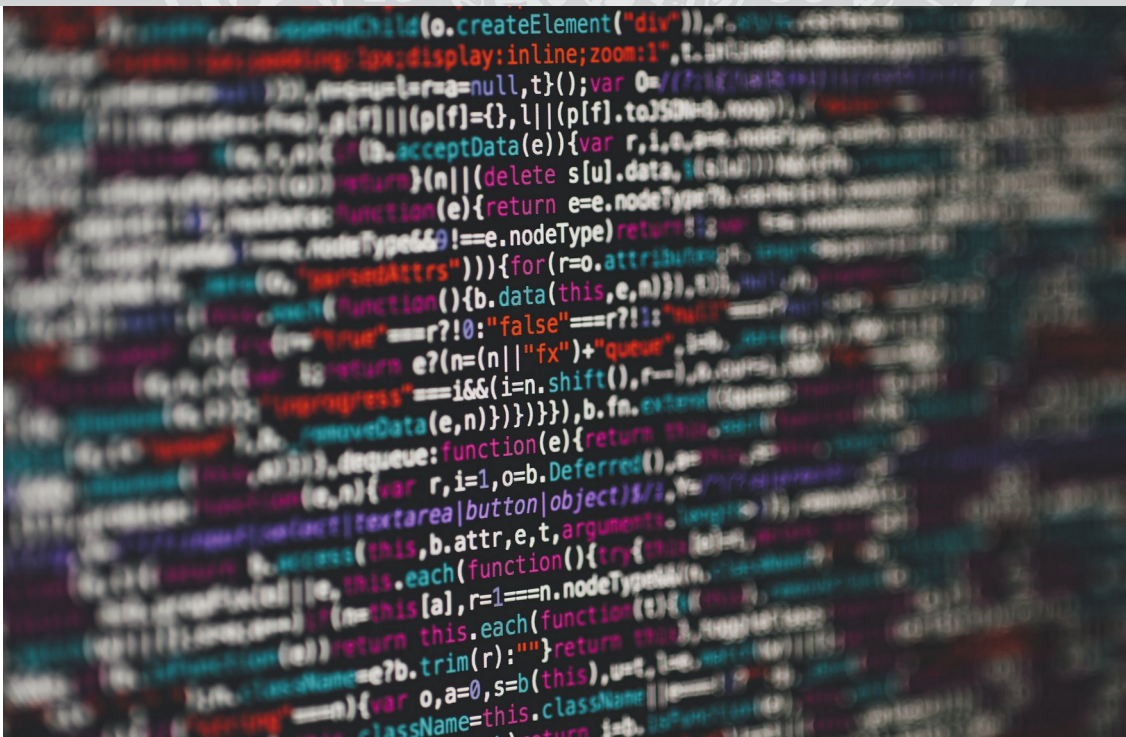
JMU-CERT

Beschreibung nach RFC 2530

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG



Inhaltsverzeichnis

Historie

Datum	Version	Autor	Änderungen
09.09.2020	1.0	Jens Roesen	Initiale Version

1. Über dieses Dokument

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 JMU-CERT, dem "Computer Emergency Response Team" der Julius-Maximilians-Universität Würzburg. Es stellt Informationen über das CERT bereit, wie es kontaktiert werden kann, und erläutert den Verantwortlichkeitsbereich sowie die bereitgestellten Dienste des JMU-CERT. Eine formalisierte Kurzdarstellung einer CERT-Struktur nach RFC 2350 hat sich als quasi-Standard etabliert und ist geeignet, um sich einen schnellen Über-blick über die Schnittstellen und Dienstleistungen eines CERT zu verschaffen.

1.1 Letzte Änderung

Dies ist Version 1.0, veröffentlicht am 09.09.2020

1.2 Verteilerliste für Benachrichtigungen

Neuigkeiten werden an die moderierte Mailingliste für IT-Bereichsmanager und Netzverantwortliche der JMU-Würzburg verschickt.

