

# CISO Sprechstunde

07.03.2023

Ihre Fragen?

Ihre Themen?

# Informationssicherheit an der FAU

## Warum der ganze Aufwand?

## 9 von 10 Unternehmen

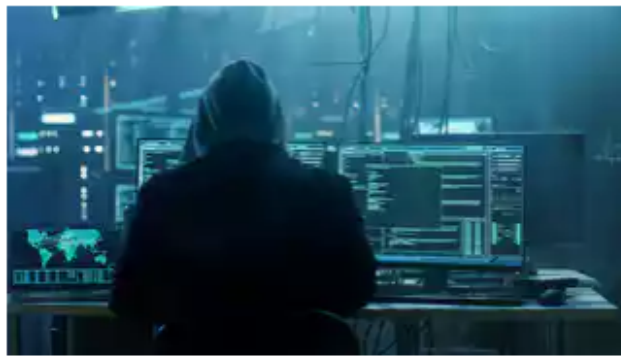
waren 2021 von Datendiebstahl, Industriespionage oder Sabotage betroffen.

## 8 von 10 Unternehmen

glauben, dass die Zahl der Cyberattacken auf ihr Unternehmen zunehmen wird. Jedes zehnte Unternehmen sieht seine geschäftliche Existenz durch Cyberattacken bedroht.

Cybersicherheit  
& Sicherheits-  
technologien

Quelle: Bitkom Research 2021



## Ransomware: Nach der Erpressung folgt umgehend die nächste Erpressung

Online-Kriminelle werden immer dreister und schlachten Opfer von Erpressungstrojanern gleich mehrfach aus.

05. Januar 2024, 13:36 Uhr 26

<https://www.heise.de/security/>



## 🔥 Kritische Schadcode-Lücke gefährdet Ivanti Endpoint Manager

Unter bestimmten Voraussetzungen können Angreifer Schadcode auf Ivanti-EPM-Servern ausführen.

05. Januar 2024, 11:18 Uhr



## Russland späht ukrainische Abwehr mit Webcams aus

Russische Geheimdienste haben sich in Webcams eingeklinkt und damit die ukrainische Verteidigung ausspioniert. Der Zugriff wurde blockiert.

05. Januar 2024, 10:46 Uhr 34



**76 attacks on institutions of higher education worldwide in 2021/22**  
**10 in Germany**



1. November 2021

**Cyberattack on the Nuremberg Institute of Technology, Germany**

Nuremberg Institute of Technology / Nuremberg Tech - Nuremberg, Bavaria, Germany



April 19, 2022

**Unauthorized access to data of a university library in Germany**

Universitätsbibliothek Leipzig - Leipzig, Germany

*Affected are about 70,000 records with personal data.*

# Informationssicherheit an der FAU

## Was macht es so schwer?

## Sicherheit

- Gegen welche Bedrohung?
- Bei welchem Risiko?
- Bei welchem Restrisiko?
- Wie sehen Sicherheitsziele aus?

## Wikipedia: Informationssicherheit

- ist ein Zustand von technischen oder nicht-technischen Systemen zur Informationsverarbeitung, -speicherung und -lagerung, der die **Schutzziele** Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen soll.
- dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von wirtschaftlichen Schäden und der Minimierung von Risiken.

# Strukturelle Herausforderungen

Die offene Struktur an der FAU ist eine Herausforderung:

- Universitätsleitung
- Fakultäten
- Gremien
- Hochschulangehörige
- Lehrstühle
- wissenschaftliche Forschung und Lehre sind frei
- Einrichtungen
- Rechenzentrum  
auch Service Provider für andere Hochschulen und Kliniken
- Kooperationen, Drittmittelprojekte
- Datenschutz nach DSGVO
- etc.



