1 Über dieses Dokument

1.1 Vorbemerkung

In Anlehnung an die RFC 2350 (Expectations for Computer Security Incident Response, http://www.ietf.org/rfc/rfc2350.txt) beschreibt dieses Dokument sowohl die organisatorischen als auch die technischen Schnittstellen zum CERT M-V, dem „Computer Emergency Response Team“ der Landesverwaltung von Mecklenburg-Vorpommern. Die formalisierte Kurzdarstellung eines CERTs nach der RFC 2350, Anhang D hat sich als De-facto-Standard etabliert und ist geeignet, um sich einen schnellen Überblick über die Schnittstellen und Dienste eines CERTs zu verschaffen. Sie ersetzt nicht die vollständige Dokumentation (Dienstespezifikation) der durch das CERT M-V realisierten und/ oder unterstützten Geschäftsprozesse, Dienstleistungen und Schnittstellen.

1.2 Datum der letzten Änderung

Version 1.3 vom 21. März 2019

1.3 Informationen über Änderungen in diesem Dokument

Inhaltliche Änderungen werden durch den Beauftragten der Landesverwaltung für Informationssicherheit (BeLVIS) bestätigt und in den CERT-Portalen im Internet und Intranet der Landesverwaltung M-V (s. Pkt. 2.10) bekannt gegeben.

1.4 Dokumentenablage

Eine aktuelle Version dieses Dokuments wird in den CERT-Portalen im Internet und Intranet der Landesverwaltung M-V (s. Pkt. 2.10) veröffentlicht und kann von dort als signierte Datei geladen werden.

2 Kontaktdaten

2.1 Name des Teams

CERT M-V (Computer Emergency Response Team Mecklenburg-Vorpommern)

2.2 Adressen

Ministerium für Energie, Infrastruktur und Digitalisierung Mecklenburg-Vorpommern

CERT M-V

Schloßstraße 6-8

19053 Schwerin

2.3 Zeitzone

Europa/Berlin Winterzeit: GMT +1

Europa/Berlin Sommerzeit: GMT +2

gemäß § 2 SoZV vom letzten Sonntag im März bis zum letzten Sonntag im Oktober

2.4 Telefonnummer

+49 (0) 385 588-8888

2.5 Telefaxnummer

+49 (0) 385 588 488-8888

2.6 E-Mail-Adresse

cert@mv-regierung.de

2.7 Weitere Telekommunikation

Auf Anfrage kann die Nummer eines Krypto-Fax bereitgestellt werden.

2.8 Kryptographisches Schlüsselmaterial für die vertrauliche Kommunikation

Für die elektronische Übermittlung vertraulicher Informationen wird die Nutzung von S/MIME bevorzugt; unterstützt werden S/MIME, PGP und Chiasmus.

2.8.1 S/MIME

Das aktuell gültige X.509-Signaturzertifikat (S/MIME) für die E-Mailadresse cert@mv-regierung.de verfügt über die nachstehenden Prüfsummen (Hashwerte):

SHA 1 Fingerprint:	F5:D4:54:46:D1:46:CB:3E:B6:73:C0:2F:52:B2:04:6A:5E:8A:F5:88
SHA256 Fingerprint:	F2:D8:40:FE:DA:BA:54:3D:86:53:0F:E9:FF:FF:4C:3D:52:D0:30:5B:EA:95:0C:FB:9F:50:BD:15:FA:24:91:33

Für den vertraulichen Informationsaustausch lauten die Prüfsummen (Hashwerte) und das Verschlüsselungszertifikat:

SHA 1 Fingerprint:	22:87:50:4A:4A:2A:09:FC:5F:B0:7B:BD:A8:91:E8:34:5C:2D:3B:E6
SHA256 Fingerprint:	7D:40:8E:E3:DD:F1:9E:67:77:81:31:22:1B:91:74:77:F0:10:CD:6E:18:03:02:F5:CF:32:CD:FA:31:47:87:63

X.509-Verschlüsselungszertifikat (PEM, 0 MB)

2.8.2 PGP/GnuPG

Aktuell gültig ist der folgende PGP-Schlüssel:

UID:	0x2B 12 81 58 CERT M-V cert@mv-regierung.de
Fingerprint:	38F4 B3A2 FF31 D4D8 DA9B 16D1 E3E7 D0E7 2B12 8158

PGP-Schlüssel (ASC, 0 MB)

2.8.3 Chiasmus

Der Schlüssel für Chiasmus wird auf Anfrage über einen vertraulichen Kommunikationskanal bereitgestellt.

2.9 Zusammensetzung des Teams

Das CERT M-V setzt sich aus Mitarbeitern des Ministeriums für Energie, Infrastruktur und Digitalisierung sowie der DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH zusammen.

Darüber hinaus werden bei Bedarf in das CERT M-V weitere Sicherheitsexperten von Verwaltungseinheiten als Mitglieder kooptiert, die auf Grund ihrer fachlichen Aufgabenwahrnehmung, Kompetenzen oder sicherheitsrelevantem Know-how das CERT M-V ziel- und zweckgerichtet unterstützen.

