Bayerischer Landtag

18. Wahlperiode 15.09.2020 Drucksache 18/9503

Schriftliche Anfrage

des Abgeordneten **Benjamin Adjei BÜNDNIS 90/DIE GRÜNEN**
vom 21.05.2020

IT-Sicherheit in systemkritischen Einrichtungen

Teil 1 – Angriffe und Auswirkungen von Cyber-Angriffen auf Krankenhäuser, Forschungseinrichtungen und Hochschulen

Teil 2 – Ausstattung, Maßnahmen und Vorschriften für Krankenhäuser, Forschungseinrichtungen und Hochschulen

Krankenhäuser, Forschungseinrichtungen und Hochschulen werden vermehrt Opfer von Hackerinnen bzw. Hackern und Cyber-Angriffen. Die Angriffe auf die Universität Gießen und das Klinikum Fürstenfeldbruck sind nur zwei Beispiele davon.

Gerade die aktuelle COVID-19-Pandemie verschärft diese Gefahr, da aufgrund der angespannten Lage – insbesondere im Gesundheitsbereich – und des erhöhten Angebotes an Online-Dienstleistungen in sämtlichen Bereichen die digitale Informations- und Kommunikationsinfrastruktur besonders beansprucht und damit angreifbar ist. Um Ausfällen vorzubeugen, muss der Fokus daher mehr denn je auf eine funktionierende IT-Sicherheit und entsprechende Vorsorgemaßnahmen gelegt werden.

Die folgende Anfrage bezieht sich auf Krankenhäuser, Forschungseinrichtungen und Hochschulen in, falls nicht anders spezifiziert, staatlicher, privater als auch freigemeinnütziger Trägerschaft.

Ich frage die Staatsregierung:

Teil 1

Hinweis des Landtagsamts: Zitate werden weder inhaltlich noch formal überprüft. Die korrekte Zitierweise liegt in der Verantwortung der Fragestellerin bzw. des Fragestellers sowie der Staatsregierung.

Drucksachen, Plenarprotokolle sowie die Tagesordnungen der Vollversammlung und der Ausschüsse sind im Internet unter www.bayern.landtag.de – Dokumente abrufbar.
Die aktuelle Sitzungsübersicht steht unter www.bayern.landtag.de – Aktuelles/Sitzungen/Tagesübersicht zur Verfügung.

Teil 2

Antwort

des Staatsministeriums für Wissenschaft und Kunst in Abstimmung mit dem Staatsministerium für Gesundheit und Pflege für den Krankenhausbereich, dem Staatsministerium für Wirtschaft, Landesentwicklung und Energie für die außeruniversitären Forschungseinrichtungen, dem Staatsministerium des Innern, für Sport und Integration für den Bereich der Cybersicherheit sowie dem Staatsministerium der Finanzen und für Heimat für die Zuständigkeit des Landesamtes für Sicherheit in der Informationstechnik
vom 12.08.2020

Teil 1

1. Anzahl und Art der Angriffe

a) Wie viele Angriffe auf die ITK-Systeme (ITK = Informations- und Telekommunikationstechnik) von Krankenhäusern, Forschungseinrichtungen und Hochschulen in privater, staatlicher und freigemeinnütziger Trägerschaft gab es in den Jahren 2017, 2018 und 2019 (bitte aufgeschlüsselt nach Art der Einrichtung, Angriffsart und Trägerschaft)?

b) Bei wie vielen dieser Angriffe konnten die Täterinnen bzw. Täter ermittelt werden (bitte aufgeschlüsselt nach Art der Einrichtung, Angriffsart und Trägerschaft)?

c) Was waren die jeweiligen Motive für die Angriffe (bitte aufgeschlüsselt nach Art der Einrichtung und Trägerschaft)?

Im Bereich der Bayerischen Polizei fungiert die Zentrale Ansprechstelle Cybercrime (ZAC) beim Landeskriminalamt als „Single Point of Contact“ für Behörden und Unternehmen, um bei Angriffen auf die IT-Infrastruktur beratend und unterstützend tätig werden zu können.

Für den angefragten Zeitraum sind der Staatsregierung auf Grundlage der im polizeieigenen Vorgangsverwaltungssystem geführten Statistikdaten aktuell folgende Falldaten bekannt:

2017: Ein Angriff auf ein Krankenhaus mittels Schadsoftware;

2018: Ein Angriff auf ein Krankenhaus mittels Schadsoftware und ein Angriff auf die Telefonanlage eines Krankenhauses;

2019: Vier Angriffe auf Krankenhäuser mittels Schadsoftware, drei Angriffe auf Hochschulen mittels Schadsoftware, zwei Angriffe auf die Telefonanlagen von Krankenhäusern sowie ein Angriff mittels Spam-E-Mails auf eine Hochschule.

