Empfehlung der
40. Mitgliederversammlung der
HRK
am 13. Mai 2025
in Magdeburg

Handlungsdruck für Hochschulen, Länder und Bund – HRK-Empfehlungen zur Cybersicherheit

HRK Hochschulrektorenkonferenz
Die Stimme der Hochschulen

Leipziger Platz 11 | Tel.: 030 206292-0 | post@hrk.de
10117 Berlin | Fax: 030 206292-15 | www.hrk.de

Ahrstraße 39 | Tel.: 0228 887-0 | post@hrk.de
53175 Bonn | Fax: 0228 887-110 | www.hrk.de

Inhaltsverzeichnis

Zusammenfassung
Die allgemeine Bedrohungslage für die Hochschulen wird von den Sicherheitsbehörden im Bereich der Cybersicherheit als extrem hoch bewertet. Aktuell können insbesondere folgende Szenarien unterschieden werden: Ransomware-Angriffe, Spionage und die Ausspähung von dissidentischen Netzwerken sowie sozialen Bewegungen. Bei diesen Bedrohungsszenarien kommt auch zunehmend Künstliche Intelligenz (KI) zum Einsatz.

Der Ausgleich zwischen Resilienz, Offenheit und digitaler Souveränität ist für die Hochschulen vor dem Hintergrund drohender Cyberangriffe eine besondere Herausforderung. Doch es gibt dafür auch Lösungsansätze und -strategien. Um diese zu entwickeln und umzusetzen, richtet die HRK nachfolgende Empfehlungen an die Hochschulen, die Länder und den Bund:

Die HRK empfiehlt den *Hochschulen*, die Aufgaben der Aufrechterhaltung des IT-Hochschulbetriebs und der Sicherung besonders schützenswerter Daten durch Konzepte abgestufter Sicherheit wahrzunehmen. Diese Konzepte müssen Prävention, Notfallpläne und Übungen umfassen, die auch mit Hilfe von Kooperationen und Beratungen erfolgen können. Bei der Vermittlung von Cybersicherheitspraktiken kommt den Hochschulen eine besondere Verantwortung zu.

Die HRK-Empfehlungen an die *Länder* betreffen die Etablierung von hochschulübergreifenden Strukturen. Meldewege und Ansprechpersonen müssen benannt sowie die Sensibilisierung für das Thema und die Weiterbildung ausgeweitet werden. Hierfür sind erhebliche zusätzliche Finanzmittel erforderlich, die auch die Unterstützung des Bundes erfordern.

An den *Bund* gehen die Empfehlungen, entsprechend seiner übergreifenden Rolle bei der Gefahrenabwehr aktiv zu werden. Dies impliziert, Warnsignale zu geben und Reaktionsmöglichkeiten aufzuzeigen, länderübergreifende Kommunikation zu fördern sowie die Forschung zu intensivieren. Im Rahmen der neuen Möglichkeiten zur Erhöhung der Cybersicherheit müssen innovative Finanzierungsmodelle auch in Zusammenarbeit mit den Ländern schnell umgesetzt werden.

I. Aktuelle Sicherheitslage

Vor dem Hintergrund ihrer Empfehlung „Informationssicherheit[1] als strategische Aufgabe der Hochschulleitung“[2] aus dem Jahr 2018 stellt die Hochschulrektorenkonferenz fest, dass ihre an die Hochschulen gerichtete Handreichung im Wesentlichen nach wie vor Geltung hat. Allerdings ist die Empfehlung angesichts der neuen Sicherheitslage nach der sogenannten „Zeitenwende“ neu zu kontextualisieren.[3]

Die Bedrohungslage für die Hochschulen wird von den Sicherheitsbehörden für den Bereich der Cybersicherheit als extrem hoch bewertet. Dies u. a. auch aufgrund des russischen Angriffskriegs auf die Ukraine, der kriegerischen Auseinandersetzungen im Nahen Osten sowie der Spannungen in Ostasien.

Hochschulen sind für potenzielle Angriffe von besonderem Interesse. Gründe hierfür sind z. B. die Personaldaten (hoch)qualifizierter Beschäftigter, die Ergebnisse aus exzellenter Forschung, die Impulse für Innovationen durch Transfer, die internationalen Kooperationen sowie der Bildungsauftrag im Sinne einer demokratischen Gesellschaft. Somit stellt sich grundsätzlich nicht die Frage, ob, sondern wann an den einzelnen Hochschulen welches Schadensereignis eintritt.

Aktuell können insbesondere folgende Bedrohungsszenarien unterschieden werden:

- Ransomware-Angriffe[4]
- Spionage[5]
- Ausspähung von dissidentischen Netzwerken.[6]

Bei diesen Bedrohungsszenarien kommt zunehmend Künstliche Intelligenz (KI) zum Einsatz. Dies gilt auch bei der Herstellung von Desinformation, die durch KI perfektioniert wird: Spam wird „intelligenter", DeepFakes[7] verfälschen in realistisch wirkender Weise Medieninhalte (Bilder, Videos, Stimmen) und als Robocalls[8] werden voraufgezeichnete Nachrichten per Telefonanruf durch computergesteuerte Anrufbeantworter wie von einem Roboter übermittelt.

