BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG **Drucksache 21/15874**
21. Wahlperiode **25.01.19**

Schriftliche Kleine Anfrage

des Abgeordneten Carsten Ovens (CDU) vom 18.01.19

und Antwort des Senats

Betr.: Wie gut sind die Hamburger Hochschulen auf Cyberangriffe vorbereitet?

Mit über 100 000 eingeschriebenen Studenten verwalten die Hamburger Hochschulen eine entsprechend große Menge an personenbezogenen Daten. Darüber hinaus werden in den IT-Systemen wertvolle und forschungssensible Daten gespeichert. Diese beiden Faktoren können dazu beitragen, dass die Hamburger Hochschulen als lohnenswertes Ziel von Hackern betrachtet werden. Die jüngsten groß angelegten Hackerangriffe auf Politiker, welche die Veröffentlichung privater wie beruflich sensibler Dokumente zur Folge hatten, haben schmerzhaft die Realität der Bedrohung durch Hacker verdeutlicht.

In Drs. 21/11952 zeichnet der Senat ein insgesamt positives Bild der Cybersicherheit an den Hamburger Hochschulen. Das Rechenzentrum der Universität Hamburg (UHH) selbst hat jedoch in den vergangenen Monaten mehrmals von hochwertigen Cyberangriffen gegen deutsche Universitäten und Forschungseinrichtungen gesprochen und vor Phishing-Mails gewarnt, die einen universitären Ursprung vortäuschen und Schadsoftware verbreiten. Es stellt sich die Frage, ob demnach der Status der Cybersicherheit an den Hamburger Hochschulen neu bewertet werden muss.

Vor diesem Hintergrund frage ich den Senat:

Die Anfrage richtet sich zum Teil auf sensible Informationen zur IT-Sicherheit der Hochschulen, deren Veröffentlichung Angriffe auf die hochschulischen IT-Systeme erleichtern und deren Schutz gefährden kann. Einzelne Antworten beschränken sich vor diesem Hintergrund auf zusammenfassende Angaben.

Dies vorausgeschickt, beantwortet der Senat die Fragen auf der Grundlage von Auskünften der staatlichen und privaten, in Hamburg staatlich anerkannten Hochschulen wie folgt:

1. *Hackerangriffe*

   a. *Wie viele Hackerangriffe gab es auf die Hochschulwebseiten, Datenbanken und sonstige über das öffentliche Netz erreichbare Server der staatlichen und privaten Hamburger Universitäten und Hochschulen seit Anfang 2017? Bitte differenziert nach Jahr, Hochschule und – soweit möglich – Fakultäten sowie kategorisiert nach Webseite beziehungsweise Datenbanken und Server darstellen.*

   b. *Wie viele dieser Hackerangriffe konnten abgewehrt werden und wie viele waren erfolgreich? Bitte differenziert nach Jahr, Hochschule und – soweit möglich – eigenständigen Fakultäten darstellen sowie*

danach, welche Daten in welchem Umfang gehackt wurden beziehungsweise verloren gingen (persönliche/forschungsbasierte).

Für die Universität Hamburg (UHH), die Technische Universität Hamburg (TUHH) und die HafenCity Universität Hamburg (HCU) siehe Drs. 21/11952.

Die TUHH hat 2017 und 2018 Vorfälle kompromittierter Webseiten und Datenbanken der TUHH dokumentiert (2017: ein Vorfall, Joomla, keine Kompromittierung nachweisbar, 2018: ein Vorfall, Bewerber-Status-Portal, erfolgreiche Passwortrateversuche einzelner Accounts aufgrund schwacher Passworte, System selbst nicht betroffen, höhere Passwortkomplexität technisch erzwungen).

An der HCU sind vereinzelte Rechner mit Viren infiziert worden, die im Rahmen der bekannt gewordenen Wellen von E-Mails mit Schadsoftware (zum Beispiel Emotet, Kryptotrojaner) weltweit verteilt wurden. Die Nutzer wurden per E-Mail gewarnt und durch Sensibilisierungsmaßnahmen geschult, sodass die Anzahl der Infektionen im Vergleich zur Anzahl der eingehenden Mails als gering einzustufen war.

An der Hochschule für Angewandte Wissenschaften Hamburg (HAW) gab es seit 2017 bis heute keine erkannten Hackerangriffe. Die Zahl abgewehrter Angriffe wird statistisch nicht erfasst. Es gab seit Mai 2018 zwei Vorfälle, bei denen Zugangsdaten einzelner Personen über erfolgreiche Phishing-Angriffe in die Hände von Angreifern gelangten. Es wurden keine weiteren Datenabflüsse festgestellt. Diese Vorfälle wurden entweder von Betroffenen selbst oder von Dritten gemeldet, die Spammails von den E-Mail-Adressen der betroffenen HAW-Benutzerinnen und -Benutzern erhalten hatten. Die Zugänge wurden daraufhin gesperrt. Diese Vorfälle hat die HAW ergänzend dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit gemeldet.