In keinem dieser Fälle konnte ein Täter oder eine Täterin ermittelt werden.

Darüber hinaus bearbeitet das Landesamt für Verfassungsschutz (BayLfV) solche Cyber-Angriffe auf Unternehmen und Einrichtungen in allen Sektoren, bei denen eine staatliche Beteiligung am Angriff nicht von Beginn an ausgeschlossen werden kann, oder soweit es sich um Angriffe gegen systemrelevante Einrichtungen handelt. Im Zeitraum 2017 bis Juni 2019 wurden dem Cyber-Allianz-Zentrum beim BayLfV insgesamt 388 Sachverhalte aus allen Bereichen bekannt, von denen 192 nachrichtendienstlich relevante Cyber-Sachverhalte mit und ohne erkennbaren Länderbezug waren. Eine Aufschlüsselung im Sinne der Fragestellung kann aus Gründen der durch das BayLfV zugesicherten Vertraulichkeit nicht erfolgen.

Zur Motivlage liegen der Staatsregierung keine gesicherten Erkenntnisse vor.

Von den außeruniversitären, bundesweit tätigen Forschungsorganisationen wurden auf Anfrage für die Jahre 2018 und 2019 zehn Cyber-Sicherheitsvorfälle angegeben. In sechs Fällen wurde ein krimineller Hintergrund erkannt.

2. IT-Sicherheit und Corona

a) Wurde seit dem Beginn der Corona-Pandemie ein erhöhtes Aufkommen an Cyber-Angriffen auf die in Frage 1 a genannten Einrichtungen festgestellt (bitte aufgeschlüsselt nach Art der Einrichtung und Trägerschaft)?

b) Wurden bestehende Unterstützungsangebote des Freistaates für die in Frage 1 a genannten Einrichtungen im Zuge der Corona-Pandemie ausgebaut?

c) Wurden bestehende Richtlinien und Mindeststandards der in Frage 1 a genannten Einrichtungen im Hinblick auf generelle technische Sicherheitsmaßnahmen sowohl aufseiten der Administration als auch der Nutzerinnen bzw. Nutzer sowie bezüglich der Schulung der Mitarbeiterinnen bzw. Mitarbeiter aufgrund der aktuellen Pandemie nochmals verschärft?

Im Bezugszeitraum konnte durch die gemeinsame Plattform der Behörden mit Cyber-Sicherheitsaufgaben, der sog. Cyberabwehr Bayern, ein umfassendes Gefährdungspotenzial identifiziert werden. Dieses hat bis dato nicht zu einer signifikanten Erhöhung der registrierten Fallzahlen geführt.

Die Corona-Pandemie führte zu einer stärkeren Inanspruchnahme der Kommunikations- und Informationsinfrastrukturen, hat die Gefahren für die Informationssicherheit als solche aber nicht verändert. Zusätzliche Unterstützungsangebote oder Richtlinien seitens der Staatsregierung waren insofern nicht erforderlich.

3. Auswirkungen auf Patientinnen und Patienten

a) Wie viele Fälle sind der Staatsregierung bekannt, in denen in den letzten zehn Jahren aufgrund von Cyber-Angriffen Patientinnen und Patienten nicht ausreichend oder nur eingeschränkt versorgt werden konnten oder verlegt werden mussten (bitte aufgeschlüsselt nach Jahren)?

b) In wie vielen Fällen konnten in den letzten zehn Jahren durch Angriffe auf die ITK-Infrastruktur Daten von Patientinnen und Patienten entwendet werden (bitte aufgeschlüsselt nach Jahren)?

c) Von wie vielen Patientinnen und Patienten konnten in den letzten zehn Jahren durch Angriffe auf die ITK-Infrastruktur Daten entwendet werden (bitte aufgeschlüsselt nach Jahren)?

4. Auswirkungen auf die Krankenhäuser

Wie groß war in den letzten zehn Jahren der durch Cyber-Angriffe entstandene wirtschaftliche Schaden für die Krankenhäuser (bitte aufgeschlüsselt nach Jahr und Trägerschaft)?

