Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Handreiking OKTT: Aansluiting bij NCSC

Ontvang als OKTT relevante dreigings- en risicoinformatie.

U vindt in deze handreiking waarom samenwerken met het NCSC relevant is voor uw schakelorganisatie, waarom het NCSC deze samenwerking zo belangrijk vindt, en welke voorwaarden zijn verbonden aan een effectieve samenwerking en informatieuitwisseling.

Achtergrond

Uw achterban is (zoals bijna alle andere organisaties) zeer afhankelijk van digitale diensten en infrastructuur. Om de continuïteit te waarborgen wordt veel aandacht besteed aan cybersecurity. Digitale infrastructuren zijn in onze samenleving sterk met elkaar verweven, waardoor cybersecurity complex en veelomvattend is. Daarmee is de noodzaak geboren om samen te zorgen voor digitale veiligheid. Dreigingen herkennen en risico's tijdig in kaart brengen is in het belang van ons allemaal. Betrokkenen moeten elkaar snel weten te vinden. Zo kunnen we door middel van samenwerking de digitale weerbaarheid binnen en ook buiten Nederland verhogen.

Wat doet het NCSC?

Het NCSC is het nationale expertisecentrum voor cybersecurity. Het NCSC heeft als doel de Nederlandse samenleving digitaal weerbaarder te maken. Het NCSC is nationale CERT en het knoop- en informatiepunt op het gebied van cybersecurity: kwetsbaarheden, incidenten en dreigingen die op nationaal niveau spelen.

Samenwerken met het NCSC

Het NCSC beschikt over informatie die relevant is voor andere organisaties dan die binnen Rijksoverheid en vitale infrastructuur. Zoals informatie over kwetsbare systemen of dreigingen, bijvoorbeeld over *ransomware*. Het NCSC kan vanuit de (wettelijke) taken en bevoegdheden ook informatie delen over dreigingen en incidenten met organisaties die door het NCSC zijn aangewezen. Deze schakelorganisaties zijn samenwerkingsverbanden (OKTT's) en computercrisisteams (CERTs of CSIRTs).

Omgekeerd kunt u het NCSC helpen door informatie terug te delen. Bijvoorbeeld over incidenten, waargenomen dreigingen of andere relevante informatie. Het NCSC kan deze informatie samenvoegen, verrijken en delen met andere partners binnen het landelijk dekkend stelsel. Zo maken we Nederland samen digitaal veilig.

Een OKTT

OKTT is een afkorting die het NCSC gebruikt voor een organisatie die 'objectief kenbaar tot taak' heeft om andere organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot andere netwerk- en informatiesystemen. Objectief kenbaar betekent dat het duidelijk moet zijn dat het delen van dit soort informatie een taak is van uw organisatie. Een OKTT vertegenwoordigt een sector, regio, ecosysteem of ander relevant verband en heeft een duidelijk gemarkeerde doelgroep.

Mogelijke informatieverschaffing

Als aangewezen OKTT kunt u verschillende informatie ontvangen:

Informatie over incidenten, dreigingen en kwetsbaarheden

Met informatie en analyses over ontwikkelingen, zoals dreigingen, kwetsbaarheden en incidenten kunnen deelnemers aan uw samenwerkingsverband tijdig de juiste acties ondernemen. Als partner van het NCSC wordt u 24 uur per dag, 7 dagen per week gewaarschuwd in het geval van ernstige kwetsbaarheden (zogenaamde High/High-meldingen). Daarnaast deelt het NCSC dreigingsbeelden en informatie over weerbaarheidsmaatregelen.

Aansluiting op het Nationaal Detectie Netwerk

Uw samenwerkingsverband kan worden aangesloten op het Nationaal Detectie Netwerk (NDN). Het NDN is een samenwerking tussen NCSC, inlichtingen- en veiligheidsdiensten, organisaties binnen de Rijksoverheid en vitale infrastructuur en partners binnen het landelijk dekkend stelsel. Via het NDN delen deze organisaties dreigingsinformatie met elkaar die gebruikt kan worden voor detectie. Na aanwijzing door het NCSC kunt u deze informatie delen met de achterban van uw schakelorganisatie en informatie terugdelen aan het netwerk. De waarde die gehaald kan worden uit aansluiting op het NDN is mede afhankelijk van de mate van volwassenheid van uw achterban op het gebied van cybersecurity.

Geautomatiseerd delen van risico-informatie

Het NCSC ontvangt informatie over IP-adressen waarop malware is waargenomen of systemen die mogelijk kwetsbaar zijn of gecompromitteerd. Als u AS-nummers, IP-adressen en domeinnamen van uw deelnemers deelt met het NCSC is het mogelijk om informatie met u te delen die betrekking heeft op deze IP-adressen, domeinnamen of AS-nummers.

Kennisdeling

Het NCSC wil met zijn partners niet alleen informatie uitwisselen, maar wil ook een rol spelen in het verbinden van organisaties. We brengen aangewezen organisaties bij elkaar om *best practices* op het gebied van cybersecurity en het effectief opereren als schakelorganisatie uit te wisselen.

