21. Wahlperiode

Deutscher Bundestag
Ausschuss für Forschung, Technologie,
Raumfahrt und Technikfolgenabschätzung

Ausschussdrucksache 21(18)24c
vom 4. November 2025

Schriftliche Stellungnahme

der Sachverständigen Claudia Plattner

Öffentliches Fachgespräch zum Thema „Forschungssicherheit“

TOP 1 der 9. Sitzung am 5. November 2025

Stellungnahme zum Fachgespräch „Forschungssicherheit“ des Ausschusses für Forschung, Technologie, Raumfahrt und Technikfolgenabschätzung am 5. November 2025, Deutscher Bundestag

Die Lage im Cyberraum ist von einer hohen Dynamik geprägt. Auch wissenschaftliche Einrichtungen und Organisationen, wie Hochschulen und außeruniversitäre Forschungseinrichtungen mit ihren umfangreichen persönlichen und forschungsbezogenen Datensätzen, sind aufgrund ihrer Bedeutung für das deutsche Innovationssystem attraktive Ziele von Cyberkriminalität und Cyberspionage. Um die Cybersicherheit von Forschungseinrichtungen zu erhöhen, müssen grundlegende Sicherheitsprinzipen konsequent umgesetzt und vorhandene Informations- und Unterstützungsangebote, wie sie etwa das Bundesamt für Sicherheit in der Informationstechnik (BSI) bereitstellt, konsequent wahrgenommen werden. Darüber hinaus braucht es weitere politische Unterstützung für Maßnahmen, wie sie im Rahmen der NIS-2-Umsetzung oder weiterer Gesetzgebungsvorhaben dringend auf den Weg gebracht werden sollten. Von besonderer Bedeutung sind weitere Detektionsbefugnisse zur besseren Angriffserkennung und zur Warnung von Betroffenen, erweiterte Befugnisse zum Schutz vor Phishing-Angriffen, der erweiterte Einsatz von Sensorik über das Regierungsnetz hinaus und die Schließung von IT-Schwachstellen. Eine solche Stärkung der gesamtstaatlichen Sicherheit würde auch zur Steigerung der Resilienz von Forschungseinrichtungen einen wichtigen Beitrag leisten.

1. Die aktuelle Lage im Cyberraum: Ein Überblick[1]

Die Bedrohungslage im Cyberraum ist nach wie vor angespannt und nimmt im Kontext geopolitischer Konflikte und hybrider Angriffe quantitativ und qualitativ weiter zu. Cyberangriffe haben massive Auswirkungen auf Staat, Wirtschaft, Wissenschaft sowie Gesellschaft und damit auf unseren Wohlstand wie auch unsere Sicherheit. Digitale Spionage und Sabotage, Desinformation und Propaganda haben über die Jahre hinweg deutlich zugenommen. Neue Technologien, wie der Einsatz von Künstlicher Intelligenz (KI) für Cyberangriffe oder für sog. Deepfakes, führen zu neuen sicherheitspolitischen Herausforderungen.

Wir erleben eine weiterhin professioneller werdende, arbeitsteilige cyberkriminelle Schattenwirtschaft. Schadprogramme als Dienstleistung (Malware-as-a-Service), also beispielsweise komplette Dienstleistungspakete vom in Umlaufbringen von Schadprogrammen, dem Eindringen in IT-Systeme über die Exfiltration und Verschlüsselung von Daten bis hin zur Abwicklung von Lösegeld- und Provisionszahlungen, sind weiterhin auf

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html

dem Vormarsch. Cyberkriminelle haben international organisierte, arbeitsteilige, hochprofessionelle und hochprofitable Netzwerke und Ökosysteme geschaffen. Wir registrieren eine fortlaufend hohe Anzahl von Angriffen auf die Bundesverwaltung, auf Kritische Infrastrukturen (KRITIS), auf Kommunen und auf Unternehmen aller Größen. Im Fokus von Cyberangriffen stehen ferner politische Institutionen wie Parlamente, Parteien und Stiftungen, aber auch auf Think Tanks.

Die größte Bedrohung stellt nach wie vor der Einsatz von Erpressersoftware (Ransomware) dar. Meist werden die erbeuteten Daten ausgeleitet, im Netzwerk des Opfers verschlüsselt, Teile davon geleakt und im Darknet angeboten. Zudem wird mit ihrer vollumfänglichen Veröffentlichung gedroht (Hack-and-Leak, Hack-and-Publish). Damit soll der Erpressungsdruck auf das Opfer erhöht werden. Derartige Angriffe richteten sich massenhaft gegen kleine und mittlere Unternehmen (KMU) und Kommunen, die meist noch unzureichend geschützt sind und daher aus Sicht von Hackern leichte Ziele darstellen. So waren von einem Cyberangriff auf einen kommunalen IT-Dienstleister Ende Oktober 2023 über 70 kommunale Kunden mit rund 20.000 Arbeitsplätzen betroffen. Die Auswirkungen derartiger Angriffe sind oftmals monatelange Ausfallzeiten bei den Betroffenen. Schätzungen zufolge wurden weltweit 1,1 Milliarden US-Dollar Lösegeld durch Ransomware-Attacken erzielt. Die Dunkelziffer dürfte vermutlich sehr viel höher liegen.

