Fachbeitrag

Michael Kost, Bastian Loibl, Peter Reuter und Matthias Stenke

#JLUoffline. Der Cyber-Angriff auf die Justus-Liebig-Universität Gießen im Dezember 2019

Verlauf, Krisenmanagement, Konsequenzen

#JLUoffline. The cyber-attack on Justus Liebig University Giessen in December 2019

Development, crisis management, consequences

https://doi.org/10.1515/abitech-2022-0005

Zusammenfassung: Am 8. Dezember 2019 wurde die Justus-Liebig-Universität Gießen (JLU) Opfer eines schwerwiegenden IT-Sicherheitsvorfalls, der von externen Angreifern verursacht worden war. Eine durchgeführte Ex-post-Analyse hat ergeben, dass die JLU durch die seinerzeit neuartige Ransomware *Ryuk* kompromittiert worden war. Der Angriff war der bis dahin größte auf eine Einrichtung der öffentlichen Hand, der bekannt geworden war. Für die rund 28 000 Studierenden und 5 500 Beschäftigten der Universität waren die folgenden Wochen durch ein Notfallmanagement gekennzeichnet. Durch rasches und konsequentes Handeln und durch eine Reihe konzertierter Maßnahmen konnte der Schaden in Grenzen gehalten werden. Eine neue IT-Governance- und Sicherheitsarchitektur, die im Dialog mit externen Gutachtern und Beratungsfirmen entwickelt wurde, soll zukünftig auch vor Angriffen besser schützen. Die Cyber-Attacke hat in vielen Hinsichten auch gezeigt, dass alle Mitarbeitenden in den Sicherheitsprozess einbezogen werden und Verantwortung tragen müssen, die Sicherheit einer Universität aktiv mitzugestalten.

Schlüsselwörter: Cyber-Attacke, IT-Governance, Justus-Liebig-Universität

Abstract: On 8 December 2019, Justus Liebig University Giessen fell victim to a serious IT security incident caused by external attackers. An ex-post analysis revealed that JLU had been compromised by *Ryuk*, a new type of ransomware at the time. The attack was the largest known to date on a public institution. For the university's approximately 28,000 students and 5,500 employees, the following weeks were characterized by emergency management. Through swift and consistent action and a series of concerted measures, the damage was kept within bounds. A new IT governance and security architecture, which was developed in dialogue with external experts and consulting firms, should also provide better protection against attacks in the future. The cyber-attack has also shown in many respects that all employees must be involved in the security process and must bear responsibility for actively helping to shape the security of a university.

Keywords: Cyber attack, IT governance, Justus Liebig University

1 Schadensvorfall und Umfang des Schadens

Am Sonntag, dem 8. Dezember 2019, wurden zunächst von Nutzenden einer Klinik in der Veterinärmedizin Probleme beim Zugriff auf ein IT-System bemerkt. Nachdem die Administratoren der Veterinärklinik festgestellt hatten, dass das System offenbar von Schadsoftware befallen war, wandten sie sich umgehend an das Hochschulrechenzentrum (HRZ) der JLU mit der Bitte um Unterstützung für das weitere Vorgehen. Zur Schadensbegrenzung wurde vom HRZ empfohlen, den Server umgehend vom Netzwerk zu trennen. Nähere Prüfungen ergaben, dass zahlreiche weitere Systeme betroffen sind, und ließen die große Tragweite des Angriffs deutlich werden. Nach Rücksprache mit dem Präsidium erfolgten daraufhin die Trennung der JLU vom Internet und das geordnete Herunterfahren der Server und Speichersysteme. Internet, E-Mail-Systeme und interne Netzwerke waren in der Folge nicht nutzbar.

Abb. 1: JLU-Präsident Prof. Joybrato Mukherjee sprach von einer „digitalen Naturkatastrophe“ (Foto: JLU/Katrina Friese)

Wegen des Verdachts auf einen Cyber-Angriff erstattete die JLU am 9. Dezember 2019 Strafanzeige gegen Unbekannt. Eine explizite Lösegeldforderung wurde nicht gestellt.

