

CSIRT Beschreibung für UniMS-CERT

1. Über dieses Dokument

Dieses Dokument enthält eine Beschreibung des **UniMS-CERT** gemäß [RFC 2350](#). Es stellt Informationen über das CERT bereit, wie es kontaktiert werden kann, und erläutert den Verantwortungsbereich sowie die bereitgestellten Dienste.

1.1 Letzte Änderung

Dies ist Version 2.0, veröffentlicht am 06.02.2026.

1.2 Verteilerliste für Änderungen

Aktualisierungen dieses Dokuments werden nicht aktiv verteilt. Die aktuelle Version kann immer an den unten genannten Orten gefunden werden und es sollte immer die aktuelle Version verwendet werden.

1.3 Orte, an denen dieses Dokument gefunden werden kann

Die aktuelle Version dieses Dokuments steht auf der Webseite des UniMS-CERT zur Verfügung:

- **Deutsch:** <https://www.uni-muenster.de/CERT/rfc2350/csirt-desc-de.pdf>
- **Englisch:** <https://www.uni-muenster.de/CERT/rfc2350/csirt-desc-en.pdf>

1.4 Authentizität dieses Dokuments

Beide Versionen dieses Dokuments wurden mit dem PGP Schlüssel des UniMS-CERT signiert. Der Fingerabdruck des Schlüssels kann auf der Webseite des UniMS-CERT gefunden werden. Der öffentliche Schlüssel kann von den üblichen Schlüsselserversn oder ebenfalls von der Webseite heruntergeladen werden.

Die Signaturen der beiden Dokumente können ebenfalls über die Webseite eingesehen werden:

- <https://www.uni-muenster.de/CERT/rfc2350/csirt-desc-de.pdf.asc>
- <https://www.uni-muenster.de/CERT/rfc2350/csirt-desc-en.pdf.asc>

2. Kontaktinformation

2.1 Name des Teams

UniMS-CERT: Computer Emergency Response Team der Universität Münster

2.2 Adresse

Universität Münster
CIT - UniMS-CERT
Röntgenstraße 7-13
48149 Münster
Deutschland

2.3 Zeitzone

Europe/Berlin, GMT+0100 (GMT+0200 von April bis Oktober)

2.4 Telefonnummer

+49 251 83 31600 (fragen Sie nach UniMS-CERT)

2.5 Faxnummer

Nur nach Rücksprache verfügbar.

2.6 Andere Telekommunikation

Mitglieder des UniMS-CERT sind auf verschiedenen CSIRT Austausch-Plattformen aktiv, z.B. den Chat Servern des [Trusted Introducer \(TI\)](#) oder des [CERT-Verbund](#).

2.7 Elektronische Mail Adresse

- cert@uni-muenster.de - Dies ist die Hauptadresse und sollte für Vorfallkommunikation genutzt werden.
- spam@uni-muenster.de - Dies ist eine spezielle Adresse zur Meldung von Phishing/Spam mit Bezug zur Universität Münster.

2.8 Öffentliche Schlüssel und andere Verschlüsselungs-Informationen

Das UniMS-CERT hat einen [PGP Schlüssel](#) und ein [X.509 Zertifikat](#).

2.9 Mitglieder

Dustin Schwerdt ist der aktuelle Leiter des UniMS-CERT. Zur einfacheren Aktualisierung und um dieses Dokument kurz zu halten, können Informationen zu weiteren Mitgliedern auf der [UniMS-CERT Webseite](#) gefunden werden.

2.10 Weitere Informationen

Seit 2018 ist das UniMS-CERT Mitglied des [CERT-Verbund](#) und des [EDUCV](#). Darüber hinaus ist das UniMS-CERT seit 2021 beim [Trusted Introducer \(TI\) Service](#) akkreditiert.

Weitere Informationen können auf der [Webseite](#) des UniMS-CERT gefunden werden.

2.11 Kontaktmöglichkeiten

Der Kontakt per E-Mail an cert@uni-muenster.de ist die bevorzugte Kontaktmöglichkeit. E-Mails an diese Adresse erreichen direkt das Ticketsystem und werden dort von den Mitgliedern im Dienst bearbeitet.

Wenn der Kontakt per E-Mail nicht möglich (oder aus Sicherheitsgründen nicht ratsam) ist, kann das UniMS-CERT auch telefonisch während der normalen Bürozeiten erreicht werden.