II. Die Hochschulen im Spannungsfeld zwischen Resilienz, Offenheit und digitaler Souveränität

Die aktuelle Sicherheitslage im Cyberbereich führt dazu, dass sich die Hochschulen in besonderer Weise im Spannungsverhältnis zwischen den Erfordernissen Resilienz, Offenheit und digitaler Souveränität befinden. Resilienz[9] ist das zentrale Konzept der Cybersicherheit. Offenheit[10] ist ein konstitutives Charakteristikum der deutschen Hochschulen. Die digitale Souveränität[11] der Hochschulen muss in der Realität angemessen ausgestaltet werden sowohl hinsichtlich der unterschiedlichen Ausgangsparameter (u. a. Größe, Expertise) als auch der Bedrohungsszenarien. Digitale Souveränität im weiteren Sinne bedeutet daher, dass Hochschulen selbstbestimmt Technologien anhand von Funktionalität, Umsetzungsgeschwindigkeit, Beherrschbarkeit, Sicherheit und Wirtschaftlichkeit auswählen. Zu beachten ist hierbei, dass man sich nicht einseitig von Produkten für die Cybersicherheit abhängig macht, die ggf. durch regulatorische Bestimmungen, z. B. im Hinblick auf Datenschutz, verboten werden. Grundsätzlich ist es hinsichtlich der Vorbereitung auf Cyberangriffe im Sinne der digitalen Souveränität wichtig, intern Fach- und Steuerungskompetenz zu bündeln, klare

Zuständigkeiten zuzuweisen und Regeln für das Zusammenwirken aller Hochschulangehörigen aufzustellen.

Der Ausgleich zwischen Resilienz, Offenheit und digitaler Souveränität stellt angesichts drohender Cyberangriffe eine besondere Herausforderung dar. Die hierfür erforderlichen Abwägungsprozesse kann eine Hochschule nur unter Berücksichtigung ihrer Ausrichtung, ihrer rechtlichen Rahmenbedingungen und nicht zuletzt ihrer zur Verfügung stehenden Ressourcen vollziehen. Einen „für alle Hochschulen gültigen" extern vorgegebenen Masterplan zur Erhöhung der Cybersicherheit gibt es daher nicht.

III. HRK-Empfehlungen zur Cybersicherheit

Vor dem Hintergrund der einleitenden Ausführungen richtet die HRK folgende Empfehlungen an die Hochschulen, die Länder und den Bund.

1. Empfehlungen an die Hochschulen

Basis- und Kernabsicherung definieren

Den Hochschulleitungen stellen sich zwei Hauptaufgaben:

- die Aufrechterhaltung des IT-Hochschulbetriebs und
- die Sicherung besonders schützenswerter Daten.

Daher empfiehlt die HRK den Hochschulen Konzepte abgestufter Sicherheit[12]: Bei der Basisabsicherung ist insbesondere der Aufbau eines individuellen Business Continuity Managements (BCM)[13] zu berücksichtigen, die hochschulweite Einführung einer Zwei-Faktor-Authentifizierung[14] sowie der Einsatz von Funktions-Mailaccounts. Zur Festlegung der Kernabsicherung sind vorab die jeweiligen in besonderem Maße zu schützenden Daten, Informationen und Systeme zu identifizieren.[15] Im Sinne des Konzepts der abgestuften Sicherheit ist somit der Umgang mit dezentralen Einheiten zu prüfen: ob man also das Ziel der eingebundenen Geschlossenheit oder der dezentralen Autarkie anstrebt.

Vorsorgen

Prävention ist wirtschaftlich, weil die Beseitigung eines eingetretenen Schadens weitaus teurer ist als der Vorsorgeaufwand. Ein effektives Instrument ist das Scannen von Schwachstellen. Veraltete Hard- und Software, z. B. in Laboren (Messgeräte oder Steuerrechner mit alten Betriebssystemen), für die keine Updates mehr vorgenommen werden können, müssen zunächst (teil-)isoliert und dann mit nachhaltiger Ersatzplanung ausgetauscht werden. Zu prüfen ist weiterhin das Risiko durch spezielle (eigen-)entwickelte Software. Ebenfalls gilt es, für alle zentralen Daten und Systeme Backups und Notfallpläne für die Wiederherstellung verfügbar zu haben. Zur Prävention von Cyberangriffen sind proaktive, regelmäßige Sicherheitsscans ggf. durch Security Operation Center (SOC)[16] möglich.

Den Notfall planen

Im Rahmen eines Business Continuity Managements (BCM) werden Notfallpläne als Kernprozesse der Hochschulen priorisiert,[17] die u. a. auch die Installation einer Notfallhotline bzw. eines Erstkontakts beinhalten.[18] In diesem Zusammenhang sind auch Checklisten oder Notfallkarten hilfreich.[19] Ebenfalls können Rahmenverträge mit Unternehmen als APT-Response Dienstleistungen[20] abgeschlossen werden. Diese Dienstleistungen unterstützen bei der Bewältigung der vielfältigen Aufgaben im Rahmen der Notfallbewältigung und bringen für diese Aufgaben spezielle Expertisen ein, die in dieser Ausprägung an den Hochschulen in der Regel nicht vorhanden sind.

