CSIRT-DSP

Ministerie van Economische Zaken en Klimaat

RFC 2350

CSIRT voor Digitale Dienstverleners
Directoraat-Generaal Bedrijfsleven en Innovatie | Directie Digitale Economie

TLP: WHITE
Versie 1.1
Maart 2019

Inhoudsopgave

1 Informatie over dit document

1.1 Laatste update

Dit is versie 1.0. Deze is gecreëerd op 18 maart 2019.

1.2 Locatie van dit document

De meest actuele versie van dit document kunt u vinden op https://csirtdsp.nl/csirt-dsp.

1.3 Distributie van wijzigingen

Wijzigingen in dit document worden gepubliceerd op de bovenstaande webpagina.

2 Contactinformatie

2.1 Naam van het team

Het Computer Security Incident Response Team voor Digitale Diensten. Dit team staat bekend onder de naam CSIRT-DSP (DSP staat voor Digital Service Providers).

2.2 Adres

CSIRT-DSP
Bezuidenhoutseweg 73
2594 AC Den Haag

Correspondentieadres:
Postbus 20401
2500 EK, Den Haag

2.3 Tijdzone

CSIRT-DSP gebruikt de Central European Time (CET) met Daylight Saving Time (DST). Dit is GMT +0100 in de winter en GMT +0200 in de zomer.

2.4 Telefoonnummer

CSIRT-DSP is 24/7 bereikbaar via dit telefoonnummer: +31 70 37 96 222

2.5 E-mailadres

CSIRT-DSP is bereikbaar via csirt@csirtdsp.nl

2.6 Publieke sleutels en informatie over encryptie

De PGP sleutel is te vinden op deze plaats en op de keyserver van Surfnet (pgp.surfnet.nl).

2.7 Teamleden

Er is geen publieke lijst van de teamleden van het CSIRT-DSP beschikbaar. Naar aanleiding van een incident zullen de teamleden zich aan een digitale dienstverlener identificeren.

2.8 Overige informatie

De website van het CSIRT-DSP is https://csirtdsp.nl

2.9 Contactpunten

Digitale dienstverleners kunnen gebruik maken van het genoemde e-mailadres, alsook via het online meldformulier. Het online meldformulier is bereikbaar via: https://csirtdsp.nl/incident-melden. Het CSIRT-DSP is tevens bereikbaar via het hierboven genoemde telefoonnummer. In het geval van zéér dringende incidenten kunnen digitale dienstverleners ook buiten kantoortijden en op weekend- en feestdagen naar dit nummer bellen.

3 Privilege

3.1 Missie

Voorkoming en beperking van het uitvallen van de beschikbaarheid of het verlies van integriteit van netwerk- en informatiesystemen van digitale dienstverleners.

3.2 Achterban

CSIRT-DSP is opgezet om digitale dienstverleners te ondersteunen bij het afhandelen van beveiligingsincidenten. Digitale dienstverleners nemen contact op met het CSIRT-DSP om melding te maken van een incident, om meer informatie op te halen over een oplossingsrichting en voor een inschatting van de situatie in de sector.
De verantwoordelijkheid ligt bij het bedrijf zelf om te bepalen of een bedrijf een digitale dienstverlener is die meldplichtig is bij het CSIRT-DSP. De criteria om dit te bepalen kunnen hier gevonden worden.

3.3 Affiliatie

Het CSIRT-DSP is onderdeel van het Ministerie van Economische zaken en Klimaat. Zij voert haar taken uit onder de Directie Digitale Economie.

3.4 Autoriteit

CSIRT-DSP is een entiteit met een wettelijk vastgelegd takenpakket. Het takenpakket komt voort uit de Nederlandse implementatie van de Europese Richtlijn Beveiliging van Netwerk en Informatiesystemen (EU 2016/1148), namelijk de Wet Beveiliging Netwerken en Informatiesystemen (Wbni).