## Aktuelle Zahlen an der FAU

901 Einrichtungsleiter haben

- 342 IT-Betreuer in 222 Einrichtungen benannt
- 812 Rundschreibenempfänger in 324 Einrichtungen benannt
- 1318 Campo-Beauftragte in 547 Einrichtungen benannt
- 644 Lehre-Verwalter in 347 Einrichtungen benannt
- 476 Arbeitsplatzverwalter in 310 Einrichtungen benannt zusammen mit den Einrichtungsleitern
- 1699 Arbeitsplatzräume in 180 Einrichtungen verwaltet haben

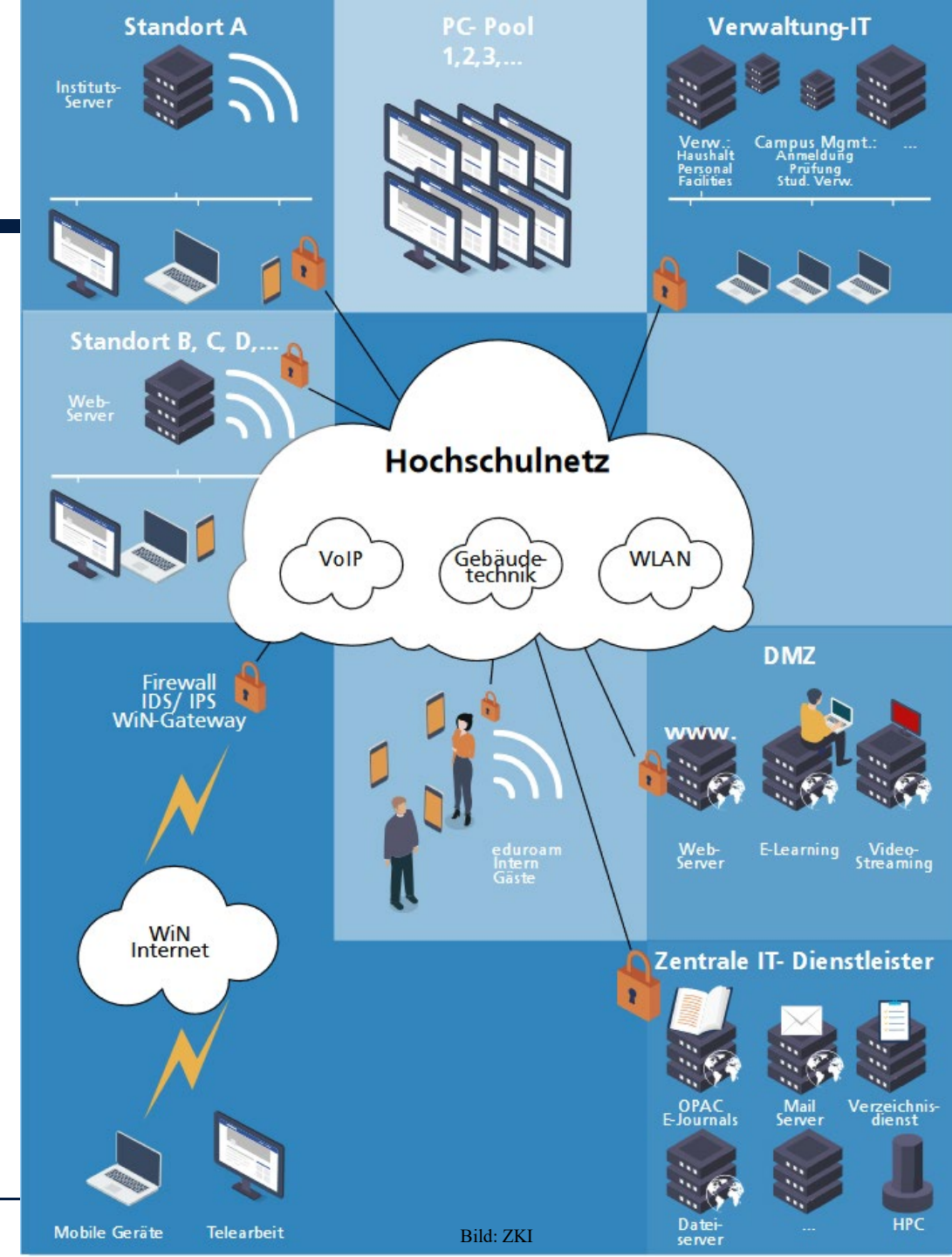
# Herausforderungen durch Digitalisierung und Services

## IT-Dienst / Prozesse / IT-Infrastruktur

- Heterogene Umgebung
- Keine oder sehr unterschiedliche Prozesse und Organisationsformen

## Typische Services

- Bereitstellung von PC-Pools
- Softwareangebote (Download) für Studierende
- E-Learning-Plattform
- Chat-/Messenger/Mail-Plattform
- Veranstaltungsaufzeichnung
- Computing / HPC
- zentraler Speicherplatz
- Web Services
- Print-Services
- Nutzersupport, etc.



