STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 14847
30 mei
2014

Convenant tussen NCSC en SURFnet

PARTIJEN

SURFnet bv, gevestigd aan het Radboudkwartier 273 te Utrecht, te dezen vertegenwoordigd door de algemeen directeur, de heer E. Bleumink;

en

De Minister van Veiligheid en Justitie, handelend als bestuursorgaan en als vertegenwoordiger van de Staat der Nederlanden, te dezen vertegenwoordigd door de directeur Cyber Security van de Nationaal Coördinator Terrorismebestrijding en Veiligheid, de heer W.M. van Gemert;

OVERWEGENDE

1. Dat de Minister van Veiligheid en Justitie in de tweede Nationale Cyber Security Strategie, die bij brief van 30 oktober 2013 aan de Tweede Kamer is aangeboden, wijst op het belang van een integrale aanpak van Cyber Security door publieke en private partijen.
2. Dat het Nationaal Cyber Security Centrum (NCSC) een dienstonderdeel is van de Nationaal Coördinator Terrorismebestrijding van het Ministerie van Veiligheid en Justitie en tot taak heeft de weerbaarheid van de Nederlandse samenleving in het digitale domein te vergroten, door zowel het bij elkaar brengen van informatie, kennis en expertise, zodat inzicht wordt verkregen in ontwikkelingen, dreigingen en trends, als het verlenen van ondersteuning bij incidentafhandeling, crisisbeheersing en crisisbesluitvorming op ICT- gebied ten behoeve van Rijksoverheid en vitale partijen.
3. Dat het NCSC gelet op deze taken het van belang acht dat ten behoeve van het versterken van de ICT-responscapaciteit nadere samenwerking tot stand komt met andere publieke en private ICT-responsorganisaties uit diverse sectoren, en dat meer in het bijzonder een Nationaal Respons Netwerk (NRN) wordt opgezet dat tot doel heeft de gezamenlijke ICT-respons op cyber security-incidenten in Nederland te versterken om zodoende incidenten sneller onder controle te krijgen.
4. Dat SURFnet zich richt op het realiseren van een geavanceerde, vertrouwde en verbindende ICT-infrastructuur voor de bij haar aangesloten instellingen uit het hoger onderwijs en onderzoek.
5. Dat SURFnet ICT-diensten beschikbaar stelt voor de bij haar aangesloten instellingen waaronder beveiligingsdiensten, en dat in het kader van de beveiligingsdienstverlening SURFcert, als onderdeel van SURFnet, ondersteuning biedt op het vlak van incident respons aan de bij SURFnet aangesloten instellingen.
6. Dat SURFnet in het kader van deze dienstverlening een belangrijke toegevoegde waarde ziet in het aansluiten op het Nationaal Respons Netwerk: het vergroten van haar expertise en het, vanwege de toegang tot aanvullende responscapaciteit, versnellen van het oplossingsproces bij grote incidenten op de infrastructuur voor de bij haar aangesloten instellingen.

SPREKEN HET VOLGENDE AF:

Artikel 1: Afkortingen en definities

In dit convenant wordt verstaan onder:
a. *CERT:* Computer Emergency Response Team, zijnde een team van mensen dat zich richt op reactieve, proactieve en adviserende dienstverlening op het terrein van ICT-respons ten behoeve van haar doelgroep;
b. *NCTV:* Nationaal Coördinator Terrorismebestrijding en Veiligheid;
c. *NCSC:* Nationaal Cyber Security Centrum;
d. *NRN:* Nationaal Respons Netwerk.

Artikel 2: Doel

Het doel van dit convenant is het bevorderen van de samenwerking tussen het NCSC en SURFnet (hierna samen te noemen: partijen) binnen de bestaande wettelijke kaders, teneinde:
– de weerbaarheid van de Nederlandse samenleving in het digitale domein en die van de SURFnet infrastructuur te vergroten;
– gezamenlijk bij te dragen aan de ontwikkeling van het Nationaal Respons Netwerk met als doel om tijdens grootschalige incidenten de capaciteiten te bundelen om zodoende de respons op cybersecurity-incidenten te versterken;
– de wederzijdse kennis en informatiepositie ten aanzien van ICT-dreigingen te versterken;

– digitale aanvallen te voorkomen dan wel om deze aanvallen tijdig en adequaat te kunnen pareren.