Üben

Cybersicherheitsübungen[21] sollten einen obligatorischen Charakter in Analogie zu Brandschutzübungen erhalten. Hinsichtlich der Vorbereitung, des Aufwandes und des Settings dieser Übungen gibt es verschiedene Trainingsszenarien, die auch bei externen Dienstleistungen angeboten werden: Niederschwellige Formate sind z. B. Planspiele, die sich auch und insbesondere auf Leitungsebene als sehr hilfreich erwiesen haben. Für operativ tätiges Hochschulpersonal kommen neben den niederschwelligen Formaten auch Koordinierungsübungen mit verschiedenen Standorten in Betracht.

Angriffsfläche verringern

Nicht alle Daten müssen zwingend über das Internet öffentlich sichtbar und abrufbar sein. Die Hochschulen sollten daher prüfen, ob und wenn ja wie weniger Daten produziert, gespeichert und öffentlich zugänglich gemacht werden.[22] Schützenswerte Informationen über z. B. IT-Sicherheitsstrukturen oder -maßnahmen sollten nicht öffentlich und/oder auf Social Media (z. B. LinkedIn) zu finden sein, weil dort Ausspähung durch besondere Filter sehr einfach erfolgen kann.

Kooperationen nutzen

Die HRK erneuert ihre Empfehlung für Kooperationen in Sachen Cybersicherheit. IT-Sicherheit ist Teamplay. Kooperationen können sich erstrecken auf Landes- und Verbundkonzepte, Kommunikationskonzepte für Störfälle, Schulungs- und Awareness-Maßnahmen, Erfahrungsaustausch und Einkaufskooperationen, Security Operation Center (SOC)[23], Peer-Audit, Peer-Penetration-Tests und Personal für Computer-Emergency-Response-Teams.[24] Voraussetzung für Kooperationen ist jedoch, dass die Zuwendungsgeber sowohl die Hochschulen zur Kooperation befähigen als auch die Kooperation stimulieren.[25]

Beratung in Anspruch nehmen

In engem Zusammenhang mit Kooperationen stehen Beratungen, die auch als Kooperation mit gemeinnützigen Organisationen (z. B. HIS, DFN, ZKI) ausgestaltet werden können. Rahmenverträge

können hier sehr nützlich sein. Beratung kann sich auch auf die psychologische Begleitung nach Cyberangriffen und Erpressungen erstrecken.

Kommunikationsfähigkeit sichern
Die HRK empfiehlt, die Kommunikation während eines Cyberangriffes durch einen Krisen- und Kommunikationsplan vorzustrukturieren.[26] Dieser sollte u. a. alternative Kommunikationskanäle vorsehen für den Fall, dass wegen des Ausfalls der Systeme plötzlich keine E-Mail-Kommunikation oder auch kein Telefonsystem mehr zur Verfügung steht. Insbesondere die Kommunikation mit Studierenden stellt während eines Angriffs eine Herausforderung dar. Wichtig ist in diesem Fall der präventive Aufbau eines „Schattensystems", das eine schnelle und sichere Kommunikation (z. B. Webseite) ermöglicht.[27]

Cybersicherheitspraktiken vermitteln
Hochschulen müssen auch Awareness und Kompetenzaufbau in Bezug auf Cybersicherheit vermitteln. Diese Maßnahmen gelten für alle Hochschulangehörigen bzw. sind für alle wichtig.[28] In Bezug auf die Studierenden bietet sich an, die Vermittlung von Kompetenzen in Bezug auf Cybersicherheit ins Curriculum zu integrieren. Je nach Hochschulprofil kann auf dieser Grundlage die fachliche Kompetenz und die Exzellenz in der Forschung in relevanten Fächern zur Erhöhung der Cybersicherheit der gesamten Hochschule beitragen.

Cybersicherheit in die Hochschulkultur einbetten
Es muss gelingen, Cybersicherheit als umfassendes gestalterisches und kulturelles Gut zu betrachten.[29] Dazu gehört auch das Praktizieren einer Fehlerkultur. Fehler in Bezug auf Cybersicherheit dürfen nicht als Versagen gewertet werden, sondern als Impuls für das gemeinsame Lernen zur Weiterentwicklung der Cybersicherheit. Anstelle einer falsch verstandenen Scham muss die offene Kommunikation über etwaige Fehler als positives Erlebnis und Ausdruck einer resilienten Hochschulkultur wahrgenommen werden.

2. Empfehlungen an die Länder

Hochschulübergreifende Strukturen etablieren
Die Länder müssen zusammen mit ihren Hochschulen übergreifende Konzepte bzw. Strategien zur Cybersicherheit entwickeln. Übergreifende Konzepte sollten auf bestehenden Kooperationen aufbauen, deren Ausbau durch entsprechende Befähigung und Anreize gefördert werden muss.[30] Bestehende Landesinitiativen können im Rahmen der Zentren für Kommunikation und Informationsverarbeitung (Rechenzentren, ZKI[31]) oder in Anlehnung an Landeseinrichtungen für digitale Hochschullehre[32] errichtet oder ausgebaut werden. Dadurch kann eine kritische Größe für Handlungseinheiten erreicht sowie der Aufbau von Core-IT-Facilities gefördert werden.

