Einzelplan 06
Ministerium für Wissenschaft, Forschung und Kultur (MWFK)

17 IT-Sicherheit an den Hochschulen in Gefahr

An vielen Hochschulen des Landes ist die IT-Sicherheit gefährdet. Insbesondere fehlt es an einer konzeptionellen Herangehensweise. Hier besteht Aufhol- und Verstetigungsbedarf.

Die Verantwortung für eine ausreichende IT-Sicherheit liegt bei der Leitungsebene der Hochschulen. Diese sollten künftig noch stärker IT-Sicherheit als Führungsaufgabe erkennen und wahrnehmen. Das Wissenschaftsministerium als Rechts- und Fachaufsichtsbehörde ist gefordert, die Hochschulen künftig nicht mehr weitestgehend allein zu lassen, sondern nach Kräften zu unterstützen.

17.1 Prüfungsgegenstand

Die Hochschulen sind ein attraktives Ziel für Hacker. Der Landesrechnungshof prüfte die IT-Sicherheit an den acht staatlichen Brandenburger Hochschulen. Die Hochschulen arbeiten zunehmend IT-gestützt. Damit steigt die Abhängigkeit von sicher und zuverlässig funktionierender Informationstechnik. Neben physischen Gefahren wie zum Beispiel Stromausfällen stellen auch Hackerangriffe eine diffuse Bedrohung für den stabilen IT-Betrieb und die IT-Infrastruktur dar. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) schätzt die IT-Sicherheitslage in Deutschland als „angespannt bis kritisch"[1] ein.

Seit Dezember 2019 waren mindestens drei deutsche Universitäten und ein Universitätsklinikum das Ziel erfolgreicher Hackerangriffe. Um weiteren Schaden zu verhindern, mussten die Hochschulen ihre Computersysteme

1 BSI (Hrsg.) (2021): Die Lage der IT-Sicherheit in Deutschland 2021. Bonn: BSI, S. 9.

präventiv – teilweise über mehrere Monate – abschalten.[2] Die Kosten zur Behebung der Schäden sind zum Teil beträchtlich. Alleine die Universität Gießen musste 1,7 Mio. Euro aufwenden.[3]

Der Landesrechnungshof prüfte querschnittlich, welche konzeptionellen, technischen und personellen Maßnahmen die Hochschulen ergriffen haben, um die IT-Sicherheit zu gewährleisten.[4] Er konzentrierte sich auf die IT-Sicherheit in den Jahren 2018 und 2019, berücksichtigte aber auch spätere Entwicklungen. Die Prüfung erfolgte anhand von einheitlichen schriftlichen Fragebögen, Interviews sowie teilweise Inaugenscheinnahmen an den Hochschulen, beginnend ab Juni 2020.

Als Prüfungsmaßstäbe legte der Landesrechnungshof allgemein anerkannte und grundlegende Standards zur Informationssicherheit zu Grunde, insbesondere den IT-Grundschutz des BSI sowie die Anforderungen der ISO-Norm 27001.[5]. In seinen Bewertungen berücksichtigte er – wie immer – die Haushaltsgrundsätze der Wirtschaftlichkeit und Sparsamkeit.

2 Vgl. für viele: Warnecke, Tilmann (2021): Hackerangriff auf die TU. Uni-Angehörige können ihre Mails nicht benutzen, die Verwaltung ist eingeschränkt. In: Der Tagesspiegel vom 4. Mai 2021, S. 18; Ruhr Universität Bochum (Hrsg.) (2020): IT-Infrastruktur der RUB ist teilweise außer Betrieb. Online unter: www.news.rub.de/servicemeldungen/2020-05-07-digitale-lehre-geht-weiter-it-infrastruktur-der-rub-ist-teilweise-ausser-betrieb [zuletzt abgerufen am 13. September 2021]; Mukherjee, Joybrato (2020): „#JLUoffline war ein Weckruf." Der Präsident der Justus-Liebig-Universität Gießen über den Cyberangriff auf seine Hochschule. Interview mit Katrin Schmermund. In: Forschung & Lehre, 27. Jg., H. 2, S. 126 f.; Forschung & Lehre (Hrsg.) (2021): BSI: Hackerangriff auf Uniklinik vermeidbar. In: Forschung & Lehre, 28. Jg., H. 2, S. 94.

3 Vgl. Helwig, Heidrun (2020): Teure Cyberattacke in Gießen: #JLUoffline kostet 1,7 Millionen Euro. Online unter: www.giessener-anzeiger.de/lokales/stadt-giessen/nachrichten-giessen/teure-cyberattacke-in-giessen-jluoffline-kostet-17-millionen-euro_22020391 [zuletzt abgerufen am 13. September 2021].

