# Abschlussbericht

## „Erarbeitung von Informationssicherheitskonzepten“

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:**

01.05.2021 – 30.06.2022

**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

Abbildungsverzeichnis ..... 3
Abkürzungsverzeichnis ..... 4
1.Einleitung ..... 5
2. Problemstellung ..... 5
2.1 Projektziele ..... 6
3. Projektvorgehen und Ablauf ..... 6
3.1 Projektteam ..... 6
3.2 Projektphasen und zeitlicher Ablauf ..... 7
3.3 Methodik der Zusammenarbeit zur Erstellung des ISK ..... 9
4. Ergebnisse des Projekts ..... 9
4.1 Ausgangssituation zu Projektbeginn ..... 9
4.2 Inhalt und Umfang des ISK ..... 12
4.3 Stand zum Ende des Projektes ..... 13
4.4 Erreichung der Projektziele ..... 13
5. Kritische Betrachtung des Projektvorhabens ..... 14
5.1 Rückmeldung der Teilnehmer ..... 14
5.2 Bewertung der Projektleitung ..... 15
6. Empfehlungen zum weiteren Vorgehen ..... 16
Anlage 1: Fragebogen zur Bestandsaufnahme inklusive übergreifender Auswertung ..... I

# Abbildungsverzeichnis

Abbildung 1: zeitlicher Projektablauf ..... 7
Abbildung 2: Verteilung der Antwortoptionen (ohne Freitextfragen) ..... 10
Abbildung 3:Befragungsergebnis: Abstimmung von Protokollierung mit dem Datenschutzbeauftragten ..... 11
Abbildung 4: Befragungsergebnis: Verantwortlichkeiten der HSL ..... 11
Abbildung 5: Befragungsergebnis: Risikobeurteilungsprozess ..... 11

# Abkürzungsverzeichnis

| | |
|---|---|
| BbgDSG | Brandenburgisches Datenschutzgesetz |
| BbgHG | Brandenburgisches Hochschulgesetz |
| DSGVO | Datenschutz-Grundverordnung |
| EZB | Europäische Zentralbank |
| ISK | IT-Sicherheitskonzept |
| ISMS | IT-Sicherheitsmanagementsystem |
| ISO | International Organization for Standardization |
| OZG | Onlinezugangsgesetz |
| PDCA | Plan-Do-Check-Act |
| ZDT | Zentrums der Brandenburgischen Hochschulen für Digitale Transformation |

# 1.Einleitung

Der vorliegende Bericht stellt den Stand zum Abschluss des Moduls 4 „Erarbeitung von Informationssicherheitskonzepten“ im Rahmen des ZDT-Projekts „IT-Konzepte, Portfolio gemeinsamer Vorlagen und Muster an den Brandenburgischen Hochschulen“ für 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 Landesbrandenburg 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.

Für Hochschulen im Land Brandenburg lassen sich mehrere Rechtsquellen identifizieren, die die Erstellung und Implementierung eines Informationssicherheitskonzeptes (ISK) verbindlich regeln. Zunächst sind Hochschulen als Verantwortliche im Sinne des Datenschutzes verpflichtet, „geeignete technische und organisatorische Maßnahmen [umzusetzen], um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“, wenn sie personenbezogene Daten verarbeiten (Art. 32 Nr. 1 DSGVO). Ähnliches regelt § 4 Abs. 1 Nr. 2 BbgDSG. Die datenschutzrechtlichen Anforderungen beziehen sich ausschließlich auf die Verarbeitung personenbezogener Daten im Sinne von Art. 4 Nr. 1 und 2 DSGVO.

Weitergehende Regelungen enthalten das Brandenburgische E-Government-Gesetz (§ 16) sowie das OZG (§ 5), welche für den jeweiligen Geltungsbereich ebenfalls die Gewährleistung angemessener technischer und organisatorische IT-Sicherheitsmaßnahmen fordern. Ausgehend von den Anforderungen des § 26 Abs. 1 BbgHG kommt den IT-Systemen für das Lehrangebot hierbei eine besondere Bedeutung zu. Ohne ein ISK können diese Anforderungen nicht erfüllt werden.

Das ISK, das im Rahmen des Projektes zu erstellen war, dient der Umsetzung der Sicherheitsstrategie einer Organisation und beschreibt die geplante Vorgehensweise einer Hochschule, um die gesetzten Sicherheitsziele der Informationssicherheitsleitlinie zu erreichen. 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. Alle Richtlinien und Prozesse, die die Informationssicherheit an der Einrichtung steuern und verbessern, basieren auf dem ISK.

Es war explizit nicht das Ziel des Projektes ein Informationssicherheitsmanagementsystem (ISMS) zu beschreiben bzw. an den Hochschulen zu etablieren. Das Projekt grenzt sich von der Entwicklung und der Implementierung eines ISMS ab. Ein ISMS definiert Regeln und Methoden, um die Informationssicherheit in einer Hochschule zu gewährleisten, während ein ISK einen Zielzustand beschreibt. Das ISMS basiert auf Prozessen, die die Erreichung eines Zielzustandes der Informationssicherheit sowie deren kontinuierliche Verbesserung ermöglichen. Hierzu stellt das Managementsystem alle notwendigen Prozesse und Methoden für die kontinuierliche Planung, Umsetzung, Überwachung und Verbesserung im Sinne eines Plan-Do-Check-Act-Ansatzes (PDCA) zur Verfügung. Mithilfe der Planung-, Umsetzungs-, Überwachungs-, und Verbesserungsprozesse wird der im ISK als Zielzustand definierten Stand der Informationssicherheit erreicht. Ein ISMS ist insofern keine Software, kein Dokument(ensatz) und keine einzelne Rolle. Vielmehr unterstützen Softwarelösungen, Dokumente und Personen das ISMS. Das ISMS stellt ein lebendiges System dar, während das ISK die planerische Grundlage bietet. Zur Implementierung bedient sich das ISMS einer Risikomethodik, die Abweichungen vom Soll-Zustand erfasst und deren Kritikalität bewertet. Mithilfe des Risikomanagements können die größten Probleme (i. S. v. dringlich und wichtig) regelmäßig erfasst und anschließend bearbeitet werden. Durch dieses iterative Vorgehen wird mithin schrittweise das Sicherheitsniveau gesteigert. Das im Projekt zu erstellende und durch die Hochschulen anzupassende ISK bildet insofern die notwendige Bedingung für die Etablierung von ISMS an den einzelnen Hochschulen.

## 2.1 Projektziele

Das Projekt verfolgte folgende strategische Ziele:

- Die Hochschulen sollen in die Lage versetzt werden, IT-Governance-Strukturen und Prozesse in Bezug auf Informationssicherheit aufzubauen.
- Ein Erfahrungs- und Wissensaustausch soll zwischen allen teilnehmenden Hochschulen etabliert und nach dem Projekt verstetigt werden.
- Das generische ISK soll die Hochschulen in die Lage versetzen, ein effektives ISK abzuleiten.
- Ausgehend von den Projekterfahrungen sollen weitere IT-Konzepte erarbeitet werden, die Synergiepotenziale heben (Proof-of-Concept).

# 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 dem verantwortlichen Berater des Beratungsunternehmens, Herrn Rico Kerstan und seitens des ZDT, Herrn Bernd Heimer

(TH Wildau), die das Projekt fachlich und inhaltlich sowie im Sinne des Projektmanagements betreuten. Eine für die Projektunterstützung und das Projektmanagement vorgesehene Mitarbeiterin der TH Brandenburg fiel kurz nach dem Projektbeginn aus, sodass die Aufgaben an das Beratungsunternehmen (KR Krisensicher Risikoberatung GmbH) übertragen wurden.

Im Rahmen einer öffentlichen Ausschreibung wurde die KR Krisensicher Risikoberatung GmbH aus Lübben (Spreewald) mit der Projektbegleitung beauftragt. Herr Rico Kerstan verfügt sowohl über eine ingenieurswissenschaftliche Ausbildung als auch einen Abschluss in strategischem Management. Er ist als Auditor für Informationssicherheit tätig. Zudem berät Herr Kerstan Organisationen beim Aufbau und der Weiterentwicklung von ISMS. Er verfügt über langjährige Erfahrung im Risiko- und Sicherheitsmanagement. Rico Kerstan war als Risk & Security Manager bei der Bundesdruckerei GmbH für die Analyse und Umsetzung von kundenspezifischen und regulatorischen Anforderungen verantwortlich (z. B. EZB-Anforderungen und ISO 27001).

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.

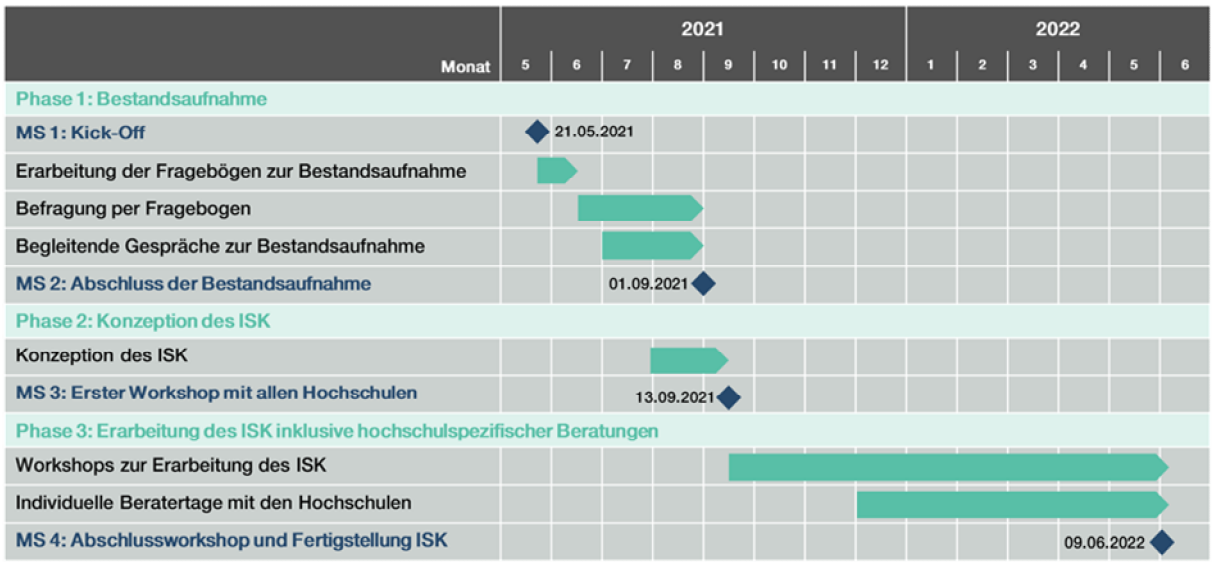



*Abbildung 1: zeitlicher Projektablauf*

Das Projekt begann am 21.05.2021 formal mit einem Kick-Off-Workshop der Projektleitung.

Die Bestandsaufnahme an den teilnehmenden Hochschulen verfolgte das Ziel, die Reifegrade unterschiedlicher Aspekte der Informationssicherheit zu erheben. Hierzu wurde ein standardisierter Fragebogen erarbeitet. Die Fragen sind in Anlage 1 zu finden. Der Fragebogen wurde im Juni 2021 an alle teilnehmenden Hochschulen versendet. Die finale Auswertung erfolgte im September. Alle angefragten Hochschulen haben an der Befragung teilgenommen.

