Veiligheids beraad

Projectplan Informatie-veiligheid

Versie: 0.9.9, 25 november 2015

Veiligheidsberaad
Postbus 7010
6801 HA Arnhem
www.veiligheidsberaad.nl
info@veiligheidsberaad.nl
026 355 24 99

Besluitvormingshistorie

Datum	Besluitvorming in	Besluit
11-11-2015	POI	Positief advies met opmerkingen
18-11-2015	BAC Informatievoorziening	Positief advies met opmerkingen
25-11-2015	DB Veiligheidsberaad	Akkoord en besluit consultatie
01-12-2015	Consultatie besturen veiligheidsregio's	
N.t.b.	NIM/NICT	
N.t.b.	BAC Informatievoorziening	
02-3-2016	DB Veiligheidsberaad	
18-3-2016	Veiligheidsberaad	

Colofon

Opdrachtgever: Portefeuillehouder Informatievoorziening Veiligheidsberaad
Contactpersoon: Mark Luijten
Titel: Projectplan Informatieveiligheid
Datum: 25 november 2015
Status: Concept
Versie: 0.9.9
Auteurs: Luud Verheijen, netwerken Informatiemanagement en ICT
Projectleider: Luud Verheijen
Review: Mark Luijten
Eindverantwoordelijk: Opdrachtgever

Managementsamenvatting

Maatschappelijke urgentie
De afhankelijkheid van digitale systemen neemt toe en veiligheidsregio's zijn in toenemende mate met andere organisaties en hun systemen verbonden. Voor de veiligheidsregio's geldt ook een onderlinge afhankelijkheid: uitval van ICT-gebaseerde diensten en processen bij een veiligheidsregio levert ook acuut een veiligheidsprobleem op bij de buurregio's. Vanuit deze wederzijdse afhankelijkheid moet er zeer aan gehecht worden dat de informatieveiligheid van alle veiligheidsregio's in basis op orde is. Informatieveiligheid vraagt dan ook meer dan ooit om aandacht van bestuur en management.

De Strategische Agenda Versterking Veiligheidsregio's 2014-2016 van het Veiligheidsberaad stelt dat de continuïteit van de samenleving gevaar loopt, als voorzieningen zoals elektriciteit, ICT, telecommunicatie en drinkwater om wat voor reden dan ook uitvallen. Grootschalige uitval kan tot maatschappelijke ontwrichting leiden.

In de zomer van 2014 is door onderzoeks- en adviesbureau PBLQ Zenc de quick scan Cybersecurity Veiligheidsregio's uitgevoerd. Uit deze scan kwam naar voren dat het niveau van informatieveiligheid bij veiligheidsregio's in totaliteit onvoldoende is. Op een schaal van 1 tot 10 scoren veiligheidsregio's gemiddeld een 5. In bijlage A is het beeld per veiligheidsregio opgenomen; deze uitkomst onderstreept de urgentie van dit project.

Bestuurlijke context
In het programma Informatievoorziening veiligheidsregio's 2015-2020, dat na bestuurlijke consultatie in de veiligheidsregio's op 12 juni 2015 is vastgesteld door het Veiligheidsberaad, is informatieveiligheid als één van de zes prioriteiten opgenomen.
De voorbereiding voor het project Informatieveiligheid is al in het voorjaar van 2014 gestart met een plan van aanpak Cybersecurity. In het Meerjarenbeleidsplan IFV 2014-2018 is cybersecurity één van de thema's in het programma 'Informatievoorziening en meldkamer'. Het onderhavige projectplan is een voortzetting van deze initiatieven.

Doelstelling
Het project Informatieveiligheid heeft als doel het verbeteren van informatieveiligheid in de veiligheidsregio's. Informatieveiligheid draait onder andere om technische maatregelen, maar zeker ook om menselijk handelen. Dit project gaat dan ook in grote mate over bewustwording en training, het uitwisselen van voorbeelden, het gebruikmaken van kennis van andere partijen, het bewaken van de voortgang, met als resultaat het behalen van de doelstelling zoals hieronder verwoord.

De doelstelling van het project Informatieveiligheid luidt als volgt:
In 2018 is binnen alle veiligheidsregio's een niveau van informatieveiligheid gerealiseerd dat bescherming biedt tegen dreigingen anders dan door terreurgroepen, inlichtingendiensten en zwaar georganiseerde (internet)criminaliteit.
Dit is vanwege de onderlinge afhankelijkheid van de veiligheidsregio's geen vrijblijvend doel. De veiligheidsregio's voeren daarom op basis van een collectief geformuleerde standaard jaarlijkse een GAP-analyse uit. Vanuit het landelijke project wordt hierop gemonitord en gerapporteerd.

Om deze bewustwording vanuit het collectieve belang ook op bestuurlijk niveau te bekrachtigen, kunnen de 25 besturen middels een intentieverklaring naar elkaar uitspreken om in de eigen regio tot het gewenste niveau van informatieveiligheid te komen.

Als uitgangspunt voor de genoemde standaard wordt de Baseline informatieveiligheid Nederlandse gemeenten (BIG) gehanteerd. De BIG zal daarbij worden aangepast met relevante onderdelen uit de norm NEN 7510 (Informatiebeveiliging in de zorg), omdat binnen sommige regio's ook ambulancezorg en/of de GGD is ondergebracht. Het resultaat is dan een specifieke baseline voor veiligheidsregio's: de Baseline Informatiebeveiliging Veiligheidsregio's (BIVR).
Bij de keuze voor de BIG speelt ook mee dat veiligheidsregio's gemeenschappelijke regelingen van gemeenten zijn (verlengd lokaal bestuur). Bedrijfsprocessen van gemeenten en veiligheidsregio's en de betrouwbaarheidseisen die aan die bedrijfsprocessen worden gesteld zijn vergelijkbaar, en de hoeveelheid informatie die tussen gemeenten en veiligheidsregio's wordt uitgewisseld is aanzienlijk.

Het halen van de doelstelling is een regionale verantwoordelijkheid. Tegelijkertijd is er zoals gezegd ook sprake van een collectief belang bij een landelijk basisniveau van informatieveiligheid. Vanuit deze wederzijdse afhankelijkheid moet er zeer aan gehecht worden dat de basisveiligheid van alle veiligheidsregio's op orde is. Tenslotte is er ook wettelijke basis voor informatieveiligheid binnen de veiligheidsregio's, zoals de Wet bescherming persoonsgegevens (inclusief de op 1 januari 2016 in werking tredende meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid College bescherming persoonsgegevens) en de Wet op de geneeskundige behandelingsovereenkomst.

Het project heeft een faciliterende rol, te weten ondersteuning bieden aan de regio's bij het behalen van de doelstelling.

Kosten
De landelijke projectkosten gedurende de jaren 2016 t/m 2018 betreffen in totaal € 300.750. Deze kosten worden gedekt vanuit het werkbudget Informatievoorziening van het Veiligheidsberaad, mits dit budget ook na 2016 beschikbaar is. Verder wordt van veiligheidsregio's capaciteit gevraagd voor de uitvoering van het landelijke project, te weten 150 uur op jaarbasis per regio.

Daarnaast zullen veiligheidsregio's zelf ook kosten moeten maken voor het ontwikkelen en implementeren van maatregelen in de eigen regio. Deze kosten zijn lastig in te schatten, kunnen per regio verschillen en kunnen substantieel zijn afhankelijk van de uitgangssituatie. In beginsel behoren kosten voor informatieveiligheid toegerekend te worden aan bedrijfsprocessen en bijbehorende applicaties.

Inhoud

1 Inleiding

1.1 Algemeen

Overheden staan net als andere organisaties voor grote uitdagingen op het gebied van informatieveiligheid. Er is steeds meer bewustwording over de maatschappelijke, financiële en politieke risico's van een slechte informatiebeveiliging, mede door incidenten als DigiNotar, Lektober en Dorifel en door schade die ontstaat door onzorgvuldig handelen van bijvoorbeeld eigen medewerkers.

Alvorens verder te gaan is het verstandig om de begrippen 'Informatieveiligheid', 'Informatiebeveiliging' en 'cybersecurity' nader toe te lichten.

Door de toenemende digitalisering is het zorgvuldig omgaan met informatie en gegevens van groot belang. Uitval van computers of telecommunicatiesystemen, het in ongerede raken van gegevensbestanden of het door onbevoegden kennisnemen dan wel manipuleren van bepaalde gegevens heeft ernstige gevolgen voor de continuïteit van een veiligheidsregio. Een betrouwbare, beschikbare en correcte informatiehuishouding is essentieel voor de dienstverlening aan burgers en bedrijven.
Binnen de organisatie komt informatie niet enkel voor in digitale vorm. Ook aan papieren archieven dienen dezelfde beveiligingseisen te worden gesteld als aan digitale archieven. Denk hierbij binvoorbeeld aan maatregelen met betrekking tot toegangsbeveiliging tot gebouwen en archiefruimten, maar bijvoorbeeld ook aan clean desk policy.

Om het doel 'informatieveiligheid' te waarborgen wordt gebruik gemaakt van de maatregel 'informatiebeveiliging'.

Informatiebeveiliging is de verzamelnaam voor de processen die worden ingericht om de betrouwbaarheid van processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen al dan niet opzettelijk incidenten. Het begrip 'betrouwbaarheid' wordt gedefinieerd aan de hand van de beveiligingskenmerken 'beschikbaarheid', 'integriteit' en 'vertrouwelijkheid'.

