Friedrich-Alexander-Universität
Erlangen-Nürnberg

FAU

CISO Sprechstunde

03.12.2025

Agenda

Aktuelles aus der FAU & der Welt

NIS2 im Hochschulumfeld

ZERO-Day Lücken

Aktuelles aus der FAU

Aktuelles aus der FAU

20.11.2025 IT Krisenstabsübung

- Einweihung des neuen Krisenstabsraumes
- Erfolgreiche Zusammenarbeit
- Durch das gewählte Szenario entstand kurzzeitig das Gefühl einer „echten“ Krise

Informationssicherheitsrichtlinie

- Abstimmung mit Juristen aus Kanzlerbüro abgeschlossen
- Derzeit Austausch mit GPR

Aktuelles aus der FAU

Vermehrt Anfragen von Administrierenden aus den Lehrstühlen mit Bitte um Unterstützung

- Positive Entwicklung
- Konstruktive Zusammenarbeit

Beispielhafte aktuelle Bedrohungen und Angriffsszenarien

- Identitätsdiebstahl für Einkauf hochwertiger Technik
- Erpressungsversuche nach uraltem Typo3-Hack

Aktuelles aus der Welt

Hackerangriff auf Hochschule Mainz

24.11.2025
Cyberangriff auf Hochschule Mainz

IT-Systeme aus Sicherheitsgründen vollständig heruntergefahren
Die Hochschule Mainz ist nach aktueller Einschätzung Ziel eines Cyberangriffs geworden.
Aus Sicherheitsgründen wurden die IT-Systeme nach erstem Verdacht am Montag, 24. November 2025, kurzfristig und vollständig heruntergefahren. Die meisten Dienste der Hochschule sind aktuell daher nicht erreichbar. Die Lehre findet in Präsenz weiterhin statt.
Derzeit analysieren die IT-Services die Gefährdung und die möglichen entstandenen Schäden. Die Ermittlungsbehörden sind involviert. Aktuell sind keine Informationen zur Dauer der Beeinträchtigung möglich.
Der zügig eingesetzte Krisenstab arbeitet daran, Studierende und Beschäftigte der Hochschule Mainz arbeitsfähig zu halten.
Studierende und Beschäftigte werden fortlaufend über den Stand der Dinge über die Campus2Go-App und die zentralen Social Media-Kanäle Instagram und LinkedIn informiert.
Die Hochschulleitung der Hochschule Mainz

https://www.hs-mainz.de/news/cyberangriff-auf-hochschule-mainz/?back=1&cHash=435504c161a476e28729345dace589e2

NIS2 im Hochschulumfeld

„Network and Information Security Directive 2“

„Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der EU“

NIS2 im Hochschulumfeld

21. November 2025: Bundesrat hat Gesetz zum Umsetzung der NIS-2-Richtlinie beschlossen*

- Verpflichtung zu einheitlichen europäischen Sicherheitsstandards
- Strengere Sicherheitsanforderungen
- Umfangreiche Meldepflichten

- https://www.bundesregierung.de/breg-de/aktuelles/nis-2-richtlinie-deutschland-2373174

NIS2 im Hochschulumfeld

Hinweis vom HITS-IS, dass Hochschulen betroffen sein könnten.

Indikatoren für Betroffenheit von Hochschulen

- Betreiber kritischer digitaler Infrastrukturen
- Zentrale IT-Dienste, wie Rechenzentrum mit Cloud-, Identitäts- oder Netzdiensten für Dritte oder Hochleistungsrechner
- Forschungsdaten von nationalem / EU-Interesse

Konkrete Beispiele: Nähe von Flughäfen, Betreiben eigener Solaranlagen, Forschung im KRITIS-Umfeld

Mögliche Folgen für die FAU

Indikatoren für Betroffenheit von Hochschulen

- Informationssicherheits-Risikomanagement
- Incident-Response- und Meldeprozesse (z. B. 24-h-Meldung)
- Lieferantensicherheitsbewertung
- Schulung von Leitung & IT
- Nachweisbare Governance (Controlling, Dokumentation)