Die von der JLU durchgeführte Ex-post-Analyse hat gezeigt, dass der Angriff Windows-basierte Systeme betraf und in verschiedenen Phasen ablief. Zunächst wurden am Freitagabend, dem 6. Dezember 2019, Windows-Domänencontroller kompromittiert. Danach wurden gezielt Datensicherungssysteme angegriffen mit dem Ziel, die vorhandenen Datensicherungen unbrauchbar zu machen. In der letzten Phase des Angriffs, die in der Nacht vom 8. auf den 9. Dezember begann, wurde schließlich über einen kompromittierten Domänen-Controller die Ransomware *Ryuk* an potenziell alle zu dieser Zeit über das Netzwerk erreichbaren Systeme in der Windows-Domäne ausgebracht und zeitlich gestaffelt ausgeführt. In dieser Nacht wurde auch das Exchange-Mailsystem, bestehend aus einem Cluster mit vier Servern, angegriffen: Zwei der Server wurden verschlüsselt und unbrauchbar gemacht, die beiden anderen wurden so manipuliert, dass eine Anmeldung auf der Systemebene nicht mehr möglich war. Von den Angreifern wurde dabei sichergestellt, dass der Exchange-Dienst weiterlief und zur Nutzung zur Verfügung stand.

Bis zur Trennung der Universität vom Internet und dem Herunterfahren der Server und Speichersysteme hat der *Ryuk*-Verschlüsselungstrojaner weitere Schäden verursacht, durch die u. a. folgende Dienste und Infrastrukturen betroffen waren:

- Die Server-Infrastruktur für die Desktop-Virtualisierung, mit der ca. 500 Arbeitsplätze in Form von PC-Pools und Recherchearbeitsplätzen in den Bibliotheken bereitgestellt werden, wurde verschlüsselt und damit unbrauchbar gemacht.
- Ein Teil der Netzlaufwerke auf den zentralen Fileservern für den Bereich Forschung und Lehre wurde mittels der verbundenen Server- und Client-Systeme ganz oder teilweise verschlüsselt. Mit Hilfe von Backups konnten alle Daten mit dem Stand der vorhergehenden Nacht wiederhergestellt werden.
- Die zum Zeitpunkt des Angriffs im JLU-Netz in Betrieb befindlichen Client-Systeme für den Bereich Forschung und Lehre wurden kompromittiert und in unterschiedlichem Umfang verschlüsselt. Dies betraf ca. 300 Clients. Aus Sicherheitsgründen mussten ca. 6 000 Windows-basierte Endgeräte auf Schadsoftware untersucht werden.

- Die Windows-Domäne für den Bereich von Forschung und Lehre wurde durch den Angriff kompromittiert und musste ebenfalls neu aufgebaut werden.
- Rund 130 Windows-basierte, größtenteils virtualisierte Serversysteme mit verschiedenen Anwendungen wie z. B. Lizenzserver, Printserver, Fachanwendungen, Softwareverteilung waren kompromittiert und in unterschiedlichem Umfang verschlüsselt. Für den Neuaufbau der Systeme konnten die dafür erforderlichen Daten von den betroffenen Systemen nach Prüfung teilweise übernommen werden bzw. es lagen verwertbare Datensicherungen vor.

Die zunächst in den Medien geäußerte Befürchtung, dass auch das Universitätsklinikum Gießen und Marburg (UKGM) von der Cyber-Attacke betroffen sei, bestätigte sich glücklicherweise nicht. Das Universitätsklinikum mit seinen beiden Standorten, das seit 2006 privatisiert ist,[1] verfügt über ein separates Netz, das von dem Angriff nicht betroffen war, sodass Betriebsabläufe und Patientenversorgung gesichert waren.

2 Diagnose des Angriffs

Von der zur Analyse des Vorfalls herangezogenen Heidelberger Firma ERNW und dem Nationalen Forschungszentrum für angewandte Cybersicherheit (ATHENE)[2] wurden forensische Analysen von Systemen vorgenommen, durch die der Ablauf des Angriffs und hierfür verwendete kompromittierte Server im Netz der JLU ermittelt werden konnten. Bei der Ex-post-Analyse konnte nachvollzogen werden, dass der Angriff mutmaßlich über bestimmte Server im Internet gesteuert worden ist. Die gewonnenen Erkenntnisse wurden dem Hessischen Landeskriminalamt (LKA) in Wiesbaden mitgeteilt.