Parallel zur Befragung wurde, nach dem Eintreffen der ersten Befragungsergebnisse, mit persönlichen Gesprächen zwischen der Projektleitung und den Ansprechpartnern der teilnehmenden Hochschulen begonnen. Die Gespräche dienten dazu, die Ergebnisse der fragebogenbasierten Auswertung zu verifizieren und mit qualitativen Antworten zu unterlegen. Die Bestandsaufnahme war am 01.09.2021 mit dem letzten Gesprächstermin abgeschlossen.

Die Bestandsaufnahme wurde durch eine zeitlich parallel stattfindende, jedoch vom Projekt losgelöste, Prüfung des Landesrechnungshofes unterstützt.

Die Ergebnisse der Bestandsaufnahme wurden durch die Projektleitung ausgewertet und sowohl das inhaltliche als auch das methodische Vorgehen für die Erarbeitung des ISK definiert. Es wurde herausgestellt, dass das ISK aus mehreren, modular zusammensetzbaren Dokumentenvorlagen bestehen soll. Die Vorlagen sollten als Richtlinien ausgestaltet werden, die durch Anpassung in Regelungen der Hochschulen überführt werden können.

Im nächsten Projektschritt wurden Vorlagen für das ISK, insbesondere Richtlinien, erarbeitet. Basierend auf den Feststellungen der Bestandsaufnahme konnte im Zuge der Erarbeitung der Vorlagen nur in geringem Maß auf Vorhandenes zurückgegriffen werden. Die Projektleitung entschied daher, dass die Richtlinien- und Dokumentenvorlagen durch die KR Krisensicher Risikoberatung GmbH vorformuliert und durch die Teilnehmer angepasst werden. Vorlagen für Checklisten und Anträge sollten durch die Hochschulen bereitgestellt werden. Die Erarbeitung der Vorlagen erfolgte in 10 Workshops sowie nachgelagerten Arbeitsphasen von in den Workshops gegründeten Arbeitsgruppen.

Ab Dezember 2021 wurden begleitend zur Erarbeitung des ISK hochschulindividuelle Beratungstermine vereinbart. Die projektbegleitende Beratung der einzelnen Hochschulen lief bis zum Abschlussworkshop am 09.06.2022. Nahezu alle Hochschulen haben das Angebot in Anspruch genommen. Offene Tage wurden allen Hochschulen angeboten. Das Gesamtkontingent von 40 Beratertagen wurde so ausgeschöpft. Wenngleich die Bedarfe der Hochschulen sich unterschiedlich darstellen, lassen sich thematische Schwerpunkte feststellen:

- Vorfall- und Ereignismanagement für IT-Sicherheitsvorfälle
- Notfallmanagement innerhalb der Hochschul-IT
- Ressourcenanforderungen und -planung für die Informationssicherheit
- Vorgehensweise bei der Implementierung eines ISK
- Bearbeitung von Feststellungen des Landesrechnungshofs

Das Projekt endete formal am 09.06.2022 mit einem Abschlussworkshop. Im Rahmen dieses Workshops wurden die Teilnehmer um inhaltliches und methodisches Feedback gebeten (siehe 5.1).

## 3.3 Methodik der Zusammenarbeit zur Erstellung des ISK

Die Zusammenarbeit zwischen den Projektteilnehmern war von Beginn an darauf ausgelegt, Stärken zu stärken. Wenngleich absehbar war, dass die Einrichtungen unterschiedliche Reifegrade aufweisen, sollten die Expertise und die Erfahrungen jeder Hochschule gleichermaßen in die Projektergebnisse einfließen. Die Ergebnisse der Bestandsaufnahme wurden insofern zwar im ersten Workshop mit allen Projektteilnehmer vorgestellt, jedoch wurde kein Bezug zu einzelnen Hochschulen genommen. Ziel war es stets den Stand der Informationssicherheit an den Brandenburgischen Hochschulen insgesamt zu erörtern.

Die Erarbeitung des ISK erfolgte auf Grundlage von Dokumentenentwürfen, die durch die KR Krisensicher Risikoberatung GmbH bereitgestellt wurden. Alle Hochschulen, auch jene ohne formale Dokumentation in Bezug auf das jeweilige Themenfeld konnten so ihre Verbesserungsvorschläge einbringen.

Der Prozess der gemeinsamen Erarbeitung folgte einem iterativen Vorgehen: In den Workshops wurden fachlich-inhaltliche Impulse zu einem Themengebiet gesetzt. Im Anschluss bildeten die Teilnehmer Arbeitsgruppen, in denen sie das Thema bzw. die jeweilige Dokumentenvorlage gemeinsam bearbeiteten. Für die Bearbeitung standen in der Regel vier Wochen zur Verfügung. Die Arbeitsergebnisse wurden im nächsten Workshop präsentiert, diskutiert und das Dokument verabschiedet.

Die Zusammenarbeit erfolgte technisch auf einer NextCloud, die durch die KR Krisensicher Risikoberatung GmbH für den Projektzeitraum bereitgestellt wurde. Die Workshops wurden rein virtuell durchgeführt. Die Projektergebnisse wurden über die KR-NextCloud verteilt.

# 4. Ergebnisse des Projekts

## 4.1 Ausgangssituation zu Projektbeginn

Die Bestandsaufnahme zu Projektbeginn zeigte einen übergreifenden Stand der Informationssicherheit an den Brandenburgischen Hochschulen. Die Ergebnisse der Bestandsaufnahme decken sich mit den Prüfergebnissen des Landesrechnungshofes[1]. Es ist festzustellen, dass alle Hochschulen über technische IT-Sicherheitsmaßnahmen – unterschiedlicher Ausprägung und Wirksamkeit – verfügten. In den meisten Hochschulen fehlen jedoch Planungs- und Steuerungsprozesse für die Informationssicherheit und die IT-Governance.

Positiv ist hervorzuheben, dass alle Befragten über ein hohes fachliches Niveau in Bezug auf IT-Sicherheit verfügen. In der Regel war den Befragten bewusst, welche Maßnahmen theoretisch zur Erreichung eines hohen Informationssicherheitsniveaus notwendig wären.

Der Fragebogen für die Bestandsaufnahme (siehe Anlage 1) ließ entweder die Auswahl aus „ja“, „nein“, „teilweise“ und „Ich kann diese Frage nicht beantworten“ zu oder es war eine

[1] Landesrechnungshof Brandenburg: Jahresbericht 2021, S. 173 ff.

Freitexteingabe möglich. Er beinhaltete 115 Fragen mit Auswahloption. Keine Hochschule beantwortete alle 115 Auswahlfragen mit „ja“. Der höchste Wert der Ja-Antworten einer Hochschule, betrug 76,5 % (n = 88). Der niedrigste Wert betrug 1,7 % (n = 2), wobei in diesem Fall die beantwortende Person erst seit wenigen Tagen mit dem Thema Informationssicherheit befasst war. Der zweitniedrigste Wert betrug 11,3 % (n = 13). Die Verteilung der Antworten auf die Antwortoptionen ist in Abbildung 2 dargestellt. Der Erfüllungsgrad (Fragen mit „ja“ beantwortet / Anzahl der Fragen mit Antwortoptionen) liegt im Median bei 30,8 %, wobei im Median 7,4 % der Fragen mit „Ich kann diese Frage nicht beantworten“ und 18,3 % mit „teilweise“ beantwortet wurden. Es ist erkennbar, dass einzelne Hochschulen deutlich vom Median abweichen.

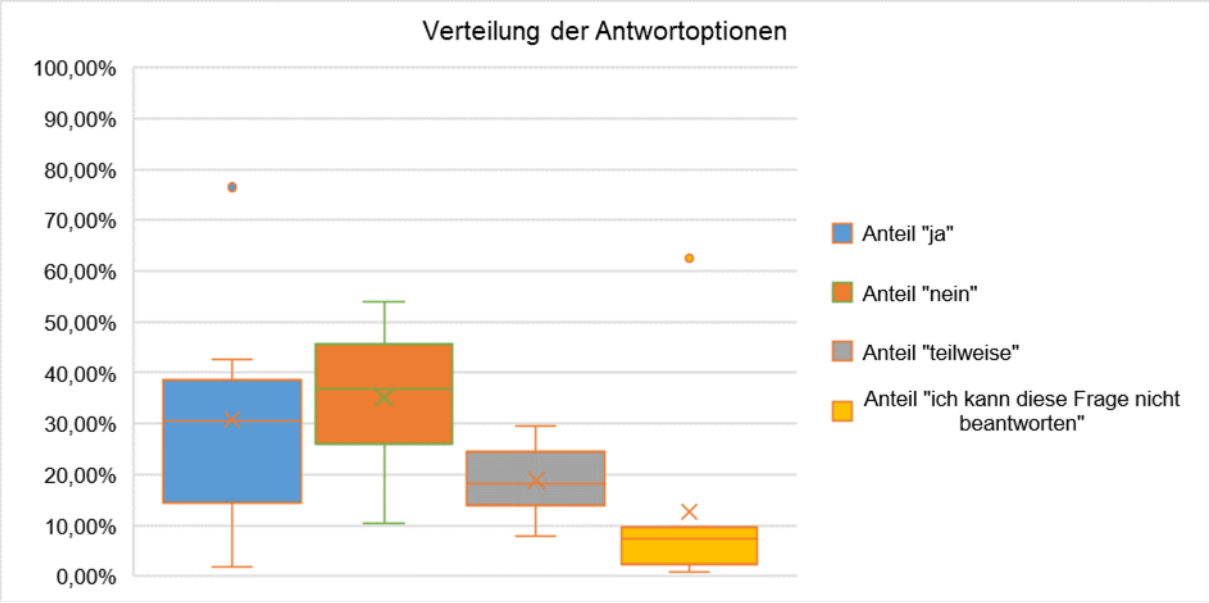



*Abbildung 2: Verteilung der Antwortoptionen (ohne Freitextfragen)*

Diese quantitative Auswertung deckt sich mit den Ergebnissen der begleitenden Gespräche zur Bestandsaufnahme: Einzelne Hochschulen verfügten bereits über einen hohen Stand der Informationssicherheit. Hingegen einige Hochschulen nur rudimentäre Strukturen zu diesem Zeitpunkt etabliert hatten. Die Hochschule mit den reifsten Strukturen für die Informationssicherheit beantwortete in Summe 87,8 % der Fragen mit „ja“ oder „teilweise“. Die darauffolgende Einrichtung erreichte 63,5 % (davon 35,7 % „ja“).

Mit dem Blick auf einzelne Fragen und Themenkomplexe lässt sich feststellen, dass vor allem gesetzliche Anforderungen mit Sanktionsrisiken bei Nichterfüllung umgesetzt werden. Ein Datenschutzbeauftragter war zum Zeitpunkt der Befragung an allen Hochschulen bestellt, ein Informationssicherheitsbeauftragter hingegen nur an vier Einrichtungen. Im Detail erfolgt die wirksame Implementierung datenschutzrelevanter Aspekte jedoch nur an einem Teil der Hochschulen, wie Abbildung 3 exemplarisch zeigt.

