**LANDTAG NORDRHEIN-WESTFALEN**
18. Wahlperiode

Drucksache **18/3669**

21.03.2023

# Antrag

**der Fraktion der CDU und
der Fraktion BÜNDNIS 90/DIE GRÜNEN**

**IT-Sicherheit an Wissenschaftseinrichtungen stärken**

## I. Ausgangslage

Digitale Systeme und Anwendungen werden an Hochschulen, Forschungseinrichtungen und Studierendenwerken alltäglich und umfassend eingesetzt. Forschung, Lehre und Verwaltung funktionieren nur noch mit digitalen Hilfsmitteln. Gleichzeitig steigt das Risiko von Hackerangriffen, insbesondere mittels sogenannter Ransomware-Angriffe. Die Bedrohungslage nimmt seit Jahren zu, Wissenschaftseinrichtungen sind fast täglich Cyberangriffen ausgesetzt. Diese erfolgen von Kleinkriminellen bis hin zu professionellen Hackerteams, die im Auftrag dritter Staaten Spionage und Sabotage betreiben. Daher ist das Thema der IT-Sicherheit in diesen Einrichtungen von enormer Bedeutung.

Das Nationale Cyber-Abwehrzentrum registrierte in den vergangenen Monaten bundesweit vermehrt Cyberangriffe auf Hochschulen in Deutschland: So waren unter anderem die Hochschule Harz, die Technische Universität Freiberg, die Hochschule Ansbach und die Hochschule für Angewandte Wissenschaften Hamburg betroffen.

Auch in Nordrhein-Westfalen wurden Hochschulen angegriffen. Dies ist aufgrund der hohen Anzahl von Hochschulen in unserem Land nicht überraschend. Im November 2022 wurde z. B. die Universität Duisburg-Essen Opfer eines Cyberangriffs. Daten wurden verschlüsselt und für ihre Freigabe Lösegeld verlangt. Durch den Angriff funktionierten die Internetseite, das E-Mail-System, PC-Anwendungen, Online-Plattformen und weitere digitale Systeme der Universität nicht mehr. Nur weil die IT-Abteilung schnell reagierte und alle Systeme abschaltete, konnte eine Beeinträchtigung des Universitätsklinikums verhindert werden. Wann alle digitalen Anwendungen wieder vollständig normal laufen, ist noch unklar. Mitte Januar 2023 wurde zudem bekannt, dass die für den Cyberangriff verantwortliche kriminelle Gruppierung Daten der Universität im Darknet veröffentlicht hat. Im Januar 2023 gab es einen weiteren Hackerangriff auf eine Hochschule in Nordrhein-Westfalen. An der Hochschule Ruhr-West mussten aus Sicherheitsgründen alle Systeme vom Netz getrennt werden. In beiden Fällen wurde die Staatsanwaltschaft Köln eingeschaltet, bei der die Zentral- und Ansprechstelle Cybercrime angesiedelt ist, und externe IT-Dienstleister hinzugezogen.

Ein sogenannter White-Hat-Hacker, dessen Ziel es ist auf Sicherheitsmängel hinzuweisen und nicht sie auszunutzen, hat im Januar 2023 bei 73 getesteten IT-Systemen von Hochschulen in ganz Deutschland in 15 Fällen Sicherheitslücken gefunden. Daraufhin wurden die

Datum des Originals: 21.03.2023/Ausgegeben: 21.03.2023

Hochschulen – darunter auch welche aus Nordrhein-Westfalen - informiert und konnten die Lücken schließen.

Hochschulen und Forschungseinrichtungen sind verstärkt im Blickfeld von Angreifergruppen, die durch das Verschlüsseln von Daten Lösegeld erpressen wollen. Der Staat kooperiert hier zu Recht nicht und zahlt keine Lösegelder. Problematisch wird es insbesondere dann, wenn entwendete Daten sensible persönliche Informationen enthalten – etwa von Patientinnen und Patienten der Universitätskliniken. Auch Hoch- und Höchstleistungsrechner stehen im Visier von Hackern, die diese superschnelle Computer kapern wollen, um damit Angriffe auf andere Systeme durchzuführen.

