BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG **Drucksache 21/11952**
21. Wahlperiode **20.02.18**

Schriftliche Kleine Anfrage

des Abgeordneten Carsten Ovens (CDU) vom 13.02.18

und Antwort des Senats

Betr.: Sind Hamburgs Hochschulen bei der Cybersicherheit gut aufgestellt?

In der Schriftlichen Kleinen Anfrage Drs. 21/5288 berichtete der Senat zur Datensicherheit und zu Hackerangriffen auf Hamburger Krankenhäuser.

Doch nicht nur medizinische Einrichtungen stehen immer häufiger im Fokus von Cyberattacken. Gerade Universitäten und Hochschulen sind ein beliebtes Ziel für Hacker, da sie über wertvolle und forschungssensible Daten verfügen.

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 und Datenbanken der staatlichen und privaten Hamburger Universitäten und Hochschulen in den Jahren 2011 bis 2017? Bitte differenziert nach Jahr, Universität beziehungsweise Hochschule sowie nach Webseite beziehungsweise Datenbanken darstellen.

b) Wie viele dieser Hackerangriffe konnten abgewehrt werden und wie viele waren erfolgreich? Bitte differenziert nach Jahr, Universität beziehungsweise Hochschule darstellen sowie danach welche Daten in welchem Umfang gehackt wurden beziehungsweise verloren gingen (persönliche/forschungsbasierte).

An der Universität Hamburg (UHH), der Technischen Universität Hamburg-Harburg (TUHH) und an der HafenCity Universität Hamburg (HCU) werden täglich Tausende Scans und Verbindungsversuche auf die Hochschulnetze durchgeführt, größtenteils automatisiert und mit dem Ziel, Schwachstellen zu finden und auszunutzen. Diese werden in der Regel durch die installierten Abwehrmaßnahmen erfolgreich abgewehrt. Einzige Ausnahme war ein Angriff auf das E-Learning-System CommSy (Webseite und Datenbank) der UHH im Jahr 2015. Dabei konnten persönliche Nutzerdaten entwendet werden. Gelöschte Daten wurden damals aus Back-ups rekonstruiert. Fälle von verlorenen Forschungsdaten sind nicht bekannt. Im Übrigen siehe hierzu Drs. 21/3361 und 21/3206.

Die TUHH hat folgende Vorfälle kompromittierter Webseiten und Datenbanken der TUHH dokumentiert: 2011: 1, Apache-Webserver gekapert, Bot-Nutzung, keine Information über Veränderung der Web-Inhalte, 2013: 1, Joomla/PHP-Script manipuliert, SPAM-Versand, keine Daten betroffen, 2015: 1, Webserver, SQL-Injection-Attacken, keine Kompromittierung nachweisbar, 2016: 1, Joomla/PHP-Script-Schwachstelle, keine Kompromittierung nachweisbar, fremder Content hinzugefügt, 2017: 1, Joomla, keine Kompromittierung nachweisbar.

Auf die Website der Hochschule für Angewandte Wissenschaften Hamburg (HAW) gab es von Ende 2013 bis Mitte 2014 mehrere wiederkehrende Angriffe durch Veränderung von Suchergebnissen, die als „Google-Viagra-Angriff/Pharma hack“ bekannt wurden. Mit scriptgesteuerter Suche wurden auf dem HAW-Webserver veränderte Dateien gefunden und entfernt. Das Content Management System wurde neu installiert und diverse Erweiterungen aktualisiert. Die Schadcodeanalyse deutete darauf hin, dass der Angriff über Formulare erfolgte, die manipulierte Parameter nicht hinreichend überprüft haben. Die Schwachstelle wurde behoben.

Die Mehrzahl der Hackangriffe auf die Hochschule für bildende Künste Hamburg (HFBK) und die Hochschule für Musik und Theater Hamburg (HfMT) zielen auf Infrastruktur mit Betreuungslücken. Hierbei sind Webdienste und Datenbanken lediglich als Angriffsvektoren relevant. Die HAW, die HFBK und die HfMT konnten die Anzahl der Hackangriffe insgesamt nicht nennen, da die Angriffe nicht registriert wurden. An der HfMT ist bekannt, dass es jeweils einen erfolgreichen Angriff in den Jahren 2014, 2016 und 2017 gab.

