Technische Universität Braunschweig

Inhalt

1 Informationssicherheit als Herausforderung 1
2 Strategische Aufgabe der Hochschulleitung 2
2.1 Definition „Informationssicherheit“ im Kontext der Hochschule 3
2.1.1 Definition „Informationssicherheit“ nach DIN/ISO/IEC 27000:2017 4
2.1.1.1 Definitionen und Kern-Eigenschaften 4

Strategische Leitlinie Informationssicherheit der TU Braunschweig

1 Informationssicherheit als Herausforderung

Wissenschaft braucht Vertrauen. Dies gilt sowohl für Forschung und Lehre als auch darauf aufbauend für den Transfer in die Gesellschaft als Kernaufgaben der TU Braunschweig. Die Informationssicherheit stellt eine unabdingbare Voraussetzung für die Erfüllbarkeit dieser Kernaufgaben durch alle beteiligten Organisationseinheiten der TU Braunschweig dar.
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, und damit auch die zentrale und dezentrale Verwaltung, in spezifischer Weise, insbesondere hinsichtlich:

- Verlust der Integrität und Verfügbarkeit von forschungs- und personenbezogenen Daten, auch in der Lehre und der Verwaltung,
- Kompromittierung von personenbezogenen Daten aller Hochschulangehörigen sowie
- Verlust der Vertraulichkeit von Daten innerhalb von Kooperationen, beispielsweise durch Spionage.

Zu den wesentlichen Gefahrenquellen für die Reduktion bzw. den Verlust von IT-Sicherheit zählen beispielsweise (zum Zeitpunkt der Verabschiedung):

- 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.
- Infizierung und Sperrung von Rechnern von TU-Angehörigen innerhalb und außerhalb des TU-Netzes, um nachfolgend Geld für die Entsperrung oder Nicht-Veröffentlichung sensibler Daten zu verlangen („Ransomware“). Gelingt z.B. die Infizierung oder Sperrung eines zentralen Hochschulrechners, so könnten Forschungs-, Lehr-, Studien- und Verwaltungsaktivitäten ad hoc für mehrere Monate zum Erliegen kommen und darüber hinaus auch sensible Daten verloren gehen. Ähnliche Folgen können eintreten, wenn Externe die Hochschulinfrastruktur für Botnetze nutzen.
- Die bewusste oder unbemerkte Weitergabe von Zugangsberechtigungen zu Teilen der IT-Infrastruktur an nicht berechtigte Personen, die im Nachgang die Verfügbarkeit von Daten oder deren Schutz verhindern.
- Die Nutzung bzw. Verarbeitung von hochschulbezogenen Daten auf Endgeräten, die nicht dem Stand der Technik entsprechend vor unberechtigtem Zugriff geschützt sind.

Hochschulen sind in besonderer Weise verwundbar. Dazu tragen u.a. bei:

- die weltweite Zusammenarbeit verschiedenster Organisationseinheiten (OEn) innerhalb der TU Braunschweig oder mit externen Partnern auf der Basis fachlichen Austausches,
- die weitgehende Autonomie vieler OEn,
- der Projektcharakter von Aktivitäten und Prozessen,
- eine vergleichsweise hohe Personalfluktuation,
- die verschiedenen Statusgruppen mit ihren unterschiedlichen Rollen und Rechten und heterogenen Awareness[1]-Leveln sowie
- die schnellen Entwicklungszyklen der Informationstechnik.

Die Herstellung und Aufrechterhaltung von Informationssicherheit bedeuten daher für die Hochschulen eine erhebliche Herausforderung[2] und kontinuierliche Aufgabe.

2 Strategische Aufgabe der Hochschulleitung

Im wissenschaftlichen Umfeld zielt der Begriff „Informationssicherheit” vorrangig auf die Aspekte Integrität, Vertraulichkeit sowie Verfügbarkeit und Austausch von Informationen. Vorranging werden elektronisch gespeicherte Daten betrachtet, unter Einbeziehung der dazugehörigen (auch manuellen) Verarbeitungsprozesse. Gleichwohl ist auch der Schutz analog vorliegender Daten Gegenstand der Informationssicherheit.
Informationssicherheit unterscheidet sich von IT-Sicherheit darin, dass das zu schützende Gut „Information“ und die zugehörigen informationsverarbeitenden Prozesse in den Vordergrund der

[1] Der Begriff „Awareness“ wird hier bewusst verwendet, weil die deutschen Entsprechungen „Bewusstsein“, „Gewahrsein“, „Aufmerksamkeit“ oder auch „Sensibilisierung“ nicht hinreichend eindeutig sind.
[2] Vgl. https://www.hrk.de/positionen/gesamtliste-beschluesse/beschluss/detail/informationssicherheit-als-strategische-aufgabe-der-hochschulleitung/ [letzter Abruf: 24.06.2021].

