HRK

Informationssicherheit als strategische Aufgabe der Hochschulleitung

Prof. Dr. M. Gross

Herausforderungen für Hochschulleitungen im Digitalen Zeitalter - Empfehlungen der HRK

- Informationskompetenz (HRK 2012)
- Digitale Lehre (HRK 2014)
- Forschungsdatenmanagement (HRK 2015)
- Informationssicherheit (HRK 2018)

Ausgangspunkt dieser Tagung

Empfehlung der 19. Mitgliederversammlung der HRK am 10. November 2015 in Kiel

„Wie Hochschulleitungen die Entwicklung des Forschungsdatenmanagements steuern können - Orientierungspfade, Handlungsoptionen, Szenarien“

Empfehlung der 25. Mitgliederversammlung der HRK am 6. November 2018 in Lüneburg

„Informationssicherheit als strategische Aufgabe der Hochschulleitung“

Empfehlung der HRK Mitgliederversammlung vom 6. November 2018

I. **Informationssicherheit als Herausforderung für Hochschulen**

II. **Die strategische Aufgabe der Hochschulleitung**

III. **Leitlinien für Prozesse zur Informationssicherheit**

Informationssicherheit

- Verlust der Integrität und Verfügbarkeit von **Forschungsdaten**
- Kompromittierung von **personenbezogenen Daten**, insbesondere von Studierendendaten
- Verlust der Vertraulichkeit von **Daten innerhalb von Kooperationen,** beispielsweise durch Spionage**.**

➢ **Hochschulen sind angreifbar, verwundbar**

Die strategische Aufgabe der Hochschulleitung

I. Informationssicherheit umfasst mehr als IT-Sicherheit

II. Informationssicherheit als übergreifende Gestaltungsaufgaben

III. Verantwortlichkeit für Organisation und Governance

IV. Rechtlicher Rahmen

I. Informationssicherheit umfasst mehr als IT-Sicherheit (a)

- Datenschutzbeauftragte kümmern sich um **personenbezogenen** Daten

I. Informationssicherheit umfasst mehr als IT-Sicherheit (a)

- Datenschutzbeauftragte kümmern sich um **personenbezogenen** Daten

- **IT Sicherheit** ist verantwortlich für die technische Sicherheit der IT in einer Organisation

I. Informationssicherheit umfasst mehr als IT-Sicherheit (a)

- Datenschutzbeauftragte kümmern sich um **personenbezogenen** Daten

- **IT Sicherheit** ist verantwortlich für die technische Sicherheit der IT in einer Organisation

- **Informationssicherheit** verfolgt, unabhängig von der Art der Daten, die

  Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Verbindlichkeit, Revisionsfähigkeit und Transparenz der Daten

I. Informationssicherheit umfasst mehr als IT-Sicherheit (b)

- **Vertraulichkeit:** Sind Ihre Daten und Informationen vor dem Zugriff Unberechtigter geschützt? Können nur Befugte Ihre Daten einsehen und bearbeiten?
- **Integrität:** Bleibt die Korrektheit Ihrer Daten während der Verarbeitung vollständig und aktuell?
- **Verfügbarkeit:** Können Ihre Daten bei Bedarf zeitgerecht und ordnungsgemäß genutzt und verarbeitet werden?
- **Authentizität**: Können die Daten jederzeit ihrem Ursprung eindeutig zugeordnet werden?

