Empfehlung der
25. Mitgliederversammlung
der HRK
am 06. November 2018
in Lüneburg

Informationssicherheit als strategische Aufgabe der Hochschulleitung

HRK Hochschulrektorenkonferenz

Die Stimme der Hochschulen

Leipziger Platz 11 Tel.: 030 206292-0 post@hrk.de
10117 Berlin Fax: 030 206292-15 www.hrk.de

Ahrstraße 39 Tel.: 0228/887-0 post@hrk.de
D-53175 Bonn Fax: 0228/887-110 www.hrk.de

Inhaltsverzeichnis

Präambel

Dieses Papier besteht im ersten Teil aus einer Empfehlung für die Hochschulleitungen und im zweiten Teil aus einer Handreichung auch für die mittlere Leitungsebene. Die Kombination dieser beiden Teile soll dazu beitragen, sowohl die Relevanz des Themas „Informationssicherheit" als auch Ansätze für Umsetzungsmaßnahmen zu vermitteln.

Teil A: Zusammenfassung für Hochschulleitungen

I. Informationssicherheit als Herausforderung für Hochschulen

Hochschulen sind wie auch andere Organisationen wachsenden Gefahren und Risiken für Information und Wissen ausgesetzt. Diese Gefahren und Risiken betreffen die Kernaufgaben Lehre, Forschung und Wissenstransfer in spezifischer Weise, insbesondere hinsichtlich

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

Dabei sind Hochschulen in besonderer Weise verwundbar: Die Freiheit von Forschung und Lehre, die weltweite Zusammenarbeit auf Basis fachlichen Austauschs, eine weitgehende Autonomie von Teileinheiten, die häufige Projektförmigkeit,die hohe Personalfluktuation, die verschiedenen Statusgruppen mit ihren unterschiedlichen Rollen und Rechten und die schnellen Entwicklungszyklen der Informationstechnik tragen dazu bei. Informationssicherheit bedeutet daher für die Hochschulen eine erhebliche Herausforderung.

Die Hochschulen haben in den vergangenen Jahren beachtliche Anstrengungen zur Absicherung ihrer Informationsverarbeitung unternommen.[1] In einer aktuellen Erhebung des Arbeitskreises Informationssicherheit der deutschen Forschungseinrichtungen[2] (AKIF) haben mehr als einhundert Hochschulen über den Status Quo ihrer Aktivitäten zur Informationssicherheit Auskunft gegeben. Anerkannt wird sowohl die hohe Relevanz dieses Themas als auch der mit der fortschreitenden Digitalisierung weiter ansteigende Handlungsbedarf. Entsprechend widmen sich viele Hochschulen dem Thema, ihre Sicherheitsstrategie fortzuentwickeln, ausgehend von einem enger gefassten IT-Sicherheitsbegriff hin zu einem weitergefassten wissenschaftsadäquaten Informationssicherheitsverständnis.

[1] Siehe auch HRK-Rundschreiben Nr. 24/2014 „IT-Sicherheit an Hochschulen und Forschungseinrichtungen" mit der Anlage „Bedeutung der IT-Sicherheit an wissenschaftlichen Einrichtungen" der Allianz der Wissenschaftsorganisationen.

[2] Der Arbeitskreis Informationssicherheit der deutschen Forschungseinrichtungen ist ein Arbeitskreis der Allianz der Wissenschaftsorganisationen, siehe auch https://www.ak-if.de/.

II. Die strategische Aufgabe der Hochschulleitung

Im wissenschaftlichen Umfeld zielt der Begriff „Informationssicherheit" vorrangig auf die Aspekte Integrität, Vertraulichkeit sowie Verfügbarkeit und Austausch von Informationen. Informationssicherheit unterscheidet sich von IT-Sicherheit darin, dass das zu schützende Gut „Information" und die zugehörigen informationsverarbeitenden Prozesse in den Vordergrund der Risikobewertung und -behandlung gestellt werden.

Informationssicherheit als Aspekt der Prozessqualität in der Hochschule zu verankern, ist nicht nur rechtlich gefordert, sondern auch eine Gestaltungsaufgabe im Rahmen der Governance-Struktur und der institutionellen Awareness[3]. Die Hochschulleitungen müssen diese Aspekte, die auch die Kultur von Forschung und Lehre umfassen, aktiv aufgreifen. Diese gestalterischen und kulturellen Dimensionen können in ihrer Gesamtheit nur von der Hochschulleitung zusammengeführt, bewertet und adressiert werden. Informationssicherheit ist somit eine originär strategische Aufgabe der Hochschulleitung und verlangt eine Einbettung in sämtliche Prozesse der Hochschule. Dabei sind Schutzmaßnahmen stets in Relation zum erzielten Sicherheitsgewinn und dem Wert der zu schützenden Güter zu setzen, weil sich nur so auf Dauer das Bedürfnis nach Sicherheit und die Freiheit von Forschung, Lehre und künstlerischer Entwicklungsvorhaben miteinander vereinbaren lassen.

Die Verantwortung der Hochschulleitung für Informationssicherheit erstreckt sich insbesondere darauf, funktionierende Strukturen für Planung, Umsetzung, Überprüfung und Verbesserung der Informationssicherheit zu schaffen. In diesen Strukturen müssen die Fachseite und die Betreiber der informationstechnischen Infrastruktur zusammenwirken wie auch die Beziehungen zu und zwischen Datenschutz, IT-Sicherheit, Justiziariat, Präsidium, Pressestelle und Vorfallsmeldestellen geregelt sein. Für die Erreichung des angestrebten Sicherheitsniveaus müssen ausreichende Ressourcen zur Verfügung gestellt werden.

