RFC 2350

1 Information über dieses Dokument

Dieses Dokument enthält Informationen zum Computer Emergency Response Team der Landesverwaltung Nordrhein-Westfalen (CERT NRW) gemäß RFC 2350[1], der üblichen standardisierten Kurzdarstellung der Aufgaben und Erreichbarkeit von Computernotfallteams.

2 Kontaktinformationen

2.1 Name des Teams

Computer Emergency Response Team der Landesverwaltung Nordrhein-Westfalen

Kurzname: CERT NRW

2.2 Postalische Adresse

Landesbetrieb Information und Technik Nordrhein-Westfalen
Referat 24, CERT NRW
Postfach 10 11 05
40002 Düsseldorf

2.3 Zeitzone

Europa/Berlin, GMT+1 und Europa/Berlin, GMT+2 gemäß §2 SoZV vom letzten Sonntag im März bis zum letzten Sonntag im Oktober

2.4 Telefon (Hotline)

+49-211-9449-2124

2.5 Fax

+49-211-9449-8884

2.6 E-Mail Adresse

cert@it.nrw.de

2.7 Public Keys und Informationen zur Signierung und Verschlüsselung

Für die elektronische Übermittlung vertraulicher Informationen empfehlen wir die Nutzung von S/MIME oder PGP Verschlüsselung.

Team PGP Key ID: 0x8C65895A

Fingerprint: 0B18 8B42 CD07 29C7 A5CE DD1F 9265 A315 8C65 895A

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

2.8 World Wide Web

Unsere Kontaktdaten und weitere Informationen zum CERT NRW finden Sie im Internet unter: https://www.it.nrw.de/informationstechnik/Services/CERT/index.html

Im Landes-Intranet stellen wir teilnehmenden Behörden und Einrichtungen des Landesverwaltungsnetzes unter http://lv.cert.nrw.de umfassendere Informationen und Handreichungen zur Verfügung.

2.9 Personelle Zusammensetzung

Das Team setzt sich zusammen aus Expertinnen und Experten verschiedener Fachdomänen wie Penetration-Testing, Vorfallserkennung, digitale Forensik sowie Vorfallsbehandlung.

Die Mitarbeiterinnen und Mitarbeiter des CERT NRW sind Bedienstete des Landesbetriebs Information und Technik Nordrhein-Westfalen (IT.NRW).

2.10 Betriebszeiten

Montag bis Freitag jeweils von 07:00 bis 17:00 Uhr

3 Organisatorischer Rahmen

3.1 Ziele und Aufgaben (Mission Statement)

Wir unterstützen die Landesverwaltung dabei, sich präventiv und reaktiv gegen IT-Angriffe zu schützen und zu verteidigen, welche die Vertraulichkeit, Integrität oder Verfügbarkeit ihrer Informations- oder Technologie-Güter gefährden oder verletzen würden. Darüber hinaus unterstützen wir bei der Untersuchung und Aufklärung von Informationssicherheitsvorfällen.

3.2 Zielgruppe (Constituency)

Unsere Dienstleistungen richten sich primär an Behörden und Einrichtungen der Landesverwaltung NRW, die am Landesverwaltungsnetz angeschlossen sind.

3.3 Domains und IP Ranges

AS 43066

IPv4 Range 93.184.128.0 - 93.184.143.255

Domain *.nrw.de

3.4 Zuständigkeiten und Befugnisse

Zusätzlich zu den unten aufgelisteten Dienstleistungen sind wir im allgemein oder spezifisch beauftragten Umfang befugt, Systeme, Software und Webseiten auf Schwachstellen hin zu überprüfen und Netzübergänge auf Angriffe und Einbrüche hin zu überwachen, sowie im zur Abwehr und Aufklärung erforderlichen Umfang Netzwerkkommunikation aufzuzeichnen und auszuwerten.

4 Services

Wir unterstützen die oder den Chief Information Security Officer (CISO) der Landesverwaltung Nordrhein-Westfalen und bieten Behörden und Einrichtungen der Landesverwaltung die nachfolgend aufgeführten Dienstleistungen[2] (Services) an.

4.1 Basisdienstleistungen

Folgende Basisdienstleistungen erbringen wir für alle Behörden und Einrichtungen der Landesverwaltung NRW, die ans Landesverwaltungsnetz angeschlossen sind:

- Bedrohungsanalyse / Threat Intelligence
- Warn- und Informationsdienst (WID)
- Unterstützung bei der Vorfallsbehandlung (Incident Handling & Response)
- Kooperation mit Sicherheitsteams (CERTs) anderer öffentlicher Einrichtungen und der Privatwirtschaft
- Beratung zu Fragen der operativen Informationssicherheit

4.2 Erweiterte Dienstleistungen

- Vorfallserkennung / Network Security Monitoring
- Schwachstellenscans
- Penetrationstests
- Vorfallsanalyse und digitale Forensik
- Trainings- und Fortbildungsveranstaltungen

5 Kooperation und verantwortungsvolle Informationsweitergabe

Wir sind Mitglied im Deutschen Verwaltungs-CERT-Verbund (VCV) sowie dem Deutschen CERT-Verbund (CV).

Wir behandeln sensible Informationen mit großer Sorgfalt und achten das Traffic Light Protocol (TLP) sowie andere Klassifizierungsschemata.

Die verantwortungsvolle Weitergabe von Schwachstelleninformation handhaben wir gemäß unserer Responsible Disclosure Policy (siehe Webseite).

[2] Weitere Informationen im Landesintranet unter: http://lv.cert.nrw.de/Aufgaben_Leistungen/index.php

6 Meldung von Informationssicherheitsvorfällen an das CERT NRW

Für eine korrekte und vollständige Erfassung und geeignete Priorisierung von Informationssicherheitsvorfällen sind uns nach Möglichkeit mindestens die folgenden Informationen zu übermitteln:

Kontaktdaten der meldenden Person

- Meldende Organisation / Behörde
- Name und Funktion der meldenden Person
- Standort / Postanschrift der Organisation / Behörde
- Telefonische Kontaktdaten für kurzfristige Rückfragen
- Angabe des Ressorts / der Abteilung / des Teams, in dem der Vorfall entdeckt worden ist
- E-Mail-Adresse der meldenden Person
- Art der Meldung (Erstmeldung / Zwischen- oder Abschlussmeldung)

Einstufung des Vorfalls aus Sicht der meldenden Organisation:

- Sind Schäden entstanden oder drohen akut?
- Wie schwer sind die entstandenen oder drohenden Schäden?
- Dringlichkeit

Technische Angaben zum festgestellten Informationssicherheitsvorfall:

- was ist passiert,
- wann ist es passiert,
- wann wurde es entdeckt,
- wie wurde es entdeckt,
- welche Maßnahmen wurden bereits eingeleitet,
- welche Schäden und Auswirkungen wurden festgestellt oder sind möglich?

Wir stellen ein Meldeformular für Informationssicherheitsvorfälle auf unserer Intranetseite zur Verfügung, welches alle diese Informationen strukturiert erfasst.