Im Allgemeinen sind die Betriebszeiten des UniMS-CERT auf die regulären Bürozeiten (07:00-17:00 Uhr, Montags bis Freitags, Feiertage ausgenommen) beschränkt. Anfragen außerhalb dieser Zeiten werden am nächsten Arbeitstag bearbeitet. Im Falle einer dringenden Notfallsituation außerhalb der regulären Arbeitszeiten, die den Verantwortungsbereich des UniMS-CERT betrifft, kann die Rufbereitschaft des [Network Operating Center \(NOC\)](#) alarmiert werden.

3. Charta

3.1 Leitbild

Aufgabe des UniMS-CERT ist die Unterstützung der Mitglieder der Universität Münster, einerseits bei der Umsetzung von proaktiven Maßnahmen, um das Risiko von IT Sicherheitsvorfällen zu reduzieren (z.B. durch Aufdeckung von Sicherheitsproblemen), und andererseits bei der Reaktion auf auftretende Vorfälle, um diese schnell und effizient zu klären. Ziel ist es, die Universität Münster, sowie die Angehörigen und Infrastruktur, vor fahrlässiger oder illegaler Nutzung ihrer IP-Adressen und Ressourcen zu schützen. Das UniMS-CERT stellt die zentrale Koordinationsstelle für IT Sicherheitsinformationen, -probleme und -vorfälle für den Verantwortungsbereich dar.

3.2 Verantwortungsbereich

Der Verantwortungsbereich des UniMS-CERT umfasst den Geltungsbereich, wie er in der "Informationssicherheitsleitlinie der Universität Münster" definiert ist. Dazu gehören alle Systeme und Nutzende von Diensten der Universität. Dezentrale Bereiche und ihre Mitglieder gehören ebenfalls zum Verantwortungsbereich. Das UniMS-CERT behandelt alle Vorfälle, die sowohl mit Systemen vor Ort, wie auch mit Systemen, die sich mit dem Netzwerk der Universität verbinden, in Verbindung stehen. Der Umfang der Unterstützung durch das UniMS-CERT hängt vom betroffenen System und den beteiligten Nutzenden ab.

Das UniMS-CERT betreut die folgenden öffentlichen IP Adressbereiche:

- 128.176.0.0/16
- 185.151.152.0/22
- 193.175.4.0/24
- 212.201.144.0/21

- 2001:638:500::/48
- 2001:4cf0::/29

Sowie die folgenden Domains: - uni-muenster.de - uni.ms - wwü.de - wwü.io

3.3 Zugehörigkeit

Das UniMS-CERT wurde am 14.01.2000 gegründet und ist im Bereich “IT-Sicherheit” des Center for Information Technology (CIT) der Universität Münster angesiedelt.

Das UniMS-CERT steht in engem Kontakt mit dem [DFN-CERT](#) und nach Bedarf verschiedenen CSIRTs deutscher Universitäten. Darüber hinaus ist das UniMS-CERT im [CERT-Verbund](#), [EDUCV](#) und [TF-CSIRT](#) aktiv.

3.4 Ermächtigung

Die “Informationssicherheitsleitlinie der Universität Münster” und die “Richtlinie zum Informationssicherheitsmanagementsystem” legen die Aufgaben sowie Zuständigkeiten des UniMS-CERT fest und stellen die Basis für die Tätigkeiten dar.

Das UniMS-CERT erwartet, mit Administrierenden und Nutzenden der Universität Münster kooperativ zusammenzuarbeiten und soweit möglich autoritäre Beziehungen zu vermeiden. Sollten allerdings die Umstände es erfordern und rechtfertigen, wird das UniMS-CERT das CIT auffordern, seine Autorität nach Bedarf, direkt oder indirekt, auszuüben, z.B. durch Sperrung von Nutzerkennungen oder Netzzugängen für Endgeräte.

Mitglieder des Verantwortlichkeitsbereichs, die gegen die Handlungen des UniMS-CERT Einspruch erheben möchten, sollten sich an den [Chief Information Security Officer](#) (CISO) oder den [Chief Information Officer](#) (CIO) der Universität Münster wenden.

4. Richtlinien

4.1 Arten von Vorfällen und Unterstützungsleistungen

Das UniMS-CERT ist berechtigt, alle Arten von Informationssicherheitsproblemen oder -vorfällen mit Bezug zur Universität Münster zu behandeln. Dies beinhaltet bereits erfolgte Vorfälle, wie auch Vorfälle, die noch erfolgen könnten.