Artikel 3: Activiteiten van het NCSC

Het NCSC zal ten behoeve van SURFnet onderstaande activiteiten verrichten:

a. *Informatie-uitwisseling:*
Het NCSC verschaft SURFnet waar mogelijk, ter voorkoming van ICT-incidenten bij de bij SURFnet aangesloten instellingen of het informeren over incidenten die mogelijk kunnen leiden tot de inzet van SURFnet, het volgende:
   – (incident) informatie met betrekking tot de SURFnet infrastructuur, die verkregen is uit de operationele processen van het NCSC, voor zover naar het oordeel van het NCSC relevant;
   – beveiligingsadviezen (*advisories*) met betrekking tot mogelijke en actuele risico's ten aanzien van software, besturingssystemen, hardware, aanvallen en *malware*, voor zover naar het oordeel van het NCSC relevant, waarbij het SURFnet vrij staat om te bepalen of en in hoeverre hieraan gevolg wordt gegeven.
   Er vindt geen uitwisseling van persoonsgegevens, zoals IP-adressen, plaats totdat partijen overeenstemming hebben bereikt over een daarbij in acht te nemen privacyprotocol. Verwerking van persoonsgegevens vindt alsdan voorts uitsluitend plaats met inachtneming van het bepaalde in de Wet bescherming persoonsgegevens.

b. *Incidentafhandeling:*
Het NCSC zal, mits zij daarvoor voldoende capaciteit beschikbaar heeft, op verzoek van SURFnet (personele) assistentie verlenen aan SURFnet bij het oplossen en afhandelen van specifieke ICT-beveiligingsincidenten. Dit laat onverlet de verantwoordelijkheid van SURFnet voor de ondersteuning van haar doelgroep bij respons op ICT-incidenten.

c. *Kennisuitwisseling:*
Het NCSC voorziet SURFnet, waar mogelijk en voor zover naar het oordeel van het NCSC relevant, van kennis en expertise aangaande de effectieve aanpak van beveiligings- incidenten en dreigingen, zoals trendrapporten, *white papers*, *factsheets*, nieuwsbrieven en presentaties op het terrein van ICT-veiligheid.

d. *Software:*
Het NCSC zal waar mogelijk, en voor zover naar het oordeel van de NCSC relevant, software (gericht op detectie, monitoring en incidentanalyse) ter beschikking stellen aan SURFnet, met als doel dat SURFnet deze software kan inzetten ten behoeve van haar taakuitoefening. SURFnet is zelf verantwoordelijk voor de implementatie, het gebruik en het onderhoud van deze software. Het NCSC kan specifieke randvoorwaarden stellen aan het gebruik van deze software.

e. *Opleidingen en stages:*
Het NCSC zal relevante informatie over opleidingsplannen delen met SURFnet. In overleg met SURFnet zal de mogelijkheid van korte (algemene of thematische) stages worden verkend. Daarnaast kunnen de SURFnet -medewerkers deelnemen aan interne cursussen van het NCSC, voor zover passend binnen de kaders van het NCSC. Eventuele kosten voor stages en opleidingen worden gedragen door de SURFnet. Het NCSC zal met SURFnet de mogelijkheden verkennen van het gezamenlijk ontwikkelen van opleidingen (voor zover deze niet worden aangeboden door marktpartijen) of het organiseren van gezamenlijke trainingen.

Artikel 4: Activiteiten van SURFnet

SURFnet zal ten behoeve van het NCSC onderstaande activiteiten verrichten:

a. *Informatie-uitwisseling:*
SURFnet verschaft het NCSC, waar mogelijk, ten behoeve van haar taakuitoefening het volgende:
   – (incident)informatie die relevant is voor de taakuitoefening van het NCSC, die verkregen is uit de operationele processen van SURFnet, voor zover naar het oordeel van SURFnet relevant.
   Er vindt geen uitwisseling van persoonsgegevens, zoals IP-adressen, plaats totdat partijen overeenstemming hebben bereikt over een daarbij in acht te nemen privacyprotocol. Verwerking van persoonsgegevens vindt alsdan voorts uitsluitend plaats met inachtneming van het bepaalde in de Wet bescherming persoonsgegevens.

b. *Incidentafhandeling:*
SURFnet zal, mits zij daarvoor voldoende capaciteit beschikbaar heeft, op verzoek van het NCSC (personele) assistentie verlenen aan het NCSC bij het oplossen en afhandelen van specifieke ICT-beveiligingsincidenten. Dit laat onverlet de verantwoordelijkheid van het NCSC bij respons op ICT-incidenten.