1.3 Orte, an denen dieses Dokument gefunden werden kann

Die aktuelle Version dieses Dokuments zur Beschreibung des JMU-CERT steht auf der Webseite des JMU-CERT zur Verfügung. Sie ist zu erreichen über:

https://www.uni-wuerzburg.de/fileadmin/cert/JMU-CERT_RFC2350_de.pdf

Bitte stellen Sie sicher, dass Sie die aktuelle Version des Dokuments nutzen.

1.4 Authentizität dieses Dokuments

Die aktuelle Version dieses Dokuments wurden mit dem PGP Schlüssel des JMU-CERT signiert. Die Signatur finden sie auf der Webseite des JMU-CERT unter:

https://www.uni-wuerzburg.de/fileadmin/cert/JMU-CERT_RFC2350_de.pdf.asc

Der öffentliche Schlüssel kann sowohl von der Webseite des JMU-CERT als auch von den üblichen Schlüsselservern heruntergeladen werden.

Weitere Informationen können in Abschnitt 2.8 gefunden werden.

2. Kontaktinformationen

2.1 Name des Teams

JMU-CERT: Computer Emergency Response Team der Julius-Maximilians-Universität Würzburg.

2.2 Adresse

JMU-CERT
Rechenzentrum
Am Hubland
97074 Würzburg

2.3 Zeitzone

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

2.4 Telefonnummer

+49 931 31 86999

2.5 Fax

+49 931 31 86999 0

2.6 E-Mail

cert@uni-wuerzburg.de

2.7 Andere Telekommunikation

Keine vorhanden.

2.8 Public Keys und Informationen zur Signierung und Verschlüsselung

Für die elektronische Übermittlung vertraulicher Informationen wird die Nutzung von die Nutzung von S/MIME- oder PGP-Verschlüsselung empfohlen.

Das JMU-CERT hat einen PGP Schlüssel mit der KeyID

`0x963DFCE3B41FC835`

und dem Fingerabdruck

7252 AB7D BAFC 4EEB 154E.

Der öffentliche Schlüssel kann sowohl von der Webseite des JMU-CERT unter https://www.uni-wuerzburg.de/fileadmin/cert/jmu-cert_pub_key.asc als auch von den üblichen Schlüsselservern heruntergeladen werden. Es wird empfohlen, den Fingerprint telefonisch zu verifizieren.

Das X.509 Zertifikat des JMU-CERT mit der Seriennummer

0x232E2F7AFDB6893FF6724805

und dem Fingerprint

SHA1:D6:CE:87:A1:74:6A:12:57:F1:4B:97:5E:42:D5:9D:21:D9:A7:88:81

kann auf den Schlüsselservern des DFN-PKI gefunden und heruntergeladen werden.

2.9 Mitglieder

Das Computer Emergency Response Team der Julius-Maximilians-Universität Würzburg (JMU-CERT) besteht aus den Sicherheitsexperten und Sicherheitsexpertinnen des Rechenzentrums, wird von der oder dem CIO in Absprache mit der Leiterin oder dem Leiter des Rechenzentrums eingesetzt und berichtet an diese oder diesen. Eine situations- oder vorfallbezogene personelle Ergänzung oder Änderung der Zusammensetzung des CERT ist möglich.

Zum Zeitpunkt der Veröffentlichung dieses Dokuments besteht das JMU-CERT aus folgenden ständigen Mitgliedern:

- Markus Krieger
- Jens Roesen

2.10 Weitere Informationen

Allgemeine Informationen über das JMU-CERT und Verweise auf empfohlene Quellen zu verschiedenen IT-Sicherheitsthemen können auf den Webseiten des JMU-CERT gefunden werden:

https://www.uni-wuerzburg.de/cert/

2.11 Betriebszeiten

Montags-Donnerstags: 08:30 Uhr bis 17:00 Uhr
Freitags: 08:30 Uhr bis 16:00 Uhr

Ausnahmen: 24. Dezember bis einschließlich 1.1. sowie gesetzliche Feiertage in Bayern.

