CISO Sprechstunde

04.02.2026

Aktuelles aus der FAU

MFA:

- UL Entscheidung ist eingereicht (SSO, VPN, Mail)
- Finanzierung des zus. Betreuungsaufwandes im RRZE scheint gesichert
- Zwei unabhängige MFA-Authentisierungspfade werden verpflichtend:
  - HW u. SW-Authenticator oder
  - SW-Authenticator auf zwei Endgeräten (z.B. Laptop und Smartphone)

Beachten Sie: Zentrales Key-Management wird sehr aufwändig … ist aktuell nicht vorgesehen

MFA

Ebenso für Zugänge unserer Internetsysteme (SSH, RDP, X-Win etc.)

KI und SW-Entwicklungs-Tools bringen zunehmend SSH-Zugänge mit (= neue Einfallstore)

Bitte sichern Sie diese verlässlich ab!

1) Passwort-Login deaktivieren → nur noch mit SSH-Keys und sicherer mit 2FA/YubiKey
2) Root-Login nur mit 2FA/YubiKey
3) SSH nur für bestimmte Benutzer erlauben
4) Fail2ban aktivieren (gegen Bruteforce Angriffe)
5) Firewall: SSH nur für ausgewählte IP Adressen
6) Port ändern (optional, hilft ein wenig gegen „Scanner“)
7) Sichere SSH-Einstellungen

- Informieren Sie sich regelmäßig über aktuelle Schwachstellen Ihrer Systeme!!!

Meldepflicht bei Geräteverlust/Diebstahl & Newsletter

Meldepflicht bei Geräteverlust oder –diebstahl

Es wird in Kürze ein Webformular für Verlustmeldungen geben (zentrale Anlaufstelle).
Je nach Szenario werden die relevanten Stellen im Haus per Mail aus dem Web-Formular entsprechend informiert.

Newsletter

Wir planen einen abonnierbaren Newsletter zur zeitnahen Information für alle Systembetreuende.

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

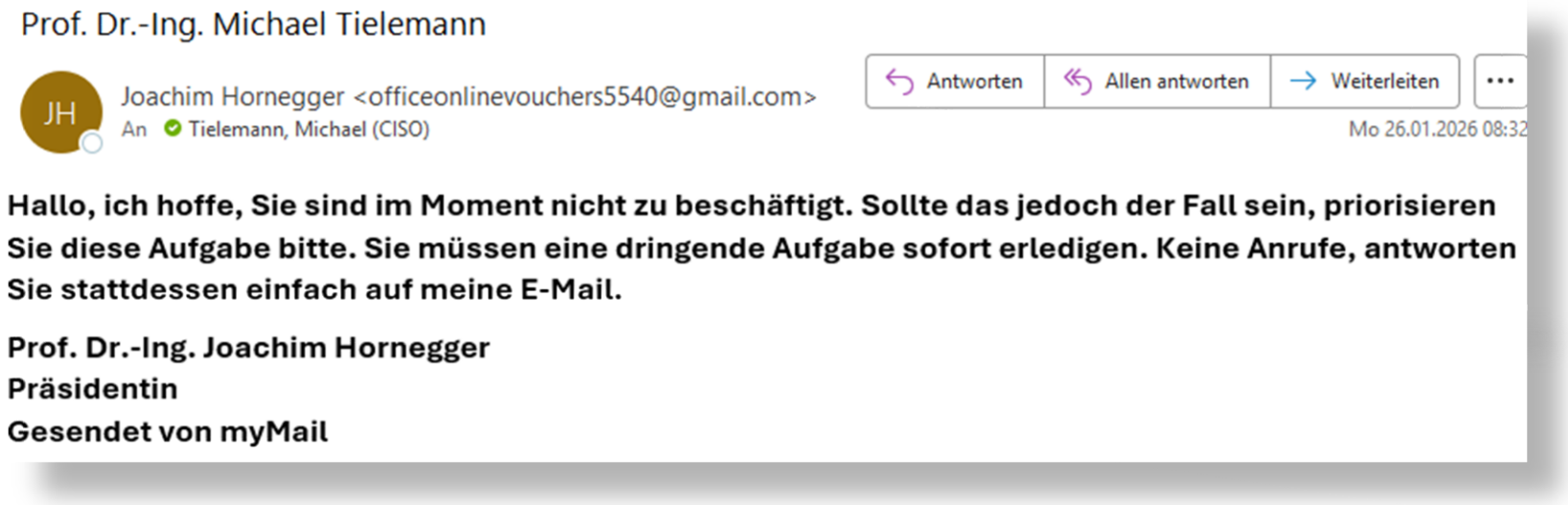
Alternativ wäre auch ein Messanger wie Matrix oder Zoom vorstellbar.