Risikobewertung und -behandlung gestellt werden. IT-Sicherheit betrachtet die technischen Aspekte und ist daher ein Teil der Informationssicherheit.
Informationssicherheit als Aspekt der Prozessqualität in der Hochschule zu verankern, ist rechtlich gefordert und damit auch eine Gestaltungsaufgabe im Rahmen der Governance-Struktur und der institutionellen Awareness. Die Hochschulleitung muss diese Aspekte für alle Handlungsfelder aktiv aufgreifen. Die daraus resultierenden 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 Umfang und Tiefe der 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 ein effizienter Technologie- und Wissenstransfer 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 und stetig weiterzuentwickeln, um aktuellen Entwicklungen unterschiedlicher Bedrohungslagen angemessen begegnen zu können. In diesen Strukturen müssen die Fachseite und die Betreibenden der informationstechnischen Infrastruktur zusammenwirken und die Beziehungen zu und zwischen den Rollen Datenschutz, Informationssicherheit, Justiziariat, Präsidium, Pressestelle und Vorfallmeldestellen geregelt sein. Für die Erreichung eines angemessenen 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 sowie
- einen kontinuierlichen Verbesserungsprozess

belegt. Melde-, Reaktions- und Dokumentationspflichten sowie das Risikomanagement sind für Informationssicherheit, IT-Sicherheit und Datenschutz in abgestimmter Weise umzusetzen und zu dokumentieren. Das tatsächlich erzielte Sicherheitsniveau hängt maßgeblich von der Berücksichtigung der Informationssicherheit bei der Neu- und Umgestaltung aller Geschäftsprozesse und Tätigkeiten sowie von der Awareness für Informationssicherheit innerhalb der Hochschule, von der vorhandenen Expertise in Informationssicherheit und IT-Sicherheit und dem erfolgreichen Zusammenspiel der oben ausgeführten Strukturen ab.

2.1 Definition „Informationssicherheit“ im Kontext der Hochschule

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.

2.1.1 Definition „Informationssicherheit“ nach DIN/ISO/IEC 27000:2017[3]

„Informationssicherheit (en: information security) Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Information. Zusätzlich können auch andere Eigenschaften wie Authentizität, Zurechenbarkeit, Nichtabstreitbarkeit und Verlässlichkeit einbezogen werden.“

2.1.1.1 Definitionen und Kern-Eigenschaften[4]

Informationssicherheit ist ein komplexes, abstraktes Konstrukt, für welches keine einheitliche Definition existiert. So beschreibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) Informationssicherheit auf Grundlage des Standards ISO 27001 als Schutz von Vertraulichkeit, Integrität und Verfügbarkeit[5]. Ähnlich definiert die U.S. amerikanische Normierungsbehörde National Institute of Standards and Technology (NIST) Informationssicherheit als Sicherstellung des Schutzes von Informationen und Informationssystemen vor unbefugtem Zugriff, Nutzung, Veröffentlichung, Störung, Modifikation oder Löschung, um Vertraulichkeit, Integrität und Verfügbarkeit[6]. Obgleich innerhalb der Wissenschaft Definitionen des Begriffs Informationssicherheit häufig auch weitere Aspekte wie etwa Authentizität und Nachweisbarkeit[7] umfassen, haben auch diese Definitionen zumeist gemein, dass sie den Schutz der drei Kerneigenschaften der Informationssicherheit, d.h. Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability) beschreiben[8]. Dabei impliziert

- Vertraulichkeit den Schutz von vertraulichen Informationen vor unberechtigtem Zugriff,
- Integrität den Schutz von Daten und Informationssystemen gegenüber unzulässiger Modifikation und Löschung von Informationen und
- Verfügbarkeit das Sicherstellen eines rechtzeitigen und verlässlichen Zugriffs auf Informationen und Informationssysteme.

Informationssicherheit bedingt die Anwendung und das Management von angemessenen Sicherheitsmaßnahmen unter Berücksichtigung einer großen Bandbreite von Bedrohungen mit dem Ziel, einen kontinuierlichen Betrieb[9] in angemessenem Umfang sicherzustellen und Beeinträchtigungen durch Informationssicherheitsvorfälle zu minimieren. Informationssicherheit wird durch die Umsetzung eines geeigneten Maßnahmenkatalogs erreicht, der im Rahmen eines operativen Risikomanagement-prozesses erarbeitet wurde. Diese Maßnahmen müssen festgelegt, umgesetzt, überwacht, überprüft und wo notwendig verbessert werden, um sicherzustellen, dass die spezifischen Informationssicherheits- und Geschäftsziele der TU Braunschweig erreicht werden. Sie werden mit Hilfe eines Informations-sicherheitsmanagementsystems (ISMS) gesteuert. Das ISMS umfasst seinerseits Richtlinien, Prozesse, Verfahren, Organisationsstrukturen, Software und Hardware zum Schutz von identifizierten