Im Jahr 2024 wurden außerdem täglich rund 300.000 neue Schadprogrammvarianten bekannt. Das BSI erfasste zudem täglich im Durchschnitt über 20.000 infizierte IT-Systeme und meldete sie an deutsche Provider. Ein großes Problem stellen IT-Schwachstellen dar. Im Berichtszeitraum 2024 wurden täglich im Durchschnitt 78 neue Schwachstellen in Softwareprodukten bekannt. Schwachstellen, insbesondere solche, für die es (noch) keine Schließmöglichkeit gibt, stellen ein großes Sicherheitsrisiko für IT-Systeme dar. Das Wissen um solche Einfallstore ist bei Hackern folglich heiß begehrt. Es besteht zudem das Risiko, dass staatliche Akteure aus dem Ausland solche Einfallstore nutzen könnten, um diese bei einer weiteren Eskalation mit dem Ziel der Sabotage auszunutzen. Eine hohe Gefahr geht außerdem von immer professioneller durchgeführten Phishing-Kampagnen aus, bei der sensible Zugangsdaten erlangt und für maliziöse Zwecke missbraucht werden.

Cyberangriffe führen zu immensen volkswirtschaftlichen Schäden. Nach Schätzungen des Branchenverbandes Bitkom belaufen sie sich im Jahr 2025 für die deutsche Wirtschaft auf rund 202,4 Milliarden Euro. Im Jahr 2024 waren es noch 178,6 Milliarden Euro gewesen. Das sind somit fast 24 Milliarden Euro mehr. Seit Jahren zeigt sich eine steigende Tendenz[2]. Um sich diese Zahlen zu vergegenwärtigen, lohnt sich der folgende Vergleich: Der Bundeshaushalt 2025 hat ein Gesamtvolumen von 502,5 Milliarden Euro. Wir haben es somit mit einer erheblichen Summe zu tun.

Angriffe im Cyberraum gehen insbesondere von staatlichen und staatsnahen Akteuren, wie APT-Gruppierungen (Advanced Persistent Threats), und finanziell motivierten Kriminellen aus. Ernstzunehmende Akteure sind ferner Hacktivisten, die in erster Linie politisch-propagandistische Zwecke verfolgen und hierzu meist auf Distributed-Denial-of-Service

[2] https://www.bitkom.org/Presse/Presseinformation/Russland-China-deutsche-Wirtschaft-Visier

(DDoS)-Angriffe zur vorübergehenden Lahmlegung von Websites setzen. In Deutschland sind nach Erkenntnissen des BSI über 25 verschiedene APT-Gruppen aktiv.

Der Verfassungsschutzbericht 2024 nennt als Hauptakteure gegen Deutschland gerichteter Spionage einschließlich nachrichtendienstlich gesteuerter Cyberangriffe insbesondere die Russische Föderation, die Volksrepublik China und die Islamische Republik Iran[3].

Im Kontext hybrider Bedrohungen und geopolitischer Konflikte, die wir insbesondere seit dem Beginn des russischen Angriffskrieges gegen die Ukraine in deutlich verschärfter Form erleben, verschwimmen die Grenzen zwischen wirtschaftlich und politisch motivierter Cyberaggression zusehends. Denn ein Ransomware-Angriff auf einen Energieversorger mit Lösegelderpressung verursacht nicht nur massive wirtschaftliche Schäden, sondern dient auch gezielt der Sabotage, um Unsicherheit und Chaos zu verursachen[4]. Der Cyberraum hat sich zu einem zentralen Austragungsort hybrider Angriffe (Cyber Conflict), zu einem Hotspot von Kriminellen (Cyber Crime), aber auch zu einer Sphäre technologischer Abhängigkeiten (Cyber Dominance) entwickelt.

Deutschland setzt der Bedrohung eine tragfähige Cybersicherheitsarchitektur entgegen. In Kooperation mit internationalen Partnern sind bereits Erfolge bei der Eindämmung von Schadprogrammen erzielt worden. Wir sind Cyberangriffen nicht schutzlos ausgeliefert. Mit der breiten Expertise seiner Mitarbeitenden konnte das BSI maßgeblich dazu beitragen, Bedrohungen frühzeitig zu entdecken, vor ihnen zu warnen und Hilfestellungen und Lösungen zur Verfügung zu stellen. Mithilfe seiner Sensorik spürte das BSI beispielsweise Botnetze durch Sinkholing auf und unterstützte damit auch bei der Strafverfolgung. Weltweit führten die zuständigen Behörden zahlreiche Takedowns gegen Botnetze cyberkrimineller Angreifergruppen durch.

