Ministerium des Innern
des Landes Nordrhein-Westfalen

Der Minister

Ministerium des Innern NRW, 40190 Düsseldorf

Präsidenten des Landtags
Nordrhein-Westfalen
Herrn André Kuper MdL
Platz des Landtags 1
40221 Düsseldorf

13 Dezember 2022

Telefon 0211 871-3398
Telefax 0211 871-3398

für die Mitglieder
des Innenausschusses

Sitzung des Innenausschusses am 15.12.2022
Antrag der Fraktion der SPD vom 30.11.2022
„Cyberangriff auf die Universität Duisburg-Essen“

Sehr geehrter Herr Landtagspräsident,

zur Information der Mitglieder des Innenausschusses des Landtags übersende ich den schriftlichen Bericht zum TOP „Cyberangriff auf die Universität Duisburg-Essen“.

Mit freundlichen Grüßen

Herbert Reul MdL

Dienstgebäude:
Friedrichstr. 62-80
40217 Düsseldorf

Lieferanschrift:
Fürstenwall 129
40217 Düsseldorf

Telefon 0211 871-01
Telefax 0211 871-3355
poststelle@im.nrw.de
www.im.nrw

Öffentliche Verkehrsmittel:
Rheinbahnlinien 732, 736, 835, 836, U71, U72, U73, U83
Haltestelle: Kirchplatz

Ministerium des Innern
des Landes Nordrhein-Westfalen

Der Minister

Schriftlicher Bericht
des Ministers des Innern
für die Sitzung des Innenausschusses am 15.12.2022
zu dem Tagesordnungspunkt
„Cyberangriff auf die Universität Duisburg-Essen“
Antrag der Fraktion der SPD vom 30.11.2022

1 Ermittlungsstand

Das Ministerium der Justiz nimmt zum Ermittlungsstand wie folgt Stellung:

„Der Leitende Oberstaatsanwalt in Köln hat dem Ministerium der Justiz unter dem 02.12.2022 zu der Frage Folgendes berichtet:

> *‚Die Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen führt auf Grundlage einer Strafanzeige der Universität Duisburg-Essen vom 28.11.2022 ein Ermittlungsverfahren gegen unbekannt wegen Erpressung unter anderem zum Nachteil der Anzeigeerstatterin.*
>
> *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 durch das Polizeipräsidium Essen geführt.‘*

Dem vorbezeichneten Bericht zufolge sei nach derzeitigem Ermittlungsstand von einem – nach Art und Ausmaß bisher ungeklärten – Datenabfluss auszugehen. Das IT-System der Geschädigten sei faktisch außer Betrieb. IT-Systeme des Universitätsklinikums Essen und des Forschungsnetzwerks Deutschland, zu denen IT-Schnittstellen bestünden, seien nach derzeitiger Erkenntnislage nicht betroffen. Eine Aussage zu dem wirtschaftlichen Schaden könne seitens der Staatsanwaltschaft derzeit nicht getroffen werden.

Eine Veröffentlichung etwaig erlangter Daten durch die Täter sei dem vorbezeichneten Bericht zufolge bisher nicht bekannt. Ein Zugriff auf weitere als die im Rahmen des vorbezeichneten Angriffs etwaig erlangten Daten sei derzeit ausgeschlossen, nachdem das IT-System der Geschädigten vom Netz genommen worden sei. Der Schutz bereits im Internet exponierter Daten sei ex-post prinzipiell nicht möglich."

Das Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen berichtet mir zur den Schäden an der IT-Infrastruktur und damit verbundenen Einschränkungen wie folgt:

„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 beziehungsweise 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 06.12.2022) daher noch nicht vor.

Durch den Cyberangriff wurde der universitäre Betrieb beeinträchtigt: Wie am 28.11.2022 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."

2 Gefährdungslage für wissenschaftliche Einrichtungen

Das Risiko für Cyberangriffe auf wissenschaftliche Einrichtungen, Wirtschaftsunternehmen, kommunale Einrichtungen und die weitere Cyberkriminalität wird in Nordrhein-Westfalen, dem Bund und den übrigen Ländern permanent bewertet. Dies gilt insbesondere im Kontext zum russischen Angriffskrieg gegen die Ukraine. Das Nationale Cyberabwehrzentrum stuft die Cyberbedrohungslage in Deutschland als unverändert hoch ein. Cyberangriffe, insbesondere durch hacktivistische und kommerziell motivierte Gruppierungen, mit möglicher Auswirkung auf Deutschland sind weiterhin wahrscheinlich. Ransomware-Angriffe stellen derzeit den Schwerpunkt der Bedrohungslage dar. Dies gilt auch für den Wissenschaftsstandort Deutschland sowie die in Nordrhein-Westfalen angesiedelten Einrichtungen.

Im Landeskriminalamt Nordrhein-Westfalen ist mit der Zentralen Ansprechstelle Cybercime ein Single Point of Contact für Wirtschaft, Behörden und wissenschaftliche Einrichtungen in Nordrhein-Westfalen etabliert. So wird eine schnelle Reaktion der Polizei auf Cyberangriffe sichergestellt. Die Koordinierungsstelle Cybersicherheit im Ministerium des Innern des Landes Nordrhein-Westfalen übernimmt eine zentrale Schnittstellenfunktion. Mit dem Operativen Austausch Cybercrime ist ein ressortübergreifender Spezialistenkreis geschaffen und der Informationsaustausch gewährleistet.

Das Ministerium der Justiz nimmt zur Gefährdungslage und möglichen Abwehrmaßnahmen wie folgt Stellung:

„Der Leitende Oberstaatsanwalt in Köln hat dem Ministerium der Justiz unter dem 02.12.2022 zu der Frage Folgendes berichtet:

‚Auf Basis der bei der Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen geführten Verfahren sind aktuell Cyber-Angriffe auf informationstechnische Infrastrukturen privater und staatlicher Stellen, darunter wissenschaftliche Einrichtungen, zu verzeichnen. Eine objektive Erkenntnislage ist aufgrund des hohen Dunkelfeldes in diesem Deliktsbereich sowie des Fehlens differenzierbarer statistischer Erfassung bei den Staatsanwaltschaften indes nicht belastbar zu gewinnen. Eine herausgehobene Betroffenheit von wissenschaftlichen Einrichtungen kann dabei jedoch aktuell nicht festgestellt werden.

Ransomware-Angriffe erfolgen regelmäßig unter Ausnutzung spezifischer IT-Sicherheitslücken der betroffenen Stelle. Insoweit dürfte eine besondere Schutzmöglichkeit für wissenschaftliche Stellen jenseits der für gegenüber dem Internet exponierten Strukturen geltenden Sicherheitsvorgaben nicht spezifisch ersichtlich sein. Nach kriminalistischer Bewertung steht überdies der monetäre Aspekt der Tatbegehung gegenüber dem Fokus auf Art und Inhalt der konkret betroffenen Daten regelmäßig im Vordergrund.“

Das Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen berichtet mir zur Informationssicherheit an Hochschulen des Landes Nordrhein-Westfalen wie folgt:

„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 beziehungsweise 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 und 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 Maileingangsver-kehr auf Schadsoftware und SPAM gefiltert. Das Projekt ist auf fünf Jahre (7/2019 bis 6/2024) angelegt und umfasst eine Fördersumme von rund einer Millionen Euro. Der damit verbundene Schutz des Maileingangsver-kehrs 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 7/2020 bis 6/2025 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 Nordrhein-Westfalen“ 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 Nordrhein-Westfalen" 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.“