Die Hochschule für bildende Künste Hamburg (HFBK) kann die Anzahl der Hackerangriffe insgesamt nicht nennen, da die Angriffe dort nicht registriert wurden. Es ist der HFBK aber bekannt, dass es im Jahr 2018 einen erfolgreichen Angriff auf einen Webserver der Fakultät Film gab, auf dem keine personenbezogenen Daten gespeichert wurden. Das betroffene Gerät wurde gelöscht und neu installiert.

An der Hochschule für Musik und Theater Hamburg (HfMT) werden täglich Hunderte Scans und Verbindungsversuche auf die Hochschulnetze, Server und Webseiten durchgeführt, größtenteils automatisiert und mit dem Ziel, Schwachstellen zu finden und auszunutzen. Diese Angriffsversuche werden in der Regel durch die installierten Abwehrmaßnahmen erfolgreich abgewehrt. Als einzigen erfolgreichen Angriffsversuch ist ein Angriff auf eine Webseite eines Instituts der HfMT im Jahr 2017 zu verzeichnen. Dabei wurden keine Daten entwendet. Die Darstellung einzelner Teile der Webseite war beeinträchtigt und mit einem Trojaner infiziert.

An der Europäischen Fernhochschule Hamburg (EURO-FH) konnten alle Hackerangriffe abgewehrt werden, ohne dass konkrete Zahlenangaben möglich sind. An der HSBA Hamburg School of Business Administration (HSBA) sind keine systematischen Angriffe auf die Server bekannt. Im Einzelfall wurde erfolglos versucht, einzelne Nutzerkonten anzugreifen. Dabei kam es zu keinem Datenverlust. An der KLU Kühne Logistics University (KLU) gab es 2017 einen Angriff auf den Email-Server, der erfolgreich abgewehrt wurde. Es wurden keine Daten entwendet, betroffene Daten (Hijacking) wurden von der Sicherung wiederhergestellt. An der Brand Academy (BA), der Bucerius Law School (BLS), der EBC Hochschule (EBC), der MSH Medical School Hamburg (MSH), der NBS Northern Business School (NBS) sowie der Evangelischen Hochschule für soziale Arbeit und Diakonie (EH) sind keine Hackangriffe verzeichnet worden.

c. Liegen Erkenntnisse vor, dass sich an den Hamburger Hochschulen die Cybersicherheitslage seit 2017 angespannt hat?

Wenn ja, inwiefern?

An der UHH verlagern sich die Bedrohungen zunehmend auf Phishing-Angriffe, bei Angriffen auf Webserver und Datenbanken wird keine Anspannung beobachtet.

An der TUHH wird ein Anstieg der Phishing-Attacken mittels nachgeahmter Webseiten registriert, wobei nach ihrer Wahrnehmung Hochschulen weiterhin selten das primäre Ziel der Angreifer sind. Zudem nimmt an der TUHH die Qualität der Spammails kontinuierlich zu, wodurch insbesondere Abteilungen mit externen E-Mail-Kontakten bei zum Beispiel Rechnungen und Bewerbungen betroffen sind. Die Anzahl der internen Nachfragen bei auffälligen E-Mails nimmt daher zu.

An der HCU hat sich die Cybersicherheitslage seit 2017 analog zur weltweiten Bedrohungslage im Internet verhalten, das heißt, es gibt generell vermehrt breit gestreute Attacken, hauptsächlich per E-Mail. Es ist nicht erkennbar, dass die Hochschulen in diesem Zusammenhang eine Sonderrolle einnehmen.

An der HfMT treten Angriffsversuche geringfügig häufiger auf.

Der HAW liegen ebenso wie der BA, BLS, EBC, HSBA, KLU, MSH und NBS keine Erkenntnisse vor. An der EURO-FH haben Spear-Phising-Angriffe via E-Mail stark zugenommen. Die E-Mails sind sehr stark auf das Unternehmen abgestimmt, indem bekannte Absender (Geschäftspartner oder Kollegen) als Absender simuliert werden, um über Anhänge oder Links den Anwender dazu zu bringen, Trojaner ins Haus zu holen. Die EH beobachtet eine hohe Belastung verursacht durch entsprechende E-Mails und Malware.