Die in den Krankenhausplan des Freistaates Bayern aufgenommenen Krankenhäuser (sog. Plankrankenhäuser) sind keine Behörden, sondern eigenständige Unternehmen, die ihre innerbetrieblichen Angelegenheiten eigenverantwortlich regeln. Insoweit besteht keine Aufsicht des Staatsministeriums für Gesundheit und Pflege und somit auch keine Auskunftspflicht der Häuser diesem gegenüber. Die Beantwortung der Fragen 3 und 4 hätte eine Einzelabfrage bei 367 Plankrankenhäusern erfordert, hierauf wurde im Hinblick auf den unverhältnismäßigen Aufwand verzichtet.

Bei den als Anstalten d. ö. R. unter staatlicher Aufsicht stehenden Universitätskliniken (und dem Deutschen Herzzentrum München) wurden nach Kenntnis der Staatsregierung keine Patientendaten entwendet und waren in den letzten Jahren auch keine Einschränkungen der Patientenversorgung, bedingt durch einen Cyber-Angriff, zu verzeichnen.

An den bayerischen Universitätsklinika entstand in den letzten Jahren durch Cyber-Angriffe kein direkter wirtschaftlicher Schaden. Vereinzelt berichten die Universitätsklinika von Cyber-Angriffen in Form von einzelnen, zumeist nicht spezifisch an die Universitätsklinika gerichteten E-Mails mit Schadsoftware. Das Deutsche Herzzentrum München berichtet einen Cyber-Vorfall im Jahr 2016 mit wirtschaftlichen Auswirkungen in Höhe von circa 20.000 Euro für die Neuinstallation von Servern.

5. Auswirkungen auf Forschungseinrichtungen und Hochschulen

a) In welchem Umfang wurden in den letzten zehn Jahren bei Angriffen auf Forschungseinrichtungen und Hochschulen nach Kenntnis der Staatsregierung personenbezogene Daten von Hochschulangehörigen (z.B. Namen, Adressen, Prüfungsergebnisse) entwendet (bitte aufgeschlüsselt nach Jahr, Trägerschaft und Anzahl betroffener Personen)?

b) In wie vielen Fällen wurden in den letzten zehn Jahren bei Angriffen auf Forschungseinrichtungen und Hochschulen nach Kenntnis der Staatsregierung bisher unveröffentlichte und vertrauliche Forschungsdaten bzw. Forschungsergebnisse entwendet (bitte aufgeschlüsselt nach Jahr und Trägerschaft)?

c) Wie groß war in den letzten zehn Jahren der durch Cyber-Angriffe entstandene wirtschaftliche Schaden für die Forschungseinrichtungen und Hochschulen (bitte aufgeschlüsselt nach Jahr und Trägerschaft)?

Nach Kenntnis der Staatsregierung wurden bei Angriffen auf die Hochschulen innerhalb der letzten zehn Jahre keine personenbezogenen Daten von Hochschulangehörigen und keine unveröffentlichten bzw. vertraulichen Forschungsdaten oder Forschungsergebnisse entwendet. Inwieweit die von nichtstaatlichen Forschungseinrichtungen berichteten Versuche, auf Forschungsinformationen zuzugreifen, erfolgreich waren, ist nicht bekannt.

Hochschulen und Forschungseinrichtungen sind wie alle Internetteilnehmer ständigen, meist ungezielten Cyber-Angriffen ausgesetzt, weshalb sie zur Prävention und Minderung von Schadenfällen organisatorische und technische Sicherheitsinfrastrukturen geschaffen haben. Die Erkennung von Cyber-Angriffen und deren Abwehr wird regelmäßig durch eigene Kräfte geleistet. Größere Schadensereignisse verursachten an Hochschulen im Einzelfall zusätzlichen Aufwand des Rechenzentrums, bis zu 50 Stunden für die Schadensbehebung und weitere personelle Aufwendungen innerhalb des unmittelbar betroffenen Bereiches. Eine außeruniversitäre Forschungsorganisation beziffert den in Bayern entstandenen Aufwand für die Schadensbehebung auf ca. 60.000 Euro innerhalb der letzten drei Jahre.

6. Angriffe auf Supercomputer der Rechenzentren I

a) Ist der Staatsregierung bekannt, von wem die Angriffe auf europäische Supercomputer u. a. des Leibniz-Rechenzentrums (LRZ) im Mai 2020 ausgingen?

b) Ist der Staatsregierung bekannt, was das Ziel hinter diesen Angriffen war?

