Convenant CERT verzekeringssector

2017

VERBOND VAN VERZEKERAARS

Overeenkomst tussen Aangesloten verzekeraars inzake samenwerking en het Computer Emergency Response Team voor de Nederlandse verzekeringssector (i-CERT)

Overwegende dat:

- verzekeraars in toenemende mate te maken krijgen met (nieuwe) dreigingen en risico's die gepaard gaan met de voortschrijdende digitalisering van de samenleving en hun interne bedrijfsvoering;
- verzekeraars deel uitmaken, en in hoge mate afhankelijk zijn, van een bredere IT-ketenomgeving die versnipperd en complex is en waarin centrale regie op informatiebeveiliging vrijwel ontbreekt;
- verzekeraars in deze ketenomgeving verantwoordelijk zijn en blijven voor grote hoeveelheden en uiteenlopende soorten (privacygevoelige) informatie, alsmede voor een adequate en continue dienstverlening aan consumenten;
- uit toezichtonderzoek en analyses van de gegevensuitwisseling en het IT-landschap van de sector blijkt dat verzekeraars relatief kwetsbaar zijn voor (de gevolgen van) digitale inbreuken en datalekken;
- cyberincidenten grote bedrijfseconomische schade veroorzaken (verstoring, advies, herstel, boetes, etc.) en daarnaast ook tot aanzienlijke reputatieschade kunnen leiden;
- een slagvaardige, snelle, operationele samenwerking en onderlinge informatiedeling, noodzakelijk is om de digitale weerbaarheid van verzekeraars te verbeteren en bovenstaande risico's te beheersen;
- verzekeraars hierdoor op het (non-concurrentiele) terrein van cyber security flinke synergievoordelen kunnen behalen en de snel stijgende kosten die gepaard gaan met noodzakelijke beveiligingsmaatregelen en -oplossingen beter in de hand kunnen houden;
- verzekeraars daarom via het Bestuur van het Verbond van Verzekeraars hebben besloten een samenwerkingsverband en sectoraal Computer Emergency Response Team (CERT) in te richten op basis van een hiertoe uitgevoerd haalbaarheidsonderzoek (zie circulaire LV-2015-40);
- het Bestuur op 15 december 2016 besloten heeft deze operationele samenwerking vast te leggen in het onderhavige convenant, met borging van de randvoorwaarden voor doorgroei naar een volwassener CERT-model;
- verzekeraars via deze CERT als 'single point of contact' in de bedrijfstak tevens gebruik kunnen maken van de product- en dienstverlening van het Nationaal Cyber Security Centrum (NCSC) en relevante informatie van andere sectorale CERT's kunnen ontvangen.

1 Begripsomschrijvingen

In dit convenant wordt verstaan onder:

i-CERT	[insurance-CERT] de centrale dienst binnen de verzekeringssector die Aangesloten verzekeraars doorlopend informeert en adviseert over digitale dreigingen, kwetsbaarheden en incidenten. De i-CERT fungeert voor verzekeraars tevens als 'single point of contact' en doorgeefluik voor operationele samenwerking en informatie-uitwisseling met Partnerorganisaties buiten de sector.
Aangesloten verzekeraar	elke verzekeraar óf verzekeringsgroep die heeft ingetekend op dit convenant en, indien voldaan is aan de hierin beschreven voorwaarden, gebruik kan maken van de dienstverlening van de i-CERT.
Contactpunt	de afdeling of medewerker van een Aangesloten verzekeraar die is aangewezen om de operationele communicatie met de i-CERT te onderhouden.
Deelnemer	een Aangesloten verzekeraar die aan de in artikel 2.2.3 vastgelegde criteria voldoet en daarom geacht wordt bij toerbeurt de i-CERT dienst uit te voeren. Aangesloten verzekeraars die ook kwalificeren als 'Deelnemer' hebben aanvullende rechten en plichten binnen het onderhavige samenwerkingsverband.
Deelnemer van dienst	de Deelnemer die conform het vastgestelde roulatiemodel aan de beurt is om de in artikelen 3 en 7.1 beschreven i-CERT taken uit te voeren.
Partnerorganisatie	het NCSC, een andere sectorale CERT of elke andere organisatie buiten de verzekeringssector waarmee de i-CERT samenwerkingsafspraken heeft gemaakt.
Interne SOC	[Security Operations Center] de gespecialiseerde afdeling *binnen* de organisatie van een Aangesloten verzekeraar die door middel van o.a. (real-time) monitoring, detectie en analyse de veiligheid van de digitale omgeving bewaakt en/of acteert op incidenten.
Interne CERT	de CERT (dan wel CSIRT - Computer Security and Incident Response Team) *binnen* de organisatie van een Aangesloten verzekeraar.
Brancheorganisatie	elke belangenvereniging van in Nederland werkzame particuliere verzekeraars.
Ketenpartij	elke externe partij waarmee een Aangesloten verzekeraar een zakelijke relatie onderhoudt en digitaal gegevens uitwisselt, zoals leveranciers, tussenpersonen, platformen, medische adviseurs, enz.
Toezichthouder	elke toezichthoudende instantie waarmee een Aangesloten verzekeraar te maken kan krijgen.