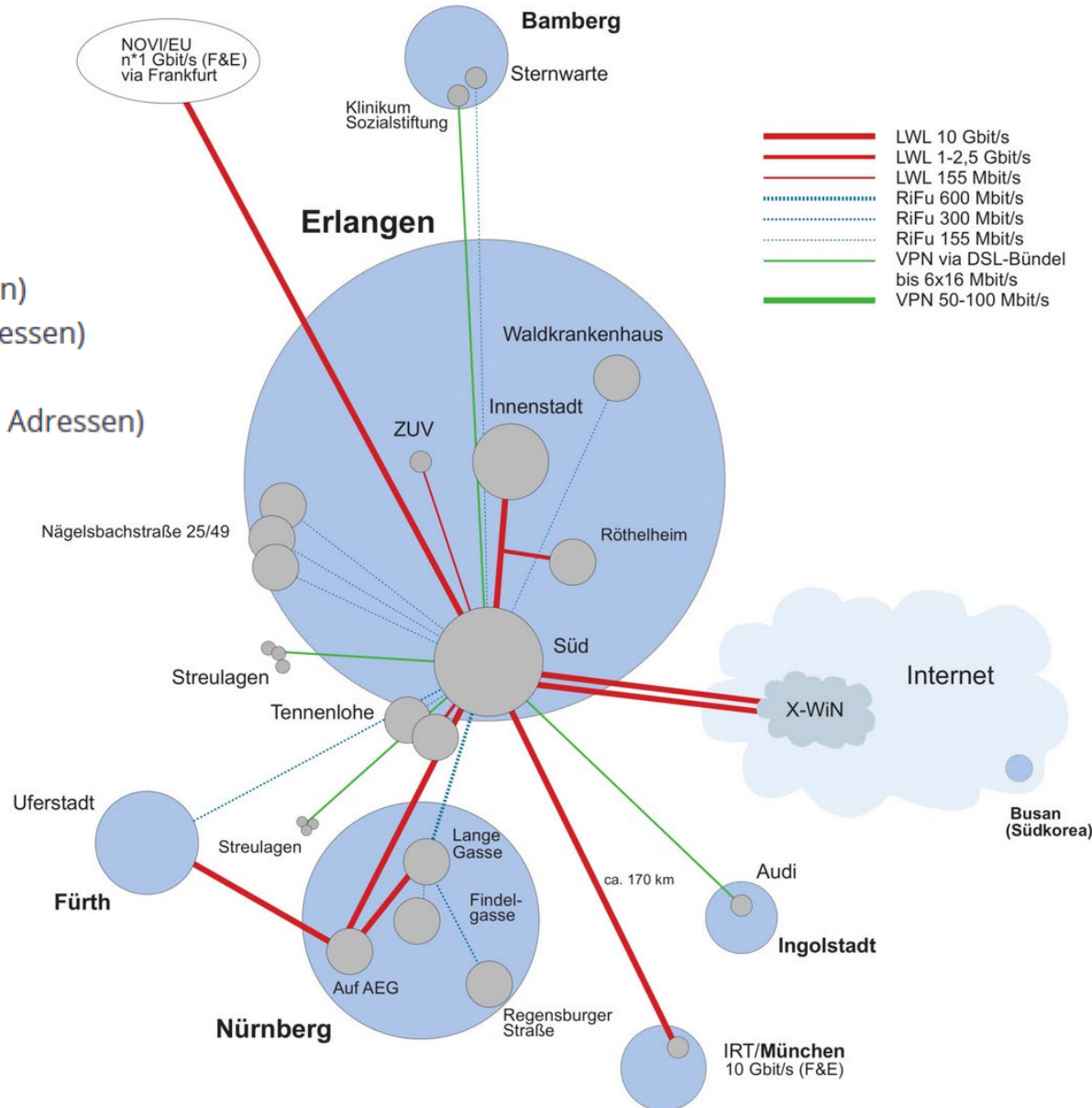
# Technische Herausforderungen

## FAU

- 131.188.0.0/16
- 10.0.0.0/8 (private Adressen)
- 192.168.0.0/16 (private Adressen)
- 2001:638:a000::/48
- fd00:638:a000::/48 (private Adressen)