Die Wahrnehmung der Verantwortung für Informationssicherheit wird – wie auch beim Thema Datenschutz – nach außen vor allem durch

- benannte Verfahrensverantwortliche
- geregelte Meldewege und Vorhandensein eines Reaktionsteams
- ein geregeltes Risikomanagement
- die Dokumentation von Sicherheitsstrategie und -maßnahmen in Form einer Leitlinie und eines Informationssicherheitskonzepts
- einen kontinuierlichen Verbesserungsprozess

belegt. Melde-, Reaktions- und Dokumentationspflichten sowie das Risikomanagement werden sinnvollerweise für Informationssicherheit, IT-Sicherheit und Datenschutz in abgestimmter Weise erfüllt. Das tatsächlich

[3] Der Begriff „Awareness" wird hier bewusst verwendet, weil die deutschen Entsprechungen „Bewusstsein", „Gewahrsein", „Bewusstheit", „Aufmerksamkeit" oder auch „Sensibilisierung" nicht so treffend sind.

erzielte Sicherheitsniveau hängt maßgeblich von der Awareness für Informationssicherheit innerhalb der Hochschule, von der vorhandenen Expertise in IT-Sicherheit und dem erfolgreichen Zusammenspiel der oben ausgeführten Strukturen ab.

III. Leitlinien für Prozesse zur Informationssicherheit

Die nachfolgende Handreichung vermittelt verallgemeinerbare Leitlinien in der Form von „Dos" und „Don'ts":

	Dos	Don'ts
Relevanz	⊕ Informationssicherheit als umfassendes gestalterisches und kulturelles Gut betrachten.	⊖ Informationssicherheit als bloße technische Herausforderung betrachten.
Schutzmaßnahmen	⊕ 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.
Doppelfunktionen	⊕ 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.
Informationssicherheitskonzept	⊕ Informationssicherheitskonzept ist Hilfsmittel für Risikobewertung und -behandlung	⊖ Kurzatmig ein Informationssicherheitskonzept erstellen, das nur Soll-Zustände dokumentiert, die stark vom Ist-Zustand divergieren
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.
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.

Teil B: Handreichung

Vorbemerkung
Diese Handreichung soll eine Orientierungshilfe für diejenigen Personen sein, die mit der Umsetzung von entsprechenden Prozessen betraut sind. In diesem Sinne umfasst die Handreichung u.a. Ausführungen sowie Vorschläge und Handlungshinweise.

Entsprechend der Komplexität des Themas Informationssicherheit und der Heterogenität der Hochschulen kann naturgemäß kein einheitliches Lösungsmodell skizziert werden. Der Handreichung liegt aber die Leitidee eines schrittweisen Vorgehens zugrunde. Grundsätzlich gilt, dass es keine vollständige Sicherheit gibt und daher der Umgang mit Vorfällen geregelt und geübt sowie die Umsetzung von Maßnahmen risikobasiert priorisiert wird.

I. Informationssicherheit als Herausforderung für Hochschulen

Wissenschaft braucht Vertrauen. Dies gilt sowohl für Forschung und Lehre als auch darauf aufbauend für den Transfer in die Gesellschaft, mithin Kernaufgaben der Hochschulen. Gerade im Zuge der Digitalisierung ist die Informationssicherheit daher eine unabdingbare Voraussetzung für das wissenschaftliche Arbeiten und das Vertrauen in die Wissenschaft.

Hochschulen sind wie auch andere Organisationen wachsenden Gefahren und Risiken für Information und Wissen ausgesetzt. Diese Gefahren und Risiken betreffen die Kernaufgaben Lehre, Forschung und Wissenstransfer in spezifischer Weise, insbesondere hinsichtlich

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

So gibt es beispielsweise Einfallstore für aktuelle Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten zu gelangen („Phishing"): Dabei können Zugangsdaten für Forschungszwecke, für Prüfungen von Studierenden oder auch für administrative Management-Instrumente Ziele solcher Phishing-Angriffe sein. Eine reale Gefahr ist Phishing auch im Zusammenhang mit Spionage-Aktivitäten. Ein weiteres bedrohliches Szenario besteht in der Infizierung und Sperrung von Rechnern, um dann Geld für die Entsperrung zu verlangen („Ransomware"). Gelingt z.B. die Infizierung oder Sperrung eines zentralen Hochschulrechners, so könnten blitzartig Forschungs-, Studien- und Verwaltungsaktivitäten zum Erliegen kommen und darüber hinaus auch sensible Daten verloren gehen. Ähnliche Folgen können eintreten, wenn Externe die Hochschulinfrastruktur für Botnetze nutzen.

Hochschulen sind in besonderer Weise verwundbar: Die Freiheit von Forschung und Lehre, die weltweite Zusammenarbeit auf Basis fachlichen

Austauschs, die weitgehende Autonomie der Teileinheiten, die häufige Projektförmigkeit, die hohe Personalfluktuation, die verschiedenen Statusgruppen mit ihren unterschiedlichen Rollen und Rechten und die schnellen Entwicklungszyklen der Informationstechnik tragen dazu bei. Informationssicherheit bedeutet daher für die Hochschulen eine erhebliche Herausforderung.