Die beim Angriff verwendete *Ryuk* Ransomware hat in der Cyberkriminalität in den vergangenen Jahren erheblich an Bedeutung gewonnen. Die Zahl der entdeckten Angriffe stieg von 5 123 im 3. Quartal 2019 auf über 67 Millionen im 3. Quartal 2020, so das Ergebnis einer Sicherheitsstudie von SonicWall.[3] *Ryuk* verschlüsselt alle Zieldateien mit einer starken Verschlüsselung und versucht auch, Datenträger-Schattenkopien zu löschen, damit Daten nicht mit alternativen Mitteln wiederhergestellt werden können. Bestimmte Dateien werden bei der Verschlüsselung übersprungen, z. B. solche, die in den Verzeichnissen Windows System32, Chrome, Mozilla oder Internet Explorer gespeichert sind, vermutlich um vor dem Hintergrund einer Lösegeldforderung die Systemstabilität zu erhalten und den Zugriff auf einen Browser zu ermöglichen. Aufgrund des Angriffsmusters auf die JLU ist davon auszugehen, dass zuvor eine initiale Infektion mit *Emotet* erfolgte[4] und im weiteren Verlauf die Schadsoftware *Trickbot* nachgeladen[5] und zum Abgreifen von Zugangsdaten sowie zur lateralen Ausbreitung im Netzwerk verwendet wurde. Trotz der im Januar 2021 vom Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldeten Zerschlagung der Emotet-Infrastruktur[6] geht von der Ryuk-Ransomware weiterhin eine große Gefahr aus: Eine weiterentwickelte Version ist bereits in der Lage, sich selbstständig in Netzwerken zu verbreiten.[7]

3 Organisatorische Sofortmaßnahmen

3.1 Sofortmaßnahmen im Hochschulrechenzentrum

Nur eine kurze Zeitspanne nach dem Auftreten der ersten Anzeichen eines offensichtlich größeren IT-Sicherheitsvorfalls kamen im Hochschulrechenzentrum (HRZ) die ersten Mitarbeiterinnen und Mitarbeiter zur Initiierung der ersten Maßnahmen zusammen, darunter die HRZ-Leitung sowie Fachexpertinnen und -experten aus allen

1 Das UKGM ist das drittgrößte Universitätsklinikum in der Bundesrepublik Deutschland. An den zwei Standorten Gießen und Marburg versorgen rund 9 600 Mitarbeiterinnen und Mitarbeiter jährlich rund 436 000 Patientinnen und Patienten in 80 Kliniken.

2 https://www.athene-center.de/ (22.11.2021).

3 Angaben nach: „Der Aufstieg der Ryuk Ransomware." In: *It-daily.net*, 19.01.21.

4 *Emotet* ist eine Familie von Computer-Schadprogrammen für Windows-Systeme in Form von Makroviren, welche die Empfänger über den Anhang sehr echt aussehender E-Mails mit Trojanern infizieren. Wenn ein Empfänger die Anlage bzw. den Anhang der E-Mail öffnet, werden Module mit Schadfunktionen nachgeladen und zur Ausführung gebracht. Als „Downloader" hat *Emotet* die Aufgabe, unbemerkt weitere Schadsoftware nachzuladen, etwa zur Verschlüsselung. *Emotet* galt lange als weltweit gefährlichste Schadsoftware. Im Januar 2021 wurde die Infrastruktur der *Emotet*-Schadsoftware von Europol unschädlich gemacht (Pressemitteilung des Bundeskriminalamts und der Generalstaatsanwaltschaft Frankfurt am Main vom 27.01.2021).

5 *Trickbot* ist ein Trojaner insbesondere für Microsoft-Betriebssysteme.

6 Pressemitteilung des BSI vom 21.01.2021. https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html (23.11.2021).

7 Angaben nach: The Open Security. https://theopensecurity.com/article/159-ryuk-ransomware-jetzt-mit-worming-selbstvermehrung/ (23.11.2021).

für diese Situation relevanten Bereichen. Innerhalb von 45 Minuten nach dem Eintreffen konnten erste Analysen den Schweregrad des IT-Sicherheitsvorfalls bestätigen, unmittelbar danach erfolgten die Information an Präsidium und Hessen-CERT[8] sowie – in Abstimmung mit dem Präsidium – die Trennung der JLU vom Internet und das Herunterfahren der Server- und Speichersysteme.