Hochschulen sind auch deshalb zunehmend Opfer von Cyberangriffen, weil ihr komplexer Aufbau, ihre dezentrale Organisation mit sehr autonomen Fachbereichen, die Kooperationen mit anderen Einrichtungen und ihre Kultur der Offenheit für Externe eine Herausforderung für ganzheitliche IT-Sicherheitskonzepte sind. Aufgrund seiner Komplexität ist ein Schutz des gesamten Hochschulnetzes illusorisch. Es erfordert daher besondere Umsicht und spezielle Vorgehensweisen, um hier IT-Sicherheit auf einem angemessen hohen Niveau sicherzustellen, ohne Lehre und Forschung zu behindern. Dazu ist es notwendig, dass über die Grenzen einzelner Einrichtungen hinaus gemeinsam einheitliche Maßnahmen definiert und diese konsequent umgesetzt werden.

Im Rahmen der in Nordrhein-Westfalen geltenden Hochschulautonomie sind die Hochschulen selbst für die Gewährleistung der IT-Sicherheit zuständig und verantwortlich. Daneben widmen sich über die Digitale Hochschule NRW (DH.NRW) 42 Hochschulen aus Nordrhein-Westfalen in Zusammenarbeit mit dem Ministerium für Kultur und Wissenschaft des Landes dem Thema der digitalen Transformation. Sie identifizieren neue Themenbereiche mit Handlungsbedarf, treten in den Diskurs über beste Lösungen ein, loten den Aufsatz kooperativer Vorhaben aus und gestalten mit der Etablierung einer hochschulübergreifenden digitalen Servicestruktur die Grundlage für den digitalen Wandel des Hochschulstandortes Nordrhein-Westfalen. Über Positions- und Strategiepapiere zeigt die DH.NRW Zielsetzungen und Handlungsoptionen auf und initiiert als Aktivitäten-Plattform digitalisierungsbezogene Kooperationen und Förderprogramme. Sie vernetzt und bündelt damit die an den Mitgliedshochschulen vorhandenen Kompetenzen im Digitalisierungskontext. Daher eignet sich die „Digitale Hochschule NRW" besonders dafür, die Herausforderungen der IT-Sicherheit für den Wissenschaftsstandort Nordrhein-Westfalen hochschulübergreifend anzugehen und zu bearbeiten.

Seit dem russischen Angriffskrieg gegen die Ukraine bewertet das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Gefährdungslage im Cyber-Raum als „hoch wie nie“. Deshalb unterstützt die Landesregierung die Hochschulen - oft im Rahmen der DH.NRW - bereits heute mit einer ganzen Reihe von Maßnahmen dabei, sich darauf gezielt besser einzustellen:

- Aus dem Sondervermögen Krisenbewältigung stehen den Hochschulen 41,15 Millionen Euro für Maßnahmen zur Verbesserung der Cybersicherheit zur Verfügung, die schnell wirksam werden können. Hierzu zählen Zertifizierungen und Beratungen zur Wirksamkeit oder zum Aufbau eines Informationssicherheitsmanagementsystems sowie von Notfall- und Recoverplänen, der Erwerb von Softwarelösungen für das Schwachstellenmanagement, die Einführung einer Zwei-Faktor-Authentifizierung, Next Generation Firewalls und die Verbesserung der Notstromversorgung.
- Die Hochschulen erhalten nach einer Vereinbarung zwischen Land und Hochschulen zur Informationssicherheit zusätzliche Unterstützung für die Informationssicherheit in Form von mehr personellen Ressourcen. Im Gegenzug verpflichten sich die Hochschulen, schnellstmöglich ihr IT-Sicherheitsniveau zu erhöhen sowie ein

hochschulübergreifendes Netzwerk zur Informationssicherheit aufzubauen. Durch den Aufbau des hochschulübergreifenden Netzwerks können Synergieeffekte genutzt werden, und das Land erhält regelmäßig Berichte über die Gefährdungslage und die Umsetzung der Informationssicherheit an den Hochschulen.

- Der Ausbau eines redundanten NRW-share für die Speicherung und Archivierung von Forschungsdaten unter der Federführung der RWTH Aachen (DataStorage.nrw) wird vorangetrieben. Hier können Forschungsdaten sicher abgelegt und über die Webplattform Coscine kooperativ zwischen den Hochschulen genutzt werden. Die Forschungsdaten werden an drei Speicherstandorten gegenseitig gesichert.
- Ein gemeinsamer IT-Dienstleiser für die Hochschulen für angewandte Wissenschaften sowie die Kunst- und Musikhochschulen wird geschaffen: Die Hochschulen für angewandte Wissenschaften bauen unter der Federführung der TH OWL einen IT-Dienstleister auf, der an zentraler Stelle diverse IT-Basis- und Clouddienste übernimmt und entsprechend vor Angriffen schützt.
- Für alle Hochschulen wird eine effektive Datensicherung eingeführt: Datensicherung.nrw bietet Leistungen für alle Hochschulen an, muss aber nur an wenigen Standorten betrieben werden. In einem ersten Schritt ist 2022 ein erster Backup-Standort gestartet, 2023 und 2024 sollen insgesamt zwei weitere hinzukommen.