In de Nationale Cyber Security Strategie (NCSS) van het Ministerie van Veiligheid en Justitie wordt 'cybersecurity' als volgt omschreven:

'*Cybersecurity is het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie.*'

Met betrekking tot de positionering van de termen 'informatiebeveiliging' en 'cybersecurity', volgt hieronder de interpretatie van prof. dr. ir. Jan van den Berg, hoogleraar Cybersecurity TU Delft:

‘*De termen ‘informatiebeveiliging’ en ‘cybersecurity’ worden vaak door elkaar gebruikt soms met dezelfde, soms met een afwijkende betekenis. Velen spreken vandaag de dag ook over cyberspace, bijvoorbeeld als een nieuw (door de mens gecreëerd) vijfde domein naast de bestaande domeinen land, water, lucht en ruimte. Een en ander roept de vraag op of informatiebeveiliging en cybersecurity (wel of niet) fundamenteel van elkaar verschillen. Geconfronteerd met de uitdaging om nieuw multidisciplinair onderzoek & onderwijs rond cybersecurity te ontwikkelen, ontstond de noodzaak om orde op zaken te stellen en de begrippen helder ten opzichte van elkaar te positioneren. Dit heeft geleid tot een nieuwe conceptualisatie rond de begrippen cyberspace en cybersecurity. Informatiebeveiliging is in deze visie onderdeel van het bredere begrip van cybersecurity.*’

Informatieveiligheid raakt de toeleverancier, verstrekker, afnemer of bronhouder van (overheids)gegevens. Dagelijkse aandacht voor informatieveiligheid en ook privacy is zeer belangrijk in de processen waarbij gegevens worden geregistreerd en uitgewisseld. Niet alleen de technische kant van informatieveiligheid en privacy is daarbij van belang. Ook het gebruik van ICT-systemen en gegevens door medewerkers in elke laag van de organisatie heeft grote invloed op de informatieveiligheid. Het is dan ook belangrijk dat overheidspartijen informatieveiligheid en privacy goed verankeren in de organisatie, door (technische) maatregelen en gedragsverandering door vergroting van het risicobesef.

De Bestuurlijke adviescommissie informatievoorziening van het Veiligheidsberaad (BAC IV) heeft in haar vergadering van 6 november 2013 aangegeven een regierol van het Veiligheidsberaad op de ontwikkeling en implementatie van continuïteitsplannen en cybersecurity van belang te achten. De regierol van het Veiligheidsberaad laat zich vertalen als sturing op het behalen van de doelstelling en tussenresultaten. Op basis van voortgangsrapportages zal het Veiligheidsberaad bijsturen indien noodzakelijk.

Op 9 april 2014 heeft de BAC IV besloten een quick scan cybersecurity uit te voeren en een plan van aanpak op te stellen.
Eind juli 2014 is deze quick scan uitgevoerd. Hieruit kwam naar voren dat het niveau van informatieveiligheid bij veiligheidsregio’s in totaliteit onvoldoende is. Op een schaal van 1 tot 10 scoren veiligheidsregio’s gemiddeld een 5. Aangetekend dient te worden dat er enkele veiligheidsregio’s zijn die relatief hoog scoren, maar er zijn ook veiligheidsregio’s die zeer laag scoren. Bij de interpretatie van de resultaten is enige voorzichtigheid geboden; vraagtekens kunnen worden gezet bij de validiteit en betrouwbaarheid van de set vragen. In ieder geval geven de resultaten een zekere tendens weer.
Zie bijlage A voor het beeld per veiligheidsregio.

In de rapportage over de quick scan schrijft PBLQ Zenc:

‘*Belangrijk bij informatieveiligheid is dat bestuurders zich bewust zijn van de risico’s die de organisatie loopt als informatie niet voldoende beveiligd blijkt te zijn. Bijvoorbeeld risico’s in termen van financiën, imagoschade of verminderd vertrouwen bij ketenpartners. Hierbij is het belangrijk te realiseren dat 100% veilig niet bestaat, maar dat het wel mogelijk is om ‘in control te zijn’ en een bewuste risicoafweging te maken. Informatieveiligheid is niet alleen een technisch aandachtspunt. Informatieveiligheid heeft ook aspecten van organisatiecultuur en bewust omgaan met gevoelige gegevens.*
Uit de antwoorden blijkt dat informatieveiligheid in regio’s nauwelijks een thema is voor bestuur of directie. Lang niet alle regio’s hebben een beveiligingsplan, of recentelijk nog specifiek aandacht besteed informatieveiligheid in audits. Ook is het vrijwel niet als specifiek thema voor de komende jaren benoemd’.

Het project Informatieveiligheid is al op 1 november 2014 gestart op basis van bovengenoemde bestuurlijke opdracht. Onderhavig projectplan in het kader van het programma Informatievoorziening Veiligheidsregio's, sluit aan op het eerdere plan van aanpak. Belangrijke elementen hierbij zijn: bewustwording en training, het uitwisselen van voorbeelden, het gebruikmaken van kennis van andere partijen en het bewaken van de voortgang. De onderwerpen informatieveiligheid en continuïteit moeten in gezamenlijkheid worden uitgewerkt.

1.2 Achtergrond en aanleiding

De volgende uitgangspunten, strategieën en ontwikkelingen vormen de context van dit projectplan:

- National Cyber Security 2, van het ministerie van Veiligheid en Justitie;
- Modelplan Continuïteit;
- Cybersecurity-programma's van de ketenpartners, met name gemeenten (met de BIG) en politie;
- Aandacht voor detectie en incidentmanagement;
- Samenwerking met vitale partners.
- VeRA 2.0 (Veiligheidsregio Referentiearchitectuur) van het Veiligheidsberaad.

Nationale Cybersecurity Strategie 2

In oktober 2013 heeft de Minister van VenJ de Nationale Cybersecurity Strategie 2 (NCSS2) aangeboden aan de Tweede Kamer. Het thema hiervan is 'Van bewust naar bekwaam' en er is een actieprogramma voor de periode 2014-2016 aan gekoppeld. Voor veiligheidsregio's is het van belang hierbij aan te haken, aangezien het een nationale strategie betreft.

NCSS1	NCSS2
Publiek-Privaat partnership	Privaat-Publieke participatie
Focus op structuren	Focus op netwerken / strategische coalities
Benoemen multi-stakeholdermodel	Verduidelijken onderlinge verhoudingen stakeholders
Capaciteitsopbouw nationaal gericht	Capaciteitsopbouw zowel nationaal als internationaal gericht
Generieke benadering: breed inzetten op weerstandverhogende maatregelen	**Risicogebaseerde** benadering: balans tussen bescherming belangen, dreiging belangen en geaccepteerd risico voor de samenleving.
Uitgangspunten benoemen	(Beleids)visie weergeven
Van onbewust naar bewust	Van bewust naar bekwaam

Modelplan Continuïteit

Zoals hiervoor reeds is aangegeven moeten cybersecurity en continuïteit in samenhang worden bezien. In 2013 begeleidde Berenschot, in opdracht van het ministerie van Veiligheid en Justitie, de 25 veiligheidsregio's bij het opstellen van hun continuïteitsplan ICT en/of elektriciteit met behulp van een modelplan. Uitgangspunt is dat de veiligheidsregio's beschikken over continuïteitsplannen. Voor zover dat niet het geval is wordt verwezen naar het modelplan Continuïteit zoals dat door Berenschot is opgesteld.

Een van de consequenties van het project Informatieveiligheid is dat bestaande continuïteitsplannen mogelijk op onderdelen zullen moeten worden aangepast.

Cybersecurityprogramma's van ketenpartners

Ten behoeve van de aansluiting bij cybersecurityprogramma's van ketenpartners zullen contacten worden onderhouden met onder meer VNG/KING (Informatiebeveiligingsdienst), de Nationale Politie en Regionale Uitvoeringsdiensten (RUD's). Verder wordt samenwerking gezocht met partijen zoals het Centrum voor Informatiebeveiliging en Privacybescherming (CIP) en The Hague Security Delta (HSD). Doel is in eerste instantie gebruik te maken van best practices bij de bewustwording en het bepalen en realiseren van een basisniveau. Bij de verdere ontwikkeling kan bovendien gezamenlijk opgetrokken worden.

Aandacht voor detectie en incidentmanagement

Het betreft hier het proces van detectie en afhandeling van incidenten dat uit de volgende stappen bestaat:

- Identificatie;
- Schade indamming (insluiting en beperking);
- Behandeling en herstel;
- Kennisgeving;
- Rapportage en evaluatie.