Die Verursacher des Angriffs und die dahinterstehenden Motive oder Ziele sind bisher nicht bekannt. Das Landeskriminalamt hat im Falle des LRZ die Ermittlungen übernommen und stimmt sich auf nationaler Ebene mit den Bundesbehörden (v. a. dem Bundeskriminalamt – BKA – und dem Bundesamt für Sicherheit in der Informationstechnik – BSI) sowie den weiteren betroffenen Landeskriminalämtern ab. Das Cyber-Allianz-Zentrum Bayern (CAZ) wurde frühzeitig informiert und ist an den Ermittlungen beteiligt.

c) Ist der Staatsregierung bekannt, ob die Angriffe durch striktere Sicherheitsmaßnahmen hätten verhindert werden können?

Die Höchstleistungsrechner im nationalen Verbund des Gauss Centre for Supercomputing (GCS) am Jülich Supercomputing Centre (JSC), am High-Performance Computing Center (HLRS) in Stuttgart und am Leibniz-Rechenzentrum (LRZ) in Garching dienen der Wissenschaft in Deutschland und Europa. Dadurch müssen diese Systeme von den Wissenschaftlerinnen und Wissenschaftlern von außerhalb der Zentren erreicht werden können. Um die Sicherheit zu gewährleisten, setzen die drei Zentren sicherheitstechnische Maßnahmen nach dem Stand der Technik ein. Die jeweiligen Zugangsrechner der Nutzer liegen aber nicht in der Hoheit der Zentren und stellen damit ein gewisses Risiko dar.

7. Angriffe auf Supercomputer der Rechenzentren II

a) Ist der Staatsregierung bekannt, ab wann der Supercomputer des LRZ voraussichtlich wieder uneingeschränkt genutzt werden kann?

Der Höchstleistungsrechner SuperMUC-NG steht seit dem 16.06.2020, das Linux-Cluster seit dem 01.07.2020 den Nutzern uneingeschränkt zur Verfügung, wobei das Cluster in mehreren Stufen seit dem 08.06.2020 wieder in Betrieb genommen wurde.

b) Ist bereits abzusehen, wie groß der finanzielle Schaden für das LRZ durch die Angriffe und die folgenden Schutzmaßnahmen sein wird?

Zusätzliche Kosten sind dem LRZ nicht entstanden. Der Schaden für die Wissenschaft sowie die Wissenschaftlerinnen und Wissenschaftler, die das System nicht nutzen konnten, ist nicht zu beziffern.

c) Welche Maßnahmen plant die Staatsregierung, damit vergleichbare Angriffe auf (Hochleistungs-)Rechenzentren und Supercomputer in Zukunft verhindert werden?

Die ausführliche Analyse des Sicherheitsvorfalls fließt in den zukünftigen Betrieb der GCS-Zentren ein, wodurch die Systeme gehärtet und Vorgaben für die Nutzer verschärft wurden. Das LRZ ist seit 2019 nach ISO/IEC 27001 bezüglich des IT-Sicherheitsmanagements zertifiziert. Der Standard erfordert eine regelmäßige Re- und Neu-Zertifizierung.

Teil 2

Ein zentrales Element, um Cyber-Angriffen vorzubeugen und im Falle eines erfolgreichen Angriffs den entstandenen Schaden möglichst gering zu halten, sind klare und strikte Regeln und Sicherheitsmaßnahmen sowohl aufseiten der Nutzerinnen und Nutzer eines Systems als auch aufseiten der Administration.

Die folgende Anfrage bezieht sich auf Krankenhäuser, Forschungseinrichtungen und Hochschulen in – falls nicht anders spezifiziert – staatlicher, privater und freigemeinnütziger Trägerschaft.

1. Technische Sicherheitsmaßnahmen aufseiten der Nutzerinnen und Nutzer

a) Welche Vorgaben und Mindeststandards im Hinblick auf das Nutzerinnen- und Nutzerverhalten (Regeln für Mailanhänge, eingeschränkte Schreiberechte u. Ä.) werden von der Staatsregierung für Krankenhäuser, Forschungseinrichtungen und Hochschulen in privater, staatlicher und freigemeinnütziger Trägerschaft (insbesondere für Krankenhäuser, welche nicht zur kritischen Infrastruktur – KRITIS – zählen) gemacht, um Angriffen vorzubeugen bzw. den möglichen Schaden zu begrenzen?

Für Krankenhäuser bestehen, soweit sie nicht gemäß § 8 b Abs. 3 und 4 BSI-Gesetz den bundesrechtlich regulierten KRITIS-Einrichtungen (wie Universitätsklinika) zuzurechnen sind, keine Vorgaben der Staatsregierung.

Das Landesamt für Sicherheit in der Informationstechnik (LSI) verantwortet die IT-Sicherheitsrichtlinien für die sichere Konfiguration und den Betrieb des bayerischen Behördennetzes. Diese Richtlinien gelten auch für die mit dem Behördennetz verbundenen Systeme der Hochschulverwaltungen.

