RFC 2350 Teaminfo (English)

Document Information

This document provides basic information about CERT NRW, its channels of communication and its roles and responsibilities according to RFC 2350[1].

2 Contact Information

2.1 Name of the Team

Computer Emergency Response Team of the public administration of the federal state North Rhine-Westfalia; shortname: CERT NRW

2.2 Address

Landesbetrieb Information und Technik Nordrhein-Westfalen

T1-4, CERT NRW

Postfach 10 11 05

40002 Duesseldorf
Germany

2.3 Time Zone

Europe/Berlin, GMT+1 and
Europe/Berlin, GMT+2 acc. §2 SoZV from last Sunday in March through last Sunday in October

2.4 Telephone Number

+49-211-9449-2124

2.5 Facsimile Number

+49-211-9449-8884

2.6 Electronic Mail Address

cert@it.nrw.de

2.7 Public Keys and Encryption Information

Encryption is recommended for exchange of sensitive information.

Team PGP Key ID:	F96A F09E 212C 0843
Fingerprint:	1961 2B20 88AF BF91 0140 9D4B F96A F09E 212C 0843

2.8 World Wide Web

https://www.cert.nrw.de/

We provide participating authorities and institutions in the state administration network with more comprehensive information and handouts on the state intranet at https://lv.cert.nrw.de.

2.9 Team Members

The team is made up of experts in various domains of information security like pentesting, network security monitoring, digital forensics and incident handling/response. All team members are employed by IT.NRW.

2.10 Hours of operation

Monday to Friday from 07:00 to 17:00.

3 Charter

3.1 Mission Statement

CERT NRW's mission is to support the public administration of North Rhine-Westfalia prevent, protect and defend against intentional and malicious attacks that would harm or hamper the confidentiality, integrity or availabilty of their information or information technology assets as well as to assist investigations of information security incidents.

3.2 Constituency

The constituency of CERT NRW is composed of all ministries, supreme federal state authorities and associated public service offices/agencies of the state administration excluding municipal administrations.

3.3 Domains and IP Ranges

AS 43066
IPv4 Range 93.184.128.0 - 93.184.143.255
Domain *.nrw.de

3.4 Responsibilities and Competences

In addition to providing below listed services CERT NRW is authorised to probe and examine systems, software, websites and other internet services within above IP range and additional agreed on scopes (in writing) for vulnerabilities and security weaknesses and to monitor network boundaries in said scopes for attacks, breaches and other threats for information security, as well as collect and in case of an indication/alert to record data needed for further investigation.

4 Services

CERT NRW supports the CISO of the federal state government of NRW and provides various services to its constituency.

4.1 Basic Services

The following basic services are provided to our constituency:

- threat analysis / threat intelligence threat information, warning and alerting
- service incident handling & response cooperation with security teams of other
- public administrations and private industry consultancy and guidance for
- operational information security (opsec)
-

4.2 Extended Services

- intrusion-/breach-detection, network security monitoring vulnerability
- scans penetration testing information security incident analysis and
- digital forensic investigations education and training
-
-

5 Co-operation and Disclosure of Information

CERT NRW ist member of the German Verwaltungs-CERT-Verbund (VCV) and Deutscher CERT-Verbund (CV).

The state of North Rhine-Westphalia is also member of Alliance for Cyber Security (Allianz für Cybersicherheit) We handle sensitive information with great care and in adherence to TLP or other applicable classification schemes.

Disclosure of vulnerability information is handled according to our responsible disclosure policy published on our website.

6 Incident Reporting

In order to accurately handle incidents we need at least the following information in an incident report:

- Who is reporting? (name, surname, functional role, organisation, postal address, telephone number, email address)
- Where did it happen / where was it detected, by whom? (organisation, organisational unit, network segment, means of detection)
- type of report (initial report, follow up or closing report)
- what damages occurred or are imminent severity of occurred or imminent damages urgency technical description of what happened, when it happened, when it was detected, how was it detected, which countermeasures have already been initiated technical description of impact and effects that occurred or are imminent

- CERT NRW provides an incident reporting form for its constituency on our intranet site.

[1] http://www.ietf.org/rfc/rfc2350.txt