Richtfunkaufpunkt am RRZE



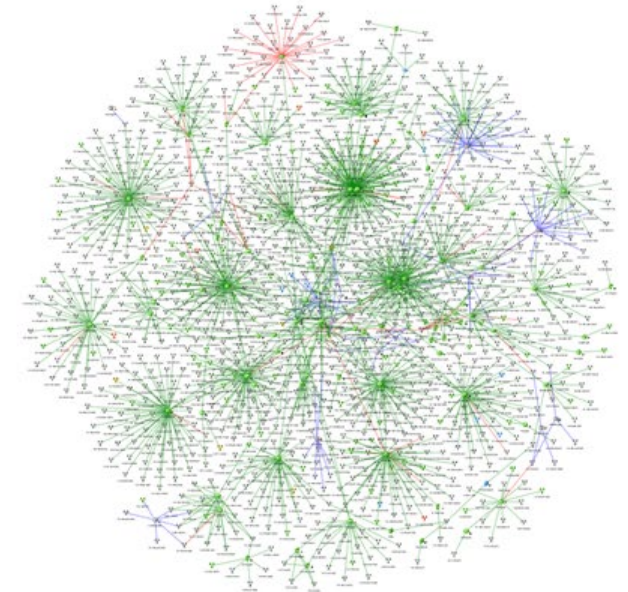
## Netzwerkdesign

Designgrundlagen:

- Hierarchisch-strukturiertes Netzwerkdesign
- Dreigliedrige Netzhierarchie (*Core-Network, Distribution-Network, Access-Network*)
- Redundanter Aufbau aller Core- und wesentlichen Distribution-Komponenten
- Zentrales Management und Betriebsverantwortung

Kennzahlen (gerundet, Stand Q2/2017):

- 200.000 verwalteten IP-Adressen
- 65.000 Endnutzern
- 1.300 IP-Subnetzen
- 1.500 LAN-Switches
- 1.200 WLAN-Access-Points
- 50 Router