Die Unterstützung durch das UniMS-CERT variiert je nach Art und Schwere des Vorfalls oder Problems, der Art und Größe der betroffenen Personengruppe, dem betroffenen System und den verfügbaren Ressourcen des UniMS-CERT zu diesem Zeitpunkt. Das UniMS-CERT behandelt Sicherheitsvorfälle gemäß der “Richtlinie zur Detektion und Behandlung von Sicherheitsvorfällen” der Universität Münster. Ressourcen werden nach folgenden Prioritäten zugewiesen, die in absteigender Reihenfolge aufgeführt sind:

- Bedrohungen für die körperliche Sicherheit von Menschen.
- Root- oder Systemlevel-Angriffe auf Systeme der zentralen Management Struktur oder auf Teile der Backbone-Netzwerkinfrastruktur.
- Root- oder Systemlevel-Angriffe auf Systeme, die große öffentliche Dienste für mehrere Nutzende oder für bestimmte Zwecke bereitstellen.
- Kompromittierung von sensiblen Managementkonten oder Softwareinstallationen, z.B. Kennungen oder Systeme zur zentralen Administration.
- Denial of Service-Angriffe auf einen der drei oben genannten Punkte.
- Alle oben genannten Vorfälle, die von der Universität Münster ausgehen und fremde Systeme betreffen.
- Groß angelegte Angriffe jeglicher Art, z.B. Sniffing, Social Engineering oder Password Cracking Angriffe.
- Kompromittierung einzelner Nutzerkennung auf Mehrbenutzer-Systemen.
- Kompromittierung von Desktop-Systemen.
- Fälschung, Falschdarstellung und andere sicherheitsrelevanten Verstöße gegen örtliche Gesetze und Vorschriften, z.B. Urheberrechtsverletzungen oder Fälschung von E-Mails
- Drohungen, Belästigungen und andere Straftaten, die individuelle Nutzerkennungen betreffen.
- Denial of Service-Angriffe auf einzelne Nutzerkennungen, z.B. durch Mailbombing.

Anderen Arten von Vorfällen, die oben nicht genannt wurden, wird eine Priorisierung anhand der erkennbaren Schwere und dem möglichen Ausmaß zugeordnet. Die Klassifizierung orientiert sich grob an der [Security Incident Classification Taxonomy](#) der Agentur der Europäischen Union für Cybersicherheit (ENISA).

Es wird darauf hingewiesen, dass das UniMS-CERT in der Regel keine direkte technische Unterstützung der Endnutzenden bietet. Endnutzende sollten sich dafür an die Administrierenden der zuständigen [IVV](#), die zuständigen IV-Sicherheitsbeauftragten ([IV-SB](#)) oder die [IT-Beratung des CIT](#) wenden. Das UniMS-CERT unterstützt diese.

Das UniMS-CERT ist sich bewusst, dass die Kenntnisse der Administrierenden an der Universität Münster sehr unterschiedlich sind, und obwohl das UniMS-CERT sich bemüht, Informationen und Unterstützung auf einer für jede Person geeigneten Stufe zu präsentieren, kann es keine Administrierenden ad-hoc schulen oder Wartungen an ihren Systemen für sie durchführen. In der Regel liefert das UniMS-CERT allerdings Hinweise zur Umsetzung geeigneter technischer Maßnahmen.

Das UniMS-CERT verpflichtet sich dazu, die IV-Sicherheitsbeauftragten (IV-SB) und Administrierenden der Universität Münster über kritische Schwachstellen zu informieren. Soweit möglich werden diese Informationen über die interne Mailingliste ivv-admins@uni-muenster.de verteilt, idealerweise bevor diese Schwachstellen aktiv ausgenutzt werden.

4.2 Kooperation, Interaktion und Offenlegung von Informationen

Alle Informationen, die das UniMS-CERT bearbeitet, werden standarmäßig als vertraulich betrachtet und nur im Bedarfsfall geteilt. Alle Mitglieder des UniMS-CERT haben eine Verschwiegenheitserklärung (NDA) unterzeichnet und befolgen übliche Richtlinien zur Weitergabe von Informationen, wie z.B. das [Traffic Light Protocol \(TLP\)](#). Das UniMS-CERT strebt die Einhaltung des Trusted Introducer (TI) [CSIRT Code of Practice \(CCoP\)](#) an.