Daten hochschulübergreifend sichern
Den Ländern wird empfohlen, eine hochschulübergreifende Datensicherung aufzubauen. Dies kann durch den Aufbau eines Basisdienstes zur Bereitstellung eines kooperativen Betriebsmodells erfolgen. Einzelne ausgewählte Hochschulen oder Einrichtungen können mit Landesmitteln den anderen Hochschulen eine Speicherinfrastruktur zur Verfügung stellen. So können die Hochschulen ihre Daten außerhalb der eigenen Infrastruktur sichern und im Störfall schnell wiederherstellen. Im Hinblick auf betriebskritische Daten insbesondere der Verwaltung kann zusätzlich noch ein getrennter „Datensafe" etabliert werden.[33]

Meldewege und Ansprechpersonen festlegen
Die HRK empfiehlt die Verbesserung von Meldewegen und die eindeutige Benennung von Ansprechpersonen. Nach den ersten Erfahrungen mit Cyberangriffen war oft nicht klar, wer bei den Ministerien und Behörden zu informieren war. Dem muss abgeholfen werden. Bisher war die Unterstützung durch Landesbehörden (z. B.: LKA, Verfassungsschutz) sehr hilfreich. Insbesondere die Informationen der Landesbehörden für Verfassungsschutz waren nützlich, erfolgten aber spät. Dagegen ist wegen der Datenschutzanforderungen die Löschfrist so kurz, dass schnelle und direkte Kommunikations- und Austauschkanäle notwendig sind.

Weiterbildung ermöglichen und durchführen
Die HRK weist darauf hin, dass Cyberangriffe sich extrem dynamisch weiterentwickeln und empfiehlt daher den Ländern die Förderung von entsprechender Weiterbildung für die Hochschulangehörigen. Gefördert werden sollte die Schulung vor Ort, Fortbildungen bei externen Anbietern, aber auch der konzeptionelle Aufbau von wissenschaftlicher Weiterbildung durch die Hochschulen. Eine besondere Vermittlung von Wissen und Kompetenzen zur Cybersicherheit bieten digitale Selbstlernmodule[34], die den üblichen zeitlich flexiblen und Remote-Arbeitsweisen von Hochschulangehörigen entgegenkommen.

Politische Fehlerkultur praktizieren
Analog zur genannten Weiterentwicklung der hochschulinternen Fehlerkultur empfiehlt die HRK das Praktizieren auch einer politischen Fehlerkultur auf Landesebene. Das Feld der Cybersicherheit ist so dynamisch und komplex, dass Fehler auch in der Interaktion zwischen Hochschulen, Behörden und Ministerien nicht ausgeschlossen werden können. Eine politische Fehlerkultur trägt in kritischen Situationen entscheidend dazu bei, dass Fehler identifiziert und schnell behoben werden können.

Grundausstattung verbessern
Die HRK fordert die Länder auf, auch im Hinblick auf die Cybersicherheit eine angemessene Grundausstattung zur Verfügung zu stellen. Zur Erhöhung der Resilienz der IT-Infrastruktur werden Investitionsmittel benötigt, ebenso sind Sachmittel für weitere Hard-

und Software erforderlich. Essentiell für die Erhöhung der Cybersicherheit ist zusätzliches Personal. Fachkräfte für Cybersicherheit werden auf allen Ebenen bis hin zum Chief Information Officer (CIO) gebraucht. Da die Aufrechterhaltung des Know-Hows zur Resilienz eine Daueraufgabe ist, sind unbefristete Stellen erforderlich. Darüber hinaus müssen aufgrund des besonderen Fachkräftemangels im IT-Bereich Stellen neu bewertet oder eine übertarifliche Bezahlung möglich gemacht werden. Derzeit wird nur ein einstelliger Prozentanteil an den IT-Gesamtausgaben für Cybersicherheit verwendet.[35] Um das vom BSI formulierte Ziel zu erreichen, wonach 20 Prozent der IT-Budgets für Cybersicherheit vorgesehen werden sollen,[36] bedarf es einer erheblichen Kraftanstrengung. Diese kann nur mit Unterstützung des Bundes durch innovative Finanzierungsmodelle geleistet werden. (siehe unten)

Forschungsförderung ausweiten
Die HRK empfiehlt den Ländern die Förderung von Forschung zum Thema Cybersicherheit, ggf. zusammen oder in Abstimmung mit dem Bund. (siehe unten)

3. Empfehlungen an den Bund

Gefahren abwehren
Die HRK empfiehlt dem Bund, angesichts der Bedrohungslage entsprechend seiner übergreifenden Rolle in der Gefahrenabwehr noch aktiver zu werden.

Diese Rolle ergibt sich aus der internationalen Dimension der Cybersicherheit. Hier existiert ein Spannungsfeld, da Organisationen aus Wirtschaft und Gesellschaft internationale Kooperation auch mit Staaten betreiben, die nicht die Werte liberaler Demokratien teilen. Dies gilt auch für die globale Wissenschaftskooperation. Bei Angriffen sind Hochschulen ebenso Einfallstore, insbesondere zur Erlangung von Daten über Kooperationspartnerschaften, Transferorganisationen und das gesamte Innovationssystem. Cyberangriffe auf Hochschulen gefährden somit auch die Wettbewerbsfähigkeit der deutschen Wirtschaft.

In der nationalen Dimension besteht in Deutschland in Fragen der Gefahrenabwehr grundsätzlich eine dezentrale Zuständigkeit der Länder. Angesichts der Bedrohungslage ist jedoch auch hier der Bund gefordert, da es länderübergreifende Gefährdungslagen gibt und die Gesamtheit der deutschen Hochschullandschaft durchaus Maßstäbe verdient, die im Falle einer nationalen kritischen Infrastruktur gelten. Darüber hinaus muss es 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.

