HOCHSCHULE
RAVENSBURG-WEINGARTEN
UNIVERSITY
OF APPLIED SCIENCES

ERFAHRUNGEN UND KONSEQUENZEN AUS HACKERANGRIFFEN UND INFORMATIONSSICHERHEITSMANAGEMENT AN DEN HOCHSCHULEN IN BW

3. FACHTAGUNG DIGITALE VERWALTUNG, APRIL 2024

Prof. Dr. Christoph Andriessens

christoph.andriessens@rwu.de

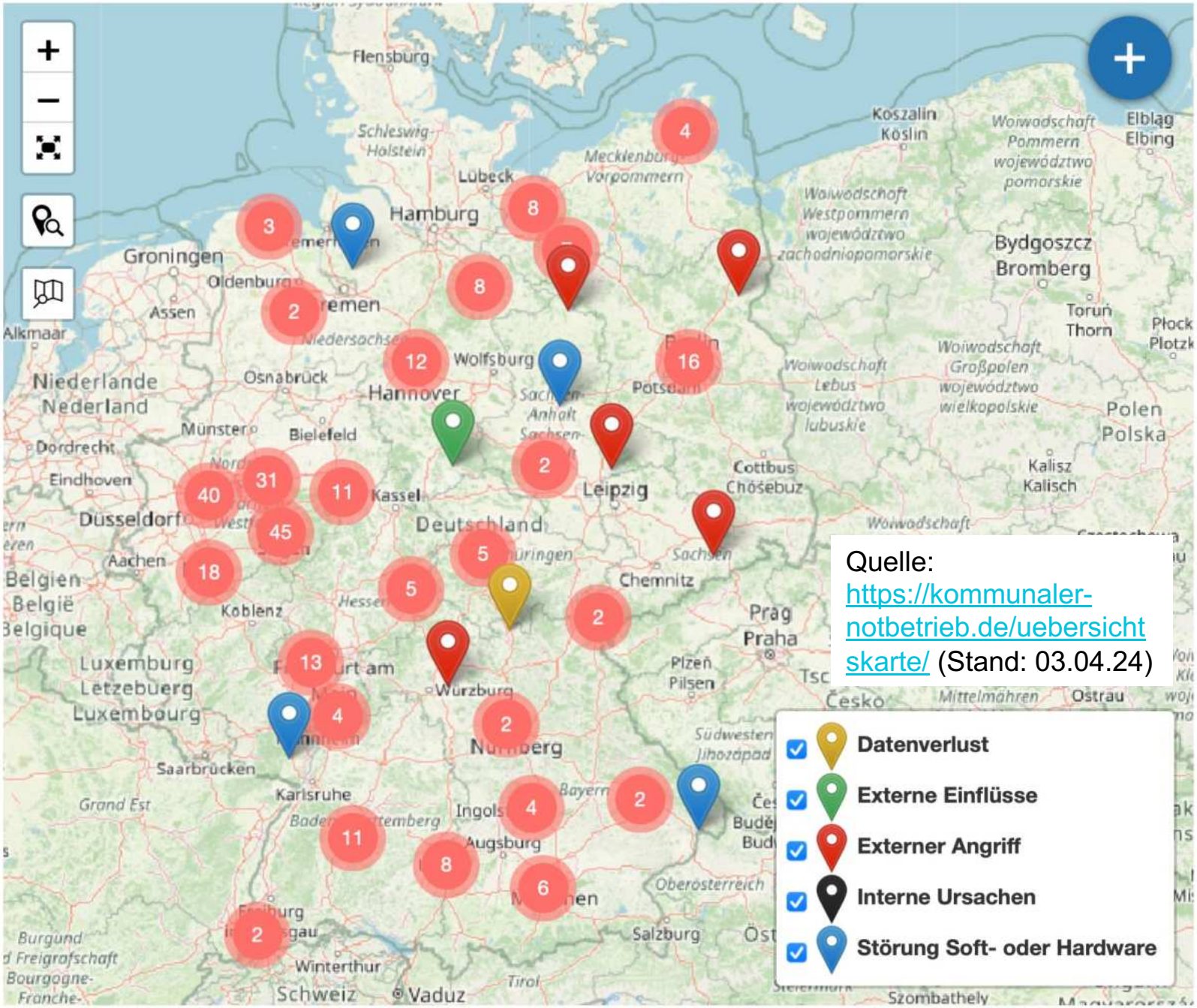
Prof. Dr-Ing. Christoph Andriessens
Zur Person

