Abschlussbericht

„IT-Sicherheitskonzeption und Austauschplattform“

Im Rahmen des Projekts

IT-Konzepte, Portfolio gemeinsamer Vorlagen und Muster an den Brandenburgischen Hochschulen

des Zentrums der Brandenburgischen Hochschulen für Digitale Transformation (ZDT)

Verantwortliche Hochschule:

Technische Hochschule Wildau

Hochschulen im Konsortium:

Brandenburgische Technische Universität Cottbus-Senftenberg
Europa-Universität Viadrina
Fachhochschule Potsdam
Filmuniversität Babelsberg KONRAD WOLF
Hochschule für nachhaltige Entwicklung Eberswalde
Technische Hochschule Brandenburg
Universität Potsdam

Projektzeitraum:

01.10.2022 – 31.12.2022

Projektleiter:

Bernd Heimer
03375 508 500
bernd.heimer@th-wildau.de

Bernd Heimer, Projektleiter

Projektbegleitung:
Krisensicher Risikoberatung GmbH
Rico Kerstan
03546 934 74 42
kerstan@krisensicher-werden.de
www.krisensicher-werden.de

Alle Ausführungen des Abschlussberichtes beziehen sich ausschließlich auf das Modul 4 des ZDT Projektes „IT-Konzepte, Portfolio gemeinsamer Vorlagen und Muster“, das in der Verantwortung der Technischen Hochschule Wildau umgesetzt wurde.

Inhalt

Abkürzungsverzeichnis

ISB	Informationssicherheitsbeauftragte/r
ISK	Informationssicherheitskonzept
ISMS	Informationssicherheitsmanagementsystem
MWFK	Ministerium für Wissenschaft, Forschung und Kultur
RIT	Rat der IT-Beauftragten
ZDT	Zentrums der Brandenburgischen Hochschulen für Digitale Transformation

1.Einleitung

Der vorliegende Bericht stellt den Stand zum Abschluss des Moduls 4 „IT-Sicherheitskonzeption und Austauschplattform“ im Rahmen des ZDT-Projekts „IT-Konzepte, Portfolio gemeinsamer Vorlagen und Muster an den Brandenburgischen Hochschulen“ für die 8 brandenburgische Hochschulen dar. Alle Ausführungen des Abschlussberichts beziehen sich ausschließlich auf dieses Modul, das in der Verantwortung der Technischen Hochschule Wildau umgesetzt wurde.

2. Problemstellung

Aufgrund stetig steigender Anforderungen an die IT-Governance an Hochschulen wurde das Projekt zur Erarbeitung von Informationssicherheitskonzepten im Rahmen des vom Zentrum der Brandenburgischen Hochschulen für Digitale Transformation (ZDT) getragenen Programms "IT-Konzepte, Portfolio gemeinsamer Vorlagen und Muster an den Brandenburgischen Hochschulen" im Sommer 2021 initiiert. Da die staatlichen Hochschulen des Landes Brandenburg in einem vergleichbaren externen Kontext agieren (gemeinsamer Rechtsraum mit vergleichbaren Strukturen und Prozessen), sollten durch eine kooperative Erarbeitung und Pflege von Vorlagen und Mustern für Informationssicherheitskonzepte, die in den Hochschulen vorhandenen und die für das Projekt bereitgestellten Ressourcen, gebündelt sowie Mehrfacharbeit vermieden werden.

Im Rahmen einer ersten Projektphase wurde ein generisches Informationssicherheitskonzept (ISK) in Zusammenarbeit aller Brandenburgischen Hochschulen erarbeitet. Das ISK ist das zentrale Dokument bzw. der zentrale Dokumentensatz bei der Initiierung des Sicherheitsprozesses einer Hochschule. Das Konzept, das aus mehreren Teilkonzepten bestehen kann, legt die planerische Grundlage für die Informationssicherheit fest. Alle Richtlinien und Prozesse, die die Informationssicherheit an der Einrichtung steuern und verbessern, basieren auf dem ISK.