Warnsignale geben und Reaktionsmöglichkeiten aufzeigen
Der Bund muss helfen, Frühwarnsysteme zu verbessern, sowie mehr Informationen für Reaktionsmöglichkeiten bereitstellen. So sollte z. B. das Bundesamt für Sicherheit in der Informationstechnik (BSI) mehr hochschulspezifische Informationen für eine Notfallplanung und Dienstleistungen anbieten. Auch ein bundesweiter Service zur Auffindung von Sicherheitslücken erscheint notwendig. Denkbar sind auch bundesweite Planspiele, Präventionsmaßnahmen und Sensibilisierungsprogramme.

Die HRK hält eine Verbesserung des Informationsflusses zwischen und mit den Nachrichtendiensten für geboten und sieht darin eine besondere Rolle des Bundes. Beispielsweise muss das Bundesamt für Verfassungsschutz im Falle eines Angriffs parallel die zuständigen Landesämter für Verfassungsschutz und die betroffenen Hochschulen informieren dürfen, was derzeit nur in einem einzigen Land möglich ist. Wünschenswert ist ein strukturiertes Zusammenspiel von Vorfallsmeldung durch die Hochschulen einerseits und Informationsvermittlung durch die Dienste andererseits. Dabei ist aber zu beachten, dass die Nachrichtendienste nicht in die Hochschulautonomie eingreifen dürfen.

Forschung intensivieren
Bereits jetzt fördert der Bund vielfältige Projekte zur Sicherheit im IT-Bereich.[37] Die HRK würdigt die bisherige Forschungsförderung des Bundes zum Thema Cybersicherheit und empfiehlt einen Ausbau der entsprechenden Programme. Darüber hinaus sollte der Bund Forschungsprojekte u. a. für neue Schutz- und Abwehrtechnologien fördern. Zudem muss die Entwicklung von neuen Sicherheitsstandards im EU-Kontext gefördert und Programme zur Weiterentwicklung der digitalen Souveränität aufgestellt werden.

Verantwortung finanziell neu ausgestalten
Aufgrund der Rolle des Bundes bei der Gefahrenabwehr, der internationalen Dimension von Cybersicherheit, der Notwendigkeit zur länderübergreifenden Kooperation sowie der Koordination von arbeitsteiligen Servicezentren ergibt sich eine Zuständigkeit des Bundes. Die HRK fordert eine Förderung, mit der der Bund die Anstrengungen der Hochschulen und der Länder für die Cybersicherheit bündelt, abrundet und konsolidiert sowie dabei einen übergreifenden Rahmen auch für länderübergreifende Kooperationen bildet. Benötigt wird eine agile und unbürokratische Förderung, um die Cybersicherheit möglichst schnell und deutlich zu erhöhen. Da Maßnahmen zur Erhöhung der Cybersicherheit auch in die Strategien der Hochschulen einzubetten sind, muss eine Förderung auch diesbezügliche Aufwände und Konzepte umfassen. Angesichts der Bedrohungslage für Bildung, Forschung und innere Sicherheit ist die HRK für innovative Lösungsansätze und entsprechende Finanzierungsmodalitäten offen.

Anlage 1: Glossar

Ausspähung von dissidentischen Netzwerken: Diese Ausspähung kann z. B. politische Dissidenten, religiöse Minderheiten sowie die LGBTQ- oder Frauenbewegung aus ausländischen Regimen zum Ziel haben. Meist geht es darum, nicht nur in Deutschland existierende Netzwerke auszuspähen, sondern deren Kontakte bzw. Spiegelnetzwerke in den Ursprungsländern zu identifizieren, um diese politisch und strafrechtlich zu verfolgen. Dies stellt eine neue Qualität der Bedrohung von Leib und Leben der Betroffenen dar.

Business Continuity Management (BCM): Notfallmanagement, das umfassend sämtliche Aktivitäten steuert, die einen geordneten Betrieb nach Schadensereignissen zum Ziel haben.[38] Das BSI-Konzept des Business Continuity Management ist Teil eines Informationssicherheits-Managements (ISM).[39]

Core-IT-Facilities: Einrichtungen an Hochschulen, in denen Geräte, Expertise und Methoden vorgehalten werden. Teure und nur mit Spezialwissen zu bedienende Geräte werden hier zentral gebündelt und Forschenden und Externen zugänglich gemacht. Mit Core Facilities können Hochschulen nicht nur Geld sparen, sondern auch gezielt Lücken in ihrem Gerätepark schließen. Neben effizienter Auslastung der Geräte werden Kosten für Wartungen und Reparaturen geteilt.[40]

Cybersicherheit und Informationssicherheit: Der Begriff der „Cybersicherheit" hat gegenüber dem Konzept der „Informationssicherheit" an Relevanz gewonnen: Der Begriff der Cybersicherheit stellt das Risiko eines Angriffs über Kommunikationsnetze und vernetzte Systeme und die gebotene Schadensminimierung in den Vordergrund.

