CSIRT DSP

Ministerie van Economische Zaken en Klimaat

RFC 2350

CSIRT for Digital Service Providers

TLP: WHITE
Versie 1.5
August 2020

Index

1 Document information

1.1 Latest version

This is version 1.5. This document version has been created on the 27th of August 2020.

1.2 Document location

The latest actual version of this document can be found on: https://csirtdsp.nl/csirt-dsp.

2 Contactinformation

2.1 Teamname

The Cyber Security Incident Respone Team for Digital Service Providers, also known as CSIRT-DSP.

2.2 Address

CSIRT-DSP
Bezuidenhoutseweg 73
2594 AC Den Haag

Correspondondence address:
Postbus 20401
2500 EK, Den Haag

2.3 Timezone

CSIRT-DSP uses CET (Central European Time) from the last Sunday of October until the last Saturday of March and CEST (Central European Summer Time) from the last Sunday of March until the last Saturday of October.

2.4 Telephone number

+31 70 37 96 222 (Available 24/7)

2.5 E-mailaddress

csirt@csirtdsp.nl

2.6 Public PGP keys

The PGP key can be found here and on the Surfnet keyserver (pgp.surfnet.nl).

2.7 Team members

There is no public list of teammembers available. In case of an incident, members of the CSIRT-DSP will identify themselves towards the Digital Service Provider.

2.8 Website

https://csirtdsp.nl

2.9 Contact in case of incident

Digital Service Providers can use the e-mail address csirt@csirtdsp.nl, or use the online incident report form. The incident report form is available at: https://csirtdsp.nl/incident-melden. The CSIRT-DSP can also be reached for incidents on +31 70 37 96 222.

The CSIRT-DSP is available on business days between 09.00-17.00.
Outside of these hours, a duty officer will be reachable in case of urgent incidents on the telephone number provided in paragraph 2.4.

3 Charter

3.1 Mission statement

To prevent and limit the disruption of availability or loss of integrity of network and informationsystems of digital service providers (ANNEX III of the NIS Directive EU 2016/1148).

3.2 Background information

CSIRT-DSP was formally established late 2018 to support digital service providers in handling security incidents. Digital service providers contact the CSIRT-DSP to report incidents, or to receive situational reports relevant to their sector.
It is the responsibility of the organization to determine if it is a digital service provider and is obliged to report to the CSIRT-DSP. The criteria for a mandatory report can be found here .

3.3 Affiliation

The CSIRT-DSP is part of the Dutch Ministry of Economic Affairs and Climate Policy. The CSIRT-DSP acts under the Digital Economy Department.

3.4 Authority

CSIRT-DSP is an entity with legally defined duties. The Dutch transposition of the EU directive on security of network and information systems (EU 2016/1148), called the “Wet Beveiliging Netwerken en Informatiesystemen (Wbni)” determines the legal duties for the CSIRT-DSP.

4 Policy

4.1 Incidenttypes and support

The CSIRT-DSP is tasked to receive incident reports and preliminary warnings from digital service providers who fall under the Dutch transposition of the NIS directive. The CSIRT-DSP also proactively distributes threat intelligence with her sector and enhances her visibility to this sector.

4.2 Cooperation, communication and publication

The CSIRT-DSP is part of and known within various networks and communities. The CSIRT-DSP also makes use of European and global sources and cooperates with the Dutch NCSC, as well as other international (national) CSIRT’s.

4.3 Authentication and communication

Communication with the CSIRT-DSP should preferably happen by e-mail or the online incident report form. If the content of the communication is sensitive or authentication is required, the CSIRT-DSP PGP key can be used to sign the e-mail. Sensitive information sent towards CSIRT-DSP should be encrypted with the public CSIRT-DSP team PGP year key.

5 Services

5.1 Incident Response

CSIRT-DSP provides support for cybersecurity incidents at digital service providers. This is done by:

- Registering incident reports (as described in the 'Wbni');
- Actively collect, analyze and distribute information from and to digital service providers;
- To share relevant information with an incident reporter.

The digital service provider is responsible for the resolving the incident. CSIRT-DSP will to the best of its abilities provide support and overview of incidents on a national level.

5.2 Information sharing

CSIRT-DSP continuously collects information to assist digital service providers in securing their infrastructure and data. The collected information is shared with the digital service providers. In case information shared with third parties is considered to be confidential or traceable to a digital service provider the frameworks described in the 'Wbni' are observed and maintained.

CSIRT-DSP distributes information through:

- Organizations such as the Digital Trust Center and other branche organizations;
- By sharing various products developed by the CSIRT-DSP with digital service providers who registered to receive this product;
- Direct contact with digital service providers. This can occur because the CSIRT-DSP deems it a necessity to share information directly with a digital service provider or because a digital service provider requests information.

The sharing of information occurs on an ad-hoc basis. CSIRT-DSP only shares information when it is deemed to contribute to the information security of digital service providers in the Netherlands.

6 Reporting an incident

6.1 To the CSIRT-DSP

No special forms are required to report an incident to the CSIRT-DSP. An e-mail to csirt@csirtdsp.nl suffices, but it is preferred to use the incident report form on the website. This form can be found here: https://csirtdsp.nl/incident-melden. This incident report form also provides the ability for reporters to directly inform the supervising agency, 'Agentschap Telecom'.

7 Disclaimer

The accuracy and availability of the information in this document can't be guaranteed. The CSIRT-DSP does not accept any liability for damage caused by the absence or inaccuracy of the information in this document.