2 Algemeen

2.1 Doelstellingen

2.1.1 Aangesloten verzekeraars stellen zich met dit convenant gezamenlijk tot doel:

a) hun digitale weerbaarheid te verhogen;
b) schade door informatiebeveiligingsincidenten te beheersen;
c) de snel stijgende kosten die in algemene zin gepaard gaan met cyber security af te remmen (stimuleren kostenefficiency);
d) sturing op informatiebeveiliging in de keten te verbeteren;
e) het vertrouwen van klanten en stakeholders in de sector te verhogen.

2.2 Samenwerkingsverband

2.2.1 Aangesloten verzekeraars werken conform dit convenant samen om de i-CERT dienst mogelijk te maken. Hiernaast kunnen zij op basis van dit convenant overige gezamenlijke activiteiten ontplooien die bijdragen aan de doelstellingen.

2.2.2 Inrichting, ondersteuning en uitvoering van de i-CERT dienst vindt primair plaats door, en onder verantwoordelijkheid van, Aangesloten verzekeraars die aan de criteria voldoen om ook als Deelnemer te worden aangemerkt.

2.2.3 Een Aangesloten verzekeraar wordt ook als Deelnemer aangemerkt als deze:

a) lid is van het Verbond van Verzekeraars (hierna: ‘het Verbond’) of van een andere Brancheorganisatie die de inhoud van dit convenant voor haar leden onderschrijft;
b) volgens de gegevens van het Centrum voor Verzekeringsstatistiek (CVS) tot een concern behoort dat een aandeel van 5% of meer van de totale Nederlandse verzekeringsmarkt vertegenwoordigt;
c) over een interne CERT en/of SOC, of een afdeling met een vergelijkbare functie, beschikt;
d) redelijkerwijs kan voldoen aan de in dit convenant gestelde verplichtingen en geen zwaarwegende omstandigheden aandraagt die anders uitwijzen.

2.2.4 De Deelnemers geven gezamenlijk, op roulatiebasis, invulling aan de onder artikel 3.1 bedoelde dienstverlening van de i-CERT.

2.2.5 Alle Aangesloten verzekeraars, met nadrukkelijk inbegrip van verzekeraars die niet als Deelnemer kwalificeren, verlenen de medewerking die voor een goede uitvoering van de i-CERT dienst vereist is.

2.2.6 De Deelnemers zetten zich er individueel en gezamenlijk, actief voor in om:

a) de i-CERT dienst verder te ontwikkelen en te professionaliseren;
b) samenwerkingsverbanden met Partnerorganisaties tot stand te brengen die de informatiepositie en effectiviteit van de i-CERT bevorderen.

2.2.7 Een verzekeraar die aan de in artikel 2.2.3 genoemde criteria voldoet, kan zich uitsluitend als Deelnemer bij het samenwerkingsverband aansluiten.

2.2.8 Voor het functioneren van de i-CERT zijn de door het Verbond op sectorniveau vastgestelde beleidskaders en doelstellingen leidend.