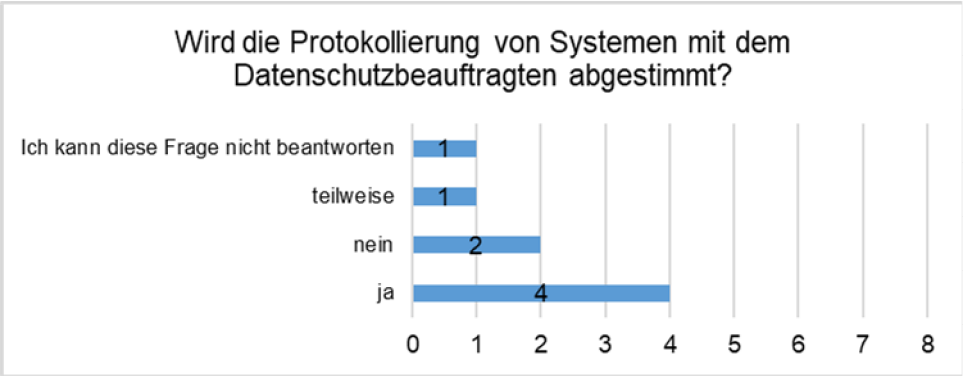



*Abbildung 3:Befragungsergebnis: Abstimmung von Protokollierung mit dem Datenschutzbeauftragten*

Eine mögliche Ursache könnten der Grad der Verantwortungsübernahme bzw. -definition durch die Hochschulleitungen (HSL) und die Implementierung der damit verbundenen Steuerungswerkzeuge sein, wie Abbildung 4 und Abbildung 5 beispielhaft zeigen.

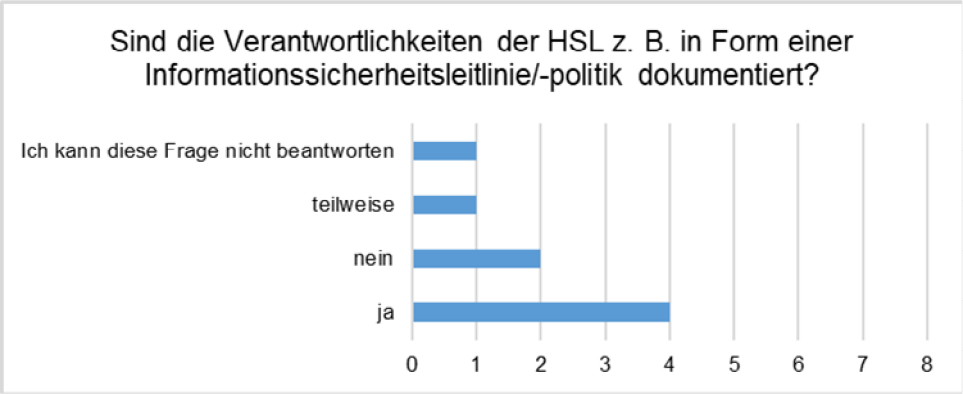



*Abbildung 4: Befragungsergebnis: Verantwortlichkeiten der HSL*

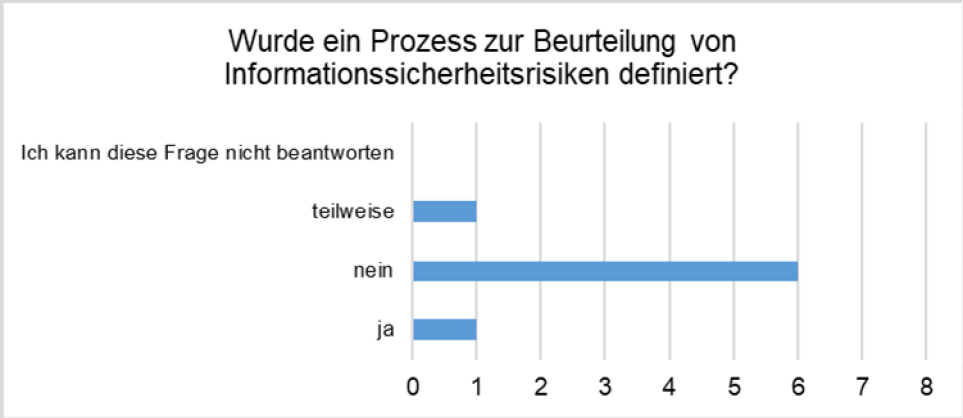



*Abbildung 5: Befragungsergebnis: Risikobeurteilungsprozess*

Zusammenfassend ließen sich aus der Bestandsaufnahme folgende Feststellung ableiten:

- Es liegen an wenigen Hochschulen freigegebene und bekanntgemachte Richtlinien und Prozesse für die Informationssicherheit vor.
- Es existieren nur an einer Hochschule Informationssicherheitsstrukturen und -prozesse, die die gesamte Hochschule umfassen.
- Informationssicherheit wird in der Regel als Erfüllung von externen Anforderungen betrieben.

- An den meisten Hochschulen stehen keine oder nicht ausreichende Ressourcen für eine wirksame Steuerung der Informationssicherheit zur Verfügung, teilweise ist die Verantwortung nicht definiert und delegiert.
- Die Dezentralisierung von IT-Strukturen schafft eine Komplexität, insbesondere an den Universitäten mit technischen Studiengängen, die schwer erfasst und gesteuert werden kann.
- Die Hochschulen sind untereinander nur in geringem Umfang und nicht strukturiert vernetzt. Jede Hochschule schafft eigene Insellösungen.

## 4.2 Inhalt und Umfang des ISK

Das ISK wurde derart konzeptioniert, dass den Hochschulen konkrete Dokumentenvorlagen für die Schaffung grundlegender Regelungen an die Hand gegeben wurden. Das ISK folgt bewusst keiner vordefinierten Methodik (z. B. ISO 27001 nativ, BSI-IT-Grundschutz), um den Hochschulen Wahl- und Handlungsfreiheit zu gewähren.

Das erarbeitete ISK umfasst folgende Themengebiete:

- Vorgaben für die Dokumentation von Informationssicherheitsrichtlinien
- Organisation der Informationssicherheit (Rollenkonzept)
- Kommunikationsmatrix (intern / extern)
- Überprüfung- und hochschulinterne Auditprozesse
- Berichtswesen
- Änderungssteuerung und Projektmanagement
- Personalsicherheit, Kompetenz und Ausbildung
- Verwaltung von Informationswerten (Asset-Management), Nutzung, Archivierung und Entsorgung von Werten
- Umgang mit mobilen Endgeräten
- Kennwörter
- Nutzer- und Rechteverwaltung
- Kryptografie
- Rahmenvorgaben für die physische Sicherheit von IT-Räumen
- physische Zutrittssteuerung
- Nutzungsvorgaben für IT
- Software- und Systementwicklung
- Umgang mit Lieferanten und Dienstleistern
- Vorfall- und Ereignismanagement
- IT-Sicherheit im Notfall

- Compliance
- Administration und Betrieb von IT
- Risikomanagement für Informationssicherheit

Für jedes Themengebiet wurde eine Dokumentenvorlage geschaffen und durch die Projektmitglieder verabschiedet. Das ISK, das aus dem Projekt entstanden ist, stellt insofern eine Sammlung von Dokumentenvorlagen dar. Das Arbeitsergebnis wurde als ZIP-Ordner zum Download bereitgestellt.

## 4.3 Stand zum Ende des Projektes

Zum Ende des Projektes fand planmäßig keine Erhebung des Standes der Informationssicherheit statt. Eine quantitative Auswertung liegt nicht vor. Aktuell sind in den Hochschulen sehr viele Aktivitäten mit der Zielsetzung einer Weiterentwicklung der Informationssicherheit der Einrichtung zu verzeichnen.

Es lässt sich qualitativ übergreifend feststellen, dass die Zusammenarbeit der Projektmitglieder im Verlauf – auch außerhalb der Projekttermine und Arbeitsgruppen – intensiviert wurde.

Die Arbeitsgruppen haben produktiv und diszipliniert die jeweiligen Themen bearbeitet. Alle Themen wurden adressiert und alle geplanten Dokumentenvorlagen wurden im Verlauf des Projektes verabschiedet.

Die hochschulindividuellen Beratungstermine haben häufig die Feststellungen des Landesrechnungshofes adressiert und konkrete Ergebnisse in Bezug auf die Erreichung der Termine zur Abstellung von Mängeln erzeugt.

## 4.4 Erreichung der Projektziele

Die in Kapitel 1 vorgestellten Ziele des Projektes wurden allesamt erreicht. Das Projekt wurde zeitgerecht, in vollem Umfang und im vereinbarten Budgetrahmen abgeschlossen. Das erarbeitete ISK umfasst alle geplanten Themen und liefert qualitativ hochwertige Vorlagen für ein ISK. Die teilnehmenden Hochschulen sind in die Lage versetzt ein effektives ISK für die eigene Einrichtung abzuleiten und im Anschluss zu implementieren.

# 5. Kritische Betrachtung des Projektvorhabens

## 5.1 Rückmeldung der Teilnehmer

Die Projektteilnehmer wurden im Rahmen des Abschlussworkshops am 09.06.2022 um qualifiziertes Feedback zum Projektverlauf und der -methodik gebeten. Die nachstehenden Ergebnisse sind eine Zusammenfassung der Rückmeldungen. Mehrfachnennungen sind nicht hervorgehoben. Es fand keine Wertung der Projektleitung statt.

**Positive Rückmeldungen**

- Das Engagement der Teilnehmer ermöglichte eine effektive Projektumsetzung.
- Das Format der Zusammenarbeit gewährleistete Offenheit und Austausch auf der Arbeitsebene.
- Der fachliche Austausch half den Teilnehmern an der eigenen Einrichtung.
- Das Ergebnis (ISK) stellt eine wesentliche Arbeitserleichterung und Ressourceneinsparung für die Entwicklung eines hochschulindividuellen ISK dar.
- Die Themensetzung war angemessen und effektiv.
- Die Art der Zusammenarbeit war effektiv und produktiv.

**Negative Rückmeldungen**

- Der Wechsel der Ansprechpartner einzelner Hochschulen im Projektverlauf führte zu Irritationen.
- Die hochschulindividuelle Beratung begleitend zur Entwicklung des ISK erfolgte zu früh und hätte nach Fertigstellung erfolgen sollen.
- Die vom Beratungsunternehmen gelieferten Vorlagen hätten in Teilen mehr spezifische Anforderungen von Brandenburgischen Hochschulen beinhalten können.

**Erkenntnisse der Teilnehmer**

- Das Thema „Informationssicherheit“ ist spannend und eine intensivere Auseinandersetzung lohnt sich.
- Die Hochschulen haben in weiten Teilen ähnliche Herausforderungen bei der Implementierung von Informationssicherheit („geteiltes Leid“).
- Es bleiben viele Baustellen an der eigenen Einrichtung offen, über die nun aber mehr Klarheit herrscht.

**Wünsche**

- Eine längere Projektlaufzeit wäre, insbesondere für die hochschulspezifische Beratung, hilfreich gewesen.
- Einzelne Themen sollten weiter vertieft werden.
- Der Austausch sollte verstetigt werden.
- Die BSI-Grundschutzmethodik sollte ein Schwerpunkt sein.

