LANDTAG
NORDRHEIN-WESTFALEN
18. WAHLPERIODE

VORLAGE
18/562

A10

**Ministerium für
Kultur und Wissenschaft
des Landes Nordrhein-Westfalen
Die Ministerin**

Ministerium für Kultur und Wissenschaft
des Landes Nordrhein-Westfalen, 40190 Düsseldorf

An den Vorsitzenden
des Wissenschaftsausschusses
Herrn Prof. Dr. Daniel Zerbin MdL
Platz des Landtags 1
40221 Düsseldorf

12. Dezember 2022

Aktenzeichen:
221
bei Antwort bitte angeben

Ina Brandes

Sitzung des Wissenschaftsausschusses am 14.12.2022
TOP 4 „*Hackerangriff auf die Universität Duisburg-Essen*“, Bericht der Landesregierung

Sehr geehrter Herr Vorsitzender,

die SPD-Fraktion hat den o. g. Bericht beantragt. Dieser Bitte komme ich gerne nach.

Mit freundlichen Grüßen

Ina Brandes

Anlage

Völklinger Straße 49
40221 Düsseldorf
Telefon 0211 896-4338
Telefax 0211 896-4555
poststelle@mkw.nrw.de
www.mkw.nrw

Öffentliche Verkehrsmittel:
S-Bahnen S 8, S 11, S 28
(Völklinger Straße)
Rheinbahn Linie 709
(Georg-Schulhoff-Platz)
Rheinbahn Linien 706, 707
(Wupperstraße)

Ministerium für
Kultur und Wissenschaft
des Landes Nordrhein-Westfalen
Die Ministerin

Schriftlicher Bericht
der Ministerin für Kultur und Wissenschaft
an den Wissenschaftsausschuss

„Hackerangriff auf die Universität Duisburg-Essen"

Die Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW) führt auf Grundlage einer Strafanzeige der Universität Duisburg-Essen vom 28.11.2022 ein Ermittlungsverfahren gegen unbekannt wegen Erpressung u. a. zum Nachteil der Anzeigeerstatterin, wie der Leitende Oberstaatsanwalt in Köln dem Ministerium der Justiz unter dem 02.12.2022 berichtet und hierzu u. a. Folgendes mitgeteilt hat:

„Am 27.11.2022 um 04.00 Uhr stellte der Beauftragte für die IT-Sicherheit fest, dass sämtliche auf den Servern der Universität gespeicherten Daten durch unbekannte Täter verschlüsselt wurden. Zugleich wurde ein im Namen einer in der Vergangenheit wegen Ransomware-Angriffen auf Gesundheits- und Bildungseinrichtungen in Erscheinung getretenen Gruppierung verfasstes Erpresserschreiben auf den Servern abgelegt, in der die Geschädigte aufgefordert wird, über im Einzelnen bezeichnete Webseiten im Darknet und dort verwaltete E-Mail-Adressen in Kontakt mit den unbekannten Tätern zu treten. Für den Fall der Verweigerung der Kontaktaufnahme wird die Veröffentlichung vorgeblich bei der Geschädigten entwendeter Daten angedroht.

Auf polizeilicher Ebene werden die andauernden Ermittlungen im Rahmen einer Besonderen Aufbauorganisation (BAO) durch das Polizeipräsidium Essen geführt."

Derzeit wird eine Überprüfung aller Systeme unter Beteiligung externer Expertise für Cyber-Forensik vorgenommen, um ein sicheres und umfängliches Schadensbild zu erzeugen sowie Spuren der Cyberkriminellen zu sichern, die für die Ermittlungsarbeiten der eingeschalteten Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen der Staatsanwaltschaft Köln benötigt werden. Der Erstellung des Schadensbildes geht eine vollumfängliche Analyse aller Systeme einschließlich der Bereinigung voraus, um eventuell hinterlassenen Schadcode der Angreifer zu identifizieren und damit einen erneuten Angriff in der Phase der Reaktivierung bzw. Wiederherstellung der Systeme zu verhindern. Erst in

der abschließenden Phase wird ermittelt werden können, ob es zu einem Schaden gekommen ist, der über eine Störung des Universitätsbetriebes aufgrund der Betroffenheit der digitalen Systeme hinausgeht. Diese Arbeiten der hoch komplexen Analyse laufen derzeit auf Hochtouren, ein vollumfängliches Schadensbild liegt (Stand 6. Dezember 2022) daher noch nicht vor.

