Team-Informationen nach RFC2350

04.02.2019

Version 2.9

Vorbemerkung

Dieses Dokument beschreibt in Anlehnung an RFC 2350 (*Expectations for Computer Security Incident Response*, http://www.ietf.org/rfc/rfc2350.txt) die technische und organisatorische Schnittstelle zum CERT-rlp, dem „Computer Emergency Response Team“ für die Landesverwaltung von Rheinland-Pfalz. Eine formalisierte Kurzdarstellung einer CERT-Struktur nach RFC2350 hat sich als quasi-Standard etabliert und ist geeignet, um sich einen schnellen Überblick über die Schnittstellen und Dienstleistungen eines CERT zu verschaffen. Sie ersetzt nicht die vollständige Dokumentation der durch ein CERT realisierten Geschäftsprozesse, Dienstleistungen und Schnittstellen, sondern soll diese ergänzen.

Kontaktinformationen

Name des Teams

„CERT-rlp“, das *Computer Emergency Response Team* für die Landesverwaltung von Rheinland-Pfalz.

Postalische Adresse

CERT-rlp
Landesbetrieb Daten und Information
Valenciaplatz 6
D-55118 Mainz

Zeitzone

Europa/Berlin, GMT +1, GMT +2 von April bis Oktober

Team-Telefonnummer

+49 6131 605-600

Faxnummer

+49 6131 605-55360 (Standard-Fax, unverschlüsselt)

eMail-Adresse

Folgende E-Mail-Adresse ist gültig:

soc@cert.rlp.de

Für die elektronische Übermittlung vertraulicher Informationen wird die Nutzung von Verschlüsselung empfohlen. Unterstützt wird PGP und Chiasmus.

Folgender öffentlicher PGP-Schlüssel gilt zurzeit:

```
ID:              56C31CEB
Fingerprint:     AE1BEF4F9DD94958A5BA7A848ECE5AC056C31CEB
```

Der öffentliche PGP-Schlüssel steht zum Download auf dem Internet-Webserver bereit. Es wird empfohlen, den Fingerprint telefonisch zu verifizieren.

Der symmetrische Schlüssel für Chiasmus wird auf Anfrage vertraulich bereitgestellt.

World Wide Web

Informationssicherheitsplattform (rlp-Netz-intern): https://informationssicherheit.rlp/de/cert-rlp/

Internet-Webserver: https://cert.rlp.de/

Zusammensetzung des Teams

Das CERT-rlp setzt sich aus Mitarbeitern im LDI sowie nachgelagert aus dezentralen IT-Sicherheitsbeauftragten und -teams der Zielgruppe innerhalb der Landesverwaltung von Rheinland-Pfalz zusammen.

Betriebszeiten

Montags-Donnerstags: 08:00 Uhr bis 16:30 Uhr
Freitags: 08:00 Uhr bis 13:00 Uhr
(Ausnahmen: 24. und 31. Dezember sowie gesetzliche Feiertage in Rheinland-Pfalz)

Die telefonische Erreichbarkeit des CERT-rlp über die Team-Telefonnummer ist außerhalb der Betriebszeiten über den LDI Helpdesk rund um die Uhr sichergestellt (First Level).

Organisatorischer Rahmen

Ziele und Aufgaben (Mission Statement)

Die Ziele und Aufgaben des CERT-rlp stellen sich wie folgt dar:

- Bereitstellung einer zentralen organisatorischen und technischen Anlaufstelle für die rheinland-pfälzische Landesverwaltung in Bezug auf vorbeugende, reaktive und nachhaltige Maßnahmen bei Sicherheitsvorfällen in IT-Systemen;
- Entwicklung und strukturierte Verteilung von vorbeugenden Handlungsempfehlungen zur Vermeidung von IT-Sicherheitsvorfällen für die anzusprechende Zielgruppe;
- Entwicklung und Durchführung von nachhaltigen Maßnahmen zur Bildung und zum Ausbau eines Sicherheitsbewusstseins.

Zielgruppe (Constituency)

Die Dienstleistungen des CERT-rlp richten sich organisatorisch primär an die obersten Landesbehörden der rheinland-pfälzischen Landesverwaltung. Technisch umfasst dies dem Grunde nach die entsprechende Teilmenge der direkt am vom LDI betriebenen landesweiten rlp-Netz angeschlossenen Organisationseinheiten.

Innerhalb der angesprochenen Behörden und Organisationseinheiten richten sich die Dienstleistungen des CERT-rlp an die jeweils verantwortlichen dezentralen IT-Sicherheitsteams bzw. IT-Sicherheitsbeauftragte. Es ist aufgrund der kombinierten Struktur des CERT-rlp zu unterscheiden zwischen den zentralen Dienstleistungen des CERT-rlp Kernteams im LDI und den konkreten dezentralen CERT-Dienstleistungen vor Ort.

Domains und IP-Ranges

CERT-rlp ist zuständig für das Netz 83.243.48.0/21 sowie sämtliche Domains die auf das genannte Netz auflösen (u.a. *.rlp.de).