3 Taakstelling

3.1 Dienstverlening

3.1.1 De i-CERT dienst heeft in ieder geval de volgende taken:

a) het doorlopend verzamelen en ontvangen van voor verzekeraars (mogelijk) relevante informatie over incidenten;
b) het doorlopend verzamelen en ontvangen van voor verzekeraars (mogelijk) relevante *actuele en urgente* kwetsbaarheden, dreigingen en Indicators of Compromise;
c) het (pro-actief en gericht) delen van deze informatie met Aangesloten verzekeraars en Partnerorganisaties die hier (mogelijk) belang bij hebben;
d) het actief identificeren van incidenten die bij meerdere Aangesloten verzekeraars tegelijkertijd spelen en het – indien door betrokkenen gewenst – coördineren van gezamenlijke acties in deze gevallen;
e) het opbouwen en aanbieden van *situational awareness* in de sector en de ketenomgeving;
f) het monitoren op, en delen van, marktspecifieke kennis op het terrein van cyber security.

3.1.2 Aanvullend hierop kan de i-CERT vrijblijvend de volgende taken uitvoeren:

a) het bieden van handelingsperspectieven en/of het adviseren over de afhandeling van incidenten;
b) het signaleren van meer algemene (niet-urgente) gemeenschappelijke kwetsbaarheden en het aandragen van oplossingen hieromtrent.

3.1.3 Uitgesloten van de dienstverlening van de i-CERT zijn nadrukkelijk:

a) het beschikbaar stellen van capaciteit voor bijstand bij het oplossen en afhandelen van specifieke beveiligingsincidenten. Dit is en blijft een eigen verantwoordelijkheid van elke Aangesloten verzekeraar;
b) het melden van eventuele datalekken en/of IT-incidenten in het kader van relevante wetgeving;
c) het leggen of onderhouden van contact met Toezichthouders;
d) het leggen of onderhouden van contact met Ketenpartijen naar aanleiding van ontvangen informatie. Na coördinatie door de i-CERT in het kader van artikel 3.1.1 sub d kan deze actie – uitsluitend met instemming van de overige betrokkenen – wel bij de Deelnemer van dienst komen te liggen. Voorwaarde is dat deze zélf een zakelijke relatie met de Ketenpartij heeft en de kwestie vanuit die rol aanhangig maakt.

3.2 Bereikbaarheid, reactietijden en voertaal

3.2.1 Voor Aangesloten verzekeraars en Partnerorganisaties is de i-CERT in het kader van de taken onder artikel 3.1.1. standaard bereikbaar tijdens kantoortijden (maandag t/m vrijdag van 09.00 t/m 17.30 uur, uitgezonderd zon- en feestdagen, telefonisch of per e-mail).

3.2.2 De i-CERT antwoordt standaard binnen één werkdag op berichten die zij per e-mail ontvangt. Dit staat los van de verschillende termijnen voor het afhandelen van ontvangen informatie (zie hiervoor artikel 7.1.5).

3.2.3 Uitsluitend in het kader van artikel 3.1.1 sub a t/m sub b, en slechts bij incidenten die naar oordeel van de meldende partij een hoge prioriteit hebben, is de i-CERT óók buiten kantoortijden bereikbaar en operationeel (24 uur per dag, 7 dagen per week, 365 dagen per jaar, uitsluitend telefonisch).

3.2.4 Operationele communicatie door én met de i-CERT – voor zover in het kader van de hierboven beschreven dienstverlening – vindt altijd plaats in het Engels. Anderstalige berichten worden in beginsel niet behandeld. Meer algemene communicatie over o.a. de activiteiten en administratie van de i-CERT kan ook in het Nederlands plaatsvinden.

4 Overige samenwerkingsprojecten en -activiteiten

4.1.1 Aangesloten verzekeraars streven ernaar, op intekenbasis, overige gezamenlijke activiteiten te ontplooien die niet direct gerelateerd zijn aan de uitvoering van de i-CERT, maar wel bijdragen aan de in artikel 2.1.1 beschreven doelstellingen van dit convenant. In dit kader kan het gaan om onder meer:

a) gezamenlijke inkoop van security diensten of producten, met inachtneming van compliance aan mededingingswetgeving;
b) organisatie en/of ontwikkeling van bewustwordingsactiviteiten;
c) organisatie van workshops en trainingen ter bevordering van kennis en kunde van (IT) security medewerkers;
d) organisatie van *cyber resilience* oefeningen;
e) deelname aan incidentsimulaties en -oefeningen op nationaal niveau (NCSC).

