een finale prioritering is gekeken naar de belasting per actiehouder en zijn onderwerpen per actiehouder verspreid over verschillende fasen. Een en ander resulteert in onderstaande fasering. Bij een aantal onderwerpen zullen meerdere actiehouders betrokken zijn. Degene met het grootste aandeel in dit onderwerp is aangegeven als actiehouder. In het volgende hoofdstuk wordt per hoofdonderwerp een korte toelichting gegeven.

Fase	**Onderwerp**	**Actiehouder**
Q1	Technische kwetsbaarheden	I&A
Q1	Beheer van incidenten	Werkgroep IV&P
Q1	Veilig personeel	P&O
Q1	Beleid	CISO
Q1	Toegangsbeveiliging	Proceseigenaar
Q2	Cryptografie	I&A
Q2	Bedrijfscontinuïteit	I&A
Q2	Audits	CISO
Q2	Wettelijke eisen	JuZa
Q2	Leveranciers	Proceseigenaar

Q3	Ontwikkelprocessen	Proceseigenaar
Q3	Informatiebeveiligingsorganisatie	CISO
Q3	Bedrijfsmiddelen	SO
Q3	Beheer van operationele systemen	I&A
Q3	Veilige omgeving	I&A / P&O
Q3	Netwerk	P&O

Toelichting per hoofdonderwerp

Technische kwetsbaarheden	Informatie over kwetsbaarheden verkrijgen en detecteren van aanvallen is goed ingeregeld. Beleid en procedures moeten op organisatieniveau eenduidig, vastgelegd en bekrachtigd zijn zodat geborgd is dat preventieve en correctieve maatregelen doorgevoerd worden.
Beheer van incidenten	Informatiebeveiligingsgebeurtenissen worden herkend en gesignaleerd. Rapportage hierover moet ingeregeld worden, zodat de organisatie kan leren van deze gebeurtenissen.
Veilig personeel	Personeel moet gedurende de hele loopbaan weten wat de verantwoordelijkheden zijn om bedrijfsinformatie te beschermen en te beveiligen. Bewustzijnsopleiding en training moeten structureel ingeregeld worden. Er moet een disciplinaire procedure bekend zijn.
Beleid	Beleidsbeslissingen en IB-maatregelen moeten in lijn zijn met de BIO. Bepalen of dit passend, adequaat en doeltreffend is moet gebeuren via de (bestaande) bestuurs- en P&C-cycli.
Toegangsbeveiliging	Toegangsrechten moeten toegekend en ingetrokken worden volgens vaststaande procedures. Dit wordt meegenomen in het project IAM. Inhoudelijke beoordeling van functiescheiding en toegangsrechten moeten periodiek plaatsvinden.
Cryptografie	Beleid en procedures voor cryptografisch sleutelbeheer moeten worden vastgelegd.
Bedrijfscontinuïteit	Bedrijfscontinuïteit wordt gewaarborgd door o.a. redundante componenten en up-to-date back-ups. Het continuïteitsplan moet in lijn met de bedrijfsstrategie en externe eisen herijkt worden.
Audits	Uitwerken en vaststellen van een auditplan waarin de PDCA-cyclus op gestructureerde wijze is afgedekt.

Wettelijke eisen	Vaststellen van een strategie en aanpak om te anticiperen op ontwikkelingen in wetgeving en contracten. Beleid en procedures moeten op organisatieniveau eenduidig, vastgelegd en bekrachtigd zijn.
Leveranciers	Leveranciers die toegang hebben tot informatiesystemen moeten worden gemonitord, beoordeeld en ge-audit. Hun prestaties moeten periodiek beoordeeld worden.
Ontwikkelprocessen	Procedures voor updates moeten eenduidig, vastgelegd en bekrachtigd zijn. Vastleggen hoe moet worden omgegaan met testgegevens
Informatiebeveiligingsorganisatie	Taken, bevoegdheden en verantwoordelijkheden vastleggen. Rapportagelijnen moeten eenduidig, vastgelegd en bekrachtigd zijn. Adviezen en toetsen van de CISO moeten bindend zijn.
Bedrijfsmiddelen	Het gebruik van bedrijfsmiddelen moet aantoonbaar aan de regels voldoen. Informatie moet geclassificeerd zijn.
Beheer van operationele systemen	De wijzigingsprocedure moet eenduidig, vastgelegd en bekrachtigd zijn. Test- en productieomgevingen moeten gescheiden zijn.
Veilige omgeving	Techniek: hardening en MDM moeten worden ingezet. Mens: een bewustwordingsprogramma moet geborgd worden en gebruikers moeten een gebruikersovereenkomst tekenen.
Netwerk	Techniek is reeds op orde. Mens: In de vertrouwelijkheidsovereenkomst moet de vertrouwelijke aard van deze informatie omschreven staan.