4 Um sicherheitsrelevante Lücken der IT-Sicherheit an den Hochschulen nicht offenzulegen, konnten einzelne Prüfungsfeststellungen nicht in den Jahresbericht aufgenommen werden. Zudem musste auf eine zu umfangreiche Detailtiefe verzichtet werden.

5 Darüber hinaus wandte der Landesrechnungshof die Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik – Leitlinien und gemeinsame Maßstäbe für IT-Prüfungen – (IT-Mindestanforderungen 2020) in der Fassung vom August 2020, die Leitlinie für die Informationssicherheit in der Landesverwaltung Brandenburg (Informationssicherheitsleitlinie) in der Fassung vom 14. April 2014 sowie die Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung, Version 2.0 des IT-Planungsrates in der Fassung vom 6. Dezember 2018 an.

17.2 Prüfungsergebnis

17.2.1 IT-Sicherheit stiefmütterlich finanziert

Das MWFK weist den staatlichen Hochschulen im Land Brandenburg ihre Haushaltsmittel global zu. Die Hochschulen bewirtschaften die pauschalen Zuschüsse im Rahmen ihrer Hochschulautonomie weitgehend unabhängig und eigenständig, so auch für IT-Betrieb und Informationssicherheit.

Die Hochschulen teilten dem Landesrechnungshof mit, für IT-Sicherheit in den geprüften Jahren jährlich insgesamt rund 1,2 Mio. Euro verausgabt zu haben.[6] Die jährlichen Ausgaben je Hochschule lagen zwischen 25.000 und 687.000 Euro. Die Hälfte der Hochschulen gaben jährlich weniger als 120.000 Euro für IT-Sicherheit aus.

Bei diesen Werten ist allerdings zu berücksichtigen, dass mehrere Hochschulen ihre Ausgaben für IT-Sicherheit mangels gesonderter Mittelausweisung lediglich schätzen konnten. Eine Hochschule konnte ihre IT-Sicherheitsausgaben gar nicht beziffern.

Einzelne Hochschulen finanzierten zudem Maßnahmen zur IT-Sicherheit nicht aus der Grundfinanzierung. Sie nutzten stattdessen unregelmäßig zur Verfügung stehende Sonder- und Drittmittel, obwohl Ausgaben für IT-Sicherheit im Regelfall laufend anfallen.

Keine Hochschule stellte Wirtschaftlichkeitsuntersuchungen für Maßnahmen der IT-Sicherheit an. Die einzelnen Maßnahmen waren ganz überwiegend nicht in ein übergreifendes IT-Sicherheitskonzept integriert.

17.2.2 Zu wenig Personal für IT-Sicherheit

An den Hochschulen arbeitete 2018 Personal im Umfang von 128 Vollzeitäquivalenten (VZÄ) in den zentralen IT-Einheiten. Im Folgejahr waren es 11 VZÄ mehr. Mit dezidierten Aufgaben der IT-Sicherheit wurden in beiden Jahren jeweils rund 13 VZÄ betraut, davon 9 VZÄ bei nur einer Hochschule. Keine Hochschule verfügte über Personal, das sich ausschließlich mit IT-Sicherheit befasste.

Die Hochschulen unterließen es weitestgehend, die Aufgaben im Bereich der IT-Sicherheit zu erfassen und konkret zu beschreiben. Ebenso wenig

6 Berücksichtigt wurden Ausgaben für Hardware, Software und Personal.

ermittelten sie den Personalbedarf für die Erfüllung dieser Aufgaben. Die Hochschulen gaben vielmehr an, dass sich die personellen Kapazitäten „historisch entwickelt" hätten.[7]

Zwar wurde den Mitarbeitenden, die IT-Sicherheitsaufgaben übernahmen, von den Hochschulen grundsätzlich die Teilnahme an IT-Sicherheitsfortbildungen ermöglicht. Trotz der dynamischen Entwicklungen in der IT-Sicherheit wurden diese jedoch nur schwach nachgefragt.

Fünf der acht Hochschulen verfügten organisatorisch über dezentrale IT-Einheiten, die ihre IT-Systeme relativ autonom im Hochschulnetz betrieben. Das birgt die Gefahr, dass IT-Sicherheitsvorkehrungen der zentralen IT dort nicht umgesetzt werden.