3. Charta

3.1 Ziele und Aufgaben (Mission Statement)

Aufgabe des JMU-CERT ist die Unterstützung der Julius-Maximilians-Universität Würzburg (JMU) bei folgenden Themen:

- Beratung zu und Umsetzung von proaktiven IT-Sicherheitsmaßnahmen
- Leitung der Analyse, Bearbeitung und Aufkärung von Informationssicherheitsvorfällen im Zusammenhang mit der Nutzung von Rechnern, IP-Adressen und Kennungen in bzw. an der JMU Würzburg sowie Berichtspficht über diese an den CIO bzw. an die auf Landes- und Bundesebene für Informationssicherheit definierten Stellen.
- Zusammenarbeit mit anderen Stellen innerhalb der JMU Würzburg, die mit IT-Sicherheit und Datenschutz befasst sind
- Kooperation mit dem DFN-CERT und anderen vergleichbaren Einrichtungen

3.2 Zielgruppe (Constituency)

Die Dienstleistungen des JMU-CERT richten sich an alle Einrichtungen der Julius-Maximilians-Universität Würzburg und innerhalb der genannten Einrichtungen primär an die IT-Bereichsmanager.

3.3 Verantwortlichkeitsbereich

Der Verantwortlichkeitsbereich des JMU-CERT umfalls die folgenden IP-Adressbereiche und Domains:

- 132.187.0.0/16
- 2001:0638:0A09::/48
- uni-wuerzburg.de
- uniwue.de
- edu-bayern.de
- studisoft.de
- uni-wuerzburg.eu
- uni-wue.eu

3.4 Mitgliedschaften

Das JMU-CERT ist Mitglied der Arbeitsgruppe deutscher Hochschulen, Lehr- und Forschungseinrichtungen EDUCV (https://www.educv.de/).

Das JMU-CERT arbeitet im Bedarfsfall mit diversen CERTs und CSIRTs anderer Einrichtungen zusammen.

3.5 Zuständigkeiten und Befugnisse (Authority)

Das JMU-CERT arbeitet unter der Schirmherrschaft des CIO und mit Autorität des Rechenzentrums der Julius-Maximilians-Universität Würzburg (JMU). (In der Zukunft: Weitere Informationen zum Mandat und zur Autorität des JMU-CERTkönnen der "Informationssicherheitsleitlinie der Julius-Maximilians-Universität Würzburg " entnommen werden.)

Das JMU-CERT erwartet, mit IT-Bereichsmanagern, Netzverantwortlichen, Systemadministratoren und Benutzern der JMU Würzburg kooperativ zusammenzuarbeiten und soweit möglich autoritäre Beziehungen zu vermeiden. Sollten allerdings die Umstände es erfordern und rechtfertigen, wird das JMU-CERT seine Autorität nach Bedarf direkt oder indirekt ausüben.

4. Richtlinien

4.1 Arten von Vorfällen und Unterstützungsleistungen

Das JMU-CERT ist berechtigt, alle Arten von IT-Sicherheitsvorfällen an der Julius-Maximilians-Universität Würzburg (JMU) und den unter 3.3 beschriebenen Verantwortungsbereich zu behandeln.

Die Unterstützung durch das JMU-CERT variiert je nach Art und Schwere des Vorfalls oder Problems, der Art des Anfragenden, der Größe der betroffenen Benutzergruppe und den Ressourcen des JMU-CERT zu diesem Zeitpunkt, es erfolgt aber in jedem Fall eine Rückmeldung durch das JMU-CERT.

Es wird darauf hingewiesen, dass das JMU-CERT keine direkte Unterstützung von Endnutzern anbietet. Beschäftigte der JMU Würzburg werden gebeten, sich an die für ihren Bereich tätigen IT-Bereichsmanager bzw. Netzverantwortliche zu wenden. Studierende wenden sich mit ihrem Anliegen bitte an den IT-Support des Rechenzentrums (https://www.rz.uni-wuerzburg.de/it-support/).