CIO-Fraud

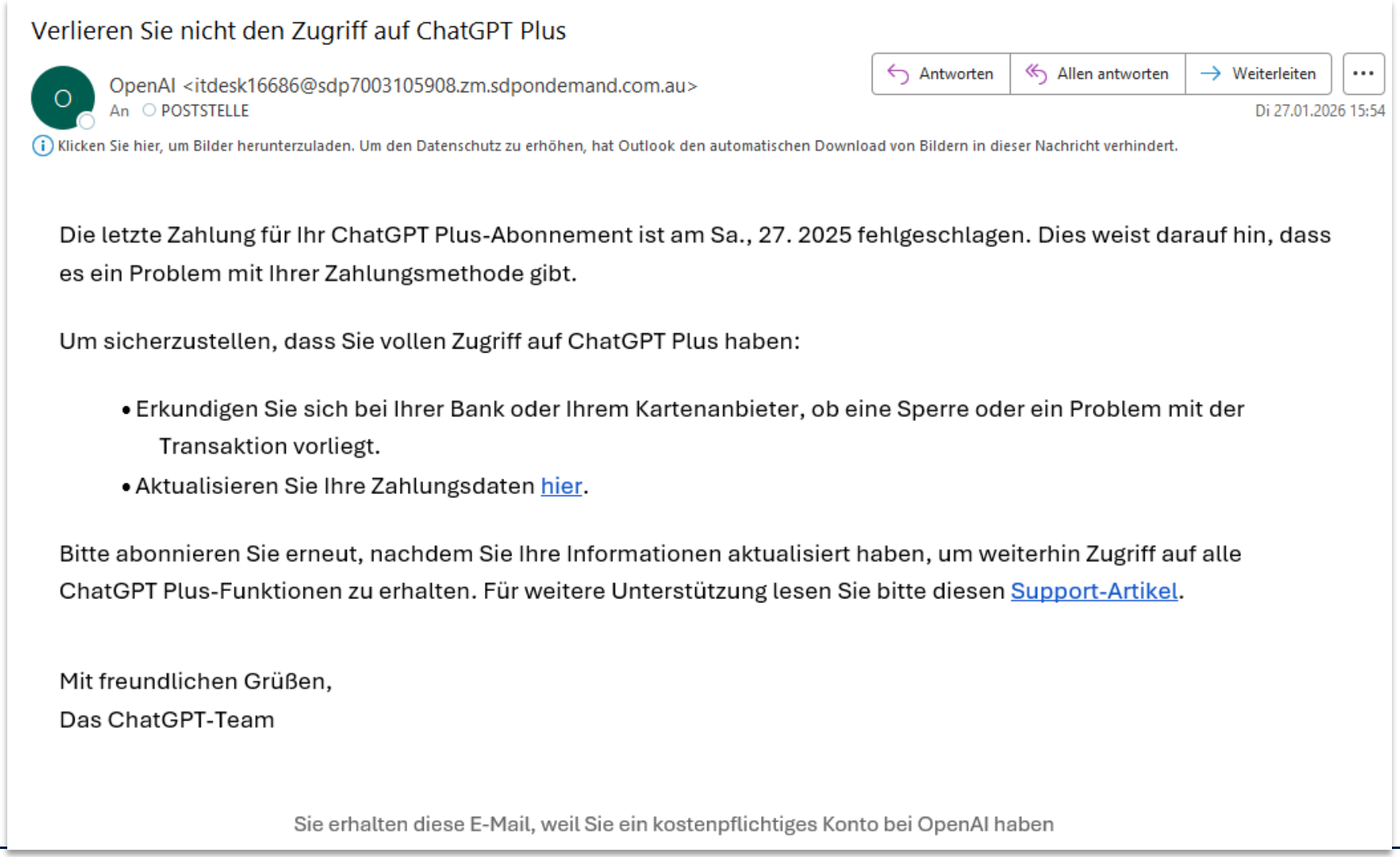
Aktueller Fall mit CIO-Fraud Angriff:

CIO-Fraud ist eine Form von Betrug durch Social Engineering:
Kriminelle geben sich z. B. als CIO/CEO/Geschäftsführung oder IT-Leitung aus und bringen Mitarbeitende dazu, Geld zu überweisen, Zugangsdaten herauszugeben oder sicherheitskritische Aktionen auszuführen.

