HIS-HE:Forum
3|2025

Mathias Stein, Maren Lübcke, Harald Gilch

Cybersicherheit an Hochschulen: Föderale Ansätze und (gemeinsame) Wege

HIS-Institut für Hochschulentwicklung e. V.
Goseriede 13a | D-30159 Hannover | www.his-he.de

Dr. Mathias Stein
Geschäftsbereich Hochschulmanagement
Tel.: +49 511 169929-27
E-Mail: stein@his-he.de

Dr. Maren Lübcke
Geschäftsbereich Hochschulmanagement
Tel.: +49 511 169929-19
E-Mail: luebcke@his-he.de

Dr. Harald Gilch
Geschäftsbereich Hochschulmanagement
Tel.: +49 511 169929-32
E-Mail: gilch@his-he.de

25. November 2025

ISBN 978-3-948388-47-8

Abstract

In den vergangenen Jahren haben Cyberangriffe auf Hochschulen deutlich zugenommen – von alltäglichen Phishing- und Spam-Attacken bis hin zu mutmaßlich staatlich gesteuerten Operationen. Cybersicherheit ist damit zu einem zentralen Handlungsfeld für Hochschulen und Wissenschaftspolitik geworden.

Die Studie des HIS-Instituts für Hochschulentwicklung e. V. (HIS-HE) untersucht erstmals systematisch, wie die Bundesländer Cybersicherheit an Hochschulen fördern. Grundlage der Studie sind eine Dokumentenanalyse sowie Befragungen von Wissenschaftsministerien und Computer Emergency Response Teams (CERTs) im Sommer 2024.

Die Ergebnisse zeigen ein heterogenes Bild: Einige Länder verfügen über umfassende Strategien und zentrale Anlaufstellen, während andere auf autonome Hochschullösungen setzen. Unterschiede bestehen in der Verankerung von Zuständigkeiten, der Ausgestaltung von Unterstützungsleistungen und der Zusammenarbeit zwischen Hochschulen und Landesstrukturen. CERTs sind zwar häufig auch für Hochschulen zuständig, werden aber nur wenig genutzt.

Die rechtlichen Rahmenbedingungen – von der NIS-2-Richtlinie bis hin zu Landes-IT-Gesetzen – sowie die Vielfalt an (föderalen) Zuständigkeiten prägen den Handlungsrahmen maßgeblich. Die Studie verdeutlicht: Cybersicherheit ist kein rein technisches, sondern ein strategisches Handlungsfeld, das sowohl die Hochschulen als auch die zuständigen Ministerien betrifft. Hochschulen müssen Krisenmanagementprozesse etablieren und Zuständigkeiten regeln, während die Ministerien entsprechende Unterstützungsstrukturen bereitstellen und den institutionellen Rahmen gestalten. Länderübergreifende Kooperationen und systematischer Wissenstransfer sind entscheidend für den erfolgreichen Aufbau resilienter Systeme.

Inhaltsverzeichnis

Abstract I
Inhaltsverzeichnis II
1 Cybersicherheit und Hochschulen: Ziele und Methodik 1
1.1 Cyberangriffe und Bedrohungslage 1
1.2 Untersuchungsziel und Fragestellungen 2
2 Erhebungsmethodik 3
3 Rahmenbedingungen für Cybersicherheit 4
3.1 Aktuelle Bedrohungslagen 4
3.2 Rechtliche Grundlagen 6
3.3 Föderale Zuständigkeiten 7
4 Umfrageergebnisse: Länderministerien und CERTs 10
4.1 Ministerielle Cybersicherheitsansätze 10
4.2 CERT-Unterstützungsleistungen 12
5 Cybersicherheit an Hochschulen: Situation in den Bundesländern 14
5.1 Baden-Württemberg 14
5.2 Bayern 17
5.3 Berlin 19
5.4 Brandenburg 21
5.5 Bremen 23
5.6 Hamburg 25
5.7 Hessen 27
5.8 Mecklenburg-Vorpommern 29
5.9 Niedersachsen 30
5.10 Nordrhein-Westfalen 32
5.11 Rheinland-Pfalz 35
5.12 Saarland 37
5.13 Sachsen 39
5.14 Sachsen-Anhalt 41
5.15 Schleswig-Holstein 43
5.16 Thüringen 45
6 Erkenntnisse und Bewertung 47
7 Literaturverzeichnis 51
Anhang 59
Anhang 1 Fragebogen CERT-Umfrage 59
Anhang 2 Fragebogen Wissenschaftsministerien 60

1 Cybersicherheit und Hochschulen: Ziele und Methodik

1.1 Cyberangriffe und Bedrohungslage

Cyberangriffe auf Hochschulen haben nicht nur erheblich zugenommen, sondern sind auch komplexer geworden. Dabei umfassen diese Angriffe ein breites Spektrum und reichen von Störung und Sabotage über datenorientierte Angriffe und Zugriffs- sowie Kontrollübernahme bis hin zu professionell organisierten Ransomware-as-a-Service-Modellen (RaaS), bei denen Erpressungssoftware als Dienstleistung vermarktet wird (BSI, 2024). Die Bandbreite der angreifenden Akteure reicht von ideologisch motivierten Gruppen und kriminellen Organisationen bis hin zu staatlichen Akteuren. Auch Insider-Bedrohungen spielen eine bedeutende Rolle. So stellt beispielsweise der aktuelle Digital Defence Report von Microsoft fest: „In 2024, Education and Research became the second most targeted sector by nation-state threat actors." (Microsoft, 2024, S. 12). Dem Bericht zufolge werden Bildungs- und Forschungseinrichtungen nicht nur zum Ziel, um an Informationen und Forschungsergebnisse zu gelangen; sie werden auch als Trainingsraum genutzt, um Vorgehensweisen und Methoden für Cyberangriffe zu testen. Gleichzeitig werden die Grenzen zwischen staatlichen und privaten Akteuren sowie zwischen Cybercrime und hybrider Kriegsführung immer fließender (vgl. u. a. Bitkom, 2025).

Vor dem Hintergrund dieser Entwicklungen ist Cybersicherheit inzwischen ein zentrales Thema für Hochschulen und Hochschulleitungen geworden. Im jüngsten Hochschul-Barometer des Stifterverbandes schätzten die befragten Hochschulleitungen die Gefahr durch Cyberangriffe für Hochschulen in Deutschland allgemein mit insgesamt 97,3 % als groß oder eher groß ein. Dabei gab aber lediglich die Hälfte der Hochschulleitungen (53,4 %) an, zumindest für einige Hochschulbereiche über Notfallpläne für Cyberangriffe zu verfügen (Stifterverband, 2025, S. 38 f.). Anfang 2025 hat das Präsidium der Hochschulrektorenkonferenz (HRK) die künftige Bundesregierung dazu aufgefordert, „angesichts der Bedrohungslage entsprechend seiner übergreifenden Rolle in der Gefahrenabwehr aktiv zu werden" (HRK, 2025, S. 2). Diese Rolle ergebe sich aus der internationalen Dimension von Cybersicherheit und der länderübergreifenden Gefährdungslage. Es müsse, so die Empfehlung der HRK, „Aufgabe des Bundes sein, zur länderübergreifenden Vernetzung der relevanten Hochschulen und Hochschulverbünde beizutragen und hierfür Impulse zu geben. Das gilt insbesondere für die Zusammenführung von Konzepten und Initiativen der Länder." (Ebd.)

Doch welche Initiativen gibt es überhaupt und welche Strategien verfolgen die Länder, um ihre Hochschulen im Kampf gegen Cyberangriffe zu unterstützen? Und was sind zentrale Aspekte und Handlungsfelder, die sich aktuell im Spannungsfeld zwischen Cybersicherheit und Hochschulautonomie ergeben?

Das HIS-Institut für Hochschulentwicklung e. V. (HIS-HE) beobachtet diese Entwicklungen seit einigen Jahren. Dabei betrachtet HIS-HE nicht primär technische Aspekte oder IT-Fragen, sondern fokussiert auf „die Gesamtorganisation Hochschule aus Sicht der Hochschulleitung" (Gilch et al., 2023, S. 1). Der Blick geht also über das reine „IT-Problem" hinaus und richtet sich auf organisatorische und strukturelle Aspekte. Fallen IT-Systeme in der Hochschulverwaltung, Forschung oder Lehre aus, kann dies – auch kurzfristig – gravierende Folgen für die Arbeitsorganisation und die Steuerung von Hochschulen haben. Welche Auswirkungen Cyberangriffe haben können und wie sich Hochschulen darauf vorbereiten und im Krisenfall reagieren sollten – diese Fragen stehen im Mittelpunkt der Arbeit von HIS-HE. Die vorliegende Studie betrachtet nicht einzelne Hochschulen, sondern analysiert, wie die Länder die Cybersicherheit ihrer Hochschulen unterstützen.

Zentrale Fragen sind: Ist Cybersicherheit eine autonome Aufgabe der Hochschulen, die sich aus der Freiheit von Forschung und Lehre ableitet? Oder unterstützen die Länder ihre Hochschulen durch übergreifende Programme, finanzielle Förderung und zentrale Vorgaben dabei, sich intensiv mit Cybersicherheit zu beschäftigen und Vorsorgemaßnahmen umzusetzen? Diese Fragen soll die vorliegende Studie beantworten.

1.2 Untersuchungsziel und Fragestellungen

In der Studie werden die Bundesländer hinsichtlich ihrer Aktivitäten, Programme und Maßnahmen zur Förderung der Cybersicherheit an Hochschulen analysiert. Dabei wird nicht bewertet, welche Ansätze „besser" oder „schlechter" sind. Stattdessen werden die verschiedenen Aktivitäten individuell dargestellt, damit die Beteiligten voneinander lernen können. Die Studie soll sowohl auf Hochschulebene als auch auf Länderebene Diskussionen anstoßen. Anhand von Beispielen aus verschiedenen Bundesländern werden Anregungen gegeben, wie sich Hochschulen und Länder intensiver mit Cybersicherheit und Krisenmanagement nach Cyberangriffen beschäftigen können. Durch die Betrachtung der Bundesländer werden übergreifende Aspekte und Themen sichtbar, die unabhängig von den spezifischen Regelungen im Bundesland einen allgemeinen Charakter haben. Die Darstellung entspricht dem Stand von März 2025. Falls wir Programme, Initiativen oder wichtige Aspekte nicht aufgeführt haben, bitten wir dies zu entschuldigen. Gerne können Sie uns entsprechende Hinweise übermitteln, damit wir diese bei einer Aktualisierung berücksichtigen können.

2 Erhebungsmethodik

Die Studie basiert auf einer Desk-Research sowie zwei Umfragen, für die im Sommer 2024 die Wissenschaftsministerien und die Computer Emergency Teams (CERTs) der Bundesländer sowie des Bundes befragt wurden.

Die Befragung der Wissenschaftsministerien der Bundesländer erfolgte in Form einer Online-Umfrage. Die im Juni 2024 durchgeführte Befragung richtete sich vor allem an die im Organigramm der Ministerien ausgewiesenen zuständigen Stellen für Cybersicherheit, IT-Sicherheit oder im weiteren Sinne für die Digitalisierung der Hochschulen. In den Fällen, in denen die Zuständigkeit nicht eindeutig ersichtlich war, wurden die für die Hochschulen zuständigen Fachreferate kontaktiert. Im Mittelpunkt, der auf neun Fragen begrenzten Umfrage standen die Relevanz des Themas Cybersicherheit für das Ministerium, Unterstützungsmaßnahmen und Zuständigkeiten.[1] Parallel dazu wurden die Pressestellen der CERTs der Bundesländer sowie das CERT des Bundes per E-Mail kontaktiert. Diese können im Ernstfall eines Cyberangriffes die betroffenen Einrichtungen unterstützen und wurden befragt, inwieweit ihre Leistungen auch für Hochschulen zur Verfügung stehen bzw. von diesen nachgefragt werden.[2]

Ergänzt wurden die beiden Befragungen durch eine Desk Research, bei der eine Auswertung der relevanten Literatur, Berichte und Internetseiten zu Stichpunkten wie Cybersicherheit, IT-Sicherheit, Notfallmanagement und Hochschulen vorgenommen wurde. Darüber hinaus wurden die entsprechenden Gesetzesinitiativen, Strategiepapiere und Stellungnahmen der verschiedenen Ministerien der Bundesländer gesichtet, wofür insbesondere die Parlamentsdatenbanken der Länder genutzt wurden.[3] Ziel war es, Länderübersichten anzufertigen, die die Unterstützungsleistungen der Länder im Überblick darstellen.

[1] Die Fragebögen der beiden Umfragen sind im Anhang beigefügt (vgl. Anhang 1 und Anhang 2).

[2] An dieser Stelle ist darauf hinzuweisen, dass auf übergreifender Ebene das Deutsche Forschungsnetz (DFN) mit dem Dienst DFN-Security und die DFN-CERT Service GmbH Unterstützung im Bereich IT-Sicherheit anbietet. Der DFN bietet seinen Mitgliedern verschiedene Security Services an, die als Basisleistungen allen Mitgliedern des DFN zur Verfügung stehen. Bei besonderen Sicherheitsanforderungen können „erweiterte Leistungen“ ergänzt werden. Das DFN-CERT wurde 1993 zunächst als Computer-Notfallteam für die Anwender des DFN-Vereins gegründet und bietet inzwischen als wissenschaftsnahes Unternehmen verschiedene Leistungen und Dienste für Hochschulen und Forschungseinrichtungen im Bereich Cyber-Sicherheit an. Zudem haben einzelne Hochschulen eigene CERTs etabliert – zum Beispiel die Fachhochschule Münster (FHMS-CERT) oder die Universitäten in Bielefeld (UBI-CERT), Osnabrück (UOS-CERT), Stuttgart (RUS-CERT), Dresden (TUD-CERT) und Frankfurt (GU-CERT). Da der Fokus dieser Studie auf den Ländern und dem Umgang mit dem Thema Cyber-Angriffe auf Hochschule liegt, wurden diese CERTs, der DFN und DFN-CERT nicht befragt.

[3] Um eine bessere Nachvollziehbarkeit der Ergebnisse zu gewährleisten, sind die Druckschriften im Literaturverzeichnis aufgelistet.

3 Rahmenbedingungen für Cybersicherheit

Die Gefährdungslage für Hochschulen, die durch die zunehmende Digitalisierung der Hochschullandschaft noch zunimmt, erfordert zunächst ein Grundverständnis der verschiedene Sicherheitsbegriffe. Für Deutschland sind die Vorgaben und Bestimmungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) von zentraler Bedeutung. Auf die BSI-Standards wird im Kapitel 3.3 noch detaillierter eingegangen.

Auch wenn die Begrifflichkeiten teilweise synonym verwendet werden, so haben sich doch drei zentrale Termini etabliert, die sich in ihrem Umfang und ihrer Ausrichtung unterscheiden (vgl. u. a. Eckert, 2023). Der umfassendste Sicherheitsbegriff ist die **Informationssicherheit**, die auf den Schutz von Informationen unabhängig von ihrer Form oder ihrem Speichermedium abzielt. Sie umfasst neben technischen Aspekten auch infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen. Die klassischen Schutzziele der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, wobei sowohl digitale als auch analoge Datenträger berücksichtigt werden. In Deutschland bilden die BSI-Standards 200-1 bis 200-3 die Grundlage für Informationssicherheitsmanagementsysteme (ISMS). Parallel dazu konzentriert sich die **IT-Sicherheit** auf die systematische Absicherung informationsverarbeitender IT-Systeme und digitaler Strukturen. Als Teilbereich der Informationssicherheit befasst sich IT-Sicherheit mit digitalen Informationen und deren technischem Schutz. Der BSI-IT-Grundschutz stellt hierfür etablierte Standards und Vorgehensweisen bereit. **Cybersicherheit** fokussiert sich auf Bedrohungen aus dem Cyberraum, insbesondere auf gezielte digitale Angriffe, vernetzte Systeme und die Herausforderungen der vernetzten Gesellschaft. Die drei Begriffe stehen in einem hierarchischen Verhältnis zueinander: Informationssicherheit ist der Oberbegriff, IT-Sicherheit ist ein Teilbereich und Cybersicherheit legt den Fokus auf Bedrohungen aus dem Cyberraum.[4]

3.1 Aktuelle Bedrohungslagen

Einen für die Hochschulen spezifischen Überblick über (öffentlich bekannt gewordene) Cyberangriffe auf Hochschulen weltweit bietet die Internetseite von KonBriefing.[5] Die Seite listet – mit Stand März 2025 – 45 Cyberangriffe auf deutsche Hochschulen auf. Für das Saarland, Brandenburg, Thüringen oder Mecklenburg-Vorpommern sind noch keine Cyberangriffe ausgewiesen (vgl. Abbildung 1). In der Antwort der Bundesregierung auf eine Anfrage im Bundestag zum Thema „Cyberangriffe auf Wissenschaft und Forschung in Deutschland“ wird eine ähnliche Größenordnung genannt: Demnach sind dem „Bundeskriminalamt für den Zeitraum 2022 bis 2024 mit Stand 19. Juni 2024 42 Cyberangriffe auf Hochschulen und Wissenschaftseinrichtungen bekannt geworden“ (Deutscher Bundestag, 2024, S. 3).

[4] Ein Glossar zu den verschiedenen Begrifflichkeiten im Bereich Cybersicherheit bietet u.a. die Cybersicherheitsagentur Baden-Württemberg an. https://www.cybersicherheit-bw.de/glossar.

[5] Zur besseren Nutzbarkeit des Dokuments sind die Links zu den Einrichtungen und Programmen der Länder direkt im Fließtext hinterlegt. Die Links sind aktuell zum Stand Veröffentlichungsdatum.

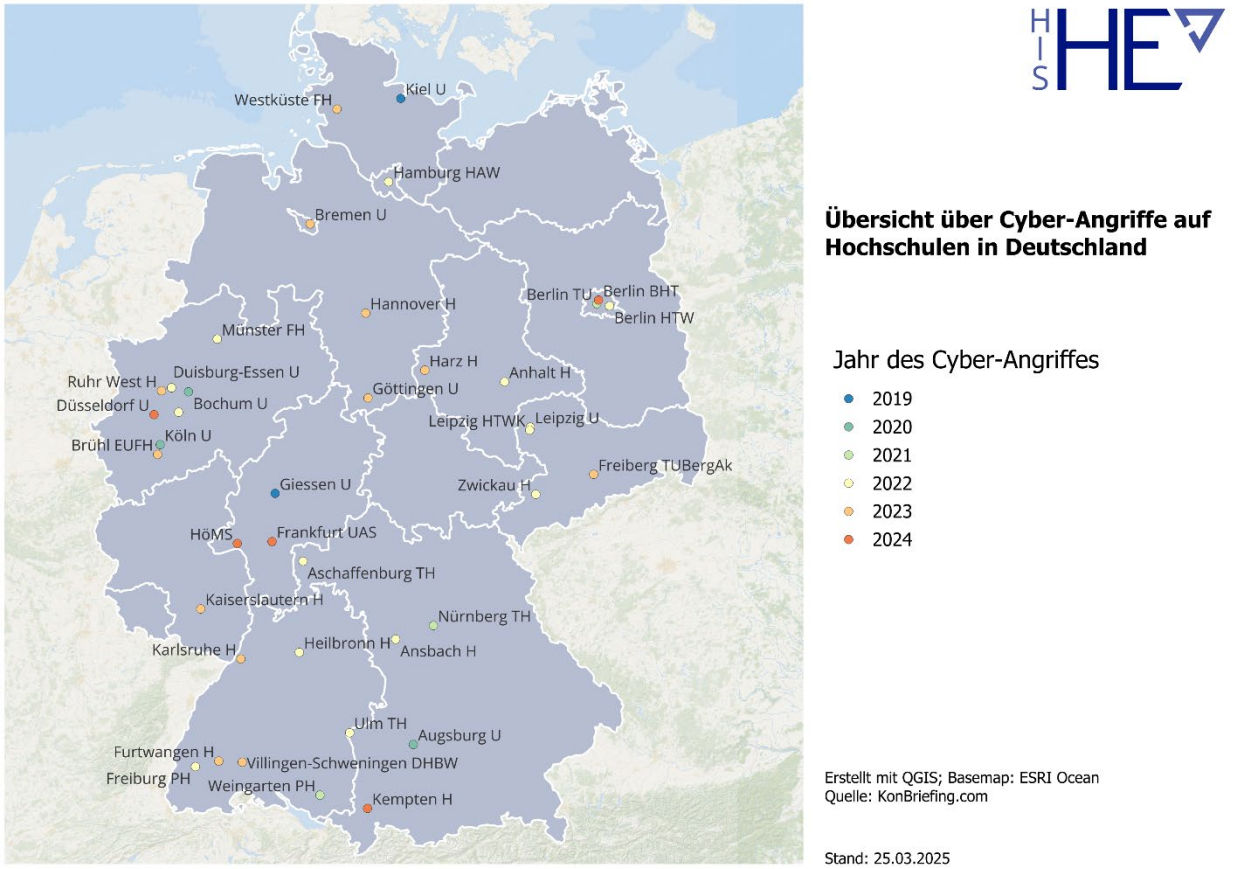

Abbildung 1: Übersicht über Cyberangriffe auf Hochschulen in Deutschland

Diese Zahlen unterliegen jedoch einer Reihe von Einschränkungen. Eine zentrale Einschränkung ist, dass es keine einheitliche Definition von Cyberangriffen gibt. So unterscheidet beispielsweise das Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg (MWK BW) in seiner Antwort auf den Antrag „Cybersicherheit an den Hochschulen in Baden-Württemberg“ (Landtag von Baden-Württemberg, 2023a) zwischen verschiedene Arten von Cyberangriffen. Laut Rückmeldung des Ministeriums lassen sich folgende Cyberangriffe unterscheiden:

- „Cyberangriffe wie Portscans, Spam-Mails oder Phishing-Angriffe“, die „täglich tausendfach auf die Hochschulen“ erfolgen
- seit 2018 ca. 107 Cyberangriffe, „die über die zahlreichen täglichen von den Hochschulen routinemäßig abgewehrten Angriffe hinausgingen“
- „Schwerwiegende Angriffe auf Netzwerke oder von Verschlüsselungstrojanern bewegen sich dabei im einstelligen Bereich“
- „in den letzten Jahren immer wieder Cyberangriffe auf akademische Einrichtungen, die mutmaßlich von fremden Nachrichtendiensten initiiert werden“ (Ebd. S. 3)

Eine weitere Einschränkung besteht in der fehlenden Meldepflicht für Cyberangriffe auf Hochschulen, sodass es kein zentrales Register gibt, in dem u. a. über die Art des Angriffs, Folgeerscheinungen und Folgekosten erfasst werden.