Samenwerking met vitale partners

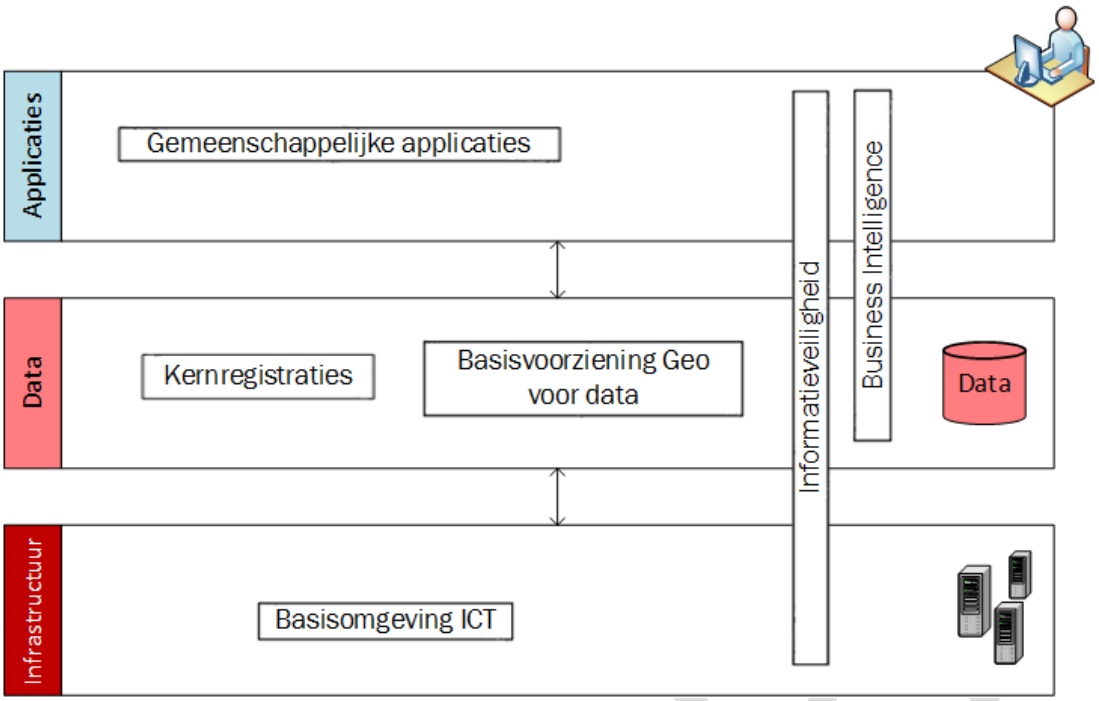
Het IFV kan een coördinerende en faciliterende rol spelen in de samenwerking van veiligheidsregio's met partners op het gebied van informatieveiligheid; bijvoorbeeld in het op een veilige manier uitwisselen van informatie. Mogelijk dat hiervoor convenanten kunnen worden afgesloten voor zover deze er niet zijn.

Veiligheidsregio Referentiearchitectuur 2.0

Er wordt in het kader van de Veiligheidsregio Referentiearchitectuur (VeRA 2.0) gedacht aan een katern Informatiebeveiliging (zoals ook bij de overkoepelende overheidsarchitectuur NORA opgenomen). Dit is tevens een stap om het gewenste basisniveau te borgen in de (referentie)architectuur. Het katern Informatiebeveiliging moet vastgesteld worden door het Veiligheidsberaad.

1.3 Samenhang met programma IV

Informatieveiligheid draagt bij aan de bedrijfscontinuïteit en is een noodzakelijke voorwaarde voor een succesvolle implementatie van de overige vijf projecten. Informatieveiligheid heeft zowel betrekking op de infrastructuur als op data, applicaties en de organisatie. Dit is als volgt weergegeven in het programmaplan.



1.4 Samenhang met andere projecten

Er bestaat samenhang tussen de resultaten van dit project en elk ander project dat de informatievoorziening raakt binnen veiligheidsregio's en tussen veiligheidsregio's en ketenpartners. In dergelijke projecten dient aandacht te worden besteed aan het stellen van specifieke eisen ten aanzien van informatiebeveiliging voor zowel de ICT-infrastructuur (backup, uitwijk, firewall, intrusion detection etc.), applicaties (secure software development, toegangscontrole etc.), data (opslag, transport, toegankelijkheid encryptie etc.) alsmede de organisatorische aspecten inclusief bewustwording/gedrag.

Ook is er een relatie met het project Continuïteit van de Samenleving (één van de zes projecten uit de Strategische Agenda). Het Veiligheidsberaad heeft op 12 juni 2015 ingestemd met dat projectplan.
Het project Continuïteit van de Samenleving heeft tot doel de samenwerking tussen ministeries, veiligheidsregio's en vitale bedrijven te verbeteren, waarbij vooral ingezoomd wordt op dreigingen ten aanzien van de vitale infrastructuur. Daarbij worden voorzieningen zoals drinkwater, elektriciteit, gas, olie, ICT & telecom, waterkeringen en nucleaire voorzieningen beschouwd als de vitale infrastructuur. Uitval van cruciale ICT-voorzieningen is daarin opgenomen, omdat het een ontwrichtend effect kan hebben op de samenleving.

2 Doelstelling en resultaten

2.1 Visie

In de NCSS2 (zie 1.2.1) is de volgende visie verwoord:

"Nederland zet samen met zijn internationale partners in op een veilig en open cyberdomein, waarin de kansen die digitalisering onze samenleving biedt volop worden benut, dreigingen het hoofd worden geboden en fundamentele rechten en waarden worden beschermd."

De visie achter NCS2 is universeel en is dus ook van toepassing op het project Informatieveiligheid binnen het programma Informatievoorziening Veiligheidsregio's. In de visie van NCS2 worden maatregelen in het kader van cybersecurity vanuit een drietal invalshoeken vormgegeven:

- Veiligheid;
- Vrijheid;
- Maatschappelijke groei.

Veiligheid

Cybersecurity gaat zowel over de veiligheid van ICT als over de veiligheid van daarin opgeslagen informatie. Uitval van ICT-gebaseerde diensten en processen kan grote maatschappelijke gevolgen hebben. Bij uitval van vitale diensten en processen is er zelfs kans op maatschappelijke ontwrichting. Het beschermen van persoonsgegevens, staatsgeheimen en andere gevoelige informatie, is essentieel voor het vertrouwen dat partijen hebben in het cyberdomein. Voor de veiligheidsregio's geldt bovendien dat informatieveiligheid weliswaar een regionale verantwoordelijkheid betreft, maar dat de gevolgen van uitval van ICT-gebaseerde diensten en processen ook effect heeft op de veiligheid van buurregio's. Er is daarmee sprake van een gemeenschappelijke verantwoordelijkheid.

Vrijheid

Het beschermen van fundamentele rechten en waarden, vergt inzet van vele partijen en dient in (inter)nationaal verband te gebeuren. De aanpak die wordt voorgestaan is het ontwikkelen van internationale normen en standaarden.
Naast voor overheden is hier een belangrijke rol weggelegd voor partijen uit de private sector en maatschappelijke organisaties. Nederland maakt zich hier onder meer hard voor binnen de Verenigde Naties, tijdens internationale cyberspace-conferenties en in andere multistakeholdersettings zoals het Internet Governance Forum.

Maatschappelijke groei

De innoverende kracht die uitgaat van verdergaande digitalisering is een belangrijke stimulans voor maatschappelijke groei. Het gaat daarbij zowel om economische groei als om de mogelijkheden die digitalisering biedt aan de samenleving, bijvoorbeeld in de vorm van onderwijstoepassingen, mogelijkheden tot het onderhouden van sociale contacten, maar ook verbeterde overheidsvoorzieningen. Door de kabinetsdoelstelling om het mogelijk te maken dat burgers en bedrijven in 2017 hun zaken met de overheid digitaal kunnen afhandelen,

wordt een extra slag in de realisatie van de iOverheid gemaakt. Daarmee wordt het maatschappelijk belang van de iOverheid nog groter. Maatregelen op het gebied van veiligheid en cybersecurity zijn daarom essentieel en brengen de nodige investeringen met zich mee.

2.2 Doelstelling

De doelstelling van het project Informatieveiligheid luidt als volgt:

In 2018 is binnen alle veiligheidsregio's een niveau van informatieveiligheid gerealiseerd, dat bescherming biedt tegen dreigingen anders dan door terreurgroepen, inlichtingendiensten en zwaar georganiseerde (internet)criminaliteit.

Opgemerkt dient te worden dat veiligheidsregio's verantwoordelijk zijn voor het behalen van de doelstelling en dat het IFV, in de vorm van projectleiding/begeleiding, vooral een faciliterende rol heeft.

Het behalen van de doelstelling is een regionale verantwoordelijkheid. Tegelijkertijd is er ook sprake van een collectief belang bij een landelijk basisniveau van informatieveiligheid. Uitval van ICT-gebaseerde diensten en processen bij een veiligheidsregio leveren ook acuut een veiligheidsprobleem op bij de buurregio's. Vanuit deze wederzijdse afhankelijkheid moet er zeer aan gehecht worden dat de basisveiligheid van alle veiligheidsregio's op orde is.

Diverse wet- en regelgeving biedt daarnaast ook handvatten om te spreken van een wettelijke verplichting. Onder andere zijn dit de Wet bescherming persoonsgegevens (Wbp), inclusief de op 1 januari 2016 in werking tredende meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid College bescherming persoonsgegevens (Cbp), en de Wet op de geneeskundige behandelingsovereenkomst (WGBO).
Verder komen op het gebied van Europese privacywet- en regelgeving nieuwe nationale wettelijke verantwoordelijkheden en verplichtingen op veiligheidsregio's, die van invloed kunnen zijn op het project Informatieveiligheid. In vogelvlucht zijn dit de belangrijkste aspecten uit de privacywet- en regelgeving om in ieder geval rekening mee te houden:

1. Accountability: de privacyhuishouding moet aantoonbaar op orde zijn (beleid, cultuur, processen en techniek);
2. Privacy by design: bij nieuwe ontwikkelingen moet privacy in de designfase al worden geborgd;
3. Verplichte aanstelling Functionaris Gegevensbescherming;
4. Meldplicht datalekken: datalekken moeten worden gemeld bij Cbp en bij alle 'getroffenen'";
5. Boetebevoegdheid Cbp: bevoegd om boetes tot € 810.000,- op te leggen voor:
   a. Privacyhuishouding niet aantoonbaar op orde;
   b. Niet tijdig melden datalek;
   c. Niet aanstellen Functionaris Gegevensbescherming;
6. Overgangstermijn voor bestaande gegevensverwerkingen van 2 of 3 jaar om deze compliant te krijgen;
7. Nieuwe gegevensverwerkingen moeten vanaf 1 januari 2016 meteen aan de nieuwe wetgeving voldoen.