In einer aktuellen Erhebung des „Arbeitskreises Informationssicherheit der deutschen Forschungseinrichtungen (AKIF) haben mehr als einhundert Hochschulen über den Status Quo ihrer Aktivitäten zur Informationssicherheit Auskunft gegeben. Anerkannt wird sowohl die hohe Relevanz dieses Themas als auch der mit der fortschreitenden Digitalisierung weiter ansteigende Handlungsbedarf. Entsprechend widmen sich sehr viele Hochschulen diesem Thema, ausgehend von einem enger gefassten IT-Sicherheitsbegriff hin zu einem weitergefassten wissenschaftsadäquaten Informationssicherheitsverständnis.

Eine Konkretisierung solcher Herausforderungen vor allem im Hinblick auf den Schutz personenbezogener Daten und die diesbezüglichen Nachweispflichten ergibt sich aus der am 25. Mai 2018 in Kraft getretenen EU-Datenschutz-Grundverordnung (DSGVO). Die DSGVO führt insbesondere erweiterte Dokumentations- und Meldepflichten ein. Dabei können Synergien für den Datenschutz und für die Informationssicherheit genutzt werden, die unterschiedlichen Ausrichtungen müssen aber beachtet werden.

II. Die Aufgabe der Hochschulleitung

1. Informationssicherheit umfasst mehr als IT-Sicherheit

Der Begriff der „Informationssicherheit" wird durch verschiedene Standardisierungsorganisationen definiert (siehe nachstehend die Definition nach ISO/IEC/DIN), doch heben diese Definitionen meist auf ein allgemeines Unternehmensumfeld ab. Für die Wissenschaft und ihre Arbeitsweise – und die Hochschulen im Besonderen – ist eine wissenschaftsbezogene Auslegung hinsichtlich Zielsetzung und Behandlung erforderlich.

Definition „Informationssicherheit" nach DIN/ISO/IEC 27000:2015
2.33 Informationssicherheit (en: information security)
Aufrechterhaltung der Vertraulichkeit (2.12), Integrität (2.40) und Verfügbarkeit (2.9) von Information;
Anmerkung zum Begriff: Zusätzlich können auch andere Eigenschaften wie Authentizität (2.8), Zurechenbarkeit, Nichtabstreitbarkeit (2.54) und Verlässlichkeit (2.62) einbezogen werden.

Informationssicherheit umfasst drei Hauptaspekte: Vertraulichkeit, Verfügbarkeit und Integrität. Informationssicherheit bedingt die Anwendung und das Management von angemessenen Sicherheitsmaßnahmen unter Berücksichtigung einer großen Bandbreite von Bedrohungen mit dem Ziel, anhaltenden geschäftlichen Erfolg und einen kontinuierlichen Geschäftsbetrieb (Business Continuity) sicherzustellen und Beeinträchtigungen durch Informationssicherheitsvorfälle zu minimieren. Informationssicherheit wird durch die Umsetzung eines geeigneten Maßnahmenkatalogs erreicht, die durch den festgelegten Risikomanagementprozess ausgewählt und mit Hilfe eines ISMS[4] gesteuert werden, das Richtlinien, Prozesse, Verfahren, Organisationsstrukturen, Software und Hardware zum Schutz von identifizierten Informationswerten umfasst. Diese Maßnahmen müssen festgelegt, umgesetzt, überwacht, überprüft und wo notwendig verbessert werden, um sicherzustellen, dass die spezifischen Informationssicherheits- und Geschäftsziele der Organisation erreicht werden. Es wird erwartet, dass relevante Informationssicherheitsmaßnahmen nahtlos in die Geschäftsprozesse der Organisation integriert werden.

Der Maßstab „Qualität" und damit verbunden die Qualitätssicherung spielen eine herausragende Rolle in der Wissenschaft. Belastbare Daten müssen daher sowohl den Erfordernissen der Qualitätssicherung als auch der Informationssicherheit genügen. Zudem agieren Hochschulen in einem globalen Umfeld und befinden sich in offenem Austausch mit der Gesellschaft. Hieraus ergibt sich für die Hochschulen ein Spannungsfeld, welches deutlich macht, dass zwischen den Schutzzielen abwogen werden muss:

- Einerseits impliziert das Postulat einer „Offenheit", von digitalen Forschungsprozessen, -methoden und -ergebnissen (Open Access, Open Science, Open Data) und von Lehrinhalten (Open Educational Resources), dass die Schutzziele Integrität und Verfügbarkeit einen besonders hervorgehobenen Stellenwert haben.
- Andererseits besteht auch der Wunsch nach Vertraulichkeit, der sich aus der Notwendigkeit von geschützten Bereichen für die wissenschaftliche Zusammenarbeit und nicht zuletzt aus dem wissenschaftlichen Wettbewerb ergibt.

[4] Informationssicherheits-Managementsystem.

Die notwendigen Abwägungen hinsichtlich der Schutzzielbildung und Risikoeinschätzung können nur aus der Wissenschaft selbst – selbstverständlich im Rahmen der geltenden Gesetze – getroffen werden. Informationssicherheit unterscheidet sich somit von IT-Sicherheit darin, dass das zu schützende Gut „Information" und die zugehörigen informationsverarbeitenden Prozesse in Forschung, Lehre und Wissenstransfer in den Vordergrund der Risikobewertung und -behandlung gestellt werden.