## 5.2 Bewertung der Projektleitung

Die Projektleitung bewertet das Projektvorgehen sowie das -ergebnis als positiv. Die Zusammenarbeit zwischen den Hochschulen stellte sich als effektiv dar und war für die Erreichung der Projektziele hilfreich.

Es zeigt sich, dass das iterative Vorgehen und die Zusammenarbeit der Arbeitsgruppen wirksam funktionierten. Festzustellen ist, dass beides einer engen Steuerung bedurfte. Es ist davon auszugehen, dass ohne diese Steuerung die Projektziele nicht vollständig im vereinbarten Zeitraumen zu erreichen gewesen wären.

In Bezug auf die Bestandsaufnahme ist festzustellen, dass die Befragungstiefe für den Stand der Informationssicherheit an den Hochschulen zu detailliert war. Mehrwertstiftend waren in diesem Zusammenhang die Gespräche zur Bestandsaufnahme, die den Teilnehmern die Möglichkeit boten, den Stand in einem vertraulichen Rahmen zu erörtern. An einzelnen Einrichtungen konnte der Sinn bestimmter Fragen und der Bezug zur Informationssicherheit erst im Gespräch erklärt werden.

Die von den Teilnehmern kritisierte Projektlaufzeit, wird im Hinblick auf die Projektziele, als ausreichend bewertet. Wenngleich die hochschulspezifischen Beratertage in Teilen mehr als Maßnahmen zur Sensibilisierung verstanden werden können, denn als Umsetzungsworkshops, scheint dies der Steigerung der Informationssicherheit an den Hochschulen zuträglich. Es ist nicht davon auszugehen, dass die Durchführung der Beratungen nach der Finalisierung zu anderen Ergebnissen geführt hätte. Dies ist im Wesentlichen der Ausgangssituation geschuldet. Festzustellen ist, dass der Beratungsbedarf an den Hochschulen die Anzahl an bereitgestellten Beratertagen deutlich übersteigt.

In Bezug auf die inhaltliche Ausgestaltung des ISK und die zugrundeliegende Methodik, stellt die Projektleitung fest, dass eine Fokussierung auf den BSI-IT-Grundschutz, wie gewünscht, weder zum Zeitpunkt des Projektes noch einheitlich für alle Hochschulen in Brandenburg sinnvoll erscheint. Zum einen sind die Unterschiede der Methoden zwischen BSI-IT-Grundschutz und nativem Vorgehen nach ISO 27001 zum Zeitpunkt der Erstellung des ISK wenig relevant. Zum anderen muss die Auswahl einer Methodik auch den externen Anforderungen an die Hochschulen gerecht werden. Beispielsweise können Transferpartner aus der Wirtschaft spezifische Zertifizierungsanforderungen stellen (wie im Falle der TH Wildau) oder internationale Forschungspartner stellen solche Anforderungen. Insbesondere in den genannten Kontexten, scheint die gewünschte Fokussierung auf den BSI-IT-Grundschutz, die vor allem national Anerkennung genießt, nicht hilfreich. Das BSI hält auf seiner Webseite eine

Liste mit bestehenden Zertifikaten ISO27001 auf Basis IT-Grundschutz [2]vor. Aktuell sind 144 Zertifikate erteilt. Keines davon ist direkt einer Hochschule zuzuordnen – es existieren jedoch zwei Zertifikate mit entsprechendem Bezug: eine Uniklinik und eine Datentreuhandstelle einer Medizinischen Fakultät. Mit Stand 31.12.2020 waren in Deutschland 3.367 Standorte auf Basis ISO 27001 zertifiziert (insgesamt 1.281 Zertifikate). Im Rahmen der ISO-Zertifizierung können mehrere Standorte unter ein Zertifikat fallen (Multi-Site-Zertifizierung). 187 Zertifikate entfielen auf den Sektor „Bildung" (Branchenscope 33 nach IAF). Eine weitere Konkretisierung wird durch die International Organization for Standardization nicht vorgenommen[3]. Es ist jedoch bekannt, dass mehrere Hochschulen über eine Zertifizierung nach ISO 27001 verfügen[4]. Aus Sicht der Projektleitung resultierte die Präferenz der Teilnehmer, die sich eine stärkere Fokussierung auf die Grundschutz-Methodik wünschten, zudem vor allem aus der beruflichen Vorprägung.

# 6. Empfehlungen zum weiteren Vorgehen

Die Fortsetzung der Bemühungen in Bezug auf die Etablierung wirksamer Informationssicherheitsstrukturen an den Brandenburgischen Hochschulen wird dringend empfohlen. Das im Projekt erarbeitete ISK stellt eine wesentliche Basis für diesen Prozess dar. Der im ISK etablierte Standard bildet zudem eine Grundlage für weitere Skalierungspotenziale.

Konkret werden zudem folgende Empfehlungen für das weitere Vorgehen gegeben:

- Externe Unterstützung zur Initiierung des Informationssicherheitsprozesses an den Hochschulen auf Basis des ISK sollte allen Projektbeteiligten bereitgestellt werden. Hierbei sollte ein Betreuungszeitraum von mindestens 12 Monaten angenommen werden. Der Beratungsaufwand wird, in Abhängigkeit des Reifegrades der Hochschule, auf 10 bis 30 Beratertage je Hochschule geschätzt.
- Die im Projekt geschaffene Basis zum persönlichen Austausch der Verantwortlichen für Informationssicherheit sollte verstetigt werden. Hierbei sollte gewährleistet werden, dass der Austausch moderiert und durch fachliche Impulse begleitet wird. Konkret bieten sich Workshops zu den Themen Awarenessmaßnahmen für Hochschulangehörige, Weiterbildungsmaßnahmen für Informationssicherheitsbeauftragte und IT-Sicherheitsverantwortliche, Lenkung und Steuerung von Dokumentation sowie gemeinsame Prozesse und Strukturen für gegeneitige Audits und Überprüfungen an.

[2] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Managementsystemen/ISO-27001-Basis-IT-Grundschutz/ErteilteZertifikate/iso27001zertifikate_node.html

[3]https://isotc.iso.org/livelink/livelink?func=ll&objId=21901590&objAction=Open&nexturl=%2Flivelink%2Flivelink%3Ffunc%3Dll%26objId%3D18808772%26objAction%3Dbrowse%26viewType%3D1

[4] Beispielhaft: https://www.tuvsud.com/de-de/wissenswert/newsletter/value-newsletter/1-2022/universitaet-freiburg-tuev-sued-zertifiziert-it-sicherheitsmanagement, https://www.wiesentbote.de/2020/05/25/jetzt-zertifiziert-informationssicherheit-an-der-universitaet-bayreuth/ sowie TH Wildau

- Es sollte ein Brandenburg-einheitliches Aus- und Weiterbildungsprogramm für Fachkräfte für Informations- und IT-Sicherheit geschaffen werden, um einen einheitlichen Mindestausbildungsstand zu gewährleisten.
- Die Initiierung des Informationssicherheitsprozesses sowie die Implementierung von wirksamen Informationssicherheitsstrukturen im Sinne eines ISMS erfordern Ressourcen. Die Hochschulen sollten mit ausreichenden Mitteln ausgestattet werden, um für die Steuerung des Prozesses ein Vollzeitäquivalent an jeder Einrichtung zu schaffen. Die Ressourcen sollten langfristig durch externe Beratungsexpertise oder ein Expertenteam aus den Hochschulen ergänzt werden.
- Die Hochschulen verfügen über unterschiedliche fachliche Niveaus und Schwerpunkte, insbesondere ausgehend von der Profilierung der Einrichtung. Durch eine Cluster- oder Schwerpunkt-Bildung könnten die Stärken einzelner Hochschulen auch an anderen Hochschulen nutzbar gemacht werden, z. B. im Rahmen von Inhouse-Beratungen.
- Die Reaktion auf Vor- und Notfälle an den Hochschulen ist wenig geplant. Der Beratungsbedarf in diesem Themenfeld war, obwohl es sich lediglich um ein Schnittstellenthema handelt, an größten. Ausgehend von den Erfahrungen dieses Projektes sollte ein kooperatives Projekt der Brandenburgischen Hochschulen initiiert werden, dass die Bewältigungsfähigkeit der Einrichtungen bei IT-Vor-/Notfällen und in widrigen Situationen im Allgemeinen stärkt.
- Die Prüfung des Landesrechnungshofes hatte, begleitend zum Projekt, einen wesentlichen Einfluss auf die Umsetzungsgeschwindigkeit von Maßnahmen zur Steigerung der Informationssicherheit. Es sollten verpflichtende externe Prüfungen etabliert werden (z. B. im Rahmen von Zertifizierungen oder vergleichbar mit den Nachweisen von KRITIS-Betreibern gegenüber dem BSI). Hierbei ist darauf zu achten, dass die Kerntätigkeiten der Hochschulen (Forschung, Lehre und Transfer) von den Prüfungen umfasst sind.

# Anlage 1: Fragebogen zur Bestandsaufnahme inklusive übergreifender Auswertung

## Auswertungsteil der geschlossenen Fragen

### 1. Verantwortung der HS-Leitung

1.1) Haben Sie die Verantwortlichkeiten der Hochschulleitung (HSL) definiert (Strategische Gesamtverantwortung, Risiko-/ Chancenmanagement und -vorsorge)?

n=8

| | |
|---|---|
| ja | 25% |
| nein | 37.5% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 25% |

1.2) Sind die Verantwortlichkeiten der HSL z. B. in Form einer Informationssicherheitsleitlinie/-politik dokumentiert?

n=8

| | |
|---|---|
| ja | 37.5% |
| nein | 50% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 0% |

1.3) Haben Sie strategische Sicherheitsziele abgeleitet? Sind die allgemeinen Ziele (Vertraulichkeit, Verfügbarkeit, Integrität) auf Ihrem Kontext angepasst bzw. spezifiziert?

n=8

| | |
|---|---|
| ja | 50% |
| nein | 37.5% |
| teilweise | 0% |
| Ich kann diese Frage nicht beantworten | 12.5% |

1.4) Wurde dokumentiert, was ein Informationssicherheitvorfall ist?

n=8

| | |
|---|---|
| ja | 12.5% |
| nein | 87.5% |
| teilweise | 0% |
| Ich kann diese Frage nicht beantworten | 0% |

1.5) Haben Sie einen oder mehrere Personen die operative Verantwortung für die Informationssicherheit übertragen?

n=8

| | |
|---|---|
| ja | 50% |
| nein | 25% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 12.5% |

### 2. Verantwortung des ISB

2.2) Wurden die Verantwortlichkeiten und Aufgaben des ISB dokumentiert?

n=4

| | |
|---|---|
| ja | 50% |
| nein | 0% |
| teilweise | 25% |
| Ich kann diese Frage nicht beantworten | 25% |

2.3) Wurde die Befugnisse des ISB bestimmt?

| | | n=4 |
|---|---|---|
| ja | 50% | |
| nein | 25% | |
| teilweise | 0% | |
| Ich kann diese Frage nicht beantworten | 25% | |

2.4) Haben Sie bestimmt, für welche Dokumente der ISB verantwortlich ist?

| | | n=4 |
|---|---|---|
| ja | 0% | |
| nein | 25% | |
| teilweise | 25% | |
| Ich kann diese Frage nicht beantworten | 50% | |