- Div. berufliche Stationen in **Softwareindustrie** und **IT-Betrieb**
- **Professor für Informatik**
- **ISB / CISO** der RWU
- **Sprecher des AK ISB** (Arbeitskreis der Informationssicherheitsbeauftragten der nicht-universitären Hochschulen und des HSZ BW)
- Mitglied des **Kooperationsverbundes bwInfoSec**
- Mitglied des **Fachbeirats des Hochschulservicezentrums** (HSZ) BW

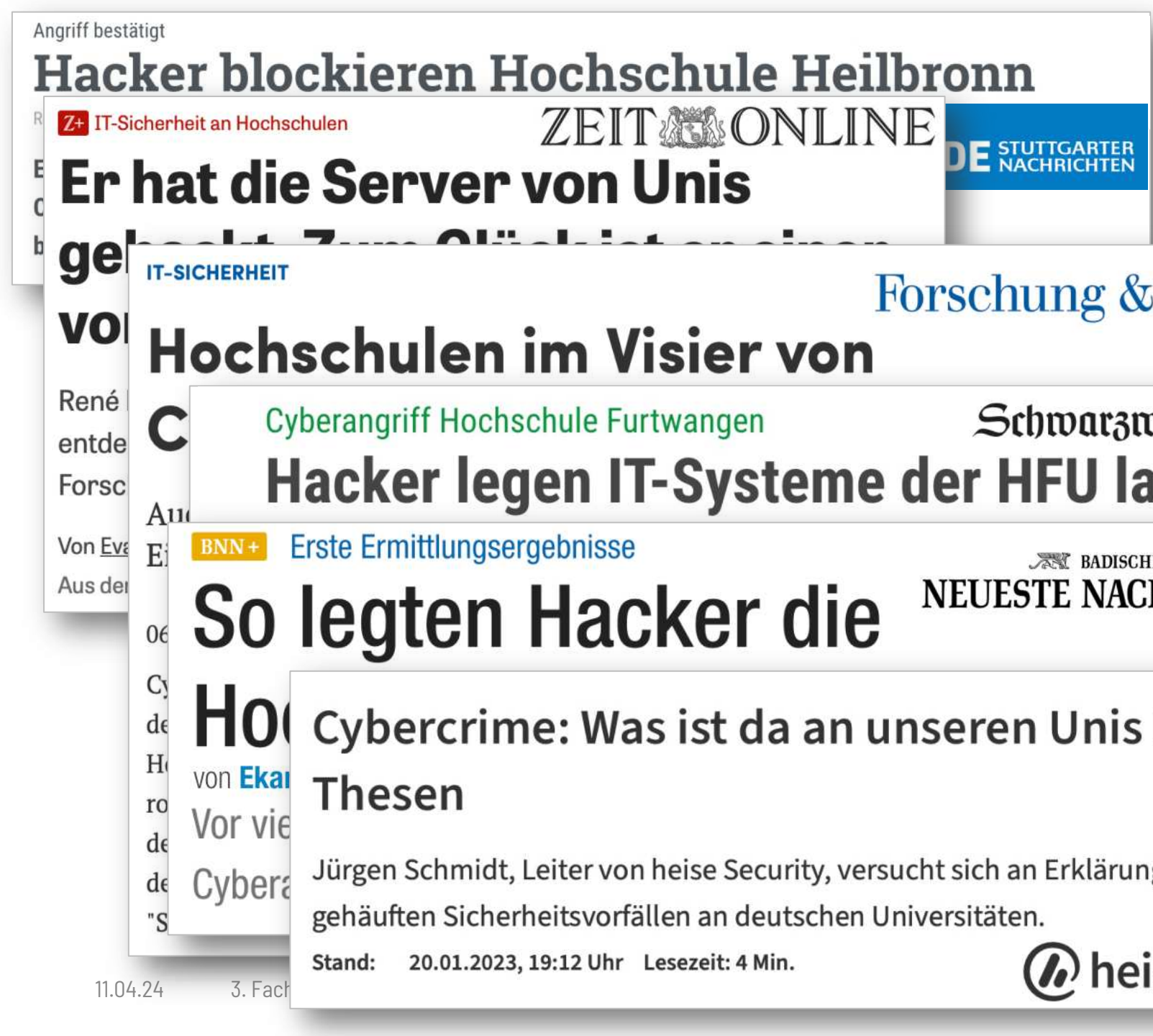
Vorfälle auf kommunaler Ebene

Dreistellige Anzahl von Kommunen betroffen?

IT-Sicherheitsvorfälle in Kommunalverwaltungen



Quelle: https://kommunaler-notbetrieb.de/uebersichtskarte/ (Stand: 03.04.24)



Auswahl bekannter Fälle an Hochschulen in BW …

Bedrohungslage, soweit durch Menschen verursacht

Jede Kommune, jede Hochschule ist auf internationalem Parkett

Akteure

- Innentäter (absichtlich und unabsichtlich)
- Technisch interessierte Personen
- Cyberkriminelle, z.T. organisiert
- Cyberterroristen
- Wirtschaftsspionage
- Staatliche Akteure (z.B. Nachrichtendienste, internationale Beeinflussung)
    - Förderung anderer Akteure

Möglichkeiten

- Hohe Automatisierung
- Einfaches internationales Agieren
- Hohe Arbeitsteiligkeit
- Z.T. hochprofessionell aufgestellte Organisationen
- Bis zu einem gewissen Niveau leicht verfügbares Wissen
- Leicht verfügbare Werkzeuge
- Werkzeuge mietbar „as a Service“