c. *Kennisuitwisseling:*
SURFnet zal, waar mogelijk en voor zover naar het oordeel van SURFnet relevant, kennis en expertise met betrekking tot de informatiebeveiliging van haar organisatie actief delen met het NCSC. Desgevraagd zal zij daarbij op dit terrein kennis en expertise met het NCSC delen met het oog op relevante publicaties van het NCSC over cyber security gerelateerde onderwerpen.
SURFnet zal, waar mogelijk en passend, haar expertise op het gebied van het configureren van

specifieke beveiligingssoftware delen met het NCSC.

d. *Opleidingen/stages:*
SURFnet zal relevante informatie over opleidingsplannen delen met het NCSC. In overleg met het NCSC zal de mogelijkheid van korte (algemene of thematische) stages worden verkend. Daarnaast kunnen NCSC-medewerkers deelnemen aan interne cursussen van SURFnet, voor zover passend binnen de kaders van SURFnet. Eventuele kosten voor stages en opleidingen worden gedragen door het NCSC. SURFnet zal met het NCSC de mogelijkheden verkennen van het gezamenlijk ontwikkelen van opleidingen (voor zover deze niet worden aangeboden door marktpartijen) of het organiseren van gezamenlijke trainingen.

Artikel 5: Werkafspraken

1. Na ondertekening van dit convenant zullen partijen ten behoeve van een verdere praktische invulling daarvan, indien wenselijk, gezamenlijke werkafspraken opstellen. Hierin zullen in elk geval ook de gegevens van de contactpersonen van partijen worden opgenomen.

2. Wijzigingen in de lijst van contactpersonen van een partij worden zo spoedig mogelijk, doch uiterlijk binnen vijf werkdagen, doorgegeven aan de andere partij.

Artikel 6: Publiciteit

Partijen zullen alle externe communicatie betreffende dit convenant, en de daaruit volgende samenwerking, voorafgaand aan publicatie met elkaar afstemmen.

Artikel 7: Overleg

Partijen zullen in het kader van de goede uitvoering van dit convenant periodiek, en ten minste eenmaal per jaar, overleg voeren.

Artikel 8: Vertrouwelijkheid en aanvullende verplichtingen

1. Partijen verplichten zich over en weer de in het kader van de uitvoering van dit convenant uitgewisselde kennis en informatie vertrouwelijk te behandelen en deze geheel noch gedeeltelijk aan enige derde bekend te maken, behoudens voor zover een verplichting tot openbaarmaking voortvloeit uit de wet of een rechterlijke uitspraak. Tevens is een partij bevoegd om de aldus verkregen kennis en informatie aan derden kenbaar te maken, voor zover dit nodig is ten behoeve van de eigen taakuitoefening, indien de andere partij daarvoor uitdrukkelijk toestemming heeft verleend en dit binnen de geldende wettelijke kaders is toegestaan.

2. Partijen dragen ervoor zorg dat hun personeelsleden, die met de in het vorige lid bedoelde gevoelige of vertrouwelijke informatie in aanraking komen, een geheimhoudingsverklaring ondertekenen. Daarnaast zullen partijen de integriteit van hun personeelsleden waarborgen, bij voorkeur middels een veiligheidsonderzoek.

3. Onverminderd het bepaalde in de artikelen 3 en 4 zullen partijen bij de uitwisseling van informatie gebruik maken van het Traffic Light Protocol (TLP) om de informatie te kenmerken, tenzij anders wordt overeengekomen. Het TLP is opgenomen als Bijlage 1 bij dit convenant.

4. Indien de kans bestaat dat vertrouwelijke bedrijfs- of persoonsgebonden informatie bij anderen dan partijen bekend wordt, nemen partijen de nodige maatregelen om dat te voorkomen.

5. Partijen zijn verplicht elkaar (mogelijke) schendingen van de vertrouwelijkheid van informatie, direct na kennisname hiervan, te melden.

Artikel 9: Kosten

Alle door deze samenwerking ontstane kosten worden gedragen door de partij waartoe het personeel dan wel de middelen, waarmee de kosten zijn gemoeid, behoren, tenzij in dit convenant anders is overeengekomen.

Artikel 10: Afdwingbaarheid

Dit convenant is niet in rechte afdwingbaar.

Artikel 11: Wijziging en beëindiging

1. Indien zich omstandigheden voordoen die aanleiding kunnen geven dit convenant te wijzigen, zullen partijen over de noodzaak hiertoe in onderling overleg treden.