2.5) Haben Sie festgelegt, für welche Risiken der ISB verantwortlich ist?

| | | n=4 |
|---|---|---|
| ja | 25% | |
| nein | 50% | |
| teilweise | 0% | |
| Ich kann diese Frage nicht beantworten | 25% | |

2.6) Wurde ein Risiko für die Unabhängigkeit des ISB analysiert, wenn dieser gleichzeitig Risikoeigner ist?

| | | n=4 |
|---|---|---|
| ja | 50% | |
| nein | 25% | |
| teilweise | 0% | |
| Ich kann diese Frage nicht beantworten | 25% | |

## 3. Risikomanagement

3.1) Wurde ein Prozess zur Beurteilung von Informationssicherheitsrisiken definiert?

| | | n=8 |
|---|---|---|
| ja | 12.5% | |
| nein | 75% | |
| teilweise | 12.5% | |
| Ich kann diese Frage nicht beantworten | 0% | |

3.2) Wurden einheitliche Kriterien für Eintrittswahrscheinlichkeiten von Risiken festgelegt?

| | | n=8 |
|---|---|---|
| ja | 12.5% | |
| nein | 62.5% | |
| teilweise | 25% | |
| Ich kann diese Frage nicht beantworten | 0% | |

3.3) Wurden einheitliche Kriterien für Schäden von Risiken festgelegt?

| | | n=8 |
|---|---|---|
| ja | 12.5% | |
| nein | 62.5% | |
| teilweise | 25% | |
| Ich kann diese Frage nicht beantworten | 0% | |

3.4) Wurden bereits Risikoanalysen durchgeführt?

n=8

| | |
|---|---|
| ja | 12.5% |
| nein | 62.5% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 12.5% |

3.5) Werden die Risikoanalyse regelmäßig überprüft?

n=8

| | |
|---|---|
| ja | 12.5% |
| nein | 62.5% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 12.5% |

3.6) Kennen Sie die wesentlichen Informationssicherheitsrisiken in Ihrer HS?

n=8

| | |
|---|---|
| ja | 37.5% |
| nein | 0% |
| teilweise | 37.5% |
| Ich kann diese Frage nicht beantworten | 25% |

3.8) Haben Sie Kriterien definiert, wann Risiken als akzeptiert gelten?

n=8

| | |
|---|---|
| ja | 12.5% |
| nein | 75% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 0% |

3.10) Existiert ein Risikobehandlungsplan und ein Prozess zur Nachverfolgung der Maßnahmen?

n=8

| | |
|---|---|
| ja | 12.5% |
| nein | 75% |
| teilweise | 0% |
| Ich kann diese Frage nicht beantworten | 12.5% |

## 4. Änderungssteuerung

4.1) Haben Sie einen Prozess, der vor der Einführung neuer IT-Verfahren oder bei Änderung vorhandener IT-Verfahren die Informationssicherheit (IS) betrachtet?

n=8

| | |
|---|---|
| ja | 0% |
| nein | 50% |
| teilweise | 37.5% |
| Ich kann diese Frage nicht beantworten | 12.5% |

4.2) Existiert ein Formular (analog/digital) für solche Änderung? Wenn vorhanden, bitte stellen Sie dieses in einer separaten E-Mail bereit.

n=8

| | |
|---|---|
| ja | 0% |
| nein | 100% |
| teilweise | 0% |
| Ich kann diese Frage nicht beantworten | 0% |

## 5. Dokumententierte Informationen

5.1) Gibt es einheitliche Vorgaben für die Dokumentation für IT-Verfahren?

n=8

| | |
|---|---|
| ja | 12.5% |
| nein | 75% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 0% |

5.2) Existiert ein Prozess für die Erstellung, Prüfung und Freigabe von Vorgabedokumenten für IT-Verfahren?

n=8

| | |
|---|---|
| ja | 0% |
| nein | 100% |
| teilweise | 0% |
| Ich kann diese Frage nicht beantworten | 0% |

5.3) Wird die Dokumentation durch elektronische Hilfsmittel unterstützt? (z.B. Dokumentenmanagementssystem, SharePoint, Confluence)

n=8

| | |
|---|---|
| ja | 12.5% |
| nein | 50% |
| teilweise | 25% |
| Ich kann diese Frage nicht beantworten | 12.5% |

5.4) Gibt es ein einheitliches Klassifikationsschema für die Vertraulichkeit vom Dokumenten (z. B. öffentlich, intern, vertraulich)?

n=8

| | |
|---|---|
| ja | 12.5% |
| nein | 50% |
| teilweise | 37.5% |
| Ich kann diese Frage nicht beantworten | 0% |

## 6. Kommunikation und Berichtswesen

6.1) Sind die Rollen identifiziert, die für wirksame Informationssicherheit miteinander geplant kommunizieren müssen? (z.B. in Form eines Kommunikationsplanes)

n=8

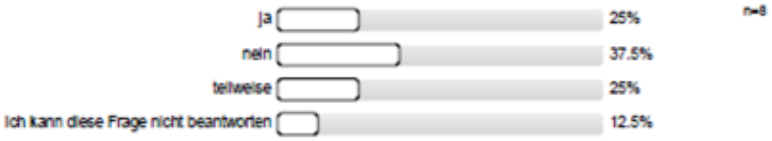
| | |
|---|---|
| ja | 25% |
| nein | 50% |
| teilweise | 25% |
| Ich kann diese Frage nicht beantworten | 0% |

6.2) Existieren Regeltermine zwischen Datenschutz und Informationssicherheit?

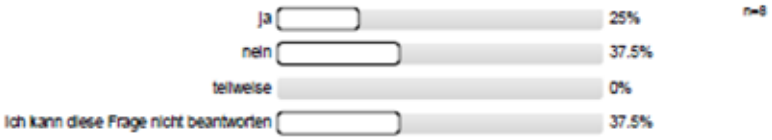
n=8

| | |
|---|---|
| ja | 25% |
| nein | 37.5% |
| teilweise | 25% |
| Ich kann diese Frage nicht beantworten | 12.5% |

6.3) Wurde festgelegt, in welcher Form, durch wen und wie häufig der HSL zu Informationssicherheit berichtet wird (Präsentation / schriftlich / mündlich)?

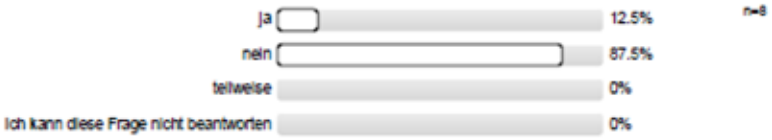



6.5) Ist die Kommunikation mit Behörden geplant? (z.B. mit der Datenschutzbehörde, CERT, BSI, ...)

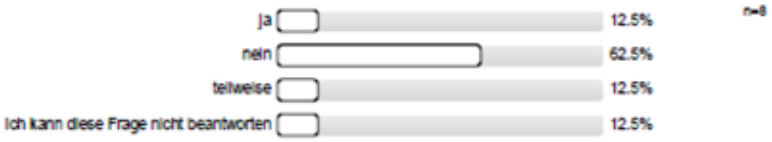



## 7. interne Überprüfungen

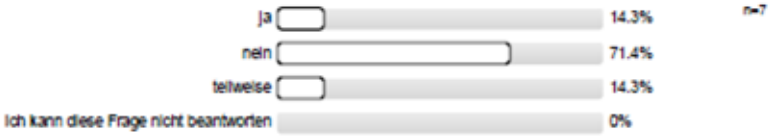
7.1) Existieren Vorgaben für die interne Überprüfung der Informationssicherheit, z. B. im Rahmen von Audits oder Revisionen?



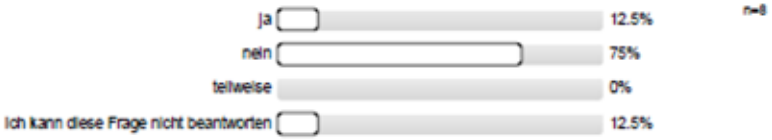

7.2) Haben Sie ein Programm aufgestellt, das interne Überprüfungen der Informationssicherheit zeitlich plant und alle Themen umfasst?




7.3) Gibt es Nachweise zu durchgeführten Audits? (Auditprotokolle, Auditplan, Auditcheckliste und Auditfeststellungen)




7.4) Haben Sie festgelegt, wie mit Abweichungen aus solchen Überprüfungen umgegangen wird und wie diese nachverfolgt werden?




## 8. Mobile Endgeräte

8.1) Haben Sie den Lebenszyklus von HS-eigenen Mobilgeräten beschrieben? (vom Wareneingang bis zur Außerbetiebnahme)

n=8

| | |
|---|---|
| ja | 0% |
| nein | 62.5% |
| teilweise | 25% |
| Ich kann diese Frage nicht beantworten | 12.5% |

8.3) Haben Sie festegelegt, ob für Mitarbeitende der HS-Verwaltung die Verwendung privater Endgeräten innerhalb der IT-Infrastruktur der HS zulässig oder untersagt ist?

n=8

| | |
|---|---|
| ja | 50% |
| nein | 37.5% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 0% |

8.4) Sind Regeln für die Verwendung privater Endgeräte definiert?

n=8

| | |
|---|---|
| ja | 25% |
| nein | 37.5% |
| teilweise | 0% |
| Ich kann diese Frage nicht beantworten | 37.5% |

8.5) Nutzen Sie ein Mobile-Device-Management-System?

n=8

| | |
|---|---|
| ja | 12.5% |
| nein | 75% |
| teilweise | 0% |
| Ich kann diese Frage nicht beantworten | 12.5% |

8.6) Haben Sie bestimmt, wie Daten auf mobilen Endgeräten zu sichern sind?

n=8

| | |
|---|---|
| ja | 12.5% |
| nein | 37.5% |
| teilweise | 37.5% |
| Ich kann diese Frage nicht beantworten | 12.5% |

8.7) Haben Sie festgelegt, wer bei Verlust oder Beschädigung von Mobilgeräten oder beim Verdacht auf Angriff oder Missbrauch von Daten und Informationen, zu informieren ist?

n=8

| | |
|---|---|
| ja | 37.5% |
| nein | 50% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 0% |

8.9) Wurde für Mitarbeitende der HS-Verwaltung und für HS-eigene Geräte festgelegt, welche Apps aus den offiziellen App-Stores heruntergeladen werden dürfen (Whitelist)?

n=8

| | |
|---|---|
| ja | 12.5% |
| nein | 75% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 0% |

8.10) Wurde für Mitarbeitende der HS-Verwaltung und für HS-eigene Geräte bestimmt, welche Apps nicht installiert werden dürfen?

n=8

| | |
|---|---|
| ja | 12.5% |
| nein | 75% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 0% |

## 9. Personalsicherheit und Maßregelung

9.1) Wurde ein Prozessablauf für die Einstellung neuer Mitarbeiter definiert?

n=8

| | |
|---|---|
| ja | 50% |
| nein | 0% |
| teilweise | 25% |
| Ich kann diese Frage nicht beantworten | 25% |

9.2) Wurde der Prozess des Austritts eines Mitarbeiters definiert?

n=8

| | |
|---|---|
| ja | 50% |
| nein | 0% |
| teilweise | 25% |
| Ich kann diese Frage nicht beantworten | 25% |