2.3 Beoogde resultaten

De in 2.2 omschreven doelstelling kan behaald worden door het realiseren van de volgende resultaten:

1. In 2018 is er een basisniveau informatieveiligheid geïmplementeerd in alle veiligheidsregio's, dat tenminste het niveau heeft van de 'Baseline informatieveiligheid Nederlandse gemeenten' (BIG);
2. In 2018 is informatieveiligheid geborgd in alle veiligheidsregio's, zodat het bereikte basisniveau gehandhaafd blijft.

In z'n algemeenheid zijn veiligheidsregio's het er over eens om als uitgangspunt de Baseline informatieveiligheid Nederlandse gemeenten (BIG) te hanteren. Echter, de BIG zal moeten worden aangepast met relevante onderdelen uit de norm NEN 7510 (Informatiebeveiliging in de zorg) omdat binnen sommige regio's ook ambulancezorg en/of de GGD is ondergebracht. Het resultaat is dan een specifieke baseline voor veiligheidsregio's: de Baseline Informatiebeveiliging Veiligheidsregio's (BIVR). Daarnaast speelt voor de keuze van de BIG mee dat veiligheidsregio's gemeenschappelijke regelingen van gemeenten zijn (verlengd lokaal bestuur). Bedrijfsprocessen van gemeenten en veiligheidsregio's en de betrouwbaarheidseisen die aan die bedrijfsprocessen worden gesteld zijn vergelijkbaar, en de hoeveelheid informatie die tussen gemeenten en veiligheidsregio's wordt uitgewisseld is aanzienlijk.

Binnen het project zal het basisniveau informatieveiligheid 'SMART' worden gemaakt, door de ongeveer 300 maatregelen die de BIG bevat te reduceren tot de 50 à 60 belangrijkste maatregelen. Deze subset van maatregelen vormt dan het referentiekader (standaard) voor veiligheidsregio's.

2.4 Reikwijdte en projectbegrenzing

Het in 2018 te bereiken niveau van informatieveiligheid beperkt zich tot:

- Veiligheidsregio's intern;
- Informatie-uitwisseling tussen veiligheidsregio's onderling;
- Informatie-uitwisseling tussen veiligheidsregio's en (keten)partners.

Informatieveiligheid van organisaties anders dan veiligheidsregio's is 'out of scope'.
Daar waar mogelijk zullen eisen worden gesteld aan providers van cloudtoepassingen. Deze providers zullen moeten aantonen dat ze voldoen aan de internationale standaard ISO/IEC 27002:2013.

Controle op de beheerfase is geen onderdeel van project en is dus 'out of scope'. Dit betekent dat veiligheidsregio's verantwoordelijk zijn voor het *op niveau houden* van informatieveiligheid conform de dan geldende normen en standaarden.

2.5 Randvoorwaarden

Een kritische succesfactor is voldoende medewerking door de veiligheidsregio's.
Veiligheidsregio's zullen capaciteit ter beschikking moeten stellen; bij voorkeur capaciteit van leden van de netwerken Informatiemanagement en ICT.
Geschat wordt dat de benodigde capaciteit een factor drie is van die van de projectleider. De projectleider levert 1248 uur op jaarbasis. Dit betekent dat veiligheidsregio's in totaal 3744 uur dienen te leveren. Dit komt dus neer op 150 uur op jaarbasis per veiligheidsregio. Deze capaciteit wordt vooral besteed aan het ontwikkelen van producten zoals het in 2.3 genoemde referentiekader, informatiebeveiligingsbeleid etc.. Let wel: dit aantal uren is exclusief de uren die besteed moeten worden aan de regionale invulling van informatieveiligheid. Uitgangspunt is standaardproducten te ontwikkelen die door elke veiligheidsregio gebruikt kunnen worden. De basis van deze producten wordt gevormd door de producten die reeds ontwikkeld zijn door de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID) en de Informatiebeveiligingsdienst voor gemeenten (IBD).

Als veiligheidsregio's onvoldoende capaciteit leveren, dan is de kans groot dat het project mislukt.

3 Business Case

3.1 Rechtvaardiging

Continuïteit van primaire processen in de OOV-sector is cruciaal. Doordat processen steeds afhankelijker worden van informatietechnologie, kan uitval leiden tot maatschappelijke ontwrichting en zelfs levensbedreigend zijn.

Voor wat informatievoorziening betreft, zijn gemeenten en veiligheidsregio's in belangrijke mate van elkaar afhankelijk: informatiestromen bewegen heen en weer tussen gemeenten en veiligheidsregio's. Dit geldt zeker voor wat betreft het op orde houden van de crisisbeheersing en rampenbestrijding, waarbij de inzet van informatietechnologie niet meer is weg te denken.
Daarnaast geldt dat uitval van ICT-gebaseerde diensten en processen bij een veiligheidsregio ook acuut een veiligheidsprobleem oplevert bij de buurregio's. Vanuit deze wederzijdse afhankelijkheid moet er zeer aan gehecht worden dat de basisveiligheid van alle veiligheidsregio's op orde is.
Als veiligheidsregio's niet informatieveilig zijn, dan bestaat verder de kans dat (keten)partners mogelijk niet meer willen samenwerken. Zoals in 1.1 reeds aangegeven, blijkt dat het niveau van informatieveiligheid bij veiligheidsregio's verbetering behoeft. Door de verwevenheid met bedrijfsprocessen van (keten)partners zal de impact van een cyberaanval vele malen groter zijn dan vijf jaar geleden.

De jaarlijkse wereldwijde schade door cybercrime wordt geschat op € 325 miljard. Onderzoek van TNO geeft aan dat cybercrime de Nederlandse economie jaarlijks ongeveer € 10 miljard kost (1,5% van het Bruto Nationaal Product). Deze raming zou kunnen betekenen dat de schade door cybercrime voor gemeenten jaarlijks ongeveer €300 miljoen bedraagt.
Voor veiligheidsregio's is het schadebedrag onbekend. Wel zijn er informatiebeveiligingsissues bekend met het Landelijk crisismanagementsysteem (LCMS) en in een veiligheidsregio.
Het aantal gemelde cyberaanvallen op overheidswebsites en -systemen is in de afgelopen twee jaar verdubbeld. Het Nationaal Cyber Security Centrum (NCSC) krijgt bijna dagelijks bericht over een aanval. Van mei 2014 tot mei 2015 kwamen er 293 meldingen binnen bij het NCSC. Ook het aantal aanvallen op bedrijven is toegenomen.
De aanvallers zijn vaak criminele organisaties en buitenlandse overheden op zoek naar waardevolle informatie. De laatste maanden is een toename te zien in het gebruik van cryptoware door hackers. Dat is software waarmee hackers bestanden op andere computers kunnen versleutelen. De aanvallers willen de versleuteling opheffen voor geld.
In maart waren er twintig meldingen van cryptoware, de meeste daarvan bij de rijksoverheid. Het mag duidelijk zijn dat herstel met aanzienlijke kosten gepaard kan gaan.

Minstens zo belangrijker echter is het voorkomen van de schade die ontstaat door het gedrag van eigen medewerkers. Menselijke fouten en slordigheden kunnen tot hoge kosten leiden.

In enkele veiligheidsregio's heeft in het verleden een incident plaatsgevonden. Hieronder worden de belangrijkste effecten beschreven van een veiligheidsregio die in 2015 met het Cryptolocker-virus te maken heeft gehad.

- *Gedurende 1 dag zijn enkele basisvoorzieningen op het gebied van ICT uit de lucht geweest: systeem voor toegang tot het netwerk, het intranet, de mailvoorziening en de file-servers (vakgroepschijven).*
- *Gedurende 1 dag hebben een flink aantal secundaire processen stilgelegen vanwege uit de lucht zijn van onder meer de financiële systemen, P&O-systemen, facilitaire systemen en documentsystemen en genoemde basisvoorzieningen.*
- *Gedurende 1 dag is een aantal systemen, ondersteunend aan het primair proces, uit de lucht geweest. Dit betrof met name de Geo-omgeving, systeem voor mobiele operationele informatie, document/processensysteem en het planningsysteem.*
- *Kritische systemen zoals GMS, P2000 en C2000 werden niet geraakt.*
- *Bijeenroepen van Kernteam Continuïteit en een aantal procesverantwoordelijken: impact op de dag zelf (gedurende een groot deel van die dag) voor een groot aantal medewerkers.*
- *Primaire focus en extra inzet van de afdeling ICT gedurende enkele dagen alleen gericht op incidentbeheersing en vervolgens op het op een veilige wijze weer in de lucht brengen van de systemen.*
- *Gedurende 1 dag is het netwerk gescheiden geweest van het meldkamerdomein waardoor operationele informatie niet meer geautomatiseerd gedeeld kon worden. Hiermee werden weliswaar primaire processen geraakt maar deze zijn niet in gevaar geweest. Er is namelijk overgegaan tot spraakoverdracht van operationele informatie.*
- *Verlies van data.*
- *Extra inspanning om het HR-systeem weer volledig in de lucht te krijgen.*
- *Extra inzet externen (€ 6.700,-).*

Van veiligheidsregio's wordt verwacht dat zij onder alle omstandigheden hun werk blijven doen; informatieveiligheid draagt bij aan bedrijfscontinuïteit en voorkomt imagoschade. Het is daarom van groot belang dat de veiligheidsregio's goed zijn voorbereid op beveiligingsrisco's. Dit betekent dat van tevoren is nagedacht over de mogelijke gevolgen van risico's en de maatregelen die daarvoor noodzakelijk zijn.