Durch den Cyberangriff wurde der universitäre Betrieb beeinträchtigt: Wie am 28. November 2022 bekannt gegeben wurde, musste in Folge des Angriffs die gesamte IT-Infrastruktur heruntergefahren und vom Netz getrennt werden. Zentrale Dienste wie PC-Anwendungen, E-Mail und Festnetztelefonie standen nicht und stehen derzeit zum Teil mit Einschränkungen zur Verfügung. Gleichwohl kann der Lehrbetrieb regulär in Präsenz fortgeführt werden. Die digitalen Lernplattformen können zwar derzeit nur innerhalb des Campusnetzwerks genutzt werden, aber Systeme wie Moodle oder die Cloudlösung Sciebo stehen zur Verfügung.

Durch die frühzeitige Entscheidung, die Universität komplett vom Netz zu nehmen sowie die Verbindung zum Universitätsklinikum zu trennen, ist das Universitätsklinikum Essen nicht von dem Cyberangriff betroffen.

Auswirkungen auf Prüfungstermine oder -fristen können nicht vollständig vermieden werden: Am 29. November 2022 wurde bekanntgegeben, dass für alle schriftlich einzureichenden Prüfungsarbeiten die Abgabefristen im Zeitraum vom 28. November 2022 bis 12. Dezember 2022 pauschal um jeweils 14 Tage (vom Tag der eigentlichen Abgabe an) verlängert wurde. Arbeiten, die durch die Verlängerung an einem Wochenende oder Feiertag einzureichen wären, sind entsprechend über die Terminbriefkästen einzureichen. Am 30. November 2022 hat die Mercator School of Management ihre für Anfang Dezember geplante Prüfungsphase in die erste Woche nach den Weihnachtsferien (ab Dienstag, 10. Januar 2023) verschoben. Über eventuelle kurzfristige Änderungen der Prüfungstermine und Prüfungsfristen werden Studierende und auch die Öffentlichkeit fortlaufend informiert unter www.uni-due.org.

Dem einleitend genannten Bericht des Leitenden Oberstaatsanwalts in Köln zufolge sind auf Basis der bei der ZAC NRW geführten Verfahren aktuell Cyber-Angriffe auf informationstechnische Infrastrukturen privater und staatlicher Stellen, darunter wissenschaftliche Einrichtungen, zu

verzeichnen. Eine objektive Erkenntnislage ist - so der Leitende Oberstaatsanwalt in Köln - aufgrund des hohen Dunkelfeldes in diesem Deliktsbereich sowie des Fehlens differenzierbarer statistischer Erfassung bei den Staatsanwaltschaften indes nicht belastbar zu gewinnen und eine herausgehobene Betroffenheit von wissenschaftlichen Einrichtungen aktuell nicht festzustellen.

Der Leitende Oberstaatsanwalt in Köln hat ferner darauf hingewiesen, dass Ransomware-Angriffe regelmäßig unter Ausnutzung spezifischer IT-Sicherheitslücken der betroffenen Stelle erfolgten, eine besondere Schutzmöglichkeit für wissenschaftliche Stellen jenseits der für gegenüber dem Internet exponierten Strukturen geltenden Sicherheitsvorgaben nicht spezifisch ersichtlich sein dürfte und nach kriminalistischer Bewertung der monetäre Aspekt der Tatbegehung gegenüber dem Fokus auf Art und Inhalt der konkret betroffenen Daten regelmäßig im Vordergrund stehe.

Informationssicherheit hat auch im Hochschulumfeld eine immer größer werdende Relevanz. Die Hochschulen sind täglich hunderten von Angriffen ausgesetzt, die aber in der Regel nicht erfolgreich sind bzw. nicht mit einem Schadenereignis verbunden sind. Aufgrund ihrer offenen Struktur und ihrer systemisch bedingten heterogenen IT-Landschaften sehen sich Hochschulen hier einer besonderen Herausforderung gegenüber, die nicht mit einem geschlossenen Behörden- oder Firmennetzwerk vergleichbar ist. Tendenziell kann gesagt werden, dass Hochschulen mit eher technischer Ausrichtung stärker im Fokus der Angriffe stehen. Die Angriffswege Spear Phishing und CEO Frauding waren an allen Hochschulen feststellbar und sind durch Sensibilisierung des Personals weitgehend folgenlos geblieben.

Um die Cybersicherheit an den Hochschulen nicht zu gefährden und den Angreifern nicht zusätzliche detaillierte Informationen über konkrete Maßnahmen einzelner Hochschulen zur Verfügung zu stellen, können keine detaillierten Aussagen zum Schutz der Hochschulen gegen Cyberangriffe gemacht werden.