17.2.3 Informationssicherheitsbeauftragte: zwingend erforderlich, aber selten vorhanden

Die Hochschulen sind gehalten, Informationssicherheitsbeauftragte zu bestellen. Diese sind organisatorisch unabhängig und direkt den Hochschulleitungen unterstellt.[8]

Nur drei Hochschulen hatten bei Prüfungsbeginn Informationssicherheitsbeauftragte eingesetzt. Zwei Hochschulen nahmen eine Bestellung im Verlauf der Prüfung vor.

Den bereits berufenen Informationssicherheitsbeauftragten stand ein Arbeitszeitanteil von 5 bis 20 Prozent für diese Funktion zur Verfügung. Einige übernahmen überwiegend Aufgaben im operativen IT-Betrieb.

Zudem waren an einigen der Hochschulen die Informationssicherheitsbeauftragten nicht konsequent in IT-sicherheitsrelevante Verfahren und Entscheidungen eingebunden. In Einzelfällen waren sie darüber hinaus nur rudimentär mit der IT-Infrastruktur vertraut.

7 Vgl. ISMS.1.A6 BSI IT-Grundschutz, demnach eine geeignete übergreifende Organisationsstruktur für Informationssicherheit vorhanden sein muss.

8 Vgl. ISMS.1.A4 BSI IT-Grundschutz und A.6.1.2 ISO-Norm 27001.

17.2.4 Informationssicherheitsleitlinien: ein rares Gut

Im Prüfungszeitraum hatten nur drei der acht Hochschulen eine nach ISMS.1.A3 BSI IT-Grundschutz[9] vorgesehene Informationssicherheitsleitlinie in Kraft gesetzt, welche die grundlegenden Informationssicherheitsziele und -strategien fixiert. Deshalb war es dem Landesrechnungshof an fünf Hochschulen nicht möglich zu prüfen, ob sie in angemessenem Maße übergeordnete IT-Sicherheitsziele festlegten und eine adäquate Informationssicherheitsstrategie verfolgten.

17.2.5 IT-Sicherheitskonzept für Verwaltung und Wissenschaft

Aus der übergreifenden IT-Sicherheitsstrategie sind gesonderte Sicherheitskonzepte abzuleiten. In diesen soll der spezifische Schutzbedarf der eingesetzten Systeme und Daten festgehalten werden. Dabei sind vor allem die unterschiedlichen Aufgaben der Hochschulverwaltung und des wissenschaftlichen Bereichs zu berücksichtigen. Zudem sollen aus den Schutzbedarfen angemessene Sicherheitsmaßnahmen abgeleitet werden.[10]

Fünf der acht Hochschulen konnten dem Landesrechnungshof kein Sicherheitskonzept für die Verwaltung vorlegen. Für den Wissenschaftsbereich lag nur an einer Hochschule ein Sicherheitskonzept vor.

17.2.6 IT-Sicherheitsmängel an Arbeitsplatzrechnern

Das Verhalten der Mitarbeitenden ist ein maßgeblicher Erfolgsfaktor für den Schutz der Hochschulnetze und der Daten. Ihre Bedeutung wird regelmäßig unterschätzt.[11]

Sensibilisierung und Schulung der Mitarbeitenden

Strukturierte Sensibilisierungs- und Schulungsprogramme zur Informationssicherheit wurden von den Hochschulen weitestgehend weder konzipiert noch durchgeführt.[12] Nur in Ausnahmefällen boten sie eigene oder

9 Vgl. auch A.5.1 ISO-Norm 27001.

10 Vgl. ISMS.1.A10 BSI IT-Grundschutz.

11 Vgl. ENISA (Hrsg.) (2020): Insider Threat. ENSIA Threat Landscape. From January 2019 to April 2020. ENISA: Attiki.

12 Vgl. Baustein ORP.3 BSI IT-Grundschutz.

externe Schulungsmaßnahmen und Sensibilisierungen regelmäßig an. Die Sensibilisierung der Nutzenden in Informationssicherheit erfolgte hauptsächlich schriftlich über Awareness-E-Mails sowie Merkblätter und Informationen auf den Internetseiten der Hochschulen.