Kaufen Sie bitte niemals Amazon-Gutscheine im FAU-Auftrag



Phishing



Verlieren Sie nicht den Zugriff auf ChatGPT Plus

O

OpenAI <itdesk16686@sdp7003105908.zm.sdpondemand.com.au>
An POSTSTELLE

Antworten | Allen antworten | Weiterleiten | ...

Di 27.01.2026 15:54

Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den automatischen Download von Bildern in dieser Nachricht verhindert.

Die letzte Zahlung für Ihr ChatGPT Plus-Abonnement ist am Sa., 27. 2025 fehlgeschlagen. Dies weist darauf hin, dass es ein Problem mit Ihrer Zahlungsmethode gibt.

Um sicherzustellen, dass Sie vollen Zugriff auf ChatGPT Plus haben:

- Erkundigen Sie sich bei Ihrer Bank oder Ihrem Kartenanbieter, ob eine Sperre oder ein Problem mit der Transaktion vorliegt.
- Aktualisieren Sie Ihre Zahlungsdaten hier.

Bitte abonnieren Sie erneut, nachdem Sie Ihre Informationen aktualisiert haben, um weiterhin Zugriff auf alle ChatGPT Plus-Funktionen zu erhalten. Für weitere Unterstützung lesen Sie bitte diesen Support-Artikel.