Ausgehend von den Erkenntnissen der ersten Projektphase wurde im Herbst 2022 eine zweite Projektphase initiiert, in der die einzelnen Hochschulen bei der Adaption unterstützt werden sollten. Zudem sollte die Kooperation der Hochschulen in Bezug auf die Informationssicherheit weiter gestärkt werden. Es war explizit nicht das Ziel des Projektes ein Informationssicherheitsmanagementsystem (ISMS) zu beschreiben bzw. an den Hochschulen zu etablieren.

2.1 Projektziele

Das Projekt verfolgte folgende strategische Ziele:

- Ausgehend von den Vorlagen und Mustern aus der ersten Projektphase sollen die Hochschulen in die Lage versetzt werden, die Informationssicherheit im eigenen Haus zu konzeptionieren.

- Zudem soll eine kollaborative Austauschplattform geschaffen werden, die dem Austausch der Hochschulen dient und eine Bündelung von Ressourcen ermöglicht.

3. Projektvorgehen und Ablauf

3.1 Projektteam

Das Projektteam bestand aus der Projektleitung und den Projektmitgliedern, die sich aus den teilnehmenden Hochschulen rekrutierten.

Die Projektleitung bildete sich aus der Teilprojektleitung seitens des verantwortlichen Beraters des Beratungsunternehmens, Herrn Rico Kerstan und seitens der Leadhochschule, Herrn Bernd Heimer (TH Wildau), die das Projekt fachlich und inhaltlich sowie im Sinne des Projektmanagements betreuten.

Im Rahmen einer öffentlichen Ausschreibung wurde die KR Krisensicher Risikoberatung GmbH aus Lübben (Spreewald) mit der Projektbegleitung beauftragt. Als Berater waren Herr Rico Kerstan und Dr. Dirk Stahl tätig. Jeder Berater betreute zugewiesene Hochschulen individuell über den Projektzeitraum.

Die Projektmitglieder wurden durch die teilnehmenden Hochschulen an die Projektleitung gemeldet. Über den gesamten Projektzeitraum stand mindestens ein Ansprechpartner je Hochschule formal zur Verfügung. An einzelnen Hochschulen kam es im Projektverlauf zum Wechsel der Ansprechpartner.

3.2 Projektphasen und zeitlicher Ablauf

Das Projekt gliederte sich in drei Phasen:

1) Bestandsaufnahme zur Informationssicherheit pro Hochschule durch einen vorgelagerten Fragebogen und einem hochschulspezifischen Workshop,
2) kollaborative Erarbeitung eines generischen ISK und
3) hochschulspezifischer Beratungen pro Einrichtung.

Der zeitliche Ablauf der Phasen ist in Abbildung 1 dargestellt.

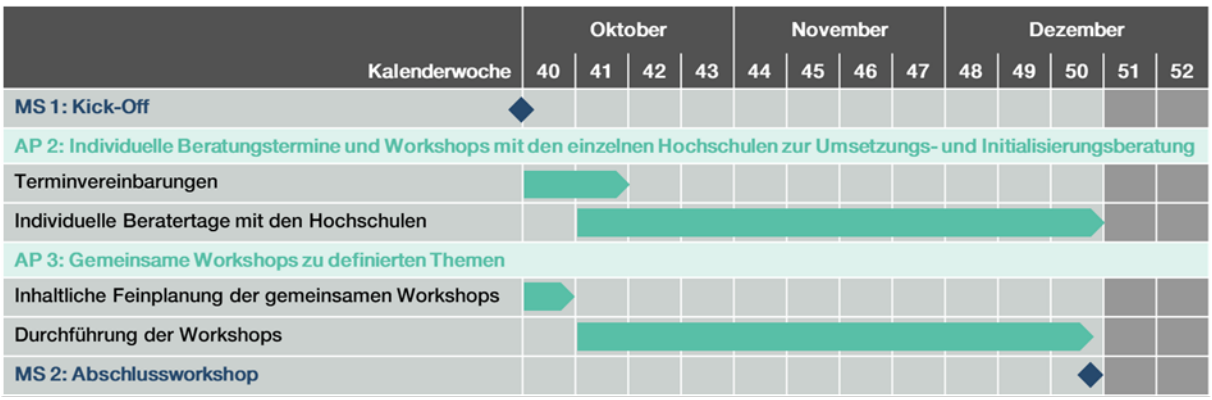

Abbildung 1: zeitlicher Projektablauf (Plan)

Das Projekt begann in KW 41 formal mit einem Kick-Off-Workshop der Projektleitung.

