UNIVERSITÄT BIELEFELD

Informationssicherheitsrichtlinie zum

Computer Emergency Response Team der Universität Bielefeld (UBI-CERT)

Version	1.0.0	vom 19.01.2024
Status	In Kraft	
Zuständig	ISB/DISM	
Klassifizierung	Intern	
Zielgruppe	Universitätsleitung, Betreiber von Informationstechnik, Informationssicherheitsmanagement, UBI-CERT	
Reviewzyklus	jährlich	
Freigabe durch	Dr. Stefan Becker (Kanzler)	am 15.03.2024

Inhaltsverzeichnis

1 Zweck

Die Universität Bielefeld betreibt entsprechend der Informationssicherheitsleitlinie ein Computer Emergency Response Team (UBI-CERT). Diese Richtlinie regelt die Aufgaben des UBI-CERT, die zur Vermeidung, Erkennung und Behandlung von Informationssicherheitsvorfällen unternommen werden. Darüber hinaus werden die Befugnisse und Verantwortlichkeiten des UBI-CERT zur Risikominimierung und zur Gefahrenabwehr festgelegt.

2 Geltungsbereich

Diese Richtlinie regelt die Grundsätze für die Etablierung und den Betrieb des UBI-CERT und gilt hochschulweit. Primäre Zielgruppe sind die Universitätsleitung, die Betreiber*innen von Informationstechnik, die Beauftragen für Datenschutz u. Informationssicherheit und die jeweiligen Managementsysteme.

3 Definitionen

Folgende Begriffe werden im Kontext dieser Richtlinie verwendet:

- **Schwachstelle**
  Im Sinne der Informationstechnik sind Schwachstellen Fehler innerhalb der eingesetzten Hard- und Software. Sie können unter anderem durch mangelhafte Programmierung, Konfiguration und Bedienung von IT-Systemen entstehen und zu einer Gefährdung der Grundwerte der Informationssicherheit (Integrität, Vertraulichkeit und Verfügbarkeit) führen. Schwachstellen sind nicht auf technische Verwundbarkeiten begrenzt, sondern schließen auch organisatorische Probleme ein, die beispielsweise durch Regelungslücken entstehen können.
- **Sicherheitsproblem**
  Ein Sicherheitsproblem liegt vor, wenn eine Schwachstelle durch eine Bedrohung ausgenutzt werden kann und damit zu einer Gefährdung der Grundwerte der Informationssicherheit führen kann. Ein tatsächlicher Schaden ist jedoch noch nicht eingetreten.
- **Sicherheitsrelevantes Ereignis**
  Als sicherheitsrelevantes Ereignis wird ein Ereignis bezeichnet, welches sich negativ auf die Informationssicherheit auswirken kann. Wenn ein sicherheitsrelevantes Ereignis registriert wird, ist dies üblicherweise auf die Verletzung einer Policy, den Versuch eine Sicherheitsmaßnahme zu umgehen oder auf die (versuchte) Ausnutzung einer Schwachstelle zurückzuführen. Ein sicherheitsrelevantes Ereignis wird erst dann zu einem Informationssicherheitsvorfall, wenn eine Schadwirkung eingetreten ist.
- **Informationssicherheitsvorfall**
  Ein Informationssicherheitsvorfall ist gegeben, wenn eine tatsächliche Beeinträchtigung mindestens einer der drei Grundwerte der Informationssicherheit vorliegt. Typische

Folgen sind u.a. ausgespähte, manipulierte oder zerstörte Informationen. Die Ursachen dafür sind dabei vielfältig: darunter fallen fahrlässige Handlungen (z.B. fehlerhafte Konfiguration) und vorsätzliche Handlungen, beispielsweise Angriffe aus dem Internet oder Verstöße gegen interne Regelungen. Aber auch technisches Versagen, Unfälle oder externe Ereignisse können Ursachen von Informationssicherheitsvorfällen sein.