Schwacher Passwortschutz

Alle Hochschulen hatten Passwortvorgaben getroffen und technisch umgesetzt. Nach den Mindestvorgaben konnten die Nutzenden jedoch teilweise nicht ausreichend komplexe Kennwörter wählen.[13]

Fehlende Bildschirmsperren

Nur bei drei Hochschulverwaltungen war vorgegeben, dass die Beschäftigten Bildschirmsperren beim Verlassen des Büros zu aktivieren haben. Lediglich eine der Hochschulen richtete für die Verwaltung eine automatische Bildschirmsperre ein, allerdings erst nach 20 Minuten.[14]

Installation gefährlicher Software

An fünf der acht Hochschulen können die Mitarbeitenden im wissenschaftlichen Bereich an den Computern ungehindert selbst Software installieren. Dies hat zur Folge, dass die installierte Software weder von der IT-Einheit überprüft noch erfasst wurde.[15]

Veraltete Dateiformate in E-Mails

Alle Hochschulen schränken den Empfang von E-Mail-Anhängen ein. Zum Teil können die Nutzenden nach einem Warnhinweis die E-Mails mit potenziell gefährlichen Anhängen eigenständig öffnen.[16]

13 Vgl. BSI (Hrsg.) (2019): Sichere Passwörter – Faktenblatt. Online unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/sichere_passwoerter_faktenblatt.pdf?__blob=publicationFile&v=1 [zuletzt abgerufen am 13. September 2021].

14 Vgl. SYS.2.2.A1 BSI IT-Grundschutz.

15 Vgl. A.12.6.2 der ISO-Norm 27001.

16 Das BSI warnt im Grundschutz-Baustein APP.1 ausdrücklich vor schädlichen Inhalten in Office-Dokumenten.

17.2.7 Gefahrenquelle Hochschulnetz

Der Landesrechnungshof untersuchte, wie die Hochschulnetze geplant, aufgebaut und betrieben wurden. Dabei stellte er fest, dass die Hochschulnetze grundsätzlich gut vor Hackerangriffen geschützt sind. Dennoch erkennt der Landesrechnungshof weiteres Verbesserungspotenzial.

Fehlende Redundanz von Netzwerktechnik

Einige Hochschulen haben die zentralen Router und Switche nicht redundant[17] ausgelegt, sodass hier ein Single Point of Failure[18] bestand. Fallen diese Systemkomponenten aus, wird die Funktionalität und Verfügbarkeit des IT-Gesamtsystems oder anderer Komponenten beeinträchtigt, möglicherweise bis hin zum Ausfall.

Umgang mit DDoS-Angriffen

Hackerangriffe erfolgen sehr oft als sogenannte Distributed-Denial-of-Service-(DDoS-)Angriffe. Hierbei wird die Nichtverfügbarkeit von Internetdiensten durch die Überlastung der Internetanbindung infolge einer hohen Anzahl an Serveranfragen von vielen Quellen, sogenannten Bots, herbeigeführt.[19] Nur fünf der acht Hochschulen konnte eine DDoS-Schutzlösung vorweisen.

17.2.8 (Un-)Sicherheit der Serverräume

An mehreren Hochschulen fand der Landesrechnungshof Serverräume vor, die bauseitig nicht für den Rechenzentrumsbetrieb ausgelegt sind.

Nutzung von Serverräumen als Lager

Einige Hochschulen nutzten ihre Serverräume gleichzeitig als Lagerräume. Die Einlagerungen von u. a. Pappkartons und Kopiergeräten stellten potenzielle Brandlasten dar.[20]

17 Unter Redundanz wird das mehrfache Vorhandensein von gleichartigen Ressourcen eines technischen Systems verstanden. Die Redundanz stellt ein wesentliches Prinzip zur Realisierung hochverfügbarer IT-Infrastrukturen dar. Vgl. BSI (Hrsg.) (2013): Band G, Kapitel 7: Prinzipien der Verfügbarkeit. Bonn: BSI, S. 6.

18 Ein Single Point of Failure stellt einen Bestandteil eines technischen Systems dar, dessen Ausfall den Ausfall des gesamten Systems verursachen kann.

19 Vgl. BSI (Hrsg.) (2020): Die Lage der IT-Sicherheit in Deutschland 2020. Bonn: BSI, S. 29.

20 Vgl. INF.1.M3 BSI IT-Grundschutz.

Brandschutz

Die Serverräume mehrerer Hochschulen waren nicht mit Rauchmeldern, Brandschutztüren oder einer Feuerlöschanlage ausgestattet.[21] Eine frühe Branderkennung und ein schnelles Eingreifen tragen aber zum Schutz des Personals und der Technik bei.

Notstromversorgung

Zwar verfügten alle Hochschulen über eine batteriebetriebene unterbrechungsfreie Stromversorgung (USV). Diese war jedoch nicht an allen Hochschulen so ausgelegt, ein sicheres Herunterfahren der IT-Systeme durch die Mitarbeitenden zu ermöglichen. Über ein zusätzliches Dieselnotstromaggregat verfügten lediglich zwei Hochschulen.[22]

Klimaanlage

Um eine Überlastung der Systeme zu verhindern, haben die Hochschulen ihre Serverräume mit Klimaanlagen ausgestattet. In einzelnen Hochschulen ist die notwendige Klimatisierung der Serverräume bei Ausfall der primären Klimaanlage jedoch nicht sichergestellt.[23]

17.2.9 Laxer Umgang mit Sicherheitsvorfällen

Der Landesrechnungshof erhob, welche Verfahren und Maßnahmen die Hochschulen ergriffen haben, um schädlichen Einwirkungen schnell entgegenzutreten und Schäden zu verhindern.