Projectrisico's

In 2022 wordt een aanpassing van de norm ISO27002, waarop de BIO en NEN7510 gebaseerd zijn, verwacht. Dat betekent dat de normen waar nu naar verwezen en naartoe gewerkt wordt, anders worden qua inhoud. Op de prioritering zal deze aanpassing geen invloed hebben aangezien de thema's gelijk blijven. Inhoudelijke aanpassing van de overheidsmaatregelen zijn pas bij de in 2023 geplande evaluatie van de BIO aan de orde. De ontwikkelingen op dit gebied zullen wel door de Security Officer op de voet gevolgd worden zodat hierop geanticipeerd kan worden waar mogelijk en opportuun.

Risico	Mitigerende maatregelen
Een incident [1] dwingt ons acties in andere volgorde op te pakken	Flexibiliteit in prioriteitstelling met behoud van focus op hoofdonderwerpen
Resources – tijd; Er is onvoldoende tijd beschikbaar van de actiehouder of de collega's die nodig zijn voor het uitvoeren van de acties	Gedegen inschatting van de benodigde tijd Eventueel budget voor inhuren van ondersteuning
Prioriteiten veranderen; o.a. door nieuwe ontwikkelingen	Periodieke afstemming over de gestelde prioriteiten in combinatie met nieuwe ontwikkelingen
Resources – kennis; Er is onvoldoende kennis van BIO en NEN 7510 aanwezig in de organisatie om de acties gedegen uit te kunnen voeren	Inschatting vooraf waar we mogelijk ondersteuning bij nodig hebben en budget voor het inhuren daarvan
Managementverantwoordelijkheid – eigenaarschap	Meenemen van de proceseigenaren in de planvorming

Projectbenodigdheden

Resources

In de fasering is reeds aangegeven dat de te realiseren doelstellingen bij verschillende actiehouders liggen. Elke actiehouder zal inzet van zijn/haar team nodig hebben. Per team zal tijd vrij gemaakt moeten worden voor het uitwerken en invoeren van de maatregelen. Hieronder een globale inschatting van het benodigde aantal dagen per onderwerp.
Deze inschatting is de benodigde tijd voor het neerzetten gedegen basis. Na het doorvoeren van deze maatregelen wordt de PDCA cyclus opgenomen in de reguliere processen en daarmee business as usual. De tijd die dit structureel vraagt is niet meegenomen in dit plan.

Fase	Onderwerp	Actiehouder	Aantal dagen
Q1	Technische kwetsbaarheden	I&A	8
Q1	Beheer van incidenten	Werkgroep IV&P	4
Q1	Veilig personeel	P&O	8
Q1	Beleid	CISO	4
Q1	Toegangsbeveiliging	Proceseigenaar	8
Q2	Cryptografie	I&A	3
Q2	Bedrijfscontinuïteit	I&A	8
Q2	Audits	CISO	5
Q2	Wettelijke eisen	JuZa	3
Q2	Leveranciers	Proceseigenaar	6
Q3	Ontwikkelprocessen	Proceseigenaar	4
Q3	Informatiebeveiligingsorganisatie	CISO	4

Q3	Bedrijfsmiddelen	SO	6
Q3	Beheer van operationele systemen	I&A	6
Q3	Veilige omgeving	I&A / P&O	3
Q3	Netwerk	P&O	4

Naast de inzet van de actiehouders en hun teams wordt inzet van het kernteam Informatieveiligheid en Privacy (IV&P) verwacht. Dit kernteam zal tweewekelijks bij elkaar komen om voortgang en risico's te bewaken.

Projectorganisatie

Stuurgroep = CISO , FG, Manager bedrijfsvoering

- Budgetverantwoordelijk, zorgdragen voor draagvlak binnen MT, prioriteitstelling, acceptatie eindresultaat
- 2 uur per 2 weken

Projectleider = Security Officer

- Bewaken voortgang & resultaat, uitzetten acties, inhoudelijke ondersteuning
- 1 dag per week

Werkgroep / kernteam IV&P = Adviseur I&A, Informatiemanager, Adviseur A, Security Officer, Privacy Officer

- Inhoudelijke ondersteuning aan actiehouders, uitvoeren acties, communicatie met de achterban
- Inzet 1 dagdeel per week van de werkgroep.
- Minimaal 1 dag per week ondersteuning van Security Officer en Privacy Officer.