- **Weitreichender Informationssicherheitsvorfall**
  Nach Beschreibung des BSI sind zielgerichtete Cyberangriffe als weitreichende Informationssicherheitsvorfälle einzustufen (auch als Advanced Persistent Threats – APT bekannt.) Dabei verschaffen sich die Angreifer einen dauerhaften Zugriff zu dem Netzwerk einer Organisation und weiten diesen Zugriff auf weitere IT-Systeme bzw. die Infrastruktur aus, so dass letztendlich die komplette Produktionsumgebung betroffen sein kann.
- **Gefahr im Verzug**
  Gefahr im Verzug (GiV) bezieht sich auf eine Sachlage, bei dem nur durch ein sofortiges Eingreifen eine drohende Gefahr oder ein Schaden abgewendet werden kann.

4 Aufbauorganisation

Das UBI-CERT ist ein zentrales Element des Informationssicherheitsmanagements der Universität Bielefeld. Die Dienstleistungen und Aufgabenfelder des UBI-CERT werden durch die Universitätsleitung in dieser Richtlinie festgelegt.

Die Mitglieder des UBI-CERT bestehen aus hauptamtlichem Personal und sind organisatorisch dem BITS zugeordnet. Das UBI-CERT ist eine eigenständige Organisationseinheit in der Abteilung ‚Netze und IT-Sicherheit' des BITS. Die personelle Sollausstattung hat den Umfang von vier Vollzeitäquivalenten. Die Wahrnehmung der im Abschnitt 5 beschriebenen Aufgaben muss dauerhaft gewährleistet sein, eine Umwidmung der Ressourcen muss mit der Universitätsleitung abgestimmt werden.

Das UBI-CERT kommuniziert im Rahmen seiner Aufgabenstellung direkt mit dem Informationssicherheitsbeauftragten (ISB), dem Informationssicherheitsmanagement (ISMS) und den involvierten Parteien.

Die Dienstleistungen des UBI-CERT sind nicht auf das BITS begrenzt, sondern stehen allen Fakultäten und Einrichtungen der Universität Bielefeld zur Verfügung.

5 Aufgaben des UBI-CERT

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. Dabei handelt sich um folgende Aufgabenfelder:

- Prävention
  Vorbeugende Maßnahmen treffen, so dass Sicherheitsprobleme nicht zu Informationssicherheitsvorfällen eskalieren.
- Detektion
  Aufbau von Fähigkeiten, um Informationssicherheitsvorfälle zeitnah zu identifizieren, um Gegenmaßnahmen zu ergreifen und dadurch negative Auswirkungen möglichst zu verhindern.
- Reaktion
  Vorbereitungen treffen, um nach dem Eintreten eines Informationssicherheitsvorfalls die Schadwirkung zu begrenzen. Übernahme der Koordination bei der Bearbeitung von Informationssicherheitsvorfällen.
- Nachhaltigkeit
  Aufbereitung der Erkenntnisse aus Informationssicherheitsvorfällen (‚Lessons Learned'), mit dem Ziel, zu einer kontinuierlichen Verbesserung des Informationssicherheitsmanagements beizutragen.
- Weitere Aufgaben
  Zu den weiteren Aufgaben des UBI-CERT gehört die Administration zentraler Sicherheitsdienste, um bei Gefahr in Verzug handlungsfähig zu sein.

5.1 Prävention

5.1.1 Schwachstellenmanagement

Alle Betreiber*innen von Informationstechnik an der Universität Bielefeld stehen in der Verantwortung, ihre IT-Systeme aktuell zu halten, die Ausnutzung von bekannten Schwachstellen zu unterbinden und kritische Sicherheitslücken an das UBI-CERT zu melden.

Das UBI-CERT unterstützt die Betreiber*innen von Informationstechnik bei der Identifizierung und Bewertung von technischen Schwachstellen in deren informationstechnischen Infrastrukturen.

Eine Voraussetzung für ein effizientes Management von Schwachstellen ist die Dokumentation der Informationstechnik, die bei den Betreiber*innen eingesetzt wird. Ohne eine vollständige

Datenbasis[1] ist eine Risikobewertung der Schwachstelle und eine Priorisierung der Maßnahmen im Rahmen des Patch- und Änderungsmanagements nicht bzw. nur unbefriedigend möglich.