Notfallkonzepte und Notfallhandbücher

Ein Notfallkonzept hat zum Ziel, Notfälle effektiv zu bewältigen und kritische Geschäftsprozesse schnell wiederaufzunehmen.[24] Doch nur wenige Hochschulen dokumentierten in einem Notfallkonzept ihre IT-Systeme und einen Plan zum Umgang mit einem Ernstfall.

Praxistaugliche Notfallhandbücher mit Handlungsanweisungen für kritische Schadereignisse, Wiederanlaufplänen und Informationen zu

21 Vgl. INF.2.A8, INF.2.A9, INF.2.A17, INF.1.M17 und INF.1.M22 des BSI IT-Grundschutz.

22 Vgl. INF.2.A3, INF.2.A25 und INF.5.A16 BSI IT-Grundschutz.

23 Vgl. INF.2.A16 BSI IT-Grundschutz.

24 Vgl. DER.4.A7 BSI IT-Grundschutz.

Kapazitäts- und Verfügbarkeitsanforderungen an einzelne IT-Systeme und IT-Anwendungen fehlten in fünf Hochschulen.[25]

Bearbeitung von Sicherheitsvorfällen

Lediglich eine Hochschule arbeitete standardisiert mit einem Formblatt zur Meldung von Sicherheitsvorfällen sowie zur anschließenden Protokollierung der getroffenen Maßnahmen. Zwei weitere Hochschulen verfügten zwar über ein entsprechendes Muster, setzen es jedoch nicht ein.[26]

17.2.10 Rolle des MWFK zwischen Hochschulautonomie und IT-Sicherheit

Das MWFK fördert das hochschulübergreifende Zentrum für Digitale Transformation (ZDT) an der TH Wildau. Die Einrichtung sollte ursprünglich die Digitalisierung von Verwaltungsleistungen der Hochschulen vorantreiben, befasst sich aber zunehmend auch mit Fragen der IT-Sicherheit.

Doch das MWFK unterstützte den Austausch der Hochschulen untereinander etwa durch Best-Practice-Vergleiche nicht. Es unterstützte die Hochschulen nicht bei der Zusammenarbeit auf dem Gebiet der IT-Sicherheit. Das hätte die Arbeit an den einzelnen Hochschulen erleichtern können.

Ebenso fehlten ministerielle Vorgaben zur Gewährleistung der IT-Sicherheit an den Hochschulen. Im Prüfungsverlauf äußerten die Hochschulen, dass sie konkrete Vorgaben im Kontext der IT-Sicherheit begrüßen würden. Sie sähen das nicht als Eingriff in die Hochschulautonomie.

Darüber hinaus gaben die Hochschulen an, ganz überwiegend keinen Kontakt zum MWFK betreffend IT-Sicherheitsfragen zu haben. Konkrete Ansprechpersonen im Ministerium waren den IT-Einheiten nicht bekannt.

17.3 Folgerungen

IT-Sicherheit an Hochschulen ist angesichts ihrer hohen Vulnerabilität und der daraus resultierenden hohen monetären und nichtmonetären Schadensrisiken kein nachrangiger Aspekt der universitären Aufgaben. Die Hochschulleitungen sollten die Gewährleistung von IT-Sicherheit vielmehr als Kernaufgabe verstehen. Der Landesrechnungshof sieht das MWFK

25 Vgl. DER.4.A1 BSI IT-Grundschutz.

26 Vgl. Baustein DER2.1 BSI IT-Grundschutz.

gefordert, gemeinsam mit den Hochschulen die IT-Sicherheit weiter zu verbessern.

Hierzu sollten das MWFK und die Hochschulen sicherstellen, dass die IT-Sicherheit dauerhaft und in ausreichendem Maße aus den Globalzuweisungen finanziert werden kann. Um wirtschaftlich und sparsam in IT-Sicherheit zu investieren, bedarf es strukturierter Sicherheitskonzepte und eines Überblicks über die verausgabten Mittel.