Auf europäischer Ebene bietet das seit 2022 bestehende European Repository of Cyber Incidents (EuRepoC) einen datenbasierten Überblick über Cyber-Bedrohungen an. Laut EuRepoC fanden in Deutschland im Zeitraum vom 01.01.2000 bis zum 18.06.2025 23 Cyberangriffe auf Einrichtungen im Bereich „Education", sieben im Bereich „Science" und 15 im Bereich „Research" statt.[6]

3.2 Rechtliche Grundlagen

Um die Handlungsoptionen von Ländern und Hochschulen im Bereich der Cybersicherheit zu verstehen, muss zunächst die rechtliche Ausgangslage geklärt werden. Regelungen und Rechtsvorschriften zu Cybersicherheit und Informationssicherheit finden sich auf europäischer, nationaler und subnationaler Ebene (vgl. als Überblick Kipker, 2020). Der „Cybersecurity Navigator" ist eine Online-Sammlung von Rechtsvorschriften, Normen und Standards im Bereich Cybersicherheit. Mit Stand Dezember 2024 listet er übergreifend 571 Rechtsvorschriften allein auf transnationaler Ebene auf. Auf Bundesebene sind es 618 Regelungen, auf Landesebene kommen 1.016 Vorschriften hinzu.

Auf **europäischer Ebene** spielt insbesondere die „Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14.12.2022 über Maßnahmen für ein hohes, gemeinsames Cybersicherheitsniveau in der Union" (NIS-2-Richtlinie, 2022) eine besondere Rolle. Die NIS-2-Richtlinie regelt unter anderem die Netzwerk- und Informationssicherheit sowie die Berichtspflichten. Als EU-Richtlinie gilt die NIS-2 nicht direkt, sondern muss in nationales Recht umgesetzt werden. Dies ist in Deutschland noch nicht erfolgt; es liegen jedoch erste Gesetzesentwürfe des Bundesministeriums des Innern (BMI) vor (vgl. „Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtline und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung – NICS2UmsuCG", 2024). Eine weitere zentrale rechtliche Vorgabe ergibt sich aus der Datenschutz-Grundverordnung (DSGVO, 2016). In der DSGVO – wie auch in der NIS2-Richtlinie – sind rechtliche Rahmenbedingungen zur Prävention und zum Vorgehen nach einem Cyberangriff festgelegt. Präventive Maßnahmen gemäß DSGVO umfassen beispielsweise „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen" zu treffen, „um ein dem Risiko angemessenes Schutzniveau zu gewährleisten" (DSGVO, 2016, Art. 17, Abs. 2).

Ein zentrales Gesetz auf **Bundesebene** ist das IT-Sicherheitsgesetz, das erstmals 2015 veröffentlicht wurde und 2021 mit der Einführung des „Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0, 2021)" erweitert wurde. Daneben ist das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI) vom 14. August 2009, zuletzt geändert 2021 (BSIG, 2009), zu nennen. Es enthält unter anderem Regelungen zu Meldepflichten, Informationsaustausch sowie zu Kritischen Infrastrukturen (KRITIS). Neben diesen übergreifenden, nationalen Regelungen bestehen auch entsprechende Regelungen und Gesetze in den Bundesländern. Spezifische Cyber- bzw. IT-Sicherheitsgesetze gibt es derzeit in Baden-Württemberg (CSG BW), Bayern (BayDIG), Hessen (HITSiG), Niedersachsen (NDIG), dem Saarland (IT-SiG SL) und Sachsen (SächsISichG).

[6] Vgl. https://eurepoc.eu/table-view/.

Diese spezifischen Regelungen in den Bundesländern sind nicht nur entscheidend hinsichtlich der Vorgaben und den Rahmenbedingungen für die Cybersicherheit in den Hochschulen, sondern spielen auch bei der Umsetzung der NIS-2-Vorgaben und der Vorgaben für die Kritischen Infrastrukturen (KRITIS) eine Rolle. Eine Umsetzung der NIS-2-Regelung im Bereich Bildungs- und Hochschulbereich ist nur unter Mitwirkung der Länder möglich, wobei einzelne Aspekte der Richtlinie bereits auf Länderebene umgesetzt sind bzw. deren Umsetzung geplant ist (vgl. u. a. Rehbohm, T. & Moses, F., 2023).

3.3 Föderale Zuständigkeiten

Für die Cybersicherheit an Hochschulen sind neben den rechtlichen Grundlagen auch die **institutionellen Strukturen** und deren praktische Umsetzung entscheidend. Auf Bundesebene übernimmt das BSI als Bundesoberbehörde im Geschäftsbereich des BMI laut BSI-Gesetz eine zentrale Rolle bei der Umsetzung der Cybersicherheit in Deutschland. So betreibt das BSI das Nationale IT-Lagezentrum und organisiert federführend die Zusammenarbeit im Nationalen Cyber-Abwehrzentrum sowie beim Schutz Kritischer Infrastrukturen (KRITIS). Darüber hinaus hat das BSI mit verschiedenen Bundesländern Kooperationsvereinbarungen getroffen. Derzeit bestehen solche Vereinbarungen mit den Ländern Saarland, Niedersachsen, Hessen, Sachsen-Anhalt, Rheinland-Pfalz, Sachsen und Bremen.[7] Weitere zentrale Aufgaben des BSI betreffen die operative IT- und Cybersicherheit, Forschung und Forschungsförderung, die Bereitstellung einer Informationsaustausch- und Kooperationsplattform sowie Normung und Zertifizierung. In diesem Zusammenhang hat das BSI verschiedene Standards veröffentlicht:

- BSI-Standard 200-1: Managementsysteme für Informationssicherheit
- BSI-Standard 200-2: IT-Grundschutz-Methodik
- BSI-Standard 200-3: Risikomanagement
- BSI-Standard 200-4: Business Continuity Management
- BSI-Standard 100-4: Notfallmanagement[8]

Auch wenn diese Standards nicht spezifisch auf Hochschulen und Wissenschaftseinrichtungen ausgerichtet sind, können sie entsprechend angepasst und genutzt werden. Hierfür hat insbesondere der Verein „Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e. V." (ZKI) bereits 2019 zusammen mit dem BSI das „IT-Grundschutz-Profil für Hochschulen" veröffentlicht, welches in der Version 2022.0.0 vorliegt (ZKI, 2022). Aktuell hat das ZKI ein Business Continuity Management (BCM)-Profil für Hochschulen als Community Draft (ZKI, 2025) herausgegeben, welches in Zusammenarbeit mit dem BSI entstanden ist und den BSI-Standard 200-4 ergänzt.

Im BSI-Gesetz ist ebenso geregelt, welche Institutionen IT-Sicherheitsvorfälle melden müssen – derzeit Bundesbehörden und Betreiber Kritischer Infrastrukturen (KRITIS). **Kritische Infrastrukturen** sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen. Aktuell sind zehn Sektoren

[7] Vgl. u. a. Pressemitteilung zu „Kooperation gewinnt" – Workshop zu abgeschlossenen Kooperationsvereinbarungen mit den Ländern, 19.8.2024, https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Workshop_Kooperationsvereinbarungen_Laender_240819.html.

[8] Vgl. https://www.bsi.bund.de/dok/6603458.

definiert.[9] Von diesen werden acht Sektoren durch das BSI-Gesetz (2009, § 10, Abs. 1) reguliert.[10] Zum Stichtag 30.09.2024 waren beim BSI 1.128 Betreiber mit insgesamt 2.086 Anlagen als KRITIS registriert – darunter auch Universitätskliniken als Gesundheitseinrichtungen von übergeordneter Bedeutung.[11] Vor dem Hintergrund der notwendigen Umsetzung der europäischen NIS-2-Richtlinie auf nationaler Ebene muss auch die KRITIS-Regelung bzw. das damit verbundene BSI-Gesetz neu geregelt werden. Hierzu hat die Bundesregierung das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz als Referentenentwurf (Bundesregierung, 2024a) auf den Weg gebracht und 2024 veröffentlicht. Parallel dazu hat die Bundesregierung im November 2024 den Entwurf eines Gesetzes zur Stärkung der Resilienz kritischer Anlagen, das sogenannte KRITIS-Dachgesetz, vorgeschlagen (Bundesregierung, 2024b). Beide Gesetzesvorhaben sind aktuell noch im Entwurfs- bzw. Abstimmungsprozess. Unabhängig davon wird sich voraussichtlich die Zahl der KRITIS in Deutschland erhöhen – allein aufgrund der durch die NIS-2-Regelung notwendigen Anpassung der Sektoren und der Grenzwerte.

Ein möglicher zusätzlicher Sektor laut NIS-2 ist der Bereich Forschung. Forschungseinrichtungen werden laut NIS-2 definiert als Einrichtungen, „deren primäres Ziel es ist, angewandte Forschung oder experimentelle Entwicklung im Hinblick auf die Nutzung der Ergebnisse dieser Forschung für kommerzielle Zwecke durchzuführen, die jedoch Bildungseinrichtungen nicht einschließt“ (Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates (NIS-2-Richtlinie), 2022, Art. 6, Abs. 41). Inwieweit der Sektor Forschung auch in Deutschland eingeführt wird, ist derzeit offen. In seiner Sitzung am 03.11.2023 hat der IT-Planungsrat von Bund und Ländern jedoch explizit darum gebeten, dass „die Länder und [der] Bund, von der Option, den Anwendungsbereich der NIS-2-Richtlinie auf Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene und Bildungseinrichtungen zu erstrecken, keinen Gebrauch […] machen“ (IT-Planungsrat, 2023). Eine Begründung für diesen Beschluss liegt nicht vor. In Reaktion auf diese Empfehlung hat beispielsweise der Bundesverband IT-Sicherheit e. V. (TeleTrusT) in einem offenen Brief gefordert, den Beschluss zurückzunehmen und Kommunen und Bildungseinrichtungen gesetzlich zu IT-Sicherheitsmaßnahmen zu verpflichten (Bundesverband IT-Sicherheit, 2023).

Aufgrund der föderalen Struktur Deutschlands ist die **Cybersicherheitsarchitektur** durch ein Zusammenspiel zwischen Bund und Ländern geprägt. Zur Koordination der Aktivitäten bestehen verschiedene zentrale Gremien – auf nationaler (übergreifender) Ebene insbesondere die Länderarbeitsgruppe Cybersicherheit der Innenministerkonferenz sowie die AG Informationssicherheit des IT-Planungsrates (BMI, 2021, S. 21). Das BMFTR ist beispielsweise eingebunden im Nationalen Cybersicherheitsrat (NCSR), im IT-Rat des Bundes und dem Verwaltungsrat des Informationstechnikzentrum Bund (ITZBund) (vgl. Herpig & Dutke, 2023, S. 148). Im Rahmen der Innenministerkonferenz (IMK) haben die Bundesländer eine gemeinsame „Leitlinie zur

[9] Die Sektoren sind Energie, Ernährung, Finanz- und Versicherungswesen, Gesundheit, Informationstechnik und Telekommunikation, Medien und Kultur, Siedlungsabfallentsorgung, Staat und Verwaltung, Transport und Verkehr sowie Wasser. Einen Überblick bietet u. a. das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) an https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/sektoren-branchen_node.html.

[10] Die Ausnahmen sind die Sektoren „Staat und Verwaltung“ sowie „Medien und Kultur“, die gemäß der Bund-Länder-AG bestimmt werden.

[11] Vgl. https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/KRITIS-in-Zahlen/kritis-in-zahlen_node.html. Aus Sicherheitsgründen gibt es keine öffentlich zugängliche Liste oder Datenbank der KRITIS-Einrichtungen.

Entwicklung föderaler Cybersicherheitsstrategien“ erarbeitet und in der 214. IMK-Sitzung vom 16. bis 18.06.2021 verabschiedet.[12] Laut dem vom BMI 2020 herausgegebenen *Online Kompendium Cybersicherheit in Deutschland* beschäftigen sich „über 2.200 Akteur:innen und Initiativen in Deutschland“ thematisch mit Cybersicherheit (BMI, 2020, S. 3). Eine weitere Übersicht über Deutschlands staatliche Cybersicherheitsarchitektur hat die Stiftung Neue Verantwortung (ab 2024 umbenannt in Interface – Tech analysis and policy ideas for Europe) zuletzt im Oktober 2023 veröffentlicht (Herpig & Dutke, 2023).

In allen Bundesländern und beim Bundeskriminalamt wurden Zentrale Ansprechstellen für Cybercrime eingerichtet – die sogenannten „ZACs“.[13] Diese richten sich jedoch vorwiegend an Unternehmen, Behörden und Verbände. Einige Bundesländer haben spezielle juristische Strukturen und Organisationen aufgebaut, die sich dezidiert mit dem Bereich Cyberkriminalität beschäftigen. In Bayern besteht beispielsweise seit 2015 die Zentralstelle Cybercrime (ZCB) bei der Generalstaatsanwaltschaft in Bamberg oder in Baden-Württemberg seit 2024 das Cybercrime-Zentrum bei der Generalstaatsanwaltschaft Karlsruhe. Cyberangriffe und Cyber-Abwehr sind auch Themen für die Landesämter für Verfassungsschutz, die insbesondere Cyberangriffe beobachten, die mutmaßlich einen nachrichtendienstlichen Hintergrund aufweisen. In vielen Bundesländern gibt es Cybercrime-Kompetenzzentren in den Landeskriminalämtern (z. B. LKA NRW). Inwieweit diese auch für die Hochschulen zuständig sind, wird im fünften Kapitel für die einzelnen Bundesländer dargestellt.

[12] Vgl. https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/202106_16-18.html?nn=4812206.

[13] Als Gesamtübersicht vgl. https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html.

4 Umfrageergebnisse: Länderministerien und CERTs

4.1 Ministerielle Cybersicherheitsansätze

Von den 16 angeschriebenen Ministerien hat HIS-HE insgesamt acht Rückmeldungen erhalten. Fünf (62,5%) der antwortenden Ministerien bewerten das Thema Cybersicherheit von Hochschulen als sehr relevant. Ein Ministerium ordnet die Relevanz als gering ein, während zwei Ministerien eine mittlere Relevanz angaben.

Die strukturelle Verankerung des Themas im jeweiligen Ministerium ist unterschiedlich und teilweise in Kombination verschiedener Optionen:

- eigene Referent:innenstelle
- zusätzliche Stabstelle für Informationssicherheit inkl. Stellvertretung
- Beauftragtenstelle für Informationssicherheit
- Chief Information Security Officer (CISO) im Ressort
- Ansprechperson für Informationssicherheit für Hochschulen.

Ohne explizite Stelle wird das Thema im Fachreferat IT oder im Referat für Hochschulen mitbearbeitet. Zwei Ministerien planen in Zusammenarbeit mit den Hochschulen eigene Security Operations Centers.

Bei den offenen Antworten zu den Unterstützungsleistungen lassen sich verschiedene Formen unterscheiden, je nachdem, ob die Unterstützung verschiedene Einzelmaßnahmen kombiniert oder ob das Ministerium ein umfassendes Unterstützungsangebot im Bereich Cybersicherheit bietet. Weiterhin unterscheiden sich die Maßnahmen darin, ob sie den einzelnen Hochschulen individuell zur Verfügung gestellt werden, als zentrales Landesangebot konzipiert sind oder ob das zuständige Ministerium ein Netzwerkmodell der Hochschulen unterstützt, bei dem die Hochschulen die entsprechenden Angebote selbst bereitstellen (vgl. Abbildung 2).

	je Hochschule	**als zentrales Landesangebot**	**als Netzwerkmodell der Hochschulen**
Umfassende Maßnahmen im Bereich Cybersicherheit	Aufbaumodell	Zentralmodell	Netzwerkmodell
Einzelmaßnahmen	Individualmodell	Mischmodell	Individuelles Netzwerkmodell

Abbildung 2: Unterstützungsmodelle

Aus den sechs Modellen lassen sich drei zentrale Organisationsformen ableiten, wobei die Übergänge zwischen den Modellen fließend sind. Einzelmaßnahmen zur Unterstützung im Individual-, Zentral- und Netzwerkmodell sind insbesondere:

Individualmodell: Direkte Unterstützung einzelner Hochschulen

- Personalförderung: Finanzierung von Dauerstellen für Informationssicherheitsbeauftragte an den Hochschulen, von zusätzliche Dauerstellen im Bereich Cybersicherheit oder von befristeten Stellen als Übergangslösung
- Infrastrukturförderung: Finanzielle Unterstützung für Hardware, Software und bauliche Maßnahmen
- Technische Services: Systematische Scans zur Erkennung von Sicherheitslücken und Fehlkonfigurationen
- Standards: Individuelle Abstimmung zur Umsetzung von BSI-Standards.

Zentralmodell: Landesweite Angebote für alle Hochschulen

- Technische Infrastruktur: Aufbau Security Operation Centers, Bereitstellung von IT-Basisdiensten für eine hochschulübergreifende Datensicherung, Anti-Spam-Cluster
- Bildung und Vernetzung: Selbstlernakademie für Cyber- und IT-Sicherheit, Cybersicherheitstage, Trainings und Veranstaltungen,
- Kooperation: Netzwerke zur Stärkung der Informationssicherheit, Meldewesen zwischen Hochschulen,
- Beschaffung: Landesweite Rahmenverträge für Sicherheitstools, technische Tools für Schwachstellenanalysen.

Netzwerkmodell: Unterstützung der Eigeninitiativen der Hochschulen

- Sensibilisierung: Durchführung von Awarenesskampagnen
- Technische Maßnahmen: Sicherheitsscans, zentrale Netzgeräteverzeichnisse, Multi-Faktor-Authentifizierung, Patchmanagement
- Kompetenzaufbau: Personal- und Prozessschulungen, Entwicklung von Notfallplänen, Aufbau von Information Security Management Systemen
- Beratung: Kompetenzzentrum für IT-Sicherheit zur Hochschulberatung

Die Analyse zeigt zudem, dass die Länder je Unterstützungsbereich unterschiedliche Präferenzen wählen (vgl. Abbildung 3). So dominiert der Individualansatz bei Themen wie Informationssicherheitsbeauftragten und BSI-Standards, während landesweite Ansätze überwiegend bei IT-Infrastrukturdiensten, Weiterbildungsangebote und Austauschgremien genutzt werden. Unterstützungslücken bestehen bei Audits und Zertifizierungen. Etwa die Hälfte der befragten Ministerien bietet in diesem Bereich keine Unterstützungsangebote an. Auch Unterstützung im Bereich IT-Personalfragen (z. B. hinsichtlich Finanzierung, Gewinnung und Entwicklung) wird von drei der acht Länder als nicht vorhanden bezeichnet.

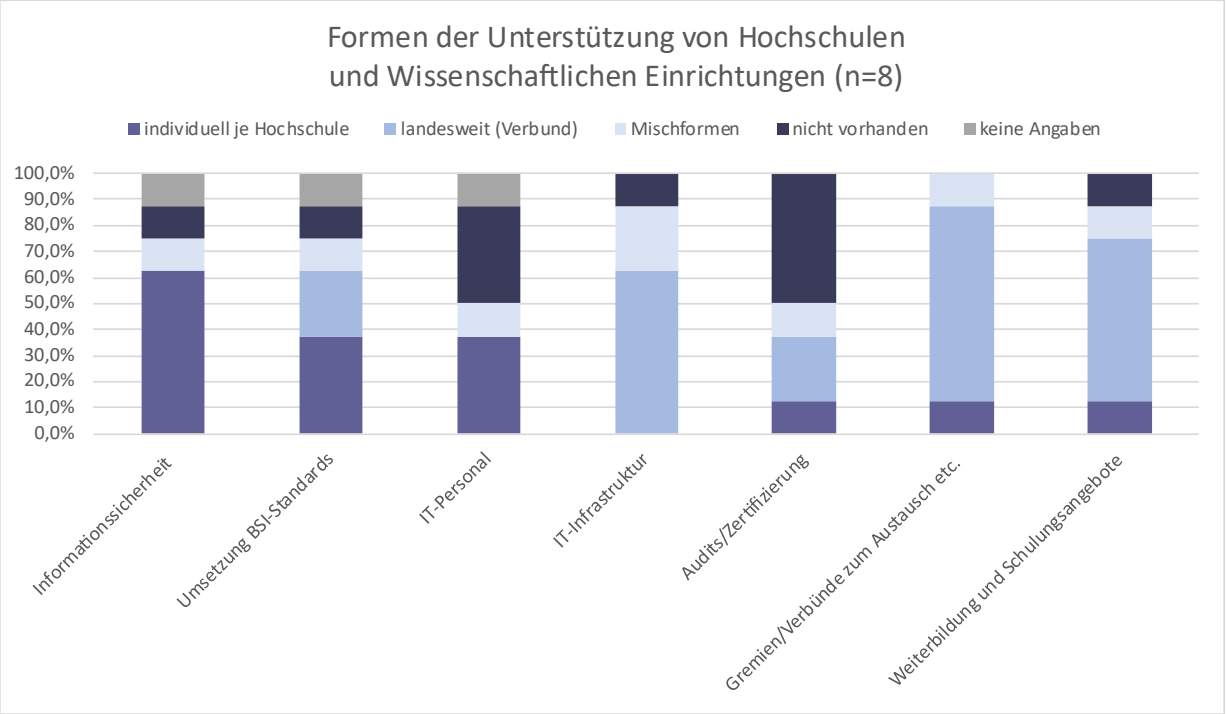

Abbildung 3: Formen der Unterstützung von Hochschulen und wiss. Einrichtungen

4.2 CERT-Unterstützungsleistungen

Die Frage nach der Unterstützung von Hochschulen durch die CERTs der Länder wurde sowohl den Ministerien als auch den CERTs selbst gestellt. Von den 14 angeschriebenen CERTs[14] haben acht Einrichtungen geantwortet. Die CERTs in Nordrhein-Westfalen, Rheinland-Pfalz und dem Saarland sowie das CERT des Bundes haben mitgeteilt, dass sie nicht für Hochschulen und wissenschaftliche Einrichtungen zuständig sind (vgl. Abbildung 4).

[14] Das CERT-Nord bietet gemeinschaftlich Dienstleistungen für die Bundesländer Bremen, Hamburg, Sachsen-Anhalt und Schleswig-Holstein an.