5 Rechten

5.1 Aangesloten verzekeraars

5.1.1 Alle Aangesloten verzekeraars:

a) kunnen gebruik maken van i-CERT diensten zoals beschreven in artikel 3;
b) worden vroegtijdig geïnformeerd over door het Stuurgroep van dit convenant (voorgenomen) projecten en activiteiten in het kader van artikel 4 en in de gelegenheid gesteld hieraan deel te nemen;
c) kunnen via het Operationeel Overleg voorstellen doen om de i-CERT dienst te verbeteren;
d) kunnen via de Stuurgroep voorstellen doen voor projecten of activiteiten in het kader van artikel 4.

5.2 Deelnemers

5.2.1 Alle Aangesloten verzekeraars die tevens als Deelnemer kwalificeren, in aanvulling op hetgeen onder artikel 5.1.1 is beschreven:

a) zijn bevoegd via de Stuurgroep conform artikel 8.1 mee te beslissen over de invulling, ontwikkeling en aansturing van de i-CERT dienst;
b) zijn bevoegd via de Stuurgroep projecten en activiteiten in het kader van artikel 4 in gang te zetten en hiervoor de (rand)voorwaarden vast te stellen;
c) krijgen, uitsluitend wanneer de i-CERT tegelijktijdig kennis draagt over kritische informatie voor meerdere belanghebbende verzekeraars, prioriteit in het kader van artikel 3.1.1. sub c.

6 Plichten

6.1 Aangesloten verzekeraars

6.1.1 Alle Aangesloten verzekeraars:

a) geven informatie over bij hen intern bekende incidenten, die (mogelijk) relevant kunnen zijn voor andere verzekeraars, zo snel en volledig mogelijk door aan de i-CERT;
b) geven informatie over *actuele en urgente* kwetsbaarheden, dreigingen en Indicators of Compromise, die (mogelijk) relevant kunnen zijn voor andere verzekeraars, zo snel en volledig mogelijk door aan de i-CERT;
c) waarborgen dat informatie die zij bij de i-CERT aanleveren géén koersgevoelige of mededingingsrechtelijk bezwaarlijke informatie bevat (zoals bedrijfsgevoelige gegevens, gegevens over verzekeringsproducten of prijzen, etc.);
d) waarborgen dat informatie die zij bij de i-CERT aanleveren uitsluitend feitelijkheden en géén persoonsgegevens bevat;
e) wijzen intern een afdeling of medewerker aan die, als enig Contactpunt, alle operationele communicatie met de i-CERT onderhoudt. Bij voorkeur wordt deze rol belegd bij de interne SOC/CERT;
f) voorzien de i-CERT van technische gegevens over hun eigen IT-landschap, waaronder in gebruik zijnde domeinnamen, URL's, IP-adressen/ranges en eventuele AS-nummers;
g) voorzien de i-CERT van actuele contactgegevens van dit Contactpunt, waaronder ten minste een (standaard) e-mailadres en telefoonnummer;
h) zorgen ervoor dat dit Contactpunt bereikbaar is tijdens kantoortijden (maandag t/m vrijdag van 09.00 t/m 17.30 uur, uitgezonderd zon- en feestdagen);
i) zijn na het ontvangen van informatie vanuit de i-CERT primair zelf verantwoordelijk voor de verdere interne afhandeling hiervan en eventueel benodigde maatregelen/vervolgacties;
j) waarborgen dat informatie die zij vanuit de i-CERT ontvangen binnen de eigen organisatie uitsluitend wordt gedeeld met de onder artikel 6.1.1. sub e aangewezen medewerker(s) of functionarissen op het terrein van informatiebeveiliging die deze informatie aantoonbaar nodig hebben voor een adequate afhandeling (*need-to-know*);
k) verlenen naar vermogen hun medewerking aan verzoeken vanuit de i-CERT om (aanvullende) informatie;

l) zijn in relatie tot de i-CERT gehouden alle overige afgesproken procedures te volgen en gebruik te maken van de vastgestelde tools en voorzieningen*;*
m) doorlopen het intakeproces zoals beschreven onder artikel 9.1.1.

