



Technische  
Universität  
Braunschweig



# **IT- und Informationssicherheit: die Gratwanderung zwischen Fahrlässigkeit und Overkill. Eine Annäherung.**

Dietmar Smyrek, Vizepräsident der TU Braunschweig, 20.6.2024

# Gliederung

- Vorstellung AK Digitale Transformation der Universitätskanzler\*innen
- Berührungspunkte der Kanzler\*innen zum Thema IT-Sicherheit
- Notwendigkeit der IT-Sicherheit und strategisches Dilemma
- Komplexität des Themas
- Lösungsansatz
- Fazit

# Arbeitskreis Digitale Transformation

## Profil:

- Ständiger Arbeitskreis der Universitätskanzler\*innen
- HAWn und Musik-/Kunsthochschulen als ständige Mitglieder

## Fokus:

- Verwaltungsdigitalisierung
- Rechtliche und finanzielle Aspekte von Digitalisierungsthemen
- Bewertung von Perspektiv- und Potentialthemen

## Output u.a.:

- Vernetzung (u.a. mit HRK, KMK, RFII, Stiftung Hochschulzulassung, DFN, ZKI oder mit Projektstrukturen)
- Positionspapiere, Handreichungen, Fortbildungsveranstaltungen
- Erfahrungsaustausch und Anbahnung von Kooperationen



# Jahresbericht 2022 eines Landesrechnungshofes

*Auszug:*

„Die HOCHSCHULE X muss ihre **IT-Organisation konsolidieren**, den **Personalaufwand nachvollziehbar ermitteln** und ein hochschulweites, revisionssicheres Lizenzmanagement einführen. Zudem versäumte es das Präsidium der HOCHSCHULE X, die **internen Vorgaben zum Datenschutz, zur Informationssicherheit sowie zur Verarbeitung personenbezogener Daten stetig an die geltende Rechtslage anzupassen**.

Auch das Ministerium für Wissenschaft und Kultur versäumte es, auf rechtzeitige Anpassungen der hochschulinternen Regelungen zu IT-Sicherheit und Datenschutz hinzuwirken.“

# Berührungspunkte der Kanzler\*innen zum Thema

- Als Mitglied der Hochschulleitung mitverantwortlich für die strategische Entwicklung der Hochschule
- Verantwortlich für die Verwaltungsprozesse und deren Daten
- Verantwortlich für den
  - internen Rechtsrahmen
  - Organisationsfragen und die „richtige“ Verantwortungsdelegation bei dezentraler IT
  - Personalmanagement: Fachkräfte finden und binden
- Z.T. Mitglied im CIO-Board oder auch direkt verantwortlich für die IT
- Verantwortlich für die
  - Finanzierung
  - Wirtschaftlichkeit
  - Risikomanagementsysteme

**→ Verantwortung und Mitgestaltung der Prioritäten auch im Kontext IT-Sicherheit!**

# Angriffe auf Hochschulen sind eine reale Gefahr

IT-Menschenrechte e.V. / Cyberangriffe

|          |                                                                                                                                                                                                    |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Februar  | Université de Neuchâtel, Cyberangriff<br>Hochschule Anhalt, Cyberangriff                                                                                                                           |
| März     | Technische Hochschule Aschaffenburg, Cyberangriff                                                                                                                                                  |
| April    | Universitätsbibliothek Leipzig, Unbefugter Datenzugriff<br>Hochschule für Technik und Wirtschaft Berlin, Cyberangriff                                                                              |
| Mai      | AMC Wirtschaftsakademie GmbH, Cyberangriff                                                                                                                                                         |
| Juni     | Pädagogische Hochschule Freiburg, Cyberangriff<br>Medizinische Universität Innsbruck, Cyberangriff<br>FH Münster, Cyberangriff                                                                     |
| Juli     | Bergische Universität Wuppertal, Cyberangriff<br>Technische Universität Braunschweig, Cyberangriff                                                                                                 |
| Oktober  | Hochschule Ansbach, Cyberangriff<br>Hochschule für Technik, Wirtschaft und Kultur Leipzig, Cyberangriff<br>Hochschule Heilbronn, Cyberangriff<br>Technische Universität Braunschweig, Cyberangriff |
| November | Technische Hochschule Ulm, unbefugter Zugriff<br>Uni Duisburg-Essen, Cyberangriff                                                                                                                  |
| Dezember | Uni Duisburg-Essen, DDoS-Attacke<br>FH Zwickau, Cyberangriff<br>Hochschule für Angewandte Wissenschaften Hamburg, Cyberangriff                                                                     |



Angriffe auf Hochschulen von Januar 2021 bis Februar 2023  
Zusammenstellung aus Pressemitteilungen und medialer  
Berichterstattung

📍 2023 📍 2022 📍 2021



Technische  
Universität  
Braunschweig

# Informationssicherheit (IS) ist für Hochschulleitungen wichtig, weil wir ...

- die Aufgabenerfüllung der Hochschule erhalten wollen,
- dienstliche und personenbezogene Daten schützen wollen,
- gesetzliche Anforderungen erfüllen müssen und
- den Ruf der Hochschule bewahren wollen.



## Warum jetzt?

- auf aktuelle Bedrohungslagen reagieren müssen,
- aktuelle und zukünftige Informationssicherheitsvorfälle vermeiden müssen und
- Verwarnungen und Kontrollen (auch Vor-Ort) durch Aufsichtsbehörden vermeiden sollten.

# Dilemma beim Thema IT-Sicherheit?

## ▪ Finanzierung

Der „Kuchen“ ist an jeder Hochschule verteilt. Jedes Mehr an IT-Sicherheit führt zu einem Weniger bei anderen Leistungen. **Einschränkungen? Finanzierbarkeit?**

## ▪ Wirtschaftlichkeit

Grundsatz: Man sollte genau so viele Ressourcen einsetzen, dass es gerade reicht, um die Ziele zu erreichen. Wie viel ist genug?