Die Behandlung des Themenfelds Informationssicherheit kann dementsprechend nur durch Zusammenwirken der Fachseite (Forschung, Lehre, Wissenstransfer, Administration) mit der IT-Seite erfolgen. Insbesondere die Entwicklung von Rahmenbedingungen für Prozesstransparenz sowie Verhaltensregeln in Form von Leit- und Richtlinien müssen von der Hochschule gestaltet und getragen werden und können nicht alleine Aufgabe des operativen IT-Dienstleisters sein. Dabei muss das Tragen von Risikoentscheidungen in die Prozesse der Hochschule intergiert werden. Die Aufgabe, Informationssicherheit als Aspekt der Prozessqualität in der Organisation Hochschule zu verankern, beschränkt sich somit nicht nur auf die Herstellung von IT-Sicherheit im engeren Sinn. Informationssicherheit ist nicht nur rechtlich gefordert, sondern vielmehr Teil einer übergreifenden Gestaltungsaufgabe im Rahmen der institutionellen Awareness[5] und der Governance-Strukturen und -Prozesse.

2. Informationssicherheit als übergreifende Gestaltungsaufgabe

Bei der Etablierung von institutioneller Awareness für Informationssicherheit geht es vor allem darum, Hochschulangehörige zu sensibilisieren und zu qualifizieren. Es gilt zu vermitteln, dass gerade im Bereich der Informationssicherheit jede Person ihren Beitrag leisten kann. Dieses institutionelle Bewusstsein kann nur dann erfolgreich sein, wenn es nicht nur konzipiert und implementiert, sondern gelebt, also kontinuierlich erprobt und verbessert wird. Zu dessen nachhaltiger Förderung ist es unerlässlich, dass das Thema Informationssicherheit auch als Bildungsauftrag wahrgenommen und entsprechend in der Lehre adressiert wird.

Maßnahmen zur Awareness
Maßnahmen zur Awareness sollten sowohl die Beschäftigten als auch die Studierenden als Zielgruppe ansprechen. Möglich sind Ideenwettbewerbe, Vorträge sowie Info-Stände mit Postern, Flyern, personalisierten Passwortkarten, und Give-Aways. Entsprechende Informationen können auch auf der hochschuleigenen Website oder hochschuleigenen Newslettern oder Studierendenzeitschriften verbreitet werden. Zum Thema Phishing sind Online-Selbstlerntests und auch eine Phishing-Beratung denkbar.

Die Hochschulleitungen müssen das Thema Awareness mit den diversen Aspekten, die auch die Kultur von Forschung und Lehre umfassen, aktiv aufgreifen. Diese gestalterischen und kulturellen Dimensionen können in

[5] Der Begriff „Awareness" wird hier bewusst verwendet, weil die deutschen Entsprechungen „Bewusstsein", „Gewahrsein", „Bewusstheit", „Aufmerksamkeit" oder auch „Sensibilisierung" nicht so treffend sind.

ihrer Gesamtheit nur von der Hochschulleitung zusammengeführt, bewertet und adressiert werden. Informationssicherheit ist somit eine originär strategische Aufgabe der Hochschulleitung. Informationssicherheit darf nicht als bloße technische Herausforderung, sondern muss als umfassende Aufgabe der Organisationsentwicklung betrachtet werden.

Für die Hochschule insgesamt, aber auch für ihre Teileinheiten müssen als Referenzpunkte für die Informationssicherheit immer die Kernprozesse der jeweiligen Einheiten sein. Schutzmaßnahmen dürfen daher nicht kontextlos maximiert werden: Der Aufwand für die Schutzmaßnahmen ist stets in Relation zum erzielten Sicherheitsgewinn und dem Wert der zu schützenden Güter zu setzen, weil sich nur so auf Dauer das Bedürfnis nach Sicherheit und die Freiheit der Forschung, Lehre und künstlerischen Entwicklungsvorhaben miteinander vereinbaren lassen. Für die Bestimmung der akzeptierten Risiken muss eine entscheidungsfähige Organisation und Governance vorhanden sein.

3. Verantwortlichkeit für Organisation und Governance

Die Verantwortung der Hochschulleitung für Informationssicherheit erstreckt sich vor allem darauf, funktionierende Strukturen zu schaffen bzw. zu erhalten sowie ausreichende Ressourcen für die Erreichung des angestrebten Sicherheitsniveaus zur Verfügung zu stellen.

Während die Hochschulleitung die Verantwortung für die Informationssicherheit trägt, wird die Organisation und Durchführung des Informationssicherheitsmanagements an einen nachgeordneten Verfahrensverantwortlichen oder Beauftragten wie Chief Information Security Officers (CISO) oder Informationssicherheitsbeauftragte (ISB) delegiert, die in einer Stabstelle bei der Hochschulleitung angesiedelt werden können. In diesem Zusammenhang ist es für die Legitimation der Position wichtig, dass die Hochschulleitung anstelle einer informellen Benennung das entsprechende Mandat offiziell und formell erteilt. Verfahrensverantwortliche sollten etwaige Zielkonflikte mit den Leitungen von internen Hochschuleinheiten dialogisch austragen können. Daher erscheint z.B. eine Personalunion zwischen Beauftragung für Informationssicherheit und Leitung eines Rechenzentrums als nicht ratsam. Ebenso sollte eine Person nicht gleichzeitig Datenschutz- und Informationssicherheitsbeauftragte sein. Ein CISO/ISB trägt insbesondere die Verantwortung für das so genannte Informationssicherheitskonzept, also für die Dokumentation der Informationssicherheitsrisiken sowie zugehöriger durchgeführter und geplanter Maßnahmen.