Kommunen und Hochschulen
Gemeinsamkeiten … und Unterschiede

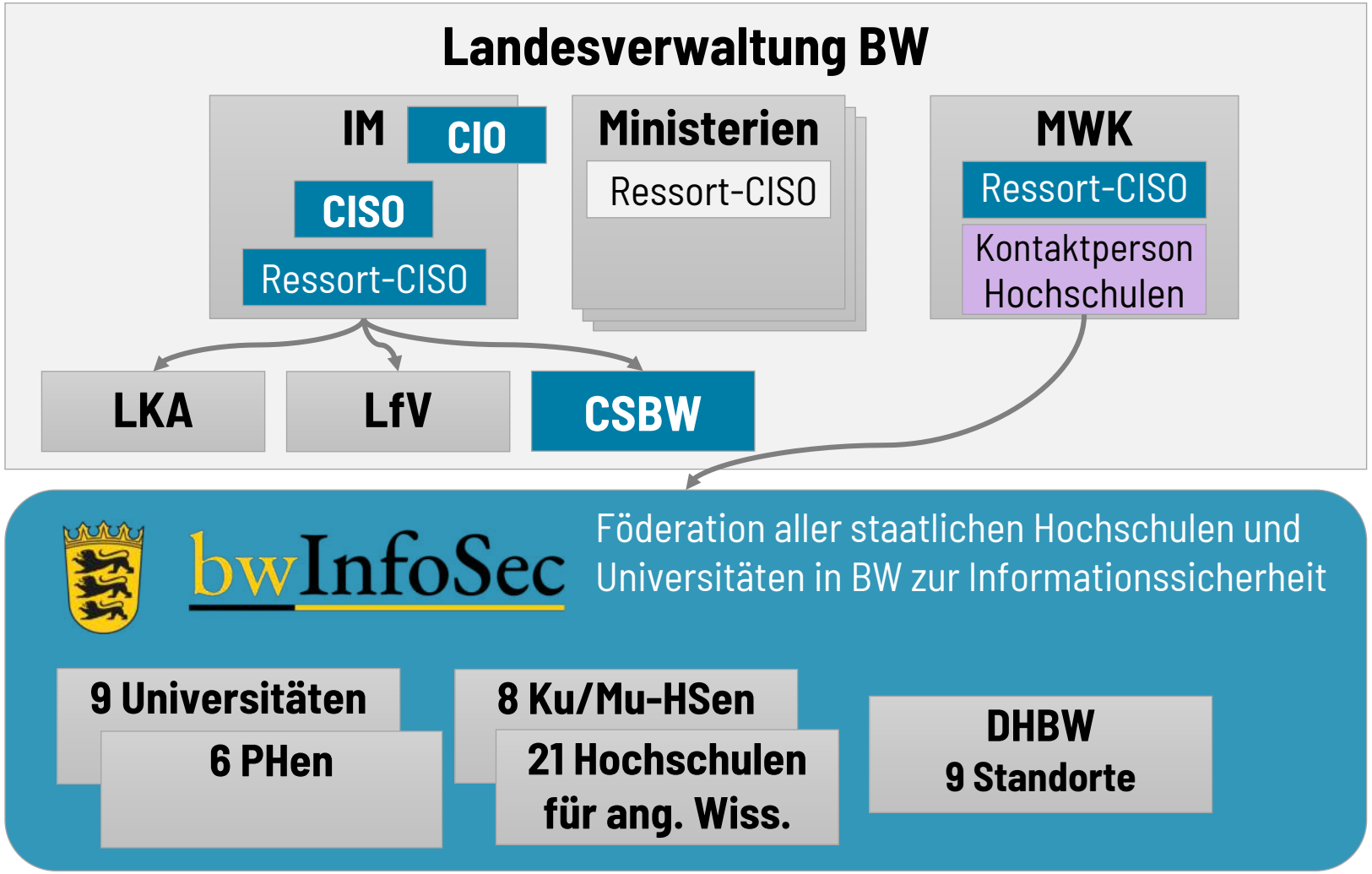
Gemeinsamkeiten

- Aufgaben in der öffentlichen Verwaltung, Funktion wird mit Funktionsfähigkeit des Staates verbunden
- Kooperationen schon länger üblich
- Über Jahre hinweg (aus heutiger Sicht) eher „naiver" Einsatz von Computern
- Große und wachsende Abhängigkeit von IT, gewachsene und wachsende Komplexität
- IT-Tarifkorsett des öff. Dienstes
- Änderungen … schon mal langwierig