6.2 Deelnemers

6.2.1 Aangesloten verzekeraars die tevens als Deelnemer kwalificeren, in aanvulling op hetgeen onder artikel 6.1.1 is beschreven:

a) zijn bij toerbeurt, conform een nader uit te werken roulatiemodel, als *Deelnemer van dienst*, verantwoordelijk voor de uitvoering van de i-CERT dienst;
b) wijzen binnen hun interne SOC en/of CERT medewerker(s) aan met het volledige mandaat om de bijbehorende taken – waar mogelijk binnen de bestaande bedrijfsvoering – conform artikel 7 uit te voeren;
c) zorgen er voor dat deze medewerkers voldoende gekwalificeerd en geïnformeerd zijn om deze taken effectief uit te voeren;
d) zorgen er tijdens hun toerbeurt voor dat de i-CERT dienst te allen tijde bereikbaar en operationeel is (incl. achtervang bij ziekte/calamiteiten);
e) zorgen er te allen tijde voor dat de in het kader van artikel 7 afgesproken voorzieningen en tools voor de uitvoering van de i-CERT dienst intern beschikbaar en operationeel zijn;
f) leveren een evenredige financiële bijdrage indien de Stuurgroep unaniem besluit deze voorzieningen en/of tools voor de i-CERT dienst gezamenlijk in te kopen;
g) doorlopen het intakeproces zoals beschreven onder artikel 9.1.2 en 9.2.

7 Uitvoering

7.1 Werkzaamheden Deelnemer van dienst

7.1.1 De door de Deelnemer van dienst aangewezen medewerker(s) geeft/geven uitvoering aan de werkzaamheden die vereist zijn in het kader van artikel 3.1, artikel 7 en de hiervoor vastgestelde werkinstructies/procedures.

7.1.2 Deze werkzaamheden vinden volledig, adequaat en tijdig plaats.

7.1.3 Informatievergaring in het kader van artikel 3.1.1 sub a en sub b vindt standaard plaats op basis van vooraf afgesproken bronnen. De Deelnemer van dienst monitort deze bronnen tijdens kantooruren zo veel mogelijk *real-time.* Het staat hem vrij om in dit kader aanvullende (eigen) bronnen in te zetten.

7.1.4 Onderdeel van de werkzaamheden is het onderhouden van operationele contacten met Aangesloten verzekeraars en Partnerorganisaties., waaronder het beheer van een bestand met Contactpuntgegevens en het doorgeven van technische gegevens van Aangesloten verzekeraars aan het NCSC t.b.v. monitoring.

7.1.5 Distributie en/of gerichte communicatie van relevante informatie in het kader van artikel 3.1.1 sub c vindt – afhankelijk van de classificatie van de informatie – plaats binnen vastgestelde termijnen conform onderstaande tabel:

Classificatie / soort	Termijn doorgifte	Aan	Wijze
Critical (w.o. in ieder geval NCSC-informatie over 'besmette' domeinnamen, URL's, IP-adressen/ranges en eventuele AS-nummers).	7 x 24: binnen 1 uur na ontvangst	Uitsluitend aan Aangesloten verzekeraars waarop de informatie betrekking heeft.	Telefonische melding binnen de gestelde termijn. Vervolgens een aanvullende attendering via het standaard-communicatiekanaal.
High	Na ontvangst tijdens kantoortijden: binnen 1 uur en op dezelfde dag	Alle Aangesloten verzekeraars	Via het standaard-communicatiekanaal.
Medium	Na ontvangst tijdens kantoortijden: binnen 4 uur	Alle Aangesloten verzekeraars	Via het standaard-communicatiekanaal
Low	Wekelijks	Alle Aangesloten verzekeraars	Via de standaard wekelijkse rapportage ('end of week')

7.1.6 Voorafgaand aan communicatie/distributie van informatie in het kader van artikel 3.1.1 sub c vindt in beginsel géén filtering of nadere duiding van de informatie plaats.

7.1.7 Informatie die betrekking heeft op een door een Aangesloten verzekeraar gemeld incident, wordt geanonimiseerd verspreid. Uitsluitend met instemming van een primaire bron (al dan niet op verzoek), maakt de i-CERT de identiteit van de getroffen partij bekend.

7.1.8 In het kader van artikel 3.1.1. sub e t/m f verzorgt de Deelnemer van dienst een 'end of week' rapportage. Hierin wordt conform een vast format een (beknopt) overzicht opgenomen van door de i-CERT gesignaleerde ontwikkelingen, relevante algemene dreigingen en ontwikkelingen binnen de markt en publiek bekende incidenten.

7.1.9 Ten behoeve van managementrapportages vindt, aan de hand van een (beknopt) aantal afgesproken kengetallen, een registratie plaats van ontvangen en afgehandelde informatie en uitgevoerde activiteiten.