Das BSI beobachtet die Lage der Cybernation Deutschland in den fünf Dimensionen Bedrohung, Angriffsfläche, Gefährdung, Schadwirkung und Resilienz, wobei die Resilienz den vier anderen Dimensionen positiv entgegenwirkt. Trifft eine Bedrohung, etwa ein Schadprogramm, auf eine Angriffsfläche, zum Beispiel einen Webserver, entsteht eine Gefährdung. Dringt das Schadprogramm durch, wirkt sich das negativ aus, zum Beispiel wenn Daten abfließen. Um Schadwirkungen möglichst abwehren zu können, ist eine ausgeprägte Resilienz notwendig. **In wenigen Tagen erscheint der neue Bericht des BSI zur Lage der IT-Sicherheit 2025**.

2. Risiken für Hochschulen und außeruniversitäre Forschungseinrichtungen im Cyberraum

Hochschulen und außeruniversitäre Forschungsorganisationen sind zentrale Säulen des deutschen Forschungs- und Innovationssystems. Sie sind Innovationsantreiber, weltweit vernetzt und leisten einen wesentlichen Beitrag für die Wettbewerbs- und Zukunftsfähigkeit der Bundesrepublik Deutschland und der Europäischen Union (EU). Deutsches Know-how, etwa aus den Bereichen Chemie, Biotechnologie, Maschinenbau, Luft- und Raumfahrt sowie Medizin genießt international einen hervorragenden Ruf und ist weltweit gefragt. Die

[3] https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/verfassungsschutzberichte/2025-06-10-verfassungsschutzbericht-2024.html

[4] https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Blog/Cyberaggression_250216.html

deutschen Forschungseinrichtungen verfügen über umfangreiche Forschungs- und Entwicklungsdaten mit teils sensiblen Inhalten, komplexe Forschungsanlagen und Laborausstattung, Rechenzentren und zunehmend auch Bibliotheksclouldsysteme. Zudem sind auf den Servern viele personenbezogene Daten über Forschende, Studierende und Verwaltungspersonal sowie inländische und ausländische Kooperationspartner gespeichert. Diese Fülle an Daten und Informationen macht deutsche Hochschulen und Forschungseinrichtungen zu hochattraktiven Zielen für Cyberkriminelle, die Geld erpressen oder persönliche Daten für weitere kriminelle Zwecke stehlen wollen, aber auch für staatliche Akteure wie fremde Nachrichtendienste, die sich für sensibles technologisches Know-how, Forschungsergebnisse oder auch für Dissidenten und missliebige Forschende interessieren. Im Kontext der sicherheitspolitischen Zeitenwende, die zu einem Aufschwung der sicherheits- und verteidigungsbezogenen Forschung in der deutschen Wissenschaftslandschaft führen könnte, dürfte sich das Interesse fremder Mächte an deutschem Know-how noch steigern. Zunehmend stehen bei bestimmten Angreifergruppen auch politische Motive im Vordergrund.

Um Zukunftstechnologien wie Künstliche Intelligenz, Quantentechnologien, die Mobilfunkgeneration 6G, Halbleiter- oder Cloudtechnologien ist international ein harter Wettlauf im Gange. Eine besondere Dimension erreicht dieser Umstand vor dem Hintergrund zunehmender geopolitischer Rivalitäten und damit verbundener technologischer Abhängigkeiten. Wissenschaftliche Fortschritte in den genannten Bereichen und der erfolgreiche Innovationstransfer in den Markt können einen entscheidenden Beitrag zur digitalen Souveränität und zur internationalen Wettbewerbsfähigkeit leisten.

Deutschlands Wissenschaftslandschaft steht immer stärker im Fokus von Cyberangriffen. Cyberangriffe sind aus Sicht von Hackern ein effektives Instrument, um an sensibles Wissen und persönliche Daten zu gelangen. Sie stellen daher eine erhebliche Bedrohung für unsere Wissenschaft, Wirtschaft und Sicherheit dar. Und sie führen mitunter zu gravierenden finanziellen (Folge)Schäden, etwa durch Kosten für IT-Krisenmanagement und IT-Neubeschaffungen oder Wiederherstellung der Arbeitsfähigkeit der Verwaltung, aber auch zu Reputationsschäden.

Aufgrund ihrer Größe und Heterogenität, komplexer und weitverzweigter IT-Infrastrukturen, fehlender oder unzureichender Trennung zwischen privater und institutioneller IT, der Vielzahl an Schnittstellen, aber auch unterschiedlich ausgeprägter IT-Kompetenzen von Personal und Studierenden, sind wissenschaftliche Einrichtungen in hohem Maße verwundbar. Hinzu kommt der internationale Vernetzungsgrad, hier insbesondere auch Partnerschaften zu wissenschaftlichen Einrichtungen in Staaten mit autoritären Systemen. Hochschulen und außeruniversitäre Forschungseinrichtungen befinden sich in einem starken Spannungsverhältnis zwischen Wissenschaftsfreiheit und Offenheit einerseits und Sicherheitserfordernissen andererseits.

