Antrag N01: Cyberangriffe abwehren - Hochschulen schützen!

Laufende Nummer: 31

Antragsteller*in:	Juso-Hochschulgruppen Nordrhein-Westfalen
Status:	angenommen in geänderter Fassung
Sachgebiet:	N - Digitale Gesellschaft

Cyberangriffe abwehren - Hochschulen schützen!

Cyberangriffe auf Hochschulen und Wissenschaftseinrichtungen sind schon lange keine Ausnahmefälle mehr. Laut dem Bundeskriminalamt gab es zwischen 2022 und 2024 mindestens 42 dieser Angriffe auf Hochschulen und Wissenschaftseinrichtungen, welche Schäden in Millionenhöhe verursachten. Im Jahr 2024 waren unter anderem die HHU Düsseldorf, die Universität Potsdam, die University of Applied Sciences in Frankfurt am Main und die Berliner Hochschule für Technik von Ransomeware-Angriffen und weiteren Cyberattacken betroffen. Durch diese Angriffe werden zum einen Daten gestohlen oder verschlüsselt und erst nach Lösegeldzahlungen wieder freigegeben. Außerdem wird der Hochschulbetrieb enorm eingeschränkt, da Verwaltung, Forschung und Lehre auf digitale Infrastruktur angewiesen sind. Dabei sind Hochschulen und Wissenschaftseinrichtungen durch ihre offene Struktur, die Vielzahl von dezentralen Einrichtungen, der starken Vernetzung mit internationalen Forschungsakteur*innen sowie der Speicherung von hochsensiblen Daten und Forschungsergebnissen ein lohnendes Ziel für Cyberkriminelle und staatlich gelenkte Akteur*innen.

Cyberangriffe - was ist das eigentlich?

Immer wieder kommt es an Hochschulen zu sogenannten Ransomware-Angriffen, bei denen Schadsoftware Daten verschlüsselt und erst gegen die Zahlung eines Lösegelds wieder freigegeben werden. Betroffene Einrichtungen stehen dabei nicht nur vor der unmittelbaren Gefahr, dass wichtige Forschungsdaten verloren gehen, sondern auch vor der Erpressung, dass gestohlene Daten im Darknet veröffentlicht werden. Ebenfalls relevant sind Angriffe, die gezielt auf den Diebstahl von Daten abzielen: Sei es die Sammlung persönlicher Informationen von Studierenden und Mitarbeitenden oder der Abgriff vertraulicher Forschungsergebnisse in besonders innovativen und politisch brisanten Bereichen. Hinzu kommen klassische Denial-of-Service-Attacken, bei denen durch massenhafte Anfragen Server überlastet und damit zentrale Dienste lahmgelegt werden. Technisch ausgefeilter sind Man-in-the-Middle-Angriffe, bei denen sich Angreifende unbemerkt in die Kommunikation zwischen zwei Parteien einschalten und Daten manipulieren oder abhören können, sowie SQL-Injections, die gezielt Datenbanken kompromittieren, indem bösartiger Code in Abfragen eingeschleust wird. Besonders gefährlich sind Zero-Day-Schwachstellen, also Sicherheitslücken, die noch unbekannt sind und für die es daher keine Abwehrmechanismen gibt, und DNS-Tunneling, bei dem Daten über eigentlich harmlose Namensanfragen im Internet versteckt übertragen werden. All diese Techniken fallen unter den Oberbegriff Malware, also Schadsoftware, die Systeme manipuliert, blockiert oder ausspioniert.

Die Ziele der Angriffe sind unterschiedlich: Einerseits werden Forschungsergebnisse, die im internationalen Wettbewerb großen wirtschaftlichen Wert besitzen, zum Ziel. Andere Angriffe zielen auf personenbezogene Daten, die gesammelt oder verkauft werden. Hochschulen werden zu Zahlung von Lösegeldern gedrängt und

Hochschulinfrastrukturen werden zur Verbreitung von Spam oder weiteren Schadprogrammen genutzt. Dabei sind es nicht nur Einzelpersonen oder kriminelle Banden, die solche Attacken durchführen. Immer häufiger wird von koordinierten Angriffen berichtet, die im geopolitischen Kontext stehen und durch staatliche oder halbstaatliche Akteure aus Ländern wie Russland oder China gesteuert werden.