Diese Maßnahmen tragen dazu bei, das Schutzniveau der IT-Sicherheit an den Hochschulen in relevanter Weise zu erhöhen. Da Stillstand auf dem Feld der Informationstechnik jedoch Rückschritt bedeutet, müssen diese Maßnahmen mit weiteren Schritten ergänzt und erweitert werden. So sollte vor allem die Vereinbarung zur Informationssicherheit zwischen Land und Hochschulen kurzfristig erweitert werden, um so zusätzliche Maßnahmen zum Schutz der Verwaltungs-IT in den Hochschulen, für ein verbessertes Notfallmanagement und die zügige Wiederherstellung von IT-Diensten ohne Datenverluste zu vereinbaren. Dazu sollten u. a. gehören:

- die Implementierung und Zertifizierung der Standard-Absicherung nach der IT-Grundschutz-Methodik des BSI für die Verwaltungs-IT der Hochschulen sowie die Daten- oder IT-Services mit hohem Schutzbedarf innerhalb von drei Jahren,
- die schrittweise Einführung der Zwei-Faktor-Authentifizierung sowie eines Notfallmanagements (gemäß BSI-Standards) innerhalb eines festgelegten Zeitraums von drei Jahren,
- regelmäßige Awareness-Maßnahmen für alle Mitarbeitenden und Studierenden,
- die Erarbeitung einer hochschulspezifischen Wiederherstellungsstrategie mit regelmäßigen Wiederanlauftests,
- ein hochschulübergreifendes Schwachstellenmanagement, Penetrationstests und Echtzeitanalyse von Sicherheitsalarmen sowie
- die sukzessive Verlagerung von IT-Infrastruktur aus der Peripherie der Hochschulen in ein zentrales Rechenzentrum (IT-Sicherheit, Energiekosten etc.).

Ein wichtiger Baustein, um den Schaden im Angriffsfall zu minimieren, sind Backups und ein rigides Backup-Schema, das eine zeitlich versetzte und dezentrale Aufbewahrung von Backups vorsieht. Hier gehen die nordrhein-westfälischen Hochschulen bereits im Projekt Datensicherung.nrw gemeinsam voran. Doch auch hier sind weitere Maßnahmen notwendig.

Im Sicherheitsmanagement an Hochschulen ist besonders wichtig, schnell und fortlaufend auf Basis von Fakten, Erfahrungen und neuen, auch wissenschaftlichen, Erkenntnissen die IT-Sicherheitsrichtlinien und Handlungsempfehlungen weiterzuentwickeln, um disruptiven

Entwicklungen rechtzeitig zu begegnen. Dazu gehört auch die Technologiefrüherkennung (Technology Forecasting), die rechtzeitig auf Neuerungen hinweist.

Sogar verschlüsselte Daten bieten keinen dauerhaften Schutz vor Einsichtnahme durch Unbefugte. Schon heute wird von Cyberangriffen berichtet, deren Ziel es nicht ist, unverschlüsselte Daten zu stehlen und zu missbrauchen. Vielmehr sollen aktuell gut geschützte, weil verschlüsselte, Daten erbeutet und diese entschlüsselt werden, sobald Quantencomputer dazu in der Lage sind. Daher ist es wichtig, frühzeitig mit den Planungen zu beginnen, wie von klassischer auf Post-Quanten-Kryptographie umgestellt werden kann. Da Hochschulen und Forschungseinrichtungen selbst zu diesen Themen forschen, lassen sich Synergieeffekte nutzen. Auch die Forschung zu anderen Aspekten der IT-Sicherheit und Informatik sollte von Wissenschaftseinrichtungen selbst angewandt werden. Zum gegenseitigen Nutzen können die Einrichtungen hier als Experimentier- und Pionierfeld dienen. Deshalb ist es wichtig, diese Forschungsbereiche weiter zu stärken.