Hochschulen sind sich der Bedeutung des Themas digitale Sicherheit offenbar durchaus bewusst. Laut dem Hochschul-Barometer des Stifterverbandes und der Heinz Nixdorf-Stiftung (2024) sehen 97,3% der Hochschulleitungen das Risiko durch Cyberangriffe insgesamt als groß oder eher groß an. Allerdings wird das Thema nur von einem Bruchteil von ihnen als „Chefinnen- oder Chefsache“ behandelt. Bei vielen Hochschulen mangelt es außerdem an

Sensibilisierungsmaßnahmen und Schulungsangeboten für Personal und Studierende sowie an IT-Notfallplänen[5].

3. Erkenntnisse und Unterstützungsleistungen des BSI

Das BSI hat Kenntnis von mehreren mutmaßlich Geschädigten aus Deutschland aus den Sektoren Bildung und Forschung, welche auf Leak-Seiten von Angreifern zum Zweck der Erpressung genannt wurden. Seit Beginn der Erfassung von Nennungen auf Leak-Seiten im Jahr 2019 wurden 28 mutmaßlich Geschädigte aus diesen Sektoren Deutschland zugeordnet. Weltweit wurden über 1.000 mutmaßlich Geschädigte aus den Sektoren Bildung und Forschung erfasst.

Insbesondere in englischsprachigen Ländern konnten wiederholt Angriffswellen gegen Bildungseinrichtungen zu Beginn von Semestern und Schulhalbjahren beobachtet werden. Dies geht wahrscheinlich auch auf eine andere Form der Finanzierung der Einrichtungen über beispielsweise Stiftungen statt über die Öffentliche Hand zurück. Eine Einrichtung der Öffentlichen Hand zahlt in der Regel kein Lösegeld, wohingegen eine anderweitig finanzierte Institution eher zur Zahlung bereit ist bzw. zahlt.

Öffentlich bekannte Vorfälle des Jahres 2024 waren unter anderem Angriffe auf das Fraunhofer-Institut für Arbeitswirtschaft und Organisation (Ransomware), die Hans-Böckler-Stiftung (Ransomware), die Berliner Hochschule für Technik (Ransomware) oder die Universität der Bundeswehr München (Datenabfluss).

Als letztes Jahr der zentrale Server der Berliner Hochschule für Technik (BHT) durch die Ransomware-Gruppe Akira heruntergefahren und teilweise verschlüsselt wurde, betraf das tausende Menschen. Die Verwaltung war lahmgelegt, wichtige IT-Projekte wurden bis zu drei Monate unterbrochen, die Arbeitsfähigkeit von Forschenden war mehrere Monate beeinträchtigt. Der Schaden lässt sich schwer beziffern, auch bei der Reputation. Die Hochschule selbst nimmt an, dass darunter sogar die Zahl der neu eingeschriebenen Bachelor- und Masterstudierenden im Sommersemester gelitten haben könnte, was sich indirekt auch auf den Haushalt der Hochschule ausgewirkt habe. Als Problem erwies sich die Zahl unbesetzter Stellen beim IT-Rechenzentrum. Positiv war das schnelle Handeln der Hochschule und die Erkenntnis, dass es zukünftig klarerer organisatorischer und strengerer technischer Maßnahmen zur Erhöhung der Cyberresilienz bedürfe[6].

Dem BSI liegt kein umfassender Gesamtüberblick zu Cyberangriffen auf Hochschulen und Wissenschaftseinrichtungen innerhalb der EU oder weltweit vor. Öffentlich zugängliche Berichte und Pressemeldungen zeigen jedoch, dass Cyberangriffe auf Hochschulen und Forschungseinrichtungen ein weltweites Phänomen sind[7]. Im Vereinigten Königreich waren nach Angaben der Regierung in diesem Jahr mehr als 90% der 32 befragten Universitäten (higher education institutions) Ziel von Cyberangriffen. Es wird insgesamt eine hohe

[5] https://www.hochschul-barometer.de/2024/digital
[6] https://www.bht-berlin.de/fileadmin/oe/hrz/akira-post-mortem.pdf
[7] https://konbriefing.com/en-topics/cyber-attacks-universities.html

Betroffenheit von Bildungseinrichtungen festgestellt[8]. Das European Repository of Cyber Incidents (EuRepoC), eine von einem europäischen Forschungskonsortium betriebene Datenbank, listet für die EU-Mitgliedstaaten zwischen dem 01.01.2000 und dem 31.10.2025 49 Vorfälle im Sektor „Research“ und 25 im Sektor „Science“ auf. Für Deutschland weist die Datenbank 16 Vorfälle im Bereich „Research“ und sieben im Bereich „Science“ aus[9].