Mitgliedschaften

Das CERT-rlp ist Mitglied im Deutschen CERT-Verbund, einer Allianz deutscher Sicherheits- und Computer-Notfallteams (http://www.cert-verbund.de/). Weiterhin ist das CERT-rlp Mitglied im bundesweiten VerwaltungsCERT-Verbund, einer Kooperation zwischen CERTs auf Länder- und Bundesebene.

Zuständigkeiten und Befugnisse

Das CERT-rlp erfasst, bewertet und klassifiziert sicherheitsrelevante Schwachstellen von IT-Systemen und veröffentlicht diese Informationen als Empfehlungen über den Warn- und Informationsdienst (WID) an die IT-Sicherheitsverantwortlichen in den rheinland-pfälzischen Landesbehörden. Die Verantwortung für die Umsetzung des vom CERT-rlp ausgesprochenen Empfehlungen verbleibt jeweils dezentral vor Ort in der Landesbehörde bei den dort zuständigen IT-Sicherheitsverantwortlichen, Administratoren bzw. den damit beauftragten zuständigen Mitarbeiterinnen und Mitarbeitern.

Eine Ausnahme bilden ressortübergreifende IT-Sicherheitsvorfälle mit möglichen Auswirkungen auf die landesweite IT-Infrastruktur. Reaktive Maßnahmen werden in enger Kooperation mit den Ansprechpartnern in der Zielgruppe abgestimmt und in dezentraler Verantwortung umgesetzt und, falls erforderlich, vom CERT-rlp koordiniert. Soweit es die Sicherheitslage erfordert, können gemäß den Vorgaben in der rlp-Netz-Policy vom rlp-Netzbetreiber LDI eigenverantwortlich Anschlüsse vom Netz getrennt werden.

Dienstleistungen

Reaktion

Das CERT-rlp implementiert reaktive Dienstleistungen für die Entgegennahme, Klassifikation und Dokumentation von Alarmmeldungen über IT-Sicherheitsvorfälle innerhalb der Zielgruppe. Sie nimmt weiterhin koordinierende und unterstützende Aufgaben bei ressortübergreifenden Vorfällen wahr.

Prävention

Das CERT-rlp implementiert präventive Dienstleistungen für die Entgegennahme, Klassifikation und Dokumentation von Warnmeldungen über für die Zielgruppe relevante IT-Sicherheitslücken. Ein weiterer Schwerpunkt liegt auf der Entwicklung und Verteilung von landesweiten Empfehlungen für IT-Sicherheitsstandards an die Zielgruppe.

Nachhaltigkeit

Das CERT-rlp führt Sicherheitsberatungen und Weiterbildungen im Bereich der IT-Sicherheit durch. Des Weiteren werden die Angebote auf der Informationsplattform IT-Sicherheit im Intranet des rlp-Netzes ständig weiterentwickelt.

Vorfallmeldung

Für eine korrekte und vollständige Erfassung von IT-Sicherheitsvorfällen sind gemäß CERT-rlp Meldestandard mindestens die folgenden Informationen zu übermitteln:

- TLP-Klassifizierung der Meldung (TLP:WHITE, TLP:GREEN, TLP:AMBER oder TLP:RED)
- Meldende Organisation / Behörde
- Name und Funktion des Melders
- Erreichbarkeit für Rückfragen (Telefon- und eMail-Adressen, die zeitnah erreichbar sind)
- Datum / Uhrzeit (wann ist das Ereignis eingetreten?)
- Vorläufige Klassifizierung durch den Meldenden:
  - Externer Angriff
  - Datenverlust
  - Sicherheitslücke
  - Verstoß gegen IT-Sicherheitsrichtlinien
  - Störung von Software-/Hardware-Komponenten
  - Interne Ursachen
  - Externe Einflüsse
  - Besondere Erkenntnisse
- Beschreibung des Sachverhalts mit folgenden Leitfragen:
  - Was wurde festgestellt / was ist passiert?
  - Wer bzw. was ist betroffen?
  - Welcher Schaden wurde bereits festgestellt?
  - Ist eine Kompromittierung weiterer Systeme in anderen Organisationen wahrscheinlich?
  - Wurden bereits (Gegen-) Maßnahmen ergriffen? Wenn ja, welche?
  - Wurden bereits weitere Stellen informiert
- Zweck der Information / Erwartete Reaktion durch das CERT-rlp (Mehrfachauswahl möglich):
  - Zur Kenntnisnahme
  - Bitte um Rückruf
  - Freigabe zur Aufnahme in den Lagebericht
  - Explizite Freigabe zur Aufnahme in den Lagebericht erforderlich
  - Bitte um Einschätzung / Stellungnahme
  - Unterstützung erforderlich (Anforderung MIRT)
- Optional: Vorschläge des Meldenden zum weiteren Vorgehen
- Optional: Sonstiges / freie Anmerkungen

Kontakt

CERT-rlp

LANDESBETRIEB DATEN UND INFORMATION
Valenciaplatz 6
55118 Mainz

Telefon 06131 605-600
Telefax 06131 605-55360
E-Mail: soc@cert.rlp.de
Internet: https://cert.rlp.de
Intranet: https://informationssicherheit.rlp/de/cert-rlp/