RheinlandPfalz
MINISTERIUM FÜR WISSENSCHAFT UND GESUNDHEIT

LANDTAG
Rheinland-Pfalz
18/6326
VORLAGE

Ministerium für Wissenschaft und Gesundheit
Postfach 32 20 | 55022 Mainz

Vorsitzende des Ausschusses
für Wissenschaft
Frau Marion Schneid, MdL
Landtag Rheinland-Pfalz
Platz der Mainzer Republik 1
55116 Mainz

DER MINISTER

Mittlere Bleiche 61
55116 Mainz
Telefon 06131 16-0
Telefax 06131 16-29 57
clemens.hoch@mwg.rlp.de
www.mwg.rlp.de

9. September 2024

Mein Aktenzeichen	Ihr Schreiben vom	Ansprechpartner/-in / E-Mail	Telefon / Fax
0102-0005#2023/0016-1501 MB Bitte immer angeben!		Lucas Muth lucas.muth@mwg.rlp.de	06131 16-2871 06131 16-2997

27. Sitzung des Ausschusses für Wissenschaft am 28.08.2024

TOP 7 : Hackerangriff auf die Universität Koblenz
Antrag der Fraktion der CDU
nach § 76 Abs. 2 GOLT - V 18/6232 -
hier: schriftliche Berichterstattung

Sehr geehrte Frau Vorsitzende,

der o. g. Tagesordnungspunkt wurde in der Sitzung des Ausschusses mit der Maßgabe der schriftlichen Berichterstattung durch die Landesregierung für erledigt erklärt. Daher berichte ich wie folgt:

Die aktuelle Häufung von Cyberangriffen auf Hochschulen und Wissenschaftseinrichtungen hat verheerende und kostenintensive Folgen für die Hochschulen und den Staat. Dies trifft nicht nur Rheinland-Pfalz, sondern Einrichtungen in der gesamten Bundesrepublik. So hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Bedrohungslage für Deutschland in seinem letzten Lagebericht so hoch eingeschätzt wie noch nie. Der Angriffskrieg in der Ukraine und die globalen Spannungen zwischen China und den USA sowie der Konflikt im Nahen Osten hat diese Entwicklung weiter verstärkt.

Erfolgreiche Angriffe schädigen die Geschäftsprozesse der Hochschulen stark, so zum Beispiel durch:

- Blockade der digitalisierten Prozesse (wie z.B. Zulassung, Einschreibung, Campus-Management-Systeme) und des Rechnungswesens der Hochschule,
- Diebstahl der Zugangsdaten, Übernahme und Sabotage von einzelnen Systemen mit Erpressungsversuchen,
- Übernahme der zentralen Nutzer- und Geräteverwaltung mit größeren Ausfallzeiten,
- Erpressungsversuche und Verkauf der erbeuteten Daten.

Die in der am 10.05.2024 erschienenen Ausgabe der Rheinzeitung geschilderten Vorgänge entsprechen im Wesentlichen den Tatsachen. Im darin dargestellten Fall der Universität Koblenz konnte durch das besonnene und schnelle Handeln der Universitätsleitung jedoch Schlimmeres verhindert werden.

Der Angriff erfolgte bereits am 06.05.2024. Noch am gleichen Tag hat der Präsident der Universität Koblenz, Herr Professor Wehner – der in einem engen Austausch mit dem Ministerium für Wissenschaft und Gesundheit steht –, den mutmaßlichen Datenangriff gemeldet und alle notwendigen Sofortmaßnahmen eingeleitet. Herr Präsident Wehner berichtete, dass das potenzielle Datenleck aufgrund des Sicherheitsmonitorings der universitären IT-Systeme frühzeitig entdeckt wurde.

Als Sofortmaßnahmen wurden durch die Universitätsleitung folgende Schritte eingeleitet: Nachdem das Datenleck identifiziert worden war, wurde das Anmeldeportal des Allgemeinen Hochschulsports umgehend vom Netz genommen. Alle betroffenen Personen wurden unmittelbar über das potentielle Datenleck und notwendige sicherheitsrelevante Schritte informiert.

Ebenso hat die Universitätsleitung bereits am 07.05.2024 Strafanzeige gestellt; die Polizei und Staatsanwaltschaft haben die Ermittlungen aufgenommen. Das strafrechtliche Ermittlungsverfahren dauert noch an.

Darüber hinaus wurden am gleichen Tag der Landesbeauftragte für den Datenschutz und die Informationsfreiheit und die Hochschule Koblenz als Mitbetreiber des AHS informiert.

Alle Dienste des ZIMT (Zentrum für Informations- und Medientechnologien) wurden unmittelbar durch strengere Zugriffsregeln der Universitäts-Firewall gesichert.

