CSIRT Beschreibung für WWU-CERT

CSIRT Beschreibung für WWU-CERT
1. Über dieses Dokument
    1.1 Letzte Änderung
    1.2 Verteilerliste für Benachrichtigungen
    1.3 Orte, an denen dieses Dokument gefunden werden kann
    1.4 Authentizität dieses Dokuments
2. Kontaktinformation
    2.1 Name des Teams
    2.2 Adresse
    2.3 Zeitzone
    2.4 Telefonnummer
    2.5 Faxnummer
    2.6 Andere Telekommunikation
    2.7 Elektronische Mail Adresse
    2.8 Öffentliche Schlüssel und andere Verschlüsselungs-Informationen
    2.9 Mitglieder
    2.10 Weitere Informationen
    2.11 Kontaktmöglichkeiten
3. Charta
    3.1 Leitbild
    3.2 Verantwortlichkeitsbereich
    3.3 Förderung und Zugehörigkeit
    3.4 Ermächtigung
4. Richtlinien
    4.1 Arten von Vorfällen und Unterstützungsleistungen
    4.2 Kooperation, Interaktion und Offenlegung von Informationen
    4.3 Kommunikation und Authentifizierung
    4.4 Reaktionszeit
5. Dienste
    5.1 Information Security Event Management
    5.2 Information Security Incident Management
    5.3 Vulnerability Management
    5.4 Situational Awareness
    5.5 Knowledge Transfer
6. Meldung von Sicherheitsvorfällen
7. Haftungsausschluss
8. Copyright

1. Über dieses Dokument

Dieses Dokument enthält eine Beschreibung des **WWU-CERT** gemäß RFC 2350. Es stellt Informationen über das CERT bereit, wie es kontaktiert werden kann, und erläutert den Verantwortlichkeitsbereich sowie die bereitgestellten Dienste des WWU-CERT.

1.1 Letzte Änderung

Dies ist Version 1.2, veröffentlicht am 27.04.2021.

1.2 Verteilerliste für Benachrichtigungen

Aktualisierungen dieses Dokuments werden über die interne Mailingliste iv-sicherheit@uni-muenster.de bekanntgegeben. Ansonsten kann die aktuelle Version 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 zur Beschreibung des CSIRT steht auf der Webseite des WWU-CERT zur Verfügung:

- **Deutsch:** https://www.uni-muenster.de/ziv.cert/CSIRT-descr-de.pdf
- **Englisch:** https://www.uni-muenster.de/ziv.cert/CSIRT-descr-en.pdf

1.4 Authentizität dieses Dokuments

Beide Versionen dieses Dokuments wurden mit dem PGP Schlüssel des WWU-CERT signiert. Der Fingerabdruck des Schlüssels kann in Abschnitt 2.8 oder auf der Webseite des WWU-CERT gefunden werden. Der öffentliche Schlüssel kann von den üblichen Schlüsselservern heruntergeladen werden.
Die Signaturen der beiden Dokumente können ebenfalls über die Webseite eingesehen werden:

- https://www.uni-muenster.de/ziv.cert/CSIRT-descr-de.pdf.asc
- https://www.uni-muenster.de/ziv.cert/CSIRT-descr-en.pdf.asc

2. Kontaktinformation

2.1 Name des Teams

WWU-CERT: Computer Emergency Response Team der Westfälischen Wilhelms-Universität (WWU) Münster

2.2 Adresse

WWU IT
WWU-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 WWU-CERT)

2.5 Faxnummer

`+49 251 83 31552` (dies ist *kein* sicheres Fax)

2.6 Andere Telekommunikation

Einige Mitglieder des WWU-CERT sind auf verschiedenen online CSIRT 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 Vorfallskommunikation genutzt werden.
- spam@uni-muenster.de - Dies ist eine spezielle Adresse zur Meldung von Phishing/Spam mit Bezug zur Universität Münster (WWU).

2.8 Öffentliche Schlüssel und andere Verschlüsselungs-Informationen

Das WWU-CERT hat einen PGP Schlüssel mit der KeyID 0xC01D356E und dem folgenden Fingerabdruck:

- `DAFE C355 08F3 CB67 2DF7 C3C2 76E4 1181 C01D 356E`

Der Schlüssel und seine Signaturen können auf den üblichen großen Schlüsselservern gefunden werden, z.B. https://pgp.surfnet.nl.