Verantwortung liegt ganz ausdrücklich bei der Universitätsleitung

Zero-Day Lücken

Zero-Day-Schwachstellen

BSI Vortag Video: https://www.youtube.com/watch?v=6DKvGl8HTfo

8 Zero-Day-Schwachstellen werden pro Tag durch das BSI behandelt

Zero-Day-Schwachstellen sind Sicherheitslücken in Software, Hardware oder Firmware, die dem Hersteller noch unbekannt sind

- d.h. es gibt also keinen offiziellen Patch, zum Zeitpunkt des Angriffs

Der Begriff „Zero Day“ bedeutet, dass Entwickler null Tage Vorlaufzeit hatten, um die Schwachstelle zu beheben.

Zero-Day-Schwachstellen

Was macht Zero-Day-Schwachstellen so gefährlich?

- Unentdeckt: Der Hersteller weiß noch nichts davon
- Kein Patch verfügbar
- Gezielte Angriffe: Oft für Spionage, Ransomware oder Sabotage genutzt
- Hoher Wert: Zero-Days werden auf dem Schwarzmarkt oder für staatliche Cyberangriffe gehandelt

Typische Ziele: Betriebssysteme, Browser, Office-Software, VPNs, IoT-Geräte.

Zero-Day-Schwachstellen

Wie werden Zero-Days ausgenutzt?

Angreifer nutzen unbekannte Schwachstellen z. B. durch:

- präparierte E-Mail-Anhänge
- manipulierte Webseiten (Drive-by-Downloads)
- kompromittierte Software-Updates
- Netzwerkangriffe auf Firewalls, VPNs oder Server

Zero-Day-Schwachstellen

Wie kann man sich gegen Zero-Day-Angriffe schützen?

Da es keinen Patch gibt, setzt man auf Risikominimierung & Erkennung:

1. **Systeme konsequent aktuell halten**
   Auch wenn Zero-Days unbekannt sind, schließen Updates vergleichbare bekannte Lücken und verhindern Eskalationen.
2. **Mehrschichtige Sicherheitsstrategie (Defense in Depth)**
   - Firewall + IDS/IPS
   - Endpoint-Protection (EDR/XDR)
   - Netzwerksegmentierung
   - Least-Privilege-Prinzip (Benutzer, Programme oder Systeme nur genau die Berechtigungen geben, die sie für ihre aktuelle Aufgabe unbedingt benötigen – und nicht mehr)

Zero-Day-Schwachstellen

3. Verhaltensbasierte Schutzsysteme

Statt nur Signaturen zu prüfen, erkennen sie auffälliges Verhalten, z. B.:

- unerwartete Speicherzugriffe
- ungewöhnliche Prozessketten
- verdächtige Netzwerkkommunikation

4. **Application Whitelisting**

Nur zugelassene Programme dürfen laufen – unbekannter Schadcode wird blockiert.

Zero-Day-Schwachstellen

4. Seriöse Sicherheitssoftware nutzen

Achte auf:

- Verhaltensschutz, nicht nur Virensignaturen
- Echtzeitschutz & Webschutz

Beispiel: integrierter Windows Defender ist gut, wenn aktuell

Zero-Day-Schwachstellen

5. Misstrauen bei E-Mails (Hauptangriffsweg!)

Nicht klicken, wenn:

- In der Mail Druck erzeugt wird („Sofort handeln!“)
- Dateianhänge unerwartet mitkommen
- Zahlungs- oder Login-Daten gefordert werden

Zero-Day + Phishing = häufige Kombination

Zero-Day-Schwachstellen

6. Warnzeichen erkennen

Sofort handeln, wenn:

- Lüfter laufen im Leerlauf
- Programme starten ohne Grund
- Browser öffnet sich selbst
- Unerwartete Passwort-Zurücksetzungen

➔ **Gerät offline nehmen, System prüfen (lassen)**

Friedrich-Alexander-Universität
Erlangen-Nürnberg

FAU

Vielen Dank
für Ihre Aufmerksamkeit