Das Zusammenwirken von Informationssicherheit, Datenschutz und operativer IT-Sicherheit sowie mit Hochschulleitung, Justiziariat, Notfallzentrale und Pressestelle muss geregelt, beschrieben und vermittelbar sein. Hierbei bestehen naturgemäß Überlappungsbereiche, die im günstigen Falle das Zusammenwirken in den Hochschulen befördern. Ebenso besteht eine Herausforderung darin, dass die Informationssicherheit als Prozess betrachtet sich selbst wieder in allen Prozessen der Hochschule wiederfindet. Somit ist auf der einen Seite die gesamte Aufbauorganisation

betroffen, auf der anderen Seite sind klare Entscheidungswege und Verantwortungsübernahmen für die Handlungsfähigkeit hinsichtlich Informationssicherheit erforderlich.

Trotz der Heterogenität in der Hochschullandschaft in Bezug auf Governance im Allgemeinen und in Bezug auf die Governance der Informationsverarbeitung und -versorgung im Besonderen ist es möglich, allgemeine Prinzipien an lokale Gegebenheiten anzupassen. Allerdings kann festgestellt werden, dass Klarheit in Bezug auf die Übernahme von Rechten/Pflichten und Verantwortung insbesondere hinsichtlich dezentraler und zentraler Aufteilung sowie in Bezug zu Risikobewertung und Risikoakzeptanzentscheidung herzustellen ist.

Vorgehensweise zur Klärung von Verantwortlichkeiten: RACI-Charts
Differenzierte Rollenmodelle können durch sogenannte RACI-Charts und daraus abgeleiteter Varianten unterstützt werden. RACI (für „Responsible, Accountable, Consulted, Informed") unterscheidet bspw. zwischen Durchführungsverantwortung und Rechenschaftspflicht/Gesamtverantwortung. Vielfältige Varianten dazu existieren in der Literatur. Dieses Klären von differenzierten Verantwortlichkeiten hinsichtlich Informationssicherheit in Kern- und Unterstützungsprozessen von Lehre, Forschung, Wissenstransfer und Administrations hilft auch einem sukzessiven Vorgehen, welches Prozesse nach ihrer Priorität behandelt.

Zudem kann grundsätzlich darüber entschieden werden, inwieweit sich einzelne Statusgruppen beim Eintritt in die Hochschule schriftlich zur Einhaltung der Regeln zur Informationssicherheit sowie zur Qualifizierung in Sachen Informationssicherheit verpflichten müssen. Das „Onboarding" bietet sich auch als Gelegenheit für Awareness-Maßnahmen an.

4. Rechtlicher Rahmen

Aus rechtlicher Perspektive müssen Informationssicherheit und Datenschutz immer zusammen, aber dialogisch, betrachtet werden. Während aus der Perspektive der Informationssicherheit Risiken für die Hochschule als Organisation bewertet werden, richtet der Datenschutz sein Augenmerk auf die Risiken der Verletzung der informationellen Selbstbestimmung der in der Hochschule und ihrem Umfeld tätigen natürlichen Personen wie Studierenden, Wissenschaftlerinnen und Wissenschaftlern, Angestellten und Probanden. Datenschutzrisiken können Informationsrisiken beinhalten wie auch Informationsrisiken zu Datenschutzrisiken führen können. Die Arten der Klassifikation und die Ableitungen der Risikobehandlung aber können aufgrund der unterschiedlichen Perspektiven differieren. Auch abseits datenschutzrelevanter Vorgänge bestehen Anforderungen an die Informationssicherheit, insbesondere hinsichtlich Vertraulichkeit, etwa in Bezug auf Urheberrecht und Patentschutz sowie Geheimhaltungsverpflichtungen im Rahmen von Kooperationsverträgen.

Maßgebliche Rechtsnormen sind für die Informationssicherheit das aufgrund der EU-Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS) novellierte IT-Sicherheitsgesetz und für den Datenschutz die o.g. EU-Datenschutz-Grundverordnung (EU-DS-GVO). Weitere einschlägige Rechtsnormen sind u.a. das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz), das Telemediengesetz und Telekommunikationsgesetz, Landesdatenschutzgesetze, das Strafrecht sowie untergesetzliche ggf. landesspezifische Normen und Standards.

Im Mittelpunkt dieser Rechtsnormen stehen Begriffe wie z.B. „Stand der Technik" sowie die Prüfkriterien „Zumutbarkeit", „Erforderlichkeit", „Geeignetheit" und „Angemessenheit". Diese Rechtsbegriffe müssen angesichts der Dynamik technischer Entwicklung immer wieder auf die Belange der jeweiligen Hochschule ausgerichtet und durch die verantwortlichen Personen umgesetzt werden. Rechtliche Vorgaben sollten mithin nicht kontextlos betrachtet und verfolgt werden.

5. Erstellung und Fortschreibung eines Informationssicherheitskonzeptes

Ziel jeder Hochschule ist es, ein angemessenes Informationssicherheitsniveau zu erzielen und zu erhalten. Hierfür müssen Informationsrisiken bewertet und behandelt werden. Als Hilfsmittel für die zugehörige Planung und Umsetzung werden die identifizierten Risiken sowie die umgesetzten und geplanten Maßnahmen in einem Informationssicherheitskonzept (fort-) geschrieben.