Noch am späten Nachmittag des 8. Dezember 2019 gab es im HRZ ein erstes Krisentreffen mit dem HRZ-Leiter und allen Abteilungsleitungen unter der Federführung des zuständigen Vizepräsidenten für Wissenschaftliche Infrastruktur. Am Abend wurden im HRZ erste „Action Teams" für die Bereiche Datennetz sowie Linux- und Windows-Server eingerichtet. In den Tagen darauf folgten weitere Teams für Clients, den Endgeräte-Scan und die Produktion und Verteilung von USB-Sticks und Anleitungen für Virenscans. Diese Teams hatten die Aufgabe, die für ihren Sachbereich relevanten Arbeitspakete zu benennen und gezielt umzusetzen. Für jedes dieser Teams zeichnete eine Koordinatorin oder ein Koordinator verantwortlich, der die Arbeitsergebnisse, aber auch auftretende Schwierigkeiten an die Personalkoordination kommunizierte, die wiederum an den Krisenstab zu berichten hatte. Im HRZ wurde ein Organisations- und Kommunikationsteam (auch für die Personalkoordination) eingerichtet, um eine direkte Kommunikation der Arbeitsebene Präsidium – Krisenstab – HRZ zu etablieren. Für Anfragen von Bediensteten an das zentrale Krisenmanagement und als Ersatz für das ebenfalls vom Vorfall betroffene Helpdesk-System des HRZ wurden Hotlines eingerichtet. Aufgrund der Nichtverfügbarkeit des Mailsystems wurden vom HRZ über einen kommerziellen Anbieter provisorische Mailadressen für Präsidiumsmitglieder und Bereiche mit zentraler Funktion im Krisenmanagement bereitgestellt.

Bereits am Tag des Vorfalls veranlasste das HRZ mit Hilfe des Rechenzentrums der Philipps-Universität Marburg (UMR) und des DFN-Vereins (Deutsches Forschungsnetz)[9] die Einrichtung einer temporären JLU-Webpräsenz auf den Servern der UMR. Die temporäre JLU-Homepage ging am Nachmittag des darauffolgenden Tages online.

Schon früh war offensichtlich, dass die personellen Ressourcen des Hochschulrechenzentrums nicht annähernd ausreichen würden, um die anstehenden Analyse- und Wiederherstellungsaufgaben insbesondere in den dezentralen Einrichtungen zu bewältigen. Daher wurde auf externe Unterstützung von verschiedenen Seiten zurückgegriffen.

Als IT-Fachleute und Kundige vor Ort waren die Mitglieder der Informations- und Kommunikationsmanagement Arbeitsgemeinschaft (IKM-AG) der JLU als sogenannte Paten unter Anleitung des HRZ u. a. bei den in mehreren Durchläufen durchzuführenden Scans, bei der Installation von Antivirensoftware und der Neuinstallation von Endgeräten in den dezentralen Einrichtungen eine große Hilfe. Zur Unterstützung des Wiederaufbaus und insbesondere der sehr zeitaufwändigen Prüfung sämtlicher Endgeräte (PC, Server) der JLU wurde von den benachbarten Hochschulen IT-Fachpersonal zur Verfügung gestellt. Die von ihren Hochschulen entsandten IT-Fachleute wurden von ihren örtlichen Kolleginnen und Kollegen in die umzusetzenden Maßnahmen eingeführt.

Die E-Mail-Fähigkeit konnte zum 19. Dezember 2019 mit dem System *Dovecot/Horde Webmail* wiederhergestellt werden. Bis zur Wiederaufnahme des Lehrbetriebes nach der Weihnachtspause konnten alle hierfür wichtigen digitalen Funktionen angeboten werden. Gleichwohl waren vor allem bei der Nutzung von Windows-Netzlaufwerken (winfile) und allen Verwaltungsabläufen die Auswirkungen des Cyberangriffes bis weit ins Jahr 2020 spürbar.

3.2 Ausgabe neuer Passwörter für alle JLU-Accounts

Eine besondere organisatorische Herausforderung stellte die Ausgabe neuer Passwörter für den Account der Justus-Liebig-Universität dar. Aus Sicherheitsgründen mussten alle Passwörter der vorhandenen ca. 38 000 JLU-Accounts zurückgesetzt und neu an die jeweiligen Nutzerinnen und Nutzer ausgegeben werden. Eine individuelle Zusendung per Post schied aufgrund kurzfristig nicht zugänglicher Adressdaten, aber auch aus Sicherheitsgründen aus. Damit war nur eine persönliche Abholung der durch das Hochschulrechenzentrum gedruckten und kuvertierten Passwortbriefe unter Vorlage eines amtlichen Lichtbildausweises und mit Bestätigung der Ausgabe durch Unterschrift möglich. Die Passwortausgabe erfolgte organisiert durch ein Team der Verwaltung insbesondere in zwei großen Wellen, bei denen allein ca. 200 Beschäftigte mitgearbeitet haben: Da die Passwörter Voraussetzung für die wiederaufgebaute E-Mail-Nutzungsmöglichkeit sowie alle weiteren Schritte für die Nutzerinnen und Nutzer waren, erfolgte die Ausgabe umgehend und zügig. Die erste Ausgabemöglichkeit wurde bereits in der Vorweihnachtswoche vom 16. bis 20. Dezember 2019 angeboten. Hierzu