Mit freundlichen Grüßen,
Das ChatGPT-Team

Sie erhalten diese E-Mail, weil Sie ein kostenpflichtiges Konto bei OpenAI haben

Risikomanagement

SOC

Bild: ChatGPT

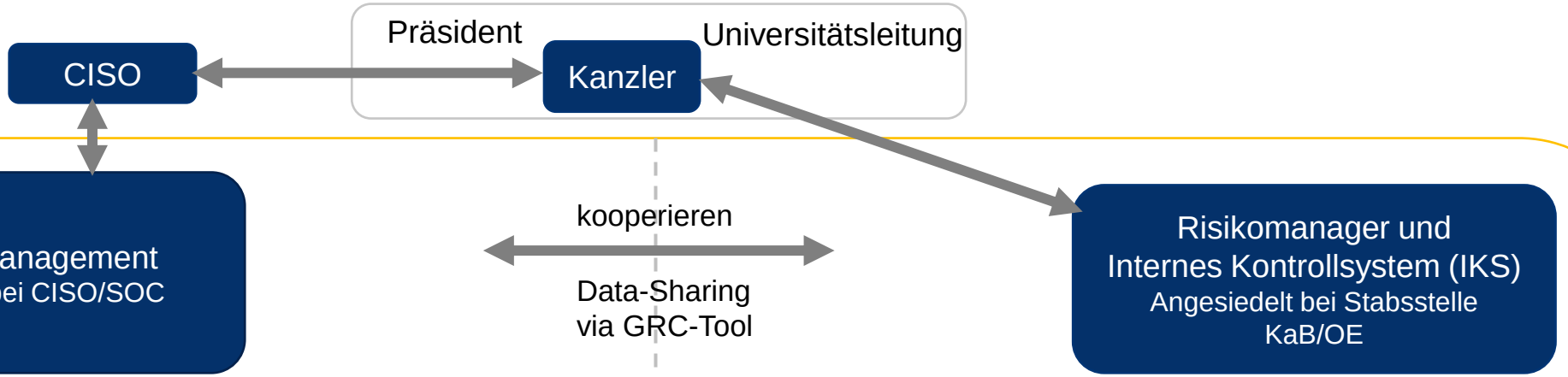
Rahmenbedingungen

Notwendigkeit von Risikomanagement

Rahmenvereinbarung Hochschulen 2023 – 2027	Hochschulvertrag 2023 – 2027
Digitale Transformation, Digitalisierung in Wissenschaft, Lehre und Verwaltung *„Zentrale Bedeutung hat die Gewährleistung eines hohen Niveaus von IT-Sicherheit und -Resilienz. Insbesondere richten die Hochschulen ein internes Informationssicherheitsmanagementsystem (ISMS) […] ein… (S. 26)“*	**Qualitätssicherung in Forschung, Lehre und Verwaltung** *„Die FAU strebt an, die internen und externen Chancen und Risiken für die künftigen Haushalte der FAU im Rahmen eines Chancen- und Risikomanagements systematisch zu kontrollieren und zu bewerten, mit dem Ziel, frühzeitig Entwicklungen zu erkennen, die den Erfolg der FAU fördern oder deren Fortbestand gefährden.* *Neben der Risikoidentifikation und -analyse stehen die Prozessschritte Risikobehandlung und -kontrolle sowie quantitative Forecasting-Methoden zur Sicherstellung eines transparenten und passgenauen Ressourceneinsatzes im Focus.“ (S. 23)*
	Digitale Transformation, Digitalisierung in Wissenschaft, Lehre und Verwaltung *„Das durch die Stabsstelle IT-Sicherheit entwickelte Hochschul-Informationssicherheitsprogramms (HISP) wird Rahmen des Digitalverbundes hochschulintern entlang der definierten Aufgabenfelder bis zum Ende der Laufzeit der Rahmenvereinbarung fortgeführt.“ (S. 18)*

Gesamt-Risikomanagement-Organisation

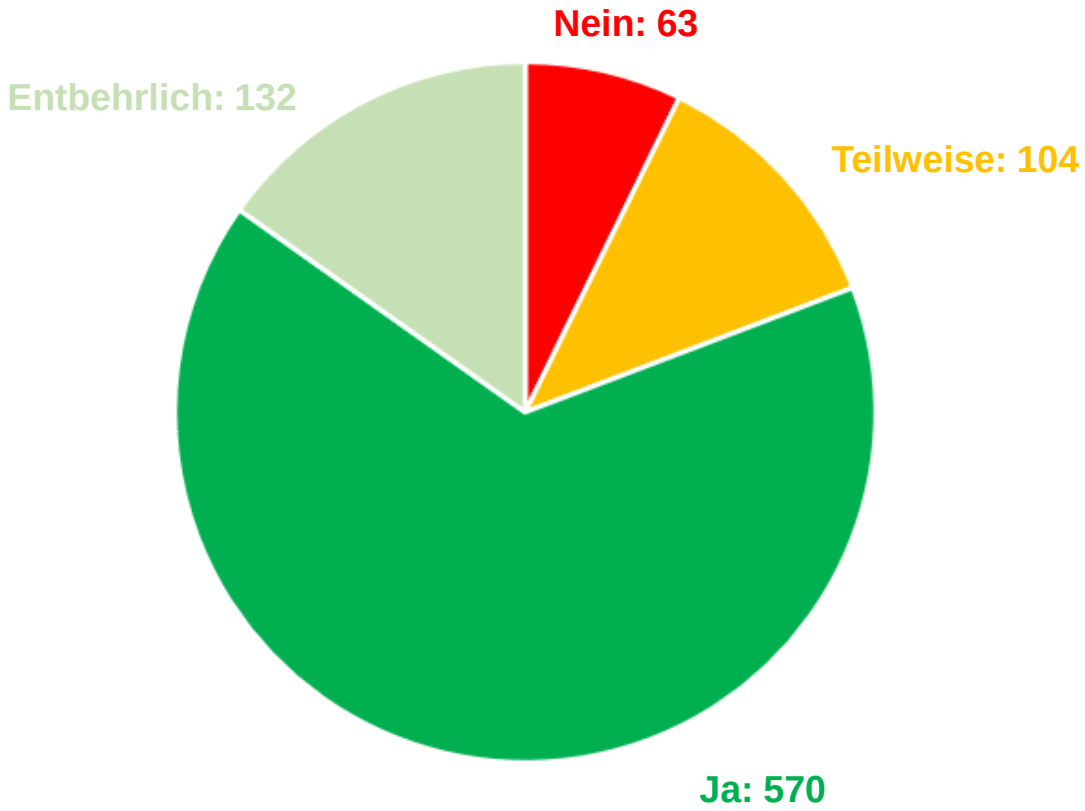
Zusammenarbeit mit dem allgemeinen Risikomanagement



