CISO Sprechstunde

02.07.2025

Aktuelles aus der FAU

Aktuelles

News

1. Die **Dienstvereinbarung** zum SIEM/IDS/IPS wurde durch GPR und Datenschutz genehmigt.
   Nach über drei Jahren kann es nun mit dem Betrieb eines SIEM losgehen

2. Die Erstellung der **Informationssicherheitsrichtlinie** (IS-R) mit KB ist nahezu abgeschlossen
   - Benennung von ISB an allen Einrichtungen

3. **Phishing** Proof of Concept startet am 01.07 und läuft bis 31.07. mit freiwilligen Teilnehmern
   - Weitere Freiwillige sind herzlich willkommen

4. Uni Würzburg hat **2FA** flächendeckend eingeführt.
   2FA-Planungen für die FAU werden aufgenommen

Lehrstuhl IT: Windows-Defender auf älteren PCs machte Schwierigkeiten

Untersuchung von Daten-Archive mit mehreren Virenscannern zeigte zahlreiche Malware-Funde, zum Teil sehr alte Versionen.

Quellen dafür waren

- Chip-Installer
- FAUbox-Verzeichnisse (xxx.pdf.exe, xxx.doc)
- Treiber-Software von kompromittierten Herstellerseiten

Unsere Empfehlungen

- Keine Downloads von chip.de
- Beim Austausch von Dateien mit anderen Hochschulen Sicherheitsstufe einbauen (Virenscanner)
- Immer auch mal die Archive scannen
- Wir unterstützen gerne bei Analysen, aber auch bei der Konzeptentwicklung an Lehrstühlen

Aktuelles

Betrug

Antworten | Allen antworten | Weiterleiten | Archivieren | Junk | Löschen | Mehr

Von [redacted]

An

30.06.2025, 04:05

Betreff **Vorübergehende Aktualisierung unserer Bankverbindung – FAU-Stipendium (Ukraine)**

Sehr geehrter [redacted]

zunächst möchte ich mich für die kurzfristige Kontaktaufnahme an diesem Morgen entschuldigen.

Unser Finanzdienst hat uns soeben darüber informiert, dass es aufgrund von **vorübergehenden Einschränkungen auf dem Konto**, das wir Ihnen in unserer E-Mail vom **06. Juni 2025** mitgeteilt hatten, zu einer **temporären Aktualisierung unserer Bankverbindung** gekommen ist.

Wir bitten Sie daher, für die Überweisung der Spende **ausschließlich die nachfolgend angegebenen Kontodaten** zu verwenden:

- **Kontoinhaber**: M.A. Perez Gimeno – Friedrich-Alexander-Universität Erlangen-Nürnberg
- **IBAN**: DE53 3701 9000 1011 1337 48
- **BIC**: BUNQDE82
- **Verwendungszweck**: BKZ 417005813370, FAU Scholarship (Ukraine)

Für die Aktualisierung unserer Buchhaltung bitten wir Sie höflich, uns **nach erfolgter Überweisung eine Kopie der Zahlungsbestätigung** zukommen zu lassen.

Wir danken Ihnen nochmals herzlich für Ihre wertvolle Unterstützung unserer Studierenden.

Mit freundlichen Grüßen

[redacted]

tionale Forschungsbeziehungen und Innovationsstrategie
en-Nürnberg (FAU)

Polizeianzeige von 2 Betrugsversuchen in 10 Tagen

LSI warnt ebenfalls vor Betrugsfällen

Friedrich-Alexander-Universität
Erlangen-Nürnberg

FAU

Vortrag in der UL

Willkommen

- IT-Krise
- IT-Krisenstäbe
- Vom Chaos zum Normalbetrieb
- Status und To-dos

IT-Krisenstab

Vorfallsarten

Vorfallsart	Erläuterung	Behandlung
Einfache Störung Incident	Kurzzeitiger Ausfall von Prozessen oder Ressourcen mit nur geringem Schaden	Behandlung ist Teil der üblichen Störungsbehebung
Notfall Major Incident	Länger andauernder Ausfall von Prozessen oder Ressourcen mit hohem oder sehr hohem Schaden	Behandlung verlangt besondere Notfallorganisation
Krise	Auf Institution **begrenzter verschärfter Notfall**, der die **Existenz** der Institution **bedroht** oder die Gesundheit oder das Leben von Personen beeinträchtigt	Da Krisen **nicht breitflächig die Umgebung oder das öffentliche Leben beeinträchtigen**, können sie, zumindest größtenteils, innerhalb der Institution selbst behoben werden
Katastrophe	Räumlich und zeitlich nicht begrenztes Großschadensereignis, zum Beispiel als Folge von Überschwemmungen oder Erdbeben	Aus Sicht einer Institution stellt sich eine Katastrophe als Krise dar und wird intern durch deren Notfallorganisation in Zusammenarbeit mit den externen Hilfsorganisationen bewältigt