Soweit die Anfrage Forschung und Lehre betrifft, setzen die jeweiligen Institutionen in Eigenverantwortung technische und organisatorische Informationssicherheitsmaßnahmen um. Die Einrichtungen orientieren sich dabei an Standards wie dem BSI-Grundschutz oder ISO/IEC-2700X.

b) Falls keine Vorgaben existieren, plant die Staatsregierung, entsprechende Vorgaben und Mindeststandards zu entwickeln?

Soweit keine gesetzlichen Vorgaben bestehen, unterstützt und begleitet die Staatsregierung die Entwicklung von einrichtungsbezogenen Mindeststandards bei Krankenhäusern und Hochschulen.

So fördert das Staatsministerium für Gesundheit und Pflege derzeit das Projekt „Smart Hospitals“ der Universität der Bundeswehr in Neubiberg. Ziel des Projektes ist es, anhand von Erhebungen bei den Krankenhäusern einen Maßnahmenkatalog zu entwickeln, der den Krankenhäusern als Leitfaden für die Einrichtung einer zeitgemäßen IT-Infrastruktur und Etablierung entsprechender Sicherheitsmaßnahmen dient. Die erste Version dieses Katalogs wird im Herbst 2020 fertiggestellt und dann den Krankenhäusern kostenlos zur Verfügung gestellt werden.

Die bayerischen staatlichen Hochschulen haben vor dem Hintergrund ihrer besonderen Aufgabenstellung in Forschung und Lehre die Umsetzung hochschulspezifischer Informationssicherheitskonzepte beschlossen. Bei deren Entwicklung werden sie von der durch das Staatsministerium für Wissenschaft und Kunst geschaffenen hochschulübergreifenden Stabsstelle IT-Sicherheit unterstützt. Sie haben sich darüber hinaus auf ein Hochschul-Informationssicherheitsprogramm (HISP) verständigt, das ein gemeinsames, hochschulübergreifendes Vorgehen bei der Planung und Festlegung von organisatorischen und technischen Maßnahmen vorsieht.

c) In welchem Intervall werden diese Vorgaben evaluiert, auf ihre Aktualität geprüft und aktualisiert?

Um die Verwaltungsanwendungen im bayerischen Behördennetz bestmöglich zu schützen, passt das LSI die technischen Verfahren und Vorgaben durch regelmäßige Analyse dem Stand der Technik an. Bei kurzfristigem Handlungsbedarf werden entsprechende Warnmeldungen mit Sicherheitsanweisungen herausgegeben. Im Rahmen des gesetzlichen Auftrags stehen diese Aktualisierungen auch anderen öffentlichen Einrichtungen und Unternehmen zur Verfügung.

Bei Hochschulen und außeruniversitären Forschungseinrichtungen erfolgt die Anpassung entsprechend der Fortschreibung der einschlägigen Standards für die IT-Sicherheit und der daran orientierten Audit-Kriterien.

2. Technische Sicherheitsmaßnahmen aufseiten der Administration

a) In welchem Intervall wird das ITK-Personal der in Frage 1 a genannten Einrichtungen zum Thema IT-Sicherheit geschult (bitte aufgeschlüsselt nach Art der Einrichtung und Trägerschaft)?

b) Hat bzw. plant die Staatsregierung Vorgaben für die in Frage 1 a genannten Einrichtungen im Hinblick auf die Systemadministration (Trennung Administrator-/Nutzerkonto, Trennung von Rechten, Offline-Backups u. Ä.), um Angriffe zu verhindern oder im Falle eines erfolgreichen Angriffs den Schaden zu minimieren?

c) In welchem Intervall werden diese Vorgaben evaluiert, auf ihre Aktualität geprüft und aktualisiert?

Die Schulung von technischem Personal und die Umsetzung technischer Sicherheitsmaßnahmen aufseiten der IT-Administration unterfallen der innerbetrieblichen Organisation. Bei Hochschulen und außeruniversitären Forschungseinrichtungen werden entsprechende Schulungsmaßnahmen, aufbauend auf den jeweils geltenden Standards, regelmäßig mindestens einmal jährlich durchgeführt. Dabei sind zentrale Einheiten bei den außeruniversitären Forschungseinrichtungen und die Stabsstelle IT-Sicherheit bei den staatlichen Hochschulen in die inhaltliche Vorbereitung eingebunden.