2. Das Rechenzentrum der UHH berichtet in mehreren Meldungen, letztmalig am 3. Januar 2019, von zielgerichteten Phishing-Angriffen.

a. Wurden die gefälschten E-Mails von einer tatsächlichen E-Mail-Adresse der Universität verschickt oder wurde durch sogenanntes Link-Spoofing eine Absenderadresse der Universität Hamburg lediglich suggeriert?

i. Wenn ersteres: Ist der zuständigen Behörde bekannt, wie der Zugang zum Mailsystem erfolgte?

ii. Wenn ersteres: Ist der zuständigen Behörde bekannt, welche weiteren Daten bei diesem Zugang abgegriffen wurden? Und ist die Sicherheitslücke geschlossen?

b. Ist der zuständigen Behörde bekannt, wie viele Mitarbeiter und Studenten der UHH durch die Phishing-Angriffe geschädigt wurden beziehungsweise lässt sich eine Schätzung anstellen?

c. Hat die UHH Maßnahmen ergriffen, um die Sicherheit seiner IT-Systeme zu erhöhen?

Wenn ja, welche?

Wenn nein, warum nicht?

Nach Angaben der UHH wurde die Absenderadresse der UHH lediglich suggeriert. Der zuständigen Behörde und der UHH ist nicht bekannt, wie viele Mitarbeiter und Studenten der UHH durch die Phishing-Angriffe geschädigt wurden. Im Übrigen sieht die zuständige Behörde in ständiger Praxis davon ab, ohne Datenbasis Prognosen oder Schätzungen vorzunehmen. Die IT-Systeme der UHH unterliegen einem ständigen Verbesserungsprozess und werden bedarfsgerecht den aktuellen Sicherheitsanforderungen angepasst. Der primäre Fokus liegt derzeit auf der Absicherung des Übergangs zum Internet und der damit in Verbindung stehenden Kontrollmechanismen.

3. Eine weitere Meldung des Rechenzentrums der UHH besagt, dass im Jahr 2018 zum wiederholten Male Mitarbeiter Zugangsdaten am Telefon an vermeintliche IT-Mitarbeiter gutgläubig mitgeteilt haben.

a. Wie viele dieser Fälle sind der zuständigen Behörde bekannt?

Der zuständigen Behörde sind keine Fälle bekannt.

b. Die Mitteilung des Rechenzentrums zu diesen Vorfällen beinhaltet die Ankündigung einer Begrenzung des Mailversands auf 100

E-Mails pro Stunde. Wurde mithilfe der widerrechtlich erlangten Zugangsdaten Schadsoftware oder Ähnliches per E-Mail versandt?

Nach Auskunft der UHH: ja.

c. Liegen der zuständigen Behörde darüber hinaus Kenntnisse vor, dass mithilfe der Zugangsdaten personenbezogene oder forschungssensible Daten abgegriffen werden konnten beziehungsweise immer noch werden könnten?

Nein.

i. Sollten Zugangsdaten zu E-Mail Konten der UHH in unbefugte Hände gelangen: Ist es nach wie vor möglich, sich mithilfe der Zugangsdaten in die Rechnernetze der Universität einzuwählen?

Nein, die betroffenen Benutzerkonten werden nach Auskunft der UHH umgehend gesperrt und die Nutzer müssen ihr Passwort ändern.

ii. Welche Maßnahmen werden ergriffen, um diese Angriffe aufzudecken (zum Beispiel Intrusion-Detection-Systeme)?

iii. Wird per SSL verschlüsselter Traffic von der UHH entschlüsselt und auf verdächtige Aktivitäten geprüft?

Derzeit wird an der UHH automatisiert bei verschiedenen Services auf Anomalitäten geprüft. Zusätzliche Maßnahmen werden mit Blick auf eine mögliche Gefährdung der IT-Systeme der UHH nicht benannt.

d. Welche Lehren hat die UHH aus diesem Vorfall und vorangegangenen Vorfällen für seine Personalschulung gezogen?

Es ist seitens der UHH geplant, in Zusammenarbeit mit anderen deutschen Hochschulen eine gemeinschaftliche umfangreiche E-Learning-Einheit zur Verfügung zu stellen.

e. Gibt es für Mitarbeiter der UHH verpflichtende Passwortrichtlinien?

Ja, siehe https://www.rrz.uni-hamburg.de/services/sicherheit/passworte/passwortrichtlinie-v10.pdf.

f. Wie oft und in welchem Umfang finden für die Mitarbeiter der Universität Hamburg verpflichtende Schulungen zum Thema Cybersicherheit statt?

