Technische Hochschule Rosenheim
Technical University of Applied Sciences

Lage der Cybersicherheit

Prof. Dr. Reiner Hüttl

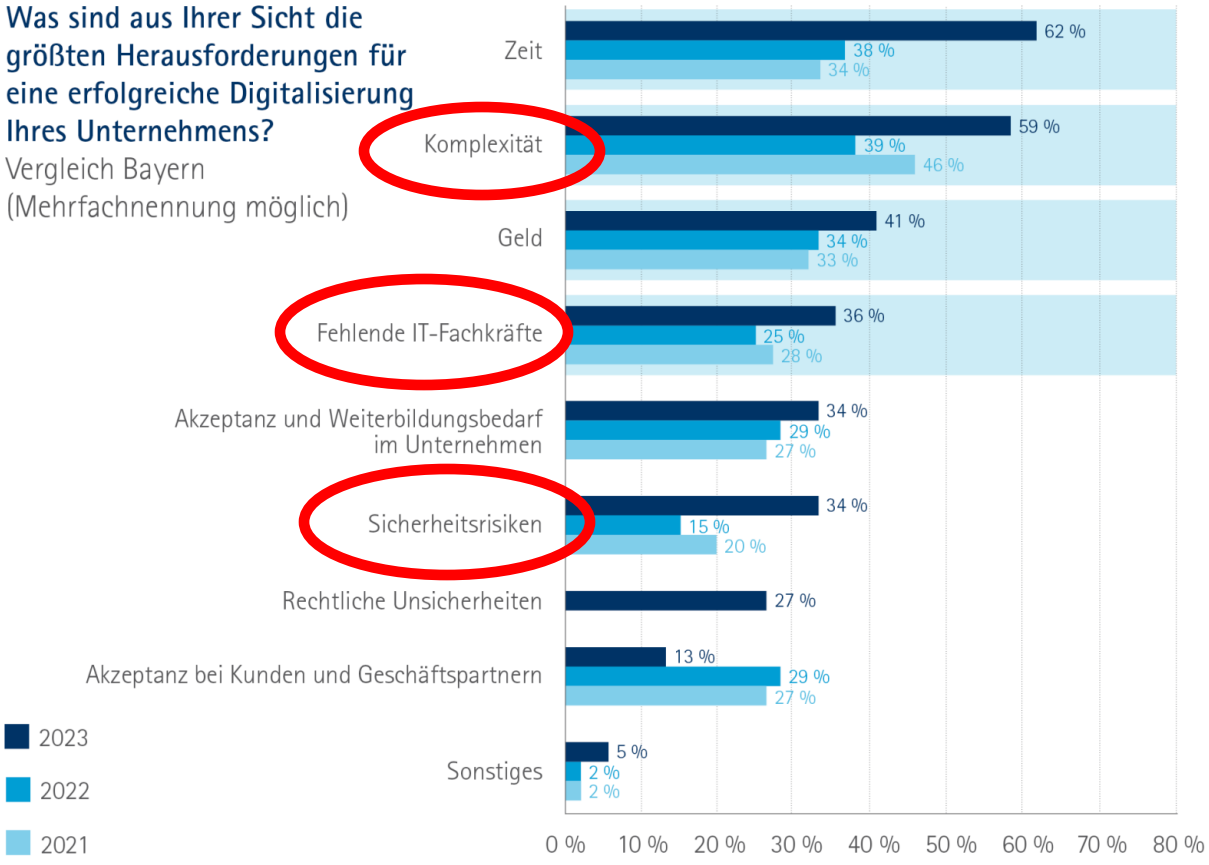
BIHK-Reihe zur IT-Sicherheit 2024

Lage der Cybersicherheit

- Relevanz der Cybersicherheit
- Aktuelle Bedrohungslage
- Herausforderung für Unternehmen
- Strategien und Lösungen
- Ausblick in die Zukunft