Es folgten Terminvereinbarungen mit den einzelnen Hochschulen für Termine zu Individualberatungen. Die Termine mit den Hochschulen wurden durch je einen Berater pro Hochschule zwischen Mitte Oktober und 31.12.2022 durchgeführt. Die Themen wurden mit den Hochschulen im Vorfeld abgestimmt. Die Inhalte sind den hochschulindividuellen Berichten entnehmbar. Zusammenfassend wurden folgende Themen bearbeitet:

- Anpassung des Informationssicherheitskonzeptes an die Hochschule
- Initialisierung des Informationssicherheitsprozesses
- Ressourcen für IT-Sicherheit und Aufbauorganisation
- Abgrenzung des Geltungsbereichs
- Definition einer Informationssicherheitspolitik
- Risikomanagement
- Umgang mit dezentralen IT-Strukturen
- Vorfall- und Ereignismanagement
- Schnittstelle zum Notfall- und Krisenmanagement

Parallel wurden zwei Workshops mit allen Hochschulen geplant und durchgeführt (21.11.2022 und 05.12.2022). Die Workshops umfassten folgende Themen:

- Awareness-Maßnahmen für Hochschulangehörige, Schulungskonzeption, Schulungsplattform und -angebot:
    - Zielgruppen der Awareness-Maßnahmen
    - Konzeption der Pflichtinhalte und optionalen Inhalte
    - Prüfung der Möglichkeiten des zentralen Betriebs durch eine Brandenburgische Hochschule sowie Übersicht von Anbietern
    - Maßnahmenplanung zur weiteren Bearbeitung
- Kompetenzprofile und Weiterbildungsmaßnahmen für Informationssicherheitsbeauftragte und IT-Sicherheitsverantwortliche
    - Definition von Zielgruppen für Weiterbildungsmaßnahmen (Identifikation kritischer Rollen)
    - Anforderungsanalyse / Qualifikationsprofile
    - Weiterbildungsziele
    - Bedarfsanalyse innerhalb der Hochschulen
    - Maßnahmenplanung zur weiteren Bearbeitung
- Steuerung von Dokumentation, Dokumentenmanagement
    - Anforderungsanalyse
    - Vorstellung bestehender Lösungen innerhalb der Hochschulen
    - Übersicht von Anbietern
    - Prüfung der Möglichkeiten des zentralen Betriebs durch eine Brandenburgische Hochschule
    - Maßnahmenplanung zur weiteren Bearbeitung
- Risikomanagement für die Informationssicherheit: Minimallösungen zum Einstieg (Impulsvortrag mit anschließender Diskussion)
    - Warum ist ein Risikomanagement für die Konzeption der Informationssicherheit sinnvoll?
    - Was braucht es mindestens, um den Einstieg zu finden?

    - Ist die Frage der Methodik (ISO 27001 vs. IT-Grundschutz) in der Konzeptphase von Relevanz?
- Funktion des ISB an der Hochschule (als Gruppendiskussion)
    - Welche von persönlichen und fachlichen Anforderungen werden an den ISB gestellt (z. B. Aus- und Weiterbildungen)?
    - Welche Anforderungen bestehen an die Funktion (z. B. Position, Zeitbudget, Eingliederung in die Organisation, notwendige Befugnisse)?
- Stärkung und Formalisierung des Austausches zwischen den Hochschulen
    - Welche Ressourcen sind für die Verstetigung der Arbeitsgruppe notwendig?
    - Welche gemeinsamen Prozesse und Strukturen (z. B. für Audits) sind denkbar?

Das Projekt endete formal am 31.12.2022.