Digitale Souveränität: Sie zielt auf institutioneller Ebene im engeren Sinne vor allem auf eigene IT-Dienstleistungen, die Vermeidung von irreversiblen Abhängigkeiten sowie die Einflussnahme der Hochschulen auf verwendete Software.[41]

DeepFake: Kofferwort von „deep learning" und „fake". Deepfake bezeichnet einen durch KI erzeugten oder manipulierten Bild-, Ton- oder Videoinhalt, der wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähnelt und einer Person fälschlicherweise als echt oder wahrheitsgemäß erscheinen würde.[42]

Offenheit: Konstitutives Charakteristikum der deutschen Hochschulen. Die Hochschulen wollen und können ihrem Auftrag nach Bildung, Forschung, Transfer und demokratischem Dialog nur nachkommen, wenn Sie offen gegenüber der Gesellschaft sowie nationalen und internationalen Kooperationen unterschiedlichster Art sind.[43] Quantitative Indikatoren für diese Offenheit sind die hohe Fluktuation bei den 2,9 Mio. Studierenden und knapp

800.000 Hochschulbeschäftigen sowie die Anzahl von knapp 37.000 internationalen Kooperationen. Dies veranschaulicht die große Herausforderung für die Hochschulen bei der Herstellung größtmöglicher Resilienz.

Ransomware-Angriffe: Hochschulrechner werden infiziert und mittels Verschlüsselung zum Zweck der Erpressung von Geld gesperrt. Solche Angriffe haben in den letzten Jahren stark zugenommen. Dabei verschwimmen zunehmend die Grenzen von privaten und staatlichen Angriffen.

Resilienz: Zentrales Konzept der Cybersicherheit. Resilienz wirkt vor allem auf das Ziel hin, „nach einem Angriff möglichst schnell in einen arbeitsfähigen Systemzustand zurückzufinden“[44]. Dem liegt die Erkenntnis zugrunde, dass sich eine „hundertprozentige Sicherheit in keinem (Cyber)sicherheitssystem erzeugen lässt“[45]. Diesem Hauptziel der Rückkehr in den arbeitsfähigen Zustand dienen auch die Prävention sowie die spätere Anpassung des Systems auf mindestens demselben Niveau wie vor dem Angriff.

Robocalls: Kofferwort von „robot“ und „calls“. In Robocalls werden voraufgezeichnete Nachrichten per Telefonanruf durch computergesteuerte Anrufbeantworter wie von einem Roboter übermittelt.

Security Operation Center (SOC): Überprüft regelmäßig die IT-Systeme von beteiligten Hochschulen auf mögliche Sicherheitslücken, stellt Informationen zu aktuellen Gefahren bereit und durchforstet das Darknet nach Daten der Hochschulen, etwa geleakten Zugangsdaten. Wenn Hacker in ein System eindringen sollten, kann das SOC die Hochschulen zudem durch forensische Analyse und bei der Schadensbehebung unterstützen.[46]

Spionage: Diese wird nach wie vor von staatlichen Stellen betrieben, wobei auch zunächst unbeteiligte eigene Staatsangehörige (z. B. Studierende und Gastwissenschaftler:innen) zur Spionage eingespannt werden. In jüngster Zeit standen als Spionageziele die Weiterentwicklung von Hochtechnologie, Kooperationen mit dem Verteidigungssektor, politische Analysen sowie geographische Daten und Karten im Mittelpunkt.

Anlage 2: Zur Entstehung der Empfehlungen

Die vorliegenden Empfehlungen sind in der Ständigen HRK-Kommission für Digitalisierung erstellt worden. Geleitet wird die Kommission von der HRK-Vizepräsidentin für Digitalisierung und wissenschaftliche Weiterbildung, Frau Professorin Dr. Ulrike Tippe. Der Kommission gehören als ständige Mitglieder Herr Professor Dr. Philipp Ahner, Herr Malte Dreyer, Herr Professor Dr. Hannes Hartenstein, Herr Professor Dr. Wolfram Horstmann, Herr Professor Dr. Michael Jäckel, Frau Professorin Constanze Langer, Herr Professor Dr. Gerhard Lauer, Herr Jens Andreas Meinen, Herr Professor Dr. Jörg Müller-Lietzkow, Frau Paula Paschke, Herr Professor Dr. Hans Pongratz, Herr Professor Dr. Arnd Steinmetz und Herr Professor Dr. Jens Weiß an. Betreut wird die Kommission von Herrn Dr. Elmar Schultz von der HRK-Geschäftsstelle.

Ausgangspunkt der Entstehung war eine Anhörung der Kommission am 4. November 2024 zum Thema „Cybersicherheit an Hochschulen: Balance zwischen Resilienz, digitaler Souveränität und Offenheit". Angehört wurden Herr Dr. Christian Grimm, Frau Professorin Dr. May-Britt Kallenrode, Herr Oliver Kaczmarek, Frau Professorin Dr. Maria Leitner, Herr Dr. Florian Rautenberg und Herr Professor Dr. Fabian Schmieder. Die Ergebnisse der Anhörung wurden durch eine Fokusrunde am 18. November 2024, dem Vortag der HRK-Mitgliederversammlung, sowie durch einen Austausch mit Frau Professorin Dr. Haya Schulmann, Herrn Professor Dr. Michael Backes und Herrn Thomas Franke im Rahmen der Kommissionssitzung am 28. Januar 2025 ergänzt.

Die HRK dankt allen Beteiligten für ihre Beiträge.