	IS-Risikomanagement (nach BSI-Standards)	**Zentrales Risikomanagement (nach IDW PS 981)**
Zielsetzung	Schutz der Informationssicherheit (Verfügbarkeit, Vertraulichkeit, Integrität)	Erreichung der Organisationsziele durch frühzeitige und systematische Identifikation, Bewertung und Steuerung von Risiken.
Einbettung	Informationssicherheits-Managementsystem (ISMS)	Bestandteil des Governance- und Steuerungssystems
Risiken	Informationssicherheits-Risiken	Alle Risiken (strategisch, operativ, rechtlich, finanziell, personell & IT/IS-Risiken)
Nutzen	Informationssicherheit, Resilienz, Schutz vor Cyberangriffen	Risikoorientierte Steuerung, Transparenz, Schadenabwehr & Chancennutzung

Wie viele BSI-Anforderungen sind umgesetzt?

Status der bisher erfassten RRZE-Gruppen



SUMME bewerteter Anforderungen: 869

Umsetzungsstand

Informationssicherheits-Risikomanagement nach BSI

Status bis	Maßnahmen	Status
Dez. 2025	**IS-Leitlinie** und **IS-Richtlinie** eingereicht, aber noch nicht freigegeben. Weitere ISMS-Dokumente vorbereitet, wie z.B. eine IS-RM-Richtlinie.	🟡 in Bearbeitung
	Strukturvorerfassung des RRZE durch das IS-Risikomanagement-Team	✅ abgeschlossen
	Erste Strukturerfassungen und Kontrollassessments mit Asset Owner nach BSI IT-Grundschutz (u.a. ca. ¼ des RRZE sowie eines Pilot-Lehrstuhls)	✅ abgeschlossen
	Netzplan ZUV erstellt	✅ abgeschlossen
	„Internes“ Audit des RRZE abgeschlossen (mit HITS IS)	✅ abgeschlossen
	ISMS-Dokumentenmanagement-System aufgebaut	✅ abgeschlossen
Dez. 2027	Strukturerfassung und Kontrollassessments des restlichen RRZE (¾)	🟡 in Bearbeitung
	Zusammenführung der ZUV-Erfassung nach IDW mit dem IS-Risikomanagement, sowie Erfassung weiterer Bereiche	🟡 in Bearbeitung
	Einführung von Bereichs-ISBs an der gesamten FAU	⬜ in Planung

BSI IT-Grundschutz

Download-Adressen zum BSI Grundschutz

Übersicht:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

BSI-Standards:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html

ISB und ISMS

Mit Blick auf die anstehende InfoSec Richtlinie (IS-R) werden ISB-Schulungen vorbereitet und nach Verabschiedung angeboten.

Nach der Schulung sollte ein ISB:

- Risiken strukturiert bewerten und dokumentieren können
- Sicherheitsmaßnahmen priorisieren und nachhalten können
- Maßnahmen, Vorfälle steuern und Eskalationen auslösen können
- In einem übergeordneten ISMS organisatorisch sauber agieren können
- auditsicher dokumentieren können

Aktuelles aus der Welt

Schwachstellen 2026

heise.de

Alert!

OpenSSL: 12 Sicherheitslecks, eines erlaubt Schadcodeausführung und ist kritisch

In OpenSSL wurden 12 Sicherheitslücken entdeckt – mit KI-Tools. Eine davon gilt als kritisch. Aktualisierte Software steht bereit.

> In der quelloffenen Verschlüsselungsbibliothek OpenSSL haben IT-Forscher 12 Sicherheitslücken entdeckt, eine davon gilt als kritisch. Angreifer können dadurch etwa Schadcode einschleusen. Bemerkenswert ist auch, dass die IT-Sicherheitsforscher die Schwachstellen mit KI-Systemen aufgespürt haben.

Q: cisa.gov

Was können wir für Sie tun?

Ihre Fragen?

Ihre Wünsche?