



CISO Sprechstunde

07.01.2026

Einen guten Start in's neues Jahr 2026

Schon die **Römer** feierten am 31. Dezember das Jahresende. Sie ehrten den Gott Janus, der mit zwei Gesichtern für Vergangenheit und Zukunft stand. 1582 legte die **Kirche** mit einem neuen Kalender fest: Der 31. Dezember wird für alle zum **offiziellen Jahresende**. Weil an diesem Tag auch Papst Silvester I. starb, nennen wir ihn heute „**Silvester**“.



Q: Wikipedia



Aktuelles aus der FAU



MFA:

- UL Entscheidung ist vorbereitet (SSO, VPN, Mail)
- Zugänge für Intersysteme werden folgen (SSH, RDP etc.)

NIS2 (Cybersicherheitsrichtlinie der Europäischen Union):

- „Betroffenheit“ der FAU oder deren Teilbereiche ist noch in Klärung
- Es gibt Argumente für eine Betroffenheit:
 - Drittmittel-Großprojekte
 - Industriekooperationen
 - zentrale IT-Infrastrukturen
 - HPC
 - Dienstleistungen für Dritte (Verbundprojekte, Exzellenzcluster, andere HS)
 - ≥ 50 Beschäftigte oder > 10 Mio. € Jahresbudget/Umsatz etc.

Kanzlermail (17.12.2025)

- ... **Meldepflicht bei Geräteverlust oder -diebstahl:** Wird ein dienstlich genutztes IT-Gerät (Laptop, Smartphone, Tablet, PC o.ä.) entwendet oder geht es verloren, ist dies unverzüglich an den [Chief Information Security Officer \(CISO\)](#) zu melden. Sind von dem Vorfall auch personenbezogene Daten betroffen (...), ist zusätzlich eine Meldung an den [Datenschutzbeauftragten \(DSB\)](#) erforderlich.
- **Verpflichtende Verschlüsselung von Datenträgern: Alle mobilen Endgeräte** (Laptops, Smartphones, Tablets), die FAU Daten verarbeiten, müssen mit einer vollständigen Verschlüsselung des Datenträger ausgestattet sein. Der Zugriff darf ausschließlich mit einer persönlichen PIN bzw. einem Passwort möglich sein. **Stationäre PCs** sind ebenfalls mit einer vollständigen Verschlüsselung der Datenträger und persönlicher PIN/Passwort abzusichern, sofern auf ihnen personenbezogene oder anderweitig schützenswerte FAU Daten verarbeitet werden.
- Details zur Verschlüsselung finden Sie unter <https://www.intern.fau.de/informationstechnik-it/regelungen/konzepte/verschluesselung-datentraeger/>.

Bitte beachten Sie, dass diese Vorgaben verbindlich und grundsätzlich sofort – jedoch spätestens bis zum 31.01.2026 - umzusetzen sind. Für Rückfragen stehen Ihnen CISO und DSB und für technische Unterstützung Ihre lokalen IT-Betreuungspersonen jederzeit zur Verfügung.

- Die Regelung wird noch in ein „amtliches Dokument“ überführt, vermutlich in die Informationssicherheits-Richtlinie.
- Gilt auch für den Wissenschaftsbereich.
- Technische Details zur Verschlüsselung finden sich unter <https://www.intern.fau.de/informationstechnik-it/regelungen/konzepte/verschluesselung-datentraeger/>
- 52 Verlustmeldungen in 2025

FAQ zur Verschlüsselung kommt in Kürze:

- Drucker
- Email Dienstkonto
- Rechner/Server im RRZE Serverraum
- Rechner in CIP-Pools
- Private Endgeräte etc.



Aktuelles aus der Welt



- Der Katalog der missbrauchten Schwachstellen der US-amerikanischen Cybersicherheitsbehörde CISA ist im Jahr 2025 um rund 20 Prozent angewachsen. Damit beschleunigte sich der Zuwachs.

Von den beobachteten Angriffen auf Schwachstellen nutzten Ransomware-Banden 24 der neu im Jahr 2025 aufgenommenen Lücken aus.
(Q: heise.de)



Q: cisa.gov

- Top 10 Ranking:

1. Microsoft (39)
2. Apple (9)
3. Cisco (8)
4. Fortinet (8)
5. Google Chromium (7)

6. Ivanti (7)
7. Linux-Kernel (7)
8. Citrix (5)
9. D-Link (5)
10. Oracle (5)
11. Sonicwall (5)

- Für Admins stellt der „Known Exploited Vulnerabilities“-Katalog der CISA (CVE) damit weiterhin eine wichtige Quelle für zügig zu patchende Schwachstellen dar: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
 - ➔ manueller Aufwand ist zu groß
 - ➔ Schwachstellen-Scanner der FAU für Internetsysteme prüft u.a. CVE automatisch
 - ➔ zur Client Installation wenden Sie sich bitte an soc@fau.de

Was können wir für Sie tun?



Ihre Fragen?

Ihre Wünsche?