9.3) Erfolgt im Rahmen der Einstellung eine Sicherheitsüberprüfung? (z. B. Abfrage von Führungszeugnissen, Plausibilitätsprüfung von Lebensläufen, Vorlage von Originalzeugnissen)

n=8

| | |
|---|---|
| ja | 25% |
| nein | 12.5% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 50% |

9.4) Haben Sie einen Prozess für den Umgang mit Verstößen definiert (Maßregelung)?

n=7

| | |
|---|---|
| ja | 14.3% |
| nein | 14.3% |
| teilweise | 28.6% |
| Ich kann diese Frage nicht beantworten | 42.9% |

9.5) Existiert ein Schulungs- und Sensibilisierungskonzept im Hinblick auf Informationssicherheit?

n=8

| | |
|---|---|
| ja | 12.5% |
| nein | 62.5% |
| teilweise | 25% |
| Ich kann diese Frage nicht beantworten | 0% |

9.6) Werden entsprechende Schulungs- und Weiterbildungsnachweise aufbewahrt?

n=8

| | |
|---|---|
| ja | 25% |
| nein | 37.5% |
| teilweise | 0% |
| Ich kann diese Frage nicht beantworten | 37.5% |

## 10. Verwaltung und Handhabung von Werten

10.1) Haben Sie alle Informationswerte inventarisiert?

n=8

| | |
|---|---|
| ja | 0% |
| nein | 12.5% |
| teilweise | 62.5% |
| Ich kann diese Frage nicht beantworten | 25% |

10.2) Sind die schützenswerten Informationswerte identifiziert (Kronjuwelen)?

n=8

| | |
|---|---|
| ja | 62.5% |
| nein | 0% |
| teilweise | 25% |
| Ich kann diese Frage nicht beantworten | 12.5% |

10.4) Gibt es einen Prozess zur sicheren Löschung und Vernichtung von Datenträgern?

n=8

| | |
|---|---|
| ja | 50% |
| nein | 0% |
| teilweise | 37.5% |
| Ich kann diese Frage nicht beantworten | 12.5% |

10.5) Gibt es einen Prozess zur sicheren Vernichtung von Papierakten?

n=8

| | |
|---|---|
| ja | 37.5% |
| nein | 0% |
| teilweise | 50% |
| Ich kann diese Frage nicht beantworten | 12.5% |

10.6) Sind für alle Informationswerte die Verantwortlichen bestimmt?

n=8

| | |
|---|---|
| ja | 12.5% |
| nein | 37.5% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 37.5% |

## 11. Kennwörter

11.1) Wurde die Grundsätze für sichere Kennwörter festgelegt?

n=8

| | |
|---|---|
| ja | 87.5% |
| nein | 0% |
| teilweise | 0% |
| Ich kann diese Frage nicht beantworten | 12.5% |

11.2) Haben Sie die Anforderung an die Kennwortverwaltung festgelegt? (z. B. der Nutzer muss den Passwort bei der ersten Anmeldung ändern; Temporäre Kennwörter müssen dem Nutzer auf eine sichere Weise, d. h. über einen anderen Weg als der Nutzername kommuniziert werden)

n=8

| | |
|---|---|
| ja | 62.5% |
| nein | 0% |
| teilweise | 25% |
| Ich kann diese Frage nicht beantworten | 12.5% |

11.3) Wurde ermittelt, was die Anforderungen für Kennwörter für privilegierte Zugangsberechtigungen (z. B. Administrator-Kennungen) sind?

n=8

| | |
|---|---|
| ja | 50% |
| nein | 25% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 12.5% |

11.4) Haben Sie spezifische Regelungen für die Verwendung von privilegierten Konten definiert?

n=8

| | |
|---|---|
| ja | 37.5% |
| nein | 25% |
| teilweise | 37.5% |
| Ich kann diese Frage nicht beantworten | 0% |

11.5) Haben Sie Vorgaben für Fälle, in denen die Verwendung von Benutzername und Kennwort aus Gründen z. B. der Nutzerfreundlichkeit nicht möglich ist, gemacht?

n=8

| | |
|---|---|
| ja | 0% |
| nein | 87.5% |
| teilweise | 0% |
| Ich kann diese Frage nicht beantworten | 12.5% |

11.6) Wurden die Pflichten der Anwender in Bezug auf die Kennwortnutzung festgelegt? (z. B. Kennwörter, die für private Zwecke genutzt werden, dürfen nicht für Dienstzwecke benutzt werden)

n=8

| | |
|---|---|
| ja | 50% |
| nein | 25% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 12.5% |

## 12. Zugangssteuerung

12.1) Haben Sie einen Prozess für die Erteilung und die Änderung von Zugangsrechten definiert?

n=8

| | |
|---|---|
| ja | 25% |
| nein | 12.5% |
| teilweise | 50% |
| Ich kann diese Frage nicht beantworten | 12.5% |

12.2) Werden Änderungen an Rechten genehmigt und dokumentiert?

n=8

| | |
|---|---|
| ja | 25% |
| nein | 0% |
| teilweise | 50% |
| Ich kann diese Frage nicht beantworten | 25% |

12.3) Werden die vergebenen Rechte regelmäßig überprüft?

n=8

| | |
|---|---|
| ja | 12.5% |
| nein | 50% |
| teilweise | 25% |
| Ich kann diese Frage nicht beantworten | 12.5% |

12.4) Wird dies dokumentiert?

n=8

| | |
|---|---|
| ja | 12.5% |
| nein | 50% |
| teilweise | 25% |
| Ich kann diese Frage nicht beantworten | 12.5% |

12.5) Ist der Entzug von Rechten bei Änderungen oder Ausscheiden von Mitarbeitern sichergestellt?

n=8

| | |
|---|---|
| ja | 50% |
| nein | 0% |
| teilweise | 37.5% |
| Ich kann diese Frage nicht beantworten | 12.5% |

## 13. Kryptographie

13.1) Haben Sie Vorgaben für Verwendung von sicheren kryptographischen Verfahren definiert? (z. B. welche Verfahren dürfen für was verwendet werden?)

n=8

| | |
|---|---|
| ja | 25% |
| nein | 62.5% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 0% |

13.2) Ist der Lebenszyklus von kryptographischen Schlüsseln geregelt?

n=8

| | |
|---|---|
| ja | 37.5% |
| nein | 50% |
| teilweise | 0% |
| Ich kann diese Frage nicht beantworten | 12.5% |

## 14. Physische Sicherheit

14.1) Haben Sie physische Sicherheitszonen in Bezug auf Serverrämen, IT-Verteilerräumen und Rechenzentren basierend auf der Kritikalität von Informationswerten festgelegt?

n=8

| | |
|---|---|
| ja | 50% |
| nein | 25% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 12.5% |

14.2) Sind Regeln für die Sicherheit an den Zonengrenzen definiert?

n=8

| | |
|---|---|
| ja | 25% |
| nein | 25% |
| teilweise | 37.5% |
| Ich kann diese Frage nicht beantworten | 12.5% |

14.3) Gibt es Vorgaben für die Sicherheit von Serverrämen, IT-Verteilerräumen und Rechenzentren?

n=8

| | |
|---|---|
| ja | 62.5% |
| nein | 25% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 0% |

14.4) Haben Sie die Verwaltung von physischen Schlüsseln oder Zutrittsrechten zu Räumen geregelt?

n=8

| | |
|---|---|
| ja | 37.5% |
| nein | 12.5% |
| teilweise | 37.5% |
| Ich kann diese Frage nicht beantworten | 12.5% |

14.5) Ist dokumentiert wer wo Zutritt hat?

n=8

| | |
|---|---|
| ja | 62.5% |
| nein | 0% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 25% |

14.6) Werden die vorhandenen und ausgegebenen Schlüssel oder die vergebenen Zutrittsrechte regelmäßig überprüft?

n=8

| | |
|---|---|
| ja | 37.5% |
| nein | 12.5% |
| teilweise | 25% |
| Ich kann diese Frage nicht beantworten | 25% |

## 15. interner IT-Betrieb

15.1) Gibt es dokumentierte und allen zugängliche Vorgaben für die Benutzung von IT-Systemen?

n=8

| | |
|---|---|
| ja | 50% |
| nein | 25% |
| teilweise | 25% |
| Ich kann diese Frage nicht beantworten | 0% |

15.2) Hat Ihre HS für alle Systeme Update- und Patchzyklen definiert?

n=8

| | |
|---|---|
| ja | 12.5% |
| nein | 37.5% |
| teilweise | 50% |
| Ich kann diese Frage nicht beantworten | 0% |

15.3) Wurden der Verantwortlichern für Patches und Update für alle IT-Systemes definiert und dokumentiert?

n=8

| | |
|---|---|
| ja | 0% |
| nein | 50% |
| teilweise | 37.5% |
| Ich kann diese Frage nicht beantworten | 12.5% |

15.4) Existieren Vorgaben wann, was und in welchen Systemen wie lange protokolliert werden muss? (z. B. Admin-Logs)

n=8

| | |
|---|---|
| ja | 25% |
| nein | 50% |
| teilweise | 25% |
| Ich kann diese Frage nicht beantworten | 0% |

15.5) Sind die gesetzlichen, vertraglichen und sonstigen regulatorischen Vorgaben für die Protokollierung bekannt und dokumentiert?

n=8

| | |
|---|---|
| ja | 12.5% |
| nein | 25% |
| teilweise | 50% |
| Ich kann diese Frage nicht beantworten | 12.5% |

15.6) Wurden die Protokollierung mit dem Datenschutzbeauftragten abgestimmt?

n=8

| | |
|---|---|
| ja | 50% |
| nein | 25% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 12.5% |

15.7) Sind Maßnahmen zur Überwachung von z. B. Storage, CPU, Lasten im Sinne einer Kapazitätssteuerung etabliert?

n=8

| | |
|---|---|
| ja | 87.5% |
| nein | 0% |
| teilweise | 0% |
| Ich kann diese Frage nicht beantworten | 12.5% |

15.8) Werden die Ergebnisse der Kapazitätssteuerung ausgewertet und Maßnahmen abgeleitet?

n=8

| | |
|---|---|
| ja | 75% |
| nein | 0% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 12.5% |

15.9) Wurden Maßnahmen für den Schutz vor Schadsoftware für E-Mails etabliert?

| | | n=8 |
|---|---|---|
| ja | 87.5% | |
| nein | 0% | |
| teilweise | 0% | |
| Ich kann diese Frage nicht beantworten | 12.5% | |

15.11) Wurden Maßnahmen für den Schutz vor Schadsoftware für Wechseldatenträger etabliert?

| | | n=8 |
|---|---|---|
| ja | 37.5% | |
| nein | 12.5% | |
| teilweise | 37.5% | |
| Ich kann diese Frage nicht beantworten | 12.5% | |

15.13) Hat die HS für die HS-eigenen Systeme Verfahren für die Datensicherung (Back-up) definiert und etabliert?

| | | n=8 |
|---|---|---|
| ja | 75% | |
| nein | 0% | |
| teilweise | 12.5% | |
| Ich kann diese Frage nicht beantworten | 12.5% | |

15.14) Wurden die Häufigkeit der Datensicherung für diese Systeme bestimmt?