4 Beleid

4.1 Incidenttypes en steunniveau

Het is de taak van het CSIRT-DSP om incidentmeldingen, vroegtijdige waarschuwingen en alarmmeldingen te ontvangen van digitale dienstverleners die onder de Wbni vallen. Daarnaast deelt het CSIRT-DSP actief dreigingsinformatie met de sector en verbetert zij haar zichtbaarheid voor de sector.

4.2 Samenwerking, communicatie en publicaties

Het CSIRT-DSP is onderdeel van of bekend bij verschillende netwerken en gemeenschappen. Daarnaast maakt het CSIRT-DSP gebruik van Europese en mondiale bronnen en modellen, en werkt samen met het Nederlandse NCSC, om invulling te geven aan haar takenpakket.

4.3 Authenticatie en communicatie

Communiceren met het CSIRT-DSP kan bij voorkeur via e-mail en het online meldformulier. Als de inhoud van de communicatie gevoelig is of authenticatie vereist is, zal de CSIRT-DSP PGP key gebruikt worden voor het signereren van het e-mailbericht. Gevoelige communicatie richting CSIRT-DSP dient versleuteld te zijn met de team PGP year key. Voor dringende meldingen is het CSIRT-DSP altijd telefonisch bereikbaar op het eerder genoemde telefoonnummer.

5 Diensten

5.1 Incident Response

CSIRT-DSP levert ondersteuning bij incidenten bij digitale dienstverleners. Dit doet zij door:

- Meldingen (zoals beschreven in de Wbni) aan te nemen en te registreren;
- Actief informatie op te halen, te beoordelen en terug te koppelen aan de digitale dienstverlener;
- Aanwezige relevante informatie te delen met een melder.

De digitale dienstverlener is zelf verantwoordelijk voor het oplossen van het incident. Het CSIRT-DSP zal de digitale dienstverlener zo goed mogelijk ondersteunen en het overzicht van incidenten op nationaal niveau bewaren.

5.2 Informatie delen

CSIRT-DSP verzamelt continu informatie om digitale dienstverleners te helpen hun infrastructuur en informatie beter te beveiligen. CSIRT-DSP deelt deze informatie met digitale dienstverleners. Voor zover het gaat om het delen van vertrouwelijke informatie die herleidbaar is tot een digitale dienstverlener met derden worden de kaders die de Wbni hierover stelt in acht genomen.

CSIRT-DSP deelt informatie door middel van:

- Organisaties zoals het Digital Trust Center en brancheorganisaties;
- Direct contact met specifieke digitale dienstverleners. Dit kan doordat het CSIRT-DSP dit zelf als noodzakelijk ziet om met een digitale dienstverlener te delen, danwel doordat een digitale dienstverlener zelf een informatieverzoek doet bij CSIRT-DSP.

Het delen van informatie gebeurt op ad-hoc basis. CSIRT-DSP deelt informatie indien deze kan bijdragen aan de informatiebeveiliging van DSP's in Nederland.

5.3 Samenwerken

CSIRT-DSP zoekt actief de samenwerking met digitale dienstverleners. Daarnaast werkt CSIRT-DSP samen met andere cybersecurity teams in haar netwerk. CSIRT-DSP werkt zodoende actief samen met het NCSC en de nationale CSIRT's van andere Europese lidstaten. Op die manier wisselt zij informatie uit over actualiteiten in Nederland in de andere lidstaten van de Europese Unie.

6 Rapporteren over incidenten

6.1 Aan het CSIRT-DSP

Er zijn geen speciale formulieren vereist om een incident te melden bij het CSIRT-DSP . Een e-mail naar csirt@csirtdsp.nl volstaat. Wel heeft het voorkeur om incidenten te melden via het online meldformulier. Dit is te vinden op https://csirtdsp.nl/incident-melden.

7 Disclaimer

Van alle informatie in dit document kan de nauwkeurigheid en beschikbaarheid niet worden gegarandeerd. In geen geval accepeeert het CSIRT-DSP aansprakelijkheid voor schade opgelopen door de afwezigheid of onnauwkeurigheid van de informatie in dit document.