8 Die Aufgaben des Computer Emergency Response Teams (CERT) in Hessen werden mittlerweile durch den Bereich Cybersecurity im Hessen3C (Cyber Competence Center) wahrgenommen. Das CERT-Hessen ist in diesem Bereich personell aufgegangen. Siehe https://innen.hessen.de/sicherheit/hessen3c/cert (23.11.2021).

9 https://www.dfn.de/ (23.11.2021).

Abb. 2: Warteschlangen im Campusbereich Sport/Kugelberg bei der Ausgabe der neuen Passwörter (Foto: JLU/Katrina Friese)

wurde eine große Halle auf dem Campusbereich Sport/Kugelberg mit ca. 30 Ausgabestationen getrennt nach Mitarbeiterinnen und Mitarbeitern und Studierenden ausgestattet, die mit zahlreichen Helferinnen und Helfern täglich in der Zeit von 8 bis 20 Uhr besetzt waren.

Zur Bewältigung des großen Andrangs der JLU-Mitglieder wurde ein Rundparcours zwischen Ein- und Ausgang definiert, der mit Absperrbändern und einer entsprechenden Beschilderung markiert war. Nachts wurden die Passwortbriefe auf dem Gelände eingeschlossen und von einem Sicherheitsdienst, der auch tagsüber vor Ort war, bewacht. Im Rahmen der ersten Welle konnten ca. 22 000 Passwortbriefe ausgegeben werden. Die zweite Ausgabemöglichkeit wurde analog zu dem bewährten Vorgehen der ersten Ausgabe in der ersten Vorlesungswoche nach der Weihnachtspause vom 13. bis 17. Januar 2020 angeboten. In der Zeit zwischen und nach den beiden Ausgabewellen konnten Passwortbriefe im JLU-Hauptgebäude zu definierten Zeitfenstern jeweils am Vormittag und Nachmittag abgeholt werden. JLU-Mitglieder, die aus nachvollziehbaren Gründen ihre Passwörter nicht persönlich abholen konnten, konnten über ein Web-Formular auf der JLU-Website einen Antrag auf Durchführung eines Video-Ident-Verfahrens stellen. Die Anträge wurden über ein Ticketsystem durch das Rechtsdezernat bearbeitet und bei Vorliegen der geforderten Voraussetzungen an ein Team aus JLU-Beschäftigten weitergereicht, das die entsprechenden Video-Ident-Verfahren mit Ende-zu-Ende-Verschlüsselung durchführte. Während des Verfahrens wurde, ebenso wie bei einer persönlichen Passwort-Abholung, das entsprechende Ausweisdokument geprüft und das darauf befindliche Ausweisfoto per Live-Videokonferenz abgeglichen. Nach einer positiven Identitätsprüfung wurde ein PDF-Dokument mit dem Zugangspasswort erstellt und innerhalb des Video-Chats übermittelt.

4 Krisenmanagement

Am Tag des Vorfalls, dem 8. Dezember 2019, fand eine erste Krisensitzung unter der Leitung des Präsidenten mit Beteiligung des Vizepräsidenten für Wissenschaftliche Infrastruktur (VPW), der Kanzlerin, des Leiters des Hochschulrechenzentrums, des IT-Sicherheitsbeauftragten, der JLU-Pressestelle und des Leiters des Präsidialbüros statt. Am Montag, dem 9. Dezember 2019, wurde ein Krisenstab

eingesetzt, der von da an das universitätsweite Krisenmanagement koordinierte.