Die EBC Hochschule (EBC) hatte in den Jahren 2013 und 2014 je einen dokumentierten Hackerangriff auf die Webseite der Hochschule. Beide Angriffe konnten erfolgreich abgewehrt werden. Die EURO-FH hatte im Abfragezeitraum keine erfolgreichen Hackversuche auf ihre Systeme. Es gab in den Jahren 2012 bis 2016 jeweils eine DDOS-Attacke auf das Netz des Hosters, die durch Gegenmaßnahmen des Hosters erfolgreich abgewehrt werden konnte. Die KLU Kühne Logistics University (KLU) hatte einen Angriff auf ihren Email-Server im Jahr 2017. Dieser wurde erfolgreich abgewehrt. Es wurden keine Daten entwendet, betroffene Daten (Hijacking) wurden von der Sicherung wiederhergestellt.

An der Hamburger Fernhochschule (HFH) finden Hackerangriffe, soweit sie als automatisierte Zugriffsversuche auf offene Ports definiert werden, laufend statt. Die Anzahl kann die HFH nicht beziffern. Keiner von diesen Angriffen war bislang erfolgreich. Weitergehende, gezielte Hackerangriffe gab es an der HFH nicht.

An der Brand Academy (BA), der Bucerius Law School (BLS), der HSBA Hamburg School of Business Administration (HSBA), der MSH Medical School Hamburg (MSH), der NBS Northern Business School sowie der Evangelischen Hochschule für soziale Arbeit und Diakonie (EH) sind keine Hackangriffe verzeichnet worden.

2. Maßnahmen

a) Verfügen die staatlichen und privaten Hamburger Universitäten und Hochschulen über eigene Strategien und Maßnahmenpläne zur Cybersicherheit beziehungsweise um solche Hackerangriffe abzuwehren?

Wenn ja, über welche und seit wann?

Wenn nein, warum nicht? Bitte differenziert nach Jahr, Universität beziehungsweise Hochschule sowie nach Maßnahmen und Strategien darstellen.

An der UHH wurde im Jahr 2014 mit dem Erlass einer Informationssicherheitsleitlinie ein Informationssicherheitsbeauftragter bestellt. Die technischen Schutzmaßnahmen, die in abgestuft abgesicherten Netzkonzepten betrieben werden, beruhen auf Richtlinien (zum Beispiel Net-Policy), die das Regionale Rechenzentrum (RRZ) seit über zehn Jahren formuliert und fortschreibt. Die Server und die Endgeräte werden nach dem jeweiligen Stand der Technik betrieben, Schadsoftware-Abwehr, System-Updates und die technische Weiterentwicklung haben hohe Priorität. Das universitätsweite IT-Sicherheitskonzept wird stetig weiterentwickelt.

Die HAW ist in der Betreuung der DFN-CERT Services GmbH. Dieses ist im Auftrag des Vereins Deutsches Forschungsnetz tätig und erteilt praktische Angebote zur Erhöhung der Netzwerk- und Cybersicherheit. Die HAW erhält Warnhinweise bezüglich Produktschwachstellen und konkreter Störer. Zudem gibt es Prüfdienste, die Systeme der Hochschulen in Hinblick auf Konfigurationsprobleme analysieren. Die Abwehr von Hackerangriffen erfolgt im Rahmen des Sicherheitsmanagements und Betriebs.

An der HCU werden gängige Schutzmaßnahmen vor Cyberangriffen seitens der IT umgesetzt: Virenscanner, Patchmanagement, Firewalls und ein Rollen- und Berechtigungskonzept. Die HCU erstellt derzeit ein strukturiertes Informationssicherheitsmanagementsystem (ISMS) und damit weitergehende Strategien und Maßnahmenpläne. Dazu wurde Ende 2017 ein Informationssicherheitsbeauftragter eingestellt.

An der HFBK bestehen Strategien und Best Practices, um betroffene Systeme vom Netz zu nehmen, zu löschen und gegebenenfalls neu zu installieren.

