Digitalverbund Bayern

eduCSIRT

Security Incident Response für die bayerischen Hochschulen

Beschreibung gemäß RFC 2350

Zielsetzung dieses Dokuments

Dieses Dokument beinhaltet eine Beschreibung des eduCSIRT gemäß RFC 2350 und umfasst Kontaktdaten, den Kundenkreis und die angebotenen Dienste.

INHALT

1 DOKUMENTENINFORMATIONEN

1.1 FREIGABE UND VERÖFFENTLICHUNG

Diese Version des Dokuments wurde am 24.01.2025 durch den Steuerkreis HITS IS freigegeben und veröffentlicht.

1.2 VERTEILERLISTE FÜR BENACHRICHTIGUNGEN

Keine.

1.3 VERFÜGBARKEIT DIESES DOKUMENTS

Die aktuelle Version dieses Dokuments finden Sie auf dem offiziellen eduCSIRT-Webauftritt

https://eduCSIRT.bayern/rfc2350

1.4 AUTHENTIZITÄT DIESES DOKUMENTS

Dieses Dokument wurde mittels PGP vom eduCSIRT signiert. Den entsprechenden PGP-Schlüssel zur Überprüfung finden Sie auf dem offiziellen Webauftritt unter

https://eduCSIRT.bayern/contact

1.5 ÄNDERUNGSHISTORIE

Version	Datum	Änderung
1.0	24.01.2025	Initiale Version

Die aktuelle Version dieses Dokuments ist verfügbar unter https://eduCSIRT.bayern/rfc2350

2 KONTAKTINFORMATION

2.1 ALLGEMEINE INFORMATIONEN

Name des CSIRT	eduCSIRT
Gründungsdatum	11. März 2024
Adresse	eduCSIRT Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften Boltzmannstraße 1 85748 Garching bei München
Zeitzone	Europa/Berlin (UTC+01 und UTC+02 DST)
Telefonnummer	Nicht verfügbar
E-Mail	info@eduCSIRT.bayern
Webseite	https://eduCSIRT.bayern

2.2 ÖFFENTLICHE SCHLÜSSEL UND VERSCHLÜSSELUNG

PGP-Schlüssel	Siehe https://eduCSIRT.bayern/contact
S/MIME-Zertifikat	Siehe https://eduCSIRT.bayern/contact

2.3 MITGLIEDER

Diese Information ist öffentlich nicht verfügbar.

2.4 BETRIEBSZEITEN

Die regulären Geschäftszeiten des eduCSIRT sind von Montag bis Donnerstag von 9:00 bis 17:00 und Freitag von 9:00 bis 15:00 mitteleuropäischer Zeit [Ausnahme: gesetzliche bayerische Feiertage, sowie der 24.12. und 31.12.].

2.5 KUNDENKONTAKT

Im Notfall können Sie uns über das Webformular https://eduCSIRT.bayern/incident oder per E-Mail an incident@eduCSIRT.bayern kontaktieren.

Allgemeine Fragen können Sie an info@eduCSIRT.bayern richten.

3 SATZUNG

3.1 MISSION

Die Aufgabe des eduCSIRT ist es, die bayerischen staatlichen Hochschulen bei der Behandlung auftretender IT-Sicherheitsvorfälle zu unterstützen.

Die Liste der Kunden der bayerischen staatlichen Hochschulen wird vom Bayerischen Digitalverbund bereitgestellt (siehe https://digitalverbund.bayern/digitalverbund-bayern-2/mitglieder/)

3.2 ZUGEHÖRIGKEIT

Das eduCSIRT ist Teil des Hochschulübergreifenden IT-Service Informationssicherheit (HITS IS) zur Unterstützung der bayerischen Hochschulen.

3.3 FINANZIERUNG

Das eduCSIRT wird finanziert durch das Bayerische Staatsministerium für Wissenschaft und Kunst (StMWK) und die teilnehmenden Hochschulen.

3.4 VERANTWORTUNGSBEREICH

3.4.1 Kunden

Die Kunden des eduCSIRTs sind die bayerischen staatlichen Hochschulen des Digitalverbunds Bayern, sowie das Leibniz Rechenzentrum (LRZ) der Bayerischen Akademie der Wissenschaften.

3.4.2 Netze, Domänen und Autonome Systeme

Im Verantwortungsbereich des eduCSIRT liegen die Netze der bayerischen staatlichen Hochschulen.

4 Richtlinien

4.1 Arten von Vorfällen und Support Level

Im Rahmen des eduCSIRT werden alle IT-Sicherheitsvorfälle behandelt, die innerhalb des Kundenkreises auftreten oder drohen aufzutreten. Das Support Level hängt ab von der Art und Schwere des Vorfalls, der Anzahl an betroffenen Organisationen und der verfügbaren Ressourcen zum Zeitpunkt des Eintritts.