3. Ergebnisse des Projekts

3.1 Ausgangssituation zu Projektbeginn

Mit der ersten Phase des Projektes „IT-Konzepte, Portfolio gemeinsamer Vorlagen und Mustern an den Brandenburgischen Hochschulen“ wurde ein standardisierter Dokumentensatz für ein Informationssicherheitskonzept erarbeitet. Der Umgang der einzelnen Hochschulen mit den entstandenen Richtlinien war unterschiedlich. In vielen Fällen wurde mit einer Anpassung der Vorlagen bereits nach dem Abschluss der ersten Phase begonnen. In anderen Fällen erfolgten bis zum Beginn der zweiten Projektphase, die in diesem Bericht adressiert wird, kaum Aktivitäten.

Der Stand der einzelnen Hochschulen zu Projektbeginn ist detailliert in hochschulspezifischen Berichten dokumentiert.

Zusammenfassen lässt sich feststellen, dass in allen Hochschulen zu Beginn der Projektphase die Funktion eines Informationssicherheitsbeauftragten (ISB) zur Disposition stand. Der Stand Bearbeitung der einzelnen Bestandteile des ISK war unterschiedlich, zumeist wurden aber erst einzelne Dokumente bearbeitet oder mit der Arbeit an diesen begonnen.

3.2 Stand zum Ende des Projektes

In allen Hochschulen konnte zum Ende des Projektes, trotz der kurzen Projektlaufzeit, eine Steigerung des Reifegrades erreicht werden. Im Mittel betrug die Steigerung 0,5 Punkte (ausgenommen TH Brandenburg und TH Wildau[1]).

Die Mittelwerte zum Stand der Informationssicherheit sind in Abbildung 2 dargestellt.

[1] Die TH Wildau betreibt ein zertifiziertes ISMS nach ISO 27001 mit einem entsprechend hohen Reifegrad. Um das Ergebnis nicht zu verfälschen, wurden die Werte nicht in die Berechnung einbezogen. Aufgrund fehlender Partizipation im Projekt wurden für die TH Brandenburg keine Werte erhoben.