Daher ist das UBI-CERT berechtigt, regelmäßige Schwachstellenscans an der Universität Bielefeld durchzuführen. Es handelt sich dabei um passive – nicht invasive – Schwachstellenscans, die identifizierten Sicherheitslücken werden dabei nicht ausgenutzt.

Das UBI-CERT bewertet den Schweregrad der identifizierten Schwachstellen auf Grundlage eines allgemein akzeptierten Standards (beispielsweise dem Common Vulnerability Scoring System - CVSS[2]) und informiert die Betreiber*innen von Informationstechnik über die Ergebnisse. Wenn der Schweregrad einer Schwachstelle als ‚kritisch' eingestuft wird, sind die Betreiber*innen von Informationstechnik verpflichtet, diese Schwachstellen zeitnah zu schließen oder Maßnahmen zur Risikominimierung zu ergreifen und das UBI-CERT über den Umsetzungsstand der Maßnahmen zu informieren.

5.1.2 Erfassung von Bedrohungen / Threat Intelligence

Als Threat Intelligence wird das strategische Sammeln von Informationen über potenzielle Bedrohungen, identifizierte Angriffsmerkmale und der handelnden Akteure (/Angreifer) verstanden und geht damit über die Anforderungen an das Schwachstellenmanagement hinaus.

Dazu werden üblicherweise externe Datenquellen für Informationssicherheit überwacht oder Mailinglisten/Newsfeeds abonniert und die Informationen ausgewertet, um festzustellen, ob es sich um eine relevante Bedrohung für die Universität Bielefeld handelt. Auf Grundlage der Einschätzung solcher Informationen werden die Erkenntnisse in Form von Warnungen oder Alarmierungen zielgerichtet verteilt.

Erkenntnisse über neue Bedrohungen oder aktuelle Angriffe werden auch innerhalb der Cybersecurity-Community (u.a. Deutscher CERT-Verbund, EDUCV[3]) untereinander ausgetauscht. Ebenso besteht die Möglichkeit Dienste zu nutzen, die von Cybersecurity-Community zur Verfügung gestellt werden (u.a. die ‚Malware Information Sharing Plattform' – MISP).

Das UBI-CERT bringt sich aktiv in den EDUCV ein, um in der Cybersecurity-Community sichtbar zu werden.

[1] Beispielsweise in Form einer Konfigurationsmanagementdatenbank (/Configuration-ManagementDataBase - CMDB).
[2] https://www.first.org/cvss
[3] https://www.educv.de/

5.2 Detektion

Das UBI-CERT betreibt für die Universität Bielefeld ein Security Information and Event Management System (SIEM). Mittels eines SIEM werden Logdaten zentral erfasst, korreliert und analysiert, um Sicherheitsprobleme zu erkennen. Dazu leiten alle Betreiber*innen von Informationstechnik relevante[4] Protokolldaten von ihren Logservern an das zentrale SIEM weiter.

Sollte es Gründe geben, die gegen eine zentrale Auswertung sprechen, sind die Betreiber*innen von Informationstechnik verpflichtet, die Protokolldaten in ihrem Verantwortungsbereich selbst auszuwerten und Informationssicherheitsvorfälle zu melden.

Das zentrale SIEM wertet die Daten automatisch aus und löst einen Alarm aus, wenn ein ungewöhnliches Verhalten oder schädliche Aktivitäten von einer Regel (UseCase) erkannt wurden. Ein UseCase kann beispielsweise für eine hohe Anzahl fehlgeschlagener Logins eingerichtet werden oder für spezifische Indicators of Compromise (IoC). Bei aktuellen IoCs ist mit einer hohen Wahrscheinlichkeit davon auszugehen, dass Aktivitäten eines Angreifers im Netzwerk der Universität Bielefeld identifiziert werden können.

Der Fokus der Tätigkeiten des UBI-CERT im Kontext Detektion liegt bei der Analyse der sicherheitsrelevanten Ereignisse und der Erstellung neuer ‚Use Cases', d.h. bei der Erstellung von Regeln, bei denen das SIEM einen Alarm auslöst.