Bundesland	CERT	Unterstützungsleistungen für Hochschulen
Baden-Württemberg	CSBW - Cybersicherheit Baden-Württemberg	ja
Bayern	CAZ	ja
Berlin	ITDZ Berlin	keine Rückmeldung
Brandenburg	CERT-Brandenburg	keine Rückmeldung
Bremen	CERT-Nord	ja
Hamburg	CERT-Nord	ja
Hessen	Hessen3C	ja
Mecklenburg-Vorpommern	CERT-MV	ja
Niedersachsen	N-CERT	ja
Nordrhein-Westfalen	CERT NRW	nein
Rheinland-Pfalz	CERT-rlp	nein
Saarland	CERT Saarland	nein
Sachsen	SAX.CERT	ja
Sachsen-Anhalt	CERT-Nord	ja
Schleswig-Holstein	CERT-Nord	ja
Thüringen	ThüringenCERT	keine Rückmeldung
Bundesrepublik Deutschland	CERT-BUND	nein

Abbildung 4: Übersicht Zuständigkeit von CERTs

Die überwiegende Mehrheit der CERTs ist prinzipiell auch für Hochschulen und wissenschaftliche Einrichtungen zuständig. In den Antworten und Anmerkungen zum Fragebogen wird aber deutlich, dass die Dienste und Angebote der CERTs der Länder nur in sehr geringem Maße von Hochschulen in Anspruch genommen werden.

5 Cybersicherheit an Hochschulen: Situation in den Bundesländern

Die Darstellung der verschiedenen Aktivitäten der Länder im Bereich der Cybersicherheit an Hochschulen ergänzt die Ergebnisse der Umfragen. Sie basiert auf öffentlich zugänglichen Quellen und folgt – soweit möglich – einer einheitlichen Grundstruktur:

- bisherige (exemplarisch ausgewählte) Cyberangriffe auf Hochschulen
- (übergeordnete) IT-Sicherheitsstrategie des Landes
- hochschulspezifische Regelungen und Maßnahmen
- Überblicksdarstellung der zuständigen Behörden und Anlaufstellen

Für jedes Bundesland werden zudem tabellarisch die übergreifenden politischen und behördlichen Zuständigkeiten, die zentralen Einrichtungen und koordinierenden Stellen sowie Initiativen, Projekte oder Verbünde im Hochschul- und Wissenschaftsbereich dargestellt. Da der Fokus auf der übergreifenden Ebene liegt, werden Einzelprojekte und Einrichtungen innerhalb der Hochschulen nicht separat aufgelistet. In Einzelfällen werden weitere Akteure und Initiativen mit – im weitesten Sinne – Bezug zum Thema aufgeführt, soweit diese von Bedeutung für die Themenfelder Cyber- und IT-Sicherheit an Hochschulen und wissenschaftlichen Einrichtungen sind.

5.1 Baden-Württemberg

Auf Hochschulen in Baden-Württemberg gab es in den vergangenen Jahren mehrere Cyberangriffe – unter anderem im Jahr 2022 auf die Pädagogische Hochschule Freiburg und die Hochschule Heilbronn oder 2023 auf die Hochschule Karlsruhe und die Hochschule Furtwangen. Laut einer Stellungnahme des Ministeriums für Wissenschaft, Forschung und Kultur Baden-Württemberg (MWK-BW) auf eine Anfrage im Landtag zum Thema „Cybersicherheit an Hochschulen in Baden-Württemberg“ wurden dem Ministerium seit Sommer 2018 „rd. 107 Cyberangriffe auf Hochschulen bzw. Hochschuleinrichtungen mitgeteilt, die über die zahlreichen täglichen, von den Hochschulen routinemäßig abgewehrten Angriffe hinausgingen.“ Darüber hinaus wurden schwerwiegende Angriffe „im einstelligen Bereich“ bekannt, die aber „bis zum Jahr 2020“ keinen „unmittelbaren Schaden in monetärer Hinsicht“ verursachten (Landtag von Baden-Württemberg, 2023a, S. 3).

Auch vor diesem Hintergrund hat das Land frühzeitig die Cybersicherheitsarchitektur angepasst und 2015 das E-Government-Gesetz Baden-Württemberg (EGovG BW) sowie 2021 das Cybersicherheitsgesetz Baden-Württemberg (CSG BW) und im gleichen Jahr die Cybersicherheitsstrategie Baden-Württemberg (Ministerium des Inneren, für Digitalisierung und Kommunen, 2021) verabschiedet. Mit dem CSG BW wurde die Cybersicherheitsagentur Baden-Württemberg (CSBW) gegründet, die seit dem 1.1.2022 tätig ist und u. a. das CERT BWL übernommen hat. Die CSBW und das CERT BWL nehmen eine Schlüsselrolle in der Cybersicherheit für das Bundesland ein und bieten u. a. einen Warn- und Informationsdienst sowie damit verbundene Handlungsempfehlungen an. Die Hochschulen sind an den Warn- und Informationsdienst angebunden und das CERT BWL ist in Krisenfällen eine der ersten Anlaufstellen. Darüber hinaus bietet das CSBW den Hochschulen

eine ganze Reihe von Beratungsangeboten an, die von individueller Beratung bis hin zu Workshops reichen.[15] Laut Rückmeldung des MWK-BW auf eine Anfrage im Landtag Ende 2023 stand „zunächst die gegenseitige Vernetzung und Ausgestaltung der operativen Zusammenarbeit“ (Landtag von Baden-Württemberg, 2023b, S. 6) im Fokus der bisherigen Zusammenarbeit zwischen Hochschulen und CSBW. Darauf aufbauend soll „zwischen dem Hochschulbereich und der CSBW eine gesonderte Vereinbarung i. S. d. § 2 Absatz 2 Satz 2 des Cybersicherheitsgesetzes Baden-Württemberg geschlossen werden, um die Zusammenarbeit auf operativer, strategischer und taktischer Ebene auszugestalten“ (Landtag von Baden-Württemberg, 2023a, S. 6). Baden-Württemberg hat zudem eine Vereinbarung über eine vertiefte Zusammenarbeit mit dem BSI getroffen, in dessen Rahmen 2019 u. a. ein Verbindungsbüro in Stuttgart eröffnet wurde.[16]

Die Hochschulen haben bereits im Sommer 2019 mit dem Aufbau des Hochschulnetzwerkes bwInfoSec begonnen. Dieser Zusammenschluss aller Universitäten und Hochschulen des Landes hat zum Ziel, gemeinsam die Informationssicherheit zu verbessern. Das MWK-BW unterstützt die Bestrebungen und hat zum Beispiel seit 2020 zur Etablierung von Beauftragten für Informationssicherheit an den Hochschulen 58 Stellen mit Sachmittelausstattung bereitgestellt. Darin enthalten ist ein zwölfköpfiges Kernteam des bwInfoSec an den Standorten in Reutlingen (für die Hochschulen für Angewandte Wissenschaften) und in Heidelberg (für die Universitäten).

Neben dem Informationsaustausch zwischen den Hochschulen soll das Netzwerk durch Beratungs- und Sensibilisierungsleistungen, Hilfestellungen bei der Bewältigung von Vorfällen leisten und durch den zentralen Betrieb von Sicherheitstools die Cyber-Abwehr der Hochschulen stärken. Dafür bestehen zum Beispiel eine gemeinsame Arbeitsgruppe zwischen bwInfoSec und der CSBW. Darüber hinaus bestehen Kooperationen mit dem Landeshochschulnetz BelWü und dem bwCampusNetz. Ferner vernetzt bwInfoSec die beteiligten Institutionen hochschulartübergreifend in verschiedenen Arbeitsgruppen (u. a. zur Multifaktorauthentifizierung, zum Aufbau eines Information Security Management Systems (ISMS), zu Formulierung einer Informationssicherheitsleitlinie und zur Sensibilisierung von Mitarbeiterinnen und Mitarbeiter). Insgesamt stellt das Ministerium seit dem Jahr 2020 jährlich rund 6,25 Mio. Euro bzw. seit 2023 jährlich rund 6,5 Mio. Euro an Unterstützungsleistungen zur Verfügung (Landtag von Baden-Württemberg, 2023a, S. 6). Innerhalb des MWK BW gibt es zudem seit 2018 eine Ansprechperson für die Informationssicherheit der Hochschulen, die auf Seite der Behörde die Thematik betreut. Das CSBW wie auch das MWK-BW haben an der Umfrage von HIS-HE teilgenommen.

Eine Überblicksdarstellung der zuständigen Behörden und Anlaufstellen für Cybersicherheit in Baden-Württemberg enthält Tabelle 1.

[15] Vgl. https://www.cybersicherheit-bw.de/beratungsangebote-fuer-hochschulen.

[16] Vgl. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2019/Verbindungsbuero-Stuttgart-140219.html.

Politische und behördliche Zuständigkeiten

▪ Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg (IM-BW), u. a.
  ▪ Abt. 4: Digitalisierung, Ref. 44: Informations- und Cybersicherheit
  ▪ Verbindungsstelle des BSI für Süddeutschland in den Räumen des IM-BW
▪ Ministerium für Wissenschaft, Forschung und Kunst (MWK-BW), u. a.
  ▪ Abt. 4: Hochschulen und Digitalisierung
▪ Beauftragter der Landesregierung für Informationstechnologie (CIO BW)
▪ Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI)
▪ Landesamt für Verfassungsschutz Baden-Württemberg (LfVBW)

Zentrale Einrichtungen und koordinierende Stellen
▪ Landesoberbehörde IT Baden-Württemberg (BITBW) ▪ Zentrale Ansprechstelle Cybercrime (ZAC BW) sowie Kriminalinspektion 5 (Cybercrime, Digitale Spuren) beim LKA BW ▪ Cybersicherheitsagentur Baden-Württemberg (CSBW), u. a.   ▪ CERT BWL
Initiativen, Projekte oder Verbünde im Hochschul- und Wissenschaftsbereich

▪ Föderation bwInfoSec
▪ Landeshochschulnetz Baden-Württemberg (BelWü)
▪ bwCampusNetz
▪ FZI Forschungszentrum Information, Karlsruhe (FZI), u. a.
  ▪ Forschungsschwerpunkt Safety, Security and Law
▪ Sicherheitsforum Baden-Württemberg
  ▪ Gremium zur Unterstützung von Unternehmen und Forschungseinrichtungen beim Schutz gegen Sabotage, Spionage und Know-How-Verlust

Tabelle 1: Aktivitäten und Initiativen zur Cybersicherheit in Baden-Württemberg

5.2 Bayern

Im Jahr 2020 erfolgte einer der ersten Cyberangriffe auf eine Hochschule im Bundesland auf die Universität Augsburg. Seitdem erfolgten immer wieder Cyberangriffe auf Hochschulen und Wissenschaftseinrichtungen – unter anderem im Jahr 2022 auf die Technische Hochschule Aschaffenburg und die Hochschule Ansbach sowie zuletzt im Jahr 2024 auf die Hochschule Kempten.

Bayern hat im Rahmen der Initiative Cybersicherheit Bayern bereits 2013 das Cyber-Allianz-Zentrum (CAZ) im Bayerischen Landesamt für Verfassungsschutz gegründet. 2015 folgte u. a. die Zentralstelle Cybercrime (ZCB) bei der Generalstaatsanwaltschaft in Bamberg und 2017 – als erstes Bundesland in Deutschland – das Landesamt für Sicherheit in der Informationstechnik (LSI). Die Bayerische Cybersicherheitsstrategie wurde seit 2013 kontinuierlich ausgebaut und zum Beispiel 2020 die Cyberabwehr Bayern ins Leben gerufen, um vor allem die Kooperation zwischen den Behörden zu stärken. Das Bayerische Digitalgesetz (BayDiG) folgte 2022 und im Jahr 2023 wurde die überarbeitete Cybersicherheitsstrategie 2.0 (Bayerisches Staatsministerium des Innern, für Sport und Integration, 2023) veröffentlicht. Laut Cybersicherheitsstrategie 2.0 bilden Wirtschaft und Wissenschaft ein gemeinsames Handlungsfeld, in dem es u. a. darum geht, eine „Verbesserung des Anzeigeverhaltens (Dunkelfeldaufhellung) im Deliktfeld Cybercrime“ (ebd., S. 17) zu erreichen. Maßnahmen im Handlungsfeld sind beispielsweise „C2. Ausbau des Schutzes kritischer Infrastrukturen“ sowie „C3. Stärkung der IT-Sicherheit in staatlichen Hochschulen“.

Auf Seiten der Hochschulen in Bayern wurde Ende 2021 die IT-Strategie der bayerischen Hochschulen beschlossen (IT-Strategie der bayerischen Hochschulen, 2021) und der „Digitalverbund Bayern“ gegründet, wobei dem Digitalverbund alle staatlichen und staatlich geförderten Hochschulen sowie das Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften angehören. Das Bayerische Staatsministerium für Wissenschaft und Kunst (StMWK BY) unterstützt und fördert den Digitalverbund sowie die damit verbundenen Projekte. Parallel wurden u. a. in der „Rahmenvereinbarung Hochschulen 2023 bis 2027“ zwischen der Bayerischen Staatsregierung (2023) und den Hochschulen festgelegt, dass die Hochschulen ein internes Information Security Management Systems (ISMS) entsprechend dem bayerischen Hochschul-Informationssicherheitsprogramms (HISP)[17] einrichten müssen. Eine weitere Vorgabe in den Rahmenbedingungen ist die Zusammenarbeit mit dem „Hochschulübergreifenden IT-Service Informationssicherheit“ (HITS-IS), welches im Rahmen des Digitalverbundes Bayern seit 2022 seine Dienste anbietet. Das HITS IS stellt konkrete Unterstützungsleistungen (wie z. B. Schwachstellenscans, Beratung zum Thema Business Continuity Management und Erstanalyse bei Sicherheitsvorfällen) zur Verfügung und baut aktuell das Cyber Security Incidence Response Team (eduSCIRT Bayern) auf. Der Vorläufer von HITS IS – die Stabsstelle Informationssicherheit der bayerischen, staatlichen Hochschulen und Universitäten – hat 2020 das bereits genannten Hochschulinformationssicherheitsprogramm (HISP, Stabsstelle Informationssicherheit der bayerischen, staatlichen Hochschulen und Universitäten, 2020) veröffentlicht. Den Hochschulen steht auch das CAZ in Fragen der Cyberspionage und -sabotage zur Verfügung. Das Angebot reicht hier von Sensibilisierungsmaßnahmen bis hin zur konkreten Fallberatung. An der Umfrage teilgenommen haben das CAZ und das StMWK BY.

[17] Vgl. die Version 1.0 (2020) unter https://www.tha.de/Binaries/Binary45562/HISP-V1.pdf&ved=2ahUKEwiOoNilxIeMAxXh9rsIHQYmIqMQFnoECBsQAQ&usg=AOvVaw0AxcgE1I43ve_4S--AAiAp.

Eine Überblicksdarstellung der zuständigen Behörden und Anlaufstellen für Cybersicherheit in Bayern enthält Tabelle 2.

Politische und behördliche Zuständigkeiten

▪ Bayerisches Staatsministerium des Innern, für Sport und Integration (StMI), u. a.
  ▪ Abt. E Verfassungsschutz, Cybersicherheit, Sachgebiet E5 Cybersicherheit und Geheimschutz
▪ Bayerisches Staatsministerium für Digitales (StMD), u. a.
  ▪ Abt. A Digitales Bayern, Ref. A5 Informationssicherheit und Cybercrime
  ▪ IT-Beauftragter der Bayrischen Staatsregierung / CIO
▪ Bayerisches Staatsministerium der Finanzen und für Heimat (StFMH), u. a.
  ▪ Abt. VII Digitalisierung, Breitband und Vermessung, Ref. 77: Grundsatzfragen der IT, IT-Sicherheit, digitale Technologie
▪ Bayerisches Staatsministerium für Wissenschaft und Kunst (StMWK), u. a.
  ▪ Abt. Z Zentrale Angelegenheiten, Digitalisierung und IT, Ref. Z.5 IT an Hochschulen und im Kunstbereich
▪ Bayerische Landesbeauftragte für den Datenschutz (BayLfD)
▪ Bayerisches Landesamt für Datenschutzaufsicht (LDA)
▪ Bayerisches Landesamt für Verfassungsschutz (LfV)
▪ Bayerisches Landesamt für Sicherheit in der Informationstechnik (LSI)
▪ Landesamt für Sicherheit in der Informationstechnik (LSI) inkl.
  ▪ Bayern-CERT

Zentrale Einrichtungen und koordinierende Stellen
▪ IT-Dienstleistungszentrum des Freistaats Bayern (IT-DLZ) ▪ Cyber-Allianz-Zentrum Bayern (CAZ) im Bayrischen Landesamt für Verfassungsschutz (LfV) ▪ Zentrale Ansprechstelle Cybercrime für die Wirtschaft (ZAC) beim Bayerischen Landeskriminalamt (LKA) ▪ Zentralstelle Cybercrime Bayern (ZCB) bei der Generalstaatsanwaltschaft Bamberg
Initiativen, Projekte oder Verbünde im Hochschul- und Wissenschaftsbereich
▪ Digitalverbund Bayern im Hochschulbereich, u. a.   ▪ Hochschulübergreifender IT-Services für Informationssicherheit (HITS IS) ▪ Stabsstelle IT-Recht an der Universität Würzburg ▪ Projekt eduCSIRT Bayern ▪ IT-Sicherheitscluster e.V ▪ Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC)

Tabelle 2: Aktivitäten und Initiativen zur Cybersicherheit in Bayern

5.3 Berlin

Auch in Berlin sind Hochschulen Ziel von größeren Cyberangriffen geworden – zum Beispiel 2021 die Technische Universität Berlin, 2022 die Hochschule für Technik und Wirtschaft Berlin und 2024 die Berliner Hochschule für Technik. Weitere bekannte Angriffe waren 2023 auf das Museum für Naturkunde Berlin und das Helmholtz-Zentrum Berlin (HZB). Die Position der Senatsverwaltung für Wissenschaft, Gesundheit und Pflege (SenWGP) zum Thema wird in einer Antwort auf eine Anfrage zum Cyberangriff auf das Naturkundemuseum deutlich: „Die in dem zuständigen Referat betreuten außeruniversitären Forschungseinrichtungen sind rechtlich selbständig und tragen insofern selbst die Verantwortung für eine funktionierende IT-Sicherheit. Bei Einrichtungen, die als juristische Personen des öffentlichen Rechts organisiert sind, bestehen staatliche Eingriffsmöglichkeiten im Wege der Staats- und Rechtsaufsicht, soweit die Voraussetzungen hierfür gegeben wären“ (Abgeordnetenhaus Berlin, 2024, S. 3f.). Auf übergeordneter Ebene wird Cybersicherheit im Koalitionsvertrag 2023-2026 eine besondere Rolle zugewiesen, da „[g]erade die Hauptstadt Berlin […] einen erhöhten Sicherheitsstandard“ (Koalitionsvertrag 2023-2026, 2023, S. 16) benötigt. Die Umsetzung erfolgt u. a. durch den Landesbevollmächtigten für Informationssicherheit, den Bereich IKT-Sicherheit sowie die AG Cybersicherheit im Referat III A der Senatsverwaltung für Inneres und Sport. Ein übergreifendes IT-Sicherheitsgesetz besteht nicht. Den rechtlichen Rahmen legen die Leitlinie zur Informationssicherheit (Berliner Senatsverwaltung für Inneres und Sport, 2017) sowie das Gesetz zur Förderung des E-Government (EGovG Bln, 2016) fest. Eine Meldepflicht der Hochschulen für Cyberangriffe ist darin nicht festgelegt (Abgeordnetenhaus Berlin, 2021a, S. 1).

Zentraler Dienstleister für die Berliner Verwaltung ist das IT-Dienstleistungszentrum (ITDZ), welches auch ein Cyber Defense Center und ein CERT-Team unterhält (Abgeordnetenhaus Berlin, 2023, S. 2-39). Der Fokus des ITDZ und des CERT liegt auf der Berliner Verwaltung. Ein weiteres Angebot besteht seitens der Digital Agentur Berlin (DAB), jedoch vorrangig für Berliner Unternehmen. Die DAB bietet beispielsweise kostenfreie Hilfe im IT-Notfall (inkl. Cyberhotline), Cyberwerkstätten, IT-Sicherheitschecklisten zur Selbstprüfung oder praxisorientierte online-Formate an.

Im Zuge der Corona-Maßnahmen hat das Land den Hochschulen Mittel im Rahmen des Virtual-Campus-Programms zur Verfügung gestellt – insbesondere zum Auf- und Ausbau der IT-Infrastrukturen. Die Umsetzung erfolgt in der Regel pro Hochschule; übergreifende Maßnahme für IT-Systeme und damit für IT-Sicherheit fanden nur bedingt statt. Es bestehen aber eine Reihe von Austauschrunden zum Beispiel zu den Themen IT-Sicherheit und IT-Leitung (vgl. Abgeordnetenhaus Berlin, 2021b). Eine Rückmeldung des CERT Berlin und der SenWGP zu den beiden Umfragen liegen nicht vor.

Eine Überblicksdarstellung der zuständigen Behörden und Anlaufstellen für Cybersicherheit in Berlin enthält Tabelle 3.

Politische und behördliche Zuständigkeiten

▪ Der Regierende Bürgermeister – Senatskanzlei, u. a.
  ▪ Landesbevollmächtigter für Informationssicherheit/IKT-Steuerung
▪ Senatsverwaltung für Inneres und Sport, u. a.
  ▪ AG Kritische Infrastrukturen, Cybersicherheit im Ref. III A
  ▪ Verfassungsschutz in Abt. II
▪ Senatsverwaltung für Wissenschaft, Gesundheit und Pflege, u. a.
  ▪ Abt. Z – Zentrales, Ref. Z D – Infrastruktur
▪ Berliner Beauftragter für Datenschutz und Informationsfreiheit

Zentrale Einrichtungen und koordinierende Stellen
▪ IT-Dienstleistungszentrum (ITDZ) inkl.   ▪ Cyber Defense Center und CERT-Berlin ▪ Zentrale Ansprechstelle Cybercrime (ZAC) für die Berliner Wirtschaft ▪ Digital Agentur Berlin (DAB)
Initiativen, Projekte oder Verbünde im Hochschul- und Wissenschaftsbereich
▪ Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS, u. a.   ▪ Forschungsthemen Digitale Vernetzung und Sicherheit/Zertifizierung

Tabelle 3: Aktivitäten und Initiativen zur Cybersicherheit in Berlin

5.4 Brandenburg

KonBriefing verzeichnet noch keine Cyberangriffe auf eine Hochschule in Brandenburg. Laut Bericht des Ministeriums für Wissenschaft, Forschung und Kultur Brandenburg (MWFK BB) in einer Sitzung des Ausschusses für Wissenschaft, Forschung und Kultur sind die Hochschulen des Landes aber „regelmäßig Cyberangriffen unterschiedlichster Art und Intensität ausgesetzt“ (Landtag Brandenburg, 2023a, S. 1). Im Jahr 2021 stellte der Landesrechnungshof Brandenburg bei seiner Prüfung der IT-Sicherheit an den Hochschulen verschiedene Defizite fest: „IT-Sicherheit stiefmütterlich finanziert“, „Zu wenig Personal für IT-Sicherheit“ sowie „Informationssicherheitsbeauftragte: zwingend erforderlich, aber selten vorhanden“ (Landesrechnungshof Brandenburg, 2021, S. 173-187). Zur Rolle des MWFK BB führt der Bericht an, dass „ministerielle Vorgaben im Kontext der IT-Sicherheit“ fehlen und die Hochschulen „ganz überwiegend keinen Kontakt zum MWFK betreffend IT-Sicherheitsfragen“ haben (ebd., S. 181). Auch vor diesem Hintergrund hat das Land verschiedene Initiativen gestartet, wobei übergeordnet die Landesregierung im Jahr 2021 das „Digitalprogramm 2025“ verabschiedet hat (vgl. Landesregierung Brandenburg, 2022). Unabhängig davon besteht im Bundesland kein übergeordnetes IT-Sicherheitsgesetz, jedoch eine „Leitlinie für die Informationssicherheit in der Landesverwaltung Brandenburg und der Justiz“ (2024).