| | | n=8 |
|---|---|---|
| ja | 75% | |
| nein | 0% | |
| teilweise | 12.5% | |
| Ich kann diese Frage nicht beantworten | 12.5% | |

15.15) Werden Tests zu Rücksicherungen (Restore) in geplanten Abständen druchgeführt?

| | | n=8 |
|---|---|---|
| ja | 37.5% | |
| nein | 0% | |
| teilweise | 50% | |
| Ich kann diese Frage nicht beantworten | 12.5% | |

15.16) Existieren Vorgaben, wie die erfolgreiche Rücksicherung durch die Nutzer der Systeme getestet wird?

| | | n=8 |
|---|---|---|
| ja | 12.5% | |
| nein | 62.5% | |
| teilweise | 25% | |
| Ich kann diese Frage nicht beantworten | 0% | |

15.18) Haben Sie ein zentrales Zeitsignal für alle IT-Systeme von einer vertrauenswürdigen Quelle? (z. B. NTP-Server)

| | | n=8 |
|---|---|---|
| ja | 87.5% | |
| nein | 0% | |
| teilweise | 0% | |
| Ich kann diese Frage nicht beantworten | 12.5% | |

15.19) Finden in Ihrer HS Schwachstellenscans und/oder Penetrationstests statt?

n=8

| | |
|---|---|
| ja | 25% |
| nein | 37.5% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 25% |

## 16. Schwachstellen-Management

16.3) Ist die Verantwortung für die Bewertung technischer Schwachstellen dokumentiert?

n=8

| | |
|---|---|
| ja | 0% |
| nein | 75% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 12.5% |

16.4) Fließen technische Schwachstellen in die Risikoanalysen für Informationssicherheitsrisiken ein?

n=8

| | |
|---|---|
| ja | 37.5% |
| nein | 50% |
| teilweise | 0% |
| Ich kann diese Frage nicht beantworten | 12.5% |

## 17. Netzwerk- und Kommunikationssicherheit

17.1) Existiert ein dokumentiertes Netzwerkdiagramm/Netzstrukturplan?

n=8

| | |
|---|---|
| ja | 75% |
| nein | 0% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 12.5% |

17.2) Existieren unterschiedliche interne Netzwerke (Netzwerktrennung)?

n=8

| | |
|---|---|
| ja | 75% |
| nein | 0% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 12.5% |

17.4) Werden die internen Netzwerke (LANs oder VLANs) durch weitergehende Sicherheitsmaßnahmen voneinander getrennt (z. B. durch eine Firewall)?

n=8

| | |
|---|---|
| ja | 75% |
| nein | 0% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 12.5% |

17.6) Sind die Qualitätsmerkmale für die internen Netze bestimmt (z. B. Bandbreite), mit den Nutzern abgestimmt und dokumentiert?

n=8

| | |
|---|---|
| ja | 12.5% |
| nein | 62.5% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 12.5% |

17.7) Gibt es Vorgaben für die Anbindung Dritter an das Netz (z. B. Site-to-Site-VPN)?

| | | n=8 |
|---|---|---|
| ja | 37.5% | |
| nein | 37.5% | |
| teilweise | 25% | |
| Ich kann diese Frage nicht beantworten | 0% | |

17.8) Existieren Vorgaben für den Schutz vertraulicher Informationen bei der Übermittlung an Dritte (z. B. im Rahmen von Forschungs- oder Transferprojekten)?

| | | n=8 |
|---|---|---|
| ja | 12.5% | |
| nein | 37.5% | |
| teilweise | 25% | |
| Ich kann diese Frage nicht beantworten | 25% | |

17.9) Werden Informationen bei der Übermittlung an Dritte geschützt (z. B. Transportverschlüsselung)?

| | | n=8 |
|---|---|---|
| ja | 37.5% | |
| nein | 0% | |
| teilweise | 50% | |
| Ich kann diese Frage nicht beantworten | 12.5% | |

## 18. Software- und Systementwicklung

18.1) Findet an Ihrer HS Softwareentwicklung für HS-eigene Software im weitesten Sinne statt? (Softwareentwicklung meint jede Anpassung von Quellcode oder die Erstellung individueller, ausführbarer Programme unter Nutzung von Quellcode)

| | | n=8 |
|---|---|---|
| ja | 75% | |
| nein | 0% | |
| teilweise | 12.5% | |
| Ich kann diese Frage nicht beantworten | 12.5% | |

18.2) Existieren Vorgaben für die sichere Softwareentwicklung, sofern die entwickelte Software innerhalb der HS eingesetzt wird?

| | | n=8 |
|---|---|---|
| ja | 12.5% | |
| nein | 62.5% | |
| teilweise | 25% | |
| Ich kann diese Frage nicht beantworten | 0% | |

18.3) Werden Änderungen am Quellcode dokumentiert?

| | | n=8 |
|---|---|---|
| ja | 25% | |
| nein | 0% | |
| teilweise | 50% | |
| Ich kann diese Frage nicht beantworten | 25% | |

18.4) Existieren Vorgaben für Tests und Abnahmen von neuer Software?

| | | n=8 |
|---|---|---|
| ja | 25% | |
| nein | 50% | |
| teilweise | 25% | |
| Ich kann diese Frage nicht beantworten | 0% | |

18.5) Werden Tests in einer sicheren Umgebung durchgeführt?

| | | n=8 |
|---|---|---|
| ja | 62.5% | |
| nein | 0% | |
| teilweise | 25% | |
| Ich kann diese Frage nicht beantworten | 12.5% | |

18.6) Sofern Testdaten eingesetzt werden, werden diese unter Beachtung des Datenschutzes genutzt? (z. B. Pseudonymisierung)

| | | n=8 |
|---|---|---|
| ja | 62.5% | |
| nein | 0% | |
| teilweise | 25% | |
| Ich kann diese Frage nicht beantworten | 12.5% | |

## 19. Dienstleistersteuerung

19.1) Sind die Richtlinien und Verfahren für die Zusammenarbeit mit Auftragnehmern und Dienstleistern definiert, die die Informationssicherheit bei der Zusammenarbeit betreffen?

| | | n=8 |
|---|---|---|
| ja | 25% | |
| nein | 25% | |
| teilweise | 50% | |
| Ich kann diese Frage nicht beantworten | 0% | |

19.2) Werden mit Lieferanten und Dienstleistern konkrete Vereinbarungen zum Schutz von Informationen getroffen (technische und organisatorische Maßnahmen), die über den Datenschutz hinausgehen?

| | | n=8 |
|---|---|---|
| ja | 37.5% | |
| nein | 25% | |
| teilweise | 25% | |
| Ich kann diese Frage nicht beantworten | 12.5% | |

19.4) Werden Nachweise für die Erfüllung der Anforderungen angefordert? (z. B. in Form von Zertifikaten)

| | | n=8 |
|---|---|---|
| ja | 12.5% | |
| nein | 37.5% | |
| teilweise | 0% | |
| Ich kann diese Frage nicht beantworten | 50% | |

19.5) Führen Sie Lieferanten- oder Dienstleisteraudits im Sinne der Informationssicherheit durch?

| | | n=8 |
|---|---|---|
| ja | 0% | |
| nein | 87.5% | |
| teilweise | 0% | |
| Ich kann diese Frage nicht beantworten | 12.5% | |

19.7) Gibt es vertragliche Regeln die Auftragnehmer beim Betreten sicherheitsrelevanter Räumlichkeiten erfüllen müssen? (z. B. Arbeit nur unter Aufsicht)

n=8

| | |
|---|---|
| ja | 25% |
| nein | 50% |
| teilweise | 0% |
| Ich kann diese Frage nicht beantworten | 25% |

## 20. IT-Sicherheit im Notfall

20.1) Gibt es Mindestvorgaben für die Vertraulichkeit, Verfügbarkeit und Integrität im Notfall oder in der Krise?

n=8

| | |
|---|---|
| ja | 0% |
| nein | 75% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 12.5% |

20.2) Existiert ein IT-Notfallhandbuch, das den Umgang mit und die Wiederherstellung nach Notfällen und Krisen beschreibt?

n=8

| | |
|---|---|
| ja | 12.5% |
| nein | 62.5% |
| teilweise | 25% |
| Ich kann diese Frage nicht beantworten | 0% |

20.3) Wurde ein Verantwortlicher für Notfälle bestimmt? (z. B. Notfallbeauftragter)

n=8

| | |
|---|---|
| ja | 12.5% |
| nein | 50% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 25% |

20.5) Ist der Verantwortliche für die Informationssicherheit (z. B. ISB oder IT-SiBe) in das Notfall- und/oder Krisenteam eingebunden?

n=7

| | |
|---|---|
| ja | 14.3% |
| nein | 28.6% |
| teilweise | 14.3% |
| Ich kann diese Frage nicht beantworten | 42.9% |

20.6) Finden Notfallübungen auf Basis des Notfallhandbuches statt?

n=8

| | |
|---|---|
| ja | 12.5% |
| nein | 62.5% |
| teilweise | 12.5% |
| Ich kann diese Frage nicht beantworten | 12.5% |

## 21. Compliance

21.1) Sind die wesentlichen rechtlichen Vorgaben für die Informations- und IT-Sicherheit in Ihrer HS identifiziert und bekannt?

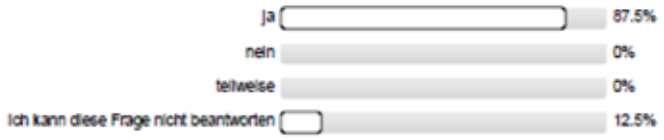
n=8

| | |
|---|---|
| ja | 37.5% |
| nein | 0% |
| teilweise | 50% |
| Ich kann diese Frage nicht beantworten | 12.5% |

21.2) Existiert eine Lizenzverwaltung für alle Softwareprodukte?

n=8

21.3) Ist ein Datenschutzbeauftragter bestellt?




n=8

21.4) Existiert ein vollständiges Verzeichnis der Verarbeitungstätigkeiten/Verarbeitungsverzeichnis?

n=8

## 1. Verantwortung der HS-Leitung

1.6) Wie heißt die Funktion (z. B. Informationssicherheitsbeauftragte/r (ISB) oder IT-Sicherheitsbeauftragte/r)?

- Es sind zwei IT-Mitarbeiter, die sich aufgrund ihres Aufgabengebietes mit der Thematik befassen. Einen Beauftragten außerhalb der IT existiert nicht.
- ISB
- Informationssicherheitsbeauftragte/r (ISB)
- Informationssicherheitsbeauftragter
- dezentrale Verantwortung (keine gesonderte Bezeichnung)

## 2. Verantwortung des ISB

2.1) Wo ist die Funktion ISB organisatorisch verortet?

- Angebunden an CIO
- Berufener der Hochschlleitug direkt der HSL unterstellt
  https://www.th-wildau.de/files/2_Dokumente/Sonstiges/Organisation-der-TH-Wildau.pdf
- Untersteht der Hochschulleitung, wurde explizit so formuliert - praktisch Organisatorisch der/ dem Kanzler:in und nicht der/dem Präsident:in
- es gibt keinen
- kein ISB

## 3. Risikomanagement

3.7) Bitte nennen Sie diese exemplarisch.