---

[1] Zur Begriffsabgrenzung zwischen Informations- und Cybersicherheit siehe Glossar.
[2] HRK (2018), Informationssicherheit als strategische Aufgabe der Hochschulleitung, 6. November, https://www.hrk.de/positionen/beschluss/detail/informationssicherheit-als-strategische-aufgabe-der-hochschulleitung/, letzter Zugriff: 28.3.2025.
[3] Zu berücksichtigen ist auch, dass sich die rechtlichen Rahmenbedingungen weiterentwickelt haben. So hat zum 18.10.2024 die NIS-2-Richtlinie zum Cybersicherheitsniveau in der EU (Network and Information Systems (NIS)) die bisherige NIS-Richtlinie vom 23.6.2017 aufgehoben. Der Cyber Resilience Act (CRA) vom 10.12.2024 stellt zudem Sicherheitsanforderungen an Hard- und Software-Produkte. Möglich ist, dass auch DORA (Digital Operational Resilience Act) vom 17.1.2023 – ein regulatorischer Rahmen, der darauf abzielt, die digitale Widerstandsfähigkeit aller Unternehmen im EU-Finanzsektor zu stärken – auf andere Sektoren ausstrahlt.
[4] Siehe Glossar.
[5] Ebenda.
[6] Ebenda.
[7] Ebenda.
[8] Ebenda. Kofferwort von „robot" und „calls".
[9] Ebenda.
[10] Ebenda.
[11] Ebenda.

[12] Vgl. HRK (2018), Informationssicherheit, S. 12f, 16.
[13] Siehe Glossar.
[14] Bei nicht vorhandenen Diensthandys kommen als Lösungsansatz Hardware-Tokens oder z.B. YubiKeys in Frage.
[15] Eine Differenzierung nach Basis- und Kernabsicherung entspricht der IT-Grundschutz-Methodik des BSI. BSI, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_2_Sicherheitsmanagement/Lektion_2_09/Lektion_2_09_node.html, letzter Zugriff: 28.3.2025. Die Frage der Festlegung, was "Kritische Daten, Informationen und Systeme" sind und was nicht, erscheint nicht als trivial. Indikatoren könnten eine besondere Gefährdung von Assets, ein irreparabler Schaden oder eine Existenzbedrohung sein.
[16] Siehe Glossar.
[17] Als Orientierung dienen: ZKI (Hrsg., 2023) Handreichung zur Vorbereitung auf Informationssicherheitsvorfälle, https://zenodo.org/records/10130339, letzter Zugriff: 28.3.2025 und HIS-HE (2023), Krisenmanagement nach Cyberangriffen – Handlungsempfehlungen, https://medien.his-he.de/publikationen/detail/krisenmanagement-nach-cyber-angriffen-handlungsempfehlungen, letzter Zugriff: 28.3.2025.
[18] So verfolgt das DFN die Idee einer „112-Nummer" in Anlehnung an die Feuerwehrnummer 112.
[19] BSI, Maßnahmenkatalog zum Notfallmanagement, https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/Notfallkarte/Massnahmenkatalog_Notfallmanagement.pdf?__blob=publicationFile&v=3 , Stand: Mai 2021, letzter Zugriff: 28.3.2025 und BSI, IT-Notfallkarte „Verhalten bei IT-Notfällen, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/IT-Notfallkarte/it-notfallkarte_node.html, letzter Zugriff: 28.3.2025.
[20] Dienstleistungen zur Abwehr laufender oder erfolgter Angriffe bei gezielten Angriffen starker Gegner (Advanced Persistent Threat, APT), siehe BSI (2025), Liste der qualifizierten APT-Response Dienstleistungen, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.html, Stand: 23.1.2025, letzter Zugriff: 28.3.2025.
[21] Ziele bzw. Lernziele solcher Übungen sind: Erleben von bestimmten Situationen, Treffen bestimmter Entscheidungen, Kommunikation innerhalb des Teams und mit Externen, Testen von Notfallplänen, Durchführen von Dokumentation sowie technische Analyse in kurzer Zeit. Zit.n. Leitner, HRK-Anhörung 4.11.24.
[22] Das Konzept der „Digital Sobriety" umfasst auch den Gedanken der Energiesparsamkeit und die Verminderung des digital-ökologischen Fußabdrucks.
[23] Siehe Glossar.
[24] HRK (2018), Informationssicherheit, https://www.hrk.de/fileadmin/redaktion/hrk/02-Dokumente/02-01-Beschluesse/HRK_MV_Empfehlung_Informationssicherheit_06112018.pdf, 6.11.2018, S. 15, letzter Zugriff: 28.3.2025; HRK (2021), Momentum der Digitalisierung nutzen, https://www.hrk.de/fileadmin/redaktion/hrk/02-Dokumente/02-01-Beschluesse/2021-06-08_HRK-S-Entschliessung_zu_digitalen_Lehrinfrastrukturen.pdf), 8. Juni 2021, S. 5, letzter Zugriff: 28.3.2025; HRK (2023), „Digitale Hochschule", https://www.hrk.de/fileadmin/redaktion/hrk/02-Dokumente/02-01-Beschluesse/2023-11-14_HRK-MV_Entschliessung_Digitale-Hochschule-Kooperationen.pdf, 14.11.2023, S. 12, letzter Zugriff: 28.3.2025.
[25] Ebenda, S. 6f.
[26] HRK (2018), Informationssicherheit, S. 5, 14f.
[27] Die komplette Verlagerung der Kommunikation auf einzelne Messengerdienste stellt erfahrungsgemäß keine Lösung dar.
[28] Vgl. HRK (2018), Informationssicherheit, S. 9.
[29] HRK (2018), Informationssicherheit, S. 4, 5, 9.
[30] HRK (2023), „Digitale Hochschule", S. 6f.
[31] ZKI, https://www.zki.de/ueber-den-zki/mitglieder/, letzter Zugriff: 28.3.2025.
[32] Netzwerk Landeseinrichtungen für digitale Hochschullehre, https://netzwerk-landeseinrichtungen.de/, letzter Zugriff: 28.3.2025.