Grundsätzlich sind die von den Hochschulen ergriffenen Maßnahmen sehr stark von den an der jeweiligen Hochschule bereits eingesetzten Mitteln der Cyberabwehr abhängig. Neben dem Ausbau der technischen und automatisierten Abwehr von Angriffen liegen Ausbauschwerpunkte

in der Stärkung der Sensibilität des Personals (Awareness-Schulungen) zur Abwehr von Social Engineering als rasch wirksame Maßnahme und der Umsetzung des IT-Grundschutzes als langfristige Strategie. Mit dem Projekt SecAware.nrw unterstützt das Land die Hochschulen hierbei. Ziel des Projektes ist es, ein Online-Lernangebot zu schaffen, das die Nutzerinnen und Nutzer an den Hochschulen sensibilisiert und die entsprechenden IT-Kompetenzen im Kontext Cyberattacken schafft bzw. stärkt. Die Lerninhalte decken das gesamte Feld der Cyber- und Informationssicherheit ab und konfrontieren die Lernenden mit Gefährdungslagen ihrer jeweiligen digitalen Arbeits- und/oder Alltagswelt.

Die Hochschulen in Nordrhein-Westfalen sind an das Forschungsnetz des Vereins zur Förderung eines Deutschen Forschungsnetzes e. V. (DFN e.V.) angeschlossen. Der DFN e.V. erweitert aktuell seine Maßnahmen zur Cybersicherheit im Forschungsnetz mit dem neu konsolidierten Dienst DFN.Security. Die Einführung erfolgt in drei Phasen und soll Mitte 2023 abgeschlossen sein. Die Hochschulen erhalten mit diesem Basisdienst Warnmeldungen zu möglichen Sicherheitsvorfällen mit Bezug zu IP-Adressen (Phase 1) sowie eine Überwachung einer begrenzten Anzahl von IT-Systemen auf Kompromittierungen durch eine Logfile-Analyse (Phase 2) und durch ein aktives Dienstemonitoring (Phase 3).

Zur Absicherung von Haveriefällen haben sich die Hochschulen auf ein kooperatives Dienstekonzept für die Datensicherung geeinigt, das Anfang diesen Jahres gestartet ist. Ziel ist, mit Datensicherung.nrw eine effektive Datensicherung, die an wenigen Hochschulen betrieben werden muss, für alle Hochschulen anzubieten. In einem ersten Schritt hat das Land hierfür rund 11 Millionen Euro für die Lizenzen und für einen ersten Backup-Standort an der RWTH Aachen zur Verfügung gestellt. Weitere Backup-Standorte sollen folgen.

Mit dem Projekt „security.nrw“ fördert das Land die Beschaffung einer Landeslizenz von Schutzsoftware. Der Sicherheitsschutz umfasst alle dienstlich genutzten Endgeräte. Zusätzlich wird der Maileingangsverkehr auf Schadsoftware und SPAM gefiltert. Das Projekt ist auf fünf Jahre (7/2019 bis 6/2024) angelegt und umfasst eine Fördersumme von rund eine Million Euro. Der damit verbundene Schutz des Maileingangsverkehrs soll mittelfristig in das innovative Projekt „Anti-Spam-Cluster.nrw“ integriert werden, dass vom Land mit rund 2,5 Millionen Euro für

die Zeit von Juli 2020 bis Juni 2025 gefördert wird. Mit diesem Projekt soll die Abwehr von E-Mails mit schädlichen Inhalt auf eine zukunftsweisende und ausfallsicherere Basis an den Hochschulen gestellt werden. Dieses Projekt soll sich dank der verwendeten Cloud-Technologie nahtlos als weiterer Dienst in zukünftige Clouddienste der „Digitalen Hochschule NRW" integrieren.

Die Hochschulen wollen zukünftig im „Netzwerk Informationssicherheit.nrw" stärker zusammenarbeiten und sich gegenseitig in Havariefällen unterstützen. Hierzu hat das Land auf Empfehlung der „Digitalen Hochschule NRW" die Ausschreibung „Netzwerk Informationssicherheit.nrw" veröffentlicht. Damit soll zu Mitte 2023 der Aufbau einer hochschulübergreifenden Beratungs- und Koordinierungsstruktur zur Stärkung der Informationssicherheit an den Hochschulen in Nordrhein-Westfalen und zum Aufbau einer Informationssicherheitskultur erfolgen. Das Land fördert den Aufbau über drei Jahre mit rund zwei Millionen Euro.