7.1.10 Aan het einde van zijn toerbeurt zorgt de Deelnemer van dienst voor een goede overdracht van werkzaamheden aan de eerstvolgende Deelnemer die aan de beurt is om de i-CERT dienst uit te voeren.

7.2 Uniformiteit

7.2.1 De Deelnemers zijn gehouden om de afspraken in dit convenant gezamenlijk te concretiseren in bijbehorende uniforme procedures, werkinstructies en voorzieningen. Deze worden vastgesteld via de in artikel 8 beschreven Governance.

7.2.2 Om de uniformiteit in de uitvoering te bevorderen, nemen de uitvoerend medewerkers van de Deelnemers minimaal 1 keer per jaar deel aan een 'kalibratieworkshop' die wordt georganiseerd door het Operationeel Overleg.

7.3 Minimale eisen voorzieningen en tools

7.3.1 Voor de uitvoering van de i-CERT dienst zorgen de Deelnemers voor een standaard communicatiekanaal dat voldoet aan relevante wet- en regelgeving op het terrein van privacy en gegevensbescherming en voldoende waarborgen biedt voor een vertrouwelijke gegevensuitwisseling.

7.3.2 Voor de bereikbaarheid van de i-CERT in het geval van incidenten met een hoge prioriteit, stelt het Verbond een centraal telefoonnummer beschikbaar. Dit telefoonnummer staat altijd doorgeschakeld naar (de uitvoerend medewerker van) de Deelnemer van dienst.

7.3.3 Voor de reguliere bereikbaarheid en een goede informatievoorziening over de dienstverlening en procedures van de i-CERT, stelt het Verbond een centraal e-mailadres en een website met een herkenbare domeinnaam beschikbaar.

8 Governance

8.1 Stuurgroep

8.1.1 Besluitvorming over, aansturing van, en toezicht op de i-CERT dienst is een verantwoordelijkheid van de Deelnemers. De Deelnemers geven gezamenlijk invulling aan deze verantwoordelijkheid via de Stuurgroep. De Stuurgroep opereert binnen de door het Verbond vastgestelde beleidskaders.

8.1.2 De Stuurgroep kan zelfstandig bevoegdheden, verantwoordelijkheden en door Deelnemers beschikbaar gestelde middelen aanwenden om de in artikel 2.1.1. beschreven doelstellingen te bereiken.

8.1.3 De Stuurgroep houdt toezicht op naleving van dit convenant en in het bijzonder van compliance aan mededingingsregelgeving bij uitvoering van de i-CERT dienst (zoals geborgd in artikel 6.1.1 sub c en j).

8.1.4 De Stuurgroep rapporteert jaarlijks aan de Commissie CBV van het Verbond en adviseert – gevraagd of ongevraagd – over gewenste acties of beleidsontwikkelingen op sectorniveau ten behoeve van een effectieve uitvoering van de i-CERT dienst

8.1.5 Elke Deelnemer is verplicht zich in de Stuurgroep te laten vertegenwoordigen door één medewerker op managementniveau. Het betreft bij voorkeur de CISO of het hoofd van de interne SOC/CERT

8.1.6 De Stuurgroep staat onder voorzitterschap van een bij meerderheid gekozen vertegenwoordiger van één van de Deelnemers.

8.1.7 Een adviseur van het Verbond heeft tevens zitting in de Stuurgroep en vervult hierin de rol van secretaris.

8.2 Operationeel Overleg

8.2.1 Monitoring van de uniformiteit en kwaliteit van de operationele dienstverlening van de i-CERT vindt plaats door het hiertoe ingestelde Operationeel Overleg, dat hierover rapporteert aan de Stuurgroep.

8.2.2 Het Operationeel Overleg doet voorstellen voor procedures, werkinstructies en voorzieningen die nodig zijn om effectief invulling te geven aan dit convenant, signaleert vanuit de praktijk verbeterpunten, relevante ontwikkelingen en trends en geeft advies ten behoeve van de meerjarenplanning van de Stuurgroep.

8.2.3 Het Operationeel Overleg rapporteert signalen van niet-naleving van dit convenant en meer in het bijzonder signalen van niet-naleving van artikel 6.1.1 sub c en j aan de Stuurgroep.