[33] Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen (2025), Cybersicherheit, https://www.mkw.nrw/themen/wissenschaft/wissenschaftspolitik/cybersicherheit, letzter Zugriff: 28.3.2025.
[34] Ein gutes Beispiel hierfür ist SecAware.nrw, ein Online-Selbstlernangebot zum Thema Cyber- und IT-Sicherheit für die Hochschulen in Nordrhein-Westfalen. Ebenda.
[35] Angaben für diesen Status Quo finden sich nicht in der Literatur. Im Austausch mit vielen Einrichtungen in Deutschland und der EU hat sich jedoch ergeben, dass gegenwärtig zwei bis fünf Prozent der Ausgaben des gesamten IT-Personals für Cybersicherheit verwendet werden. Dies entspricht bezogen auf die IT-Gesamtausgaben einem Anteil von ein bis vier Prozent.
[36] Diese BSI-Vorgabe bezieht sich auf Staaten und Unternehmen, die zwanzig Prozent ihrer IT-Ausgaben für die Cybersicherheit ausgeben sollten, 7.4.2024, https://www.ad-hoc-news.de/sonstige/die-praesidentin-des-bundesamtes-fuer-sicherheit-in-der/65115311, letzter Zugriff: 2.5.2025. Hochschulen sind in Bezug auf sensible Innovations- und Personaldaten vergleichbar mit Unternehmen und dem Staat.
[37] BMBF (2025), Förderprojekte aus dem Bereich Vernetzung und Sicherheit digitaler Systeme, https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte, letzter Zugriff: 31.3.2025.
[38] BSI (2022), Glossar und Abkürzungsverzeichnis, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Standard200_4_BCM/Standard_200-4_BCM_Glossar.pdf?__blob=publicationFile&v=4, S. 4, letzter Zugriff: 31.3.2025.
[39] BSI (2023), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Standard200_4_BCM/Standard_200-4_BCM_Flyer.pdf?__blob=publicationFile&v=2, Stand September 2023, letzter Zugriff: 31.3.2025.
[40] Jedicke, Philipp (2024), Core Facilities: Geteilte Forschungsinfrastruktur – ein Zukunftsmodell? https://www.forschung-und-lehre.de/forschung/geteilte-forschungsinfrastruktur-ein-zukunftsmodell-6429, Forschung und Lehre vom 23.5.2024, letzter Zugriff: 31.3.2025.
[41] Vgl. HRK (2023), „Digitale Hochschule", S. 11f. Weiterführend Wissenschaftsrat (2023), (https://www.wissenschaftsrat.de/download/2023/1580-23.pdf?__blob=publicationFile&v=11), Oktober 2023, letzter Zugriff: 31.3.2025 und Krupka, D. (2020), Dimensionen digitaler Souveränität – ein Überblick. In: Gesellschaft für Informatik (Hrsg.) Schlüsselaspekte digitaler Souveränität, Arbeitspapier, https://gi.de/fileadmin/GI/Allgemein/PDF/Arbeitspapier_Digitale_Souveraenitaet.pdf). S. 4-7, letzter Zugriff am 31.3.2025.
[42] EU-Verordnung über künstliche Intelligenz, Kapitel I, Art. 3, Nr. 60, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401689 vom 13. Juni 2024, letzter Zugriff: 31.3.2025.
[43] Normativer Ausdruck dieses Wesensmerkmals sind z. B. Konzepte wie „Offene Hochschulen für den Aufstieg durch Bildung", https://offene-hochschulen.de/, letzter Zugriff: 31.3.2025; HRK (2015), „Weltoffene Hochschulen", 11.11.2015, https://www.hrk.de/weltoffene-hochschulen, letzter Zugriff: 31.3.2025 und das Insistieren auf der „Offenheit der Teilnahme" bei gesellschaftlichen Auseinandersetzungen", vgl. HRK (2024), Hochschulen als freien Diskursraum sichern, (https://www.hrk.de/fileadmin/redaktion/hrk/02-Dokumente/02-01-Beschluesse/2024-05-14_Entschliessung_Hochschulen-als-freien-Diskursraum-sichern.pdf, 14.5.2024, letzter Zugriff 31.3.2025.
[44] HRK (2018), Informationssicherheit, S. 14.
[45] Ebenda.
[46] Nordrhein-Westfalen (2024), Für mehr Cybersicherheit! Hochschulen starten gemeinsames Security Operation Center, https://www.mkw.nrw/fuer-mehr-cybersicherheit-hochschulen-starten-gemeinsames-security-operation-center, 27.6.2024, letzter Zugriff: 31.3.2025.