Der Landesrechnungshof sieht es kritisch, dass die dezidierten Aufgaben in der IT-Sicherheit sowie der Zeitbedarf zu ihrer Erfüllung nicht ermittelt und den Mitarbeitenden dezidiert zugewiesen wurden. Die Hochschulen kümmerten sich zu wenig um die IT-Sicherheitsaufgaben. Zudem waren die Arbeitszeitanteile zur Wahrnehmung der IT-Sicherheitsaufgaben zu gering bemessen.

Sofern an den Hochschulen dezentrale IT-Einheiten bestanden, konnten Sicherheitsmaßnahmen der zentralen IT-Einheiten umgangen werden. Bei einer Hackerattacke auf die TU Berlin drangen Angreifende über die dezentralen IT-Systeme der Hochschule ein und verschafften sich hierüber Zugang bis in die zentrale IT.[27] Der Landesrechnungshof hält es daher für notwendig, dass die dezentralen IT-Einheiten in die IT-Sicherheitsstrukturen der Hochschulen konsequent eingebunden werden und eine klare Kompetenzverteilung zwischen den beiden Ebenen besteht.

Problematisch war zudem, dass die meisten Hochschulen keine Informationssicherheitsbeauftragte mit der notwendigen Unabhängigkeit einsetzten. Sie müssen außerhalb des operativen IT-Betriebs stehen, um diesen effektiv kontrollieren zu können. Die Hochschulen sollten – gegebenenfalls gemeinsame – Informationssicherheitsbeauftragte einstellen.

Der Landesrechnungshof hält eine Informationssicherheitsleitlinie für elementar, um systematisch die grundsätzlichen Anforderungen und Ziele der IT-Sicherheit zu bestimmen und daraus eine Informationssicherheitsstrategie abzuleiten. Mit einer von der Hochschulleitung beschlossenen Informationssicherheitsleitlinie übernimmt diese auch die Verantwortung für Informationssicherheit und ihr Stellenwert innerhalb der Hochschulen wird verdeutlicht.

27 Christ, Sebastian (2021): Kampf an 1000 Einfallstoren. In: Der Tagesspiegel vom 30. August 2021, S. 21.

Der Landesrechnungshof sieht es kritisch, dass sieben Hochschulen es versäumten, für den Verwaltungs- und den Wissenschaftsbereich Informationssicherheitskonzepte zu erarbeiten. Mithin bleibt fraglich, ob die Maßnahmen geeignet und wirtschaftlich sind, die IT-Sicherheitsziele für die einzelnen Systeme und Daten zu erreichen. Hier erkennt der Landesrechnungshof Nachholbedarf.

Für die IT-Systeme sind auch die Nutzenden verantwortlich. Nicht allen sind die Gefahren durch Hackerattacken bewusst. Daher sind Vorgaben, Anweisungen und Sicherheitsrichtlinien für die Nutzenden von hoher Bedeutung. Für sie ist eine (verpflichtende) Sensibilisierung und Schulung essenziell.

Um die Konten der Nutzenden besser vor unberechtigtem Zugriff zu schützen, empfiehlt der Landesrechnungshof den Hochschulen, die Komplexität der Mindestanforderungen an Passwörter zu steigern.

Zudem sollten zum Schutz der PC-Systeme automatische Bildschirmsperren an jedem Arbeitsplatz nach einer festgelegten Zeitspanne von wenigen Minuten der Inaktivität eingeführt werden.

Der Landesrechnungshof hält die Installation von Software durch die Nutzenden im Grundsatz für problematisch. Weder wird die installierte Software vor ihrer Installation geprüft, noch haben die IT-Einheiten einen Überblick über die aufgespielten Programme und möglichen Sicherheitsrisiken.

Handlungsbedarf erkennt der Landesrechnungshof auch bei der konsequenten Sperrung von Dateiformaten mit potenzieller Schadsoftware in den Anhängen von E-Mails durch die Hochschulen. Hierdurch kann das Risiko von erfolgreichen Angriffen mit Schadsoftware verringert werden.

Auch die technische Infrastruktur an den Hochschulen ist ausbaufähig. Es sollte geprüft werden, inwiefern die Redundanz der Netzwerkhardware verbessert werden kann, um die Ausfallsicherheit weiter zu erhöhen. Des Weiteren empfiehlt der Landesrechnungshof den Hochschulen, eigene Maßnahmen oder eine Dienstleisterlösung zur Abwehr von DDoS-Angriffen zu implementieren.

Gerade in Technikräumen ist es wichtig, einen Brand schnell festzustellen und zu bekämpfen. Der Brandschutz in den Serverräumen sollte einer kritischen Analyse unterzogen werden.