Topologische Darstellung der IP-Subnetze der FAU

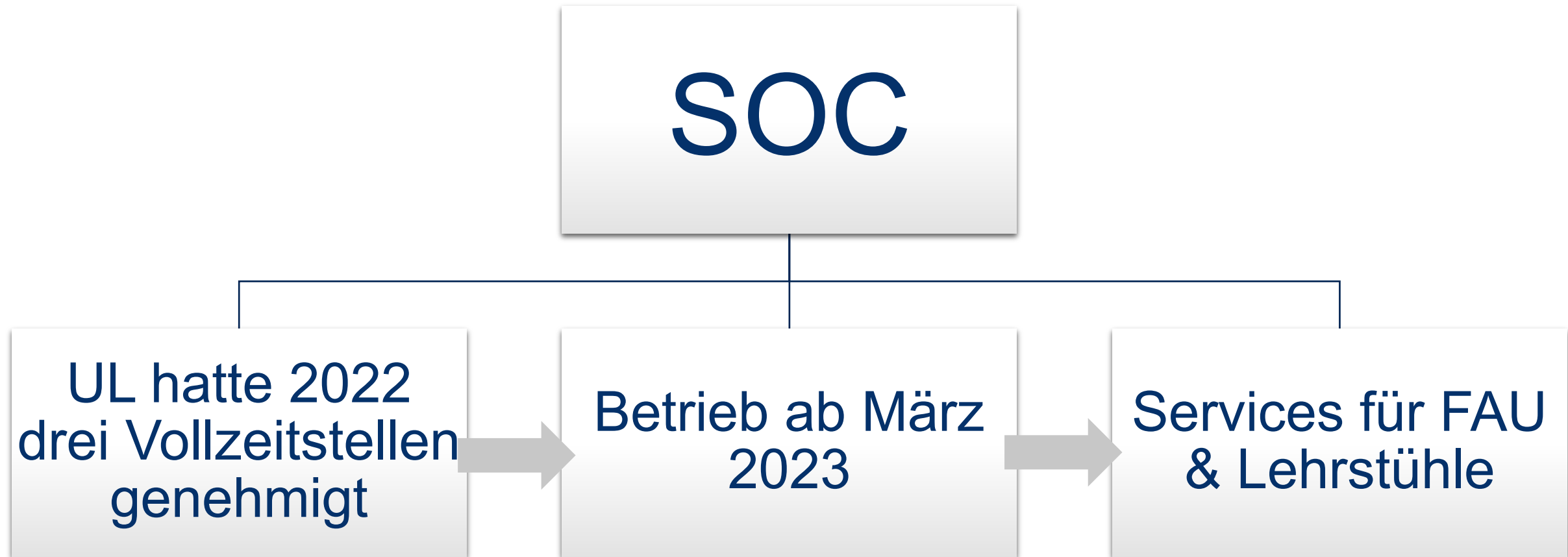
# Informationssicherheit an der FAU

## Was tun wir?

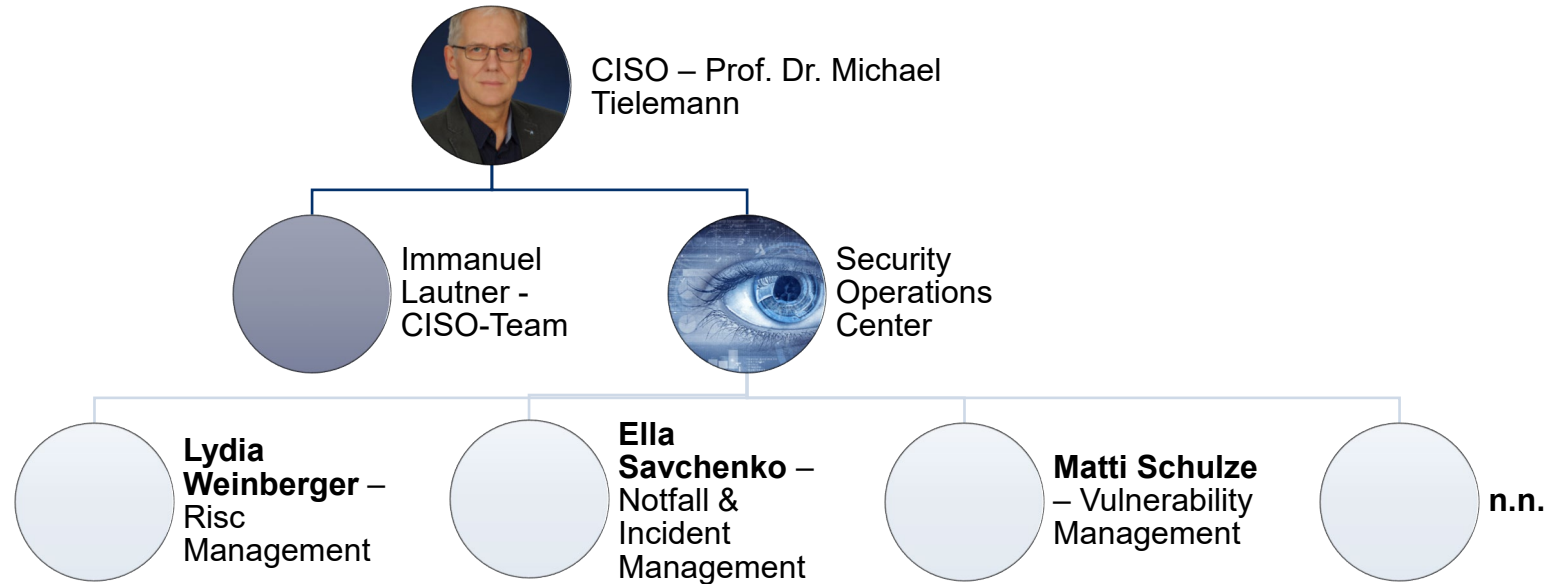
## Welche Maßnahmen wurden bis dato gestartet?