Die bestehenden Schutzmechanismen reichen oft bei weitem nicht aus. Viele Hochschulen lassen nach wie vor schwache oder gemeinsam genutzte Passwörter zu, veraltete Systeme und unzureichende Trennung zwischen zentralen und dezentralen IT-Strukturen machen Angriffe einfach. Notwendige Schulungen werden zu selten durchgeführt, Reaktionspläne fehlen oder sind kaum eingeübt. Projekte wie AIGIS zeigen allerdings, dass es auch anders geht: Dort wird eine sogenannte Zero-Trust-Architektur erprobt, die grundsätzlich davon ausgeht, dass kein System innerhalb einer Hochschule automatisch vertrauenswürdig ist. Jeder Zugriff wird geprüft, Berechtigungen sind auf das Nötigste beschränkt und Kommunikation zwischen einzelnen Diensten ist durch Segmentierung, Verschlüsselung und strenge Authentifizierung geschützt. Dieses Modell ist international Standard und sollte auch an allen deutschen Hochschulen umgesetzt werden.

Für uns als Juso Hochschulgruppen ist der Schutz von Forschung und Lehre nicht nur eine technische, sondern auch eine politische Frage. Forschung ist gesellschaftliches Eigentum und darf nicht durch kriminelle Gruppen oder geopolitische Interessen instrumentalisiert werden. Der Staat hat die Pflicht, öffentliche Einrichtungen so auszustatten, dass Bildung und Forschung frei von Erpressung und Spionage stattfinden können. Zugleich ist es notwendig, dass wir uns nicht in eine neue Abhängigkeit von globalen Technologiekonzernen begeben, sondern digitale Souveränität und solidarische Lösungen fördern. Der Schutz von Hochschulen vor Cyberangriffen ist daher Teil einer sozialistischen Hochschulpolitik, die die Rechte von Studierenden, Mitarbeitenden und Forschenden auf Sicherheit und Datenschutz ernst nimmt. Um diese Forderungen umzusetzen, reicht es nicht, nur an die Verantwortung einzelner Hochschulen zu appellieren. Bund und Länder müssen Hochschulen so ausstatten, dass ein substantieller Anteil der IT-Budgets in Sicherheit investiert werden kann.

Unsere Forderungen für (cyber-)sichere Hochschulen

- Verbindliche Sicherheitsarchitektur einführen: Zentral bereitgestellte und kontrollierte Sicherheitsstrukturen mit gesicherten Zugangspunkten zu kritischen Infrastrukturen (z.B. über SSH-Gateways) ermöglichen einheitliche Sicherheitsstandards für alle Hochschulen und schaffen so Handlungssicherheit und Entlastung für die einzelnen Hochschulen
- Zero-Trust-Architektur umsetzen: Kein System wird automatisch als vertrauenswürdig eingestuft, jeder Zugriff wird geprüft. Jeder Zugriff soll geprüft, Berechtigungen auf das minimal Notwendige begrenzt sowie Segmentierung und Verschlüsselung durchgesetzt werden, damit Angriffe frühzeitig unterbunden und ihre Auswirkungen begrenzt werden können.
- Digitale Souveränität stärken: Abhängigkeit von proprietärer Software (insbesondere aus den USA) reduzieren und Open-Source-Lösungen gezielt ausbauen und fördern, um langfristig die Kontrolle über IT-Infrastruktur zu behalten und Datenschutz zu gewährleisten.

- Ausreichende Finanzierung sicherstellen: Bund und Länder müssen Hochschulen so ausstatten, dass ein substantieller Anteil der IT-Budgets in Sicherheit investiert werden kann
- Hauptamtliche Stellen für Informationssicherheit schaffen: Jede Hochschule muss eine unabhängige, ausreichend bezahlte hauptamtliche Stelle für Informationssicherheit einrichten, um die Hochschulen auf den Ernstfall vorzubereiten und sicherzustellen, dass richtig reagiert wird.
- Schulungen und Notfallpläne etablieren: Regelmäßige Sicherheitsschulungen durchführen und Reaktionspläne entwickeln und einüben
- Sicherheitsstandards modernisieren: Keine Zulassung von gleichen Passwörtern für verschiedene Systeme und bessere Trennung von zentralen zu dezentralen Systemen