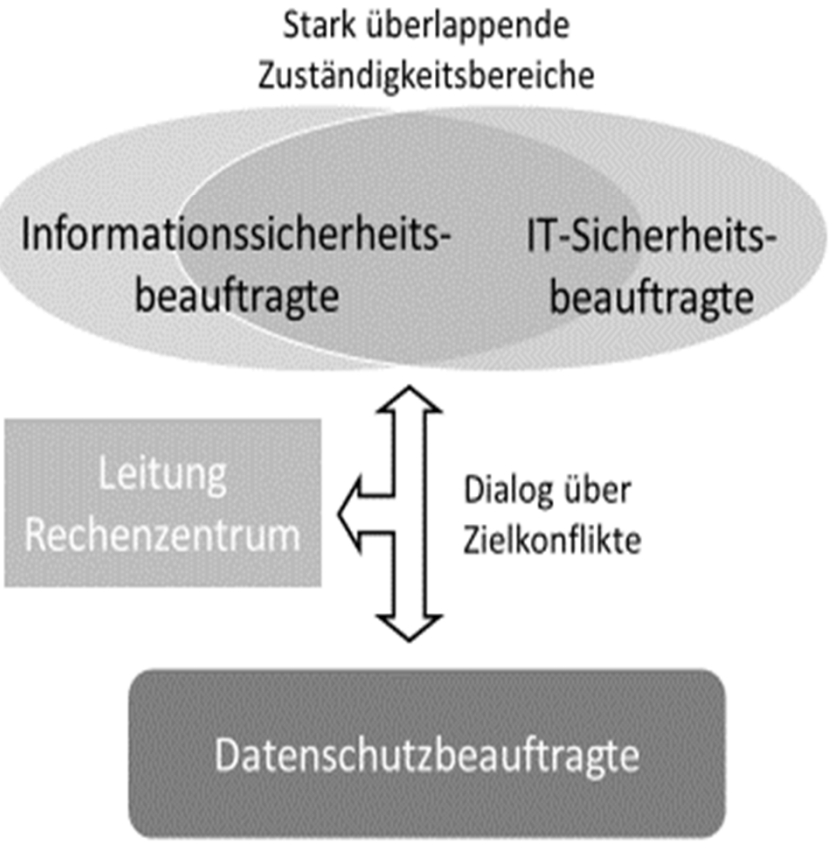
I. Informationssicherheit umfasst mehr als IT-Sicherheit (c)

- **Verbindlichkeit:** Die Beteiligung von Nutzenden und Systemen an einer IT-Transaktion kann eindeutig nachgewiesen werden.
- **Revisionsfähigkeit**: Die rechtssichere Nachweisfähigkeit über Herkunft von Daten sowie deren Verarbeitung und der jeweils daran Beteiligten muss gegeben sein.
- **Transparenz:** Verfahrensweisen bei der Verarbeitung von Daten sind vollständig, aktuell und in einer Weise dokumentiert, dass sie nachvollzogen werden können.

II. Informationssicherheit als übergreifende Gestaltungsaufgaben

- Sensibilisierung und Qualifizierung der HS Angehörigen
- Umfasst alle Bereiche von Lehre, Forschung und Verwaltung
- Technische Herausforderung sowie Organisationsentwicklung
- Aufwand der Maßnahme in Relation zu Sicherheitsgewinn sowie dem zu schützenden Gut

III. Verantwortlichkeit für Organisation und Governance



III. Verantwortlichkeit für Organisation und Governance

Klärung von differenzierten Verantwortlichkeiten

- Unterstüzung von differenzierten Rollenmodellen durch sogenannte RACI-Charts (für „**R**esponsible, **A**ccountable, **C**onsulted, **I**nformed“)

- Unterscheidung zwischen Durchführungsverantwortung und Rechenschaftspflicht/Gesamtverantwortung!

IV. Rechtlicher Rahmen

- Informationssicherheit und Datenschutz muss immer zusammen betrachtet werden

  - **Informationssicherheit** bewertet Risiken für die Hochschule als Organisation
  - **Datenschutz** betrachtet die Risiken der Verletzung der informationellen Selbstbestimmung der in der Hochschule und ihrem Umfeld tätigen Personen

Die strategische Aufgabe der Hochschulleitung (Fortsetzung) (siehe Empfehlung)

V. Erstellung und Fortschreibung eines Informationssicherheitskonzeptes

VI. Umgang mit Störfällen

VII. Ressourcen

VIII. Kooperationen für Informationssicherheit

IX. Zertifizierungen und Audits

Die strategische Aufgabe der Hochschulleitung **(Fortsetzung)** (siehe Empfehlung)

V. Erstellung und Fortschreibung eines Informationssicherheitskonzeptes

VI. Umgang mit Störfällen

VII. **Ressourcen**

VIII. Kooperationen für Informationssicherheit

IX. Zertifizierungen und Audits

VII. Ressourcen

Unterstützung nutzen!

