Amtliche Mitteilungen Nr. 45/2017 30.08.2017

Leitlinie Informationssicherheit an der Technischen Hochschule Wildau

Herausgeber:
Der Präsident:
Technische Hochschule Wildau
Körperschaft des öffentlichen Rechts

Hochschulring 1
15745 Wildau
Tel.: 03375/508-0
Fax: 03375/500324

Inhaltsverzeichnis

Stellenwert der Informationsverarbeitung

An einer modernen und fortschrittlichen Hochschule findet die Informationsverarbeitung mit Hilfe von Informations- und Kommunikationstechnik statt und spielt somit eine Schlüsselrolle bei der Aufgabenerfüllung (Studium und Lehre, Forschung und Transfer, etc.).
Alle Bereiche der Technischen Hochschule Wildau verarbeiten in ihren Prozessen, Verfahren oder Abläufen Informationen. Zu nennen sind hier die Hochschulverwaltung, die zentralen Einrichtungen, die Fachbereiche, Einrichtungen für Aus- und Weiterbildung, Stabsstellen und beauftragten Personen.
Die Hochschulleitung erkennt, dass sich die Risiken und die zu erwartenden Auswirkungen bei der Informationsverarbeitung verändern und für die Hochschule eine Existenzbedrohung annehmen können.
Mit der amtlichen Mitteilung 44/2017 unterstreicht die Hochschulleitung die Bedeutung der Informationssicherheit für die Hochschule und bestätigt die Übernahme der Gesamtverantwortung für den Informationssicherheitsprozess.
Die vorliegende Leitlinie beschreibt die allgemeinen Ziele, Strategien und Organisationsstrukturen, welche für die Initiierung und Etablierung eines ganzheitlichen Informationssicherheitsprozesses an der Technischen Hochschule Wildau erforderlich sind.
Im vorliegenden Text wird durchgängig die männliche Form benutzt. Im Sinne des Gleichbehandlungsgesetzes sind diese Bezeichnungen als nicht geschlechtsspezifisch zu betrachten.

Grundsätze der Informationssicherheit

Ziel der Informationssicherheit ist es, die Risiken, die auf die Grundwerte der Informationssicherheit – Vertraulichkeit, Integrität und Verfügbarkeit – wirken, auf ein akzeptierbares Maß zu reduzieren. Die Informationssicherheit umfasst neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten Informationen.
Die Grundwerte der Informationssicherheit bedeuten:

Vertraulichkeit:
Vertrauliche Informationen sind vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen. Zu den Schutzobjekten gehören die gespeicherten oder transportierten Nachrichteninhalte und die Informationen über den Kommunikationsvorgang (wer, wann, wie lange, mit wem etc.).

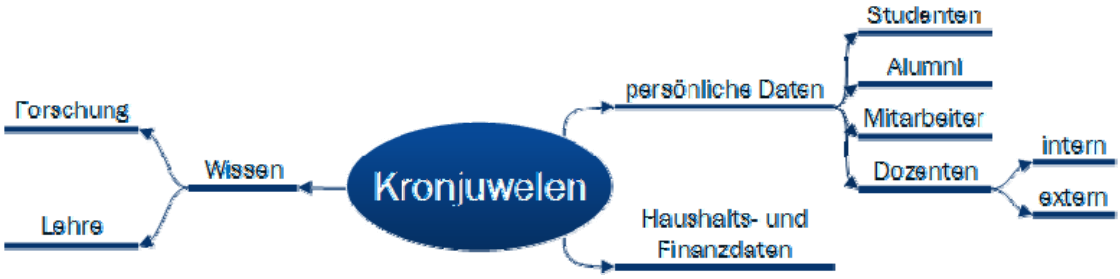
Integrität:
Der Begriff der Integrität bezieht sich sowohl auf Informationen als auch auf IT-Systeme. Integrität der Informationen bedeutet deren Vollständigkeit und Korrektheit. Vollständigkeit bedeutet, dass alle Teile der Information verfügbar sind. Korrekt sind Informationen, wenn sie den bezeichneten Sachverhalt unverfälscht wiedergeben. Im Bezug auf IT-Systeme bezeichnet die Integrität die vollständige und unveränderte Funktionsweise der Systeme.

Verfügbarkeit:
Die notwendigen Informationen stehen dem Anwender zum richtigen Zeitpunkt am richtigen Ort zur Verfügung.

Übergreifende Ziele

Um an der TH Wildau Informationssicherheit zu etablieren, ist es von elementarer Bedeutung, diejenigen Informationen der Hochschule zu identifizieren, die eine Möglichkeit der existenziellen Bedrohung der Hochschule darstellen. Diese Informationen werden in einer Bedrohungsanalyse identifiziert und stellen die Kronjuwelen der TH Wildau dar.
Für die TH Wildau sind die identifizierten Kronjuwelen:

- Wissen
- persönliche Daten
- Haushalts- und Finanzdaten



Die Bedeutung der Kronjuwelen für die Hochschule wird nachfolgend erläutert.

