CISO Sprechstunde

04.03.2026

Aktuelles aus der FAU

MFA:

- UL-Entscheidung pro MFA liegt vor.
- Zwei unabhängige MFA-Authentisierungspfade sind verpflichtend:
  - HW u. SW-Authenticator, oder
  - SW-Authenticator auf zwei Endgeräten (z.B. Laptop und Smartphone).
- Zielgruppen gerechter Projektplan zur Umsetzung wird durch RRZE entwickelt.

CISO/SOC Newsletter und Matrix-Chat

Newsletter

Wir planen einen abonnierbaren Newsletter **News und Tipps zur Cybersicherheit** zur zeitnahen Information für alle Systembetreuende.

Über diesen Kanal sollen wichtige Informationen zu kritischen Schwachstellen, aktuellen Sicherheitsvorfällen etc. geteilt werden.

Abonnierbar über https://www.idm.fau.de/go/mail/subscriptions

Matrix-Chat

Zusätzlich gibt es einen Matrix-Chat: https://chat.fau.de/#/room/#infosec:fau.de

Von den IS-relevanten veröffentlichten Regelungen an der FAU sind ca. 2/3 älter als 6 Jahre, ohne angepasst worden zu sein. Seit 2020 hat sich die IT-Umgebung jedoch stark geändert.

Bereich	2020	2026
Arbeitsumgebung	Bürozentriert, on-prem, wenig Home-Office	Vielfach digitaler, Hybrid-Standard, Cloud/SaaS-Abhängigkeit
Netzwerksicherheit	VPNs, Perimeter-/Gateway-Security	Zero Trust, Identitäts-/Gerätekontrolle
Angriffsflächen	Phishing, einfache Ransomware	KI-gestütztes Phishing, Supply-Chain, Cloud-Konten, IoT
Ransomware & KI	Manuelle Verschlüsselung	KI-gestützt, Daten-Exfiltration

Kanzlermail zur Verschlüsselung

FAQ zum besseren Verständnis der geforderten Verschlüsselung in speziellen Situationen werden in Kürze unter
https://www.intern.fau.de/informationstechnik-it/regelungen/konzepte/verschluesselung-datentraeger/
veröffentlicht.

Gibt es zu dem Thema Fragen?

Als Hilfestellung wird ein **Handbuch zur Informationssicherheit** für Departments und Lehrstühle entstehen.

Eine auf die unterschiedlichen Situationen angepasste Handreichung und Orientierungshilfe.

Aktuelles aus der Welt

Android

ALERT

Patchday: Attacken auf Android-Smartphones beobachtet

vor 2 Stunden | heise Security

https://www.heise.de/news/Patchday-Attacken-auf-Android-Smartphones-beobachtet-11196456.html

Google Android: Mehrere Schwachstellen

CVSS Base Score	CVSS Temporal Score	Meldung	Datum	Stand
9.8 (kritisch)	9.4 (kritisch)	LSI-SEC-2026-0569	03.03.2026	03.03.2026

Betroffene Systeme

Betriebssystem

- Android

Software

03.03.2026

- Google Android 14 <2026-03-01
- Google Android 15 <2026-03-01
- Google Android 16-qpr2 <2026-03-01
- Google Android 16 <2026-03-01
- Google Android <2026-03-05

Produktbeschreibung

Das Android Betriebssystem ist eine quelloffene Plattform für mobile Geräte. Die Basis bildet der Linux-Kernel.

Angriff

Angriff

Ein Angreifer kann mehrere Schwachstellen in Google Android ausnutzen, um sich erweiterte Berechtigungen zu verschaffen, beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen oder andere nicht näher spezifizierte Angriffe durchzuführen.

6G Mobilfunk ein Radarsystem?

heise.de

6G als riesiges Radarsystem: ETSI* sieht Gefahren für Privatsphäre und Sicherheit

6G-Funk soll auch die Umgebung **aktiv ausleuchten**. ETSI warnt vor Gefahren für Sicherheit und Privatsphäre durch dieses „Sensing“.

Paradigmenwechsel mit 6G: Mit „**Integrated Sensing and Communications**“ (**ISAC**) soll das Mobilfunknetz der nächsten Generation zu einer Art riesigem Radarsystem machen.

6G soll Funkreflexionen nutzen, um Objekte, Entfernungen, Geschwindigkeiten und menschliche Bewegungen in Echtzeit zu erfassen. Bringt **Vorteile** für „autonomes Fahren“ oder die industrielle Automatisierung.

Brisant ist vor allem das „unbefugte Sensing“: Kriminelle könnten 6G-Signale missbrauchen, um z.B. ohne Erlaubnis Karten von Gebäuden zu erstellen oder die Position von Personen zu tracken.

Da ISAC-Signale oft auch Kommunikationsdaten enthalten, besteht zudem die Gefahr, abgehört zu werden: Ein Zielobjekt könnte quasi als Empfänger fungieren und vertrauliche Informationen aus den Radarsignalen abgreifen.

Es soll darum gehen, das Vertrauen in 6G von vornherein durch ein „**Security by Design**“-Konzept zu verankern.

*EU-Telekommunikationsnormungsbehörde

Zero-Days verkauft

Hauptsitz in Melbourne

Einer der größten Verteidigungsauftragnehmer der USA

Manager bei Rüstungskonzern: 87 Monate Gefängnis für den Verkauf von Zero-Days

Der Rüstungskonzern L3Harris sammelt auch Zero-Day-Exploits für ausgewählte Regierungen. Ein Manager hat solche an einen Russen verkauft und muss nun in Haft.

25.02.2026 14:33 Uhr 14 | heise online

Das Ende für RSA und ECC naht 2032

BSI

Neue Verschlüsselungs-Empfehlungen des BSI: Das Ende für RSA und ECC naht

Das Bundesamt fordert, klassische asymmetrische Verschlüsselungsverfahren ab 2032 nur noch in Kombination mit Post-Quanten-Kryptographie einzusetzen.

11.02.2026 13:14 Uhr 74 | heise Security

Was können wir für Sie tun?

Ihre Fragen?

Ihre Wünsche?