Eine Maßnahme des MWFK BB ist beispielsweise die gemeinsame Weiterentwicklung der Verwaltungs-IT der Hochschulen (vgl. Landtag Brandenburg, 2023b, S. 1), wofür insbesondere das bereits im Jahr 2019 gegründete Zentrum der Brandenburgischen Hochschulen für Digitale Transformation (ZDT) genutzt wird. Das ZDT als Kooperationsverband koordiniert verschiedene Digitalisierungsprojekte und bietet Veranstaltungen zum Thema Informationssicherheit an. Maßnahmen zur IT-Sicherheit werden ebenfalls überprüft, insbesondere um technische Einzellösungen zu vermeiden. So wurden u. a. Materialien zur Einführung eines Informationssicherheitskonzeptes für Hochschulen erarbeitet. Parallel hat das MWFK BB der Universität Potsdam ein Projekt zur Bereitstellung einer Plattform für IT-Sicherheitsschulungen und -Trainings übertragen. Zudem sollen an jeder Hochschule Informationssicherheitsmanagementsysteme eingeführt werden und jede Hochschule hat Informationssicherheitsbeauftragte benannt (vgl. Landtag Brandenburg, 2023b). Über eine Zertifizierung der IT-Sicherheit verfügt bisher allein die Technische Hochschule Wildau. Rückmeldungen des CERT Brandenburg oder des MWFK BB zu den beiden Umfragen von HIS-HE liegen nicht vor.

Eine Überblicksdarstellung der zuständigen Behörden und Anlaufstellen für Cybersicherheit in Brandenburg enthält Tabelle 4.

Politische und behördliche Zuständigkeiten

▪ Ministerium des Innern und für Kommunales (MIK), u. a.
  ▪ Abt. 6: Digitalisierung, E-Government und IT-Leitstelle
  ▪ Verfassungsschutz
▪ Ministerium für Wissenschaft, Forschung und Kultur (MWFK)
▪ Landesbeauftragte für Datenschutz und Akteneinsicht (LDA)

Zentrale Einrichtungen und koordinierende Stellen
▪ Brandenburgischer IT-Dienstleister (ZIT-BB)   ▪ inkl. CERT-Brandenburg ▪ Cyber-Competence-Center (CCC) im Landeskriminalamt (LKA) ▪ Zentrale Ansprechstelle Cybercrime (ZAC) im Landeskriminalamt (LKA) für Wirtschaftsunternehmen und Behörden ▪ Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer- und Datennetzkriminalität Cottbus
Initiativen, Projekte oder Verbünde im Hochschul- und Wissenschaftsbereich
▪ Zentrum der Brandenburgischen Hochschulen für Digitale Transformation (ZDT) ▪ Hasso-Plattner-Institut für Digital Engineering gGmbH (HPI), u. a.   ▪ Forschungsgebiet Cybersecurity

Tabelle 4: Aktivitäten und Initiativen zur Cybersicherheit in Brandenburg

5.5 Bremen

Die Universität Bremen wurde im Jahr 2023 Ziel eines Cyberangriffes. KonBriefing verzeichnet keine weiteren Angriffe auf Hochschulen in Bremen. In einer Stellungnahme des Bremer Senats heißt es aber: „Gleichwohl hat die Freie Hansestadt Bremen für die Bereiche Hochschulen, Forschungseinrichtungen, Krankenhäuser und die öffentliche Verwaltung im Land Bremen in 2019: 20, 2020: vier, 2021: sechs und im 1. Halbjahr 2022: sieben Ereignisse […] notiert“ (Bremische Bürgerschaft, 2022, S. 4). Auch vor diesem Hintergrund wurde 2023 die „Bremische Cybersicherheitsstrategie“ verabschiedet, in der eine Maßnahme die „stärkere Vernetzung von Hochschulen, Wirtschaft und Behörden [ist], um auf das Thema Cybersicherheit aufmerksam zu machen“ (Senator für Inneres im Auftrag des Senats der Freien Hansestadt Bremen, 2023, S. 71). Zur besseren Koordinierung und Steigerung der digitalen Resilienz wurde 2023 die Zentralstelle Cybersicherheit eingerichtet, die zukünftig als Ansprechstelle auch für wissenschaftliche Akteure dienen soll.[18] Darüber hinaus hat das Land 2024 eine Kooperationsvereinbarung zur Cybersicherheit mit dem BSI abgeschlossen.[19] Ein IT-Sicherheitsgesetz besteht aktuell nicht.

Zusammen mit den Bundesländern Hamburg, Sachsen-Anhalt und Schleswig-Holstein betreibt Bremen das CERT-Nord, welches organisatorisch und personaladministrativ bei dem Landesdienstleister Dataport AöR angesiedelt ist. Das CERT Nord ist dabei keine Einrichtung von Dataport, sondern „ist den CISOs der Trägerländer unterstellt und berichtet anlassbezogen und regelmäßig über Themen der Informationssicherheit an das zentrale Informationssicherheitsmanagement der Landesverwaltung[en]“ (Schleswig-Holsteinischer Landtag, 2023, S. 38). Laut Rückmeldung von Dataport auf die Umfrage von HIS-HE richten sich die Angebote des CERT Nord „derzeit primär an die Landesverwaltung und in diesem Maße auch an Hochschulen und wissenschaftliche Einrichtungen in öffentlicher Trägerschaft“. Im Antwortschreiben wurde dazu ergänzt, dass die meisten Hochschulen den Service des DFN-CERT nutzen. Ein Informationssicherheitsmanagementsystem nach CISIS12 baut – in Abstimmung mit den anderen Hochschulen – derzeit die Universität Bremen auf (vgl. Bremische Bürgerschaft, 2022, S. 9). Eine Rückmeldung der Senatorin für Umwelt, Klima und Wissenschaft auf die Umfrage von HIS-HE liegt nicht vor.

Eine Überblicksdarstellung der zuständigen Behörden und Anlaufstellen für Cybersicherheit in Bremen enthält Tabelle 5.

[18] Vgl. https://www.inneres.bremen.de/inneres/innere-sicherheit/zentralstelle-cybersicherheit-28457.

[19] Vgl. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/240815_Kooperation_Bremen.html.

Politische und behördliche Zuständigkeiten

▪ Der Senator für Inneres der Freien Hansestadt Bremen, u. a.
  ▪ Ref. 36 Zentralstelle Cybersicherheit
▪ Der Senator für Finanzen der Freien Hansestadt Bremen, u. a.
  ▪ Abt. 4 Zentrales IT-Management, Digitalisierung öffentlicher Dienste
▪ Die Senatorin für Umwelt, Klima und Wissenschaft der Freien Hansestadt Bremen
▪ Landesamt für Verfassungsschutz Bremen
▪ Der Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen

Zentrale Einrichtungen und koordinierende Stellen
▪ Dataport AöR der Länder Hamburg, Schleswig-Holstein, Bremen und Sachsen-Anhalt ▪ CERT Nord für die Verwaltungen der Länder Hamburg, Schleswig-Holstein, Bremen und Sachsen-Anhalt ▪ Zentrale Ansprechstelle Cybercrime (ZAC) des Landeskriminalamtes (LKA) Bremen
Initiativen, Projekte oder Verbünde im Hochschul- und Wissenschaftsbereich
▪ Universität Bremen   ▪ u. a. Team Informationssicherheit

Tabelle 5: Aktivitäten und Initiativen zur Cybersicherheit in Bremen

5.6 Hamburg

Für Hamburg ist insbesondere der Cyberangriff auf die HAW Hamburg bekannt geworden, der Ende 2022 erfolgte. Für die übergreifende Struktur in Richtung Cybersicherheit in der Freien und Hansestadt Hamburg (FHH) ist das Amt für IT und Digitalisierung der Senatskanzlei zuständig, wobei laut Rückmeldung der Behörde für Wissenschaft, Forschung und Gleichstellung (BWFG HH) damit auch die Hochschulen adressiert werden. Nach den Vorgaben der FHH, die ein Rahmen-Sicherheitskonzept sowie ein „Konzept zur Einführung des IT-Grundschutzes in der FHH“ (RaSiKo, 2016) beinhaltet, müssen sich auch die Hochschulen am IT-Grundschutzkonzept des BSI ausrichten. Übergreifend besteht eine Digitalstrategie Hamburg, die der Senat 2020 verabschiedet hat (Senatskanzlei, 2020). Daneben existieren für die einzelnen Behörden der FHH eigene Digitalstrategien – u. a. für die BWFG HH (2024). Ein eigenes Cybersicherheitsgesetz besteht derzeit nicht aber eine Informationssicherheitsleitlinie für die Freie und Hansestadt Hamburg (IS-LL, 2013). Als zentraler Dienstleister nutzt die FHH ebenfalls Dataport, womit das CERT-Nord für Hochschulen zur Verfügung steht – insbesondere durch Unterstützung bei der Identifizierung, Behebung von Schadensfällen sowie Beratung zum Thema Cybersicherheit. Grundsätzlich bearbeiten „[d]ie Hochschulen […] Themen der Informationssicherheit in unterschiedlichen aufbauorganisatorischen und prozessualen Strukturen autonom und in eigener Zuständigkeit“ (Bürgerschaft der Freien und Hansestadt Hamburg, 2023, S. 1). Unabhängig davon plant die BWFG HH – laut Rückmeldung auf die HIS-HE-Umfrage – gemeinsam mit den Hochschulen den Aufbau eines Security Operations Centers (SoC). Zudem wird – laut Antwort des Senats auf die bereits angeführte Kleine Anfrage – eine Vereinbarung der Landeshochschulkonferenz angestrebt, „mit dem Ziel, die IT-Infrastrukturen gemäß den sich verändernden Sicherheitsbedarfen konzeptionell, organisatorisch und technisch neu auszurichten“ (Bürgerschaft der Freien und Hansestadt Hamburg, 2023, S. 1).

Der Landesrechnungshof hat im Jahresbericht 2023 die „IT in den Hochschulen“ näher betrachtet und ist zum Ergebnis gekommen, dass die Hochschulen zum einen „die für die Verwaltungsaufgaben einschlägigen Senatsvorgaben zur Informationssicherheit nicht oder nur teilweise umgesetzt [haben] und […] damit die Sicherheit des IT-Betriebs“ gefährden. Zum anderen nutzen die Hochschule „die Potenziale zur Kooperation bei der IT noch nicht ausreichend“ (Rechnungshof Freie und Hansestadt Hamburg, 2023, S. 224).

Eine Überblicksdarstellung der zuständigen Behörden und Anlaufstellen für Cybersicherheit in Hamburg enthält Tabelle 6.

Politische und behördliche Zuständigkeiten

▪ Senatskanzlei der Freien und Hansestadt Hamburg inkl.
  ▪ Amt für IT und Digitalisierung (ITD) unter der Leitung des Chief Digital Officers (CDO)
▪ Behörde für Inneres und Sport der Freien und Hansestadt Hamburg inkl.
  ▪ Landesamt für Verfassungsschutz
▪ Behörde für Wissenschaft, Forschung und Gleichstellung (BWFG)
▪ Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Zentrale Einrichtungen und koordinierende Stellen
▪ Dataport AöR der Länder Hamburg, Schleswig-Holstein, Bremen und Sachsen-Anhalt ▪ CERT Nord für die Verwaltungen der Länder Hamburg, Schleswig-Holstein, Bremen und Sachsen-Anhalt ▪ Zentrale Ansprechstelle Cybercrime (ZAC) der Polizei Hamburg,
Initiativen, Projekte oder Verbünde im Hochschul- und Wissenschaftsbereich
▪ Berufsbegleitende Weiterbildung zu Cybersicherheit und IT-Sicherheitsmanagement am Zentrum für Weiterbildung der Universität Hamburg

Tabelle 6: Aktivitäten und Initiativen zur Cybersicherheit in Hamburg

5.7 Hessen

Einer der ersten bekannten Cyberangriffe auf eine Hochschule in Deutschland erfolgte 2019 auf die Justus-Liebig-Universität Gießen. Weitere Fälle in Hessen ereigneten sich u. a. 2023 auf das Universitätsklinikum Frankfurt und 2024 auf die Frankfurt University of Applied Sciences (vgl. als Überblick Hessischer Landtag, 2024a). Auch vor diesem Hintergrund hat Hessen bereits 2019 das CyberCompetenceCenter (Hessen3C) im Ministerium des Innern, für Sicherheit und Heimatschutz (HMdI) etabliert. Das Hessen3C dient als zentrale Anlaufstelle in Cybersicherheitsfragen. Laut Homepage steht das Hessen3C der Landesverwaltung, den hessischen Kommunen, Kritischen Infrastrukturen sowie hessischen kleinen und mittleren Unternehmen (KMU) zur Verfügung. Auch wenn Hochschulen und Wissenschaftseinrichtungen nicht explizit als Adressaten genannt werden, können sie dennoch einzelne Dienste nutzen – zum Beispiel das CERT Hessen. Über die Homepage des Hessen3C steht zudem permanent (24/7) eine Notfall-Hotline bei Cyber-Angriffen bzw. IT-Sicherheitsvorfällen zur Verfügung. Mit dem „Hessischen Gesetz zum Schutz der elektronischen Verwaltung“ (HITSiG, 2023) verfügt das Land über ein eigenes IT-Sicherheitsgesetz. Darüber hinaus besteht ein gemeinsamer Rechtsrahmen für Datenschutz und Informationssicherheit mit dem „Hessischen Datenschutz- und Informationssicherheitsgesetz“ (HDSIG, 2018) und 2023 wurde die Hessische Cybersicherheitsstrategie (Hessisches Ministerium des Innern, 2023) veröffentlicht.

Neben dem Hessen3C sind weitere übergreifende Institutionen die Hessische Zentrale für Datenverarbeitung (HZD) sowie der Chief Information Security Officer der Landesverwaltung (CISO) im HMdI angesiedelt, der – laut Kabinettsbeschluss – die übergreifende Verantwortung für Cybersicherheit trägt.[20] In Abstimmung mit den einzelnen Fachressorts ist der CISO maßgeblich bei der Koordinierung und Bearbeitung von landesweiten IT-Sicherheitsvorfälle beteiligt. Auf Seiten des Hessischen Ministeriums für Wissenschaft und Forschung, Kunst und Kultur (HMWK) übernimmt die Stabsstelle Interne Revision, IT-Sicherheit, Datenschutz (S IR) die Aufgaben im Ressort, wobei neben dem Informationssicherheitsbeauftragte und der Stellvertretung auch zwei weitere Referent:innen für IT-Sicherheit zur Verfügung stehen. Laut Rückmeldung auf die Umfrage ist das Thema Cybersicherheit von Hochschulen und wissenschaftlichen Einrichtungen für das HMWK sehr relevant.

Für die Umsetzung wurden insbesondere über den Digitalpakt Hochschule des Landes verschiedene Verbundprojekte gefördert, um beispielsweise die Informations- und IT-Sicherheit der Hochschulen zu fördern (vgl. Hessischer Landtag, 2024b). Laut Rückmeldung des HMWK umfassen die Maßnahmen insbesondere Schulungen des Hochschulpersonals, Awareness-Kampagnen, technische und organisatorische Maßnahmen zur Steigerung der IT-Sicherheit (wie zum Beispiel Ausbau der bestehenden Systeme zur Überwachung („Incident and Event Management“)), organisatorische IT-Sicherheitsmaßnahmen (insb. IT-Notfallkonzepte, Auf- und Ausbau Notfallkommunikation und Notprozesse, Betrieb eines Information Security Management Systems (ISMS)) sowie mittelfristiger Aufbau eines Kompetenzzentrum für IT-Sicherheit, welches – in Abstimmung mit Hessen3C – hochschulübergreifend berät. Unabhängig davon arbeiten die einzelnen Hochschulen jeweils individuell an der weiteren Ertüchtigung der lokalen Infrastruktur.

[20] Zur Unterstützung steht dem CISO das Referat Zentrales Informationssicherheitsmanagement im HMdI zu Verfügung (Abt. VII 3). Vgl. Hessisches Ministerium des Innern und für Sport (2023), S. 14.

Weitere übergreifende Maßnahmen und Angebote für Hochschulen sind die regelmäßig stattfindenden Cybersicherheitstage des CISOs des Landes sowie Cyber Range Trainings, die vom Fraunhofer Institut für Sichere Informationstechnologie (SIT) für die IT-Fachkräfte des Landes Hessen angeboten werden.[21] Die Fraunhofer Gesellschaft betreibt das nationale Forschungszentrum für angewandte Cybersicherheit ATHENE mit Hauptsitz in Darmstadt. Laut eigener Aussage ist ATHENE das größte Forschungszentrum für Cybersicherheit und Privatsphärenschutz in Europa.

Eine Überblicksdarstellung der zuständigen Behörden und Anlaufstellen für Cybersicherheit in Hessen enthält Tabelle 7.

Politische und behördliche Zuständigkeiten

▪ Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz (HMdI), u. a.
  ▪ Abt. VI Informations- und Cybersicherheit inkl. Chief Information Security Officer der hessischen Landesverwaltung (CISO)
▪ Hessisches Ministerium für Digitalisierung und Innovation (HMD) inkl.
  ▪ CIO und Bevollmächtigter für E-Government und Informationstechnologie
▪ Hessisches Ministerium für Wissenschaft und Forschung, Kunst und Kultur (HMWK), u. a.
  ▪ Abt. I Zentralabteilung, Stabsstelle S IR Interne Revision, IT-Sicherheit, Datenschutz
▪ Landesamt für Verfassungsschutz Hessen (LfV)
▪ Hessischer Beauftragter für Datenschutz und Informationsfreiheit (HBDI)

Zentrale Einrichtungen und koordinierende Stellen
▪ Hessische Zentrale für Datenverarbeitung (HZD) ▪ Hessen CyberCompetenceCenter (Hessen3C) ▪ Zentrale Ansprechstelle Cybercrime für die Wirtschaft (ZAC) im Hessischen Landeskriminalamt (LKA) ▪ Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (ZIT) in Frankfurt a.M.
Initiativen, Projekte oder Verbünde im Hochschul- und Wissenschaftsbereich
▪ Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE ▪ Fraunhofer-Institut für Sichere Informationstechnologie (SIT) ▪ Forschungsfeld Information + Intelligence an der Technischen Universität Darmstadt inkl. Cybersecurity

Tabelle 7: Aktivitäten und Initiativen zur Cybersicherheit in Hessen

[21] Vgl. https://www.sit.fraunhofer.de/de/cyberrange/.

5.8 Mecklenburg-Vorpommern

Laut KonBriefing ist Mecklenburg-Vorpommern eines der wenigen Bundesländer, in denen bisher noch keine Cyberangriffe auf Hochschulen bekannt geworden sind. Für die öffentliche Verwaltung des Landes gilt, dass IT-Sicherheitsvorfällen an das CERT M-V gemeldet werden müssen (vgl. Landtag Mecklenburg-Vorpommern, 2023, S. 2). Laut Rückmeldung des CERT M-V auf die Umfrage, ist dieses auch für die Universitäten und Hochschulen zuständig, wobei keine spezifischen Angebote bestehen. Vielmehr stehen über das Portal des CERT M-V verschiedene (übergreifende) Dienste insb. Warn- und Alarmmeldungen, Unterstützung bei Sicherheitsvorfällen sowie Sensibilisierungsveranstaltungen zur Verfügung.

Derzeit existiert kein eigenes IT-Sicherheitsgesetz im Bundesland. Seit 2014 gilt die „Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern (IS-Leitlinie M-V)“, die für die Staatskanzlei und die Ressorts der Landesregierung bindend ist. Eine Rückmeldung des Ministeriums für Wissenschaft, Kultur, Bundes- und Europaangelegenheiten (WKM MV) liegt nicht vor.

Eine Überblicksdarstellung der zuständigen Behörden und Anlaufstellen für Cybersicherheit in Mecklenburg-Vorpommern enthält Tabelle 8.

Politische und behördliche Zuständigkeiten
▪ Ministerium für Inneres, Bau und Digitalisierung Mecklenburg-Vorpommern (IM MV) u. a.   ▪ Abt. 2 Digitale Verwaltung, Ref. ISM Ressortübergreifendes Informationssicherheitsmanagement ▪ Ministerium für Wissenschaft, Kultur, Bundes- und Europaangelegenheiten Mecklenburg-Vorpommern (WKM MV) ▪ Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern ▪ Verfassungsschutz Mecklenburg-Vorpommern
Zentrale Einrichtungen und koordinierende Stellen
▪ Landesamt Zentrum für Digitalisierung MV (ZDMV) ▪ Zentrale Ansprechstelle Cybercrime (ZAC) im Landeskriminalamt Mecklenburg-Vorpommern ▪ DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH ▪ Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität (Cybercrime), Rostock
Initiativen, Projekte oder Verbünde im Hochschul- und Wissenschaftsbereich
▪ Hochschule Stralsund, u. a.   ▪ IT-Sicherheitskonferenz ▪ IT-Initiative Mecklenburg-Vorpommern (IT-Initiative-MV)

Tabelle 8: Aktivitäten und Initiativen zur Cybersicherheit in Mecklenburg-Vorpommern

5.9 Niedersachsen

In Niedersachsen erfolgten 2023 Cyberangriffe auf die Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG) sowie auf die Hochschule Hannover. Auch vor diesem Hintergrund hat die Landesregierung eine Reihe von Initiativen und Gesetzen zu Stärkung der Cybersicherheit verabschiedet. So insbesondere im Jahr 2023 unter dem Titel „Digitale Verwaltung 2030" die Strategie zur digitalen Transformation der Verwaltung des Landes[22] (Niedersächsisches Ministerium für Inneres und Sport (Hrsg.), 2023) und die Cybersicherheitsstrategie Niedersachsen (Niedersächsisches Ministerium für Inneres und Sport (Hrsg.), 2024). Bereits seit 2019 verfügt das Bundesland mit dem Niedersächsischen Gesetz über digitale Verwaltung und Informationssicherheit (NDIG) über einen entsprechenden Rechtsrahmen.