In de Nationale Cybersecurity Strategie 2 wordt het belang van verdergaande digitalisering en de innoverende kracht die daarvan uitgaat, gezien als een belangrijke stimulans voor maatschappelijke groei. Een goede informatiebeveiliging is daarbij een randvoorwaarde.

3.2 Baten en kosten

Baten en maatschappelijk rendement

De baten van een goede informatiebeveiliging zijn veelal maatschappelijk, te weten:

- Bedrijfscontinuïteit;
- Betrouwbaarheid;
- Robuustheid.

Daarnaast zijn er besparingen door het niet laten ontstaan van kosten, als gevolg van verstoring van de werkprocessen en ontvreemding van gegevens.

Deze baten zijn moeilijk op voorhand te kwantificeren; enkel door het uitvoeren van een risicoanalyse op de betreffende bedrijfsprocessen kunnen de baten helder in beeld worden gebracht.

Kosten

Landelijke projectkosten

Van januari 2016 tot en met juni 2018, dus voor een periode van 2½ jaar, is een landelijk projectleider nodig voor gemiddeld drie dagen (24 uur) per week. Deze projectleider coördineert en faciliteert de activiteiten van de veiligheidsregio's op basis van een collectief plan (zie 5.1.1). Daarnaast worden kosten begroot voor inhuur van derden, communicatie etc.

Deze landelijke projectkosten worden gedekt vanuit het werkbudget Informatievoorziening van het Veiligheidsberaad, omdat het een begeleidingsproject betreft. Voorbehoud is dat dit budget ook na 2016 beschikbaar is.

Op jaarbasis bedragen de kosten:

Omschrijving	Bedrag
Salariskosten projectleider (1.248 uur à € 60,- o.b.v. detachering VR)	€ 74.880,-
Btw (21%)	€ 15.725,-
Handling fee IFV (1,85%)	€ 1.676,-
Reiskosten projectleider	€ 5.000,-
Inhuur expertise (derden)	€ 15.000,-
Diversen/onvoorzien	€ 5.000,-
Communicatie	€ 3.000,-
Totaal	**€ 120.281,-**

Voor de jaren 2016 t/m 2018 betekent dit:

Jaar	Bedrag
2016	€ 120.281,-
2017	€ 120.281,-
2018 (tot 1 juli)	€ 60.140,-
Totaal	**€ 300.702,-**

Verder wordt van veiligheidsregio's capaciteit gevraagd voor de uitvoering van het landelijke project, te weten 150 uur op jaarbasis per regio.

Regionale kosten

Verder moeten veiligheidsregio's ieder zelf de maatregelen ontwikkelen en implementeren. Deze kosten verschillen per veiligheidsregio; afhankelijk van de uitgangssituatie, kunnen deze kosten substantieel zijn.
In principe behoren kosten voor informatieveiligheid toegerekend te worden aan bedrijfsprocessen en bijbehorende applicaties; in ieder geval behoren ze in beschouwing te worden genomen bij lopende trajecten/projecten.

Te denken valt bijvoorbeeld aan kosten voor:

- Inzet medewerkers;
- Op orde brengen van beheer van vitale informatiesystemen;
- Aanschaf, implementatie en beheer van firewall, antivirussoftware en 'intrusion detection-' en 'intrusion prevention-systemen';
- Aansluiten bij een 'security operations center' (SOC), zoals bijvoorbeeld de IBD;
- Beperken van risico's door bijvoorbeeld inrichten van uitwijkvoorzieningen;

- Herontwerpen van bedrijfsprocessen;
- Ontwikkelen, implementeren en auditen van beleid en procedures (bijvoorbeeld beleid t.a.v. wachtwoorden en mobiele apparatuur);
- Herontwerp van software (‘secure software development);
- Invoering van de functie ‘Chief information security officer’ (CISO);
- Inhuur van derden voor begeleiding, opleiding en training;
- Het volgen van de Masterclass Informatieveiligheid OOV;
- Deelname aan congressen en symposia over informatieveiligheid en -beveiliging;
- etc.

Wat dit betekent voor veiligheidsregio’s, is lastig in te schatten. Een en ander is ook afhankelijk van de maatregelen die veiligheidsregio’s reeds hebben genomen. Verdedigbaar is om een bepaald percentage van de structurele ICT-uitgaven te nemen, dat aan informatiebeveiliging dient te worden besteed.
Gartner, een internationaal onderzoeks- en adviesbureau in de informatietechnologiesector, geeft aan dat het gebruikelijk is dat tussen de 5 en 10% van het IT-budget aan IT-beveiliging wordt besteed.
De Taskforce BID, op 13 februari 2013 door minister Plasterk (BZK) voor een periode van twee jaar in het leven geroepen, geeft aan dat in veel corporate ICT-budgetten tussen 8 en 12 % van het budget besteed wordt aan security.
Naar verwachting zullen deze kosten in de loop van de tijd afnemen, door samenwerking op het gebied van ICT-infrastructuur en applicaties (de projecten ‘Landelijke ICT-voorziening’ en ‘Gemeenschappelijke applicaties’ binnen het programma Informatievoorziening Veiligheidsregio’s).

4 Aanpak en planning

4.1 Aanpak

Zoals in hoofdstuk 1 is aangegeven, is het project Informatieveiligheid al op 1 november 2014 gestart. Tijd is besteed aan onder meer de volgende zaken:

- Het analyseren van de resultaten van de quick scan en rapportage richting veiligheidsregio's;
- Het op gang brengen van een bewustwordingsproces bij veiligheidsregio's;
- Afstemming en overleg met organisaties zoals de Taskforce BID, de IBD, het Centrum voor Informatiebeveiliging en Privacybescherming (CIP);
- Het bezoeken van congressen/symposia en deelname aan bijeenkomsten van cybersecurity-communities;
- Overleg met adviseurs en leveranciers van informatiebeveiligingsproducten;
- Organiseren van bijeenkomsten informatieveiligheid;
- Vergaren en delen van kennis;
- etc.

De groeiende belangstelling voor deelname door veiligheidsregio's aan de bijeenkomsten Informatieveiligheid die het project met enige regelmaat organiseert, laat zien dat het bewustwordingsproces (de belangrijkste doelstelling in 2015) haar vruchten afwerpt. Veiligheidsregio's nemen hun verantwoordelijkheid t.a.v. informatieveiligheid serieus en zijn bereid om hierin te investeren.

Om deze bewustwording vanuit het collectieve belang ook op bestuurlijk niveau te bekrachtigen, zal een gezamenlijke intentieverklaring worden opgesteld, waarin de 25 besturen naar elkaar uitspreken tot het gewenste niveau van informatieveiligheid te komen.

De veiligheidsregio's voeren bovendien op basis van de collectief geformuleerde standaarden een jaarlijkse GAP-analyse uit. Vanuit het landelijke project wordt hierop gemonitord en gerapporteerd.

Korte termijn

Op korte termijn dient de focus te liggen op het hanteerbaar maken van de BIG voor veiligheidsregio's. Niet alles in de BIG is even relevant; gekeken moet worden naar díe maatregelen uit de BIG die op korte termijn het meeste resultaat opleveren ('laaghangend fruit') zoals bijvoorbeeld de implementatie van een robuust wachtwoordbeleid.
Complicerende factor is dat de BIG op onderdelen mogelijk te beperkt is omdat binnen sommige regio's ook ambulancezorg en/of de GGD is ondergebracht. In dergelijke gevallen kan de NEN 7510 (Informatiebeveiliging in de zorg) uitkomst bieden.
Mogelijk dat de BIG samengevoegd moet worden met relevante onderdelen uit de NEN 7510, met als resultaat een soort Baseline Informatiebeveiliging Veiligheidsregio's (BIVR).

4.2 Overall planning

Jaar	Activiteit
2015	> Bewustwording, aanbieden handreiking > Projectplan Informatieveiligheid 2016-2018
2016	> Projectplan binnen programma IV akkoord > Bestuurlijke intentieverklaringen > Detailplan > Bepalen baseline Informatieveiligheid veiligheidsregio's > Verbeterplannen per veiligheidsregio > Implementatie in veiligheidsregio's (indien gewenst o.b.v. landelijke pilots)
2017/2018	> Implementatie in veiligheidsregio's > Basisniveau Informatieveiligheid landelijk gerealiseerd
2018	> Borging basisniveau Informatieveiligheid en afsluiting project

4.3 Planning per activiteit en tussenresultaten

De onderstreepte items hieronder geven de tussenresultaten weer.

2015 Q4 Projectplan Informatieveiligheid 2016-2018
Definitieve goedkeuring van het projectplan door het Veiligheidsberaad op 18 maart 2016.

2016 Q1 Detailplan
In januari 2016 zal een detailplan worden opgesteld met daarin onder meer een nader uitgewerkte projectstructuur, concrete stappen (activiteiten) en mijlpalen (producten).

Baseline Informatieveiligheid
Met de BIG als vertrekpunt, wordt de baseline voor veiligheidsregio's bepaald, met input vanuit de regio's. Daarnaast kunnen relevante onderdelen uit de NEN 7510 aan de baseline worden toegevoegd.