- **Leit- und Richtlinien**  
Allg. Richtlinie ist erstellt, Cyber-Richtlinie nahezu fertig
- **Risikomanagement**  
Welche Risiken hat die FAU?
- **Schwachstellen Management**  
Kontinuierlicher Schwachstellenüberwachung unserer ca. 3500 Internetsysteme
- **Notfallmanagement & Incident Response Management**  
WAS und WIE machen wir in IT-Notfällen oder IT-Katastrophen?
- **InfoSec-Konzepte für Departments und Lehrstühle**  
liegen vor, müssen noch an die FAU-Realität adaptiert werden

➔ **Gründung eines Security Operations Center (SOC)**



# Wer ist das Infosecurity Team & SOC?



More Info:



### Aufgaben eines Security Operations Center

- **überwacht** Aktivitäten auf exponierten Systemen (Servern, Websites, Netzwerken, Anwendungen, Endgeräten und anderen Systemen) auf Schwachstellen und Anomalien
- übernimmt eine Führungsrolle beim **Security Incident Response**
- kümmert sich um die **Analyse des Sicherheitsvorfalls**, untersucht die Quelle, übernimmt die Berichterstellung über aufgedeckte Schwachstellen und das Verhindern ähnlicher Vorfälle in der Zukunft
- einzig zu dem Zweck, mögliche **Sicherheitsbedrohungen** aufzuspüren und so schnell wie möglich abzuwenden
- behandelt Probleme möglichst in Echtzeit und sucht gleichzeitig kontinuierlich nach Möglichkeiten, den Sicherheitsstatus der Organisation zu **optimieren (Zielvorstellung)**
- **tiefgehende online Analysen von Security-Log-Daten** aus unterschiedlichen Quellen (SIEM)
- Durchsetzen von Sicherheitsrichtlinien und -verfahren
- u.v.m.

# Informationssicherheit an der FAU

## Sind wir innovativ genug?

# Sicherheit von Passwörtern

Aktueller Bericht <https://www.homesecurityheroes.com/ai-password-cracking/>

- Sicherheitsexperten des IT-Unternehmens Home Security Heroes haben [eine Untersuchung veröffentlicht](#), wie sich Passwörter mithilfe des KI-gestützten Tools PassGAN knacken lassen.
- Obwohl zum Trainieren der KI "nur" 15 Millionen Passwörter verwendet worden sind, legen die Ergebnisse nahe, dass die Methode effizienter arbeiten dürfte als bisher genutzte Software.
- Die Forschungsergebnisse zeigen, dass 51 Prozent der gängigen Passwörter innerhalb von einer Minute, 65 Prozent innerhalb einer Stunde, 71 Prozent innerhalb eines Tages und 81 Prozent innerhalb eines Monats geknackt werden können.
- Test your Pwd: <https://www.homesecurityheroes.com/ai-password-cracking/> (bitte keine aktuell verwendete Pwds eingeben, nur ähnliche)

## Time It Takes Using AI to Crack Your Password [2023]



# OF CHARACTER	Numbers Only	Lowercase Letters	Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	4 Seconds
7	Instantly	Instantly	22 Seconds	42 Seconds	6 Minutes
8	Instantly	3 Seconds	19 Minutes	48 Minutes	7 Hours
9	Instantly	1 Minutes	11 Hours	2 Days	2 Weeks
10	Instantly	1 Hours	4 Weeks	6 Months	5 Years
11	Instantly	23 Hours	4 Years	38 Years	356 Years
12	25 Seconds	3 Weeks	289 Years	2K Years	30K Years
13	3 Minutes	11 Months	16K Years	91K Years	2M Years
14	36 Minutes	49 Years	827K Years	9M Years	187M Years
15	5 Hours	890 Years	47M Years	613M Years	14Bn Years
16	2 Days	23K Years	2Bn Years	26Bn Years	1Tn Years
17	3 Weeks	812K Years	539.72M Years	2Tn Years	95Tn Years
18	10 Months	22M Years	7.23Bn Years	96Tn Years	6Qn Years

Bild: Home Security Heroes

---

# Informationssicherheit an der FAU

## Die Richtlinie

- 
- Der Text liegt beim GPR zur Abstimmung/Freigabe, da einige Teile Mitbestimmungspflichtig sind.
  - Der Entwurf