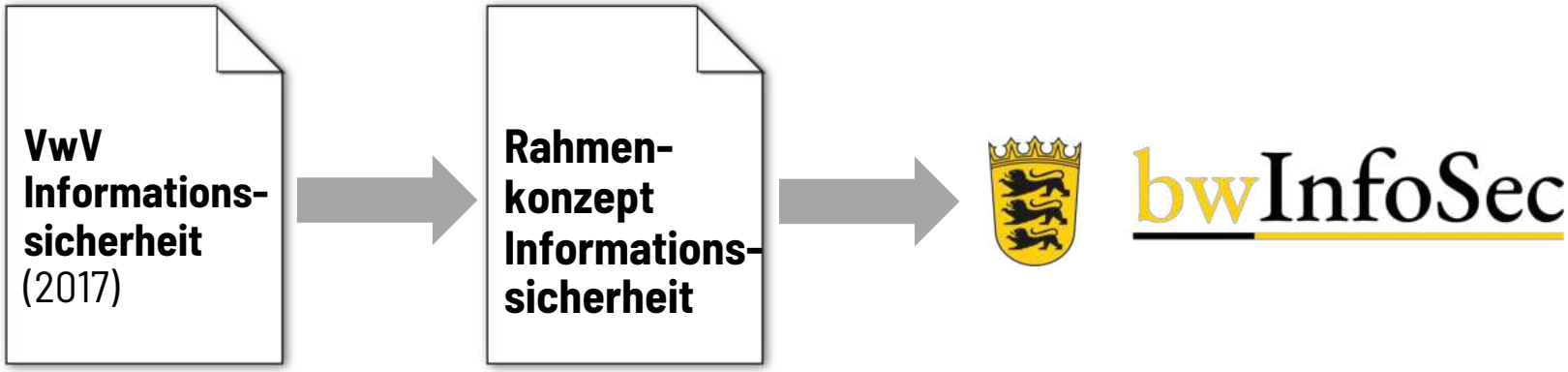
Besonderheiten der Hochschulen

- Autonomie
- Rechtsaufsicht des MWK
- Offene Netze, ggf. viele tausende und wechselnde Benutzer
- Große Freiheiten für Professoren sowie Forschung und Lehre nach Art. 5 Abs. 3 GG
    - Dezentral betriebene IT-Systeme
    - Experimentelle IT-Systeme
- Teilweise großes IT-Know-How, das aber eher in Forschung und Lehre als Betrieb fließt

Sicherheitsorganisation der Hochschulen BW
...innerhalb der Landesverwaltung



Gründung Hochschul-Föderation bwInfoSec
Umsetzung der VwV Informationssicherheit



- **VwV Informationssicherheit** verpflichtet Landesverwaltung zur Einführung eines Informationssicherheitsmanagementsystems nach **BSI IT-Grundschutz / ISO 27001**
- Damit auch Hochschulen betroffen (mindestens in bestimmten Bereichen)
- MWK fragt Hochschulen: Was benötigt Ihr zur Umsetzung?
- Hochschulen: Es geht nur gemeinsam – entwickeln zusammen das **Rahmenkonzept Informationssicherheit**
- Damit wird 20/21 die landesweite Föderation **bwInfoSec** gegründet

Sicherheitsorganisation der Hochschulen BW
Föderation bwInfoSec unter der Lupe

bwInfoSec

Kooperativ

Steuerkreis
Strategie, Leitung Kernteam
1 Sprecher nicht-universitär, 1 Sprecher universitär,
dazu weitere Hochschulvertreter

Kooperations-verbund
Beratungsgremium
verschiedene Stakeholder IT / InfoSec / **MWK** / AKs

Kernteam
Zentrale Dienste und Koordination für alle
12 Stellen, 2 Standorte
(Hochschulservicezentrum HSZ BW, Uni HD)

Lokal