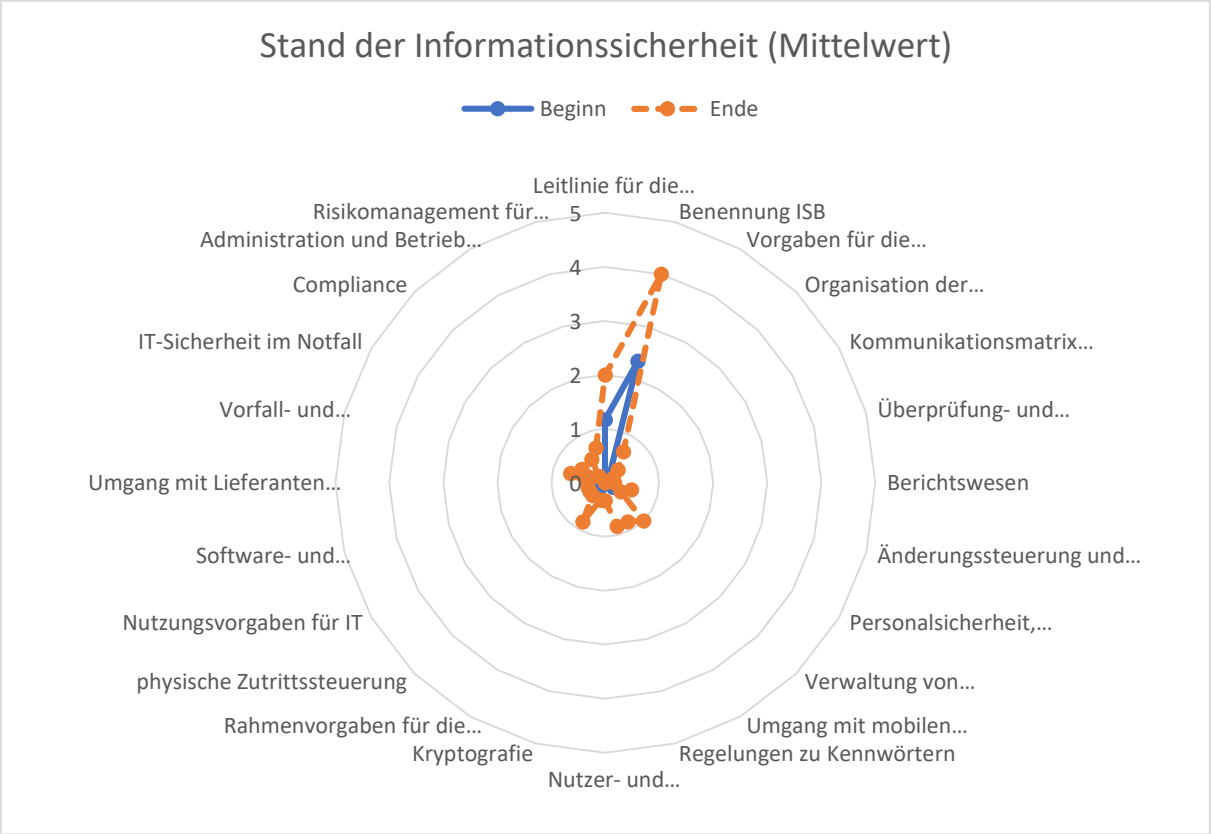

Abbildung 2: Mittlere Entwicklung des Standes der Informationssicherheit (siehe auch Fußnote 1)

Zum Ende des Projektes waren die wesentlichen Grundlagen an allen Hochschulen geschaffen, um das ISK zu planen und zu implementieren.

Die Workshops haben zudem wichtige Erkenntnisse über die Möglichkeiten der weiteren Zusammenarbeit aufgezeigt. Zum einen konnte ein gemeinsames Verständnis über Vorgehensweisen bei der Implementierung des ISK gewonnen werden. Zum anderen wurde ein fachlicher Austausch zu spezifischen Fragestellungen vorangetrieben. Beispielhaft ist hier die Stellung der/s Informationssicherheitsbeauftragten innerhalb der Einrichtungen zu nennen.

Die in Kapitel 1 vorgestellten Ziele des Projektes wurden alle erreicht. Das Projekt wurde zeitgerecht, in vollem Umfang und im vereinbarten Budgetrahmen abgeschlossen.

4. Kritische Betrachtung des Projektvorhabens

Das Projekt konnte erfolgreich abgeschlossen werden. Die Zusammenarbeit zwischen den Hochschulen stellte sich als effektiv dar und war für die Erreichung der Projektziele hilfreich.

Der Zeitrahmen für die Projektdurchführung war sehr knapp bemessen, so dass die hochschulindividuellen Beratungstermine eng getaktet werden mussten. In Nachfolgeprojekten sollte berücksichtigt werden, dass die Einrichtungen zwei bis vier Wochen nach einem Beratungstermin benötigen, um die besprochenen Inhalte umzusetzen. Aufgrund des Umfanges der Beratertage war der Zeitrahmen im vorliegenden Projekt nicht ausreichend.

Eine Hochschule beteiligte sich nicht aktiv an den Workshops. Zudem wurde an dieser nur ein Beratungstermin durchgeführt. Das übrige Kontingent konnte, nach Rücksprache mit der Projektleitung, umverteilt werden. Aufgrund der fehlenden Partizipation konnte kein umfassendes Bild zum Stand der Informationssicherheit gewonnen werden. Für künftige Projekte sollte über eine Malus-Regelung für die Nicht-Inanspruchnahme von bereitgestellten Ressourcen nachgedacht werden.

5. Empfehlungen zum weiteren Vorgehen

Die Fortsetzung der Bemühungen in Bezug auf die Etablierung wirksamer Informationssicherheitsstrukturen an den Brandenburgischen Hochschulen wird empfohlen. An den aktiv beteiligten Hochschulen wurde die Grundlage für eine wirksame Steuerung der Informationssicherheit geschaffen. Es ist festzustellen, dass die Bedarfe der Hochschulen, trotz vergleichbaren Kontexten, unterschiedlich sind. Insofern sollte bei künftigen Projekten mehr Raum für die individuellen Bedarfe der Hochschulen geschaffen werden.

