Empfehlungen der Ständigen
Kommission Digitalisierung
am 5. Februar 2025
in Bonn

Bedrohungslage erhöht Handlungsdruck für den Bund: HRK-Empfehlungen zur Stärkung der 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

Die Hochschule ist gelähmt: Studierende und Lehrende haben keinen Zugriff auf Lernplattformen, Forschende und die kooperierende Wirtschaft fürchten um ihre sensiblen Forschungsergebnisse, das Universitätsklinikum bangt um seine Patientendaten, die Verwaltung sorgt sich um die Auszahlung der Gehälter, der finanzielle Schaden ist unabsehbar.

Solche oder ähnliche Szenarien sind wiederkehrende Realität bei Cyberangriffen. Die Bedrohungslage für die Hochschulen wird mittlerweile von den Sicherheitsbehörden als extrem hoch bewertet. Aktuell können insbesondere folgende Szenarien unterschieden werden: Ransomware-Angriffe (Lösegeldforderungen), Spionage sowie die Ausspähung von dissidentischen Netzwerken und sozialen Bewegungen. Bei diesen Bedrohungsszenarien kommt auch zunehmend Künstliche Intelligenz (KI) zum Einsatz. Cybersicherheit liegt in der gemeinsamen Verantwortung der Hochschulen, der Länder und des Bundes. An den Bund richtet die HRK nachfolgende Appelle:

Gefahren abwehren!
Die HRK empfiehlt dem Bund, angesichts der Bedrohungslage entsprechend seiner übergreifenden Rolle in der Gefahrenabwehr aktiv 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.[1] 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.

[1] https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte.

Anlage: 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. Der HRK-Präsident und das HRK-Präsidium haben die Empfehlungen gebilligt.

Die HRK dankt allen Beteiligten für ihre Beiträge.