2.10 Weitere Kontaktangaben

Internetauftritt: http://www.cert.m-v.de/

CERT-Portal im Intranet (Lotse): https://portal30.cn.mv-regierung.de/pz/certmv

Betriebszeiten des CERTs M-V:

Montag bis Donnerstag	8:00 bis 16:30 Uhr
Freitag	8:00 bis 14:00 Uhr

(Ausnahmen: 24. und 31. Dezember sowie an den gesetzlichen Feiertagen in Mecklenburg-Vorpommern)

3 Organisationsrahmen

3.1 Mandat (Mission Statement)

Das CERT M-V ist gemäß der Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern (IS-Leitlinie M-V) vom 12.05.2014 das CERT der Landesverwaltung Mecklenburg-Vorpommern. Es nimmt insbesondere folgende Aufgaben wahr:

- Entwicklung und strukturierte Verteilung von vorbeugenden Handlungsempfehlungen zur Vermeidung von Sicherheitsvorfällen,
- Koordinierung und Umsetzung von Maßnahmen bei Sicherheitsvorfällen mit ressortübergreifender Bedeutung,
- Entwicklung und Durchführung von nachhaltigen Maßnahmen zum Aufbau und zur weiteren Verbesserung des Sicherheitsbewusstseins,
- Beratung der Kommission für Informationssicherheit der Landesverwaltung und

- Unterstützung der Arbeit der Informationssicherheitsbeauftragten der Behörden seiner Zielgruppe.

3.2 Zielgruppen (Constituency)

Die Dienstleistungen des CERTs M-V werden für die Landesverwaltung M-V und deren nachgeordneten Behörden sowie für den Landesdienstleister, der DVZ M-V GmbH, erbracht.

Die Basisdienste stehen ebenfalls den Kommunen in Mecklenburg-Vorpommern zur Verfügung.

3.3 Zugehörigkeit

Das CERT M-V ist in die Informationssicherheitsorganisation der Landesverwaltung eingebunden und dem Beauftragten der Landesverwaltung für Informationssicherheit (BeLVIS) direkt unterstellt.

Das CERT M-V ist Mitglied im VerwaltungsCERT-Verbund (VCV), einer Kooperation zwischen den CERTs auf Länder- und Bundesebene.

3.4 Zuständigkeiten und Befugnisse

Das CERT M-V koordiniert und unterstützt die Bearbeitung von ressortübergreifenden IT Sicherheitsvorfällen mit möglichen Auswirkungen auf die landesweite IT-Infrastruktur.

Die Verantwortung für die Umsetzung von Handlungsempfehlungen des CERTs M-V verbleibt jeweils in dem Verwaltungsbereich bei den dort zuständigen IT-Sicherheits-verantwortlichen bzw. den damit beauftragten zuständigen Mitarbeiterinnen und Mitarbeitern.

Bei Vorfällen mit hohem, akutem Bedrohungspotenzial ist das CERT M-V befugt, alle zur Schadensbegrenzung bzw. zur Behebung erforderlichen Maßnahmen umzusetzen. Die Maßnahmen sind jedoch zuvor grundsätzlich mit der jeweils betroffenen Behörde abzustimmen.

Das CERT M-V ist die zentrale Stelle (Single-Point-of-Contact, SPoC) für die Kommunikation zu IT-Sicherheitsvorfallmeldungen zum bzw. aus dem Bundesland M-V und mit anderen CERTs.

3.5 Autorität

Das CERT M-V arbeitet im Ressortbereich und unter der Aufsicht des Ministeriums für Energie, Infrastruktur und Digitalisierung Mecklenburg-Vorpommern.

4 Dienstleistungen

4.1 Reaktion

4.1.1 Behandlung von IT-Sicherheitsvorfällen

Die Behandlung von Sicherheitsvorfällen beinhaltet die Reaktion auf Anfragen und Berichte sowie die Analyse von Sicherheitsvorfällen und Einleitung entsprechender Gegenmaßnahmen.

4.1.2 Alarmmeldungen

Dieser Dienst umfasst die Erfassung, Aufbereitung und Weiterleitung von Informationen, in denen ein Angriffsversuch gemeldet und beschrieben wird.

Dazu gehören auch Meldungen über kompromittierte Systeme der Zielgruppen (z. B. durch Schadsoftware) und die Empfehlung kurzfristiger Maßnahmen für den Umgang mit den dadurch entstehenden Problemen.

4.2 Prävention

4.2.1 Warn- und Informationsdienst

Der Warn- und Informationsdienst (WID) informiert über mögliche Angriffe, Warnmeldungen zu neu festgestellten Sicherheitslücken sowie neue Angriffswerkzeuge und Entwicklungen.

Auf Basis solcher Bekanntgaben können die Zielgruppen ihre Systeme und Netzwerke vor neu erkannten Problemen schützen, bevor diese ausgenutzt werden.

4.2.2 Technologieüberwachung

Das CERT überwacht und beobachtet neue technische Entwicklungen, Aktivitäten von Angreifern und zugehörige Trends, um zukünftige Risiken leichter erkennen zu können.