IT-Krisenstab

Mitglieder

CIO

CISO

CIO-Office

Datenschutz

Jurist

Kanzler

Präsident

Pressestelle

RRZE-Leitung

jeweils mit Vertretung

Aufgaben des IT-Krisenstabs

Aufgaben

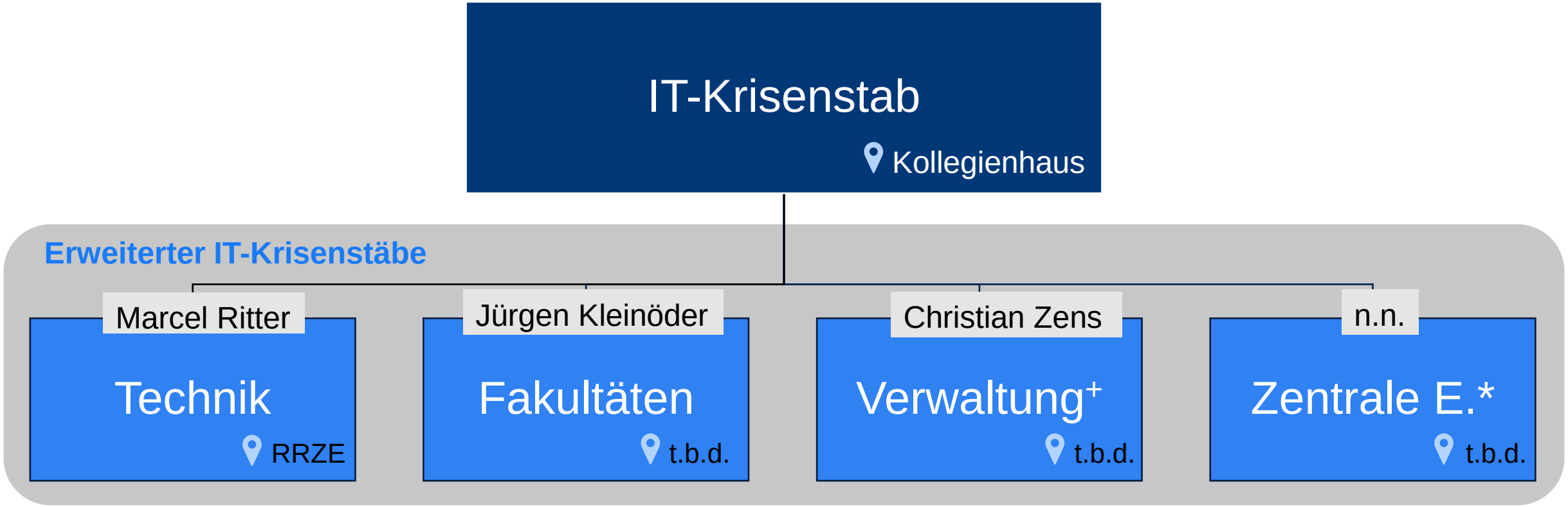
… trifft Entscheidungen zur Deeskalation die Krise bis zur Wiederherstellung der Normallage