2016 Q2 Verbeterplannen per veiligheidsregio
Op basis van jaarlijkse GAP-analyses en monitoring stellen veiligheidsregio's verbeterplannen op. Een verbeterplan beschrijft de huidige en gewenste situatie inclusief de maatregelen die genomen moeten worden.

2016 Q3/ 2018 Q1 Uitvoering van de verbeterplannen en inrichten borging

2018 Q2 Afsluiting project

Tijdens het project zullen diverse formats worden ontwikkeld, bijvoorbeeld voor informatiebeveiligingsbeleid en informatiebeveiligingsplannen, risicoanalyses, dataclassificatie etc.

Deze formats dienen ter ondersteuning van regio's bij de implementatie van maatregelen zoals opgenomen in de verbeterplannen. Als basis voor de formats worden de producten uit de operationele variant van de BIG gebruikt.

Indien nodig en gewenst kunnen productontwikkelingen en implementaties in de veiligheidsregio's worden verkend met behulp van landelijke pilots in enkele regio's.

Afhankelijk van de behoefte van veiligheidsregio's wordt verder onderzocht of het wenselijk is om een aantal zaken centraal op te pakken. De gedachten gaan dan bijvoorbeeld uit naar het delen van 'Chief information security officers', door het inrichten van een pool met dergelijke functionarissen. Soortgelijke constructies kunnen een kostendrukkend effect hebben. Ook wordt dan bekeken of aansluiting bij een 'security operations center', zoals bijvoorbeeld de IBD, wenselijk is of dat alternatieven de voorkeur verdienen.

5 Organisatie

5.1 Rollen en bezetting

Opdrachtgever

Het Veiligheidsberaad treedt namens de veiligheidsregio's op als bestuurlijk opdrachtgever. Het Veiligheidsberaad stuurt op het programma via het jaarplan en het jaarverslag van het IFV. Het Dagelijks Bestuur van het Veiligheidsberaad ziet als opdrachtgever binnen de gestelde kaders toe op de uitvoering van het programma. De portefeuillehouder Informatievoorziening behartigt deze taak binnen het DB.

Het gedelegeerd opdrachtgeverschap ligt bij de voorzitter van het programmaoverleg informatievoorziening veiligheidsregio's (POI VR). Het POI stuurt op de inhoudelijke uitvoering van het programma. Het POI ziet er op toe dat verschillende geledingen van de veiligheidsregio's maximale invloed hebben op inhoudelijk uitwerking van de onderdelen van het programma.

Opdrachtnemer

Het IFV treedt op als opdrachtnemer en faciliteert en coördineert de uitvoering van het programma. Dit gebeurt in coproductie met de veiligheidsregio's[1].

De programmamanager is namens de opdrachtnemer verantwoordelijk voor de uitvoering en is budgethouder. De programmamanager rapporteert aan de directie van het IFV en legt namens de directie van het IFV inhoudelijk verantwoording af aan het POI.

Projectleider

De projectleider wordt aangesteld door de opdrachtnemer en heeft onder meer de volgende taken:

- Algehele coördinatie;
- Op gang brengen en houden van een bewustwordingsproces t.a.v. informatieveiligheid;
- Ontwikkelen en opstarten van pilots;
- Inbrengen van kennis, expertise en advies;
- Ontwikkelen van standaarden in samenwerking met veiligheidsregio's;
- Ondersteunen en motiveren van veiligheidsregio's bij de ontwikkeling en implementatie van instrumenten zoals informatiebeveiligingsbeleid etc.;
- Bewaken van de samenhang in de regionale ontwikkelingen;
- Bewaken van de voortgang in de veiligheidsregio's;
- Deelname aan landelijke communities op het gebied van informatieveiligheid en privacybescherming, zoals de practioners communities van het 'Centrum informatiebeveiliging en privacybescherming' (CIP);
- Deelname aan congressen en symposia over informatieveiligheid en informatiebeveiliging.

[1] Het bestuur van het Instituut Fysieke Veiligheid kan in opdracht van een of meer besturen van de veiligheidsregio's werkzaamheden uitvoeren ten behoeve van de veiligheidsregio's, waaronder het ondersteunen bij de uitvoering van de taak, bedoeld in artikel 22 (artikel 69 Wet veiligheidsregio's)

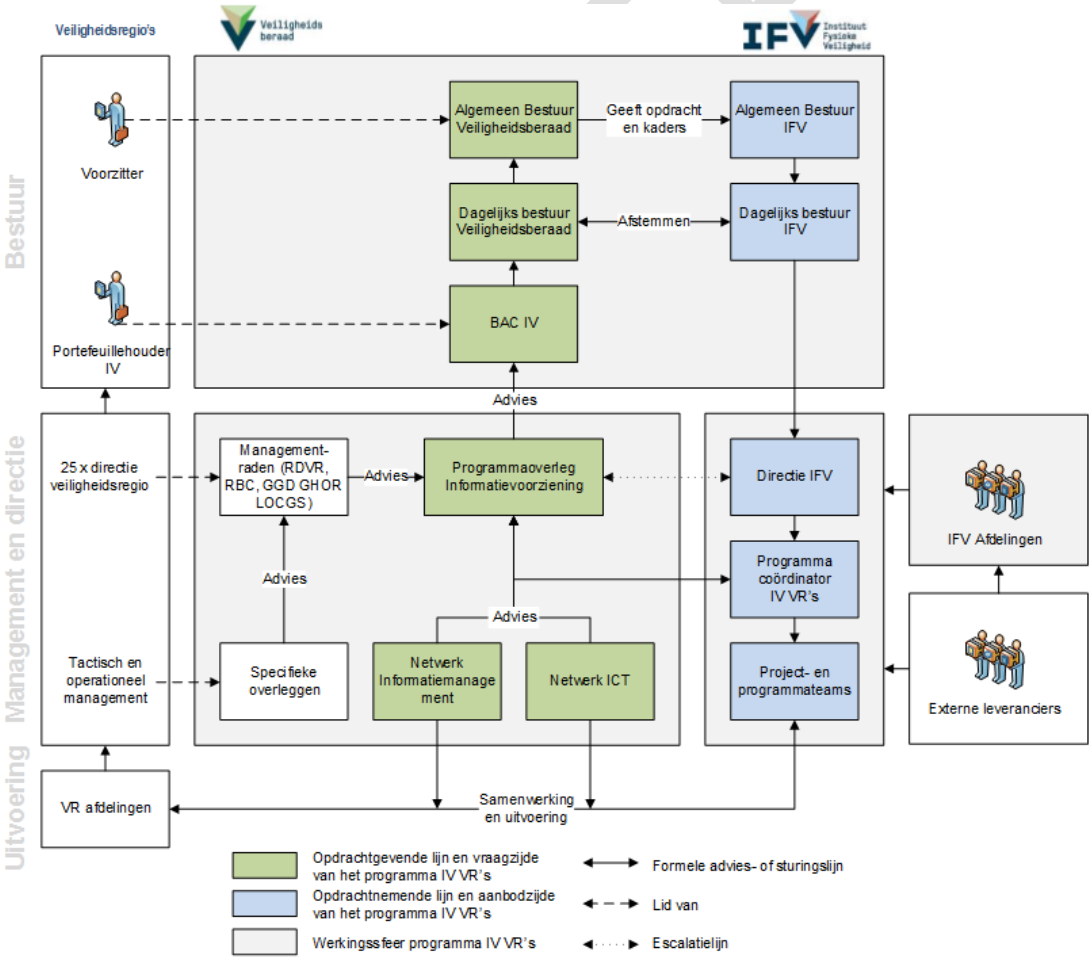
Medewerkers veiligheidsregio's

Specialisten van de veiligheidsregio's op het gebied van informatievoorziening en ICT en zo nodig leden van functionele (gebruikers)netwerken worden door de projectleider betrokken in de projectgroep. In de projectgroep worden standaarden bepaald, producten ontwikkeld en de samenhang bewaakt. De vakgroep Informatieveiligheid kan fungeren als klankbordgroep.

De projectgroep kan in wisselende samenstelling haar werkzaamheden verrichten om overbelasting van leden te voorkomen. Het uitgangspunt is dat de 25 veiligheidsregio's tezamen 3.744 uur op jaarbasis leveren (zie 2.5).
Na accordering van dit projectplan zal een detailplanning worden opgesteld waarin per deelgebied wordt aangegeven hoe de bemensing van de verschillende werkgroepen zal zijn.

5.2 Projectstructuur

In de figuur hieronder is de projectstructuur weergegeven. Het project Informatieveiligheid is één van de zes projecten uit het programma Informatievoorziening Veiligheidsregio's van het Veiligheidsberaad.



5.3 Besluitvorming

Op 9 september 2015 heeft het POI onderstaande matrix met taken, bevoegdheden en verantwoordelijkheden aangaande het programma IV vastgesteld. Het project Informatieveiligheid volgt deze lijn.