Wissen:

Nach dem Brandenburgischen Hochschulgesetz § 3 (1) dienen die Hochschulen „...der Pflege und Entwicklung der Wissenschaften und Künste durch Lehre, Forschung, Studium und Weiterbildung." und sind somit für die Durchführung von Lehre und Forschung verantwortlich. Lehre und Forschung sind folglich die elementaren Kernbereiche der Hochschule und infolgedessen Kronjuwelen.

persönliche Daten:

Persönliche Daten setzen sich aus zwei Gesichtspunkten zusammen.

Als Erstes berücksichtigt werden Zugangsdaten, im Speziellen die Zugangskennung und das dazugehörige Passwort als persönliche Daten. Es ergibt sich daraus ein erhebliches Schadenspotenzial für die Hochschule, denn die Zugangsdaten sind Grundlage für den Zugriff auf die Informationen der Hochschule und somit Grundlage für den Diebstahl von Informationen jeglicher Form.

Als Zweites berücksichtigt werden die personenbezogenen Daten als persönliche Daten. Existenzbedrohend ist an diesen Informationen nicht primär der monetäre Schaden, der bei einer Datenschutzverletzung zu erwarten ist. Viel schwerer und nicht abschätzbar sind die negativen Auswirkungen auf das Image, wenn Unzulänglichkeiten im Bereich der personenbezogenen Daten bekannt werden.

Haushalts- und Finanzdaten:

Unberechtigte Kenntnisse oder Informationen innerhalb oder außerhalb der Hochschule über die wirtschaftliche und finanzielle Situation der Hochschule sind geeignet, die Existenz der Hochschule zu bedrohen.

Einschränkungen oder Beeinträchtigungen in Prozessen, Verfahren oder Abläufen, welche die definierten Kronjuwelen verarbeiten, werden in ihrer *Verfügbarkeit* so gesichert, dass sie kurzfristig kompensiert werden können und so zu erwartende Stillstandzeiten toleriert werden können.
Wenn Sicherheitsrisiken auftreten (bekannte oder drohende Angriffe), kann die Verfügbarkeit entsprechend dem Bedrohungs- und Schadensrisiko vorübergehend eingeschränkt werden. Im Interesse der Funktionsfähigkeit der gesamten Hochschule ist der Schutz vor Schäden vorrangig.
Fehlfunktionen und Unregelmäßigkeiten, die *Integrität* der Informationen und IT-Systeme, sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel. Die Anforderungen der Informationen an die *Vertraulichkeit* haben ein normales, an der Gesetzeskonformität orientiertes Niveau.

Detailziele

Die Hochschulleitung etabliert ein Informationssicherheitsmanagementsystem (ISMS), das sich an dem Standard ISO 27001 orientiert. Der nach diesem Standard neu zu strukturierende Sicherheitsprozess hat das Primärziel, die Sicherheit der definierten Kronjuwelen zu gewährleisten.
In die Neustrukturierung des Sicherheitsprozess werden alle Organisationseinheiten der TH Wildau einbezogen, damit das Primärziel sicher zu realisieren ist.

Im Rahmen der bereits angeführten Bedrohungsanalyse sind die Organisationseinheiten der TH Wildau anhand ihrer Aufgaben zu überprüfen, inwieweit sie die als Kronjuwelen definierten Informationen verarbeiten. Auf Basis dieser Bedrohungsanalyse wird durch die Hochschulleitung eine Priorisierung der Organisationseinheiten vorgenommen. Im Sinne einer iterativen Vorgehensweise wird der Sicherheitsprozess in den Organisationseinheiten schrittweise etabliert.

Der Informationssicherheitsprozess wird in das Prozessmanagement der Hochschule integriert. Ziel hierbei ist es, die für die Informationssicherheit relevanten Informationen in der Prozessdokumentation zu berücksichtigen.

Informationssicherheit kann an der Hochschule nur etabliert werden, wenn alle Angehörigen der Hochschule aktiv mitwirken. Erklärtes Ziel ist es, alle Angehörigen der Hochschule im erforderlichen Umfang zu sensibilisieren und zu qualifizieren, um notwendige Kompetenzen bezüglich der Informationssicherheit aufzubauen bzw. zu vertiefen.