---

[3] https://www.din.de/de/mitwirken/normenausschuesse/nia/veroeffentlichungen/wdc-beuth:din21:269670716 (ISO 27001, Version 2017 ist die aktuell gültige Norm)[letzter Abruf: 24.06.2021]
[4] https://enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/uebergreifendes/Kontext-und-Grundlagen/IT-Recht/informationssicherheit [Abruf: 24.06.2021]
[5] Bundesamt für Sicherheit in der Informationstechnik, Grundschutz-Kompendium 2020, S. 15, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.pdf%3F__blob%3DpublicationFile%26v%3D6 [letzter Abruf 08.07.2021]
[6]FEDERAL INFORMATION SECURITY MODERNIZATION ACT https://www.cisa.gov/federal-information-security-modernization-act [letzter Abruf: 08.07.2021]
[7] Gordon, Lawrence A.; Loeb, Martin P. The economics of information security investment. ACM Transactions on Information and System Security 5(2002), Nr. 4, S. 438-457
[8] Dehling, Tobias; Sunyaev, Ali. Secure Provision of Patient-Centered Health Information Technology Services in Public Networks—Leveraging Security and Privacy Features Provided by the German Nationwide Health Information Technology Infrastructure. Electronic Markets 24(2014), Nr. 2, S. 89–99
[9] Im Sicherheitskontext meist als „Business Continuity“ bezeichnet.

Informationswerten. Grundsätzlich ist anzustreben, dass Informationssicherheitsmaßnahmen möglichst nahtlos in die Geschäftsprozesse der Organisation integriert werden.
Daten müssen sowohl den Erfordernissen der Qualitätssicherung als auch der Informationssicherheit genügen. Zudem agiert die TU Braunschweig in einem globalen Umfeld und befindet sich in offenem Austausch mit der Gesellschaft. Hieraus ergibt sich ein Spannungsfeld zwischen unterschiedlichen Zielen:

- das Postulat einer *Offenheit*, von (digitalen) Forschungsprozessen, -methoden und -ergebnissen (Open Access, Open Science, Open Data) und von Lehr- bzw. Lerninhalten (Open Educational Resources) impliziert, dass die Schutzziele *Integrität* und *Verfügbarkeit* einen besonders hervorgehobenen Stellenwert haben.
- Das Postulat der *Vertraulichkeit* ergibt sich aus der Notwendigkeit von geschützten Bereichen für die wissenschaftliche Zusammenarbeit und nicht zuletzt aus dem wissenschaftlichen Wettbewerb und der Zusammenarbeit mit Partnern aus der Industrie (insbesondere im Kontext der Auftragsforschung), den Vertraulichkeitsanforderungen in der Verwaltung sowie den Anforderungen des Schutzes persönlicher Daten nach DSGVO in allen Bereichen der Universität.

Die notwendigen Abwägungen hinsichtlich der Schutzzielbildung und Risikoeinschätzung müssen von den zuständigen Gremien der TU Braunschweig erarbeitet und im Rahmen der geltenden Gesetze von der Hochschulleitung in der Umsetzung beschlossen werden.
Informationssicherheit umfasst im Gegensatz zur IT-Sicherheit auch nicht-informationstechnische Systeme und sorgt dafür, dass auch nicht-digitale Systeme durch entsprechende betriebliche Organisation und Vorgaben geschützt werden. Somit holt die Informationssicherheit weiter aus als die IT-Sicherheit, da sie informationstechnische Systeme, nicht-informationstechnische Systeme, physische Sicherheit (u.a. Gebäudesicherheit) und die Organisation mit einschließt. Sie berücksichtigt dabei implizit Medienbrüche zwischen digitalen und analogen Anteilen von Prozessen.
Die Behandlung des Themenfeldes Informationssicherheit kann dementsprechend nur durch Zusammenwirken der Fachseite (Forschung, Lehre, Wissenstransfer, Administration) mit der Informations(-system) -Seite (Rechenzentrum, Bibliothek, Datenschutz), der physischen Sicherheit repräsentiert durch das Gebäudemanagement und der Definition organisatorischer Prozesse erfolgen. Insbesondere die Entwicklung von Rahmenbedingungen für Prozesstransparenz sowie Verhaltensregeln in Form von Leit- und Richtlinien werden von der Hochschule gestaltet und getragen. Die Berücksichtigung der Prozesse, für die die vorhandene IT-Technik eingesetzt wird, ist ein elementarer Bestandteil der Informationssicherheit und kann nur von den Prozessführenden sichergestellt werden. Dabei muss das Erstellen von Risikoabschätzungen und das Tragen von Risikoentscheidungen in die Prozesse der Hochschule integriert werden. Die Aufgabe, Informationssicherheit als Aspekt der Prozessqualität in der Organisation Hochschule zu verankern obliegt gemeinschaftlich den zentralen und dezentralen Organisationseinheiten. Informationssicherheit ist nicht nur rechtlich gefordert, sondern vielmehr Teil einer übergreifenden Gestaltungsaufgabe im Rahmen der institutionellen Awareness sowie der Weiterentwicklung von Governance-Strukturen und -Prozessen, bei der alle Mitglieder und Angehörige der Hochschule mitwirken müssen.

Präsidiumsbeschluss vom 09.02.2022, Bestätigung durch den Senat am 16.02.2022