Zu den Teilfragen 2 b und 2 c gilt das bei Frage 1 Ausgeführte entsprechend. Bei der Verarbeitung von Daten mit Personenbezug sind darüber hinaus die allgemeinen Anforderungen an technische und organisatorische Maßnahmen in Art. 32 Datenschutz-Grundverordnung (DSGVO) – sowie für den staatlichen Bereich in Art. 32 Bayerisches Datenschutzgesetz (BayDSG) und Art. 11 Abs. 1 Bayerisches E-Government-Gesetz (BayEGovG) – zu beachten.

3. Organisatorische Sicherheitsmaßnahmen

a) Finden Schulungen für die Mitarbeiterinnen und Mitarbeiter der in Frage 1 a genannten Einrichtungen statt, um diese für das Thema IT-Sicherheit zu sensibilisieren und mit möglichen Angriffsszenarien bekannt zu machen?

b) Wer führt diese Schulungen durch (bitte Zeitintervall mit angeben und aufgeschlüsselt nach Einrichtung und Trägerschaft)?

Die Hochschulen und außeruniversitären Forschungseinrichtungen haben unterschiedliche Formen regelmäßiger und zielgruppenorientierter Informations- und Schulungsangebote zum Thema IT-Sicherheit etabliert. Dies reicht von aktuellen Warnhinweisen bis hin zu Selbstlernkursen, in denen erworbene Kenntnisse auch überprüft werden können. Die Organisation und Durchführung der Schulungen wird von den lokalen IT-Sicherheitsbeauftragten verantwortet. Hinzuweisen ist auch auf den „IT-Sicherheitstag“, der gemeinsam vom Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften und der Technischen Universität München seit mehreren Jahren regelmäßig organisiert wird und der der Hochschulöffentlichkeit jeweils aktuelle Themen zur IT-Sicherheit aus organisatorischer und technischer Sicht vorstellt.

Bezüglich der Plankrankenhäuser liegen der Staatsregierung keine Kenntnisse zu Schulungsmaßnahmen vor.

c) In welchem Umfang haben die in Frage 1 a genannten Einrichtungen Versicherungen abgeschlossen, um sich vor möglichen Schäden von Cyber-Angriffen zu schützen (bitte aufgeschlüsselt nach Art der Einrichtung und Trägerschaft)?

Als staatliche Einrichtungen schließen die Hochschulen generell keine Versicherungen ab. Auch die nichtstaatlichen Forschungseinrichtungen haben keine entsprechende Versicherung abgeschlossen; hierfür werden zuwendungsrechtliche Gründe angegeben. Zu den Plankrankenhäusern liegen keine Informationen vor.

4. Vorgaben des Freistaates

a) Welche konkreten Schritte werden von der Staatsregierung unternommen, um die Umsetzung der zu den Fragen 1 a und 2 b genannten Vorgaben und Mindeststandards zu prüfen?

b) Welche Notfallkonzepte existieren in den in Frage 1 a genannten Einrichtungen für den Fall eines erfolgreichen Angriffs (bitte aufgeschlüsselt nach Art der Einrichtung)?

c) Falls keine Notfallkonzepte existieren, plant die Staatsregierung entsprechende Notfallkonzepte zu entwickeln oder von den jeweiligen Einrichtungen entwickeln zu lassen (bitte aufgeschlüsselt nach Art der Einrichtung)?

Die bayerischen staatlichen Hochschulen haben sich im Rahmen des Hochschul-Informationssicherheitsprogramms (s. Antwort zu Frage 1 b) auf regelmäßige Audits zur Angemessenheit und Wirksamkeit der getroffenen Informationssicherheitsmaßnahmen verständigt. Im Rahmen dieser Audits wird auch das Notfallkonzept der jeweiligen Hochschule bewertet.

Auch die von den außeruniversitären Forschungseinrichtungen entwickelten IT-Sicherheitskonzepte schließen geeignete Notfallmaßnahmen ein und unterliegen der regelmäßigen Überprüfung durch Audits.

Für den Bereich der Plankrankenhäuser liegen dem Staatsministerium für Gesundheit und Pflege keine Kenntnisse vor. Es ist jedoch davon auszugehen, dass die Krankenhäuser im Rahmen des betrieblichen Risikomanagements über entsprechende Notfallkonzepte verfügen.

5. Ausstattung I

a) Wie viele planmäßige Stellen stehen den in Frage 1 a genannten Einrichtungen im Schnitt für den Bereich IT-Sicherheit zur Verfügung (bitte aufgeschlüsselt nach Einrichtung und Trägerschaft)?

b) Wie viele davon sind jeweils aktuell im Durschnitt besetzt (bitte aufgeschlüsselt nach Art der Einrichtung und Trägerschaft)?

c) Wie viele planmäßige Stellen im Bereich der IT-Sicherheit gab es im Schnitt in den Rechenzentren der staatlichen Hochschulen pro 1 000 Studierende in den letzten zehn Jahren (bitte aufgeschlüsselt nach Jahren)?