- -
- Feuer, Ausfall oder Störung von Dienstleistern, Verstoß gegen Gesetze/Regelungen, Ausspähen/ Manipulation von Informationen, Abhören, Schadprogramm, Rouge Access Points, DDoS
- Phishing, offene Netzwerkzugänge, Patchstände
- Umgang mit priviligerten Zugängen, Innentäterproblematik, in einigen Bereichen Phishing/Vishing
- menschliches Fehlverhalten, fahrlässig oder vorsätzlich
  Qualität der organisatorische Regelungen, Dokumentationen und Kontrollen
  Systemausfälle
  vorsätzliche missbräuchliche Handlungen, Zerstörung und Diebstahl durch Dritte
  Personalausfall, Lieferschwierigkeiten, Katastrophen

3.9) Wer hat in Ihrer Hochschule (HS) die Befugnis welche Risiken akzeptierbar sind?

- -
- HSL
- Präsident
- Präsidentin
- nicht erfolgt
- nicht geklärt - Risikoakzeptanzkriterien/ Risiken sollen Kanzler:in (Haus-/Verwaltungsleitung) jährlich vorgelegt werden
- nicht geregelt

## 6. Kommunikation und Berichtswesen

6.4) Bitte nennen Sie wer, wie häufig und wie berichtet.

- CIO/IKMZ-Leitung im Rahmen regelmäßiger Jour Fixe-Termine mit der HSL
- Durch den Leiter IT werden im CIO-Gremium (bestehend aus einer Professorin, dem Kanzler und des Leiter IT) aktuelle Vorkomnisse oder Gefahrenlagen diskutiert. Die Treffen finden monatlich statt.
- ISB, halbjährig, Managementreview mündlich mit Protokoll
- Quartalsweiser-/ Halbjährlicher "Kombi-Termin" mit DSB soll stattfinden. IS-Leitlinie beschränkt sich auf "regelmäßig"

## 8. Mobile Endgeräte

8.2) Wie werden die HS-eigenen Mobilgeräten verwaltet? Haben Sie festgelegt, wie und durch wen die HS-eigenen Endgeräten installiert werden?

- Ausgabe über Ausleihvereinbarung, jedes Jahr neu zu unterschreiben, Installation durch Administrator nicht Hochschulweit
- Ausgabeliste -> Support/Installation über Zentrale IT. Festgelegt ja, dokumentiert nein
- Die hochschuleigenen mobilen und stationären IT-Geräte werden ausschließlich von den Mitarbeitern des IT-Service administriert und verwaltet.
- Laptops durch ITSZ, Tablets teilweise durch ITSZ, Smartphones durch Nutzer
- Verwaltung und zentrale Dienste, Fakultäten (Forschung und Lehre) dezentral
- in der Verwaltung werden diese durch den Bereich IT-S installiert
- nein werden nur verwaltet, Nutzer hat alle Berechtigungen

8.8) Wie und durch wen werden die Meldungen erfasst/bewertet?

- (ITSZ)
- Diese Meldungen werden durch den IT-Service bewertet und bei Bedarf an den Datenschutzbeauftragten bzw. der Hochschulleitung weitergegeben.
- ISB bzw. Erfassung durch zuständigen Admin + Meldung an ISB. Bewertung meist ISB + Fachadmin
- Informationssicherheit Team
- Vorgesetzer + Einbindung Personalrat

## 10. Verwaltung und Handhabung von Werten

10.3) Mit welchen Vorgaben schützt Ihre HS schützenswerte Informationswerte? Bitte stellen Sie dies exemplarisch für eine "Kronjuwele" dar.

- Eine Umsetzung nach BSI IT-Grundschutz wird für die Hochschule angestrebt. Für die "Kronjuwelen" wie z.B. die Hausverwaltung (Finanz-/ Personaldaten) werden im Rahmen der Kernabsicherung die Anforderungen für "Hohen Schutzbedarf" nach BSI ITGS umgesetzt.
- Mehrstufiges Konzept zur Datensicherheit, Minimal Rights, Defense in Depth, erweitertes Logging, 4 Augen Prinzip, bei neueren Projekten Zero Trust
- Personaldaten: eigenes Verwaltungsnetz, Zugangsbeschränkungen, Firewall
- Unterlagen zu Beschaffungsvorgängen werden in einem verschlossenen Raum aufbewahrt. Der Zugriff ist nur über jeweils berechtigte Personen möglich.

  Personalunterlagen werden ebenfalls in einem verschlossenen Raum aufbewahrt. Diese sind nur der Personalabteilung zugänglich.

  Serverräume: der Zugang ist nur den Mitarbeitern des IT-Service und des Gebäudemanagements gestattet.
- durch die Regelungen des ISMS

## 15. interner IT-Betrieb

15.10) Bitte beschreiben Sie diese grob.

- -
- Content Disarming im Aufbau, Spamfilterung und AV Scan vollständig,
  einige externe Inhalte werden abgelehnt (Ausnahmen vorhanden)
- E-Mails werden eingehend mehrfach durch unterschiedliche Hersteller auf Schadsoftware geprüft (DFN), ausgehend durch Cisco ESA
- SPAM-Filter, Mail-Server auf akt. Patch-Level, Awareness-Schulung der Nutzer
- Spam- und Virenschutz am Posteingangsserver
- Vorfilterung durch DFN-MailSupport
  Virenscanner auf dem Mailsever mit EndUser-Quarantäne
  Virenscanner auf den Endgeräten
  Zeitnahe Aktualisierung der Mailclients
- keine Angaben

15.12) Bitte beschreiben Sie diese grob.

- Automatischer Virenscan beim Anschluss eines Wechseldatenträgers. Dieser kann durch den Nutzer nicht abgebrochen werden.
- Deaktivierung der USB-Ports; Scan über einen Schleusenrechner mit AV; F&L unbeschränkt
- Einsatz von F-Secure/Sophos für Endgeräte
- Enterprise-Virenschutz-Software
- keine Angaben

15.17) Bitte beschreiben Sie exemplarisch das Sicherungs- und Rücksicherungskonzept für eine "Kronjuwele" Ihrer HS.

- -
- E-Mail-Server:
  mehrstufiges Verfahren:
  1. Lokales Bandlaufwerk: 1 mal wöchentlich Full Backup (Postfächer und System, tägliche differentielle Backups,
  2. Postfächer werden alle 2 Stunden mit Backupsystem synchronisiert
  3. nachts "rotierende" TAR-Archive auf Backup-Server (4 Wochen Aufbewahrung)
  4. einmal wöchentlich Kopie auf Desaster Backup Server
- Groupware: Samstags werden die Mails aller Accounts, die LDAP Datenbank, die Maildatenbanken und Indexdaten vollständig gesichert. Alle anderen Tage findet eine Sicherung der Änderungen zum vorhergehenden Stand statt (LDAP und RedoLogs). Die Vorgehensweise der Wiederherstellung der Emails ist abhängig von dem Schaden der beseitigt werden soll.
  Im Desaster Fall, dass der Server defekt ist, installiert man diesen neu, verbindet das Backuplaufwerk mit der neu eingerichteten Maschine und stellt dann zunächst den LDAP mit
  zmrestoreldap wieder her. Im Anschluß reinitialisiert man die Datenbank mit zmmyinit. Mit zmrestoreoffline –sys –a all –c stellt man dann die Mailboxen wieder her. Eine genaue Anleitung für diesen Fall findet man unter https://wiki.zimbra.com/wiki/Network_Edition_Disaster_Recovery
- Sicherungen werden täglich nach "3-2-1" Regel erstellt und automatisiert wöchentlich/täglich wiederhergestellt, getestet und Protokolliert. Gilt für alle kritischen Systeme
- Studierendendaten (Campusnet): regelm Datenbankdumps und Übertragung auf 2. Testsystem, Tests auf dem Testsystem

15.20) Wann fand der letzte Test statt?

- Schwachstellenscans, 07.05.2021
- regelmäßig
- 2017

## 16. Schwachstellen-Management

16.1) Erhält Ihre HS regelmäßig Informationen zu technische Schwachstellen und bewerten diese?

- Ja (3 Nennungen)

- Meldungen des DFN
- teilweise, z.B. durch DFN-CERT

16.2) Welche Informationsquellen nutzt Ihre HS für Schwachstellen?

- BSI, DFN-CERT, CERT-Bund, std. Onlinemedien (heise, div. Twitterfeed von Securityforschern)
- DFN
  BSI
  externe Dienstleister
  Herstellerinformationen
  Fachportale
- DFN Cert
- DFN, BSI u.a.
- DFN-Cert, Heise Security,
- Palo Alto, heise-security.de

## 17. Netzwerk- und Kommunikationssicherheit

17.3) Wie erfolgt die Trennung?

- Subnets / VLANS
- VLAN oder VPN
- VLAN, Firewall, ACLs
- VLANs, Router
- mehrere VLANs
- per VLAN und Firewallsegmentierung
- strukturell

17.5) Bitte beschreiben Sie dies grob.

- Firewalls zwischen Allgem. Netz und allen "sensiblen" Netzwerksegmenten
- Firewalls zwischen den Org. Einheiten und div. Segmenttierungen, Monitoring ob "auffällig viel" Traffic
- Trennung der Netze durch mehrstufiges Firewallsystem um den Sicherheitsansprüchen der einzelnen Netze gerecht zu werden.
- keine Angaben
- zentrale Komponente Firewall
  übernimmt Routing zwischen einzelnen Netzsegmenten

17.10) Welche technischen Möglichkeiten stellt Ihre HS Nutzern für die sichere Übermittlung von Informationen bereit?

- GWDG-Cloud
- Nach Bereichen Unterteilte Freigaben auf Fileservern.
  Freigabe auf eigener Cloud-Instanz mit Zugriffssteuerung.
  DFN Zertifikate für S/MIME / Verschlüsselung.
- Nutzerzertifikat
- SMIME Zertifikate/ PKI Infrastruktur
  SSL/TLS -Verschlüsselung
- SMIME für Mail, Box.UP also Cloudspeicher, SSL-Zertifikate für Server/Webappliaktionen
- VPN, private Cloud (Nextcloud)

## 19. Dienstleistersteuerung

19.3) Bitte nennen Sie exemplarisch Dienstleister oder Lieferanten, mit denen solche Vereinbarungen bestehen.

- AWS
- DELL
- HIS
  GWDG
  Hosteurope
  Triumph Adler
- Persis

19.6) Wie gewährleistet, dass mit Dritten, die vertrauliche oder schützenswerte Informationen empfangen, Vertraulichkeitsvereinbarungen abgeschlossen werden?

- Ich kann diese Frage nicht beantworten, Einhaltung DSGVO
- Nein nur Teilbereiche
- Nein, aber der ISB hat zumindest ein Auge drauf und fragt diese an sobald die Kenntnis vorliegt ;)
- für den zentralen Bereich ist es ein gelebter Prozess

## 20. IT-Sicherheit im Notfall

20.4) Wie heißt die Funktion und wo ist sie aufgehängt?

- Krisenstab je Szenario unterschiedlich besetzt
- Verantwortung trägt HSL. Die legt entsprechend des Notfall einen Verantwortlichen fest (z.B.: HSL, Brandschutzbeauftragter, ISB).

20.7) Wann fand die letzte IT-Notfallübung statt und was wurde geübt?

- -
- keine
- keine Angaben
- temporäre Abschaltung von Netzanlagen Februar 2019