Das WWU-CERT hat außerdem ein X.509 Zertifikat mit der KeyID 0x225CEDC99156B5C37FF43DCB und dem folgenden Fingerabdruck:

- `7F89 6686 0475 8F21 5883 885A 1B4B A1C8 60B4 AA62`

Das Zertifikat mit öffentlichem Schlüssel kann auf den Schlüsselservern der DFN-PKI gefunden werden.

2.9 Mitglieder

Thorsten Küfer (WWU IT), CISO der Westfälischen-Wilhelms Universität (WWU) Münster, (PGP KeyID: 0x4CD0C117) ist der aktuelle Leiter des WWU-CERT. Zur einfacheren Aktualisierung und um dieses Dokument kurz zu halten, können Informationen zu stellvertretenden Leitern und weiteren Mitglieder auf der WWU-CERT Webseite gefunden werden.

Management, Kooperation und Aufsicht erfolgen durch Dr. Raimund Vogl, CIO der Universität Münster (WWU) und Leiter der WWU IT.

2.10 Weitere Informationen

Seit 2018 ist das WWU-CERT Mitglied des CERT-Verbund und des EDUCV. Darüber hinaus ist das WWU-CERT seit dem 28.08.2018 beim Trusted Introducer (TI) Service gelistet.

Weitere Informationen können auf der Webseite des WWU-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 WWU-CERT auch telefonisch während der normalen Bürozeiten erreicht werden. Telefonische Nachrichten werden nicht so häufig wie E-Mails abgehört.

Im Allgemeinen sind die Betriebszeiten des WWU-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 Verantwortlichkeitsbereich des WWU-CERT betrifft, kann die Rufbereitschaft des Network Operating Center (NOC) alarmiert werden.

3. Charta

3.1 Leitbild

Aufgabe des WWU-CERT ist die Unterstützung der Mitglieder der Westfälischen Wilhelms-Universität Münster (WWU), 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 (WWU), sowie die Angehörigen und Infrastruktur, vor fahrlässiger oder illegaler Nutzung ihrer IP-Adressen und Ressourcen zu schützen. Das WWU-CERT stellt die zentrale Koordinationsstelle für IT Sicherheitsinformationen, -probleme und -vorfälle für den Verantwortlichkeitsbereich dar.

3.2 Verantwortlichkeitsbereich

Der Verantwortlichkeitsbereich des WWU-CERT umfasst den Geltungsbereich, wie er in der "Informationssicherheitsleitlinie der Westfälischen Wilhelms-Universität Münster" (ISL-WWU) definiert ist. Dazu gehören alle Systeme und Nutzer von Diensten der Universität. Dezentrale Bereiche und ihre Mitglieder gehören ebenfalls zum Verantwortlichkeitsbereich. Das WWU-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 WWU-CERT hängt vom betroffenen System und den beteiligten Nutzern ab.

Das WWU-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
- wwu.de
- wwu.io

3.3 Förderung und Zugehörigkeit

Das WWU-CERT wurde am 14.01.2000 eingerichtet und wird gefördert durch das IT-Center (WWU IT) der Universität Münster (WWU). Es ist Teil der Stabsstelle für IT-Sicherheit und arbeitet eng mit dem IT Sicherheitsteam zusammen (siehe ISL-WWU). Die Geschäftsstelle wurde bei der WWU IT eingerichtet.

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

3.4 Ermächtigung

Das WWU-CERT arbeitet unter der Schirmherrschaft und mit Autorität des IT-Centers (WWU IT) der Universität Münster (WWU). Dies wurde festgelegt und verabschiedet in der "Informationssicherheitsleitlinie der Westfälischen Wilhelms-Universität Münster" (ISL-WWU).

Das WWU-CERT erwartet, mit Systemadministratoren und Benutzern der Universität Münster (WWU) kooperativ zusammenzuarbeiten und soweit möglich autoritäre Beziehungen zu vermeiden. Sollten allerdings die Umstände es erfordern und rechtfertigen, wird das WWU-CERT die WWU IT 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 WWU-CERT Einspruch erheben möchten, sollten sich an den Chief Information Officer (CIO) oder an die IV-Kommission der Universität Münster (WWU) wenden.

4. Richtlinien

4.1 Arten von Vorfällen und Unterstützungsleistungen

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

Die Unterstützung durch das WWU-CERT variiert je nach Art und Schwere des Vorfalls oder Problems, der Art des Anfragenden, der Größe der betroffenen Benutzergruppe, dem betroffenen System und den verfügbaren Ressourcen des WWU-CERT zu diesem Zeitpunkt. 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 Benutzer 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 (WWU) ausgehen und fremde Systeme betreffen.
- Groß angelegte Angriffe jeglicher Art, z.B. Sniffing, Social Engineering oder Password Cracking Angriffe.
- Drohungen, Belästigungen und andere Straftaten, die individuelle Nutzerkennungen betreffen.