Konkret werden zudem folgende Empfehlungen für das weitere Vorgehen gegeben:

- Externe Unterstützung zur Planung, Initiierung und Umsetzung des Informationssicherheitsprozesses an den Hochschulen auf Basis des ISK sollte allen Projektbeteiligten bereitgestellt werden. Hierbei sollte ein Umsetzungszeitraum von mindestens 12 Monaten angenommen werden. Der externe Beratungsaufwand je Hochschule ist in Abhängigkeit des Reifegrades der Hochschule auf 10 bis 20 Beratertage je Hochschule einzuschätzen.
- Nach der Umsetzung des ISK sollten die Strukturen zu einem zertifizierungsreifen ISMS weiterentwickelt werden. Hierfür ist ein zusätzlicher Umsetzungszeitraum von mindestens 24 Monaten anzusetzen. Auch hier ist von einem reifegradabhänigen Volumen an externen Beratungsaufwand auszugehen. Dieser wird stark durch die Größe, Struktur und Grad der Dezentralisierung der IT der Hochschule beeinflusst.
- Die im Projekt geschaffene Basis zum persönlichen Austausch der Verantwortlichen für Informationssicherheit sollte verstetigt werden. Hierbei ist zu gewährleisten, dass der Austausch moderiert und durch fachliche Impulse begleitet wird. Für die Moderation des Austausches sind personelle Ressourcen zu benennen und eine feste Tagesordnung zu definieren. Die Austauschplattform sollte formal an das ZDT angegliedert werden und regelmäßig an RIT, CIOs und das MWFK berichten. Zudem muss eine Infrastruktur

bereitstehen, die gemeinsame Arbeiten an den Themen ermöglicht. Die Verstetigung der Austauschplattform bietet folgende Mehrwerte:

- Weiterbildung
- Austausch über Vorfälle, Debriefing
- Anpassung der Vorlagen/ISK
- Datenaustauschplattform
- aktuelle Schwerpunktthemen an den jeweiligen Hochschulen
- fachlicher Austausch
- gemeinsame Beschaffung von Volumenlizenzen
- gemeinsame Auditierung / Gap-Analysen
- gemeinsame dauerhafte Schulungskonzepte

· Die Ausgestaltung und Stellung des ISB ist an den Hochschulen sehr unterschiedlich. Dies betrifft auch die Eingruppierung. Im Rahmen eines Workshops wurden folgende Empfehlungen erarbeitet:
Die Position muss derart eingebunden sein, dass sie sowohl über die Geschehnisse des Tagesgeschäfts der IT informiert ist, als auch die notwendigen Befugnisse hat, um Themen der Informationssicherheit umzusetzen. Die Schaffung einer Stabsstelle stellt eine mögliche Lösung dar. Die Funktion des ISB muss als Vollzeitstelle ausgestattet sein, die einen klaren Arbeitsauftrag seitens der Hochschulleitung erhält (Was? Bis wann? Womit?). Der Umfang der Arbeiten ist bis zur vollständigen Einführung eines ISK an allen Hochschulen gleich groß. Somit ist gerade in den ersten Jahren nicht davon auszugehen, dass ein ISB als Nebentätigkeit oder eine ½ VZE die anstehenden Aufgaben angemessen abbilden kann. Die Neutralität und Unabhängigkeit müssen gewährleistet werden.

· Die Betriebskosten des ISMS sollten in einem eigenen Budget vom ISB verwaltet werden.

· Es sollte ein Brandenburg-einheitliches Aus- und Weiterbildungsprogramm für Fachkräfte für Informations- und IT-Sicherheit geschaffen werden, um einen einheitlichen Mindestausbildungsstand zu gewährleisten.

· Die weitere Umsetzung des ISK an den Einrichtungen bedarf der ständigen Überprüfung, um die Wahrnehmung für das Thema zu schärfen. Der Stand der Informationssicherheit an den Einrichtungen sollte regelmäßig, Empfehlung einmal jährlich, durch ein unabhängiges Audit überprüft werden. Dies kann durch Dritte oder durch die Hochschulen untereinander erfolgen. Zudem sollte Informationssicherheit ein immanenter Teil der Vereinbarungen mit den Hochschulleitungen sein. Dies kann auch die Vorbereitung für eine Regulierung der Informationssicherheit an Forschungseinrichtungen im Sinne der NIS2-Richtlinie[2] sein.

[2] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555&from=DE