In der Cybersicherheitsstrategie Niedersachsen werden insgesamt 12 Handlungsfelder aufgelistet. Im 1. Feld wird die „Intensivierung der Vernetzung der Cybersicherheitsakteurinnen und -akteure" fokussiert, wofür ein Cybersicherheitszentrum Niedersachsen eingerichtet werden soll. Das Zentrum soll als „Kompetenzknotenpunkt" sowohl den staatlichen Stellen als auch der Wirtschaft, der Wissenschaft und gesellschaftlichen Akteur:innen zur Verfügung stehen (Niedersächsisches Ministerium für Inneres und Sport, 2024, S. 12). Darüber hinaus erscheinen Hochschulen und Forschungseinrichtungen vor allem in den Handlungsfeldern „10. Fachkräfte" sowie „11. Innovative Forschung und Entwicklung". Neben der Bedeutung als Ausbildungsstätte und für den Transfer von wissenschaftlichen Erkenntnissen im Bereich Cybersicherheit, wird in der Strategie explizit darauf verwiesen, dass „Hochschulen zunehmend zu Angriffszielen im IT-Bereich" (ebd., S. 39) werden. Um dieser Entwicklung zu begegnen, hat die Landesregierung Mittel des Programms „zukunft.niedersachsen" der VolkswagenStiftung und des Niedersächsischen Ministeriums für Wissenschaft und Kultur (MWK NI) zur Verfügung gestellt. So wird mit einem Fördervolumen von 10 Millionen Euro das Verbundprojekt „Sicherung der Resilienz" finanziert. In dieses Projekt, das durch den Landesarbeitskreis für Informationstechnik/Hochschulrechenzentren (LANIT) ausgearbeitet wurde, sind die 20 (staatlichen) niedersächsischen Hochschulen eingebunden und es ist Teil der zentralen Dachinitiative Hochschule.digital Niedersachsen.[23] Diese wurde durch die Landeshochschulkonferenz Niedersachsen (LHK NI) gemeinsam mit dem MWK NI und der VolkswagenStiftung ins Leben gerufen und hat im Juni 2024 eine Gesamtstrategie 2030 verabschiedet (vgl. LandesHochschulKonferenz Niedersachsen, 2024). Diese setzt die „Gesamtrahmung über alle Handlungsfelder für die Weiterentwicklung der Digitalität der Hochschulen in Niedersachsen" (ebd., S. 9), wobei das genannte Verbundprojekt zur „Sicherung der Resilienz" der „erste Schritt zur kooperativen Prävention gegen Cyberangriffe" (ebd., S. 13) ist. Parallel unterstützt das MWK NI seit 2020 eine Kooperation zwischen dem CISPA – Helmholtz-Zentrum für Informationssicherheit aus Saarbrücken und der Leibniz Universität Hannover (LUH). Um die Forschung in den Bereichen Cybersicherheit und Datenschutz zu stärken, fördert das Land mit rund 10 Millionen Euro den Aufbau einer unselbständigen Betriebsstätte des CISPA in Hannover.[24] Um die Kooperation zwischen CISPA und LUH auf- und auszubauen, wurde ein Kooperationsgremium mit Beteiligung des niedersächsischen Wissenschafts- und des Wirtschaftsministeriums eingerichtet.

[22] Zur Digitalisierungsstrategie 2030 vgl. insb. https://niedersachsen.online/digitalstrategie-2030/.

[23] https://hochschuledigital-niedersachsen.de/home/cyberresilienz/.

[24] Vgl. Pressemitteilung des MWK vom 20.10.2020 https://www.mwk.niedersachsen.de/startseite/aktuelles/presseinformationen/neue-forschungseinrichtung-zur-cybersicherheit-in-hannover-193729.html.

Laut Rückmeldung des MWK NI auf die HIS-HE-Umfrage ist das Thema Cyber-Resilienz sehr relevant für das Ministerium. Das Referat 44 Digitalisierung, E-Government, IuK, Informationssicherheit der Zentralabteilung unterstützt die jeweiligen Fachreferate. Die Dienste des N-Certs (z. B. Warn- und Informationsdienst WID) stehen generell auch den Hochschulen zur Verfügung. Im Antwortschreiben auf die Umfrage verweist das niedersächsische CERT aber darauf, dass bisher nur wenige Anfragen zu den Diensten und keine Beratungsanfragen vorliegen. Die Hochschulen nutzen vielmehr die Beratungsangebote des DFN-CERT.

Eine Überblicksdarstellung der zuständigen Behörden und Anlaufstellen für Cybersicherheit in Niedersachsen enthält Tabelle 9.

Politische und behördliche Zuständigkeiten

▪ Niedersächsisches Ministerium für Inneres und Sport (MI), u. a.
  ▪ Stabsstelle CIO und IT-Bevollmächtigter der Landesregierung
  ▪ N-Cert im Ref. IT2 – Informations- und Cybersicherheit
  ▪ Verfassungsschutz
▪ Niedersächsisches Ministerium für Wissenschaft und Kultur (MWK), u. a.
  ▪ Abt. 4 Zentrale Dienste, Ref. 44 Digitalisierung, E-Government, IuK, Informationssicherheit
▪ Die Landesbeauftragte für den Datenschutz Niedersachsen (LfD)
▪ Landesamt für Verfassungsschutz

Zentrale Einrichtungen und koordinierende Stellen
▪ IT.Niedersachsen (IT.N) inkl.   ▪ Cyber Defence Operations Center (CDOC) ▪ Zentrale Ansprechstelle Cybercrime (ZAC) im Landeskriminalamt Niedersachsen
Initiativen, Projekte oder Verbünde im Hochschul- und Wissenschaftsbereich
▪ Landesarbeitskreis Niedersachsen für Informationstechnik/ Hochschulrechenzentren (LANIT) ▪ Hochschule.Digital Niedersachsen (HDN) ▪ Niedersachsen.Digital (Bereich Cybersicherheit)

Tabelle 9: Aktivitäten und Initiativen zur Cybersicherheit in Niedersachsen

5.10 Nordrhein-Westfalen

Seit 2020 erfolgten mehrere Cyberangriffe auf Hochschulen in Nordrhein-Westfalen – allen voran auf die Ruhr-Universität Bochum, die Universität zu Köln, die Bergische Universität Wuppertal, die Universität Duisburg-Essen und die Heinrich-Heine-Universität Düsseldorf sowie die Fachhochschule Münster, die Hochschule Ruhr West und die Europäische Fachhochschule Rhein/Erft. In der 2021 verabschiedeten Cybersicherheitsstrategie des Landes werden drei Handlungsfelder und sechs strategische Ziele formuliert, wobei „Die Landesregierung […] es sich zum Ziel gemacht [hat], den Schutz des Wissenschaftsstandorts Nordrhein-Westfalen aktiv zu stärken und die Forschung im Land weiter zu fördern." (Landesregierung Nordrhein-Westfalen, 2021, S. 37) Ein eigenes IT-Sicherheitsgesetz besteht derzeit nicht, jedoch eine Reihe von Landesvorschriften sowie das Gesetz zur Förderung der elektronischen Verwaltung in Nordrhein-Westfalen (EGovG NRW) aus dem Jahr 2016.

Vor diesem Hintergrund hat das Ministerium für Kultur und Wissenschaft (MKW NRW) eine ganze Reihe von Maßnahmen und Förderinstrumenten etabliert, wobei grundsätzlich ein kooperativer Ansatz verfolgt wird Zentrale Elemente sind die Vereinbarung zur Informationssicherheit (VZI), die zum 1. Juli 2023 in Kraft getreten ist, sowie die Vereinbarung zur Cybersicherheit (VZC), die seit dem 1. Januar 2024 gilt und im Kern eine Erweiterung und Konkretisierung der VZI ist. Mit beiden Vereinbarungen wird das Ziel verfolgt, Mindeststandards auf Basis des IT-Grundschutzes des BSI zu etablieren. Die Hochschulen und Einrichtungen erhalten im Rahmen der VZI dafür u. a. eine dauerhafte Finanzierung über rund 2,7 Mio. Euro pro Jahr für die Einrichtung von entsprechenden Stellen (Informationssicherheitsbeauftragte (ISB) bzw. Chief Information Security Officer (CISO)) gemäß BSI-Standard 200-2. Mit Unterzeichnung der VZC wurden dauerhaft weitere rd. 4,7 Mio. Euro pro Jahr für Cybersicherheit zur Verfügung gestellt. Für den Zeitraum 2024 bis 2027 stehen darüber hinaus befristete Mittel i. H. v. rund 30 Mio. Euro zur Verfügung, um insbesondere die Absicherung der Rechenzentren und der Verwaltungs-IT zu stärken. Die beiden Vereinbarungen wurden – im Einvernehmen mit der Digitalen Hochschule NRW (DH.NRW) – zwischen dem MKW NRW und den staatlichen Hochschulen sowie dem Hochschulbibliothekszentrum NRW (hbz) getroffen. Während mit Hilfe dieser Vereinbarungen Mindeststandards für die Informations- und Cybersicherheit als Basis der Kooperationen gesetzt werden, fördert das Land parallel eine Reihe von Einzelvorhaben sowie übergreifende Strukturen. Dazu zählen u. a. das Netzwerk Informationssicherheit.nrw (NISHS.nrw), ein modulares Online-Selbstlernangebot (Secaware.nrw), der Aufbau eines IT-Basisdienstes zur Bereitstellung eines kooperativen Betriebsmodells für eine hochschulübergreifende Datensicherung (Datensicherung.nrw), die Etablierung einer Cloud-Technologie als Anti-Spam-Cluster.nrw (Security.NRW) der Hochschulen sowie der Aufbau eines Security Operation Centers (SOC-Hochschulen.nrw)[25] der Hochschulen für angewandte Wissenschaften, der Kunst- und Musikhochschulen und der Deutschen Sporthochschule in Köln. Im Jahr 2023 wurde den Hochschulen zusätzlich ein Sondervermögen zur Krisenbewältigung für eine Verbesserung der Resilienz im Bereich der Cybersicherheit in Höhe von 41,2 Mio. Euro zur Verfügung gestellt (Landtag Nordrhein-Westfalen, 2023, S. 2).

Auch im Bereich von Forschung und Weiterbildung arbeiten die Hochschulen zusammen und bieten u. a. den Cyber Campus Nordrhein-Westfalen an, der seit dem Wintersemester 2020/2021 Studiengänge zu den

[25] Vgl. die Übersicht des MKW NRW https://www.mkw.nrw/themen/wissenschaft/wissenschaftspolitik/cybersicherheit.

Themen Cybersicherheit, Cyber-Kriminalität und Digitale Transformation anbietet. Das Landeskriminalamt unterhält das Cybercrime Kompetenzzentrum, welches sich – neben Unternehmen und Behörden – auch dezidiert an Institutionen der Forschung und Wissenschaft richtet. Das CERT.NRW unterstützt Behörden und Einrichtungen, die am Landesverwaltungsnetz angeschlossen sind. Die Hochschulen des Landes gehören damit nicht dazu. Mit dem Aufbau des SOC-Hochschulen.nrw wird hierfür aber ein eigenes Zentrum etabliert.[26] Weitere Unterstützungsmöglichkeiten bietet die Koordinierungsstelle Cybersicherheit des Innenministeriums.

Laut Rückmeldung des MKW NRW auf die Befragung durch HIS-HE ist übergreifendes Ziel der Behörde, durch Förderung der Kooperation unter den Hochschulen im Bereich IT-Dienste und -Serviceerbringung die Dienste zu professionalisieren und damit insgesamt die Informationssicherheit zu stärken. Neben den genannten Projekten und Förderlinien hat das MKW NRW eine Referent:innenstelle für den Bereich „Cybersicherheit an den Hochschulen“ im Referat 214 etabliert. In die Koordinierung ist zudem die Digitale Hochschule NRW (DH.NRW) als Kooperationsplattform eingebunden.

Eine Überblicksdarstellung der zuständigen Behörden und Anlaufstellen für Cybersicherheit in Nordrhein-Westfalen enthält Tabelle 10.

[26] Vgl. Pressemitteilung vom 27.06.2024 https://www.land.nrw/pressemitteilung/fuer-mehr-cybersicherheit-hochschulen-starten-gemeinsames-security-operation.

Politische und behördliche Zuständigkeiten

▪ Ministerium des Innern des Landes Nordrhein-Westfalen (IM NRW), u. a.
  ▪ Abt. 7 Digitalisierung IM und im Geschäftsbereich, Ref. 73 Koordinierungsstelle für Cybersicherheit NRW
  ▪ Verfassungsschutz NRW
▪ Ministerium für Heimat, Kommunales, Bau und Digitalisierung des Landes Nordrhein-Westfalen (MHKBD), u. a.
  ▪ Chief Information Security Officer des Landes Nordrhein-Westfalen (CISO NRW)
  ▪ Abt. 2 Digitalisierung der Landesverwaltung, Ref. 224 Informationssicherheit in der Landesverwaltung
▪ Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen (MKW NRW), u. a.
  ▪ Abt. II Hochschulen II, Ref 214 Informationsinfrastrukturen, Informationssicherheit, Digitalisierung in Studium und Lehre
▪ Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW)

Zentrale Einrichtungen und koordinierende Stellen
▪ Landesbetrieb Information und Technik Nordrhein-Westfalen (IT.NRW), u. a.   ▪ CERT NRW ▪ Cybercrime-Kompetenzzentrum beim LKA NRW ▪ Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW) bei der Generalstaatsanwaltschaft Köln ▪ Koordinierungsstelle Cybersicherheit NRW
Initiativen, Projekte oder Verbünde im Hochschul- und Wissenschaftsbereich
▪ Digitale Hochschule NRW (DH.NRW), u. a.   ▪ Anti-Spam-Cluster.NRW (Security.NRW) ▪ Netzwerk Informationssicherheit der Hochschulen in NRW (NISHS.NRW) ▪ SecAware.NRW ▪ Datensicherung.nrw – Gemeinsam für mehr Datensicherheit in NRW ▪ Cyber Campus NRW ▪ Horst-Görtz-Institut für IT-Sicherheit (HGI) an der Ruhr-Universität Bochum ▪ Institut für Internet-Sicherheit (if(is)) an der Westfälischen Hochschule

Tabelle 10: Aktivitäten und Initiativen zur Cybersicherheit in Nordrhein-Westfalen

5.11 Rheinland-Pfalz

In Rheinland-Pfalz ist laut KonBriefing bisher allein der Cyberangriff auf die Hochschule Kaiserslautern im Jahr 2023 bekannt geworden. Im Mai 2020 erfolgten aber eine Reihe von Cyberangriffen auf europäische Hochleistungsrechner, unter denen auch drei in Rheinland-Pfalz betroffen waren. Laut Information des Verfassungsschutzes waren dies das Hochleistungsrechencluster der Technischen Universität Kaiserslautern[27] sowie die beiden Hochleistungsrechner der Johannes Gutenberg-Universität Mainz (Landtag Rheinland-Pfalz, 2022a, S. 5). Die betroffenen Einrichtungen wurden im Rahmen der Sicherheitspartnerschaft Rheinland-Pfalz informiert, durch die der Verfassungsschutz zu Cyberspionage und -sabotage informiert und berät. Hochschulen und Wissenschaftseinrichtungen sind hierbei nur bedingt Adressat, da die Sicherheitspartnerschaft vor allem zwischen Landesregierung und Wirtschaftsverbänden und -kammern in Rheinland-Pfalz besteht. Die Landesregierung betreibt darüber hinaus das CERT-rlp, welches im Landesbetrieb Daten und Information (LDI) angesiedelt ist. Laut Rückmeldung des CERT-rlp ist dieses formal nicht für die Hochschulen des Landes zuständig.

Nach dem Landesgesetz zur Förderung der elektronischen Verwaltung in Rheinland-Pfalz (E-Government-Gesetz Rheinland-Pfalz (EGovGRP)) (2020), § 17, Abs. 3) müssen relevante IT-Sicherheitsvorfälle bei den Landesbehörden an das CERT-rlp gemeldet werden. Das CERT-rlp übernimmt die Koordinierung von Gegenmaßnahmen und unterstützt die Landesbehörden durch Empfehlungen und Hilfsangebote (Landtag Rheinland-Pfalz, 2022b, S. 9). Für Unternehmen bietet der Verfassungsschutz Rheinland-Pfalz das Portal Cyberschutz Rheinland-Pfalz, wobei die Informationen zu tagesaktuellen Bedrohungsindikatoren und Sicherheitshinweise auch Wissenschaftseinrichtungen zur Verfügung stehen.

Bereits 2017 wurde die Rechenzentrumsallianz Rheinland-Pfalz (RARP) etabliert, um mit übergreifenden Maßnahmen und Diensten (u. a. Aufbau zentraler Infrastrukturen und Dienste), die Cybersicherheit der Hochschulen zu stärken. Alle Hochschulen des Landes sind Mitglied in der RARP, wobei diese keine eigenen Dienste oder Infrastruktur anbietet. Die RARP dient vielmehr zur Abstimmung und Koordination zwischen den Hochschulen. Ein weiteres Element zur übergreifenden Abstimmung wurde 2023 mit dem Hochschulforum Rheinland-Pfalz gegründet.[28] Dieses dient vor allem als Dialogform zwischen den Hochschulen und dem Ministerium für Wissenschaft und Gesundheit (MWG RP) – auch in Fragen von Cybersicherheit und IT-Informationssicherheit. Eine Rückmeldung des Ministeriums auf die HIS-HE-Anfrage liegt nicht vor.

Eine Überblicksdarstellung der zuständigen Behörden und Anlaufstellen für Cybersicherheit in Rheinland-Pfalz enthält Tabelle 11.

[27] Seit dem 1.1.2023 Rheinland-Pfälzische Technische Universität Kaiserslautern-Landau.

[28] Vgl. https://mwg.rlp.de/service/pressemitteilungen/detail/wissenschaftsminister-clemens-hoch-erfolgreicher-start-des-hochschulforums-rheinland-pfalz.

Politische und behördliche Zuständigkeiten

▪ Ministerium für Arbeit, Soziales, Transformation und Digitalisierung (MASTD), u. a.
  ▪ Abt. 63 Digitalisierung, Ref. 632 Ressortübergreifende Informationssicherheit
▪ Ministerium des Innern und für Sport (MDI), u. a.
  ▪ Verfassungsschutz
▪ Ministerium für Wissenschaft und Gesundheit (MWG)
▪ Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI)

Zentrale Einrichtungen und koordinierende Stellen
▪ Zentrale Ansprechstelle Cybercrime (ZAC) beim Landeskriminalamt (LKA) ▪ Landesbetrieb Daten und Information (LDI), u. a.   ▪ CERT-rlp ▪ Landeszentralstelle Cybercrime (LZC) bei der Generalstaatsanwaltschaft Koblenz
Initiativen, Projekte oder Verbünde im Hochschul- und Wissenschaftsbereich
▪ Rechenzentrumsallianz Rheinland-Pfalz (RARP)

Tabelle 11: Aktivitäten und Initiativen zur Cybersicherheit in Rheinland-Pfalz

5.12 Saarland

Im Saarland ist laut KonBriefing bisher noch kein Cyberangriff erfolgt. An der Universität des Saarlandes hat sich aber bereits 2011 mit dem Center for IT Security, Privacy and Accountability (CISPA) ein eigener Forschungsschwerpunkt zum Thema etabliert. Das CISPA wurde 2019 in die Helmholtz-Gemeinschaft aufgenommen und ist heute eine „nationale Großforschungseinrichtung“ im Bereich Informationssicherheit (CISPA 2025). Neben der Grundlagenforschung ist das CISPA auch auf dem Gebiet der anwendungsorientierten Forschung in Cybersicherheit aktiv.

In Saarland gilt derzeit das „Gesetz zur Abwehr von Gefahren für die Daten in der Informations- und Kommunikationsinfrastruktur des Landes – Informationssicherheitsgesetz Saarland“ (IT-SiG SL, 2019), welches vorrangig die verarbeiteten Informationen der Behörden adressiert. Damit verbunden sind aber auch „sonstige der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts“ (ebd., § 1). Hochschulen unterliegen bisher keiner Meldepflicht für Cyberangriffe. Laut Rückmeldung des Ministeriums der Finanzen und für Wissenschaft (MFW SL) hat das Land der Universität des Saarlandes und der Hochschule für Technik und Wirtschaft bereits finanzielle Unterstützungsleistungen für infrastrukturelle Maßnahmen (z. B. Aufbau und Unterhaltung von Software- und Hardware-Netzwerken) gewährt. Laut Rückmeldung des CISO des Landes beschränkt sich die Zuständigkeit des Landes-CERT auf den Bereich der Landesverwaltung.

Eine Überblicksdarstellung der zuständigen Behörden und Anlaufstellen für Cybersicherheit im Saarland enthält Tabelle 12.

Politische und behördliche Zuständigkeiten
▪ Ministerium für Wirtschaft, Innovation, Digitales und Energie (MWIDE), u. a. ▪ Abt. D Digitalisierung in Wirtschaft und Verwaltung, Ref. D/6 Informationssicherheits- und Datenschutzmanagement, IT-Recht ▪ Ministerium für Inneres, Bauen und Sport (MIBS), u. a. ▪ Abt. V Verfassungsschutz ▪ Ministerium der Finanzen und für Wissenschaft (MFW) ▪ Unabhängiges Datenschutzzentrum Saarland
Zentrale Einrichtungen und koordinierende Stellen
▪ Landesamt für IT-Dienstleistungen (IT-DLZ), u. a. ▪ CERT-Saarland[29] ▪ Zentrale Ansprechstelle Cybercrime für die Wirtschaft (ZAC) ▪ Dezernat Cybercrime der Staatsanwaltschaft Saarbrücken
Initiativen, Projekte oder Verbünde im Hochschul- und Wissenschaftsbereich
▪ CISPA – Helmholtz-Zentrum für Informationssicherheit, Saarbrücken ▪ Netzwerkstelle Digitalisierung (DiNet), u. a. ▪ Themenfeld Cybersicherheit ▪ CYBR360 – Initiative zur Stärkung der Cybersicherheit inkl. ▪ „Digitaler Rettungskette“

Tabelle 12: Aktivitäten und Initiativen zur Cybersicherheit im Saarland

[29] Das CERT-Saarland wird in Zusammenarbeit mit dem Land Rheinland-Pfalz betrieben. Die Kopfstelle, der sog. SPOC, befindet sich im IT-DLZ. https://www.saarland.de/mwide/DE/portale/digitalisierung/informationssicherheit.