4.2 Meldung von Angriffen und Vorfällen

Für die Meldung von Sicherheitsvorfällen und Angriffen wird eine vertrauliche Übermittlung per verschlüsselter E-Mail empfohlen.

Damit eine weitere Bearbeitung erfolgen kann, ist es zwingend erforderlich, dass die Kontaktdaten zur eigenen Person und Einrichtung vollständig und aktuell sind. Dies umfasst:

- Name und Funktion der meldenden Person
- Standort der meldenden Person
- Telefonische Kontaktdaten der meldenden Person für kurzfristige Rückfragen
- E-Mail-Adresse der meldenden Person

Für eine schnelle und effektive Einschätzung des gemeldeten Vorfalls sind ausserdem folgende Informationen notwendig:

- Was ist passiert?
- Wann ist es passiert?
- Wann wurde es entdeckt?
- Wie wurde es entdeckt?
- Welche Resourcen (IP-Adressen, Server, Endgeräte usw.) der JMU Würzburg sind betroffen bzw. in den Vorfall verwickelt?
- Wurden bereits Maßnahmen eingeleitet? Welche Maßnahmen wurden bereits eingeleitet?
- Welche Schäden und Auswirkungen wurden bereits festgestellt oder sind möglich?

4.3 Kommunikation und Authentifizierung

In Anbetracht der Arten von Informationen, mit denen sich das JMU-CERT befasst, werden Telefone als ausreichend sicher angesehen, um auch unverschlüsselt verwendet zu werden.

Unverschlüsselte E-Mails werden nicht als besonders sicher angesehen, reichen jedoch für die Übertragung von Daten mit geringer Sicherheitseinstufung aus. Werden hoch sensible Daten per E-Mail gesendet, müssen PGP oder S/MIME zur Verschlüsselung genutzt werden.

Dateiübertragungen über das Netzwerk werden für diese Zwecke wie E-Mails behandelt: sensible Daten sollten für die Übertragung verschlüsselt werden.

Alle E-Mails mit offiziellen Aussagen des JMU-CERT oder der Teammitglieder müssen mittels X.509 oder PGP signiert werden. E-Mails mit sensiblen Informationen müssen mittels X.509 oder PGP verschlüsselt und signiert werden.

Weitere Informationen zur verschlüsselten Kommunikation mit dem JMU-CERT können in Abschnitt 2.8 gefunden werden.

Das JMU-CERT unterstützt das Traffic Light Protocol (TLP) (https://www.first.org/tlp/) zum Austausch von Informationen.

4.4 Reaktionszeit

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

Die Kontaktinformationen und Arbeitszeiten können in Abschnitt 2 dieses Dokuments gefunden werden.

5. Haftungsausschluss

Obwohl die Erstellung von Informationen, Benachrichtigungen und Warnmeldungen mit der gegebenen Sorgfalt erfolgte, übernimmt das JMU-CERT keine Verantwortung für Fehler oder Versäumnisse oder für Schäden, die durch die Verwendung der darin enthaltenen Informationen entstehen.

Dieses Dokument wird in der vorliegenden Form zur Verfügung gestellt, ohne jegliche ausdrückliche oder stillschweigende Garantie, einschließlich, jedoch nicht beschränkt auf die implizierten Garantien der Marktgängigkeit, der Eignung für einen bestimmten Zweck oder der Nichtverletzung.

Die Verwendung dieses Dokuments erfolgt auf alleinige Gefahr des Benutzers. Alle Benutzer stimmen diesen Nutzungsbedingungen ausdrücklich zu.

Wenn Sie Fehler in diesem Dokument feststellen, schicken Sie bitte eine Nachricht per E-Mail an das JMU-CERT. Wir sind bemüht, solche Fehler so schnell als möglich zu beseitigen.