Die Gewährleistung der IT-Sicherheit erfordert die Beteiligung und Zusammenarbeit zahlreicher Organisationseinheiten mit ihren je spezifischen Aufgabenstellungen, sodass eine konkrete Stellenausstattung nur mit erheblichem Aufwand ermittelt werden könnte. Unabhängig davon haben Hochschulen und nichtstaatliche Forschungseinrichtungen die Funktion eines IT-Sicherheitsbeauftragten definiert, der als zentraler Ansprechpartner Informationen bündelt, erforderliche Maßnahmen initiiert und deren Umsetzung koordiniert und verfolgt. Das damit verbundene Stundenkontingent variiert nach Größe der Einrichtung und dem bestehenden Risikopotential zwischen ca. 0,1 und 1,5 Planstellen.

Auch innerhalb eines Hochschulrechenzentrums wirken zur Gewährleistung der IT-Sicherheit verschiedene Bereiche jeweils arbeitsteilig zusammen; eine Quantifizierung der entsprechenden Personalaufwendungen wäre nur mit erheblichem Aufwand möglich, eine Aufschlüsselung der Stellenanteile über zehn Jahre hinweg ist nicht leistbar. Insgesamt kann jedoch festgestellt werden, dass im Zuge der zunehmenden Digitalisierung innerhalb der letzten zehn Jahre auch in den Rechenzentren zusätzliche Personalkapazitäten aufgebaut wurden.

6. Ausstattung II

a) Wie viele finanzielle Mittel stehen den in Frage 1 a genannten Einrichtungen durchschnittlich für IT-Sicherheit zur Verfügung (bitte aufgeschlüsselt nach Art der Einrichtung und Trägerschaft)?

Spezielle Auswertungen hinsichtlich der Ausgaben für IT-Sicherheit der einzelnen Hochschulen oder sonstigen Forschungseinrichtungen liegen nicht vor. Im Übrigen fehlt auch eine Abgrenzung, welche Aufwendungen einzubeziehen wären und wie mit zentralen Dienstleistungen zu verfahren wäre. Eine Forschungsorganisation schätzt über alle Institute hinweg den jährlichen Anteil der Sachaufwendungen für IT-Sicherheitsmaßnahmen auf ca. 2 Prozent des gesamten IT-Budgets einschließlich der darin enthaltenen Personalkosten.

Bei den Plankrankenhäusern sind notwendige Investitionen im IT-Bereich aus den jährlichen Pauschalmitteln als Teil der Krankenhausförderung zu tätigen. Die Pauschalmittel wurden bereits 2018 um 50 Mio. Euro erhöht, insbesondere um Investitionen im IT-Bereich zu erleichtern. Insgesamt stehen den Häusern aktuell Pauschalmittel in Höhe von rund 276 Mio. Euro zur Verfügung, die von den Krankenhausträgern eigenverantwortlich bewirtschaftet und aufgrund interner Überlegungen und Schwerpunktsetzungen verwendet werden. Zudem plant der Bund im Rahmen des „Zukunftsprogramms Krankenhäuser“, den bereits bestehenden Krankenhausstrukturfonds im IT- und Digitalisierungsbereich weiter zu öffnen. Es ist zu erwarten, dass künftig mehr Krankenhäuser von diesen Fördermitteln profitieren können. Damit würde der Bund eine Forderung Bayerns aufgreifen, die Förderung nicht auf die Häuser zu beschränken, die wie die Universitätsklinika der „Kritischen Infrastruktur“ (mehr als 30 000 vollstationäre Fälle im Jahr) zuzuordnen sind. Im Detail ist das Gesetzgebungsverfahren abzuwarten.

b) In welchem Umfang plant die Staatsregierung in den nächsten Jahren eine Erhöhung der Zuwendungen und Stellen für den Bereich IT-Sicherheit für die in Frage 1 a genannten Einrichtungen, welche vom Freistaat oder den Kommunen betrieben werden?

Der Krankenhausförderetat und damit die zur Verfügung stehenden Pauschalmittel sollen über die gesamte Legislaturperiode auf dem bestehenden hohen Niveau fortgeführt werden. Eine einseitige Erhöhung für kommunale Krankenhäuser ist aufgrund des gesetzlich vorgegebenen Prinzips der Trägerpluralität nicht möglich.