Die umzusetzenden Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Schaden stehen, der durch einen Sicherheitsvorfall erwartet wird. Zu bewerten sind dabei die Auswirkungen des Sicherheitsvorfalls auf die körperliche und seelische Unversehrtheit von Menschen, das Recht auf informationelle Selbstbestimmung, finanzielle Schäden, Beeinträchtigungen des Ansehens der Hochschule, die Folgen von Gesetzesverstößen und Beeinträchtigungen der Aufgabenerfüllung.

Informationssicherheitsmanagement

Zur Erreichung der Informationssicherheitsziele wurde eine Sicherheitsorganisation eingerichtet. In der Sicherheitsorganisation werden folgende Rollen und Verantwortlichkeiten definiert:

Hochschulleitung:

Sie ist aufgrund ihrer Gesamtverantwortung für die Risikovorsorge an der Hochschule auch für die Informationssicherheit verantwortlich. Die Hochschulleitung erlässt verbindliche Regeln zur Informationssicherheit für die Technische Hochschule Wildau und gibt sie den Mitarbeitern und Studierenden bekannt. Sie stellt jederzeit eine Möglichkeit zur Kenntnisnahme der aktuellen Regeln sicher.

Informationssicherheitsbeauftragter (ISB):

Die Hochschulleitung benennt einen Informationssicherheitsbeauftragten, der über eine geeignete Fachkompetenz zur Informationssicherheit verfügt. Er ist für alle operativen Belange und Fragen der Informationssicherheit der Hochschule zuständig. Der ISB berichtet in seiner Funktion direkt an den Präsidenten, als verantwortlichen Vertreter der Hochschulleitung.

Informationssicherheitsmanagement-Team (SMT):

Die Hochschule richtet ein Informationssicherheitsmanagement-Team (SMT) ein. Das SMT unterstützt den ISB bei strategischen Entscheidungen wie z. B. der Bestimmung der Sicherheits-ziele, der Sicherheitsstrategie, der Erstellung und der Anpassung des Sicherheitskonzeptes. Die Mitglieder des SMT werden nach Bedarf durch die Hochschulleitung berufen.

Datenschutzbeauftragter:

Die Hochschulleitung benennt einen Datenschutzbeauftragten, der über eine geeignete Fachkompetenz zum Datenschutz verfügt. Er ist für alle operativen Belange und Fragen des Datenschutzes der Hochschule zuständig. Er stellt dem ISB ein aktuelles Datenschutzkonzept zur Verfügung und wirkt beratend am Informationssicherheitsmanagement in Belangen des Datenschutzes mit.

Sicherheitsmaßnahmen

Für alle Prozesse, Verfahren, Informationen, IT-Anwendungen und IT-Systeme wird eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen festlegt.

Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisung und angemessene Dokumentation sichergestellt sein, dass Vertreter deren Aufgaben erfüllen können.

Gebäude und Räumlichkeiten werden durch angemessene Zutrittskontrollen geschützt. Der Zugang zu IT-Systemen wird durch angemessene Zugangskontrollen und der Zugriff auf die Informationen durch ein restriktives Berechtigungskonzept geschützt.

Auf allen IT-Systemen wird, soweit technisch möglich, ein geeigneter Schutz vor Schadsoftware eingesetzt. Alle Internetzugänge werden durch eine geeignete Firewall gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Des Weiteren unterstützen alle Angehörigen der Hochschule die festgelegten Maßnahmen durch eine sicherheitsbewusste Arbeitsweise und informieren bei Auffälligkeiten die entsprechend festgelegten Stellen.

Informationsverluste können nie vollkommen ausgeschlossen werden. Durch eine umfassende Datensicherung wird daher gewährleistet, dass beeinträchtigte Prozesse oder Arbeitsabläufe kurzfristig wieder aufgenommen werden können, wenn Teile des operativen Datenbestandes verloren gehen oder offensichtlich fehlerhaft sind.

Die Angehörigen der Hochschule informieren sich durch bereitgestellte Dokumentationen, nehmen regelmäßig an Schulungen zur korrekten Nutzung der IT-Dienste und den hiermit verbundenen Sicherheitsmaßnahmen teil. Die Hochschulleitung unterstützt dabei die bedarfsgerechte Fort- und Weiterbildung.

Fortschreibung des Informationssicherheitsprozesses

Das Informationssicherheitsmanagementsystem der Technischen Hochschule Wildau wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft. Daneben werden auch die Maßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Angehörigen der Hochschule bekannt sind, ob sie umsetzbar und in den Hochschulablauf integrierbar sind.
Die Hochschulleitung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Alle Angehörigen der Hochschule sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen weiterzugeben.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheitsniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der Informationssicherheitstechnik zu halten.

Inkrafttreten

Diese Informationssicherheitsleitlinie tritt am Tag nach ihrer Veröffentlichung in Kraft.

Wildau, 30.08.2017

Prof. Dr. L. Ungvári
Präsident