IHK UMFRAGE DIGITALISIERUNG

Technische Hochschule Rosenheim
Technical University of Applied Sciences

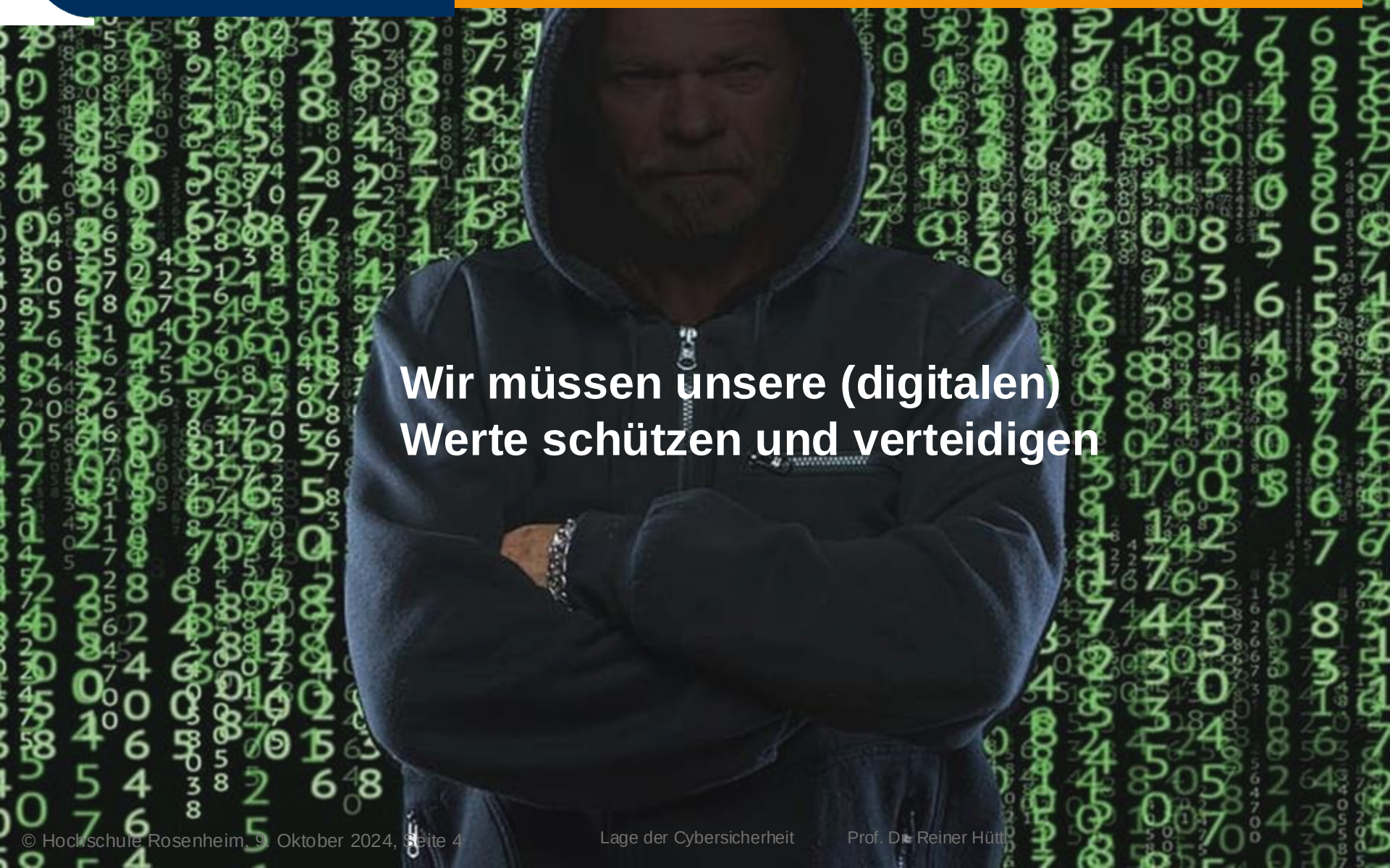


Bayerische Unternehmen bewerten ihren Stand der Digitalisierung im Schnitt mit **2,8** (Skala: 1 – 6)

https://www.ihk-muenchen.de/de/Wirtschaftsstandort/Infrastruktur/Digitale-Infrastruktur/IHK-Digitalisierungsumfrage/