5.3 Reaktion

5.3.1 Zentrale Kontaktstelle

Das UBI-CERT ist die zentrale Anlaufstelle für alle Fakultäten und Einrichtungen der Universität Bielefeld in Bezug auf Schwachstellen, sicherheitsrelevante Ereignisse und Informationssicherheitsvorfälle. Durch die Umsetzung einer zentralen Kontaktstelle - häufig auch als Single Point of Contact (SPOC) bezeichnet – wird sichergestellt, dass alle eingehenden Informationen und Anfragen zeitnah in einer definierten Vorgehensweise bearbeitet werden. Dies gilt auch für ausgehende Kommunikation, insbesondere wenn Dritte in einen Informationssicherheitsvorfall involviert sind oder bei einer Kooperation mit anderen Sicherheitsteams.

Eine Ausnahme ist die Kommunikation mit Strafverfolgungsbehörden; diese verläuft ausschließlich über das Justitiariat der Universität Bielefeld. Des Weiteren verfasst das UBI-CERT keine Meldungen für die Öffentlichkeit oder gibt Statements in irgendeiner Form ab.

[4] Art und Umfang der Protokollierung an der Universität Bielefeld wird in einer spezifischen Informationssicherheitsrichtlinie festgelegt.

Das UBI-CERT wird in das Krisenmanagement der Universität Bielefeld eingebunden (Ablauforganisation, Aufgaben im Krisenfall und Meldewege – EVALARM).

5.3.2 Behandlung von Informationssicherheitsvorfällen

Gegenstand des Managements von Informationssicherheitsvorfällen ist die Bewältigung der Auswirkungen eines Informationssicherheitsvorfalls. Ziel ist es, die Situation so zu managen, dass Verluste und Zerstörungen begrenzt, ausgenutzte Schwachstellen identifiziert und geschlossen werden, sowie Wiederherstellungszeit und -kosten zu minimieren. Das UBI-CERT orientiert sich an den vom DFN-CERT beschriebenen grundlegenden Schritten zur Bearbeitung von Informationssicherheitsvorfällen:

- Vorbereitung
- Entdeckung
- Analyse
- Eindämmung
- Kontrolle gewinnen / Wiederherstellung
- Nachbereitung

Die Reaktion auf einen Informationssicherheitsvorfall kann ein komplexes Unterfangen sein und erfordert qualifizierte Ressourcen zur Analyse der Vorfallmeldung, der Klassifizierung u. Priorisierung, technische Analysen, Umsetzung von Maßnahmen zur Schadensminimierung und -beseitigung und der Nacharbeit. Je nach Schwere eines Informationssicherheitsvorfalls ist eine Koordination der Aktionen aller Beteiligten erforderlich sowie die Kommunikation mit internen und ggf. externen Stellen.

Eine kooperative Zusammenarbeit des UBI-CERT mit den Betreibern von Informationstechnik an der Universität Bielefeld und eine sinnvolle Aufgabenverteilung zwischen allen Beteiligten ist eine Grundvoraussetzung, um die Auswirkungen von Informationssicherheitsvorfällen beherrschen zu können. Dazu bedarf es einer ausreichenden Vorbereitung und einer kontinuierlichen Verbesserung.

Das UBI-CERT erstellt dazu eine entsprechende Dokumentation (z.B. CERT-Handbuch), die beständig fortgeschrieben wird. Wichtige Themen sind:

- Kontaktlisten / Vernetzung
- Identifizierung und Bewertung von Informationsquellen
- Kommunikation und Meldewege
- Beschreibung und Weiterentwicklung der internen Prozesse zur Aufgabenbewältigung
- Checklisten
- Ausarbeitung von standardisierten Arbeitsprozeduren – Standard Operation Procedures (SOPs).

Darüber hinaus erstellt das UBI-CERT eine geeignete Außendarstellung des UBI-CERT zur Einbindung in die Cybersecurity-Community nach RFC 2350[5]. Diese formalisierte Kurzdarstellung eines CERT hat sich als quasi-Standard etabliert und ist geeignet, um sich einen schnellen Überblick über die Zielgruppe, Schnittstellen und Dienstleistungen eines CERT zu verschaffen.