- Deutschen Forschungsnetz (DFN)
- Arbeitskreis Informationssicherheit in Forschungseinrichtungen (AKIF)
- Bundesamt für Sicherheit in der Informationstechnik (BSI)

Leitlinien für Prozesse zur Informationssicherheit (I)

	Dos	Don'ts
Relevanz	⊕ Informationssicherheit als umfassendes gestalterisches und kulturelles Gut betrachten.	⊖ Informationssicherheit als bloße technische Herausforderung betrachten.
Schutz-maßnahmen	⊕ Aufwand für Schutzmaßnahmen immer in Relation zum erzielten Sicherheitsgewinn und dem Wert der zu schützenden Güter setzen.	⊖ Schutzmaßnahmen kontextlos maximieren.
Mandatierung	⊕ Informationssicherheitsbeauftragte offiziell und formell bestellen.	⊖ Informationssicherheitsbeauftragte informell benennen.

Leitlinien für Prozesse zur Informationssicherheit (II)

	Dos	Don'ts
Doppel-funktionen	⊕ Informationssicherheitsbeauftragte und Rechenzentrumsleitung sowie Datenschutz- und Informationssicherheitsbeauftragte sollen Zielkonflikte dialogisch austragen können.	⊖ Personalunion zwischen Informationssicherheitsbeauftragten und Rechenzentrumsleitung sowie Datenschutz- und Informationssicherheitsbeauftragten.
Rechtlicher Rahmen	⊕ Rechtsbegriffe in den Kontext der technischen Entwicklung und der Belange der Hochschule stellen.	⊖ Rechtliche Vorgaben kontextlos betrachten und verfolgen.
Informations-sicherheits-konzept	⊕ Informationssicherheitskonzept ist Hilfsmittel für Risikobewertung und -behandlung.	⊖ Kurzatmig ein Informationssicherheitskonzept erstellen, das nur Soll-Zustände dokumentiert, die stark vom Ist-Zustand divergieren.

Leitlinien für Prozesse zur Informationssicherheit (III)

	Dos	Don'ts
Prozessziele	⊕ Kurzfristig erreichbare Teilziele formulieren und aufeinander aufbauend in Kraft setzen.	⊖ Idealtypischen Masterplan stufenlos umsetzen.
Umgang mit Störfällen	⊕ Möglichst hohen Grad an Resilienz anstreben.	⊖ Nach hundertprozentiger Sicherheit streben.
Kommunikation bei Störfällen	⊕ Meldepflichten beachten, mit der für Kommunikation und Pressearbeit betrauten Stelle abstimmen.	⊖ Information unterdrücken.
Unterstützung	⊕ Unterstützung auch von institutionellen Dienstleistern (z.B. DFN) nutzen.	⊖ Nur auf interne Expertise zurückgreifen.

Leitlinien für Prozesse zur Informationssicherheit (IV)

	Dos	Don'ts
Ressourcen	⊕ Ressourcen ins Verhältnis zur angestrebten Reichweite und Komplexität setzen.	⊖ Ressourcen als unabdingbare Voraussetzung für jedwede Zielerreichung betrachten.
Kooperationen	⊕ Synergieeffekte nutzen und dabei eigene Verantwortlichkeit beibehalten.	⊖ Kooperationsstrukturen als Entlastung von eigener Verantwortung begreifen.
Zertifizierungen	⊕ Zertifizierungen mit Blick auf mögliche institutionelle Mehrwerte anstreben.	⊖ Zertifizierungen als Selbstzweck verfolgen.

Ziel dieses HRK Workshops
Diskussion mit den Verantwortlichen der HSen

- Welche Strategie passt zu Ihrer Hochschule?
- Wo liegen die Chancen und Risiken für Forschung und Lehre?
- Welche Ansatzpunkte gibt es für die Umsetzung der Strategien?
- Welche Vernetzungen sind möglich?

HRK

Vielen Dank für Ihre Aufmerksamkeit!