4.2.3 Monitoring

Das CERT M-V nutzt Sensorik-Systeme mit entsprechenden Auswertungsverfahren (z. B. IDS/IPS; SIEM), beobachtet die entsprechenden Protokolle und wertet die Informationen unterschiedlicher Quellen in einer ganzheitlichen Betrachtung aus. So können z. B. durch das Feststellen von Abweichungen vom Normalzustand kompromittierte Systeme schnell und zuverlässig erkannt und die Betroffenen darüber unmittelbar informiert werden.

4.2.4 Wissensmanagement

Das CERT M-V stellt für die Zielgruppen eine umfassende und übersichtliche Sammlung von nützlichen Informationen, die zur Erhöhung der Sicherheit beitragen, auf einem zentralen Portal zur Verfügung.

4.3 Nachhaltigkeit

4.3.1 Sensibilisierung des Sicherheitsbewusstseins

Das CERT M-V unterstützt die Zielgruppen bei der Information und der Sensibilisierung der Beschäftigten durch Maßnahmen wie Informationsveranstaltungen und Kampagnen zu sicherheitsrelevanten Themen.

4.3.2 Ausbildung / Schulung

Dieser Dienst beinhaltet die Durchführung von Workshops, Schulungskursen und Lernprogrammen zu sicherheitsrelevanten Themen.

4.3.3 Unterstützung der Notfallvorsorge

Das CERT M-V nutzt die gewonnenen Erfahrungen, um die Zielgruppen bei der Konzeptionierung von Vorsorgeplänen für Notfälle, Krisen und Katastrophen zu unterstützen.

Gleichzeitig beinhaltet dieser Dienst ebenfalls die Unterstützung der Informationssicherheitsbeauftragten bei der Durchführung von Notfallübungen.

5 Vorfallmeldung

Für eine korrekte und vollständige Erfassung von IT-Sicherheitsvorfällen sind dem CERT M-V nach Möglichkeit mindestens die folgenden Informationen zu übermitteln:

a) Stammdaten des Melders

- meldende Organisation / Behörde
- Name und Funktion des Melders
- Standort: postalische Anschrift der Organisation / Behörde
- Telefon- und Faxnummer des Melders, die zeitnah erreichbar ist
- Angabe des Ressorts / der Abteilung / des Teams, in dem der Vorfall entdeckt worden ist
- E-Mail-Adresse des Melders

b) Korrelation der Vorfallmeldung aus Sicht des Melders

c) Erstmeldung-/Zwischen- oder Abschlussmeldung

d) Einstufung der Vorfallmeldung aus Sicht des Melders

- Dringlichkeit
- Kritikalität

e) Angaben zum festgestellten IT-Sicherheitsvorfall

- technische Beschreibung des Vorfalls, um abzugrenzen, was aus Sicht des Melders den Vorfall ausmacht, ohne zunächst Mutmaßungen über die Ursache oder die Auswirkung anzustellen – eine neutrale und unvoreingenommene Darstellung ist in dieser frühen Phase der Vorfallbehandlung von großer Wichtigkeit.
- Beschreibung der bereits festgestellten Auswirkungen des Vorfalls, wie Einschränkungen der Verfügbarkeit von Diensten, Anwendungen oder Prozessen, Privilegieneskalation, etc. Hierzu gehört auch, mit welchen Mitteln bzw. Werkzeugen diese Auswirkungen festgestellt wurden, um eine Einschätzung bezüglich der Aussagekraft der so festgestellten Auswirkungen vornehmen zu können.
- Eine Beschreibung, wie es zur eigentlichen Feststellung bzw. Entdeckung des Vorfalls kam, wie ungewöhnliche Logfile-Einträge, ungewöhnlicher Netzwerkverkehr, ungewöhnliche Anmeldevorgänge am System, verdächtige Manipulationen im Dateisystem, etc.
- Eine technische Beschreibung der betroffenen IT-Systeme: Hier sollte der IT-Verbund abgegrenzt werden, der von dem Vorfall primär betroffen ist. Hierzu

zählen alle aktiven IT-Komponenten wie Serversysteme, Router, Firewall-Systeme, Switches, etc. Interessant sind hier insbesondere die Versions- und Patchstände der eingesetzten Betriebssysteme, der Firmware, von Anwendungen und sonstiger relevanter Software-Komponenten. Des Weiteren ist ein „umgebender“ Netzwerkplan hilfreich, um die Integration bzw. Auswirkung auf das Landesdatennetz CN LAVINE abschätzen zu können.

f) Formulierung der Erwartungshaltung gegenüber dem CERT M-V (z. B.):

- nur zur Information / keine Unterstützung erforderlich
- Anforderung von Unterstützung / Koordination

6 Haftungsausschluss

Die vorliegenden Informationen werden auf einer informellen Basis bereitgestellt. Alle Angaben wurden mit größtmöglicher Sorgfalt zusammengestellt und geprüft. Eine Haftung oder Gewährleistung für Korrektheit und Vollständigkeit der hier enthaltenen Informationen oder für sich aus der Nutzung dieser Angaben ergebende Konsequenzen kann jedoch nicht übernommen werden.