UNIVERSITÄT BIELEFELD

Computer Emergency Response Team (UBI-CERT)

Team-Informationen nach RFC2350

Version	1.0.1	vom 07.05.2024
Status	Öffentlich	
Zuständig	UBI-CERT	
Klassifizierung	TLP:WHITE	
Verteilerliste	keine	
Authentizität	Download per SSL/TLS von https://www.uni-bielefeld.de/cert	

Inhaltsverzeichnis

1 Vorbemerkung

Dieses Dokument beschreibt in Anlehnung an RFC 2350[1] grundlegende Informationen über das UBI-CERT, dem „Computer Emergency Response Team“ der Universität Bielefeld, dessen Kommunikationskanäle, Schnittstellen und Befugnisse.

2 Kontaktinformationen

2.1 Name des Teams

„UBI-CERT“, das Computer Emergency Response Team der Universität Bielefeld.

2.2 Postalische Adresse

Universität Bielefeld
Universitätsstr. 25
33615 Bielefeld

2.3 Zeitzone

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

2.4 Telefonnummer

+49 521 106-88088

2.5 Faxnummer

+49 521 106-1588088 (Standard-Fax, unverschlüsselt)

2.6 eMail-Adresse

Folgende E-Mail-Adresse ist gültig:
cert@uni-bielefeld.de

2.7 Öffentliche Schlüssel und Verschlüsselungsinformationen

Für die elektronische Übermittlung vertraulicher Informationen wird die Nutzung von Verschlüsselung empfohlen. Unterstützt wird S/MIME.

2.8 World Wide Web

Allgemeine Informationen über das UBI-CERT, sowie nützliche Hinweise zu Sicherheitseinstellungen finden Sie unter https://www.uni-bielefeld.de/einrichtungen/bits/services/kuz/support/ubi-cert/index.xml

2.9 Zusammensetzung des Teams

Informationen über die Mitglieder des UBI-CERT können über das Personen- und Einrichtungsverzeichnis der Universität Bielefeld bezogen werden:
Stefan Berge https://ekvv.uni-bielefeld.de/pers_publ/publ/PersonDetail.jsp?personId=19940848
Patric Steckstor https://ekvv.uni-bielefeld.de/pers_publ/publ/PersonDetail.jsp?personId=50236189
Lisa Voigt https://ekvv.uni-bielefeld.de/pers_publ/publ/PersonDetail.jsp?personId=184558644
Enrico Stüwe https://ekvv.uni-bielefeld.de/pers_publ/publ/PersonDetail.jsp?personId=14517376
Marc Ilgenstein https://ekvv.uni-bielefeld.de/pers_publ/publ/PersonDetail.jsp?personId=16317507

[1] (Expectations for Computer Security Incident Response, http://www.ietf.org/rfc/rfc2350.txt)

2.10 Betriebszeiten

Das UBI-CERT ist zu den üblichen Bürozeiten (Mo-Fr 8:00 – 17:00 Uhr) erreichbar.
(Ausnahmen: 24. und 31. Dezember sowie gesetzliche Feiertage in Nordrhein-Westfalen
In dringenden IT-Notfall-Situationen außerhalb der Betriebszeiten, die das UBI-CERT betreffen, können Sie die Leitwarte der Universität Bielefeld kontaktieren:

E-Mail: leitwarte@uni-bielefeld.de
Telefon: +49 521 106-7777

3 Charta

3.1 Ziele und Aufgaben (Mission Statement)

Die Zusammenführung der präventiven, reaktiven und operativen Aufgaben der Informationssicherheit in einem Team ist ein kritischer Erfolgsfaktor, um die Resilienz der Universität Bielefeld hinsichtlich Informationssicherheitsvorfällen und Cyberangriffen sicherzustellen. Dies wird durch Spezialisierung und Konzentration auf die Aufgabenstellung erreicht. Die Aufgabenfelder werden in Kapitel 5 beschrieben.

3.2 Verantwortungsbereich

Der Verantwortlichkeitsbereich des UBI-CERT umfasst den Geltungsbereich, wie er in der "Informationssicherheitsleitlinie der Universität Bielefeld" definiert ist. Dazu gehören alle Systeme und Nutzer*innen von Diensten der Universität. Dezentrale Bereiche und ihre Mitglieder gehören ebenfalls zum Verantwortlichkeitsbereich. Das UBI-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 UBI-CERT hängt vom betroffenen System und den beteiligten Nutzern ab.