Stappenplan: Samenwerking starten

Om een samenwerkingspartner te worden van het NCSC moet uw organisatie worden aangewezen als een schakelorganisatie die tot doel heeft om andere organisaties of het publiek te informeren (OKTT) of een computercrisisteam (CERT).

Met het stappenplan kunt u zelf aan de slag om aangewezen te worden als OKTT. Als uw organisatie een computercrisisteam is, vraag dan de handreiking ‘Samenwerken met het NCSC als computercrisisteam’ op.

Geen samenwerkingverband?

Wilt u samenwerken binnen uw keten, sector, regio of ecosysteem, en heeft u nog geen samenwerkingsverband? Het NCSC heeft verschillende handreikingen om u te helpen een samenwerking op te zetten. U vindt deze op ncsc.nl of neem contact op met samenwerken@ncsc.nl.

Stap 1: Kennismaking

Stuur een e-mail naar samenwerken@ncsc.nl. Wij nemen contact met u op voor een kennismaking en u wegwijs te maken in het traject.

Stap 2: Toetsing

Het NCSC moet toetsen of uw organisatie in aanmerking komt om aangewezen te worden als OKTT en de wijze waarop u de vertrouwelijkheid en de rechtmatigheid van de verwerking van de verkregen informatie waarborgt. Toetsing gebeurt aan de hand van het toetsingskader.

Toetsingscriteria

De toetsing vindt plaats op basis van de informatie die u ons aanlevert. Deze informatie geeft ons inzicht in het privacy- en securitybeleid van uw organisatie.

Uw informatiebeveiliging is op orde

De informatie die u gaat ontvangen is in sommige gevallen vertrouwelijk vanwege de inhoud. Daarom moet u kunnen aantonen dat u beveiligingsmaatregelen heeft getroffen ten aanzien van uw netwerk- en informatiesystemen. Dit is daarnaast ook

een belangrijk onderdeel van het zorgvuldig omgaan met persoonsgegevens.

U heeft uw privacybeleid op orde en voldoet aan de AVG

De informatie die u gaat ontvangen bevat vaak persoonsgegevens. Als het goed is voldoet uw organisatie al aan de AVG. Houd er bij het verwerken van de ontvangen informatie rekening mee dat IP-adressen ook persoonsgegevens zijn, en dat u voor het verwerken van deze gegevens ook moet voldoen aan de eisen van de AVG.

In het *Formulier Aanvraag toetsing aanwijzing OKTT* vindt u toelichting op de gegevensverwerking van persoonsgegevens.

Wanneer het NCSC alle informatie heeft ontvangen, streeft het NCSC ernaar de toetsing uit te voeren binnen 2 tot 3 weken. Mogelijk stellen wij u naar aanleiding van deze toetsing nog aanvullende vragen. Als het NCSC voldoende heeft kunnen vaststellen uw organisatie voldoet aan de eisen, dan wijzen wij uw organisatie aan.

Stap 3: Aansluiting

Als uw organisaties is getoetst en aangewezen dan maakt het NCSC samenwerkingsafspraken met uw organisatie. Dit doen wij in de vorm van een leidraad voor samenwerking. Hierin staat wat u mag verwachten van het NCSC en wat het NCSC verwacht van uw organisatie. Na het accepteren van deze leidraad sluiten wij uw organisatie aan op de informatievoorziening van het NCSC. Dit betekent dat u uw (operationele) contactgegevens deelt, gegevens over de AS-nummers, IP-adressen en domeinnamen van uw achterban en dat wij u aansluiten op het NDN.

Stap 4: Samenwerking

Als uw organisatie is aangesloten gaan we informatie uitwisselen. Wederkerigheid is een vereiste in de samenwerking.

Werkt u al wel samen, maar heeft u nog geen rechtsvorm?

Als u wel samenwerkt maar nog geen rechtspersoon heeft, dan kunt u bijvoorbeeld een stichting of verenging oprichten. Daarbij is het belangrijk om duidelijk in de statuten (of indien relevant een ander document) op te nemen dat uw organisatie (onder andere) tot taak heeft om deelnemers of leden te informeren over dreigingen, incidenten en kwetsbaarheden. Daarnaast moet het duidelijk zijn welke doelgroep uw organisatie heeft. Het NCSC helpt u graag met de ervaringen van anderen die een rechtspersoon voor een OKTT hebben opgericht.

Samen Nederland digitaal veilig maken

Dankzij samenwerking met uw organisatie kan het NCSC zijn 24/7 operationeel situationeel beeld verder verscherpen. Daarmee kunnen we sneller reageren op ontwikkelingen en partners in Nederland in staat stellen om tijdig de juiste maatregelen te nemen. Samen werken we aan de digitale weerbaarheid van Nederland.

Meer informatie

Wilt u meer weten over samenwerking met het NCSC en de procedure tot aanwijzing als OKTT, stuur dan een bericht naar samenwerken@ncsc.nl.

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

December 2020