FOLGEN DER DIGITALISIERUNG

Technische Hochschule Rosenheim
Technical University of Applied Sciences



Wir müssen unsere (digitalen) Werte schützen und verteidigen

Cyber Security ist für alle Unternehmen ein wichtiges Thema

- **Die Digitalisierung schreitet unaufhaltsam voran**
  - Der Anteil von IT in den Geschäftsmodellen wird in allen Branchen immer höher
  - Die meisten Innovationen heutzutage sind IT oder haben einen sehr starken IT-Bezug
- **Es werden immer mehr Schwachstellen in Software und IT-Systemen entdeckt und gemeldet**
- **Die Anzahl und Komplexität der Angriffe steigt ständig**
- **Wenn die IT-Systeme (teilweise) ausfallen sind Unternehmen (meistens) handlungsunfähig**
  - Beispiel: CrowdStrike Ausfall Juli 2024

Was sind die aktuellen Bedrohungen?

- Statistik vom BSI
- Studie von bitkom

BSI: LAGE DER IT-SICHERHEIT IN DEUTSCHLAND

Bedrohungen

- Ransomware (Erpressung, Lösegeld, Datenleaks)
- Anstieg an Schwachstellen
- Neue Schadprogramme
- Spam- und Phishing-Mails
- Identitätsdiebstahl

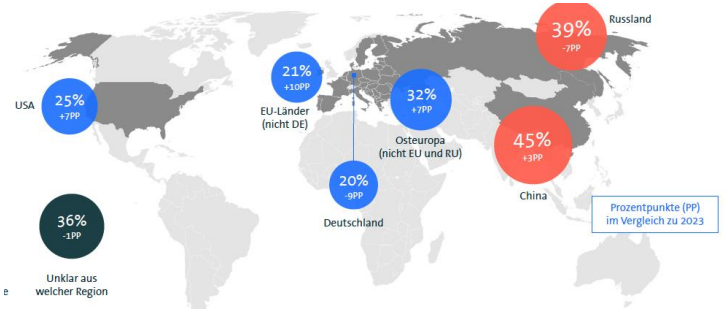
- Ausbau der Cyberkriminellen Schattenwirtschaft
- Cyberkriminelle Arbeitsteilung
- Weg des geringsten Widerstands, nicht maximales Lösungsgeld → KMU

- DDoS Hacktivism → Propaganda, Desinformation
- APT (Advanced Persistent Threats) mit Ziel Spionage oder Sabotage

KI: Chance und Risiko für Cybersicherheit

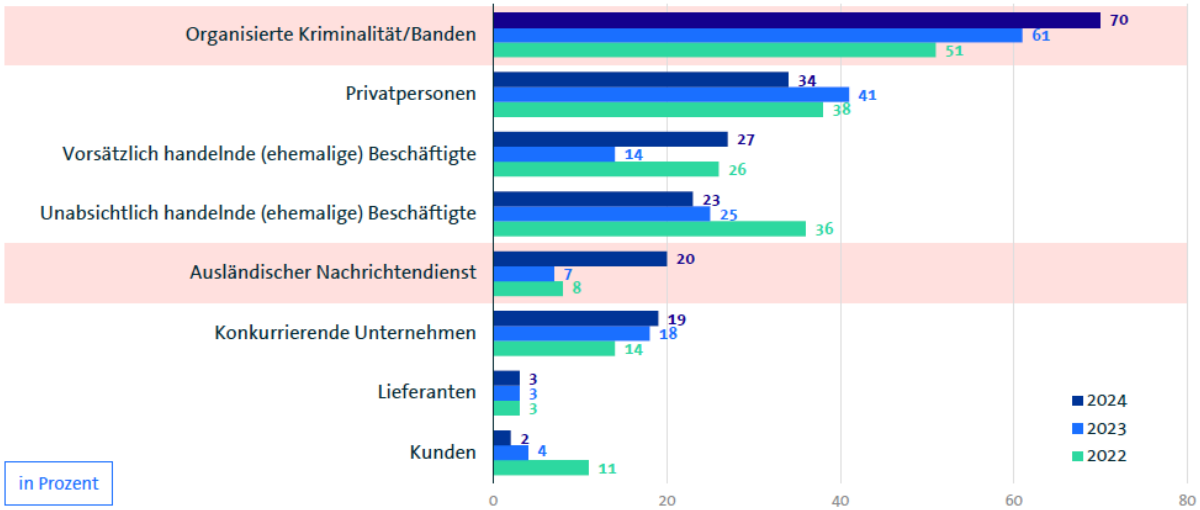
https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