Aufgrund ihrer Verantwortlichkeiten und der daraus resultierenden Vertraulichkeitserwartungen haben Mitglieder der Leitung der Universität Münster und des CIT das Recht, alle Informationen, die erforderlich zur Unterstützung der Aufklärung von Informationssicherheitsvorfällen in ihrem Verantwortungsbereich sind, zu erhalten. IV-Sicherheitsbeauftragte (IV-SB) und Administrierende der Universität Münster werden aufgrund ihrer Verantwortlichkeit auch mit vertraulichen Informationen betraut. Wenn diese Personen jedoch nicht auch Mitglieder des UniMS-CERT sind, erhalten sie nur die Informationen, die sie zur Unterstützung einer Untersuchung oder zur Absicherung ihrer eigenen Systeme haben müssen. Nutzende von Diensten der Universität Münster haben das Anrecht auf Informationen, die die Sicherheit ihrer eigenen Kennungen betreffen, und werden über mögliche Kompromittierungen informiert.

Da das UniMS-CERT die Informationssicherheitsgemeinschaft unterstützen möchte, beteiligt es sich am Austausch von vorfallsbezogenen Informationen, z.B. IOAs/IOCs, mit anderen vertrauenswürdigen Institutionen oder CSIRTs. Falls bestimmte Informationen nützlich zur Verhinderung oder Aufklärung eines Vorfalls an einer anderen Einrichtung sind, werden diese gerne geteilt. Um ethischen und rechtlichen Beschränkungen nachzukommen, werden Maßnahmen zur Anonymisierung von personenbezogenen Informationen, sowie anderer sensibler Details unternommen.

Das UniMS-CERT kooperiert mit Strafverfolgungsbehörden, was im Einklang mit der [IT-Benutzungsordnung](#) der Universität Münster steht. Die Weitergabe vertraulicher Informationen zur Durchführung von Ermittlungen kann notwendig oder sogar rechtlich erforderlich sein. In solchen Fällen wird die Rechtsabteilung der Universität Münster beteiligt. Die Menge der weitergegebenen Informationen wird immer so gering wie möglich gehalten.

Vertrauliche Informationen werden niemals mit den gesamten Mitgliedern des Verantwortungsbereichs oder gar der allgemeinen Öffentlichkeit geteilt. Sollte die Veröffentlichung von Informationen in einem größeren Rahmen notwendig sein, wird dies unter Einbeziehung der Rechtsabteilung und der Abteilung für Öffentlichkeitsarbeit erfolgen.

4.3 Kommunikation und Authentifizierung

Unverschlüsselte E-Mails werden nicht als besonders sicher angesehen, genügen jedoch für die Übertragung von Daten mit geringer Sicherheitseinstufung. Werden hoch sensible Daten per E-Mail gesendet, müssen PGP oder S/MIME zur Ende-zu-Ende Verschlüsselung genutzt werden. Dateiübertragungen über das Netzwerk werden für diese Zwecke wie E-Mails behandelt: sensible Daten sollten für die Übertragung Ende-zu-Ende verschlüsselt werden. Um die Herkunft und Integrität von übertragenen Daten zu gewährleisten, werden, soweit möglich, digitale Signaturen verwendet. Zu diesem Zweck werden alle offiziellen E-Mails des UniMS-CERT oder einzelner Mitglieder mit PGP oder S/MIME signiert. Telefone werden in der Regel als ausreichend sicher angesehen, um auch unverschlüsselt verwendet zu werden.

Das UniMS-CERT unterstützt das Traffic Light Protocol (TLP) (<https://www.first.org/tlp/>) und respektiert Beschränkungen beim Austausch von Informationen.

Wenn es erforderlich ist, Vertrauen aufzubauen, z.B. bevor man sich auf Informationen, die dem UniMS-CERT übermittelt werden, verlässt oder bevor vertrauliche Informationen offengelegt werden, wird die Identität und die Vertrauenswürdigkeit der anderen Partei in einem angemessenen Maß ermittelt. Innerhalb der Universität Münster und bei bekannten CERTs oder CSIRTs genügen Empfehlungen von

vertrauenswürdigen Personen, um jemanden zu identifizieren. Andernfalls werden geeignete Methoden verwendet, z.B. eine Suche nach FIRST-Mitgliedern, die Verwendung von WHOIS und anderen Internetregistrierungsinformationen, so wie ein telefonischer Rückruf oder ein signierter E-Mail-Austausch, um sicherzustellen, dass die andere Partei legitim ist. Eingehende E-Mails, deren Daten als vertrauenswürdig eingestuft werden müssen, werden mittels digitaler Signaturen geprüft (PGP und S/MIME werden unterstützt).