Noch am 8. Dezember wurde das zuständige Fachministerium, das Hessische Ministerium für Wissenschaft und Kunst (HMWK), über den Vorfall informiert. Ab dem 9. Dezember fanden zunächst tägliche Telefonate zwischen dem VPW und dem HMWK statt, um über den Verlauf und die Auswirkungen zu berichten. Die zuständige Ministerin Angela Dorn besuchte am 14. Dezember das HRZ, um sich vor Ort ein Bild von der Lage zu machen. Die sofortige Einbindung und die komplikationslose Kommunikation mit dem HMWK erwies sich als ausgesprochen hilfreich, u. a. in rechtlicher Hinsicht bei der Verschiebung von Prüfungs- und Rückmeldefristen für die Studierenden. Die Befürchtung, dass sich für die Studierenden aus dem Cyber-Angriff Nachteile oder gar Rückschläge im Studium ergeben könnten, erwies sich glücklicherweise als unbegründet, da die Studierendendaten nicht betroffen waren.

4.1 Krisenkommunikation

Bereits früh war in der Kommunikation der Begriff *#JLUoffline* geprägt worden. Die Priorität des Krisenstabs war, auf unterschiedlichen Kanälen zu kommunizieren, um möglichst viele der Betroffenen sowie die Öffentlichkeit mit den jeweils notwendigen Informationen zu versorgen und drängende Fragen zu beantworten. Zudem mussten innerhalb der JLU Kommunikationswege etabliert werden, um sicherheitsrelevante Anweisungen insbesondere an die Beschäftigten zu geben. Dazu wurden zwei Krisenhotlines eingesetzt, die von JLU-Beschäftigten besetzt waren, die sich freiwillig gemeldet hatten. Die *#JLUoffline*-Hotline wurde schon am 9. Dezember eingerichtet und eine zweite Hotline für technische Anfragen am 14. Dezember 2019 etabliert, um gezielt bei der Durchführung der Virenscans via USB-Sticks Unterstützung zu leisten.

Eine Behelfshomepage war am 9. Dezember aufgebaut worden, die Adresse www.uni-giessen.de wurde auf diese Seite umgeleitet. Auch wenn innerhalb des JLU-Netzes selbstverständlich kein Internetzugang möglich war, musste der Krisenstab doch davon ausgehen, dass die Mehrzahl der JLU-Mitglieder und -Angehörigen sich zunächst online über anderweitige Internetzugänge (Heimnetz, mobile Netze) über den IT-Vorfall informieren würden. Die Homepage stellte Informationen auf Deutsch und Englisch bereit und verfügte auch über eine stetig aktualisierte FAQ-Liste.

Parallel zur Webseite stellte die Pressestelle der JLU Informationen auf Social Media (Facebook, Twitter, Instagram) zur Verfügung. Über diese Plattformen teilte sie

Abb. 3: Das Telefonsystem war nicht betroffen, die Hotline wurde stark in Anspruch genommen (Foto: JLU/Katrina Friese)

auch relevante Posts von JLU-Einrichtungen und -Angehörigen mit eigenen Präsenzen auf Social Media, um diesen mehr Reichweite zu verschaffen (so z. B. Hinweise von Lehrenden zu ihren Veranstaltungen oder Informationen der Universitätsbibliothek zum Notbetrieb). Auf YouTube wurden in der Akutphase der Krisenbewältigung nach dem Cyberangriff am 13. und am 20. Dezember Videos veröffentlicht,[10] in denen der JLU-Präsident persönlich die aktuelle Lage einordnete.

Für die Universitätsleitung und kritische zentrale Anlaufstellen wurden bereits am 9. Dezember Ersatz-E-Mail-Adressen eingerichtet, sodass diese nahezu durchgehend erreichbar waren. Die E-Mail-Adressen, welche durch die Verwaltung von einzelnen internetfähigen Geräten aus ohne Verbindung zum JLU-Netz betreut wurden, kanalisierten Anfragen und gewährleisteten schnelle Rückmeldungen. Die eingehenden Anfragen lieferten für den Krisenstab wertvolle Hinweise auf akute Problemlagen und zu Bereichen, die besonderer Aufmerksamkeit, weiterer gezielter Maßnahmen oder Hilfestellungen bedurften. Sobald die E-Mail-Kommunikation wiederaufgebaut war und schrittweise mehr und mehr Einrichtungen der JLU wieder Internetzugang erhielten (insbesondere ab Januar 2020), wurde verstärkt auf JLU-interne Rundmails gesetzt, um relevante Informationen zu kommunizieren und alle Betroffenen auf dem Laufenden zu halten.

Ein weiterer zentralerer Pfeiler der universitären Informationsvermittlung während der Krisensituation waren zielgruppenspezifische Face-to-Face-Formate. Diese eigneten sich besonders gut zur Klärung von drängenden Fragen und auch zur Erläuterung komplexerer tech-

10 Die beiden Videos sind noch online verfügbar: https://www.youtube.com/watch?v=uKU_ph1M3u8, 13.12.2019, und https://www.youtube.com/watch?v=FSe-q_fqjy0, 20.12.2019 (07.12.2021).