Zwischenzeitlich wurde ein neues digitales Buchungssystem, das sich aktuell auf der Seite des Allgemeinen Hochschulsports befindet, eingeführt.

Die potenziellen „Erpresser“ haben allerdings laut einer internen Analyse nie eine Lösegeldaufforderung gestellt. Vielmehr wurde formuliert, dass Emailadressen und Passwörter bekannt sind und weiterverwendet werden könnten. Konkrete Fälle sind jedoch nicht bekannt.

Vor dem Hintergrund der aktuellen Herausforderungen und Bedrohungen kommt der IT-Sicherheit der Hochschulen eine wachsende Relevanz zu. Die Landesregierung ist sich ihrer Verantwortung bewusst und hat dieses Themenfeld daher mit einer hohen Priorität versehen.

Bereits in den Jahren 2020 bis Ende 2023 hat die Landesregierung den Hochschulen im Rahmen des Programms zur Stärkung der Digitalisierung an den Hochschulen zusätzliche Mittel u. a. für Fördermaßnahmen zur „Stärkung und Ausbau der hochschulübergreifenden digitalen Infrastrukturen und der IT-Sicherheit“ zur Verfügung gestellt.

Mithilfe dieser zusätzlichen Mittel wurde neben dem bedarfsgerechten Upgrade der Leitungsgeschwindigkeiten des Wissenschaftsnetzes Rheinland-Pfalz (WiN-RP) insbesondere auch sein redundanter Ausbau vorangetrieben, um die Resilienz des Hochschulnetzes zu stärken und die Arbeitsfähigkeit der Hochschulen bei Ausfällen im Primärnetz sicherzustellen (Projekt „Extend WiN-RP“: Umfang ca. 1 Mio. €).

Im Rahmen des Projekts „Integration zentraler IT-Infrastrukturen und IT-Dienste der Rechenzentrumsallianz Rheinland-Pfalz sowie Unterstützung beim Aufbau eines Informations-Sicherheitsmanagementsystems (ISMS) an allen Universitäten und Hochschulen des Landes“ wurden sogenannte Penetrationstests durch einen externen Auftragnehmer durchgeführt. Die Ergebnisse dieser Tests dienen den Hochschulen als Grundlage, die eigene Sicherheit zu bewerten und zu verbessern. Zudem wurde eine weitere Firma mit der Konzeption eines Informationssicherheitsmanagements an den Hochschulen beauftragt. In diesem Zusammenhang erfolgte eine Schulung für Mitarbeitende aus allen Hochschulen im Rahmen des „BSI-IT-Grundschutz-Praktiker“.

Zudem wurden zentrale Hardwareinvestitionen in Storage-Kapazitäten getätigt, um den Hochschulen unabhängig von der jeweils lokalen IT geschützte Backup-Möglichkeiten zur Verfügung stellen zu können. Für dieses Maßnahmenpaket wurden insgesamt ca. 1,5 Mio. € investiert.

Ferner nutzten einzelne Hochschulen Mittel, die ihnen für eigene Digitalisierungsbedarfe bewilligt wurden, u. a. für den Ausbau der eigenen IT-Sicherheit (z. B. Firewall, Ausbau der Serverkapazität) (Umfang ca. 100.000 €).

Die IT-Sicherheit der Hochschulen wird auch weiterhin eng von der Landesregierung begleitet. Im Januar dieses Jahres hat sich Minister Hoch mit den Hochschulpräsidentinnen und -präsidenten des Landes im Rahmen des Hochschulforums darauf verständigt, dass das Thema IT-Sicherheit mit höchster Priorität vorangebracht und bearbeitet werden soll.

Ziel ist es, in einem engen gemeinsamen Dialog hochschulübergreifend die IT-Sicherheit der Hochschulen zu stärken, Synergien in diesem Bereich (auch vor dem Hintergrund des Fachkräftemangels im IT-Bereich) zu heben und das Sicherheitsniveau an allen Hochschulen im Land auf einen gemeinsamen Mindeststandard zu setzen. Hierzu erarbeitet eine Beratungsgruppe des Hochschulforums, bestehend aus Rechenzentrumsleitern und Hochschulleitungen, derzeit ein aufeinander abgestimmtes Maßnahmenpaket, das im Rahmen des nächsten Hochschulforums diskutiert werden soll.

Im Rahmen der Haushaltsaufstellung zum Doppelhaushalt 2025/2026 wurde entsprechende Vorsorge für ein Maßnahmenpaket zur Unterstützung der Hochschulen im Bereich der Informationssicherheit getroffen.

Mit freundlichen Grüßen

Clemens Hoch