	Actoren											
Kernactiviteiten, producten of processen	Voorzitter Programmaoverleg IV	Leden Programmaoverleg IV	Secretaris Programmaoverleg IV	Programmacoördinator IV	Voorzitters netwerken IM en ICT	Portefeuillehouders NIM/NICT	Netwerk Informatiemanagement	Netwerk ICT	Functionele netwerken/gremia	Netwerken Inkoop & Verwerving	Projectleiders	Directie IFV
Projectmanagement												
Fase: Beleid												
Opstellen visiedocumenten	A	S/C	I	R	S	S	C	C	C	O	O	I
Stellen van prioriteiten	A	S/C	I	R	S	S	C	C	C	O	O	I
Verkennen en experimenteren	A	S/C	I	R	S	S	C	C	C	O	O	I
Toesten aan kaders (architectuur/standaarden)	A	S/C	I	R	S	S	C	C	C	O	O	I
Opstellen business case	A	S/C	I	I	S	S	C	C	C	O	R	I
Fase: Ontwerp												
Opstellen projectplan	A	S/C	I	I	S	S	C	C	C	O	R	I
Herijken business case	A	S/C	I	I	S	S	C	C	C	O	R	I
Opstellen projectstartarchitectuur	A	S/C	I	I	S	S	C	C	O	O	R	I
Opstellen PvE	A	S/C	I	I	S	S	C	C	C	C	R	I
Opstellen beheerplan	A	S/C	I	I	S	S	C	C	C	O	R	I
Fase: Realisatie												
Projectmanagement	A	S/C	I	I	S	S	C	C	C	O	R	I
Inkoopadvisering	A	S/C	I	I	S	S	C	C	C	R	O	I
Aanbestedingsadvisering en/of -begeleiding	A	S/C	I	I	S	S	I	I	I	R	O	I
Fase: Beheer												
Beheren van producten	I	S/C	I	I	S	S	C	C	C	O	O	A

A = Accountable (eindverantwoordelijk vanuit doelmatigheid)
R = Responsible (resultaatverantwoordelijk, als projectleider/programmacoördinator)
C = Consulted (verplicht te betrekken, door resultaatverantwoordelijke)
S = Supportive (ondersteunend aan het proces)
I = Informed (te informeren, door resultaatverantwoordelijke)
O = Out of loop (geen direct onderdeel van het proces)

(Nieuwe) activiteiten binnen het project Informatieveiligheid volgen, vergelijkbaar met het programma IV, een cyclus van beleid, ontwerp, realisatie en beheer.

5.4 Afstemming met betrokkenen

De projectstructuur zoals in 5.2 geschetst, leidt er toe dat afstemming met stakeholders geborgd is. Afstemming met derden (leveranciers, adviesbureaus etc.) zal door de projectleider worden verzorgd.

5.5 Communicatie

Over de voortgang van het project zal periodiek worden gecommuniceerd; de intentie is om elk kwartaal een voortgangsverslag te publiceren. Met afdeling Communicatie van het IFV zal nog worden overlegd op welke wijze dit het best kan geschieden.

6 Sturing en verantwoording

In dit hoofdstuk wordt ingegaan op de eisen aan de uitvoering, op de projectrisico's en tegenmaatregelen en op monitoring en rapportage.

6.1 Eisen aan de uitvoering

Het project Informatieveiligheid is een project dat geen 'tastbare' resultaten oplevert zoals applicaties, informatiesystemen etc., maar documentatie zoals een baseline Informatieveiligheid, informatiebeveiligings- en verbeterplannen (met als resultaat een adequaat niveau van informatieveiligheid).
Omdat deze zaken minder zichtbaar zijn dan applicaties en informatiesystemen, bestaat het risico dat er onvoldoende 'sense of urgency' is en het project ten onder zou kunnen gaan aan het 'geweld' van de andere vijf projecten uit het programma en/of aan regionale prioriteiten.
Het staat buiten kijf dat het project noodzakelijk is om de continuïteit van bedrijfsprocessen van veiligheidsregio's te kunnen waarborgen. Daarom dient er sprake te zijn van een stevige regie vanuit het IFV (projectleider) die mandaat moet hebben om te sturen op het behalen van tussenresultaten (milestones) zoals in 4.3 is aangegeven. Cruciaal daarbij is de bereidheid van veiligheidsregio's om de doelstelling, zoals verwoord in 2.2, te behalen.

6.2 Risico's en tegenmaatregelen

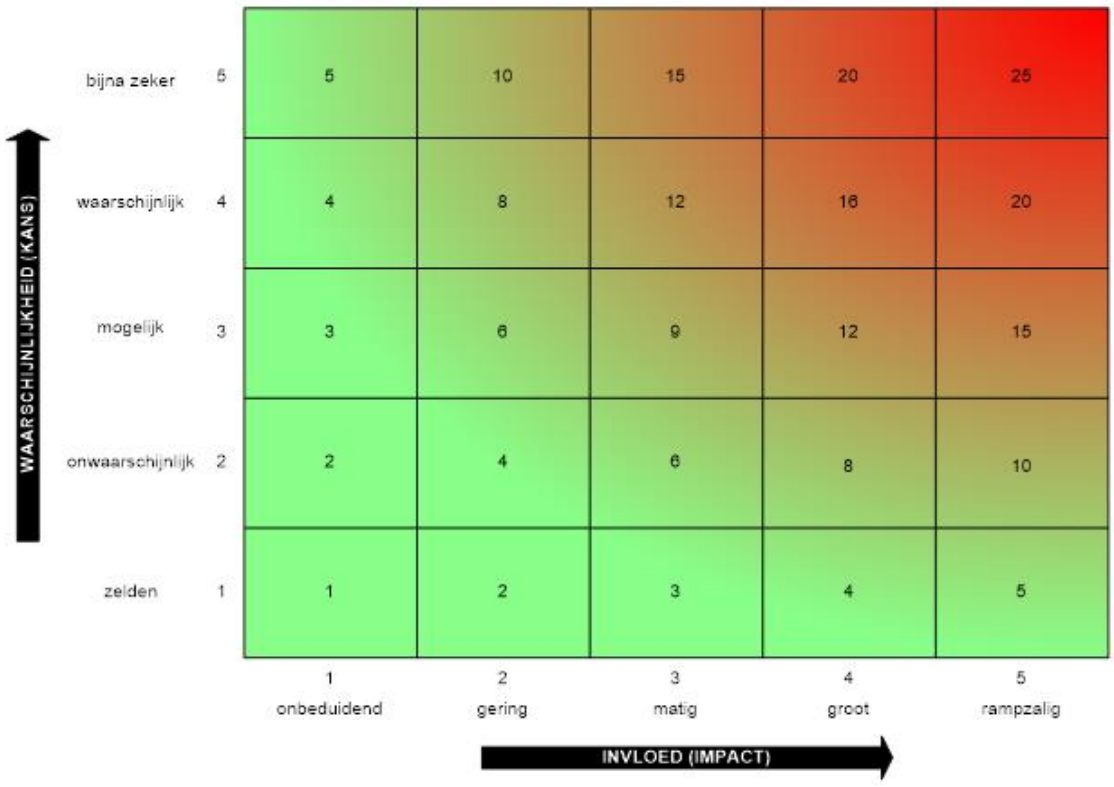
De volgende risico's en tegenmaatregelen, afgezet in een 5 x 5 risico-matrix, worden voor dit project onderkend. Het product van kans en impact wordt gezien als het risiconiveau per item (R = K x I).

Risico	Kans	Impact	Risico-niveau	Tegenmaatregel
Inzet IFV kan niet of in onvoldoende mate geleverd worden	2	4	8	Tijdig budget aanvragen via POI en DB VB
Inzet NIM/NICT en/of medewerkers veiligheidsregio's kan niet of in onvoldoende mate geleverd worden	3	3	9	In NIM/NICT ruim aandacht schenken aan het belang van informatieveiligheid. In overleg met de secretaris NIM, informatieveiligheid als vast onderdeel op de agenda zetten
Informatieveiligheid krijgt onvoldoende prioriteit in de veiligheidsregio	4	4	16	Management veiligheidsregio's wijzen op bestuurlijke prioriteit, afspraken die zijn gemaakt in het kader van het programma IV en het projectplan Informatieveiligheid, en de resultaten van de quick scan

Onvoldoende financiële middelen in veiligheidsregio's om alle noodzakelijke maatregelen te kunnen implementeren	4	4	16	Veiligheidsregio's wijzen op tijdig alloceren van middelen. Aangeven wat gevolgen kunnen zijn bij onvoldoende investeren in informatieveiligheid
Te implementeren maatregelen hebben onvoldoende draagvlak in veiligheidsregio's	3	4	12	Gevolgen aangeven van niet implementeren. Masterclass Informatieveiligheid organiseren voor management veiligheidsregio's met als belangrijkste doel bewustwording informatieveiligheid en de verantwoordelijkheid van afdelingshoofden voor de eigen (bedrijfs)processen.

Op basis van de onderstaande matrix voor risiconiveaus kan hiermee een risicoplan worden gemaakt. Risico's in het oranje/rode gebied vormen daarbij een bedreiging voor het project en dienen beperkt te worden.

5 X 5-matrix risiconiveaus



6.3 Monitoring en rapportage

Het Dagelijks Bestuur van het Veiligheidsberaad ziet als opdrachtgever binnen de gestelde kaders toe op de uitvoering van het programma. De portefeuillehouder Informatievoorziening behartigt deze taak binnen het DB.

Het POI stuurt op de inhoudelijke uitvoering van het programma geo. Het POI ziet er op toe het netwerk Informatiemanagement en de vakgroep Geo en Basisregistraties maximale invloed hebben op inhoudelijk uitwerking van de onderdelen van het programma.

Voortgangsrapportage

Per kwartaal stelt de programmamanager een voortgangsrapportage op en biedt deze namens de directie aan het POI aan. Het POI stelt de voortgangsrapportage vast. Het netwerk Informatiemanagement adviseert daarbij.