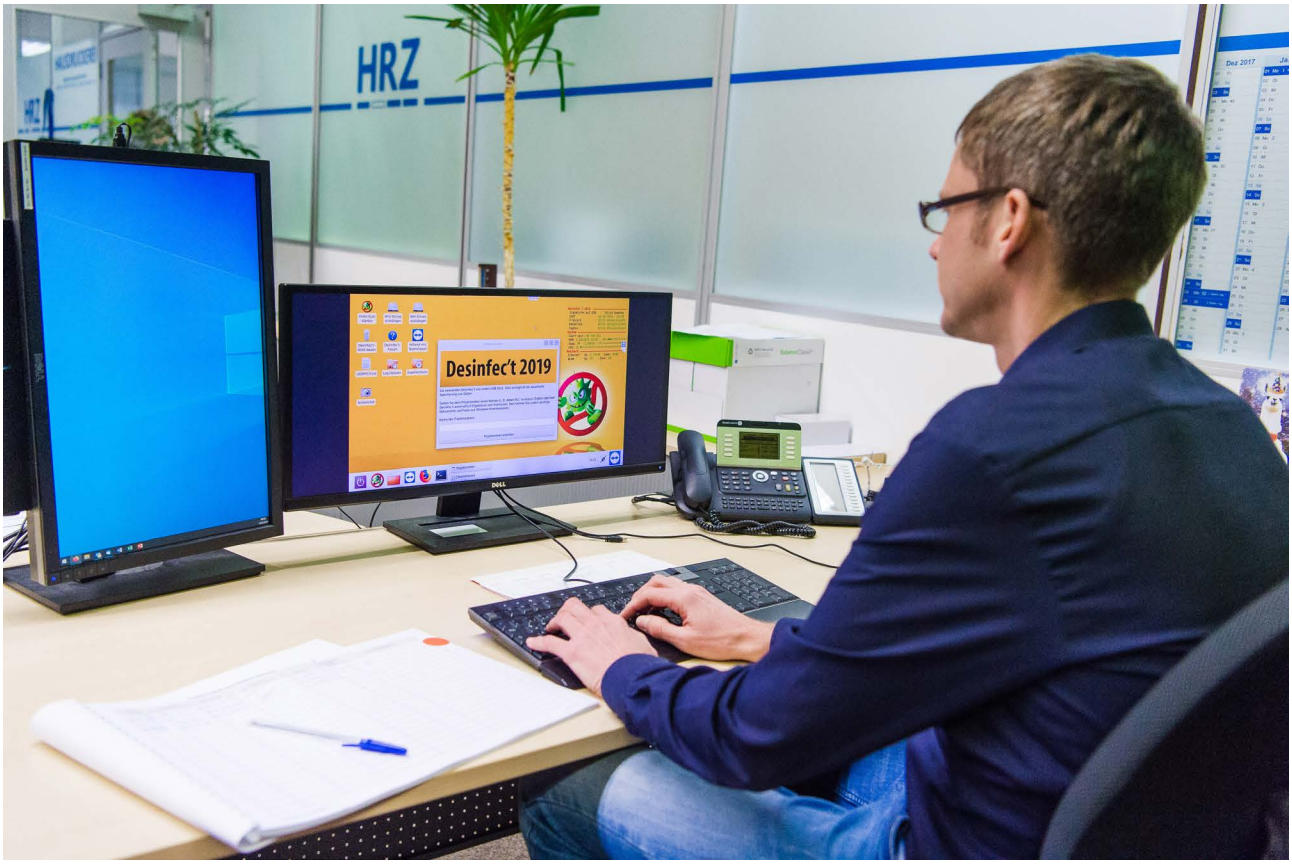


Abb. 4: Koordinierung der Viren-Scannung im HRZ (Foto: JLU/Katrina Friese)

nischer Vorgänge. Bei der Notstandskoordination und der Lagebesprechung in der Verwaltung handelte es sich um verpflichtende Dienstveranstaltungen für die Leitungsebenen der JLU, jeweils in der Gesamtuniversität und in der Präsidialverwaltung, welche als Multiplikatoren in die Universität wirkten. Auch die Zusammenkunft der Lehrenden war eine Dienstversammlung. An der Notstandskoordination nahmen die Dekaninnen und Dekane der elf Fachbereiche, die Leitungen der zentralen Einrichtungen (wie Universitätsbibliothek, Tierhaltung, Zentren), die Leitungen der Prüfungsämter, Vertreterinnen und Vertreter des CIO-Nutzerbeirats[11] und des Personalrats, die Gleichstellungsbeauftragte, der Tierschutzbeauftragte sowie der Datenschutzbeauftragte teil.