Das BSI war in den vergangenen Jahren in unterschiedlicher Form an der Unterstützung von Forschungseinrichtungen bei der Vorfallsbearbeitung beteiligt. Insbesondere im Zusammenhang mit Ransomware-Vorfällen wurden verschiedene Hilfsdokumente und Handreichungen bereitgestellt, die auch von Forschungseinrichtungen im Bereich der IT- und Krisenbewältigung genutzt werden konnten. Darüber hinaus steht das BSI, insbesondere über CERT-Bund, in regelmäßigem Austausch mit dem DFN-CERT, um relevante Informationen und Erfahrungen zu teilen.

Im Rahmen der COVID-19 Pandemie war das BSI zudem unmittelbar in die Unterstützung einer Forschungseinrichtung bei der Bewältigung eines konkreten Sicherheitsvorfalls eingebunden. Ferner wurden Sensibilisierungsmaßnahmen durchgeführt, insbesondere gegenüber außeruniversitären Forschungseinrichtungen. Auch hat das BSI externe Hinweismeldungen zu Cyberkampagnen ausgewertet und an verschiedene Universitäten und Forschungseinrichtungen weitergeleitet.

In einer vom HIS-Institut für Hochschulentwicklung (HIS-HE) erstellten und Anfang Oktober 2025 veröffentlichten Studie wurden erstmals die Cybersicherheit an deutschen Hochschulen, rechtliche Rahmenbedingungen und die Situation in den 16 Bundesländern (Aktivitäten, Programme, Maßnahmen, Akteure) untersucht. Die Untersuchung offenbart ein recht heterogenes Bild, etwa hinsichtlich ministerieller und behördlicher Zuständigkeiten, Strukturen und Unterstützungsleistungen[10].

Hochschulen fallen gemäß Föderalismusprinzip in den Kompetenzbereich der Bundesländer. Dazu zählt auch die Abwehr von Cyberangriffen auf wissenschaftliche Einrichtungen. Im Gegensatz zur Bundesverwaltung und zu Kritischen Infrastrukturen unterliegen Hochschulen keiner Meldeplicht gegenüber dem BSI oder anderer Bundesbehörden. Gleiches gilt für außeruniversitäre Forschungseinrichtungen. Diese sind rechtlich selbstständig. Es gibt kein zentrales Meldesystem für IT-Sicherheitsvorfälle auf Bundes- oder Landesebene. Es gibt keine vollständige, systematische Dokumentation mit Angaben zur Art eines Angriffs, zu Tätergruppierungen, zur Zielrichtung (z. B. Spionage, Sabotage), Schadensausmaß und -höhe, zu Folgeerscheinungen und -kosten oder Maßnahmen zur und Beteiligte an der Vorfallsbewältigung. Somit existiert kein bundes- oder länderübergreifendes Gesamtlagebild zu Cyberattacken auf Hochschulen und Forschungseinrichtungen.

Forschungseinrichtungen fallen grundsätzlich unter die NIS-2-Richtlinie der EU – der Entwurf des **„Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“** befindet

[8] https://www.universitiesuk.ac.uk/sites/default/files/uploads/UUKi%20reports/279%20FINAL%20-%20Cyber%20Security%20and%20Universities%20(002).pdf
[9] https://eurepoc.eu/de/dashboard-de/
[10] https://his-he.de/publikationen/cybersicherheit-an-hochschulen-foederale-ansaetze-und-gemeinsame-wege/

sich gerade im parlamentarischen Gesetzgebungsverfahren. Gemäß Anlage 2 zählen Forschungseinrichtungen zu den „wichtigen Einrichtungen“. Das bedeutet, dass Forschungseinrichtungen Registrierungs-, Melde- und Nachweispflichten gegenüber dem BSI unterliegen und sie angemessene Maßnahmen zum Schutz ihrer IT-Systeme ergreifen müssen.

§ 2 Nr. 12 BSIG-E definiert „Forschungseinrichtung“ als „eine Einrichtung, deren primäres Ziel es ist, angewandte Forschung oder experimentelle Entwicklung im Hinblick auf die Nutzung der Ergebnisse dieser Forschung für kommerzielle Zwecke durchzuführen; Bildungseinrichtungen gelten nicht als Forschungseinrichtungen“. Damit sind Universitäten ausgeklammert, ebenso außeruniversitäre Forschungseinrichtungen, die primär Grundlagenforschung betreiben, wie u.a. die Max-Planck-Gesellschaft und viele Mitglieder dieser Gesellschaften. Erfasst wären hingegen etwa die Fraunhofer Gesellschaft und weitere anwendungsorientiere Einrichtungen, sowie einzelne Mitglieder der großen Forschungsgesellschaften[11]. Unternehmen, „die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel nach § 2 AMG ausüben“, gehören gemäß Anlage 1 des BSIG-E zu den „Sektoren besonders wichtiger und wichtiger Einrichtungen“ (Gesundheit) mit entsprechend höheren Auflagen.