Gesamtschaden 267 Milliarden Euro,
67% durch Cybercrime



Organisierte Kriminalität und Geheimdienste greifen an

Von welchem Täterkreis gingen die Handlungen in den letzten 12 Monaten aus?



Basis: Unternehmen, die in den letzten 12 Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=812) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2024

5

bitkom

https://www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz

Was sind die Herausforderungen?
Security Challenges

- **Wachsende Komplexität der IT-Strukturen durch Digitalisierung, IoT und Industrie 4.0**
- **Mangelnde Sensibilisierung der Mitarbeiter**
- **Veraltete Systeme und IT-Infrastrukturen**
- **Mobile Work**
- **Fehlende IT-Experten, speziell im Bereich Cyber Security**

- Mangelnde Bereitschaft in IT-Sicherheit zu investieren (Personal, Prozesse, Technik)

Rechtslage und Regulierungen
Compliance

Die Rechtslage ist komplex, ständig im Fluss und überfordert teilweise KMUs

Sie schafft viel Bürokratismus und nur zum Teil wirkliche Sicherheit

- IT-Sicherheitsgesetz
- KRITIS
- NIS2
- EU GDPR, DSGVO
- AI Act
- Hacker Paragraph

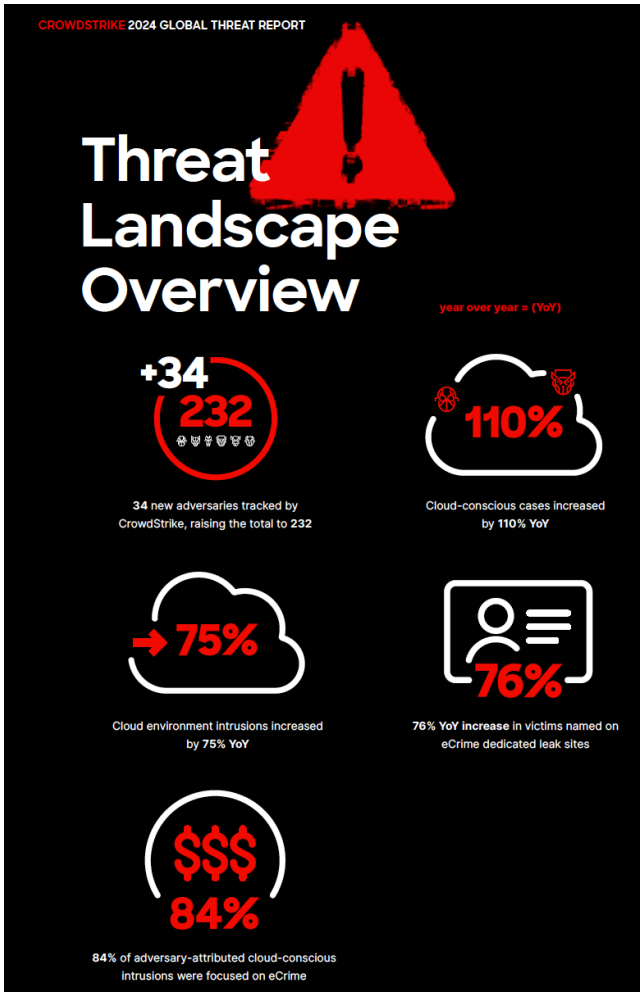
Was können Unternehmen machen? Ein Sicherheitskonzept leben