Das IT Service Center der HfMT sorgt von Anbeginn des Betriebs eigener Server an durch vielfältige Maßnahmen für deren Absicherung und optimiert diese stetig.

An der TUHH wurde im Jahr 2004 eine IT-Sicherheitsleitlinie erlassen sowie ein IT-Sicherheitsbeauftragter bestellt. Seit dem kam es unter anderem zur Einführung von Firewall, Monitoring/Reporting, VPN, Antivirus-Software, Patch-Management, IT-Sicherheitsschulungen und Private-Key-Infrastructure. Im Jahr 2015 erfolgte eine Überarbeitung und Weiterentwicklung der Sicherheitsleitlinie sowie die Bestellung eines Informationssicherheitsbeauftragten. Die oben genannten Sicherheitsmaßnahmen werden laufend fortgeführt und aktualisiert.

Die BA unternimmt seit Gründung 2010 die üblichen Maßnahmen gegen Hackerangriffe unter anderem in Form von Firewalls, Antiviren-Programmen und einer Datenspeicherung auf zusätzlich gesicherten internen Mailservern.

An der BLS wird die Sicherheit der E-Mail- und Kalender-Dienste sowie der Dokumentenablage über den Cloud-Dienstleister gewährleistet.

Die Hochschulebereiche der EBC werden durch Firewall-Systeme gesichert. Das interne Netzwerk ist durch eine physikalische Trennung vom öffentlichen Internetauftritt gesichert. Im internen Netzwerk gibt es ein Zugriffsrechtesystem. Das studentische Netzwerk ist vom Verwaltungsnetzwerk physikalisch getrennt. Im Übrigen siehe Vorbemerkung.

An der EURO-FH wird für den Webauftritt eine Webfarm, die durch ein Managed-Security-System-Team eines externen IT-Sicherheitsdienstleisters seit 2008 überwacht wird, betrieben. Sie ist durch Firewalls abgesichert. Die Server sind gehärtet und können von außen nicht administriert werden. Der Zugriff auf die Administrationsebene erfolgt über ein separates Management-Netzwerk, auf das nur die Administratoren des Security-Teams Zugriff haben. Der Datenaustausch erfolgt über verschlüsselte Leitungen. Das Hochschulnetzwerk ist über Firewallsysteme und Antivirenlösung abgesichert und verfügt über eine eigene Spamwall mit Virenschutz. Es finden Sicherheitsüberprüfungen durch IT-Sicherheitsdienstleister statt. Für den Seminarbetrieb wird ein eigenes Netzwerk betrieben. Für mobile Systeme gibt es ein eigenes WLAN-Netz. Sicherungen werden täglich über Backup-to-Disk-to-Tape angefertigt. Zusätzlich erfolgt die Erstellung von Snapshots der geänderten Dateninhalte. Gegen Verschlüsselungen von Netzwerkinhalten gibt es ein Sicherungs- und Recovery-Konzept sowie ein Rechtekonzept.

Die Serversysteme der EH werden über die Stiftung das Rauhe Haus verwaltet. Die Betreuung in Fragen der Cybersicherheit erfolgt über die IT-Verantwortlichen der Stiftung.

Die zentralen Systeme der HSBA werden in geschlossenen, nicht von außen zugänglichen Systemen gehostet beziehungsweise sind nur über VPN-Systeme erreichbar. Die HSBA nutzt externe SaaS-Systeme mit Multifaktorauthentifizierung. Teil der Strategie sind auch Rechnersicherungen.

Die KLU erstellt derzeit ein Konzept.

Die HFH nutzt zur Abwehr Back-ups und Monitoring, setzt SSL-Zertifikate ein und hält BSI-Standards ein. Aufgrund der externen Sicherheitsmanagements gibt es direkt an der HFH kein Kriseninterventionsteam zur Cybersicherheit.