Planung und Umsetzung von Informationssicherheit und damit einhergehend der Prozess zur Erstellung bzw. Fortschreibung eines Informationssicherheitskonzeptes sind naturgemäß komplex und ressourcenintensiv. Daher sollte der Fokus nicht darauf liegen, möglichst schnell „Vollständigkeit" zu erzielen. Kurzatmig erstellte bzw. fortgeschriebene Informationssicherheitskonzepte laufen Gefahr, nur Soll-Zustände zu dokumentieren, die stark vom Ist-Zustand divergieren. Stattdessen empfiehlt es sich, kurzfristig erreichbare Teilziele zu formulieren und aufeinander aufbauend in Kraft zu setzen. Entsprechend sollte von der Vorstellung Abstand genommen werden, einen idealtypischen Masterplan stufenlos umzusetzen.

Für ein schrittweises Vorgehen haben sich insbesondere folgende Leitfragen bewährt:

a) Können vordringlich zu behandelnde Risiken festgestellt werden?
b) Wie können die unterschiedlichen Daten in ihrer Bedeutung erfasst werden?
c) Wie kann die Bewertung und Behandlung von Informationssicherheitsrisiken in die Prozesse der Organisation eingebettet werden?

Zu a) Ganz offensichtlich ist für Hochschulen etwa die besondere Schutzbedürftigkeit von Studierendendaten und auch von Patientendaten. Hier kann eine Prioritätensetzung „top-down" erfolgen – solche Risiken müssen nicht erst aufwendig identifiziert werden. Ebenso ist eine grundlegende Absicherung von IT-Systemen z.B. von Rechnungshöfen gefordert. Vorgehensweisen wie etwa die IT-Grundschutz-Methodik (in der Version 200-2) oder ISIS12 bieten hierzu auch niederschwellige Basis- und Kernabsicherungen bzw. einen vereinfachten Einstieg.

Zu b) Gerade im Zusammenhang mit dem Risikomanagement ist ein mehrstufiges Vorgehen vielversprechend. Zunächst muss eine Datenklassifikation vorgenommen werden. Im Zuge eines solchen Risikomanagements können in jeder Einheit relevante Prozesse erfasst und entsprechende Risikobewertungen vorgenommen werden. Daraus lassen sich Vorschläge für zentrale und dezentrale Maßnahmen ableiten. Die erfassten Punkte und Vorschläge sollten dann zentral ausgewertet werden. Auf der Grundlage dieser Auswertung kann anschließend eine zentrale Einheit Musteranforderungen oder vorgegebene Mindestmaßnahmen an die dezentralen Einheiten zur Ausgestaltung delegieren. Die so erstellten Lösungen bieten ein hohes Maß an Einheitlichkeit bzw. Vergleichbarkeit sowie Akzeptanz.

Vorschlag: Datenklassifikation
Im Sinne von sowohl Awareness als auch Bottom-Up-Partizipation könnte man den Prozess damit beginnen, dass alle Beschäftigten in ihren Einheiten die Informationen mit besonderem Schutzbedarf klassifizieren. Diese Klassifizierung sollte umfassend sein. Ausgangspunkt kann die Grobklassifikation „öffentlich", „intern", „vertraulich" und „geheim" sein. Dabei ist zu prüfen, ob man hinsichtlich der Hochschulgruppen „Forschende", „Lehrende" und „Studierende" sowie „Verwaltung" eine Differenzierung vornehmen muss. Dieser Auftaktimpuls könnte dann für eine Erstellung von entsprechenden FAQs genutzt werden. Auf diese Weise könnte gerade in weniger IT-affinen Fachbereichen ein Problembewusstsein für Informationssicherheit geschaffen werden.

Zu c) Die nachhaltige Bewertung und Behandlung von Informationsrisiken entsteht durch Einbettung in die Prozesse in Lehre, Forschung, Wissenstransfer und Administration. Beispielsweise sollte die Informationssicherheit bei der Erstellung von Datenmanagementplänen mitbedacht werden.

Vorschlag: Erstellung von Datenmanagementplänen
Datenmanagementpläne werden bereits jetzt im Rahmen der Richtlinien mancher Forschungsförderorganisationen verlangt. Ein Datenmanagementplan beschreibt, welche Daten im Lauf der Arbeit erfasst und erzeugt werden und was während des weiteren Lebenszyklus' mit ihnen geschehen soll (Speicherung, Veröffentlichung, Zitierbarkeit, Langzeitverfügbarkeit, Anonymisierung, Löschung usw.) Ziel dabei ist es, den Anforderungen an gute wissenschaftliche Praxis zu genügen und Forschungsresultate langfristig nachvollziehbar zu machen.
(Quelle: Bibliothek der ETH Zürich: www.library.ethz.ch/content/download/12376/…/file/Datenmanagementplan_DE.pdf)

In diesen Dokumentationsprozess können Aspekte der Risikobewertung und Behandlung einfach integriert werden. Ebenso kann die entsprechende Dokumentationspflicht durch Referenz auf zentrale Dienste mit bekannten Informationssicherheitszusagen erleichtert werden.

6. Umgang mit Störfällen

Grundlage für den Umgang mit Störfällen sollte die Erkenntnis sein, dass sich hundertprozentige Sicherheit in keinem Informationssicherheitssystem erzeugen lässt. Ziel muss es deshalb sein, einen möglichst hohen Grad an Resilienz zu erreichen, also nach einem Angriff möglichst schnell in einen arbeitsfähigen Systemzustand zurückzufinden.