- 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.
- 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 Incident Classification des Trusted Introducer (TI).

Es wird darauf hingewiesen, dass das WWU-CERT in der Regel keine direkte Unterstützung der Endnutzer bietet. Endnutzer sollten sich dafür an ihren zuständigen Systemadministrator der IVV, den zuständigen IV-Sicherheitsbeauftragten (IV-SB), die IT Nutzerberatung oder den Leiter der jeweiligen Abteilung wenden. Das WWU-CERT unterstützt diese.

Das WWU-CERT ist sich bewusst, dass die Kenntnisse der Systemadministratoren an der Universität Münster (WWU) sehr unterschiedlich sind, und obwohl das WWU-CERT sich bemüht, Informationen und Unterstützung auf einer für jede Person geeigneten Stufe zu präsentieren, kann es keine Systemadministratoren ad-hoc schulen oder Wartungen an ihren Systemen für sie durchführen. In der Regel liefert das WWU-CERT allerdings Hinweise auf die Informationen, die zur Umsetzung geeigneter Maßnahmen erforderlich sind. Systemadministratoren sollen sich primär an den IV-Sicherheitsbeauftragten (IV-SB) des Bereichs wenden.

Das WWU-CERT verpflichtet sich dazu, die IV-Sicherheitsbeauftragten (IV-SB) und Systemadministratoren der Universität Münster (WWU) über potentielle Schwachstellen zu informieren. Soweit möglich werden diese Informationen über die interne Mailingliste iv-sicherheit@uni-muenster.de verteilt, idealer Weise bevor diese Schwachstellen aktiv ausgenutzt werden.

4.2 Kooperation, Interaktion und Offenlegung von Informationen

Alle Informationen, die das WWU-CERT bearbeitet, werden standarmäßig als vertraulich betrachtet und nur im Bedarfsfall geteilt. Alle Mitglieder des WWU-CERT haben eine Verschwiegenheitserklärung (NDA) unterzeichnet und befolgen übliche Richtlinien zur Weitergabe von Informationen, wie z.B. das Traffic Light Protocol (TLP). Das WWU-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 (WWU) und der WWU IT das Recht, alle Informationen, die erforderlich zur Unterstützung der Aufklärung von Informationssicherheitsvorfällen in ihrem Verantwortlichkeitsbereich sind, zu erhalten. IV-Sicherheitsbeauftragte (IV-SB) und Systemadministratoren der Universität Münster (WWU) werden aufgrund ihrer Verantwortlichkeit auch mit vertraulichen Informationen betraut. Wenn diese Personen jedoch nicht auch Mitglieder des WWU-CERT sind, erhalten sie nur die Informationen, die sie zur Unterstützung einer Untersuchung oder zur Absicherung ihrer eigenen Systeme haben müssen. Nutzer von Diensten der Universität Münster (WWU) haben das Anrecht auf Informationen, die die Sicherheit ihrer eigenen Kennungen betreffen, und werden über mögliche Kompromittierungen informiert.

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

Vertrauliche Informationen werden niemals mit den gesamten Mitgliedern des Verantwortlichkeitsbereichs 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

In Anbetracht der Arten von Informationen, mit denen sich das WWU-CERT befasst, werden Telefone als ausreichend sicher angesehen, um auch unverschlüsselt verwendet zu werden. 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 WWU-CERT oder einzelner Mitglieder mit PGP oder S/MIME signiert.

Das WWU-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 WWU-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 (WWU) 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 kein Betrüger ist. Eingehende E-Mails, deren Daten als vertrauenswürdig eingestuft werden müssen, werden beim Absender persönlich oder 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 WWU-CERT stellt verschiedene Dienste aus unterschiedlichen Bereichen der IT Sicherheit bereit. Die meisten Dienste werden nur für Mitglieder und Systeme des Verantwortlichkeitsbereichs 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 WWU-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 das IT-Sicherheitsteam)
- Training and Education

  (Nur in beschränktem Rahmen angeboten)
- Technical and Policy Advisory

  (Nur in unterstützender Rolle für das IT-Sicherheitsteam)

6. Meldung von Sicherheitsvorfällen

Aktuell existieren keine speziellen Formulare für die Meldung von Sicherheitsvorfällen an das WWU-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 WWU-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 WWU-CERT. Wir werden versuchen, solche Fehler in der nächsten Version zu beseitigen.

8. Copyright