5.13 Sachsen

Hochschulen in Sachsen waren seit 2021 mehrfach von Cyberangriffen betroffen – beispielsweise die Universität Leipzig 2021, die Westsächsische Hochschule Zwickau 2022 und die TU Bergakademie Freiberg 2023 (vgl. Sächsischer Landtag, 2023). Bereits seit 2019 gibt es das Sächsische Informationssicherheitsgesetz (SächsISichG, 2019), das unter anderem die Befugnisse des SAX.CERT regelt (§ 6 SächsISichG) und ein zentrales Meldesystem vorsieht (§ 15 SächsISichG). Das SächsISichG sieht auch vor, dass jede Hochschule des Freistaates eine:n Beauftragte:n sowie eine:n Vertreter:in bestimmt (§ 7 SächsISichG). Das SAX.CERT ist die zentrale Stelle für Informationssicherheit des Landes und bietet seine Dienstleistungen auch den Hochschulen an.

Die im SächsISichG festgelegte Meldepflicht bei Cyberangriffen gilt für staatliche und nicht-staatliche Stellen, für die das SAX.CERT online ein Meldeformular zur Verfügung stellt.[30] Damit besteht eine gesetzliche Meldepflicht für schwerwiegende Sicherheitsvorfälle (§ 16 und § 17 SächsISichG). Hochschulen und Wissenschaftseinrichtungen waren hier aber bisher nur bedingt eingebunden. Das Sächsische Ministerium für Wissenschaft und Kultur (SMWK) etabliert derzeit ein eigenes Meldeverfahren, das über die Stabsstelle Informationssicherheit des SMWK koordiniert wird. Hintergrund der Bemühungen ist neben dem SächsISichG die Strategie zur digitalen Transformation im Hochschulbereich (Landesrektorenkonferenz Sachsen, 2023), die das Ziel verfolgt, die zuständigen Stellen stärker zu vernetzen und Formen der Kooperation zu etablieren. Die ersten Verbundprojekte adressieren jedoch nicht Cybersicherheitsfragen.[31] In dem Sinne ergeben sich zwar die Vorgaben zur Informationssicherheit aus dem SächsISichG, die Verantwortung und Umsetzung liegt aber allein bei der Hochschulleitung. Neben den zentralen Angeboten des SAX.CERT (z. B. Warnmeldungen, Vulnerability Advisory Service, Identity Leak Checker), gibt es derzeit nur vereinzelt übergreifende Angebote (z. B. Nutzung Honeysen zur Erkennung von sicherheitsrelevanten Fehlkonfigurationen im Netzwerk; Beratung durch das CERT der Technischen Universität Dresden, TUD CERT).

Eine Überblicksdarstellung der zuständigen Behörden und Anlaufstellen für Cybersicherheit in Sachsen enthält Tabelle 13.

[30] Vgl. IT-Vorfall, SAX-CERT Meldeformular unter https://fs.egov.sachsen.de/formserv/findform?shortname=SID_saxcert&formtecid_2&areashortname=SMJus_SID.

[31] Eine Übersicht über Maßnahmen zur Umsetzung der Digitalisierungsstrategie in der Dimension Bildung, Wissenschaft und Forschung findet sich unter https://www.digitales.sachsen.de/massnahmenkatalog-4614.html.

Politische und behördliche Zuständigkeiten

▪ Sächsische Staatskanzlei (SK), u. a.
  ▪ Abt. 4 Digitalisierung der Verwaltung, Ref. 45 Informations- und Cybersicherheit, Kritische Infrastrukturen
▪ Sächsisches Staatsministerium für Wissenschaft, Kultur und Tourismus (SMWK), u. a.
  ▪ Stabsstelle Informationssicherheit
▪ Landesamt für Verfassungsschutz
▪ Sächsische Datenschutz- und Transparenzbeauftragte

Zentrale Einrichtungen und koordinierende Stellen
▪ Staatsbetrieb Sächsische Informatik Dienste (SID) inkl.   ▪ SAX.CERT ▪ Zentrale Ansprechstelle Cybercrime (ZAC) für Unternehmen, Behörden und Verbände des Freistaates Sachsen ▪ Cybercrime Competence Center Sachsen (SN4C) der Polizei Sachsen ▪ Zentralstelle Cybercrime Sachsen (ZCS) bei der Generalstaatsanwaltschaft Dresden
Initiativen, Projekte oder Verbünde im Hochschul- und Wissenschaftsbereich
▪ CERT der TU Dresden (TUD CERT)

Tabelle 13: Aktivitäten und Initiativen zur Cybersicherheit in Sachsen

5.14 Sachsen-Anhalt

In Sachsen-Anhalt sind bisher zwei Fälle von Cyberangriffen auf Hochschulen bekannt – 2022 auf die Hochschule Anhalt und 2023 auf die Hochschule Harz. Im Koalitionsvertrag der Landesregierung von 2021 wurde allgemein bestimmt, den Bereich der IT-Sicherheit voranzutreiben (Koalitionsvertrag 2021-2026, 2021, S. 32). Zwei zentrale Aspekte sind die Etablierung einer „Sicherheit für alle digitalen Anwendungen (Cyberallianz zwischen Hochschulen, Verbänden, Wirtschaft und Gesellschaft)" (ebd., S. 26) und die Verabschiedung eines IT-Sicherheitsgesetzes (ebd., S.104). Im Rahmen der Digitalen Agenda des Landes wird zudem das Forschungsprojekt „CyberSecurity Verbund Sachsen-Anhalt" (CSLSA) gefördert. Ziel des Verbundes ist es, die Entwicklung und Integration von IT-Sicherheitslösungen für kleine und mittlere Unternehmen sowie öffentliche Einrichtungen in Sachsen-Anhalt zu unterstützen. Ein IT-Sicherheitsgesetz wurde bislang nicht verabschiedet. In der 2023 verabschiedeten Digitalisierungsstrategie des Landes (vgl. Ministerium für Infrastruktur und Digitales, 2023) ist IT-Sicherheit ein eigenes Themenfeld mit entsprechenden Zielsetzungen. Konkrete Projekte und Maßnahmen für die Hochschulen finden sich jedoch nur vereinzelt. Um Hochschulen besser auf Cyber-Attacken vorzubereiten, wurden aus dem Corona-Sondervermögens Gelder zur Verbesserung der Resilienz durch Digitalisierung zur Verfügung gestellt.[32] Zudem besteht die IT-Kommission der Hochschulen des Landes Sachsen-Anhalt (IT-KOM LSA), die eine Beratungs- und Koordinierungsfunktion u. a. hinsichtlich der Herausforderungen für eine übergreifende IT-Infrastruktur übernimmt. Die IT-KOM LSA ist eine Kommission der Landesrektorenkonferenz der Hochschulen des Landes Sachsen-Anhalt, der neben Hochschulen auch außeruniversitäre Forschungseinrichtungen angehören. Die IT-KOM LSA hat gemeinsam mit der Hochschule Anhalt Ende 2024 zu einem ersten Landeshochschulkongress zum Thema „Cyber-Security – Herausforderungen für die Hochschulen im Land Sachsen-Anhalt" eingeladen.[33]

Laut einer Antwort der Landesregierung auf eine Kleine Anfrage über die „Digitale Infrastruktur an unseren Hochschulen" (Landtag von Sachsen-Anhalt, 2022) liegt eine zentrale Herausforderung in der Betreuung der Systeme durch Fachpersonal: „Bereits die bestehenden Stellen können derzeit nicht besetzt werden und für die gestiegenen Anforderungen an die IT-Betreuung und -Absicherung wären zusätzliche Stellen (z. B. IT-Sicherheitsbeauftragter oder HIS-Support bzw. Absicherung von Vertretungen) unbedingt erforderlich." (ebd., S. 5).

Wie die Bundesländer Hamburg, Schleswig-Holstein und Bremen nutzt Sachsen-Anhalt die Dienste von Dataport, was u. a. die Leistungen des CERT-Nord einschließt. Laut Rückmeldung von CERT-Nord richten sich das Angebot primär an die Landesverwaltung und in diesem „Maße auch an Hochschulen und wissenschaftliche Einrichtungen in öffentlicher Trägerschaft". Eine Rückmeldung des Ministeriums für Wissenschaft, Energie, Klimaschutz und Umwelt (MWU ST) auf die Umfrage liegt nicht vor.

Eine Überblicksdarstellung der zuständigen Behörden und Anlaufstellen für Cybersicherheit in Sachsen-Anhalt enthält Tabelle 14.

[32] Ziel der Förderung i. H. v. 15 Mio. Euro ist der Aufbau einer Hochschul-Cloud, um „künftig auch IT-Dienste zwischen den Hochschulen [verschieben zu können], um den möglichen Ausfall eines einzelnen Rechenzentrums infolge eines Cyber-Angriffes zu kompensieren". https://mwu.sachsen-anhalt.de/artikel-detail/corona-sondervermoegen-15-millionen-euro-fuer-aufbau-einer-modernen-hochschul-cloud.

[33] Vgl. https://www.hs-anhalt.de/hochschule-anhalt/aktuelles/landeshochschulkongress-cyber-security.html.

Politische und behördliche Zuständigkeiten

▪ Ministerium für Infrastruktur und Digitales Sachsen-Anhalt (MID), u. a.
  ▪ Chief Information Security Officer (CISO)
▪ Ministerium für Inneres und Sport (MI), u. a.
  ▪ Verfassungsschutz
▪ Ministerium für Wissenschaft, Energie, Klimaschutz und Umwelt (MWU), u. a.
  ▪ Informationssicherheitsbeauftragter der MWU
▪ Landesbeauftragte für den Datenschutz Sachsen-Anhalt

Zentrale Einrichtungen und koordinierende Stellen
▪ Dataport AöR der Länder Hamburg, Schleswig-Holstein, Bremen und Sachsen-Anhalt ▪ CERT Nord für die Verwaltungen der Länder Hamburg, Schleswig-Holstein, Bremen und Sachsen-Anhalt ▪ Zentrale Ansprechstelle Cybercrime (ZAC) im Landeskriminalamt (LKA) Sachsen-Anhalt ▪ Cybercrime Competence Center (4C) im Landeskriminalamt (LKA) Sachsen-Anhalt
Initiativen, Projekte oder Verbünde im Hochschul- und Wissenschaftsbereich
▪ Forschungsprojekt „CyberSecurity Verbund Sachsen-Anhalt“ (CSLSA) ▪ IT-Kommission der Hochschulen des Landes Sachsen-Anhalt (IT-KOM LSA)

Tabelle 14: Aktivitäten und Initiativen zur Cybersicherheit in Sachsen-Anhalt

5.15 Schleswig-Holstein

Cyberangriffe auf Hochschulen in Schleswig-Holstein gab es unter anderem auf die Christian-Albrechts-Universität zu Kiel im Jahr 2019 sowie auf die Fachhochschule Westküste im Jahr 2023. Ein weiterer Angriff erfolgte beispielsweise 2023 auf das Leibniz-Informationszentrum Wirtschaft (ZBW) in Kiel (vgl. Tunnat, 2023). Auf gesetzlicher Ebene bestehen keine Meldepflichten über IT-Sicherheitsvorfällen für Hochschulen. Laut „Bericht der Landesregierung über die Cybersicherheit unserer Infrastruktur“ sind „entsprechende Meldungen betroffener Hochschulen […] allerdings übliche Praxis“ (Schleswig-Holsteinischer Landtag, 2023, S. 49). Zur Verbesserung der IT-Sicherheit, wurden den Hochschulen des Landes gemeinsam mit der Arbeitsgemeinschaft ITSH-edu Sondermittel in Höhe von 3,4 Mio. Euro aus dem Entwicklungsbudgets im Rahmen des „Zukunftsvertrags Studium und Lehre stärken“ (ZSL) zur Verfügung gestellt. Vorgesehen sind sieben Einzelprojekte zur Verbesserung der IT-Sicherheit an den Hochschulen. Die Maßnahmen zielen auf Prävention und Reaktion in einem möglichen Krisenszenario, wobei eine hochschulübergreifende Zusammenarbeit vorgesehen ist. Laut Bericht der Landesregierung ist eine Verstetigung der Projektmittel geplant, „jedoch vor dem Hintergrund der aktuellen Haushaltslage noch nicht gesichert“ (Schleswig-Holsteinischer Landtag, 2023, S. 50).

Neben den Hochschulen des Landes sind wissenschaftliche Einrichtungen wie das GEOMAR Helmholtz-Zentrum für Ozeanforschung oder das Leibniz-Informationszentrum Wirtschaft (ZBW) in die Arbeitsgemeinschaft ITSH-edu eingebunden. Die ITSH-edu hat 2010 eine gemeinsame „IT-Sicherheitspolitik der teilnehmenden Hochschulen und Forschungseinrichtungen in Schleswig-Holstein“ (ITSH-edu, 2010) veröffentlicht. Die genannte Förderung der IT-Sicherheit durch das Land richtet sich aber allein an die Hochschulen. Generell gilt, dass die Hochschulen „ihre Aufgaben der Informations- und Cybersicherheit im Sinne der Hochschulautonomie eigenverantwortlich [wahrnehmen].“ (Schleswig-Holsteinischer Landtag, 2023, S. 49)

Auch Schleswig-Holstein nutzt ebenfalls die Dienste von Dataport und damit die Leistungen des CERT-Nord. Das Angebot richtet sich primär an die Landesverwaltung und in diesem „Maße auch an Hochschulen und wissenschaftliche Einrichtungen in öffentlicher Trägerschaft“. Eine Rückmeldung des Ministeriums für Allgemeine und Berufliche Bildung, Wissenschaft, Forschung und Kultur (MBWFK SH) zur Umfrage liegt nicht vor.

Eine Überblicksdarstellung der zuständigen Behörden und Anlaufstellen für Cybersicherheit in Schleswig-Holstein enthält Tabelle 15.

Politische und behördliche Zuständigkeiten

▪ Staatskanzlei Schleswig-Holstein (StK SH), u. a.
  ▪ Abt. 3 Digitalisierung und Zentrales IT-Management der Landesregierung, StK 37 Management des Digitalen Arbeitsplatzes, ressortübergr. Informationssicherheit und IT-Notfallversorgung
▪ Ministerium für Inneres, Kommunales, Wohnen und Sport (MIKWS SH), u. a.
  ▪ Abt. 7 Verfassungsschutz
▪ Ministerium für Allgemeine und Berufliche Bildung, Wissenschaft, Forschung und Kultur (MBWK SH)
▪ Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Zentrale Einrichtungen und koordinierende Stellen
▪ Dataport AöR der Länder Hamburg, Schleswig-Holstein, Bremen und Sachsen-Anhalt ▪ CERT Nord für die Verwaltungen der Länder Hamburg, Schleswig-Holstein, Bremen und Sachsen-Anhalt ▪ Zentrale Ansprechstelle Cybercrime (ZAC) für Unternehmen und Behörden beim Landeskriminalamt (LKA) Schleswig-Holstein
Initiativen, Projekte oder Verbünde im Hochschul- und Wissenschaftsbereich
▪ Arbeitsgemeinschaft der IT-Verantwortlichen der Hochschulen und wissenschaftlichen Einrichtungen in Schleswig-Holstein (ITSH-edu) ▪ Digitale Wirtschaft Schleswig-Holstein (DiWiSH)

Tabelle 15: Aktivitäten und Initiativen zur Cybersicherheit in Schleswig-Holstein

5.16 Thüringen

Laut KonBriefing erfolgte bisher kein Cyberangriff auf Hochschulen in Thüringen. Laut Antwort des Thüringer Ministeriums für Bildung, Wissenschaft und Kultur (TMBWK) konnten aber allein auf die Friedrich-Schiller-Universität Jena zwischen 2015 und 2020 „852 Fälle von übernommenen Mailkonten, vermutlich durch Phishing“ (Thüringer Landtag, 2020, S. 1) gezählt werden. In der übergeordneten „Thüringer Strategie zur Digitalisierung im Hochschulbereich“ (Thüringer Landespräsidentenkonferenz und das Ministerium für Wirtschaft, Wissenschaft und Digitale Gesellschaft, 2021), die für den Zeitraum 2021-2025 fortgeschrieben wurde, finden sich sieben Handlungsfelder – davon keines dezidiert für den Bereich IT-Sicherheit. Es wird vielmehr darauf verwiesen, dass zum einen mit dem IT-Dienstleistungszentrum (HS ITZ) ein zentraler Dienstleister zur Verfügung steht, der die „IT-Sicherheit und die damit verbundenen Daten- und Informationssicherheit […] für alle Services des HS-ITZ gewährleistet“ (Thüringer Landespräsidentenkonferenz, 2021, S. 23). Darüber hinaus wird den Hochschulen eine juristische Beratung – insbesondere im Hinblick auf den zunehmenden Einsatz cloudbasierter Services – sichergestellt.[34] Ein IT-Sicherheitsgesetz besteht in Thüringen derzeit nicht. Ein zentraler Baustein ist vielmehr die Thüringer Informationssicherheitsleitlinie (ThISL, 2022), die Verpflichtungen zur Umsetzung der BSI-Standards für die direkte Landesverwaltung beinhaltet.

Dem HS ITZ gehören alle Thüringer Hochschulen an, wobei das HS-ITZ eine Arbeitsgruppe IT-Sicherheit etabliert hat und seit 2024 die ZIS – Zentralstelle für Informationssicherheit und IT-Sicherheit der Thüringer Hochschulen[35] – aufgebaut wird. Ziele des ZIS sind u. a. Etablierung eines Informationssicherheitsmanagementsystems und die Entwicklung einer konsistenten Sicherheitsstrategie für alle Thüringer Hochschulen.[36] In Fällen von IT-Sicherheitsvorfällen unterstützt das ZIS. Ein CERT für die Thüringer Landesverwaltung besteht mit dem ThüringenCERT, welches am Thüringer Landesrechenzentrum angegliedert ist. Rückmeldungen des ThüringenCERT oder des TMBWK zu den Umfragen von HIS-HE liegen nicht vor.

Eine Überblicksdarstellung der zuständigen Behörden und Anlaufstellen für Cybersicherheit in Thüringen enthält Tabelle 16.

[34] Ebd. Eine Stabsstelle IT-Recht ist am HS-ITZ angesiedelt. https://www.hs-itz.de/ueber-uns/stabsstelle-it-recht.

[35] Vgl. die Governance Struktur des HS-ITZ https://www.hs-itz.de/ueber-uns/governance-struktur.

[36] Zum Stand der Behandlung von Sicherheitsfragen beim IT-Zentrum vgl. u. a. Thüringer Landtag (2020).

Politische und behördliche Zuständigkeiten
▪ Thüringer Ministerium für Inneres, Kommunales und Landesentwicklung (TMIKL), u. a. ▪ Abt. 4 Polizei, Koordinierungsstelle Cybersicherheit Thüringen ▪ Amt für Verfassungsschutz ▪ Thüringer Ministerium für Digitales und Infrastruktur (TMDI), u. a. ▪ Abt. 3 Digitale Verwaltung und Geoinformation, Ref. 31 Informationssicherheit, digitale Transformation der Kommunen und OZG-Umsetzungsstrategie ▪ Thüringer Ministerium für Bildung, Wissenschaft und Kultur (TMBWK) ▪ Der Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit (TLfDI)
Zentrale Einrichtungen und koordinierende Stellen
▪ Thüringer Landesrechenzentrum (TLRZ) inkl. ▪ ThüringenCERT ▪ Zentrale Ansprechstelle Cybercrime (ZAC) für Unternehmen und Behörden des Landeskriminalamtes Thüringen
Initiativen, Projekte oder Verbünde im Hochschul- und Wissenschaftsbereich
▪ IT-Zentrum der Thüringer Hochschulen (HS-ITZ) inkl. • Stabsstelle IT-Recht • Zentralstelle für Informationssicherheit und IT-Sicherheit der Thüringer Hochschulen (ZIS) ▪ Initiative für Cybersicherheit Thüringen (ICST) ▪ ITnet Thüringen

Tabelle 16: Aktivitäten und Initiativen zur Cybersicherheit in Thüringen

6 Erkenntnisse und Bewertung

Informations- und Cybersicherheit sowie IT-Sicherheit sind für Hochschulen und wissenschaftliche Einrichtungen zu strategisch zentralen Handlungsfeldern und Daueraufgaben geworden. Die Gefahr von Cyberangriffen nimmt zu und reicht von alltäglichen Phishing-Vorfällen über schwerwiegende Angriffe mit erheblichen Folgeerscheinungen bis hin zu hochprofessionellen nachrichtendienstlichen Angriffen, die nur bedingt verhindert und erkannt werden können.

Ein systematisches Problem besteht jedoch in der mangelnden Erfassung. Bislang fehlt eine regelhafte, **systematische Dokumentation** im Hochschul- und Wissenschaftsbereich, da weder eine einheitliche Definition von Cyberangriffen noch ein zentrales Meldesystem auf Bundes- oder Landesebene existiert. Dies erschwert die Bewertung der Gefährdungslage ebenso wie eine differenzierte Analyse der Beweggründe für Cyberangriffe (z. B. aus kriminellen, politischen oder persönlichen Motiven), den (kurz-, mittel- oder langfristigen) Folgeerscheinungen, der Schadenshöhe (insbesondere die finanziellen Kosten für Prävention, Krisenbewältigung und Wiederaufbau) sowie der Zielrichtung (z. B. Cyberspionage).

