

12.02.2020

## Antwort

der Landesregierung

auf die Kleine Anfrage 3326 vom 17. Januar 2020  
des Abgeordneten Matthi Bolte-Richter BÜNDNIS 90/DIE GRÜNEN  
Drucksache 17/8500

### **Wie steht es um die IT-Sicherheit an den nordrhein-westfälischen Hochschulen?**

#### ***Vorbemerkung der Kleinen Anfrage***

Am 8. Dezember 2019 führte ein Hackerangriff auf die Justus-Liebig-Universität Gießen dazu, dass diese alle ihre IT-Systeme abschalten musste. Nachdem eine Infektion mit der Ransomware Ryuk entdeckt wurde, wurden sicherheitshalber alle Systeme abgeschaltet, um einen flächendeckenden Befall zu verhindern. Ryuk erfolgt als weitere Infektionswelle nach einem Befall durch den Trojaner Emotet, der meist als Anhang zu einer E-Mail getarnt wird. Während Emotet Sicherheitslücken ausfindig macht und Daten ausspäht, erfolgt durch Ryuk eine Verschlüsselung der Daten zwecks Erpressung.

Für Beschäftigte und Studierende der Universität Gießen gab es in Folge dessen keinen Zugang mehr zu E-Mails, digitalen Lehrmaterialien, Vorlesungsverzeichnis, Prüfungs- und Personalverwaltung und vielen weiteren Informationen und Vorgängen, die an Hochschulen heutzutage digital erfolgen. Die Universität geht aktuell davon aus, dass erst Mitte Februar wieder grundsätzlich alle Computersysteme normal laufen werden.

Auch die Universität Maastricht und die Katholische Hochschule in Freiburg im Breisgau mussten wenige Tage nach dem Vorfall in Gießen sämtliche IT-Systeme auf Grund einer Emotet-Infektion runterfahren, im September traf es die Medizinische Hochschule Hannover. Aber auch mehrere Stadtverwaltungen und Krankenhäuser sahen sich Cyber-Attacken ausgesetzt, die teilweise für die Angreifer erfolgreich verliefen. Angriffe mit einer neuen Generation des Trojaners Emotet erfolgen seit Monaten wieder verstärkt und gezielt auf öffentliche Einrichtungen. Nicht mehr nur Unternehmen sind gefährdet, für die Cyberkriminalität bereits weltweit das größte Risiko darstellt.

Datum des Originals: 12.02.2020/Ausgegeben: 18.02.2020

Die Veröffentlichungen des Landtags Nordrhein-Westfalen sind einzeln gegen eine Schutzgebühr beim Archiv des Landtags Nordrhein-Westfalen, 40002 Düsseldorf, Postfach 10 11 43, Telefon (0211) 884 - 2439, zu beziehen. Der kostenfreie Abruf ist auch möglich über das Internet-Angebot des Landtags Nordrhein-Westfalen unter [www.landtag.nrw.de](http://www.landtag.nrw.de)

**Die Ministerin für Kultur und Wissenschaft** hat die Kleine Anfrage 3326 mit Schreiben vom 12. Februar 2020 namens der Landesregierung im Einvernehmen mit dem Minister der Finanzen, dem Minister des Innern, dem Minister für Wirtschaft, Innovation, Digitalisierung und Energie sowie dem Minister der Justiz beantwortet.

### ***Vorbemerkung der Landesregierung***

Da der Begriff „Hochschulen in NRW“ nicht näher spezifiziert ist, wird aufgrund des Gesamtzusammenhanges der Kleinen Anfrage davon ausgegangen, dass sich die Fragen auf die Universitäten und Hochschulen für angewandte Wissenschaften in der Trägerschaft des Landes sowie die staatlichen Kunsthochschulen beziehen.

- 1. *Wie viele Cyber-Angriffe hatten die Hochschulen in NRW jährlich von 2015 bis 2019 zu verzeichnen?***
- 2. *In wie vielen Fällen verliefen die Angriffe für die Angreifer erfolgreich?***

Die Fragen 1 und 2 werden zusammen beantwortet.

Für die Universitäten und Hochschulen für angewandte Wissenschaften in der Trägerschaft des Landes sowie für die staatlichen Kunsthochschulen gilt aufgrund von § 1 Abs. 6 Satz 1 EGovG NRW u.a. der § 22 EGovG NRW nicht. Deshalb koordiniert der Beauftragte der Landesregierung für Informationstechnik nicht die informationstechnische Sicherheit bei diesen Hochschulen.