4. Produkte und Angebote des BSI zur Erhöhung der Cybersicherheit

Cybersicherheit an wissenschaftlichen Einrichtungen muss Chefinnen- und Chefsache, d.h. ein Top-Thema auf Leitungsebene und Teil einer übergeordneten Strategie sein. Hierbei gilt es organisatorische, materielle und personelle Sicherheitsaspekte zu berücksichtigen. Cybersicherheit ist nicht nur als IT-Thema und damit als ausschließliche Angelegenheit der IT-Abteilung, sondern als Baustein des organisationsweiten Risikomanagements zu verstehen. Für ein funktionierendes Krisenmanagement braucht es ein organisationsweites Bewusstsein für Cybersicherheit und die Benennung klarer Verantwortlichkeiten auf Leitungsebene.

Aus Sicht des BSI wäre es zu begrüßen, wenn die zuständigen Ministerien der Länder entsprechende Unterstützungsstrukturen und Mittel bereitstellen und den institutionellen Rahmen für die Hochschulen entsprechend gestalten würden.

Der Schutz vor Cyberangriffen beginnt bereits mit der Prävention. Hierzu gehört die Vorbereitung auf einen möglichen Hackerangriff. Denn die Frage ist nicht mehr ob, sondern wann man Ziel eines Hackerangriffs wird. Von zentraler Bedeutung ist die Etablierung eines Risiko- und Notfallmanagements. Dazu zählen der Aufbau eines Informationssicherheitsmanagementsystems (ISMS) und eines Business Continuity Managements (BCM). Ein effektives BCM umfasst die Entwicklung von Notfallplänen sowie den Auf- und Ausbau von Notfallkommunikation und Notprozessen.

Die Funktionsfähigkeit des Krisenmanagements sollte durch regelmäßige Übungen zur Krisenbewältigung getestet und gesichert werden. Daneben braucht es eine regelmäßige Überprüfung der IT-Infrastruktur auf Schwachstellen. Von zentraler Bedeutung ist darüber

[11] https://dip.bundestag.de/vorgang/gesetz-zur-umsetzung-der-nis-2-richtlinie-und-zur-regelung-wesentlicher-grundz%C3%BCge/324803

hinaus die Bereitstellung von Informationsmaterialien und regelmäßigen, gegebenenfalls auch verpflichtenden Schulungsangeboten zur IT-Sicherheit für Verwaltungsmitarbeitende, Forschende und Studierende.

Das BSI steht zu allen Fragen der Cyber- und Informationssicherheit beratend und unterstützend zur Seite. Ferner gibt es speziell auf die Anforderungen und Bedürfnisse von Hochschulen entwickelte Produkte:

Mit dem **IT-Grundschutz** und dessen **Weiterentwicklung zum Grundschutz++** bietet das BSI einen Standard für alle Organisationen an, mit dem Cybersicherheit einfach und effektiv umgesetzt werden kann. Der IT-Grundschutz ist Methode, Anleitung, Empfehlung und Hilfe zur Selbsthilfe für Behörden, Unternehmen und Institutionen, die sich mit der Absicherung ihrer Daten, Systeme und Informationen befassen wollen. Dabei wird ein ganzheitlicher Ansatz zur Informationssicherheit verfolgt. Es werden technische, infrastrukturelle, organisatorische und personelle Aspekte betrachtet[12]. Der IT-Grundschutz wird kontinuierlich fortentwickelt. Derzeit läuft der Prozess zur Fortentwicklung zum Grundschutz++[13]. Fester Bestandteil des IT-Grundschutzes sind ferner die **BSI-Standards 200-1 bis 200-4[14].** Sie enthalten Empfehlungen zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen zu unterschiedlichen Aspekten der Informationssicherheit:

- 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

Speziell für Hochschulen wurde das **IT-Grundschutzprofil für Hochschulen (Version 2022.0.0)** entwickelt. Es wurde vom Arbeitskreis Informationssicherheit des Vereins „Zentren für Kommunikationsverarbeitung in Forschung und Lehre e.V. (ZKI) im Rahmen seiner Mitgliedschaft in der Allianz für Cybersicherheit und mit Unterstützung des BSI erarbeitet. Es soll Hochschulen bei der Erstellung eines Informationssicherheitskonzepts auf Basis des IT-Grundschutz unterstützen[15].

In einem Folgeprojekt hat der ZKI in Zusammenarbeit mit dem BSI ein **BCM-Profil für Hochschulen (Community Draft 2025.0.0)** erarbeitet. Es bietet Hochschulen eine Anleitung zum Aufbau eines Business Continuity Management (BCM). Ziel ist die Etablierung eines Notfall- und Krisenmanagements, um bei einem Schadensfall handlungsfähig zu bleiben und so rasch wie möglich zum Normalbetrieb zurückkehren zu können[16].

[12] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html
[13] https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/BSI_Dialog_IT-GrundschutzPlusPlus_250606.html
[14] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html
[15] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Hochschulen.html
[16] https://ak-itsm-share.zki.de/s/mSJQakxzB7jzqYe?dir=/&editing=false&openfile=true

Für den Fall akuter Sicherheitsvorfälle hält das BSI **aktuelle Listen qualifizierter Dienstleister zur DDoS-Mitigation und zur APT-Response** bereit[17].