Für die operativen Maßnahmen bei Störfällen sollten klare Zuständigkeiten z.B. für „Incident Response Teams"[6] definiert werden. Dazu gehören auch Verfahren zur Innen- und Außendarstellung von Störfällen. Aufgrund rechtlicher Vorgaben bestehen auch Meldepflichten, insbesondere in Bezug auf datenschutzrechtliche Vorfälle. Eine Abstimmung mit der für Kommunikation und Pressearbeit betrauten Stelle ist empfehlenswert. Die gemeldeten Störfälle bilden auch eine Grundlage für die Erfassung des Lagebildes zur Informationssicherheit der Hochschule. Um zu verhindern, dass Meldungen zurückgehalten werden, muss ein sorgsamer Umgang gewährleistet und Verständnis für das Vorkommen von Vorfällen vorhanden sein.

7. Ressourcen

Die postulierte Vorgehensweise eines schrittweisen Verfahrens entspricht bereits dem Bestreben nach sparsamer Verwendung von Ressourcen. Dessen unbenommen muss die Hochschulleitung ausreichende Ressourcen für die Erreichung des angestrebten Sicherheitsniveaus zur Verfügung zu stellen. Die notwendigen Ressourcen zur Etablierung eines Informationssicherheits-Managementsystems ergeben sich im Wesentlichen aus Konzepterstellung, Umsetzung und Betrieb. Grundsätzlich empfiehlt es

[6] Schnell einsatzbereite Gruppen; andere mögliche Bezeichnungen sind „Incident Response Taskforces" oder „Incident Protection Teams".

sich, nicht nur auf interne Expertise zurückzugreifen, sondern auch externe Unterstützung zu nutzen.

Vorschlag: Externe Unterstützung nutzen
In allen Phasen kann eine Hochschule Unterstützung bei den Einrichtungen

- DFN-CERT Services GmbH
- Arbeitskreis Informationssicherheit in Forschungseinrichtungen (AKIF)
- Bundesamt für Sicherheit in der Informationstechnik (BSI)

finden. Des Weiteren hält die Deutsche Initiative für Netzwerkinformation (DINI) Expertise bereit. In Anträgen an die DFG können auch Mittel dafür eingeworben werden, die in einem DFG-geförderten Projekt erzeugten Daten aufzubereiten. Zudem existieren weitere Dienstleister am Markt.

Bei der Konzepterstellung sind diverse Aufwendungen für interne und externe Beratung nicht zu unterschätzen. Ebenfalls häufig unterbewertet wird auch der notwendige Personalaufwand für die Etablierung und den Betrieb von Prozessen zur Informationssicherheit. Der genaue Ressourcenbedarf hängt natürlich von der Reichweite und Komplexität des zu etablierenden Informationssicherheits-Managementsystems ab. Für den Betrieb des Informationssicherheits-Managementsystems müssen Personalmittel auch zusätzlich z.B. für Awareness- und Schulungsmaßnahmen zur Verfügung gestellt werden. Die Zuwendungsgeber müssen im Rahmen der Grundfinanzierung entsprechende zusätzliche Ressourcen zur Verfügung stellen.

8. Kooperationen für Informationssicherheit

Aufgrund der genannten Ressourcenintensität sind Kooperationen erwägenswert. Bei Konsortialstrukturen ist zu beachten, dass nicht nur die Konsortialführung, sondern auch die jeweilige Hochschule für die Informationssicherheit verantwortlich ist. Lokale Kooperationen bieten sich besonders bei kleineren Hochschulen an, die wegen ihrer Ausstattung allein nicht die kritische Masse für Prozesse zur Informationssicherheit aufbringen. In jedem Fall sollten die Empfehlungen des Wissenschaftsrats zu regionalen Kooperationen wissenschaftlicher Einrichtungen berücksichtigt werden.

Kooperationen können sich z.B. auf folgende Bereiche erstrecken: Erstellung von Landes- und Verbundkonzepten, Kommunikationskonzepte für Störfälle, Schulungsmaßnahmen, Erfahrungsaustausch und Einkaufskooperationen sowie Peer-Audit oder Peer-Penetration-Tests[7].

Um Synergieeffekte zu erzielen, sind Standardisierung und Vergleichbarkeit sowie klare Regelungen („Policies“) vor allem in der Administration erforderlich. Tools auf dem Weg zu vergleichbaren Strukturen können

[7] Umfassende gegenseitige Sicherheitstests einzelner Rechner oder Netzwerke.

auch Zertifizierungen oder einheitliche „Business Continuity Management (BCM)"-Konzepte sein. Darüber hinaus kann die Community – bestehend aus Hochschulen und Dienstleistern – Kooperationsplattformen, gute Pseudonymisierungs- bzw. Anonymisierungswerkzeuge, sowie offene, einfach zu nutzende Verschlüsselungswerkzeuge etablieren.