Dementsprechend gilt auch die von der Landesregierung beschlossene Informationssicherheitsleitlinie NRW nicht für die Universitäten und Hochschulen für angewandte Wissenschaften in der Trägerschaft des Landes sowie für die staatlichen Kunsthochschulen, wobei auch diesen Stellen im Interesse einer einheitlichen Sicherheitspolitik der öffentlichen Verwaltung die Berücksichtigung der Leitlinie empfohlen worden ist.

Vor diesem Hintergrund wäre für die Beantwortung der erhobenen Fragen eine aktuelle Abfrage bei den Universitäten und Hochschulen für angewandte Wissenschaften in der Trägerschaft des Landes sowie den staatlichen Kunsthochschulen erforderlich. Aufgrund der Kürze der für die Beantwortung der Kleinen Anfrage zur Verfügung stehenden Zeit ist es nicht möglich, die erbetenen Auskünfte von den Hochschulen zu erlangen.

- 3. *Welche Maßnahmen haben Hochschulen und Landesregierung gegen Cyber-Angriffe auf Hochschulen ergriffen?***
- 4. *Welche Ausbaupläne haben Hochschulen und Landesregierung im Bereich IT-Sicherheit an Hochschulen?***
- 5. *Mit welchen Mitteln fördert die Landesregierung den Ausbau der IT-Sicherheit an Hochschulen?***

Die Fragen 3 bis 5 werden zusammen beantwortet.

Die Landesregierung stellt bis 2021 jährlich zusätzlich 50 Millionen Euro und danach jeweils 35 Millionen Euro für eine landesweite Digitalisierungsoffensive an den Hochschulen zur Verfügung. Aktuell erarbeitet die DH.NRW ein neues Programm, in dem das Thema „Informationssicherheit“ - auch vor dem Hintergrund der aktuellen Ereignisse an der Universität Gießen - einen Schwerpunkt bildet.

Die Landesregierung unterstützt den Ausbau der IT-Sicherheit an den Hochschulen aus Mitteln der landesweiten Digitalisierungsoffensive durch aktuell folgende Projekte:

Mit dem Projekt „security.nrw“ erfolgt die Förderung eines Konsortiums für 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 angelegt und umfasst eine Fördersumme von rd. 1 Million Euro.

Mit dem Projekt „Anti-Spam-Cluster.nrw“ soll die Abwehr von E-Mails mit schädlichen Inhalt auf eine zukunftsweisende und ausfallsicherere Basis an den Hochschulen in Nordrhein-Westfalen gestellt werden. Dieses Projekt soll sich dank der verwendeten Cloud-Technologie nahtlos als weiterer Dienst in die „hochschulcloud.nrw“ integrieren. Dieser Dienst unterstützt dabei ausdrücklich auch andere Vorhaben der DH.NRW wie die „AcademicGroupware.nrw“. Das Projekt wird mit 2,5 Millionen Euro finanziert.

Der Schutz des Maileingangsverkehrs aus dem Projekt „security.nrw“ wird mittelfristig in das „Anti-Spam-Cluster.nrw“ integriert.

Die Angebote des nordrhein-westfälischen Verfassungsschutzes zur Sensibilisierung im Kontext von Wirtschaftsspionage und Cyberangriffen stehen grundsätzlich auch den nordrhein-westfälischen Hochschulen und Forschungseinrichtungen zur Verfügung. Gerade in den letzten Jahren gab es hierzu immer wieder Kontakte zwischen dem nordrhein-westfälischen Verfassungsschutz und verschiedenen Stellen des Hochschul- und Forschungsbereichs.

Zuletzt hat der nordrhein-westfälische Verfassungsschutz im Januar dieses Jahres im Kreis der „Landesrektorenkonferenz der Universitäten e. V.“ sensibilisiert. Dabei wurde konkret das Angebot unterbreitet, auf der Ebene der Fakultäten und Institute bedarfsgerechte Sensibilisierungsvorträge abzustimmen und anzubieten. Das gleiche Vorgehen ist für die „Landesrektor\_innenkonferenz der Hochschulen für Angewandte Wissenschaften e. V.“ geplant.