Ein umfangreiches Informationsangebot bietet die von BSI und Bitkom ins Leben gerufene **Allianz für Cybersicherheit (ACS)** mit ihren mittlerweile über 8.600 Mitgliedsunternehmen und -organisationen. Die ACS umfasst ein Online-Informationspool, diverse Veranstaltungsformate und Angebote von Partnern zur Kompetenzerweiterung. Es handelt sich um das größte Netzwerk für IT-Sicherheit in Deutschland[18].

Zu NIS-2 bietet das BSI neben einer **Betroffenheitsprüfung**[19] **zahlreiche Hilfestellungen und Angebote für die Vorbereitung der Umsetzung der NIS-2-Richtlinie**[20].

5. Empfehlungen zur Erhöhung der Cybersicherheit

In seiner Stellungnahme zur Öffentlichen Anhörung des Innenausschusses (13. Oktober 2025) zum Entwurf eines „Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ hat das BSI eine Reihe von Maßnahmen zur Erhöhung der gesamtstaatlichen Cybersicherheit genannt, die im Rahmen des parlamentarischen Verfahrens oder anderer Gesetzgebungsvorhaben in dieser Legislaturperiode umgesetzt werden könnten [21]**.** Eine solche Stärkung der gesamtstaatlichen Sicherheit würde auch zur Steigerung der Resilienz von Forschungseinrichtungen einen wichtigen Beitrag leisten. Hierzu braucht es politische Unterstützung.

5.1. Erweiterte Befugnis zur Messung der Resilienz deutscher IT-Systeme und Detektion von Angreifer-Infrastrukturen

Derzeit darf das BSI Messungen zu einer Verwundbarkeit aufgrund öffentlich bekannter Schwachstellen bei öffentlich erreichbaren IT-Systemen (Resilienz-Messungen) nur in einem sehr eingeschränkten Bereich durchführen (v.a. Einrichtungen des Bundes, kritische Infrastrukturen, große digitale Dienste und Unternehmen im öffentlichen Interesse).

Das BSI sollte analog zur Mehrheit der europäischen Staaten ebenfalls zu Resilienz-Messungen für alle im deutschen IP-Raum erreichbaren IP-Adressen befugt sein. Ziel ist die Warnung der Betroffenen, damit diese möglichst zeitnah Schutzmaßnahmen ergreifen können. Die Warnung der Betroffenen sollte dadurch erfolgen, dass das BSI befugt ist, Provider zur entsprechenden Information ihrer Kundinnen und Kunden anzuweisen. Angreifer

[17] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Qualifizierte-Dienstleister/qualifizierte-dienstleister_node.html
[18] https://www.allianz-fuer-cybersicherheit.de
[19] https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Betroffenheitspruefung/nis-2-betroffenheitspruefung_node.html
[20] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Management_Blitzlicht/Management_Blitzlicht_NIS-2.pdf?__blob=publicationFile&v=4
[21] https://www.bundestag.de/resource/blob/1114918/21-4-069-Stellungnahme-BSI-NIS-2-Richtlinie-21-1501.pdf

scannen den kompletten IP-Raum regelmäßig auf Verwundbarkeiten. Ziel muss es sein, ihnen zuvorzukommen.

Ergänzend dazu sollte das BSI Befugnisse zur Detektion von Angreifer-Infrastrukturen erhalten. Die Dunkelziffer von Systemen, die durch staatliche Angreifer kompromittiert werden, ist hoch. Eine besondere Bedrohung sind Prepositioning-Angriffe. Hierbei wird Schadsoftware installiert, aber nicht aktiv genutzt, sondern für den Einsatz in einem eskalierenden Krisenfall zu Sabotagezwecken vorgehalten. Da die Schadsoftware bis zum Eintritt des Krisenfalls nicht aktiv ist, ist sie schwieriger zu erkennen. Das BSI hat aktuell keine Möglichkeit, seine Kenntnis über Angreifer und deren Werkzeuge außerhalb der Regierungsnetze einzusetzen.

Technisch ist es möglich, Angreiferserver zu identifizieren. Dies geschieht anhand bestimmter Indikatoren, etwa anhand eines bestimmten Kommunikationsverhaltens bei Command-and-Control-Server-Servern. Auf diese Weise könnte das BSI Prepositioning-Schadsoftware finden, bevor sie zum Einsatz kommt. Das BSI sollte daher in die Lage versetzt werden, im Internet nach Systemen zu suchen, die aktiv für Angriffe genutzt werden.

5.2. Ausweitung der Befugnisse gegenüber Diensteanbietern und verbesserter Schutz vor Phishing-Angriffen

Die in § 16 des neuen BSIG geregelten Befugnisse des BSI reichen insgesamt nicht aus, um einen flächendeckenden Schutz vor Cyberkriminellen zu ermöglichen.