Zum Informationssicherheitsmanagement (ISMS) an Hochschulen und Forschungseinrichtungen gehört ebenso eine tägliche Analyse und Bewertung der Informationssicherheitsrisiken und regelmäßige Schulungen des IT-Personals sowie der IT-Nutzerinnen und -Nutzer. Aufgrund der schieren Größe der Wissenschaftslandschaft sollten die Hochschulen daher über die Schaffung eines hochschulübergreifenden Computer Emergency Response Team (CERT) nachdenken. Dieses könnte Schulungen für das IT-Personal bei informationssicherheitsrelevanten Themen und Fragestellungen durchführen, regelmäßige Sicherheitstests (Schwachstellenscans und insbesondere spezifische Penetrationstests) und -übungen abhalten, die Hochschulen bei der Abwehr und Behandlung von IT-Sicherheitsvorfällen unterstützen und beraten, Audits anbieten und zentrale Tools zur Stärkung der Informationssicherheit an den Hochschulen betreiben. Außerdem sollte ein solches CERT über ein eigenes Incident Response Team (IRT) verfügen, damit die Einrichtungen diese Leistungen für den eingetretenen Schadensfall nicht mehr extern einkaufen müssen. An dieser Stelle profitieren Hochschulen, Universitätskliniken, Forschungseinrichtungen und Studierendenwerke maßgeblich, wenn sie bei Ausbau, Betrieb und Weiterentwicklung ihrer IT-Infrastruktur weitgehend miteinander kooperieren.

Zu den grundlegenden Anforderungen an IT-Systeme gehören Pläne, Maßnahmen und regelmäßige Übungen zur Reaktion auf Schadenslagen, die eine schnelle Rückkehr zum Normalbetrieb nach einem erfolgreichen Angriff ermöglichen. Vorhandene Sicherheitsmaßnahmen müssen so vereinfacht werden, dass sie für Benutzerinnen und Benutzer einfach zu verwenden sind. Zudem muss ein kontinuierlicher Prozess geschaffen werden, in dem Sicherheitsmaßnahmen fortlaufend überprüft, umgesetzt und weiterentwickelt werden. Hierzu bedarf es einer Wiederherstellungsstrategie an den Hochschulen.

## II. Beschlussfassung

Der Landtag beauftragt die Landesregierung,

- im Rahmen der DH.NRW darauf hinzuwirken, dass die Hochschulen grundlegende und einheitliche Leitlinien und Maßnahmen zur IT-Sicherheit vereinbaren und implementieren.

- mit den Hochschulen zeitnah eine Erweiterung der gemeinsamen Vereinbarung zur Informationssicherheit zu verhandeln, in der weitere Schritte zur Cybersicherheit konkretisiert werden.

- die Hochschulen aus bereiten Mitteln darin zu unterstützen, dass IT-Systeme problemlos kooperativ betrieben werden können.

- Mit den Hochschulen, Universitätsklinika, Forschungseinrichtungen der Johannes-Rau-Forschungsgemeinschaft und Studierendenwerken in Gespräche über die mögliche Schaffung eines kooperativ betriebenen Computer Emergency- Response Team einzusteigen, das unter anderem ein eigenes Incident Response Team vorhält.

- die Hochschulen und Forschungseinrichtungen aus bereiten Mitteln beim Schutz vor politischer Einflussnahme über IT-Systeme zu unterstützen.

- die Forschung an NRW-Hochschulen zur IT-Sicherheit in Nordrhein-Westfalen mit herausragenden Akteuren wie dem Exzellenzcluster CASA in Bochum und anderen Einrichtungen aus bereiten Mitteln weiter zu stärken. Wichtig sind vor allem die Forschungsschwerpunkte Risikobewertung, Netzwerksicherheit, (Post-Quanten-)Kryptographie, vertrauenswürdige Hard- und Software, Threat Analysis oder automatisierte Test- und Verifikationsverfahren für Soft- und Hardware.

- zu prüfen, wie Forscherinnen und Forschern eine bessere Datenlage zur Untersuchung von Cyberangriffen ermöglicht werden kann.

| | |
|---|---|
| Thorsten Schick | Wibke Brems |
| Matthias Kerkhoff | Verena Schäffer |
| Dr. Jan Heinisch | Mehrdad Mostofizadeh |
| Raphael Tigges | Gönül Eğlence |
| | Julia Eisentraut |
| und Fraktion | und Fraktion |