Das UBI-CERT betreut die folgenden öffentlichen IP Adressbereiche:
https://www.uni-bielefeld.de/einrichtungen/bits/services/infra/lan/ip-adressen/

3.3 Mitgliedschaften

Das UBI-CERT steht in engem Kontakt mit dem DFN-CERT und nach Bedarf verschiedenen CSIRTs deutscher Universitäten.

4 Richtlinien

4.1 Arten von Vorfällen und Unterstützungsleistungen

Das UBI-CERT befasst sich mit allen Arten von Sicherheitsvorfällen, die in seinem Zuständigkeitsbereich auftreten oder aufzutreten drohen.

Der Umfang der Unterstützung hängt von der Art und Schwere des jeweiligen Sicherheitsvorfalls, der Anzahl der betroffenen Fakultäten oder Einrichtungen und unseren derzeitigen Ressourcen ab.

Wir erwarten, dass sich angehörige der Universität an ihre jeweilige EDV Betreuung wenden.

4.2 Kooperation, Interaktion und Offenlegung von Informationen

Das UBI-CERT wird alle erforderlichen Informationen (verschlüsselt und ggf. anonymisiert) mit anderen CSIRTs, sowie mit anderen betroffenen Parteien austauschen, wenn diese in den Vorfall oder die Reaktion auf den Vorfall involviert sind.

4.3 Kommunikation und Authentifizierung

Alle E-Mails mit offiziellen Aussagen des Teams oder der Teammitglieder sollten mittels S/MIME signiert werden. E-Mails mit sensiblen Informationen sollten mittels S/MIME verschlüsselt und signiert werden.

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

4.4 Reaktionszeiten

5 Dienste

5.1 Prävention

Vorbeugende Maßnahmen treffen, so dass Sicherheitsprobleme nicht zu Informationssicherheitsvorfällen eskalieren.

5.2 Detektion

Aufbau von Fähigkeiten, um Informationssicherheitsvorfälle zeitnah zu identifizieren, um Gegenmaßnahmen zu ergreifen und dadurch negative Auswirkungen möglichst zu verhindern.

5.3 Reaktion

Vorbereitungen treffen, um nach dem Eintreten eines Informationssicherheitsvorfalls die Schadwirkung zu begrenzen. Übernahme der Koordination bei der Bearbeitung von Informationssicherheitsvorfällen.

5.4 Nachhaltigkeit

Aufbereitung der Erkenntnisse aus Informationssicherheitsvorfällen (‚Lessons Learned‘), mit dem Ziel, zu einer kontinuierlichen Verbesserung des Informationssicherheitsmanagements beizutragen.

5.5 Weitere Aufgaben

Zu den weiteren Aufgaben des UBI-CERT gehört die Administration zentraler Sicherheitsdienste, um bei Gefahr in Verzug handlungsfähig zu sein.

6 Meldung von Sicherheitsvorfällen

Aktuell wurden noch keine eigenen Formulare für die Meldung von Sicherheitsvorfällen an das UBI-CERT entwickelt. Bitte melden Sie Sicherheitsvorfälle per (je nach Schutzbedarf der Information verschlüsselter) Email an cert@uni-bielefeld.de.

Sicherheitsmeldungen sollten folgende Informationen enthalten:

- Datum und Uhrzeit des Vorfalls (Zeitzone)
- Quell IP-Adresse, Port und Protokolle
- Ziel IP-Adresse, Port und Protokolle

Nach Möglichkeit sollten Logfiles in einem standardisierten Format beigelegt werden.

7 Haftungsausschluss

Dieses Dokument wird in der vorliegenden Form ohne jegliche ausdrückliche oder stillschweigende Gewährleistung bereitgestellt, einschließlich, aber nicht beschränkt auf die stillschweigende Gewährleistung der Marktgängigkeit, der Eignung für einen bestimmten Zweck oder der Nichtverletzung von Rechten Dritter.

Die Nutzung dieses Dokuments erfolgt auf eigene Gefahr. Alle Nutzer erklären sich ausdrücklich mit dieser Nutzungsbedingung einverstanden.

Sollten Sie Fehler in diesem Dokument bemerken, senden Sie uns bitte eine Nachricht per Email. Wir werden versuchen, solche Probleme so schnell wie möglich zu beheben.