- **Lokale Sicherheitsorganisation an den Hochschulen** je nach Hochschulart und Hochschule in unterschiedlicher Ausprägung: Beispielsweise 1 ISB-Stelle pro HAW und PH
- **Themenspezifische Arbeitsgruppen**
- **Dazu allgemeine, unabhängige Arbeitskreise**:
  - Arbeitskreis der ISBs nichtuniversitärer und pädagogischer Hochschulen und des HSZ
  - CISO-Arbeitskreis der Unis

Wo stehen wir?
Und: Lessons Learned nach 6 Jahren…

- Wir sind **stärker bedroht als ursprünglich gedacht**, die Gegner sind schlecht sichtbar, einfallsreich, und dem Angreifer reicht 1 Lücke.
- Der **Aufwand ist sehr groß**, aber notwendig. Nein, wir sind nicht fertig mit dem ISMS. Wann? Gute Frage …
- **Aufbau von Zusammenarbeit** kostet Zeit und Aufwand, Stellenbesetzung im Kernteam langwierig, Wechsel aus der Aufbauphase auch
  - Vernetzung sehr lehrreich und nützlich – aller Akteure
  - Austausch in Sicherheitsfragen ist nicht leicht: Wer darf wem wann was mitteilen?
- **Kernproblem**: Weniger ISMS-Einführung und Komplexität der Standards, viel mehr die **Konsequenzen für den IT-Betrieb**. Auswirkungen können kaum überschätzt werden.
  - Alles viel, viel professioneller: U.a. mehr Know-How (mehr Breite *und* Tiefe), mehr Geschwindigkeit, bessere Kenntnis eigener aktueller Lage, 24/7-Überwachung
  - Das Aufstellen einer IT-Organisation für die heutige Anforderungen aus Sicherheit ist für eine Hochschule alleine gar nicht zu schaffen

  ➢ Wir müssen im IT-Betrieb noch **viel stärker und systematischer zusammenarbeiten. Gründung einer bwIT-Allianz** der Hochschulen?!