Gleichzeitig zeigt die Analyse der Bundesländer eine bemerkenswerte Vielfalt an Unterstützungsansätzen. Systematisiert lassen sich diese entlang zweier Dimensionen unterscheiden: **Reichweite** (umfassende Unterstützung vs. Einzelmaßnahmen) und **Umsetzungsart** (je Hochschule, als zentrales Angebot auf Landesebene oder als Netzwerkmodell der Hochschulen) (vgl. Abbildung 2). Davon ausgehend lassen sich sechs Modelle ableiten, wobei das Individual-, Zentral- und Netzwerkmodell am weitesten verbreitet sind. Im **Zentralmodell** werden Landeseinrichtungen wie beispielsweise das HITS IS Bayern gefördert, die den Hochschulen umfassende Unterstützungsmaßnahmen aus einer Hand anbieten. Im **Netzwerkmodell,** wie es derzeit bspw. in Niedersachsen aufgebaut wird, werden ebenfalls kooperative Strukturen aufgebaut, die ein ähnliches umfassendes Unterstützungsangebot wie im Zentralmodell bieten. In diesem Fall stellen die Hochschulen die Leistungen selbst zur Verfügung. Im **Individualmodell** – wie beispielsweise im Saarland – werden einzelne Maßnahmen an den jeweiligen Hochschulen gefördert. Dies kann sehr umfassend sein (dann geht es in Richtung Aufbaumodell) oder die Ministerien verweisen auf die Freiheit und Verantwortung der jeweiligen Hochschulen. In Bundesländern wie zum Beispiel Nordrhein-Westfalen werden individuelle Einzelmaßnahmen, Netzwerkmodelle und zentrale Landesangebote kombiniert. Die Übergänge zwischen den Modellen sind in dieser Typologie der Länderansätze fließend. Zudem zeigt sich übergreifend, dass die Bereitschaft der Ministerien, die Hochschulen zu unterstützen, stark davon abhängt, ob in der Vergangenheit bereits erfolgreiche Cyberangriffe auf Hochschulen des Landes durchgeführt wurden.

Unabhängig davon ist die **Ressortverantwortung** für Cybersicherheit an Hochschulen in den Landesministerien sehr unterschiedlich angesiedelt – auf übergreifender Ebene (beispielsweise beim CIO des Ministeriums), in der für Hochschulen zuständigen Fachabteilung oder bei dafür spezifisch zuständigen Referent:innen. Diese Vielfalt führt bei einem Querschnittsthema wie Cybersicherheit zu unklaren Zuständigkeiten. Ist Cybersicherheit an Hochschulen allein ein Thema für das Wissenschaftsministerium im Land oder auch für das grundsätzlich für Sicherheit zuständige Innenministerium? Zudem richtet sich der Großteil der Programme primär an Hochschulen. Spezifische Programme für außeruniversitäre Forschungseinrichtungen oder forschungsnahe Institutionen sind nur vereinzelt zu finden.

Die vielfältigen Unterstützungsansätze der Bundesländer sind in eine übergeordnete nationale und internationale Ebene eingebettet. Cybersicherheit im Hochschulbereich ist nicht mehr nur eine nationale Aufgabe, da insbesondere auf europäischer Ebene Gesetze und Rechtsvorschriften den Rahmen setzen. Aufgrund der vielfältigen Regelungen auf Landes-, Bundes- und europäischer Ebene sind die **rechtlichen Rahmenbedingungen** hochkomplex. Neben europäischen Regelungen wie der DSGVO und der NIS-2-Richtlinie existieren zahlreiche bundes- und landesrechtliche Bestimmungen. Besonders kleinere Hochschulen stehen hier vor erheblichen personellen und organisatorischen Herausforderungen. Die Dynamik des Themenfelds zeigt sich exemplarisch an der noch ausstehenden Umsetzung der NIS-2-Richtlinie, die möglicherweise auch Bildungseinrichtungen erfassen wird. Eigene Rechtsberatungsstellen für IT-Sicherheit oder kooperative Unterstützungsansätze sind bislang nur in wenigen Bundesländern etabliert.

Die europäische Dimension und die Komplexität des Themas zeigen sich auch im Bereich der übergreifenden Bedrohungsanlage, in der Cybersicherheit nur einen Aspekt darstellt. Als Teil **hybrider Bedrohungen** können Cyberangriffe die Forschungssicherheit und Resilienz wissenschaftlicher Einrichtungen übergreifend gefährden. Die Europäische Kommission definiert hybride Bedrohungen als „variety of coercive and subversive activities, which can be used in a coordinated manner by state or non-state actors" (European Commission, 2022, S. 9). Die Spionage an Hochschulen wird zunehmend als strukturelle Bedrohung wahrgenommen. So forderte der Europäische Rat im Jahr 2024 eine strukturelle Bewertung der Bedrohungslage, „damit die Lageerfassung auf der Ebene der politischen Entscheidungsträger verbessert wird" (Rat der Europäischen Union, 2024, S.3). Der Wissenschaftsrat mahnt in seinem jüngsten Positionspapier ebenfalls eine stärkere Sensibilisierung für Wissensrisiken an (Wissenschaftsrat, 2025).

Übergreifend zeigt sich, dass es auf europäischer, Landes- oder Bundesebene eine Reihe von Initiativen, Gesetzen und Rechtsverordnungen zu diesem Thema gibt. Die daraus resultierende Vielfalt an Strukturen, Organisationen und Regelungen im gesamten Bereich der Cyber- und IT-Sicherheit bildet ein **vielschichtiges Geflecht der Informationssicherheitsstruktur** in Deutschland. Oft bleibt jedoch unklar, wie Hochschulen und wissenschaftliche Einrichtungen eingebunden sind, welche Regelungen speziell für sie gelten und welche Unterstützungs- und Fördermöglichkeiten bestehen. Dabei zählen Hochschulen bzw. der gesamte Wissenschaftsbereich zu den „beliebtesten" Angriffszielen von Cyberkriminellen in Deutschland und weltweit. Gleichzeitig stellen Hochschulen einen zentralen Eckpfeiler der Cyber-Sicherheitsarchitektur dar, indem sie einerseits einen wichtigen Beitrag zur angewandten Forschung leisten und andererseits das notwendige Fachpersonal aus- und weiterbilden. Ob Hochschulen als schützenswerte Objekte gelten und entsprechend unterstützt, finanziert und gefördert werden müssen, bewerten die Bundesländer jedoch sehr unterschiedlich. Auch wenn der Fokus dieser Untersuchung auf den Ländern liegt, bleibt die Frage offen, inwieweit ein länderübergreifender Ansatz sinnvoll bzw. notwendig ist. Dies bezieht sich vor allem auf länderübergreifende Forschungs- und Wissenschaftseinrichtungen oder Verbünde – zwischen Bundesländern aber auch auf nationaler, europäischer oder internationaler Ebene. Cyber- und IT-Sicherheit ist somit ein übergreifendes Thema für eine gesamte Wissenschaftsregion – egal, ob es sich um eine Einrichtung des Landes oder des Bundes handelt – sowie auch auf länderübergreifender oder internationaler Ebene. Auf europäischer Ebene gibt es mit der Task Force CSIRT (TS-CSIRT) der Open CSIRT Foundation beispielsweise ein Austauschforum für die CERTs.

Neben diesen Rahmenbedingungen und der Einbettung in übergeordnete Entwicklungen sind Cyberangriffe auf Hochschulen bereits Realität. Die Frage ist daher längst nicht mehr, ob ein Angriff erfolgt, sondern wann und mit welchen Folgen. Damit verschiebt sich die Perspektive von Cyberangriffen auf Hochschulen: **Krisenmanagement** darf nicht nur als Reaktion auf akute Vorfälle verstanden werden, sondern muss präventiv als **kontinuierlicher Prozess** in die übergeordnete Hochschulstrategie dauerhaft eingebunden werden. Dies kann beispielsweise durch die Benennung von klaren Verantwortlichkeiten, abgestimmte Kommunikationswege und regelmäßige Übungen erreicht werden (vgl. Gilch et al., 2023).

Der Auf- und Ausbau von Cybersicherheit sowie von effektivem Krisenmanagement erfordert eine **langfristige finanzielle Absicherung**. Hier zeigt sich jedoch eine strukturelle Problematik: Ein Großteil der entsprechenden Projekte für Hochschulen ist zeitlich und finanziell befristet. Die Frage der nachhaltigen Finanzierung bleibt somit offen. Die HRK hat diese Herausforderung in ihrer Stellungnahme zur neuen Bundesregierung adressiert und fordert diese auf, „sich mit den entsprechenden Finanzmitteln entschlossen für die Stärkung der Cybersicherheit der Hochschulen als kritischer Infrastruktur einzusetzen“ (Hochschulrektorenkonferenz (HRK), 2025). Dies gilt im Endeffekt ebenso für die Landesregierungen – insbesondere in Bundesländern, die bislang primär auf die Eigenverantwortung der Hochschulen setzen. Angesichts zunehmend knapper werdender Haushalte stößt der bisherige Ansatz, nach dem Hochschulen Cyberbedrohungen eigenständig identifizieren, entsprechende Schutzmaßnahmen entwickeln und die erforderlichen Ressourcen bereitstellen, an seine Grenzen. Eine Lösung könnte in der Kombination aus konsequenter Umsetzung des BSI-Grundschutzes durch die Hochschulen und gleichzeitiger struktureller Unterstützung durch Bund und Länder liegen. Dabei erweisen sich auch kooperative Ansätze zwischen den Hochschulen als vielversprechend, um Ressourcen zu bündeln und Synergieeffekte zu nutzen.

Zudem zeigt die Untersuchung, dass Cybersicherheit **systematische Kooperationen auf mehreren Ebenen** erfordert: zwischen Hochschulen, zwischen Hochschulen und Wissenschaftseinrichtungen sowie zwischen Hochschulen und spezialisierten Einrichtungen wie den CERTs. Netzwerke und Verbünde ermöglichen nicht nur Kostenteilung und Ressourcenbündelung, sondern auch den kritischen Wissenstransfer über Bedrohungslagen, Abwehrstrategien und bewährte Praktiken. Letztendlich geht es um mehr als technische Lösungen: Es geht um den Aufbau einer **kollektiven Cybersicherheitskultur** im Wissenschafts- und Hochschulbereich, um Hochschulen als kritische Infrastruktur angemessen zu schützen und gleichzeitig ihre Rolle als Innovationstreiber und Ausbildungsstätte für Cybersicherheitsexpert:innen zu stärken.

7 Literaturverzeichnis

Abgeordnetenhaus Berlin (2021a). Drucksache, 18/28 131. (2021, 27. Juli). Abgerufen von https://pardok.parlament-berlin.de/starweb/adis/citat/VT/18/SchrAnfr/S18-28131.pdf.

Abgeordnetenhaus Berlin (2021b). Wortprotokoll, Ausschuss für Wissenschaft und Forschung, 67. Sitzung. (2021, 31. Mai). Abgerufen von https://pardok.parlament-berlin.de/starweb/adis/citat/VT/18/AusschussPr/wf/wf18-067-wp.pdf.

Abgeordnetenhaus Berlin (2023). Wortprotokoll, Ausschuss für Inneres, Sicherheit und Ordnung, 27. Sitzung. (2023, 11. Dezember). Abgerufen von https://pardok.parlament-berlin.de/starweb/adis/citat/VT/19/AusschussPr/iso/iso19-027-wp.pdf.

Abgeordnetenhaus Berlin (2024). Drucksache, 19/18 456. (2024, 15. März). Abgerufen von https://pardok.parlament-berlin.de/starweb/adis/citat/VT/19/SchrAnfr/S19-18456.pdf.

BayDiG – Gesetz über die Digitalisierung im Freistaat Bayern (2022). Abgerufen von https://www.gesetze-bayern.de/Content/Document/BayDiG.

Bayerisches Staatsministerium des Innern, für Sport und Integration (Hrsg.). (2023). *Bayerische Cybersicherheitsstrategie 2.0. modern. präventiv. resilient.* Abgerufen von https://www.bestellen.bayern.de/application/e-shop_app000002?SID=2014424623&DIR=eshop&ACTIONxSETVAL(artdtl.htm,APGxNODENR:289623,AARTxNR:03200066,AARTxNODENR:371149,USERxBODYURL:artdtl.htm,KATALOG:StMI,AKATxNAME:StMI,ALLE:x)=X.

Bayerische Staatsregierung (2023). *Rahmenvereinbarung Hochschulen 2023-2027.* Abgerufen von https://www.stmwk.bayern.de/download/22215_Rahmenvereinbarung-2023-2027_ohne-Unterschrift.pdf&ved=2ahUKEwjG3PnkypuOAxVQSP4FHQWvIsEQFnoECBgQAQ&usg=AOvVaw1r5ReI5SdDMbfVC91N7Wrv.

Behörde für Wissenschaft, Forschung, Gleichstellung und Bezirke (BWFGB) (2024). *Digitalstrategie der Behörde für Wissenschaft, Forschung, Gleichstellung und Bezirke. Kurzversion*. Abgerufen von https://digital.hamburg.de/resource/blob/845200/e1e545412748060d55e03ac4f8411b97/pdf-strategie-kurzversion-bwfb-data.pdf.

Berliner Senatsverwaltung für Inneres und Sport (2017). Leitlinie zur Informationssicherheit der Landesverwaltung des Landes Berlin. Abgerufen von https://www.berlin.de/moderne-verwaltung/prozesse-und-technik/ikt-sicherheit/leitlinie-informationssicherheit/artikel.947529.php.

Bitkom (2025). *Mehrheit der Deutschen hat Angst vor Cyberangriffen – und einem Cyberkrieg*. Abgerufen von https://www.bitkom.org/Presse/Presseinformation/Mehrheit-Angst-Cyberangriffen-Cyberkrieg.

Bremische Bürgerschaft (2022). *Drucksache, 20/1611. (2022, 27. September).* Abgerufen von https://www.bremische-buergerschaft.de/dokumente/wp20/land/drucksache/D20L1611.pdf.

BSIG – Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (2009). Abgerufen von https://www.gesetze-im-internet.de/bsig_2009/BSIG.pdf.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.) (2024). *Die Lage der IT-Sicherheit in Deutschland 2024.* Abgerufen von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&v=5.

Bundesministerium des Innern, für Bau und Heimat (BMI) (Hrsg.) (2020). *Online Kompendium Cybersicherheit in Deutschland.* Abgerufen von https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/it-digitalpolitik/online-kompendium-nationaler-pakt-cybersicherheit.pdf?__blob=publicationFile&v=9.

Bundesministerium des Innern, für Bau und für Heimat (BMI) (Hrsg.). (2021a). *Cybersicherheitsstrategie für Deutschland 2021.* https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf?__blob=publicationFile&v=3

Bundesregierung (2024a). *Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung*. Abgerufen von https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/CI1/nis2-regierungsentwurf.pdf?__blob=publicationFile&v=2.

Bundesregierung (2024b). *Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz)*. Abgerufen von https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/KM4/regentwurf-kritisDachG.pdf?__blob=publicationFile&v=3.

Bundesverband IT-Sicherheit e.V. (2023). *Offener Brief an den IT-Planungsrat.* Abgerufen von *https://www.teletrust.de/publikationen/stellungnahmen/2023/?utm*.

Bürgerschaft der Freien und Hansestadt Hamburg (2023). *Drucksache, 22/10984. (2023, 21. Februar)*. Abgerufen von https://www.buergerschaft-hh.de/parldok/dokument/82837/22_10984_landesrechnungshof_attestiert_hamburger_hochschulen_mangelhaften_schutz_der_it_infrastruktur#navpanes=0.

CISPA (2025). *Willkommen am Cispa.* Verfügbar unter https://cispa.de/de.

CSG BW – Gesetz für die Cybersicherheit in Baden-Württemberg (2021). Abgerufen von https://www.landesrecht-bw.de/bsbw/document/jlr-CSGBWrahmen.

Deutscher Bundestag (2024). Drucksache, 20/12259. (2024, 10. Juli). Abgerufen von https://dserver.bundestag.de/btd/20/122/2012259.pdf. [28.08.2025].

DSGVO (2016). *Dokument 32016R0679*. Abgerufen von https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=de.

Eckert, Claudia (2023). *IT-Sicherheit. Konzepte – Verfahren – Protokolle.* De Gruyter Oldenburg. Berlin. 11. Auflage.

EGovG Bln – Gesetz zur Förderung des E-Government (2016). Abgerufen von https://gesetze.berlin.de/bsbe/document/jlr-EGovGBErahmen.

EGov BW – Gesetz zur Förderung der elektronischen Verwaltung des Landes Baden-Württemberg (2015). Abgerufen von https://www.landesrecht-bw.de/bsbw/document/jlr-EGovGBWrahmen.

EGovG NRW – Gesetz zur Förderung der elektronischen Verwaltung in Nordrhein-Westfalen (2016). Abgerufen von https://recht.nrw.de/lmi/owa/br_bes_text?anw_nr=2&bes_id=34925&gld_nr=2&ugl_nr=2006&menu=1&sg=0&aufgehoben=N&keyword=IT-Sicherheit#det.

EGovGRP – Landesgesetz zur Förderung der elektronischen Verwaltung in Rheinland-Pfalz (2020). Abgerufen von https://landesrecht.rlp.de/bsrp/document/jlr-EGovGRPrahmen.

European Commission (2020). *The EU's Cybersecurity Strategy for the Digital Decade.* Abgerufen von *https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.*

European Commission (2022). *Tackling R&I Foreign Interference. Staff Working Document.* Abgerufen von https://data.consilium.europa.eu/doc/document/ST-5396-2022-INIT/en/pdf.

European Repository of Cyber Incidents (2025). Abgerufen von https://eurepoc.eu/table-view/ [18.06.2025].

Gilch, H., Lübcke, M. & Stein, M. (2023). *Krisenmanagement nach Cyber-Angriffen – Handlungsempfehlungen.* HIS-HE: Handreichung. Hannover: HIS- Institut für Hochschulentwicklung e. V. (HIS-HE). Abgerufen von https://his-he.de/publikationen/krisenmanagement-nach-cyber-angriffen-handlungsempfehlungen/.

HDSiG – Hessisches Datenschutz- und Informationsfreiheitsgesetz (2018). Abgerufen von https://www.rv.hessenrecht.hessen.de/bshe/document/jlr-DSIFGHErahmen.

Herpig, S. & Dutke, F. (2023). *Deutschlands staatliche Cybersicherheitsarchitektur. 11. Auflage*. Stiftung Neue Verantwortung. Abgerufen von https://www.interface-eu.org/storage/archive/files/cybersicherheits-architektur_elfteauflage1123.pdf.

Hessischer Landtag (2024a). *Drucksache, 21/193. (2024, 8. Mai).* Abgerufen von https://starweb.hessen.de/cache/DRS/21/3/00193.pdf.

Hessischer Landtag (2024b). *Drucksache, 21/397. (2024, 6. August).* Abgerufen von https://starweb.hessen.de/cache/DRS/21/7/00397.pdf.

Hessisches Ministerium des Innern und für Sport (Hrsg.). (2023). *Hessische Cybersicherheitsstrategie*. Abgerufen von https://hessen3c.de/sites/hessen3c.hessen.de/files/2023-10/hessische_cybersicherheitsstrategie_web.pdf.

HITSiG – Hessisches Gesetz zum Schutz der elektronischen Verwaltung, HITSiG (2023). Abgerufen von https://www.rv.hessenrecht.hessen.de/bshe/document/jlr-ITSiGHErahmen.

Hochschulrektorenkonferenz (HRK) (2025, 05. Februar). *Bund muss bei Cybersicherheit der Hochschulen mehr Verantwortung übernehmen* [Pressemitteilung]. Abgerufen von https://www.hrk.de/presse/pressemitteilungen/pressemitteilung/meldung/bund-muss-bei-cybersicherheit-der-hochschulen-mehr-verantwortung-uebernehmen-5104/.

Hochschulrektorenkonferenz (HRK) (2025). *Bedrohungslage erhöht Handlungsdruck für den Bund: HRK-Empfehlungen zur Stärkung der Cybersicherheit.*
Abgerufen von https://www.hrk.de/presse/pressemitteilungen/pressemitteilung/meldung/bund-muss-bei-cybersicherheit-der-hochschulen-mehr-verantwortung-uebernehmen-5104/.

IS-Leitlinie MV – Leitlinien zur Gewährleistung der Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern (2014). Abgerufen von https://www.regierung-mv.de/static/Regierungsportal/Ministerium%20f%C3%BCr%20Energie%2c%20Infrastruktur%20und%20Digitalisierung/Dateien/cert/IS-Leitlinie.pdf.

IS-LL – Informationssicherheitsleitlinie für die Freie und Hansestadt Hamburg (2013). Abgerufen von http://daten.transparenz.hamburg.de/Data-port.HmbTG.ZS.Webservice.GetRessource100/GetRessource100.svc/7f9cdbc0-aea4-4c0c-a681-38109c0901f3/Akte_FB1a.805.01-2.pdf.

IT-Planungsrat (2023). Beschluss, 2023/39 (2023, 3. November). Abgerufen von https://www.it-planungsrat.de/beschluss/beschluss-2023-39.

IT-SiG SL – Gesetz zur Abwehr von Gefahren für die Daten in der Informations- und Kommuikationsinfrastruktur des Landes (Informationssicherheitsgesetz Saarland) (2019). Abgerufen von https://recht.saarland.de/bssl/document/jlr-InfSichGSLpIVZ.

IT-SIG 2.0 – Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (2021). Abgerufen von https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf#/text/bgbl121s1122.pdf?_ts=1751962121654.

IT-Strategie der bayerischen Hochschulen Version 1.0. Erstellt von den CIOs und IT-Leiter:innen der Universitäten und Hochschulen angewandter Wissenschaft in Bayern. Abgerufen von https://www.hochschule-bayern.de/positionen/standpunkte-2022/it-strategie-der-bayerischen-hochschulen.

ITSH-edu IT-Sicherheitspolitik der teilnehmenden Hochschulen und Forschungseinrichtungen in Schleswig-Holstein (2010). Abgerufen von https://www.uni-flensburg.de/fileadmin/content/portal/die-universitaet/dokumente/satzungen/weitere-satzungen/itsh-it-sicherheitspolitik-1.pdf.

Kipker, D.-K. (Hrsg.) (2020). *Cybersecurity: Rechtshandbuch*. C.H. Beck.

Koalitionsvertrag 2021-2026: Wir gestalten Sachsen-Anhalt. Stark. Modern. Krisenfest. Gerecht. (2021). Abgerufen von https://www.sachsen-anhalt.de/fileadmin/Bibliothek/Politik_und_Verwaltung/StK/STK/Startseite_pdf_Dokumente/Koalitionsvertrag_2021-2026.pdf.

Koalitionsvertrag 2023-2026: Das Beste für Berlin. (2023). Abgerufen von https://www.berlin.de/rbmskzl/politik/senat/koalitionsvertrag/.

LandesHochschulKonferenz Niedersachsen (LHK) (Hrsg.) (2024). *Gemeinsam digital. Gesamtstrategie 2030 der Hochschule.digital Niedersachsen.* Abgerufen von https://hochschuledigital-niedersachsen.de/wp-content/uploads/2024/06/240619_Lay_HdN-Strategiepapier_Web.pdf.

Landesrechnungshof Brandenburg (2021). *Jahresbericht 2021*. Abgerufen von https://www.lrh-brandenburg.de/media_fast/250/LRH_Brandenburg_Jahresbericht_2021.pdf.

