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

LANDTAG
NORDRHEIN-WESTFALEN
18. WAHLPERIODE

VORLAGE
18/921

A09

für die Mitglieder
des Innenausschusses

1. März 2023
Seite 1 von 7

Telefon 0211 871-3254
Telefax 0211 871-

Sitzung des Innenausschusses am 02.03.2023
Antrag der Fraktion der SPD vom 16.02.2023 „Hackerangriffe auf Hochschulen in Nordrhein-Westfalen“

Sehr geehrter Herr Landtagspräsident,

zur Information der Mitglieder des Innenausschusses des Landtags übersende ich den schriftlichen Bericht zu dem TOP „Hackerangriffe auf Hochschulen in Nordrhein-Westfalen“.

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 02.03.2023
zu dem Tagesordnungspunkt „Hackerangriffe auf Hochschulen in Nordrhein-Westfalen“

Antrag der Fraktion der SPD vom 16.02.2023

Hinsichtlich des Angriffs auf die Hochschule Ruhr West hat mir das Ministerium für Kultur und Wissenschaft folgenden Beitrag zur Verfügung gestellt:

> „Am 31.01.2023 ist die Hochschule Ruhr West Opfer eines Cyberangriffs geworden. Das technische Sicherheitssystem hatte an diesem Tag verdächtige Aktivitäten aufgedeckt und gemeldet. Nach der automatisierten Abwehr dieser Aktivitäten kam es zu erneuten Aktivitäten, die zum Ziel hatten, in die Systeme der Hochschule einzudringen. Daraufhin hat die Hochschule sämtliche webbasierten Systeme umgehend, konsequent und vollständig vom Netz getrennt. Dies hat zur Folge, dass alle Kommunikationssysteme, das Campusmanagementsystem, die digitalen Lernumgebungen und die Systeme für den Personal- und Finanzbereich außer Funktion sind. In der Analyse ist deutlich geworden, dass die rechtzeitige Entdeckung und das umgehende und konsequente Vom-Netz-Nehmen aller Systeme die Fortsetzung der Angriffe wirksam vereitelt hat. Die forensische Analyse dauert an. Sie hat bislang weiterhin keine Anhaltspunkte für die Verschlüsselung von Daten ergeben. Der Datenverlust dürfte sich in sehr engen Grenzen halten. Der konkrete Datenverlust ist erst dann feststellbar, wenn die webbasierten Systeme wieder angeschlossen werden. Wann alle Systeme

wieder online sein werden, ist derzeit noch nicht abzusehen. Das Festnetz an beiden Campusstandorten ist wieder in Betrieb.
Die Online-Prüfungen für Studierende, die derzeit nur einen geringen Teil ausmachen, sind derzeit nicht möglich, Präsenzprüfungen finden dagegen statt. Ein mögliches Nichtantreten soll ohne Folgen bleiben und es soll eine kulante Regelung für ein späteres Nachholen geben. Um Studierenden und Lehrenden genügend Zeit für die Vorbereitung zu geben, wird die zweite Prüfungsphase vom 06.03. bis 18.03.2023 um zwei Wochen auf den Zeitraum vom 20.03. bis 01.04.2023 verschoben. Für Prüfungen, die zwischen dem 01.02. bis 11.02.2023 ausgefallen sind, finden Ersatzprüfungen statt. Außerdem werden für alle Prüfungen, die im gleichen Zeitraum stattgefunden haben, zusätzliche Termine (Zusatzprüfungen) angeboten.
Der Beginn der Vorlesungszeit wird um zwei Wochen auf den 03.04.2023 verschoben.

Da die Homepage der Hochschule von einem Dienstleister gehostet wird, ist diese vom Angriff nicht betroffen und wird als Kommunikationsplattform genutzt. So finden sich dort unter ständigen Aktualisierungen u.a. adressatengerechte FAQs für die unterschiedlichen Interessengruppen.
Es finden derzeit parallel Arbeiten an den Systemen und den zukünftigen Sicherheitslevels statt (z.B. 2-Faktor-Authentifizierung). Zudem fand vor Ort eine großangelegte Aktion zum Passwort-Reset statt: Mehr als 4.000 von rund 7.000 Personen haben ihr Passwort zurückgesetzt. Anfang März sollen die ersten Systeme wieder hochgefahren werden, angesichts der nachzuholenden Prüfungsphase zunächst das Campusmanagementsystem und Moodle."

Das Ministerium der Justiz hat diesbezüglich folgenden Beitrag zur Verfügung gestellt:

> „Erkenntnisse zur Identität der Täter liegen bisher nicht vor. Die Ermittlungen, auch zu den Hintergründen der Tat, dauern an."

Hinsichtlich des Angriffs auf die Universität Duisburg-Essen hat mir das Ministerium für Kultur und Wissenschaft folgenden Beitrag zur Verfügung gestellt:

> „Die Universität Duisburg-Essen hat dem Ministerium für Kultur und Wissenschaft berichtet, dass eine nachhaltige Schädigung des Lehr- und Forschungsbetriebs an der Universität trotz der temporären Einschränkungen nicht angenommen werde.
> Es seien schnelle Lösungen geschaffen worden, um Studium, Lehre, die laufenden Prüfungsarbeiten und den Verwaltungsbetrieb zu gewährleisten. Trotz des Hackerangriffs laufe der Lehrbetrieb regulär weiter. Die Noten und erbrachten Leistungen der Studierenden seien gesichert.
> Über 30.000 Studierende hätten nach dem Passwort-Reset auch von außerhalb des Campus wieder Zugriff auf die Lernplattformen Moodle und JACK. Nachdem der Zugriff auf das Informationssystem rund um Studium und Lehre und vor allem die Selbstbedienungsfunktionen des Hochschulportals HISinOne seit Jahresende nur vom Campus aus zu erreichen gewesen wäre, werde der externe Zugriff am 27.02.2023 freigeschaltet.
>
> Die Studierenden seien fortlaufend über eine schnell eingerichtete Homepage und die sozialen Medien über aktuelle Entwicklungen informiert. Sie könnten, ebenso wie die Beschäftigten der Universität Duisburg-Essen, auch wieder über Rundmails erreicht

werden. Die Nutzung von E-Mail unter Verwendung der früheren Adressen sei für alle, die ein Passwort-Reset durchgeführt haben, wieder möglich, ebenso wie der Zugriff von außen via Webmail. Es sei möglich, sich zu Prüfungen an- oder abzumelden und Studienbescheinigungen, das Semesterticket oder Notenspiegel herunterzuladen. Die Prüfungen am Ende des Wintersemesters werden wie geplant stattfinden können. In einigen Bereichen seien die Fristen für schriftlich einzureichende Prüfungsarbeiten verlängert worden. Da die Prüfungsvorbereitungen sowie die Prüfungsplanung inkl. Raumvergabe ordnungsgemäß durchgeführt werden konnten, finde die anstehende Prüfungsphase des Wintersemesters wie geplant in der vorlesungsfreien Zeit ab Mitte Februar statt. Für die von Teilen der Studierendenschaft geforderten Freiversuche habe die Universität Duisburg-Essen einen Kompromiss erarbeitet, um den Studierenden, die besondere Belastungen in der jetzigen Situation verspüren, entgegenzukommen.

Das für das Personal- und Finanzmanagement wichtige SAP System werde von einigen „Key Usern" wieder genutzt und getestet. Die volle Verfügbarkeit und die Nacharbeitung von Vorgängen der vergangenen Wochen werde noch einige Zeit erfordern.
Seit Mitte Februar sei auch das digitale Identity-Management (IDM) in Betrieb, das Benutzerkonten, Passwörter und andere Identitätsmerkmale verwaltet. Dort werden auch die Berechtigungen festgelegt, die den Zugang zu Systemen und Daten regeln, weshalb es grundlegend dafür sei, wieder den Zugriff auf Arbeits-, Lehr- und Forschungsdaten zu ermöglichen, die auf den Fileservern der Hochschule abgelegt sind. Dies würde ab dem 23.02.2023 schrittweise erfolgen.

Die in den elektronischen Laborbüchern gespeicherten Forschungsdaten stünden den Wissenschaftlerinnen und Wissenschaftlern seit Mitte Februar wieder zur Verfügung.
Die Universität Duisburg-Essen hofft auf einen hohen Grad an „Normalität" bis zum Sommersemester 2023, auch wenn bis dahin ggf. noch nicht alle Funktionen wieder vollständig hergestellt sein werden.
Nach Angaben der Universität Duisburg-Essen ist eine Liste aller Studierenden des Wintersemesters 2022/2023 veröffentlicht worden. Die Liste enthielte Namen und Kontaktdaten (postalisch, Universitäts-E-Mail-Adresse), Semesterzahl sowie Studiengangs- und Fakultätszuordnungen. Solche Listen existierten ebenfalls für die Absolventinnen und Absolventen der letzten Jahre. Telefonnummern seien nicht veröffentlicht worden. Vereinzelt seien unter den veröffentlichten Daten auch Semester- und Abschlussarbeiten, Einsichtsprotokolle zu Prüfungen, Ergebnislisten zu Einzelprüfungen oder auch Notenspiegel zu finden. Die Studierenden wären darüber per E-Mail informiert worden bzw. würden derzeit postalisch informiert.
Zusätzlich wären auch medizinisch-wissenschaftliche Daten mit Personenbezug (Vorname, Nachname, teilweise Geburtsdaten sowie teils mit Hinweis auf einen Studienkontext) gefunden worden. Die betroffenen Personen würden, soweit eine Identifizierung möglich ist, über das Universitätsklinikum Essen persönlich informiert.
Vereinzelt seien auch persönliche Verzeichnisse von Beschäftigten und darin abgelegte (arbeitsbezogene) Dateien veröffentlicht worden. Wenn daraus besondere Risiken abgeleitet werden könnten, werde die Universität weitere Schritte einleiten. Die Inhaberinnen und Inhaber der Verzeichnisse würden derzeit sukzessive persönlich informiert. Hierzu habe ein Termin mit den

Leitungen der betroffenen Organisationseinheiten stattgefunden. Die Einheiten würden dann auf Grundlage ihres Kontextwissens weitere betroffenen Personen kontaktieren.
Der behördliche Datenschutzbeauftragte der Universität Duisburg-Essen stehe in der Angelegenheit in einem stetigen Austausch mit der Landesbeauftragten für Datenschutz und Informationsfreiheit in NRW."

Das Ministerium der Justiz hat diesbezüglich folgenden Beitrag zur Verfügung gestellt:

„Erkenntnisse zur Identität der Täter liegen bisher nicht vor. Die Ermittlungen, auch zu den Hintergründen der Tat, dauern an.

Im Namen der Gruppierung „Vice Society" sind seit Mitte 2021 weltweit Ransomware-Angriffe insbesondere auf Einrichtungen des Bildungs- und Gesundheitswesens erfolgt. Weitere belastbare Erkenntnisse zu dieser Gruppierung liegen derzeit nicht vor."