Danach dürfen – wie auch schon nach der aktuellen Rechtslage – weiterhin nur Telekommunikations-Anbieter mit mehr als 100.000 Kunden adressiert werden; regionale Internet Service Provider, Universitäten, Content-Anbieter und DNS-Anbieter sind nicht einbezogen. Weiterhin erfasst die Regelung Phishing- und andere schädliche Webseiten, von denen für Wirtschaft und Gesellschaft erhebliche Gefahren im Alltag ausgehen, nicht hinreichend.

Zum anderen sollte zur Verbesserung des Schutzes vor Phishing-Angriffen eine explizite Befugnis des BSI ergänzt werden, Informationen über Phishing-Domains zu sammeln, zu verifizieren und bereitzustellen. Telekommunikations-Anbieter sollten verpflichtet werden, eigene Erkenntnisse in diese Datenbank einzubringen, selbst Informationen abzurufen und ihren Kunden zumindest optional einen DNS-basierten Schutz zur Verfügung zu stellen.

Ferner sollte es dem BSI für einen schnellen und effektiven Schutz der Betroffenen erlaubt werden, mit Unterstützung der Provider Bereinigungsbefehle selbst an kompromittierte IT-Systeme zu senden. Aktuell dürfen dies nach § 7 c Absatz 1 Satz 1 Nummer 2 BSIG nur die Telekommunikations-Provider selbst. In der Regel erfolgt aber zuvor schon eine Umleitung des Datenverkehrs auf Server des BSI nach § 7 c Absatz 3, um den Datenverkehr analysieren zu können. Während der Umleitung können Diensteanbieter keine Bereinigungsbefehle mehr versenden.

Darüber hinaus bestehen außerdem noch Regelungslücken bei der Bekämpfung von Botnetzen, die eine der größten Gefahren für die Cybersicherheit darstellen. Botnetze werden von Cyber-Kriminellen etwa zur Verbreitung von Schadprogrammen, für

Informationsdiebstahl, zum Versand von Spam-Nachrichten oder zur Durchführung von DDoS-Angriffen eingesetzt. Das BSI setzt seit mehreren Jahren erfolgreich Maßnahmen zur Abwehr von Botnetzen um, darunter auch die Umleitung von Domainnamen durch Internetprovider. Dies muss auf Domainregistrare ausgeweitet werden, um zu ermöglichen, dass die Botnetze nicht nur teilweise, sondern vollständig entschärft werden.

5.3. Sensorik zur Detektion auch außerhalb des Regierungsnetzwerkes ermöglichen

Bislang beziehen sich die Detektionsmöglichkeiten des BSI ausschließlich auf die eigene Sensorik im Regierungsnetz. Mangels Rechtsgrundlage existiert keine BSI-Sensorik außerhalb der Regierungsnetze, weshalb Meldungen der Unternehmen an das BSI prozessbedingt erst verspätet (nach Entdecken und Bewerten des Vorfalls) und nicht flächendeckend erfolgen. Dadurch gehen viele wichtige Informationen aus unternehmensbezogenen Angriffserkennungssystemen verloren. Manuelle Meldungen von Unternehmen müssen perspektivisch und zunehmend um automatisierte Datenströme ergänzt werden, um Lagebilder, Bewertungen und Maßnahmen in Echtzeit zu ermöglichen.

Es sollten daher die erforderlichen gesetzlichen Voraussetzungen geschaffen werden, dem BSI die automatisierte Entgegenahme und Verarbeitung von Informationen aus Angriffserkennungssystemen bei Unternehmen (z. B. KRITIS-Betreibern, besonders wichtigen und wichtigen Unternehmen) zu ermöglichen.

5.4. Schwachstellen schließen und IT-Sicherheitsforschende stärken

Für das BSI sind Schwachstellenmeldungen von Sicherheitsforschenden und weiteren Privatpersonen von erheblicher Bedeutung. Meldungen setzen das Vertrauen in das BSI voraus. Derzeit haben Meldende oft Sorge, dass das BSI Schwachstellen zurückhalten könnte. Hinzu kommt die Angst vor einer möglichen Strafverfolgung. Aus fachlicher Sicht des BSI sollten Sicherheitslücken grundsätzlich an die betroffenen Hersteller gemeldet werden, damit diese möglichst schnell geschlossen werden.

Das BSI sieht die dringliche Notwendigkeit, Rechtssicherheit für Forschende im Bereich der IT-Sicherheit herzustellen. Nach derzeitiger Rechtslage machen sich IT-Sicherheitsforschende strafbar, auch wenn das von ihnen verfolgte Ziel – die Aufdeckung von Sicherheitslücken und ihre Schließung, um die Cybersicherheit zu fördern – im öffentlichen Interesse liegt.

Aus Sicht des BSI leisten IT-Sicherheitsforschende einen wichtigen Beitrag zur Cybersicherheit. Meldende sollten daher durch gesetzliche Klarstellungen im Computerstrafrecht von einer Sorge vor Strafverfolgung befreit werden („Hackerparagraph“). Ein transparentes, rechtssicheres Verfahren führt zu mehr Meldungen und damit zu mehr Cybersicherheit in Deutschland.

***