8.2.4 Het Operationeel Overleg bestaat uit de in het kader van artikel 6.2.1 sub b aangewezen uitvoerende medewerkers van de Deelnemers.

8.2.5 Alle Deelnemers zijn verplicht zich tijdens elke vergadering van het Operationeel Overleg door minimaal één medewerker te laten vertegenwoordigen.

8.2.6 Het Operationeel Overleg staat onder voorzitterschap van een lid van de Stuurgroep (linking-pin functie).

8.2.7 Het Operationeel Overleg vergadert 4 keer per jaar (minimaal 2 keer per jaar fysiek en 2 keer per jaar via een conference call).

8.2.8 De precieze taakstelling van het Operationeel Overleg wordt bij nader uitwerking door de Stuurgroep vastgesteld.

8.3 Klankbordgroep

8.3.1 Feedback en adviezen van alle Aangesloten verzekeraars ten aanzien van het functioneren van de i-CERT dienst worden verzameld via de Klankbordgroep.

8.3.2 Alle medewerkers van Aangesloten verzekeraars die in het kader van artikel 6.1.1 sub e als Contactpunt zijn aangewezen mogen deelnemen aan de bijeenkomsten van de Klankbordgroep.

8.3.3 De Klankbordgroep staat onder voorzitterschap van een lid van het Operationeel Overleg.

8.3.4 De Klanbordgroep komt minimaal 1 keer per jaar bijeen.

9 Aansluiting, intake en uittreding

9.1 Aansluiting op de i-CERT dienst

9.1.1 Een verzekeraar die niet als Deelnemer kwalificeert, kan gebruik maken van de i-CERT dienst zodra:

a) deze heeft ingetekend op dit convenant via het hiervoor bestemde intekenformulier (appendix 1);
b) deze een aansluitingsformulier heeft ingevuld, met daarin onder meer de in het kader van artikel 6.1.1. sub d t/m f gevraagde gegevens, en dit heeft aangeleverd bij de Deelnemer van dienst;
c) de Stuurgroep op advies van het Operationeel Overleg concludeert dat deze aan alle in artikel 6.1 gestelde verplichtingen voldoet c.q. kan voldoen;
d) er één jaar is verstreken nadat het Bestuur van het Verbond de eerste versie van dit convenant heeft goedgekeurd (het eerste jaar geldt conform het groeimodel als ‘inwerkperiode’ voor de Deelnemers) .

9.1.2 In aanvulling op hetgeen is bepaald onder 9.1.1 geldt voor een verzekeraar die wel als Deelnemer kwalificeert, dat deze gebruik kan maken van de i-CERT dienst zodra:

a) deze bij intekening op het onderhavige convenant (via het intekenformulier in appendix 2) de intentie heeft verklaard om binnen 6 maanden aan de in artikel 6.2 gestelde voorwaarden te voldoen en voor een eerste keer de uitvoering van de i-CERT dienst op zich te nemen;
b) de Stuurgroep op advies van het Operationeel Overleg concludeert dat de verzekeraar zich maximaal inspant op deze deadline te halen en in dit kader opvolging geeft aan de in artikel 9.2 gevraagde acties.

9.2 Intake uitvoering i-CERT dienst

9.2.1 Om binnen 6 maanden bij toerbeurt uitvoering te kunnen geven aan de i-CERT dienst, doorloopt een Deelnemer het volgende intakeproces:

a) de Deelnemer ontvangt een compleet en actueel overzicht van benodigde procedures, werkinstructies, voorzieningen en tools;
b) de Deelnemer inventariseert schriftelijk in welke mate de benodigde (organisatorische en technische) voorzieningen reeds in de eigen organisatie beschikbaar en inzetbaar zijn en rapporteert hierover aan het Operationeel Overleg;
c) een lid van het Operationeel Overleg legt een werkbezoek af aan de organisatie van de Deelnemer. Tijdens dit bezoek wordt de inventarisatie besproken, ontvangt de Deelnemer adviezen en wordt gezamenlijk bepaald welke acties nog nodig zijn om te voldoen aan de (rand)voorwaarden voor uitvoering van de i-CERT dienst;
d) de Deelnemer maakt ten behoeve van het Operationeel Overleg inzichtelijk hoe en wanneer hij deze acties verwacht af te ronden;
e) Na 6 maanden, of zoveel eerder als mogelijk is, besluit de Stuurgroep op advies van het Operationeel Overleg of de Deelnemer er klaar voor is om een eerste keer de uitvoering van de i-CERT dienst op zich te nemen;
f) Bij een negatief oordeel kan de Stuurgroep de Deelnemer maximaal 2 maanden uitstel verlenen om alsnog aan de gestelde (rand)voorwaarden te voldoen. Lukt dit niet, dan vervalt in beginsel het recht van de Deelnemer om gebruik te maken van de i-CERT dienst.