Sofern die Hochschulen die Notstromversorgung ihrer Serverräume nur über eine USV sicherstellen, ist nach Auffassung des Landesrechnungshofs ein automatisiertes Herunterfahren der Systeme notwendig. Wie an einigen Hochschulen bereits geschehen, sollte zudem die Nutzung eines Dieselnotstromaggregats geprüft werden.

Nicht redundante Klimaanlagen betrachtet der Landesrechnungshof ebenfalls als problematisch. Das Öffnen der Fenster beim Ausfall der Klimaanlagen stellt keine durchgehend geeignete Maßnahme zur Klimatisierung der Serverräume dar. Zumindest sind Industrielüfter vorzuhalten. Grundsätzlich sollte eine redundante Auslegung der Klimaanlagen in Betracht gezogen werden.

Der Landesrechnungshof hält dezidierte Notfallkonzepte und Notfallhandbücher für notwendig. Damit wäre sichergestellt, dass Notfallprozesse, Vorgehensweisen, Zuständigkeiten und Meldeketten dokumentiert sind und personenunabhängig vorliegen. Zudem können vorab festgelegte Notfallkonzepte und Notfallhandbücher dazu beitragen, die Auswirkungen dynamisch verlaufender Sicherheitsereignisse einzudämmen.

Der Landesrechnungshof sieht das MWFK in der Pflicht, die Hochschulen bei der Gewährleistung der IT-Sicherheit als kompetenter Ansprechpartner aktiv zu unterstützen. Im Rahmen der Rechts- und Fachaufsicht sollte es

— Vorgaben machen und Empfehlungen aussprechen,

— die Zusammenarbeit der Hochschulen auf dem Gebiet der IT-Sicherheit fördern sowie

— sich über den Stand der IT-Sicherheit berichten lassen, um Fehlentwicklungen gegenzusteuern und Optimierungsbedarf zu erkennen.

Die Hochschulen befürworteten eine vertiefte Zusammenarbeit mit dem MWFK. Darüber hinaus waren sie offen für Vorgaben für künftige Maßnahmen zur Verbesserung der IT-Sicherheit.

17.4 Stellungnahme

Das MWFK teilt die Auffassung des Landesrechnungshofs, dass die Gewährleistung von IT-Sicherheit an den Brandenburger Hochschulen von besonderer Relevanz ist. Insofern wird die Prüfung des Landesrechnungshofs ausdrücklich begrüßt. Die Methodik der Prüfung wird als transparent, nach-

vollziehbar und geeignet zur Analyse der IT-Sicherheit an den Hochschulen anerkannt. Die vom Landesrechnungshof beanstandeten Defizite der IT-Sicherheit an den Hochschulen waren dem MWFK in der vorliegenden Menge sowie Detailtiefe bisher nicht bekannt.

Das Wissenschaftsministerium stimmt ferner mit dem Landesrechnungshof dahingehend überein, dass explizite ministerielle Vorgaben zur IT-Sicherheit an den Hochschulen bisher nicht bestehen. Die Hochschulen hätten entsprechende Wünsche auch nicht artikuliert. Zudem verweist das MWFK auf die „Leitlinie für die Informationssicherheit in der Landesverwaltung Brandenburg" in der Fassung vom 14. April 2014. Das MWFK werde prüfen, inwiefern ministerielle Vorgaben erforderlich und rechtlich möglich sind.

Ein deutlicher Dissens besteht hinsichtlich des bisherigen Agierens des Wissenschaftsministeriums bei der IT-Sicherheit. Hierzu trägt das MWFK vor: Es seien Maßnahmen ergriffen worden, damit die Hochschulen das Thema der IT-Sicherheit konzeptionell bearbeiten können. Konkret handele sich um

— ein Gutachten über die „Verwaltungs-IT der brandenburgischen Hochschulen" im Jahr 2017,
— die Mitbegründung des ZDT und die Finanzierung des dort angesiedelten Projekts „IT-Konzepte",
— die Berücksichtigung von IT-Sicherheit in einer Digitalisierungsagenda von MWFK und Hochschulen sowie
— die Auflage eines Förderprogramms, das auch die IT-Sicherheit adressiert.

Zudem stehe es den Hochschulen frei, auch ohne Unterstützung des MWFK miteinander in Austausch und Kooperation zu treten.

Eine Ansprechperson für IT-Sicherheit sei den Hochschul- und Verwaltungsleitungen bekannt. Die IT-Sicherheitsbeauftragte des MWFK habe akute Warnmeldungen an die Hochschulen weitergegeben.

Die Prüfung des Landesrechnungshofs wurde dessen ungeachtet vom MWFK unmittelbar zum Anlass genommen, gegenüber den Hochschulen tätig zu werden.