4.2 Reaktionszeit

In der Regel erfolgt unsere erste Antwort noch am selben Arbeitstag, wenn nicht, dann am nächsten Arbeitstag. Unsere Kontaktinformationen und Geschäftszeiten finden Sie in Kapitel 2.

4.3 Zusammenarbeit, Interaktion und Offenlegung von Informationen

Das eduCSIRT teilt Informationen mit anderen CSIRTs, sowie mit anderen betroffenen Parteien, wenn diese im Vorfall involviert sind. Alle Informationen über einen oder mehrere Vorfälle, die an andere Incident Response Teams weiter gegeben werden, einschließlich Details über Personen, Organisationen, IP-Adressen, Domain-Namen, sowie andere Informationen, die die Identität von Personen oder Organisationen offenbaren, werden anonymisiert, es sei denn, die betreffenden Personen oder Organisationen haben ausdrücklich etwas anderes angegeben. Zuständige Behörden, die im Rahmen ihrer gesetzlichen Befugnisse um Informationen bitten, erhalten die gewünschten Informationen im Rahmen der gesetzlichen Vorgaben unter Beachtung der verfassungs- und völkerrechtlichen Vorgaben.

4.4 Kommunikation und Authentifizierung

Das digitale Verschicken sensibler Daten erfolgt verschlüsselt, z.B. per verschlüsselter E-Mail mit S/MIME oder PGP. Informationen, welche in verschlüsselter Form erhalten werden, müssen auch langfristig verschlüsselt aufbewahrt werden. Das eduCSIRT verwendet für die Informationsklassifikation das Traffic Light Protocol.

4.5 Aufbewahrung und Löschung von Datensätzen

Personenbezogene Daten, die im Rahmen des Vorfalls gesammelt wurden, werden nach der Beendigung des Vorfalls gelöscht bzw. anonymisiert. Gesetzliche Aufbewahrungspflichten bleiben hiervon unberührt.

5 DIENSTE

Die Nutzung der Dienste des eduCSIRT ist den bayerischen Hochschulen des Digitalverbunds Bayern vorbehalten und erfordert die Teilnahme an einem Onboarding-Prozess.

5.1 REAKTIVE MASSNAHMEN BEI IT-SICHERHEITSVORFÄLLEN

Das eduCSIRT unterstützt die betroffenen Hochschulen bei der technischen und organisatorischen Bewältigung von IT-Sicherheitsvorfällen. Im Besonderen berät und unterstützt das eduCSIRT die bayerischen Hochschulen in Bezug auf die folgenden Aspekte des Vorfallsmanagements.

5.1.1 Ersteinschätzung

- Untersuchung, ob tatsächlich ein IT-Sicherheitsvorfall eingetreten ist
- Einschätzung der Schwere des IT-Sicherheitsvorfalls

5.1.2 Koordinierung

- Untersuchung der Ursache des IT-Sicherheitsvorfalls
- Kontakt mit anderen Einrichtungen herstellen, die betroffen sein könnten
- Berichte für CSIRTs der bayerischen Hochschulen bereitstellen, sowie anonymisiert für andere CSIRTs (IoCs)
- Behörden und staatliche Einrichtungen kontaktieren, falls anwendbar

5.1.3 Vorfallsbehandlung

- Unterstützung bei der Bereinigung von Systemen
- Beratung bei der Entfernung der Schwachstelle

Zusätzlich erhebt das eduCSIRT statistische Daten zu aufgetretenen IT-Sicherheitsvorfällen.

5.2 PROAKTIVE MASSNAHMEN

Zur Vorbereitung auf IT-Sicherheitsvorfälle bietet das eduCSIRT im Rahmen des Hochschulübergreifenden IT-Service Informationssicherheit (HITS IS) präventive Dienste an.

6 FORMULARE FÜR DIE MELDUNG VON VORFÄLLEN

Vorfälle können über die in Kapitel 2 definierten Kommunikationskanäle an das eduCSIRT gemeldet werden. Meldungen per E-Mail erfordern keine besondere Form. Die eduCSIRT Webseite enthält ein Formular für die Meldung von Vorfällen.

7 HAFTUNGSAUSSCHLÜSSE

Während bei der Erstellung von Informationen, Benachrichtigungen und Warnungen jede Vorsichtsmaßnahme getroffen wird, übernimmt das eduCSIRT keine Verantwortung für Fehler oder Auslassungen oder für Schäden, die sich aus der Verwendung der darin enthaltenen Informationen ergeben.