5.4 Nachhaltigkeit

Informationssicherheitsvorfälle müssen durch das UBI-CERT hinreichend dokumentiert werden. Nach Abschluss der aktiven Vorfallbearbeitung übernimmt das UBI-CERT die Nachbereitung und führt in Abstimmung mit dem Datenschutz- und Informationssicherheitsmanagement (DISM) eine Ursachenanalyse und ggf. weitere Analysen durch.

5.4.1 Handlungsempfehlungen

Erkenntnisse, die bei der Bearbeitung von Informationssicherheitsvorfällen, der Behandlung von Schwachstellen oder sonstigen Aktivitäten des UBI-CERT gewonnen werden, sind in Abstimmung mit DISM für die entsprechende Zielgruppe aufzubereiten und in Form von Handlungsempfehlungen (Lessons Learned) weiterzugegeben. Wenn technische Aspekte im Vordergrund stehen, sind die Betreiber*innen von Informationstechnik die primäre Zielgruppe, in anderen Fällen ist der*die Adressat*in üblicherweise das Informationssicherheitsmanagement.

5.4.2 Berichtswesen und Lagebild

Neben den Handlungsempfehlungen erstellt das UBI-CERT vierteljährlich einen Tätigkeitsbericht für das Informationssicherheitsmanagement. Feste Bestandteile des Berichts sind:

- Einschätzung der Bedrohungssituation (Lagebild)
- Kennzahlen für die Kerndienstleistungen Prävention, Detektion und Reaktion, anhand derer der Fortschritt hinsichtlich wichtiger Zielsetzungen abgeleitet werden kann.
- Sonstige Aktivitäten und Ereignisse

Bei besonderen Lagen stellt das UBI-CERT auch ad-hoc Berichte nach Anforderung durch das Informationssicherheitsmanagement bereit.

5.5 Gefahrenintervention

Ursache für die Gefahrenintervention kann ein Cyberangriff sein, der zu einem Informationssicherheitsvorfall mit einem hohen oder kritischen Schadenspotential (u.a. Ransomware- oder APT -Angriff) führt. Aber auch von einem einzelnen kompromittierten IT-System kann eine große Gefahr für die Universität Bielefeld ausgehen. Ebenso muss bei

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

Missbrauchsfällen und eklatanten Verstößen gegen Richtlinien der Universität Bielefeld unverzüglich gehandelt werden.

Bei Gefahr im Verzug sind die Mitarbeiter des UBI-CERT bevollmächtigt, einzelne IT-Systeme, Netzanschlüsse oder Netzsegmente - notfalls auch ohne vorherige Benachrichtigung oder Rücksprache mit der verantwortliche Stelle - vorübergehend zu sperren bzw. zu isolieren, wenn dadurch ein gravierender Schaden für die Universität Bielefeld abgewendet werden kann.

Die verantwortliche Stelle, der ISB und das DISM sind über eine solchen Maßnahme unverzüglich zu informieren. Das weitere Vorgehen wird zwischen der verantwortlichen Stelle, dem ISB und dem DISM abgestimmt. Im Konfliktfall entscheidet die*der Vorsitzende des IT-Boards über das weitere Vorgehen.

Die Maßnahmen zur Gefahrenintervention sind auch ein adäquates Mittel zur Gefahrenvorbeugung. Ein solcher Sachverhalt liegt vor, wenn die Eskalation von einem Sicherheitsproblem zu einem Informationssicherheitsvorfall droht. Dies kann der Fall sein, wenn beispielsweise IT-Systeme betrieben werden, bei denen Betriebssystem und Anwendungssoftware nicht mehr supportet werden oder Schwachstellen mit einer hohen Kritikalität vorhanden sind. Wenn ein Sicherheitsproblem nicht innerhalb einer festgelegten Frist von der verantwortlichen Stelle behoben wird, greifen die Maßnahmen zur Gefahrenintervention.