17.5 Schlussbemerkungen

IT-Systeme deutscher Hochschulen sind hoch vulnerabel. Dies zeigen die erfolgreichen Angriffe auf Wissenschaftseinrichtungen. Künftig sind sogar noch individualisiertere und komplexere Angriffe auf deren IT zu erwarten. Gleichzeitig steigt durch die zunehmende Digitalisierung die Abhängigkeit von einer sicheren IT. Infolgedessen kann auch von größeren Schadensszenarien ausgegangen werden. Deshalb sollten die Hochschulen den Empfehlungen des BSI folgen – sie sind State of the Art.

Der Landesrechnungshof begrüßt, dass das Wissenschaftsministerium einen Handlungsbedarf bei der IT-Sicherheit an den Hochschulen sieht. Er anerkennt ferner, dass das MWFK prüft, weitere Maßnahmen einzuleiten und den Kontakt zu den Hochschulen bereits aufgenommen hat. Es ist angezeigt, dass IT-Sicherheit in die Digitalisierungsagenda zwischen MWFK und Hochschulen aufgenommen wurde.

Die weitere vorgebrachte Argumentation hält der Landesrechnungshof hingegen für wenig stichhaltig. Denn das vorgelegte Gutachten aus dem Jahr 2017 hat bislang zu wenig Veränderungen insbesondere im konzeptionellen Bereich geführt. Die Hochschulen nahmen die im Gutachten festgestellten Mängel in der IT-Sicherheit nicht in ausreichendem Maße zum Anlass, geeignete Gegenmaßnahmen zu ergreifen. Das MWFK blieb hierbei passiv.

Positiv hervorzuheben ist, dass das Wissenschaftsministerium das ZDT weiter fördert. Das ZDT behandelte IT-Sicherheit bisher nur nachrangig. Angesichts der massiven Bedrohungen sollte IT-Sicherheit im Bereich des Projekts „IT-Konzepte" auch in den Fokus genommen werden.

Der Verweis auf die Informationssicherheitsleitlinie für die Brandenburger Landesverwaltung ist nur bedingt zielführend. Nach Auffassung des Landesrechnungshofs ist die Leitlinie für die Hochschulen nicht verpflichtend und darüber hinaus inhaltlich veraltet.[28]

Förderprogramme, die auch IT-Sicherheit adressieren, sind zwar grundsätzlich zielführend. Jedoch muss IT-Sicherheit als Daueraufgabe begriffen und demzufolge auch finanziert werden. Insbesondere bedarf es im Vorfeld

28 Vgl. Tz. 13.2.1 des diesjährigen Jahresberichtsbeitrags „Informationssicherheitsmanagement des Landes mit Lücken".

einer schlüssigen Gesamtplanung und Integration in das bestehende Sicherheitsgefüge.

Für den Landesrechnungshof ist nicht nachzuvollziehen, dass das MWFK davon ausgeht, dass den Hochschulen eine Ansprechperson für IT-Sicherheit bekannt sei. Diese Wahrnehmung teilte ausweislich der geführten Gespräche mit Mitgliedern der Hochschulleitungen und IT-Einheiten – selbst nach ausdrücklicher Rückfrage seitens des Landesrechnungshofs – nur eine Hochschule. Dies gilt auch für die Sicherheitshinweise der IT-Sicherheitsbeauftragten des Wissenschaftsministeriums.

Der Landesrechnungshof nimmt darüber hinaus zur Kenntnis, dass das Wissenschaftsministerium in seiner Stellungnahme nicht auf die technischen und baulichen Mängel im Bereich der IT-Sicherheit eingegangen ist. Ebenso wenig äußerte sich das MWFK zur Angemessenheit der übernommenen dezidierten IT-Sicherheitsaufgaben und deren personeller Ausstattung. Er erwartet auch hier ein Tätigwerden des MWFK.

Zunehmend erwarten staatliche und private Drittmittelgebende eine Zertifizierung der Informationssicherheit eines Managementsystems durch ein ISO 27001-Zertifikat. Das MWFK sollte auch deshalb die Hochschulen bei einer entsprechenden Zertifizierung unterstützen.

Die Hochschulen bleiben gefordert, die IT-Sicherheit technisch und konzeptionell weiter auszubauen. In diesem Zusammenhang ist auch eine hinreichende finanzielle Ausstattung im Auge zu behalten. Das MWFK muss sich aktiv in diesen kontinuierlichen Prozess einbringen. Der Landesrechnungshof wird die weiteren Entwicklungen in der IT-Sicherheit an den Hochschulen auch in Zukunft kritisch verfolgen.