4.4 Reaktionszeit

In der Regel erfolgt eine erste Antwort zeitnah noch am selben Tag. Falls dies nicht möglich ist, wird innerhalb von zwei Werktagen geantwortet.

5. Dienste

Das UniMS-CERT stellt verschiedene Dienste aus unterschiedlichen Bereichen der IT Sicherheit bereit. Die meisten Dienste werden nur für Mitglieder und Systeme des Verantwortungsbereichs angeboten, einige Dienste stehen aber auch externen Personen offen. Die verfügbaren Dienste werden nach dem [CSIRT Services Framework v2.1](#) des FIRST kategorisiert und werden hier nur stichpunktartig gelistet. Beschreibungen der einzelnen Bereiche und der jeweiligen Dienste können in der [CSIRT Services Framework Dokumentation](#) nachgelesen werden. Weitere Details zu einigen Diensten können auch auf den [Webseiten des UniMS-CERT](#) gefunden werden.

5.1 Information Security Event Management

- [Monitoring and Detection](#)
- [Event Analysis](#)

5.2 Information Security Incident Management

- [Information Security Incident Report Acceptance](#)
- [Information Security Incident Analysis](#)
- [Artifact and Forensic Evidence Analysis](#)
(Nur in besonderen Fällen und in eingeschränktem Umfang)
- [Mitigation and Recovery](#)
(Beschränkt auf die Koordination und Unterstützung für betroffene Parteien)
- [Information Security Incident Coordination](#)
- [Crisis Management Support](#)

5.3 Vulnerability Management

- [Vulnerability Report Intake](#)
- [Vulnerability Analysis](#)
(Nur in beschränktem Rahmen zur Unterstützung bei der Schwachstellenbehebung)
- [Vulnerability Disclosure](#)
- [Vulnerability Response](#)
(Beschränkt auf die Erkennung von/Suche nach Schwachstellen und Unterstützung bei der Beseitigung)

5.4 Situational Awareness

- [Data Acquisition](#)
- [Analysis and Synthesis](#)
- [Communication](#)

5.5 Knowledge Transfer

- [Awareness Building](#)

(Nur in unterstützender Rolle für die Stabsstelle Informationssicherheit)

- [Technical and Policy Advisory](#)

(Nur in unterstützender Rolle für die Stabsstelle Informationssicherheit)

6. Meldung von Sicherheitsvorfällen

Aktuell existieren keine speziellen Formulare für die Meldung von Sicherheitsvorfällen an das UniMS-CERT, aber für eine schnelle Bearbeitung sollten die folgenden Informationen immer enthalten sein:

- Datum und Zeitpunkt des Vorfalls (inklusive Zeitzone)
- Quell-IPs und -Ports, sowie genutzte Protokolle (sofern zutreffend)
- Ziel-IPs und -Ports, sowie genutzte Protokolle (sofern zutreffend)
- Vorfallsbeschreibung und mögliche weitere Details

Vorzugsweise sollte die Meldung vorfallsbezogene Log-Dateien in einem üblichen Format enthalten, z.B. Syslog oder Common Event Format (CEF). Wenn verdächtige E-Mails weitergeleitet werden, sollten diese als Anhang weitergeleitet werden, damit alle relevanten E-Mail-Header enthalten sind.

Wird eine entdeckte Schwachstelle gemeldet, sollten die üblichen Regeln für die verantwortungsvolle Offenlegung (Responsible Disclosure), wie keine schädliche Ausnutzung der Schwachstelle, Ende-zu-Ende verschlüsselte Übertragung sensibler Daten und keine Offenlegung der Schwachstelle an Dritte bis diese behoben wurde, beachtet werden.

7. Haftungsausschluss

Während bei der Erstellung von Informationen, Benachrichtigungen und Warnmeldungen jede Vorsichtsmaßnahme ergriffen wird, übernimmt das UniMS-CERT keine Verantwortung für Fehler oder Auslassungen oder für Schäden, die durch die Verwendung der darin enthaltenen Informationen entstehen. Dies gilt auch für dieses Dokument, welches „so wie es ist“ zur Verfügung gestellt wird, ohne jegliche ausdrückliche oder stillschweigende Garantie.

Wenn Sie Fehler in diesem Dokument feststellen, schicken Sie bitte eine Nachricht per E-Mail an das UniMS-CERT. Wir werden versuchen, die Fehler in der nächsten Version zu beseitigen.

8. Copyright

Copyright (C) The Internet Society (1998). All Rights Reserved.

Copyright (C) Universität Münster (2026). All Rights Reserved.