**Wirkung oft nicht messbar: Wert vermiedener Katastrophen nicht bekannt.**

## ▪ Risikomanagement

- Wir wissen, dass jede Hochschule auf unterschiedlichem Niveau betroffen sein wird.
- Wir wissen nur nicht, wann der eigene Standort *massiv* betroffen sein wird.
- Wir wissen nicht, ob der Angriff genau dort stattfindet, wo wir vorgesorgt haben.
- Wir wissen, dass ein Angriff verheerend sein kann und enorme direkte (Geld) und indirekte Kosten (Reputation usw.) verursacht.
- Wir wissen auch, dass zu viele Regeln Kreativität und Flexibilität dämpfen und wir wissen, dass sich nicht alle Hochschulmitglieder daran halten werden.

# IT-Sicherheit in all ihren Dimensionen ist komplex



# Komplexität als Feind einfacher Lösungen

Übliche Managemententscheidungen sind geprägt von folgenden Ideen / Vorgehen, z.B.:

- **Benchmarking:** Wir machen das, was andere auch machen (z.B. Anlehnung an BSI-Grundschutz), ggf. Variationen → aber: Besonderheiten jeder Hochschule.
- **Finanzierungsziel:** Wir machen genau so viel, wie wir uns leisten können.  
→ aber: Das gesamte Invest kann sich als nutzlos erweisen.
- **Expertenansatz:** Wir verlassen uns auf unsere Fachleute und lassen uns Vorschläge machen.  
→ Passt die Risikoaffinität unser Fachleute und Berater\*innen zur Hochschule?
- **Projektansatz:** Man nimmt die Standardwährung „Personenjahr“ zur Bemessung und schätzt dann je nach wahrgenommener Aufgabengröße ab.  
An Unis meist: X mal E13  
→ Personalbemessung bei IT-Sicherheit herausfordernd  
(Tagessatz externer Expert\*innen ca. 2000 €)
- **Analyse:** Eine zu umfassende Analyse reduziert die zur Implementierung von Maßnahmen nötige Zeit. Ggf. ist ein schneller Start mit „quick wins“ zu bevorzugen

# Unterschiedlichkeit und Gemeinsamkeiten von Hochschulen?

- Bedrohungslage ist identisch
- Ausgangslage der Hochschulen sehr unterschiedlich
- Gesamtkosten der IT skalieren nicht linear mit Mitarbeitenden/Studierendenzahlen (vgl. v.d.Heyde 2007)
- Finanzbedarf und Risiko stehen in direkter Abhängigkeit von den gewachsenen Strukturen an den Hochschulen (vor allem dezentrale IT-Strukturen, eingesetzte Systeme)
- Große Abhängigkeit der Verfügbarkeit von geeignetem Personal; Verfügbarkeit regional unterschiedlich
- Zunehmende Ausweitung der Anfälligkeit auch auf Betriebseinrichtungen (Gebäudeautomation, Fahrstühle, Pumpen etc.)
- Einige Bundesländer unterstützen die Hochschulen durch Strukturen u/o Finanzierung
- **IT-Sicherheit ist eine Daueraufgabe**

# Anforderungen aus der Informationssicherheits-Compliance sind komplex

- **Erfüllung von Anforderungen**
  - **Gesetzliche und regulatorische Anforderungen**
    - ✓ KonTraG, HGB, AO, DSGVO, BDSG, ITSiG, KRITIS, IT-SiKat, GoBD...
  - **Vertragliche Anforderungen**
    - ✓ Kunden, Lieferanten, Projektpartner, Versicherungen...
- **Weitere Anforderungen, z.B.:**
  - Markt, Öffentlichkeit
  - Konzern, Shareholder TISAX
  - Mitarbeitende
  - Geschäftsprozesse
  - Technik
- **Begrenzung von Risiken**
  - ✓ zur Vermeidung von Sicherheitsvorfällen

# Komplexität an Maßnahmen in den Bereichen Prävention, Notfallbewältigung und in der Zeit dazwischen



# Lösungsansatz

Wie können wir eine *angemessene* IT-Sicherheit an der Hochschule etablieren?



# Strategisches Vorgehen

**IT-Sicherheitsstrategie entwickeln,**

**daraus globale IT-Sicherheitsziele ableiten,**

**Risikoanalysen erstellen,**

**Prioritäten setzen**

**und konkrete Maßnahmen planen und umsetzen.**

**→ in der Hochschulleitung zu verankern!**

## Die Einführung von IT-Sicherheitsstrategien

ist Führungsaufgabe,

bedeutet Veränderung,

wird deshalb mit hoher Wahrscheinlichkeit  
auf Akzeptanzprobleme stoßen,

die das Projekt gefährden

und bedarf deshalb eines Change-Managements.

**→ in der Hochschulleitung zu verankern!**

# Hochschulleitung: notwendiger Treiber der IT-Sicherheit

## Aktive Unterstützung notwendig

- Ohne Ihre Führung keine effektive Informationssicherheit.
- Sichern Ressourcen und Prioritäten.

## Verbündete suchen

- Zusammenarbeit mit IT-Abteilungen, Datenschutz(management), Informationssicherheit, Fakultäten, Verwaltung und externen Expert\*innen.
- Aufbau eines Sicherheitsnetzwerkes innerhalb und außerhalb der Hochschule.

## Kommunikation fördern

- Regelmäßiges Sensibilisieren und Schulen der Mitarbeitenden.
- Sicherheitsmaßnahmen transparent und verständlich kommunizieren.





**Vielen Dank für Ihre Aufmerksamkeit!**



**Technische  
Universität  
Braunschweig**