5.6 Weitere Aufgaben

Um die Durchsetzung von Vorgaben des Informationssicherheitsmanagements zu unterstützen und die Fähigkeiten bei der Reaktion von Informationssicherheitsvorfällen und der Gefahrenabwehr zu sicherzustellen, obliegen die folgenden administrativen Aufgaben dem UBI-CERT.

- Zentrale Sicherheitsgateways
- Security Information and Event Management System (SIEM-System)
- Schwachstellenscanner und ggf. zusätzliche Sensorik

Darüber hinaus ist das UBI-CERT berechtigt, weitere Software oder Dienste zur Analyse von sicherheitsrelevanten Ereignissen und Informationssicherheitsvorfällen einzusetzen.

Das UBI-CERT muss über Freischaltungen an den zentralen Sicherheitsgateways informiert werden und hat ein Vetorecht, wenn eine Freischaltung nicht nachvollziehbar begründet ist oder sich Risiken daraus für die Universität Bielefeld ergeben können.

6 Verantwortlichkeiten

In der nachfolgenden Tabelle sind die Rollen und Verantwortlichkeiten nach der RASCI[6] Methode für die in dieser Richtlinie definierten Aufgabenfelder aufgeführt. Diese beziehen sich auf den Normalbetrieb. Je nach Schweregrad eines Informationssicherheitsvorfalls können sich die Verantwortlichkeiten verändern, beispielsweise wenn bei einem kritischen Informationssicherheitsvorfall der IT-Krisenstab einberufen wird (dazu Krisenmanagement Handbuch der Universität Bielefeld).

Aufgaben	**Universitätsleitung**	**UBI-CERT**	**IT-Betreiber*innen**	**ISB**	**DISM**	**IT-Krisenstab**	**Externe**
Bezug und Auswertung von Informationen zu Schwachstellen für relevante IT-Systeme	A	I	R				
Durchführung von Schwachstellenscans (Identifizierung von Sicherheitslücken und deren Bewertung)	A	R	S	I	I		
Einspielen von Patches / Umsetzung von Workarounds	A	(C)/I	R				
Threat Intelligence	A	R	I	I	I		S
Detektion	A	R	S	I	I		
Entgegennahme und Prüfung von Meldungen	A	R	S	I	(I)		(S)
Klassifikation und Priorisierung	A	R	C/I	I	I		
Analyse, Koordination und Dokumentation	A	R	C	I	I	(C/I)	(S)
Eindämmung / Kontrolle gewinnen / Wiederherstellung	A	S	R	I	I	(R,I)	(I)
Nachbereitung	A	R	I	I	I		
Tätigkeitsberichte erstellen	A	R	S	I	I		
Vorbereitung und kontinuierliche Verbesserung	A	R	S	I	I		

7 Mitgeltende Dokumente

- Informationssicherheitsleitlinie
- Richtlinien zum Datenschutz- und Informationssicherheitsmanagement

[6] RASCI ist ein Akronym für Responsible (R), Accountable (A), Support (S), Consulted (C) und Informiert (I) und beschreibt die Rollen und Verantwortlichkeiten in Prozessen.

- Basisschutzregelungen für Beschäftigte
- Informationssicherheitsrichtlinie zur Behandlung von Informationssicherheitsvorfällen
- Informationssicherheitsrichtlinie zur Protokollierung
- Krisenmanagement Handbuch der Universität Bielefeld

8 Abkürzungsverzeichnis

CERT ..... *Computer Emergency Response Team*
CVSS ..... *Common Vulnerability Scoring System*
DISM ..... *Datenschutz- und Informationssicherheitsmanagement*
EDUCV ..... *Educational CERT Verbund*
IoC ..... *Indicators of Compromise*
ISB ..... *Informationssicherheitsbeauftragter*
ISMS ..... *Informationssicherheitsmanagement*
SIEM ..... *Security Information and Event Management System*
SOPs ..... *Standard Operation Procedures*
SPOC ..... *Single Point of Contact*
UBI-CERT ..... *Computer Emergency Response Team der Universität Bielefeld*

9 Änderungsverzeichnis

Version (aktuelle oben)	**Datum**	**Änderungen**	**Bearbeitende**
1.0.0	19.01.2024	Finale Version	