- Implementierung eines ganzheitlichen Sicherheitskonzepts, und Risikoanalysen
- Ein erprobtes Incident- und Notfallmanagement
- Zero Trust Ansatz und kontinuierliche Überwachung
- Sensibilisierung und Schulung von Mitarbeiter
- Einsatz von Sicherheitsstandards und Zertifizierungen
- Fachlich qualifiziertes Personal einstellen

CROWDSTRIKE THREAT LANDSCAPE

Technische Hochschule Rosenheim
Technical University of Applied Sciences

CROWDSTRIKE



Identitätsbasierte und Social Engineering Angriffe mit starken Wachstum

Empfehlungen von Crowdstrike:

- **Identitätsschutz** als must have
  - Phishing resistente multifaktor Authentifizierung
  - User Awareness
  - Ausweitung auf Legacy Systems
  - Einführung von Technologien die Bedrohungen erkennen können

- Einsatz einer Plattform zum Schutz von Cloud Anwendungen
  Cloud-native-application protection platform (**CNAPP**)

https://www.crowdstrike.com/global-threat-report/

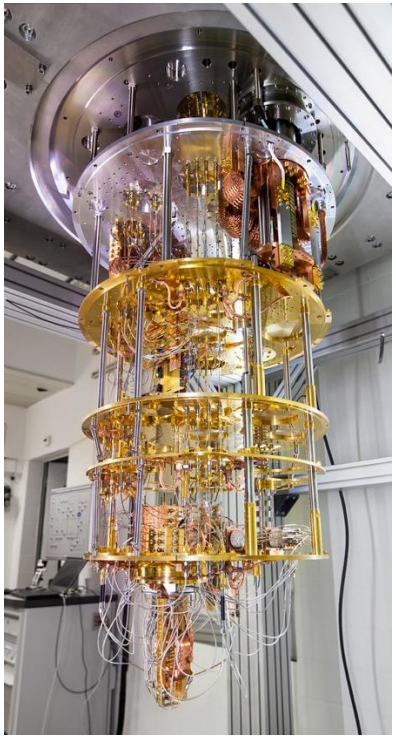
splunk> a CISCO company

Es wird ein Wettlauf zwischen Angreifern und Security Teams beim Einsatz von KI

Die 5 Cybersecurity-Prioritäten von splunk

1. Beschäftigte aus Cybersicherheit und IT-Betrieb in **Security Operations** schulen
2. Tools für Security Operations beschaffen
3. Eine **Softwarearchitektur** entwickeln und aufbauen, die Sicherheitsanalysen und Security Operations integriert.
4. **Cloud-Technologien** für Sicherheitsanalysen und Security Operations einsetzen.
5. Verstärkt **externe Ressourcen** für die Security Operations mobilisieren (z. B. Managed Security Services).

https://www.splunk.com/de_de/form/state-of-security.html



Quantencomputer
gefährden die Kryptographie

Was erwartet uns in Zukunft?

- **Künstliche Intelligenz wird immer besser**
  - **Einsatz von KI durch Angreifer**
    - Deepfakes (manipulierte Bilder, Stimmen, Videos)
    - Social Engineering
    - Automatisierung von Angriffen
    - Angriffe auf fehlerhaft erzeugten Code
  - **Einsatz von KI zur Verteidigung**
    - KI und Machine Learning zur Bedrohungserkennung
    - Automatisierte Incidence Reports

Technische Hochschule Rosenheim
Technical University of Applied Sciences

Was bietet die TH Rosenheim für die Cybersicherheit?

Studiengänge an der Fakultät für Informatik zur Ausbildung von Security Experten

- Informatik
- Wirtschaftsinformatik
- Applied Artificial Intelligence

Security Module von Experten aus der Praxis

- genua GmbH
- ITK Engineering GmbH
- HvS-Consulting AG

Technische Hochschule Rosenheim
Technical University of Applied Sciences