Landesregierung Brandenburg (Hrsg.) (2022). *Digitalprogramm des Landes Brandenburg 2025. Digital. Vernetzt. Gemeinsam.* Abgerufen von https://digitalesbb.de/ubersichtsseite/strategie/.

Landesregierung Nordrhein-Westfalen (Hrsg.) (2021). *Cybersicherheitsstrategie des Landes Nordrhein-Westfalen*. Abgerufen von https://www.cybersicherheit.nrw/de/cybersicherheit-nrw-gemeinsam-voranbringen.

Landesrektorenkonferenz Sachsen und dem Staatsministerium für Wissenschaft, Kultur und Tourismus (Hrsg.). (2023). *Strategie der digitalen Transformation im Hochschulbereich*. Abgerufen von https://www.studieren.sachsen.de/download/Strategie_dig._Transformation_im_Hochschulbereich.pdf.

Landtag Brandenburg (2023a). *Drucksache, P-AWFK 7/41 – TOP 5. (2023, 15. November).* Abgerufen von https://www.parlamentsdokumentation.brandenburg.de/starweb/LBB/ELVIS/parladoku/w7/apr/AWFK/41-007.pdf.

Landtag Brandenburg (2023b). *Drucksache, 7/8478*. (2023, 20. September). Abgerufen von https://www.parlamentsdokumentation.brandenburg.de/starweb/LBB/ELVIS/parladoku/w7/drs/ab_8400/8478.pdf.

Landtag Mecklenburg-Vorpommern (2023). *Drucksache, 8/2479. (2023, 21. August).* Abgerufen von https://www.landtag-mv.de/fileadmin/media/Dokumente/Parlamentsdokumente/Drucksachen/8_Wahlperiode/D08-2000/Drs08-2479.pdf.

Landtag Nordrhein-Westfalen (2023). *Drucksache, 18/3792. (2023, 27. März).* Abgerufen von https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMD18-3792.pdf.

Landtag Rheinland-Pfalz (2022a). *Drucksache, 18/3332 (2022, 30. Mai).* Abgerufen von https://dokumente.landtag.rlp.de/landtag/drucksachen/3332-18.pdf.

Landtag Rheinland-Pfalz (2022b). *Drucksache, 18/3334 (2022, 30. Mai).* Abgerufen von https://dokumente.landtag.rlp.de/landtag/drucksachen/3334-18.pdf.

Landtag von Baden-Württemberg (2023a). *Drucksache 17/4022. (2023, 25. Januar).* Abgerufen von https://www.landtag-bw.de/files/live/sites/LTBW/files/dokumente/WP17/Drucksachen/4000/17%5F4022%5FD.pdf.

Landtag von Baden-Württemberg (2023b). *Drucksache, 17/5525. (2023, 4. Oktober).* Abgerufen von *https://www.landtag-bw.de/files/live/sites/LTBW/files/dokumente/WP17/Drucksachen/5000/17%5F5525%5FD.pdf*.

Landtag von Sachsen-Anhalt (2022). *Drucksache, 8/1831. (2022, 4. November).* Abgerufen von https://padoka.landtag.sachsen-anhalt.de/files/drs/wp8/drs/d1831fak.pdf.

Leitlinie für die Informationssicherheit in der Landesverwaltung Brandenburg und der Justiz (Informationssicherheitsleitlinie). (2024). Abgerufen von https://bravors.brandenburg.de/verwaltungsvorschriften/informationssicherheitsleitlinie_2024#i1.

Microsoft (2024). *Microsoft Digital Defense Report. The foundations and new frontiers of cybersecurity.* Abgerufen von Abgerufen von https://www.microsoft.com/de-de/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024.

Ministerium des Inneren, für Digitalisierung und Kommunen im Auftrag der Landesregierung Baden-Württemberg (Hrsg.) (2021). *Cybersicherheitsstrategie Baden-Württemberg – Perspektive 2026.* Abgerufen von https://www.digital-laend.de/publikationen/cybersicherheitsstrategie.pdf&ved=2ahUKEwijlurTnZuOAxXoh_0HHZfGDMUQFnoECAkQAQ&usg=AOvVaw1qLlAKT5kQqrNE_eC7XA8E.

Ministerium für Infrastruktur und Digitales (Hrsg.) (2023). *Strategie „Sachsen-Anhalt Digital 2030“*. Abgerufen von https://mid.sachsen-anhalt.de/digitales/strategie-sachsen-anhalt-digital-2030.

NDIG – Niedersächsisches Gesetz über digitale Verwaltung und Informationssicherheit (2019). Abgerufen von https://voris.wolterskluwer-online.de/browse/document/a8cf0d53-edeb-3d90-8bf4-a42dbb4e8799.

Niedersächsisches Ministerium für Inneres und Sport (Hrsg.) (2023). *Digitale Verwaltung 2030. Strategie zur digitalen Transformation der Verwaltung des Landes Niedersachsen*. Abgerufen von https://www.mi.niedersachsen.de/download/200570/Digitalisierungsstrategie_2030.pdf&ved=2ahUKEwiwpOejl5uOAxWfVfEDHZ4UFZQQFnoECAkQAQ&usg=AOvVaw3dT5K8gzikVhsy724Ya_T2.

Niedersächsisches Ministerium für Inneres und Sport (Hrsg.) (2024). *Cybersicherheitsstrategie Niedersachsen*. Abgerufen von https://www.mi.niedersachsen.de/startseite/themen/it_bevollmachtigter_der_landesregierung/cybersicherheit/cybersicherheit-150587.html.

NICS2UmsuCG – Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (2024). Abgerufen von https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/nis2umsucg.html.

RaSiKo - Rahmen-Sicherheitskonzept der Freien und Hansestadt Hamburg. Version 1.1. (2016, 19. Januar). Abgerufen von http://daten.transparenz.hamburg.de/Dataport.HmbTG.ZS.Webservice.GetRessource100/GetRessource100.svc/4c792633-a668-4d5c-88eb-97494252b187/Akte_FB1a.803.73-50.pdf&ved=2ahUKEwieg-KzsJuOAxUsRPEDHYHVAgQFnoECBoQAQ&usg=AOvVaw3LEZeO_NslLmkmOGz1Lbgs.

Rat der Europäischen Union (2024). *Drucksache C/2024/3510. (2024, 30. Mai).* Abgerufen von https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:C_202403510.

Rechnungshof Freie und Hansestadt Hamburg (2023). *Jahresbericht 2023*. Abgerufen von https://www.hamburg.de/resource/blob/245950/6b5606242e8ff92ed5fb75fbdeaa5f6b/jahresbericht-2023-pdf-data.pdf.

Rehbohm, T. & Moses, F. (2023). *Föderale Cybersicherheitsarchitektur und Informationssicherheitsmanagement im Kontext der NIS-2-Richtlinie.*

Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates (2022). Abgerufen von https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555&qid=1734610756641.

Rupp, C. (2024). *Navigating the EU Cybersecurity Policy Ecosystem. A Comprehensive Overview of Legislation, Policies and Actors*. Interface – Tech analysis and policy ideas for Europe. Abgerufen von https://www.interface-eu.org/publications/navigating-the-eu-cybersecurity-policy-ecosystem.

SächsISichG – Sächsisches Informationssicherheitsgesetz (2019). Abgerufen von https://www.revosax.sachsen.de/vorschrift/18349-Saechsisches-Informationssicherheitsgeset.

Sächsischer Landtag (2023). *Drucksache, 7/12294. (2023, 20. Februar)*. Abgerufen von https://edas.landtag.sachsen.de/redas/download?datei_id=25931.

Schleswig-Holsteinischer Landtag (2023). *Drucksache, 20/1584. (2023, 7. November).* Abgerufen von https://www.landtag.ltsh.de/infothek/wahl20/drucks/01500/drucksache-20-01584.pdf.

Senator für Inneres im Auftrag des Senats der Freien Hansestadt Bremen (Hrsg.) (2023). *Bremische Cybersicherheitsstrategie 2023.* Abgerufen von https://www.inneres.bremen.de/sixcms/media.php/13/Bremische Cybersicherheitsstrategie 2023.pdf.

Senatskanzlei – Amt für IT und Digitalisierung (Hrsg.). (2020). *Digitalstrategie für Hamburg*. Abgerufen von https://www.hamburg.de/resource/blob/230646/115a3934734fbbcfe65497ba5f857fff/download-digitalstrategie-2020-data.pdf.

Stabsstelle Informationssicherheit der bayerischen, staatlichen Hochschulen und Universitäten (2020). *HISP – Hochschulinformationssicherheitsprogramm, HISP 1.0*. Abgerufen von https://www.tha.de/Binaries/Binary45562/HISP-V1.pdf&ved=2ahUKEwiq87zlyd6LAxWx9AIHHcBEFPoQFnoECBQQAQ&usg=AOvVaw0AxcgE1I43ve_4S--AAiAp.

Stifterverband für die Deutsche Wissenschaft e. V. (Hrsg.) (2025). *Hochschul-Barometer. Lage und Entwicklung der Hochschulen aus Sicht ihrer Leitungen, Ausgabe 2024.* Abgerufen von https://www.hochschul-barometer.de/.

ThISL – Informationssicherheitsleitlinie der Thüringer Landesverwaltung (2022). Abgerufen von https://finanzen.thueringen.de/fileadmin/medien_tfm/E-Government/informationssicherheitsleitlinie_thueringer_landesverwaltung.pdf.

Thüringer Landespräsidentenkonferenz und das Ministerium für Wirtschaft, Wissenschaft und Digitale Gesellschaft (Hrsg.). (2021). *Thüringer Strategie zur Digitalisierung im Hochschulbereich. Fortschreibung 2021-2025* (2021). Abgerufen von https://wirtschaft.thueringen.de/fileadmin/user_upload/Digitalstrategie-Hochschulen_2021-2025.pdf.

Thüringer Landtag (2020). *Drucksache, 7/545. (2020, 13. März).* Abgerufen von https://parldok.thueringer-landtag.de/ParlDok/dokument/74805/cyberattacken_auf_thueringer_hochschulen_und_forschungseinrichtungen.pdf.

Tunnat, Y. (2023). *Cyber-Angriff auf die ZBW: Mit Fokus auf Auswirkungen für die digitale Langzeitarchivierung*. Leibniz-Gemeinschaft.

Vereinbarung zur Informationssicherheit an den Hochschulen (VzI) zwischen den Universitäten und Hochschulen für angewandte Wissenschaften in Trägerschaft des Landes Nordrhein-Westfalen, den staatlichen Kunst- und Musikhochschulen in Nordrhein-Westfalen (Hochschulen), dem Hochschulbibliothekszentrum des Landes Nordrhein-Westfalen (hbz) und dem Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen (MWK) im Einvernehmen der Digitalen Hochschule NRW (DH.NRW) (2023). https://www.mkw.nrw/system/files/media/document/file/vereinbarung_zur_informationssicherheit_an_den_hochschulen_vzi_2023_0_1.pdf

Vereinbarung zur Cybersicherheit an den Hochschulen (VzC) zwischen den Universitäten und Hochschulen für angewandte Wissenschaften in Trägerschaft des Landes Nordrhein-Westfalen, den staatlichen Kunst- und Musikhochschulen in Nordrhein-Westfalen (Hochschulen), dem Hochschulbibliothekszentrum des Landes Nordrhein-Westfalen (hbz) und dem Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen (MWK) im Einvernehmen der Digitalen Hochschule NRW (DH.NRW) (2024). https://www.mkw.nrw/system/files/media/document/file/vereinbarung_zur_cybersicherheit_vzc_1.pdf

Wissenschaftsrat (Hrsg.) (2025). *Wissenschaft und Sicherheit in Zeiten weltpolitischer Umbrüche | Positionspapier.*
Abgerufen von https://www.wissenschaftsrat.de/download/2025/2485-25.pdf?__blob=publicationFile&v=0.

Zentren für Kommunikation und Informationsverarbeitung e.V. (ZKI) (Hrsg.) (2022). *IT-Grundschutz-Profil für Hochschulen.* Abgerufen von https://www.zki.de/fileadmin/user_upload/Downloads/IT_Grundschutz_ZKI_2022_Final.pdf.

Zentren für Kommunikation und Informationsverarbeitung e.V. (ZKI) (Hrsg.) (2025). *BCM-Profil für Hochschulen. Community Draft 2025.0.0.* Abgerufen von *https://ak-itsm-share.zki.de/s/mSJQakxzB7jzqYe?dir=/&openfile=true*.

Die angegebenen URLs wurden zuletzt am 07. Juli 2025 geprüft.

Anhang

Anhang 1 Fragebogen CERT-Umfrage

Von: Stein, Dr. Mathias
Gesendet: Freitag, 24. Mai 2024 10:11
An: [redacted]
Cc: Lübcke, Dr. Maren <[redacted]; Gilch, Dr. Harald [redacted]
Betreff: Länderumfrage - Cyber-Security für Hochschulen

Sehr geehrte Damen und Herren,

als HIS-Institut für Hochschulentwicklung e.V. unterstützen und begleiten wir Hochschulen und Ministerien bei zentralen Veränderungen und Entwicklungen – von Baulicher Hochschulentwicklung und Flächenbedarf über Nachhaltigkeit bis hin zu Organisationsentwicklung und Change-Management. Ein Thema, welches in den vergangenen Jahren im Rahmen der Digitalisierung an hoher Bedeutung gewonnen hat, ist die Gefahr von Cyber-Angriffen auf Hochschulen. Vor diesem Hintergrund haben wir im vergangenen Jahr eine Interviewstudie mit betroffenen Hochschulen durchgeführt und darauf aufbauend „Handlungsempfehlungen" für das Krisenmanagement nach Cyber-Angriffen veröffentlicht (Handlungsempfehlungen). Im Fokus der Studie stehen neben verschiedenen IT-Aspekten vor allem Fragen wie Vorbereitung und Handlungsmöglichkeiten im Krisenfall, (externe) Hilfe und Unterstützung sowie langfristige Krisenbewältigung.

Aktuell untersuchen wir den derzeitigen Stand an Maßnahmen und Beratungsstellen im Themenbereich Cyber-Security für Hochschulen und Wissenschaftseinrichtungen in den Bundesländern. Hierzu möchten wir auch sehr gern das [redacted] befragen und würden uns sehr freuen, wenn Sie uns folgende Fragen kurz beantworten könnten:

1) Umfasst der Auftrag des [redacted] auch die Unterstützung und Beratung von Hochschulen und wissenschaftlichen Einrichtungen?
   a. Wenn ja, welche speziellen Angebote bietet das [redacted] für Hochschulen und wissenschaftliche Einrichtungen an?
   b. Wenn nein, welche Einrichtungen des Landes stehen Hochschulen und wissenschaftlichen Einrichten in Fragen zur Cyber-Security zur Verfügung?
2) Wie viele Anfragen hat das [redacted] in den letzten zwei Jahren von Hochschulen und wissenschaftlichen Einrichtungen bekommen?
3) Haben Sie weitere Anmerkungen und Hinweise, die aus Ihrer Sicht im Bereich Cyber-Security für Hochschulen und wissenschaftliche Einrichtungen besonders erwähnenswert sind?

Für Anmerkungen und Rückfragen stehen wir sehr gern zur Verfügung.

Für Ihre Unterstützung bedanken wir uns herzlich.

Mit den besten Grüßen

Dr. Maren Lübcke, Dr. Harald Gilch, Dr. Mathias Stein

Dr. Mathias Stein
Geschäftsbereich Hochschulmanagement

Anhang 2 Fragebogen Wissenschaftsministerien

Fragebogen

Cybersicherheit im Hochschulbereich – Umfrage zur Unterstützung durch die Wissenschaftsministerien der Bundesländer

Cyber-Sicherheit und die Gefahr von Cyber-Angriffen auf Hochschulen und wissenschaftliche Ein-richtungen hat in den vergangenen Jahren an Bedeutung sehr stark zugenommen. Als HIS-Institut für Hochschulentwicklungen e.V. (HIS-HE) begleiten und unterstützen wir Hochschulen und Mini-sterien bei diesem Thema und haben u.a. im vergangenen Jahr eine Interviewstudie mit betroffenen Hochschulen durchgeführt. Aufbauend auf diesen Gesprächen sind „Handlungsempfehlungen" für das Krisenmanagement nach Cyber-Angriffen entstanden, um Hochschulen einen Orientierungsrah-men für mögliche Krisenszenarien zur Verfügung zu stellen (Handlungsempfehlungen). Im Fokus der Untersuchung standen neben verschiedenen IT-Aspekten vor allem Fragen wie Handlungsmöglich-keiten im Krisenfall, (externe) Hilfe und Unterstützung sowie langfristige Krisenbewältigung. Auf-grund der hohen Nachfrage an der Studie und dem Thema planen wir für den 20./21. Juni 2024 ein Forum Krisenmanagement nach Cyber-Angriffen an Hochschulen, welches in Hannover stattfindet (Forum).

Aktuell untersuchen wir den derzeitigen Stand an Maßnahmen und Beratungsstellen im Themenbe-reich Cyber-Security für Hochschulen und Wissenschaftseinrichtungen in den Bundesländern. Ziel ist es, eine übergreifende Darstellung der Angebote und Aktivitäten als eine Handreichung für Hoch-schulen zu veröffentlichen, um über Möglichkeiten, Services und Kontaktstellen zu informieren.

Die Bearbeitung des Fragebogens beansprucht etwa 5 Minuten.

Für Ihre Unterstützung bedanken wir uns herzlich.

Mit freundlichen Grüßen,

Dr. Maren Lübcke, Dr. Harald Gilch und Dr. Mathias Stein

Falls Informationen nicht verfügbar sind, lassen Sie die Felder bitte unausgefüllt.

Für Nachfragen zur Befragung oder zum Projekt stehen Ihnen Dr. Maren Lübcke (Tel.: 0511 169929-19, E-Mail: luebcke@his-he.de, Dr. Harald Gilch (Tel.: 0511 169929-32, E-Mail: gilch@his-he.de) und Dr. Mathias Stein (Tel.: 0511 169929-27, E-Mail: stein@his-he.de) zur Verfügung.

Datenschutzhinweis: Ihre Teilnahme an der Befragung ist freiwillig. Es ist selbstverständlich, dass alle gesetzlichen Bestimmungen des Datenschutzes nach der Datenschutzgrundverordnung (DSGVO) eingehalten werden. Wir versichern Ihnen, dass wir Ihre Befragungsdaten ausschließlich für Forschungszwecke nutzen werden und eine Veröffentlichung ggf. in aggregierter und anonymisierter Form stattfindet. Die erhobenen Paradaten werden ausschließlich für die folgenden Zwecke genutzt: a) Sicherstellung eines reibungsfreien technischen Ablaufs der Befragung, b) Sicherung der Datenqualität, c) Forschung. Die Einhaltung der Vorkehrungen zum Schutz Ihrer Angaben wird durch den Datenschutzbeauftragten von HIS-HE, Dr. Klaus Wannemacher, überwacht. Bei Fragen zum Datenschutz erreichen Sie ihn unter der Rufnummer 0511 169929-23 oder unter wannemacher@his-he.de.

1 Wie relevant ist das Thema Cyber-Sicherheit von Hochschulen und wissenschaftlichen Einrichtungen für Ihr Ministerium?

- ◯ 1 sehr relevant
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5 relevant

2 Wie ist das Thema Cyber-Sicherheit für Hochschulen und wissenschaftliche Einrichtungen in Ihrem Ministerium **strukturell** verankert? Inwieweit gibt es für das Thema feste Zuständigkeiten und entsprechende personelle Ressourcen? In welchem Umfang stehen diese zur Verfügung? In welchem Referat/Abteilung/Einheit sind die Zuständigkeiten verankert?

3 In welchen Bereichen bietet Ihr Bundesland den Hochschulen und wissenschaftlichen Einrichtungen Unterstützungsleistungen in welcher Form an?

	individuell je Hochschule	landesweit (Verbund)	Mischformen (z. B. für verschiedene Hochschultypen, Regionalverbünde)	nicht vorhanden	keine Antwort
Informationssicherheit (z.B. IT-Sicherheits-beauftragte)	☐	☐	☐	☐	☐
Umsetzung BSI-Sicherheitsstandard	☐	☐	☐	☐	☐
IT-Personal (Entwicklung, Finanzierung, Gewinnung, etc.)	☐	☐	☐	☐	☐
IT-Infrastruktur (landesweite Basisdienste)	☐	☐	☐	☐	☐
Audits/Zertifizierung	☐	☐	☐	☐	☐
Gremien/Verbünde zum Austausch etc.	☐	☐	☐	☐	☐
Weiterbildung und Schulungsangebote	☐	☐	☐	☐	☐

4 Welche weiteren Unterstützungsleistungen, die bis jetzt nicht genannt worden sind, gibt es in Ihrem Bundesland für Hochschulen und wissenschaftliche Einrichtungen zum Thema Cyber-Sicherheit? In welcher Form werden diese Angebote?

5 Gibt es in Ihrem Bundesland direkte Notfallunterstützung für Hochschulen und wissenschaftliche Einrichtungen im Fall eines Cyber-Angriffes (z. B. in Form eines Computer Emergency Response Team (CERT))?

- ◯ Ja
- ◯ Nein
- ◯ Kann ich nicht beurteilen

5.1 Wenn ja, Bitte erläutern Sie kurz den Leistungsumfang.

5.2 Wenn nein, befindet sich ein solches in Planung oder im Aufbau?

6 Haben Sie weitere Anmerkungen und Hinweise, die aus Ihrer Sicht im Bereich Cyber-Sicherheit in Ihrem Bundesland für Hochschulen und wissenschaftliche Einrichtungen besonders erwähnenswert sind?

7 Für welches Bundesland ist Ihr Ministerium zuständig?

- ◯ Baden-Württemberg
- ◯ Bayern
- ◯ Berlin
- ◯ Brandenburg
- ◯ Bremen
- ◯ Hamburg
- ◯ Hessen
- ◯ Mecklenburg-Vorpommern
- ◯ Niedersachsen
- ◯ Nordrhein-Westfalen
- ◯ Rheinland-Pfalz
- ◯ Saarland
- ◯ Sachsen
- ◯ Sachsen-Anhalt
- ◯ Schleswig-Holstein
- ◯ Thüringen
- ◯ Übergreifende Einrichtung

Wenn Sie über die Ergebnisse der Befragung informiert werden möchten, nennen Sie uns bitte unter diesem Link Ihre Emailadresse. Wir melden uns bei Ihnen, sobald die Ergebnisse vorliegen.

Bitte senden Sie Ihren ausgefüllten Fragebogen per E-Mail an Mathias Stein unter stein@his-he.de.

Vielen Dank für Ihre Teilnahme!