Es existiert eine freiwillige Selbstschulung über das Web-basierte Hochschul-IT-Sicherheitstraining (HITS), welches beim Multimedia Kontor Hamburg (MMKH) gehostet wird. Zusätzlich besteht für alle Beschäftigten der UHH die Möglichkeit, Fortbildungsveranstaltungen zum Thema Cybersicherheit des Zentrums für Aus- und Fortbildung (ZAF) sowie anderer externer Anbieter zu besuchen. Im Übrigen siehe Antwort zu 3. d.

g. Welches Budget steht für diese Personalschulungen zur Verfügung?

h. Wie hat sich dieses Budget seit 2014 entwickelt? Bitte nach Jahren aufschlüsseln.

Fortbildungen zum Thema Cybersicherheit können aus Mitteln der Personalentwicklung der UHH für Fortbildungen finanziert und entsprechend des jeweiligen Formats anteilig aus den Budgets für IT-Fortbildungen sowie individuelle Einzel- und Gruppenmaßnahmen gedeckt werden. Mit dem Ausbau der Personalentwicklungsangebote der UHH seit 2015 ist das Fortbildungsbudget für IT-Themen entlang der Bedarfe der verschiedenen Beschäftigtengruppen angehoben worden.

Jahr	Budget
2014	k.A.
2015	8 000,- Euro
2016	10 000,- Euro
2017	13 000,- Euro

Jahr	Budget
2018	23 000,- Euro
2019	23 000,- Euro

4. Inwieweit arbeiten die Hochschulen beim Thema Cybersicherheit zusammen? Werden Erfahrungen ausgetauscht oder Personalschulungen gemeinsam durchgeführt?

Die Informationssicherheitsbeauftragten der Hochschulen tauschen sich regelmäßig im Arbeitskreis Informationssicherheit & Datenschutz an Hochschulen (AK IDaH) aus. Dokumente werden geteilt und gemeinsame Vorhaben wie das Web-basierte Hochschul-IT-Sicherheitstraining (HITS) werden beim Multimedia Kontor Hamburg (MMKH) gehostet. Darüber hinaus wird zum Teil auch zwischen den hochschuleigenen Angeboten verlinkt. Ergänzend findet auch auf Arbeitsebene ein Erfahrungsaustausch zwischen einzelnen Hochschulen statt. Personalschulungen werden durch jede Hochschule selbst organisiert.

a. Ist ein bestimmtes Rechenzentrum federführend in der Vorgabe von Richtlinien?

Nein. Vorhandene Richtlinien werden aber anderen Hochschulen zur Verfügung gestellt und neue Entwürfe zum Teil auch gemeinsam überarbeitet. Dadurch entstehen gemeinsame Handreichungen, die von allen Hochschulen genutzt werden können.

b. Findet eine Beratung diesbezüglich durch externe Stellen statt?

Die Hochschulen werden durch die DFN-CERT Services GmbH bei konkreten Sicherheitsvorfällen im Wissenschaftsnetz unterstützt. Bei Vorfällen im FHH-Netz gibt es Unterstützung durch das „Computer Emergency Response Team“ für die Verwaltungen der Länder Schleswig-Holstein, Hamburg, Bremen und Sachsen-Anhalt (CERT Nord). In juristischen Angelegenheiten lassen sich die Hochschulen durch die Forschungsstelle Recht im Deutschen Forschungsnetz beraten.

5. In der Antwort auf Frage 2. c) der Drs. 21/11952 verneint der Senat seine Unterstützung beim Thema Cybersicherheit mit Verweis auf die Hochschulautonomie. Gibt es Pläne, angesichts der verschärften Bedrohungslage den Hochschulen mehr Unterstützung anzubieten oder zumindest in Form von Erfahrungsaustauschen seitens der Behörden der Freien und Hansestadt Hamburg zukommen zu lassen?

Die staatlichen Hochschulen erhalten Unterstützung durch die Freie und Hansestadt Hamburg zum Thema Cybersicherheit vom stadtweiten Dienstleister Dataport. Hierüber sind sie in das Sicherheitsnetzwerk „CERT Nord“ eingebunden, das „Computer Emergency Response Team“ für die Verwaltungen der Länder Schleswig-Holstein, Hamburg, Bremen und Sachsen-Anhalt. Das CERT Nord stellt Informationen zu vorbeugenden und reaktiven Maßnahmen bei Sicherheitsvorfällen in IT-Systemen bereit, versendet Sicherheitshinweise, Sicherheitsmeldungen und vorbeugende Handlungsempfehlungen und koordiniert gegebenenfalls Maßnahmen bei Schadcodebefall oder zielgerichteten Angriffen auf IT-Infrastrukturen. Im Übrigen siehe Drs. 21/11952.