Eine Aufgabenliste für den IT-Betrieb
Konsequenzen aus Lage und Standards

- Theorie: 10% des IT-Budgets für Inf.-Sicherheit (BSI sagt: 20%)
- on top, nicht Kürzung!

- Systematisches Schwachstellen-, Update- und **Patchmanagement**
- **Netzwerksegmentierung** mit Offenheit für Wissenschaft und Lehre
- **Mehrfaktorauthentifizierung** für alle Anwendungen
- Bessere Absicherung **Windows-Domänen** (Benutzerverzeichnisse und Rechte)
- Bessere **Absicherung von E-Mail** mit besserem Spamschutz, Mail-**Verschlüsselung** und Mailsignatur
- Sicheres Öffnen von **E-Mail-Anhängen** (z.B. Sandbox-/Virtualisierungslösungen)
- Breiteres und tieferes **Know-How zu Serverhärtung**
- **Zentrales Logging** (Protokollierung)
- **Überwachung** von Servern, Netzwerken und Clients **24/7** und jederzeitiger Identifizierung und **Eindämmung von Angriffen**
- Analyse von **Netzwerkflüssen**
- Network Access Management (Authentifizierung und Autorisierung für Netzwerkzugriff)
- Systematisches **Client Management**, auch für Professoren
- Systematisches, angriffsfestes **Backup**, auch für Professoren
- **Notfall- und Krisenpläne für Ausfallszenarien** (inkl. altern. Kommunikationsmöglichkeiten)
- Einführung von **Zero Trust** (Umstellung von Perimeterabsicherung auf Aufkündigung interner Vertrauensverhältnisse im Netzwerk, „Goldstandard“, aber aufwändig und komplex)

Industrialisierung
Der Vergleich zur Elektrizität in Deutschland

- **Beginn des 20. Jahrhunderts**: Strom kann nicht weit transportiert werden. Deshalb: **Strom muss dort erzeugt werden, wo er genutzt wird**
  - Lokale Schwankungen können nicht ausgeglichen werden
  - **Bis zum 1. Weltkrieg**: **4.040** stromerzeugende Unternehmen mit Gesamtleistung von **2.096 MW**, Produktionsort ist immer bekannt
- **Möglichkeiten zum Stromtransport** verbessern sich:
  - Zuerst Bildung von Regionalnetzen
  - 1930 erste Höchstspannungsleitung (220 kV) zwischen Regionalnetzen (z.B. Verbindung Rheinisches Revier [„Garzweiler“] mit Alpenwasserkraft)
  - Bis 1945 Verbundnetz für die wichtigsten Kraftwerke in Deutschland
- Strombedarf **wächst massiv**, Produktion **konzentriert** sich, **Produktionsort?**
- **2022**: **238.720 MW** (+ 11.400 %) Kraftwerkskapazität von **378** Betreibern (mit > 10MW)
  - EnBW: 10.168 MW, AKW Gundremmingen: 2.572 MW, Großkraftwerk MA (Steinkohle): 1.675 MW, Windpark „Borkum Riffgrund 2“: 464,8 MW

Industrialisierung der IT
Beispiel Hyperscaler

- Beispiel **AWS**:
  - 2016: Pro Rechenzentrum (RZ) „50.000-80.000 Server“ / „AWS adds the capacity equivalent of a FORTUNE 500 Enterprise daily“
  - Anfang 2023:
    - 96 „Availability Zones“ (AZ)
    - 1 Availability Zone = ein oder mehrere RZ

    ➢ Bei Annahme von 2 RZ mit 60.000 Server pro AZ => **11,5 Mio Server**
- Beispiel **Google**, Anfang 2023: „106 Zonen“
- Beispiel **Microsoft**, Anfang 2023: „ > 200 RZs“
- Dazu kommen jeweils weitere Einrichtungen, etwa Edge-Standorte

Quellen: Unternehmenswebsites 2023 / Hamilton, James: AWS re:Invent 2016: Amazon Global Network Overview with James Hamilton. Amazon Web Services. Online verfügbar unter https://www.youtube.com/watch?v=uj7Ting6Ckk.