Die Strategien und Maßnahmenpläne zur Cybersicherheit der MSH beruhen auf den BSI-Standards zur Internet-Sicherheit (ISi-Reihe), sowie der ISO 27001:2017 (Informationssicherheitsmanagementsysteme) in Verbindung mit ISO 27002 (IT-Sicherheitsverfahren) und dem IT-Grundschutz des BSI. Entsprechende Strategien und Maßnahmenpläne existieren an der MSH seit 2011 und werden laufend weiterentwickelt.

Hochschulwebsite und Datenbanken des Campus Management Systems der NBS werden extern gehostet. Die Dienstleister haben Verpflichtungen bezüglich Datensicherheit und Datenschutz übernommen. Die NBS entwickelt derzeit ein umfassendes IT-Sicherheitskonzept nach den Vorgaben des BSI für intern gehostete Ressourcen.

b) Verfügen die staatlichen und privaten Hamburger Universitäten und Hochschulen über eigene Kriseninterventionsteams zur Cybersicherheit beziehungsweise um solche Hackerangriffe abzuwehren?

Wenn ja, über welche, in welcher Größe und seit wann?

Wenn nein, warum nicht? Bitte differenziert nach Jahr, Universität beziehungsweise Hochschule sowie nach Krisenteam und Aufgabenstellung darstellen.

Zur Abwehr von Cyberkriminalität an der UHH agiert die Leitung des RRZ (Direktor und vier Abteilungsleiter, ergänzt durch circa sechs Fachexperten) – seit 2014 zusammen mit dem Informationssicherheitsbeauftragten – sehr eng mit dem 2013 eingerichteten CIO-Gremium der UHH (Vorsitz: Kanzler, vier Mitglieder aus dem RRZ und den Fakultäten). Sicherheitsstandards werden so jederzeit mit dem Präsidium abgestimmt, im RRZ verankert und eingehalten. Dieses gilt auch für den Krisenfall.

Die HAW hat einen behördlichen Informationssicherheitsbeauftragten benannt. Die IT-Sicherheit ist Gegenstand des HAW-eigenen Risikomanagements. Es existieren Kommunikationswege, um Informationen bei Krisen zwischen Hochschulen und CERTs auszutauschen. Der Aufbau von eigenen CERTs an Hochschulen erfolgt derzeit noch. Der behördliche Informationssicherheitsbeauftragte steht in engem Kontakt mit sowohl dem CERT-Verbund als auch mit Teams an anderen Hochschulen.

An der TUHH sind seit 2004 beziehungsweise 2006 zwei Mitarbeiter im Rechenzentrum unter anderem für Netz- und IT-Sicherheit zuständig.

Die HSBA verfügt seit 2015 über ein Kriseninterventionsteam, das auch bei Hackerangriffen aktiviert würde. Es besteht aus der Geschäftsführung der Hochschule, die abhängig von der Art der Krise durch die jeweiligen Experten ergänzt wird.

Die Cybersicherheit der EH wird durch den IT-Verantwortlichen der Stiftung Das Rauhe Haus verantwortet und betreut.

Bei der MSH wird seit 2012 ein Kriseninterventionsteam zur IT-Sicherheit eingesetzt, welches aus dem IT-Leiter und dem IT-Sicherheitsbeauftragten besteht. Abhängig von der Bedrohungslage wird es um weitere Mitarbeiter beziehungsweise externe Partner ergänzt.

Die übrigen staatlichen und privaten, staatlich anerkannten Hochschulen bilden bei Fällen der Beeinträchtigung der Cybersicherheit vorwiegend aus dem Personal der jeweiligen IT-Administrationen und gegebenenfalls unter Einbezug von entsprechenden Dienstleistern Kriseninterventionsteams. Teilweise bestehen maschinell implementierte Sicherheitsvorkehrungen.

c) Inwieweit und seit wann unterstützen der Hamburger Senat beziehungsweise die zuständigen Behörden in welchem Umfang die staatlichen und privaten Universitäten und Hochschulen bei der Abwehr von Hackerangriffen beziehungsweise bei der Herstellung von Cybersicherheit?

Die Hochschulen sind im Rahmen der Hochschulautonomie eigenverantwortlich für die Abwehr von Hackerangriffen und die Herstellung von Cybersicherheit.