Jaarverslag

Jaarlijks stelt de programmamanager een jaarverslag op, inclusief verantwoording van inkomsten en uitgaven. Het POI is verantwoordelijk voor het tijdig aanbieden van een jaarverslag, inclusief verantwoording van inkomsten en uitgaven voor vaststelling door de bestuurlijk opdrachtgever.

Delen van het jaarverslag dien voor het jaarverslag van het IFV.

7 Financiën

7.1 Budget

Het benodigde budget voor de landelijke projectkosten wordt beschikbaar gesteld vanuit het werkbudget Informatievoorziening van het Veiligheidsberaad, mits dit budget ook na 2016 beschikbaar is. Daarnaast wordt van veiligheidsregio's capaciteit gevraagd voor de uitvoering van het landelijke project, te weten 150 uur op jaarbasis per regio.

7.2 Begroting

In pararaaf 3.2.2 zijn voor de jaren 2016 t/m 2018 de landelijke projectkosten aangegeven, voor landelijke coördinatie, inhuur van aanvullend specialisme, ontwikkeling van standaarden en communicatie. Aannemelijk is te veronderstellen dat veiligheidsregio's een veelvoud van deze kosten kwijt zijn als informatieveiligheid afzonderlijk wordt opgepakt door regio's. De kracht van het project zit in het gezamenlijk tackelen van de problematiek en het te verwachte synergie-effect.

Naast bovengenoemde landelijke kosten moeten regio's rekening houden met regionale kosten, zoals eveneens genoemd in 3.2.2. Deze kunnen substantieel zijn, afhankelijk van in welke mate er al maatregelen zijn getroffen. Het lijkt verstandig om voor informatiebeveiliging, zoals reeds aangegeven, 10% van het ICT-budget te bestemmen voor de jaren 2016 en verder.

Bijlagen

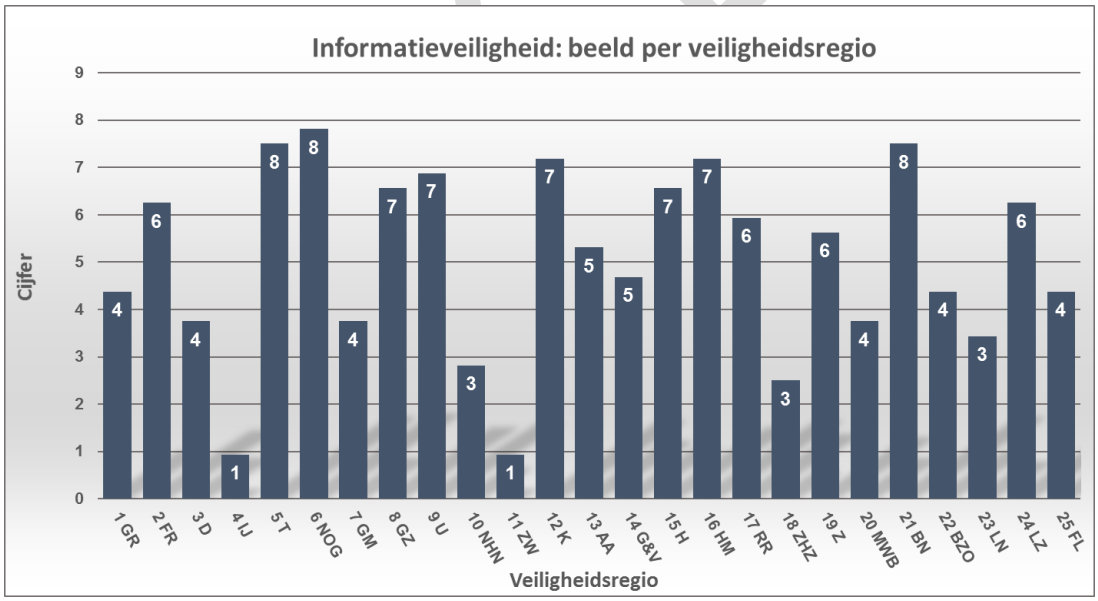
A. Beeld per veiligheidsregio

De quick scan Cybersecurity, onderdeel van de landelijke I-scan Veiligheidsregio's, bevatte de volgende acht items:

1. Directie en bestuur hebben over informatiebeveiliging gesproken;
2. Het informatieveiligheidsplan is vastgesteld;
3. Acties ter vergroting van het informatieveiligheidsbewustzijn zijn uitgevoerd;
4. Acties ter verbetering van technische aspecten van i-veiligheid zijn uitgevoerd;
5. Er is een risicoanalyse uitgevoerd;
6. Bedrijfskritische systemen zijn in kaart gebracht;
7. Controles m.b.t. uitgegeven autorisaties zijn uitgevoerd;
8. Specifieke aandacht is besteed aan informatiebeveiliging in audits.

Op een schaal van 1 tot 10 scoren de regio's gemiddeld een 5.
Vooral de antwoorden op vragen 2, 5 en 8 leverde een lage score op.

Hieronder een overzicht van de resultaten per veiligheidsregio.



Bij de interpretatie van de resultaten is enige voorzichtigheid geboden; vraagtekens kunnen worden gezet bij de validiteit en betrouwbaarheid van de set vragen. In ieder geval geven de resultaten een zekere tendens weer.

B. Lopende initiatieven binnen het project

1. **Aansluiting bij de Informatiebeveiligingsdienst van de VNG/KING (IBD)**
   De IBD richt zich op bewustwording en concrete (incident)ondersteuning aangaande informatiebeveiliging.
   Eén van de doelen van de IBD is het aan gemeenten leveren van concrete ondersteuning in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging. Hiertoe heeft de IBD, net als haar ketenpartner het NCSC, een Computer Emergency Response Team (CERT)-functie om zo preventie, detectie en coördinatie van informatiebeveiligingsincidenten binnen de gemeentelijke overheid mogelijk te maken. Voor specifieke dienstverlening vanuit de IBD is het noodzakelijk dat de IBD-CERT bepaalde gemeente-specifieke gegevens ontvangt. Hiervoor moeten gemeenten 'officieel' aansluiten bij de IBD.
   Eind april 2015 heeft er een overleg plaatsgevonden tussen de projectleider en dhr. Weerwind, burgemeester van Velsen en tevens bestuurlijk trekker van het dossier 'Informatiebeveiliging' binnen de VNG. Doel was om de mogelijkheid te verkennen van aansluiting door veiligheidsregio's bij de IBD. Vooralsnog kunnen enkel gemeenten aansluiten bij de IBD; echter veiligheidsregio's zijn gemeenschappelijke regelingen van gemeenten die grotendeels gefinancierd worden door de deelnemende gemeenten. Er is sprake van verlengd lokaal bestuur.
   Voor wat informatievoorziening betreft zijn gemeenten en veiligheidsregio's in belangrijke mate van elkaar afhankelijk: informatiestromen bewegen heen en weer tussen gemeenten en veiligheidsregio's. Er is dus een gemeenschappelijk belang en zeker voor wat betreft het op orde houden van de crisisbeheersing en rampenbestrijding waarbij de inzet van informatietechnologie niet meer is weg te denken.
   Het lijkt logisch dat gemeenten (en dus ook de IBD) een zekere verantwoordelijkheid hebben voor informatieveiligheid bij veiligheidsregio's.
   Dhr. Weerwind stond niet negatief tegenover het verzoek tot aansluiting mits dit goed zou worden onderbouwd.
   De komende periode zal in overleg met de veiligheidsregio's bekeken worden of aansluiting bij de IBD nog steeds wenselijk is of dat alternatieven de voorkeur verdienen.

2. **Opzetten van een kennis- en uitwisselingsplatform op 'MijnBrandweer'**
   Op 'MijnBrandweer' (Viadesk) is een mappenstructuur ingericht voor informatieveiligheid. De mappenindeling komt overeen met de indeling van de tactische variant van de BIG. In deze mappen kunnen veiligheidsregio's documenten plaatsen en met elkaar delen. Initieel zullen de mappen gevuld worden met producten uit de operationele variant van de BIG.

C. Dreigingen

Het niveau van informatieveiligheid zoals in 2.2 genoemd, biedt geen bescherming tegen dreigingen door terreurgroepen, inlichtingendiensten en zwaar georganiseerde (internet)criminaliteit. Hiervoor zijn aanvullende maatregelen nodig die het niveau van de BIG overstijgen; risicoanalyses zijn dan vereist.

De intentie is om in ieder geval weerstand te kunnen bieden aan de twee hieronder genoemde categorieën dreigingen. Garanties kunnen niet worden gegeven; echter door het invoeren van een robuust informatiebeveiligingsbeleid kunnen risico's wel worden geminimaliseerd.

1. Specifieke dreigingen

a. *(Ex-)werknemer*:
   - opereert van binnenuit;
   - neemt datawraak;
   - ontvreemdt bijvoorbeeld adressenbestanden, presentaties, offertes en strategische informatie.

b. *Script kiddy*:
   - gebruikt op internet vrij verkrijgbare tools;
   - probeert op goed geluk 'binnen te komen';
   - doet er weinig moeite voor.

c. *Hacker*:
   - gebruikt professionele software;
   - richt zich op de organisatie of website;
   - heeft toegang tot uitgebreide hackersbronnen;
   - houdt kennis op peil door trainingen en opleidingen.

2. Algemene dreigingen

a. Onopzettelijk menselijk handelen
b. Opzettelijk menselijk handelen
c. Onbeïnvloedbare externe factoren (bijvoorbeeld blikseminslag, overstroming etc.)
d. Technisch falen