2. Elke partij kan de andere partij schriftelijk verzoeken dit convenant te wijzigen. Wijzigingen behoeven de schriftelijke instemming van beide partijen.

3. Elke partij kan dit convenant met inachtneming van een opzegtermijn van 3 maanden schriftelijk opzeggen, onder vermelding van de reden hiervoor.

Artikel 12: Geschillen

Alle geschillen in verband met dit convenant worden in goed onderling overleg tussen de partijen beslecht.

Artikel 13: Inwerkingtreding en looptijd

1. Dit convenant treedt in werking op de datum van ondertekening door de laatste van de twee partijen en wordt aangegaan voor de duur van één jaar.

2. Na afloop van de in het eerste lid genoemde looptijd wordt dit convenant telkens stilzwijgend verlengd met één jaar, tenzij een der partijen overeenkomstig het bepaalde in artikel 11, derde lid, dit convenant schriftelijk opzegt.

Artikel 14: Publicatie in Staatscourant

1. De tekst van dit convenant wordt binnen drie maanden na ondertekening gepubliceerd in de Staatscourant.

2. Bij wijziging van het convenant vindt het eerste lid overeenkomstige toepassing.

3. Van opzegging van dit convenant wordt melding gemaakt in de Staatscourant

Artikel 15: Slotbepalingen

Dit convenant wordt aangehaald als ‘Convenant tussen NCSC en SURFnet’.

Aldus overeengekomen en in tweevoud opgemaakt, 14 mei 2014

SURFnet
Namens deze,
E. Bleumink
Algemeen directeur SURFnet

29 april 2014

De Minister van Veiligheid en Justitie,
Namens deze,
W.M. van Gemert
Directeur Cyber Security

BIJLAGE 1: TRAFFIC LIGHT PROTOCOL

TRAFFIC LIGHT PROTOCOL[1]

The international community of CERTs in Europe as assembled in the Trusted Introducer[2] has adopted in 2009 an information sharing protocol that was then already in use between various governmental CERTs, worldwide. It originally stems from the UK governmental organisation NISCC. The protocol is based on 'traffic light' colours and is as follows:

'All CERTs can have their own system of information classification with associated rules, but they will at least **recognise and support** *the following ISTLP (Information Sharing Traffic Light Protocol), following best practice in NISCC (UK) with widening acceptance in the CERT community. NOTE that an "Information Exchange" can be either in person, like a meeting of CERTs or of a CERT with their constituents, or a meeting of just a few security professionals together, but also an exchange in e-mail or over the phone or fax. The rules below apply to all of those. It is not an absolute recipe, but needs to be applied thoughtfully – the ISTLP serves the purpose of bringing more clarity in regards the rules of information sharing – it is not a purpose in itself.*

NOTE that an 'Information Exchange' can be either in person, like a meeting of CERTs or of a CERT with their constituents, or a meeting of just a few security professionals together, but also an exchange in e-mail or over the phone or fax. The rules below apply to all of those. It is not an absolute recipe, but needs to be applied thoughtfully – the ISTLP serves the purpose of bringing more clarity in regards the rules of information sharing – it is not a purpose in itself.

RED	Non-disclosable Information and restricted to representatives participating in the Information Exchange themselves only. Representatives must not disseminate the information outside of the Exchange. RED information may be discussed during an Exchange, where all representatives participating have signed up to these rules. Guests & others such as visiting speakers who are not full members of the Exchange will be required to leave before such information is discussed.
AMBER	Limited Disclosure and restricted to members of the Information Exchange; those within their organisations and/or constituencies (whether direct employees, consultants, contractors or outsource-staff working in the organisation) who have a NEED TO KNOW in order to take action.
GREEN	Information can be shared with other organisations, Information Exchanges or individuals in the network security, information assurance or CNI community at large, but not published or posted on the web.
WHITE	Information that is for public, unrestricted dissemination, publication, web-posting or broadcast. Any member of the Information Exchange may publish the information, subject to copyright. "

[1] De hier getoonde versie is identiek aan de versie van Trusted Introducer, versie 1.1. 'ISTLP – Information Sharing Traffic Light Protocol', aangepast voor de TI community door Don Stikvoort, Directeur van Trusted Introducer op 11 november 2009. Dit met toestemming van NISCC (UK), de auteur van ISTLP

[2] Zie: www.trusted-introducer.org