7. Unterstützung durch den Freistaat

a) In welchem Umfang stellt der Freistaat den in Frage 1 a genannten Einrichtungen Unterstützung organisatorischer, technischer, personeller oder sonstiger Art zur Verfügung, um die IT-Sicherheit zu verbessern?

b) In welchem Umfang plant die Staatsregierung diese Unterstützungsmöglichkeiten in den nächsten Jahren zu erhöhen (bitte geplanten Zeitrahmen angeben)?

c) In welchem Umfang werden diese Unterstützungsmöglichkeiten von den Einrichtungen in Anspruch genommen?

Für den Bereich der Hochschulen hat das Staatsministerium für Wissenschaft und Kunst die hochschulübergreifende Stabsstelle IT-Sicherheit in Augsburg geschaffen. Deren Unterstützungsangebote werden von den Hochschulen bei der Planung und Umsetzung konkreter lokaler Maßnahmen regelmäßig in Anspruch genommen.

Für die Plankrankenhäuser bestehen neben der staatlichen Krankenhausförderung keine Unterstützungen des Freistaates Bayern. Betriebskosten – wie Personalkosten – sind aus den Vergütungen der Kostenträger zu tragen. Hierzu liegt die Gesetzgebungskompetenz beim Bund. Jedoch bietet das LSI den bayerischen Plankrankenhäusern Beratungen an, die von diesen genutzt werden. Ein konkretes Unterstützungsangebot stellt die Orientierungshilfe „IT-Sicherheit in Kliniken“ dar. Mit dem weiteren Ausbau des LSI sollen diese Beratungsaktivitäten weiter intensiviert werden.

8. Beratung der Staatsregierung

a) In welcher Form lässt sich die Staatsregierung von den in Frage 1 a genannten Einrichtungen über aktuelle und geplante Maßnahmen im Bereich IT-Sicherheit informieren?

b) Wie lässt sich die Staatsregierung über aktuelle Entwicklungen im Bereich IT-Sicherheit informieren und beraten?

c) Existiert vonseiten der Staatsregierung ein übergreifendes Gesamtkonzept, wie höchstmögliche IT-Sicherheit in den einzelnen Einrichtungen gewährleistet werden kann (bitte begründen)?

Über aktuelle Entwicklungen auch zur Informationssicherheit informieren die Hochschulen regelmäßig im Rahmen der Treffen der Chief Information Officer (CIOs) der Hochschulverbünde, an denen das Staatsministerium für Wissenschaft und Kunst teilnimmt.

Das Staatsministerium für Wissenschaft und Kunst berät sich im Rahmen einer länderübergreifenden Arbeitsgruppe regelmäßig mit dem Verein zur Förderung eines Deutschen Forschungsnetzes (DFN-Verein). Dieser stellt neben der bundesweiten technischen Netzinfrastruktur auch verschiedene Dienstleistungen zur Verfügung. Hervorzuheben ist das DFN-CERT (Computer Emergency Response Team), das den Anwendern schnelle und effiziente Hilfe bei der Reaktion auf Sicherheitsvorfälle sowie Unterstützung bei der Durchführung vorbeugender Sicherheitsmaßnahmen bietet. Das DFN-CERT ist in den nationalen und internationalen CERT-Verbund eingebunden, über den Informationen zu Schwachstellen oder Warnmeldungen zu systematischen Angriffen ausgetauscht werden.

Länder- und einrichtungsübergreifend wird die Weitergabe von Gefahrenhinweisen der Sicherheitsbehörden im Wissenschaftsbereich durch den „Arbeitskreis Informationssicherheit der deutschen Forschungseinrichtungen“ (AKIF) organisiert. Darüber hinaus bietet der ZKI e.V. (Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung) mit seinen Arbeitskreisen Netzdienste sowie Servicemanagement und IT-Sicherheit eine bundesweite Plattform für den Informationsaustausch.

Als zentrale Kontaktstelle für Bayern informiert das LSI über das Bayern-CERT die Hochschulen und die Plankrankenhäuser anlassbezogen über aktuelle, als kritisch eingeschätzte Sicherheitsbedrohungen und laufende Angriffe. Darüber hinaus gibt es Warnmeldungen des BSI für die KRITIS-Sektoren an die Aufsichtsbehörden weiter.

Die vom Bund und von den Ländern geförderten außeruniversitären Forschungseinrichtungen berichten den Zuwendungsgebern im Rahmen ihrer Berichts- und Nachweispflichten über die Verwendung der institutionellen Förderung auch über Maßnahmen im Bereich IT-Sicherheit.