9.3 Uittreding

9.3.1 Een Aangesloten verzekeraar die niet als Deelnemer kwalificeert kan zich met onmiddellijke ingang uit dit convenant terugtrekken door de voorzitter van de Stuurgroep schriftelijk en gemotiveerd van dit besluit in kennis te stellen.

9.3.2 Een Aangesloten verzekeraar die wel als Deelnemer kwalificeert kan zich met inachtneming van een uittredingstermijn van zes maanden uit dit convenant terugtrekken door de voorzitter van de Stuurgroep schriftelijk en gemotiveerd van dit besluit in kennis te stellen. De Stuurgroep rapporteert hierover aan de directie van het Verbond en de Commissie CBV.

9.3.3 Omwille van de continuïteit van de i-CERT dienst zal een uittredende Deelnemer tot uiterlijk 6 maanden na dagtekening van schriftelijke kennisgeving van uittreding aan zijn (uitvoerings)verplichtingen onder dit convenant blijven voldoen.

10 Overige bepalingen

10.1 Publiekscommunicatie

10.1.1 Publieke uitingen over de activiteiten van de i-CERT vinden uitsluitend plaats in afstemming met het Verbond en met goedkeuring van eventuele overige belanghebbende partijen.

10.2 Aansprakelijkheid

10.2.1 Een Deelnemer kan, mede gelet op de plichten en eigen verantwoordelijkheden van alle Aangesloten verzekeraars zoals vastgelegd in artikel 6, niet aansprakelijk worden gesteld voor schade die ontstaat door uitoefening van de i-CERT dienst, tenzij aantoonbaar sprake is van het opzettelijk doorgeven van onjuiste/misleidende informatie of ernstige nalatigheid in het kader van artikel 6.

10.3 Geschillenregeling

10.3.1 Geschillen over de interpretatie of uitvoering van dit convenant, worden rechtstreeks voorgelegd aan de Stuurgroep.

10.3.2 Indien de Stuurgroep niet tot een unaniem oordeel kan komen, wordt de kwestie met een meerderheidsadvies voorgelegd aan de Commissie CBV van het Verbond.

10.4 Niet-naleving en sancties

10.4.1 Als een Aangesloten verzekeraar/Deelnemer van mening is dat een andere Aangesloten verzekeraar/Deelnemer dit convenant niet naleeft, kan deze zich rechtstreeks wenden tot de Stuurgroep.

10.4.2 De klagende partij voorziet de Stuurgroep van informatie en eventuele bewijsstukken die zijn klacht onderbouwen. Op initiatief van de Stuurgroep vindt hoor- en wederhoor plaats met de aangeklaagde partij.

10.4.3 Bij behandeling van de kwestie in de Stuurgroep verliezen de betrokken partijen hun eventuele stemrecht. Als de Stuurgroep niet tot een unaniem oordeel komt, wordt de kwestie met een meerderheidsadvies voorgelegd aan de Commissie CBV van het Verbond.

10.4.4 Als een meerderheid van de Stuurgroep constateert dat een partij structureel in gebreke blijft, dan kan zij bij de Commissie CBV voorstellen deze partij (tijdelijk) af te sluiten van de i-CERT dienst.

10.4.5 In alle gevallen waarin de Commissie CBV om een uitspraak wordt gevraagd, wordt de aangeklaagde partij op directieniveau geïnformeerd over de uitkomst en eventuele sancties.

10.5 Evaluatie

10.5.1 Uiterlijk twee jaar na goedkeuring door het Bestuur van het Verbond, vindt een evaluatie van de opzet en werking van de eerste versie van dit convenant plaats. Evaluaties vinden hierna minimaal elke drie jaar plaats.

10.6 Wijzigingen convenant

10.6.1 Het Bestuur van het Verbond kan op advies van de Stuurgroep en de Commissie CBV, besluiten tot wijziging van dit convenant.