Standardisierung und Vergleichbarkeit werden durch die Heterogenität der Hochschulen begrenzt. Dies hat zur Folge, dass es nicht immer ein einheitliches Modell für alle beteiligten Hochschulen geben kann. Daher müssen im Sinne der Angemessenheit abgestufte Lösungen sowohl bei Geltungsbereichen als auch bei Sicherheitslevels möglich sein. Diese Geltungsbereiche und Sicherheitslevels müssen zwischen den kooperierenden Hochschulen ausgehandelt werden. Es erscheint überdies ratsam, die Anzahl der beteiligten Hochschulen nicht zu hoch anzusetzen, damit die zu erarbeitenden Strukturen nicht zu komplex werden. Kooperationsmöglichkeiten können durch den Wettbewerb zwischen Hochschulen begrenzt werden.

Grundsätzlich sollten Kooperationsstrukturen nicht als Entlastung von eigener Verantwortung begriffen werden. Stattdessen sollten die in der Hochschule verantwortlichen Personen die durch Kooperation möglichen Synergieeffekte in den Vordergrund stellen und sich stets der eigenen Verantwortlichkeit bewusst sein.

9. Zertifizierungen und Audits

Die Notwendigkeit von Zertifizierungen ergibt sich in der Regel durch externe Fachvorgaben von Behörden und Zuwendungsgebern oder durch Industriekooperationen. Zertifizierungen sowie interne und externe Audits werden im „Modell der drei Verteidigungslinien"[8] als dritte Linie geführt (die erste Linie umfasst die operative Ebene, die zweite Linie den Eigner des Prozesses „Informationssicherheit"). Als mögliche Zertifizierer kommen die bekannten Einrichtungen (z.B. BSI-zertifizierte Auditoren, TÜV) in Frage. Zu beachten ist dabei, dass eine allgemeine Zertifizierungspflicht für Hochschulen derzeit nicht besteht. Denkbar sind auch Self-Audits, Peer-Audits und sonstige externe Audits. Audits und Self-Audits sind in diesem Bereich mit zunehmenden Anforderungen verbunden.

Die wesentliche Entscheidung bei Zertifizierungen liegt in der Klärung, welche Zertifizierung überhaupt anzustreben ist (z.B. nach ISO 27001, BSI Grundschutz). Dabei sollte zugleich mitberücksichtigt werden, welche Verfahren bei Industriekooperationen ohnehin erforderlich sind oder sein werden. Zertifizierungen und Audits oder daran angelehnte Prozesse können überdies Wettbewerbsfaktoren werden. Zertifizierungen sollten demnach nicht als Selbstzweck verfolgt, sondern immer unter dem Gesichtspunkt institutioneller Mehrwerte angestrebt werden.

[8] Das Modell zur systematischen Herangehensweise an Risiken, die in Unternehmen und Organisationen auftreten können, stammt vom Dachverband der europäischen Revisionsinstitute (ECIIA).

Anhang

Definition der Informationssicherheitsschutzziele nach DIN ISO/IEC 27000:

Authentizität: Eigenschaft einer Einheit, das zu sein, was sie zu sein vorgibt

Vertraulichkeit: Eigenschaft, dass Informationen unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden

Integrität: Eigenschaft der Absicherung von Richtigkeit und Vollständigkeit von Werten

Verfügbarkeit: Eigenschaft, einer berechtigten Einheit auf Verlangen zugänglich und nutzbar zu sein

Zurechenbarkeit: Verantwortung einer Einheit für ihre Handlungen und Entscheidungen

Nicht-Abstreitbarkeit: Fähigkeit, das Auftreten eines behaupteten Ereignisses oder einer Handlung und die verursachenden Einheiten nachzuweisen, um Streitigkeiten über das Auftreten oder Nichtauftreten des Ereignisses oder der Handlung und die Beteiligung von Einheiten an dem Ereignis zu entscheiden

Verlässlichkeit: Eigenschaft der Übereinstimmung zwischen beabsichtigtem Verhalten und den Ergebnissen

Zur Entstehung der Handreichung

Die vorliegende Handreichung ist in der Ständigen HRK-Kommission für Digitale Infrastrukturen erstellt worden. Geleitet wird die Kommission von der HRK-Vizepräsidentin für Digitale Infrastrukturen, Frau Professor Dr. Monika Gross. Der Kommission gehören als ständige Mitglieder Herr Malte Dreyer, Frau Professor Dr. Petra Gehring, Frau Professor Dr. Gudrun Gersmann, Herr Professor Dr. Hannes Hartenstein, Herr Professor Dr. Wolfram Horstmann, Frau Dr. Antje Kellersohn, Herr Professor Dr. Norbert Lossau, Herr Jens Andreas Meinen, Herr Professor Dr. Joachim Schachtner, Herr Professor André Stärk, Frau Professor Dr. Gudrun Stockmanns und Frau Dr. Beate Tröger an. Betreut wird die Kommission von Herrn Dr. Elmar Schultz von der HRK-Geschäftsstelle.

Ausgangspunkt der Arbeiten war eine Anhörung am 11. Oktober 2017. Angehört wurden Herr Alexandros Gougousoudis (Leiter Service Center IT, Berlin), Herr Klaus Keus (Bundesamt für Sicherheit in der Informationstechnik), Herr RA Dr. iur. Jan K. Köcher (Teamleiter CAT im DFN-CERT), Frau Prof. Dr. Gudrun Oevel (Leiterin IMT, U Paderborn), Herr Dr. Hans Pongratz (Vizepräsident und CIO, TU München), Herr Dr. Helfried Broer (stellv. Chief Information Security Officer, FhG) und Herr Prof. Dr. Sebastian Schinzel (Informatik, FH Münster).

Die HRK dankt allen Beteiligten für ihre Beiträge.