… gibt Anweisungen an die Notfallteams und überwacht die Lage

… stellt die interne wie auch externe Krisenkommunikation sicher

Erweiterte IT-Krisenstäbe

Ausgangslage: IT-Krisenstab und erweiterte IT-Krisenstäbe



\+ Verwaltung und VPs
* Universitätsbibliothek, Sprachenzentrum, Studentenwerk

IT-Krisenstab

Initiierte und offene Punkte

Notfalldokumente und –pläne

Checklisten

Jährliche Krisenübung

Risikomanagement

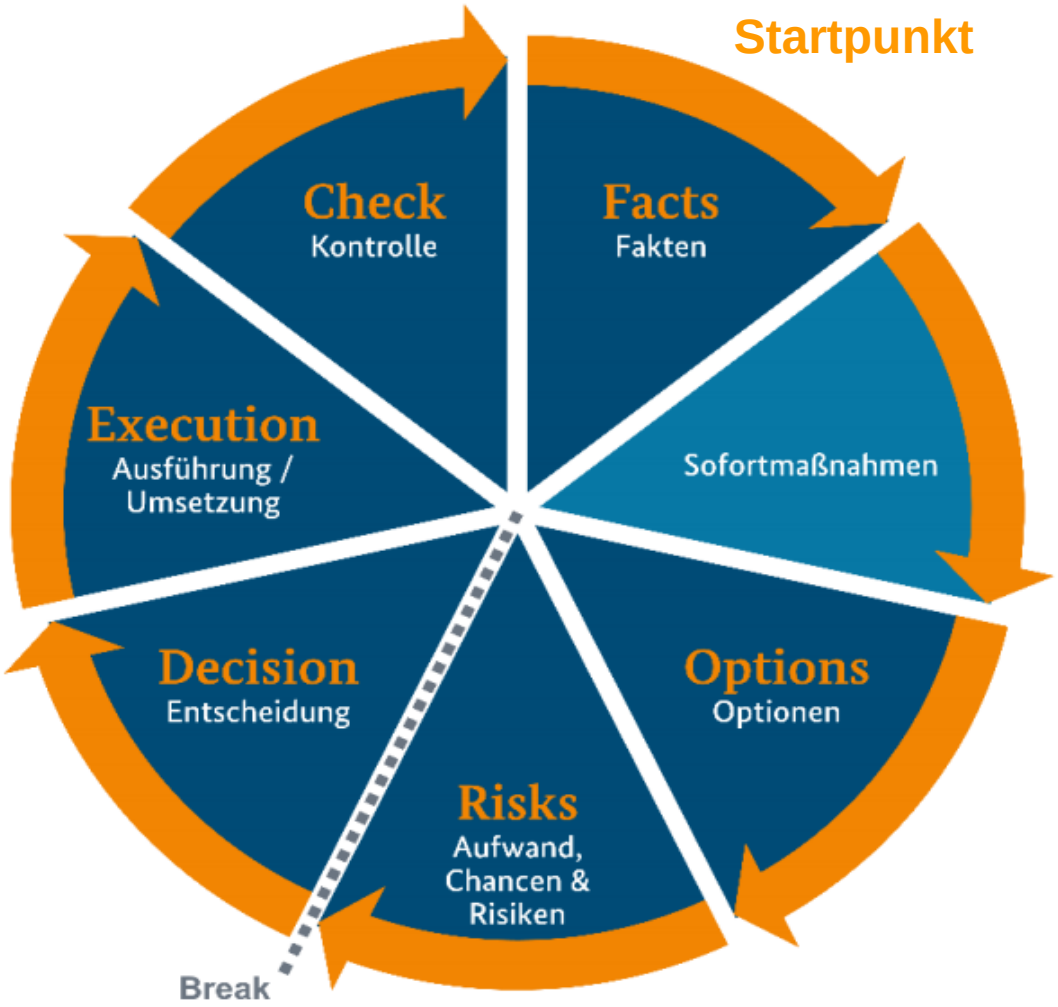
Business Continuity Management

Verbesserung der Resilienz durch techn. und org. Maßnahmen

IT-Krisenstab

Entscheidungsfindung: FOR-DEC

Struktur statt Chaos:
Eine Methode zur
Entscheidungsfindung



Erweiterte IT-Krisenstäbe

To Do

Empfehlung für erweiterte IT-Krisenstäbe (FAK, ZUV, RRZE, ZE)

1. Entwickeln Sie Risiko- und Krisenbilder für Ihren Bereich

2. Identifizieren Sie spez. Herausforderungen in der Krise

3. Was kann vorbereitet werden?
   Kommunikationswege, Kontaktlisten, Notbetrieb, Wiederanlauf etc.

Notfall Handbuch V. 1.0 (momentan noch vertraulich)

- Ist erstellt und wird weiterentwickelt
- Separate Workshops geplant
- Interne Version für alle wird kommen

Aktuelles aus der Welt

Aktuelle Meldungen

Apple, Facebook, Google

16 Milliarden gestohlene Anmeldedaten entdeckt

20.06.2025, 11:16 Uhr

Man darf nie vergessen: Cyberkriminelle versuchen immer und überall, Zugangsdaten abzugreifen.
(Foto: imago/Ikon Images)

Folgen auf:

Sicherheitsforscher entdecken Datenbanken mit insgesamt rund 16 Milliarden gestohlenen Anmeldeinformationen. Die meisten davon waren bisher nicht bekannt. Auch wenn es Überschneidungen gibt, ist die Zahl gigantisch und Nutzer sollten handeln.

Verwenden Sie bitte keine FAU Benutzernamen und Passwörter auf anderen Plattformen

Schlecht: michael.tielemann@fau.de Passw0rt

Besser: t04325b tbdhb&38dn

Benutzen Sie Passwordmanager

Empfehlung:

KeePassXC
https://www.intern.fau.de/informationstechnik-it/it-tipps-aus-dem-cio-office/#31
https://www.anleitungen.rrze.fau.de/serverdienste/multifaktor-authentifizierung/empfehlung-fuer-authentifizierungs-anwendungen/

Ob Sie betroffen sind können Sie unter https://haveibeenpwned.com/

Aktuelle Meldungen

Wegweiser im digitalen Alltag mit vielen praxisnahen und hilfreichen Tipps zur IT-Sicherheit für Verbraucherinn und Verbraucher, sowie Schritt-für-Schritt-Anleitungen und Checklisten für den Ernstfall

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Broschueren/broschueren_node.html

Cyber Gangsta’s Paradise | Prof. Merli ft. MC BlackHat

INSTITUT FÜR INNOVATIVE SICHERHEIT DER HOCHSCHULE AUGSBURG

https://www.youtube.com/watch?v=6Hcs78NTqpE

Ihre Fragen?

Ihre Wünsche?