Bis Ende Februar 2020 fanden sechs Sitzungen unter der Leitung des Präsidenten statt. In diesen Sitzungen informierte der Krisenstab zur Lage und kommunizierte verbindliche Anweisungen mit der Maßgabe, dass die Führungskräfte diese in ihren jeweiligen Bereichen bekannt machen und durchsetzen. Wie genau die Einrichtungsleitungen die Informationen jeweils in die Fläche kommunizierten, war unterschiedlich organisiert – jeweils abgestimmt auf die Einrichtungen und auf den Vertraulichkeitsgrad der Informationen. Unter anderem wurden Telefonlisten, Social Media, Aushänge und fachbereichs- oder institutsinterne Sitzungen genutzt. Selbstverständlich war die Notstandskoordination auch ein Forum für die Einrichtungen der JLU, ihre Anliegen und Fragen direkt an das Präsidium und den Krisenstab zu richten. Die Dezernatsleitungen aus der Präsidialverwaltung waren in jeder Sitzung anwesend, um Hinweise zu Krisenmaßnahmen in ihren jeweiligen Ressorts zu geben (z. B. zu Übergangslösungen beim Stellen von Urlaubsanträgen, SAP-Kontoauszügen, Gebäudeleittechnik etc.).

4.2 Interne und externe Kommunikation

Da die JLU zunächst von allen digitalen Möglichkeiten der internen Kommunikation (Rundmails, Homepage) abge-

11 Das Central Information Office der Justus-Liebig-Universität ist ein internes universitäres Beratungsgremium mit verschiedenen Untergremien, die das Präsidium in Fragen des Informations- und Kommunikationsmanagement berät. https://www.uni-giessen.de/org/cio (07.12.2021).

Abb. 5: Renaissance der Zettel: Ausleihverbuchung in der UB (Foto: JLU/Katrina Friese)

schnitten war, standen in den ersten Stunden der Krise nur die Social-Media-Kanäle der JLU (Facebook, Twitter, Instagram) als Kommunikationskanäle zur Verfügung. Eine Trennung von interner und externer Kommunikation war insbesondere in der Anfangsphase nicht möglich. Über Twitter und Instagram wurde am Abend des 8. Dezember 2019 erstmals über den „schwerwiegenden IT-Sicherheitsvorfall" informiert (bereits unter Verwendung des Hashtags *#JLUoffline*). Eine ausführlichere erste Pressemitteilung wurde am Montag, dem 9. Dezember 2019, veröffentlicht. Stück für Stück wurden in den folgenden Tagen weitere Kommunikationskanäle zur Verfügung gestellt. Sämtliche Behörden, Drittmittelgeber etc. wurden mit Schreiben vom 10. Dezember darüber informiert, dass interimsweise ein zentrales E-Mail-Postfach (Poststelle@giessen.university) eingerichtet worden sei. Am selben Tag fand eine große JLU-interne Informationsveranstaltung statt. Gesicherte Informationen wurden fortlaufend in einem FAQ-Bereich auf der Notfall-Homepage bereitgestellt. Durch die konsequente Pflege und Erweiterung des FAQ-Bereichs auf der Homepage konnte wirksam verhindert werden, dass sich falsche Informationen verbreiteten. Trotz dieser zusätzlichen Informationskanäle blieb es insbesondere bis zur Weihnachtspause bei einer sehr intensiven Nutzung der Social-Media-Kanäle der JLU. Die Beantwortung der zahlreichen Anfragen (Direktnachrichten und Kommentare) war zeitaufwändig. Zur Vermeidung von sogenannten Shitstorms waren sehr schnelle und inhaltlich konsistente Reaktionen von größter Bedeutung. Das Feedback der Nutzerinnen und Nutzer war – von wenigen Ausnahmen abgesehen – fast durchgehend von Verständnis geprägt. Shitstorms blieben aus. Zu den Erfordernissen der internen Kommunikation kam das enorme Interesse der überregionalen und sogar internationalen Medien hinzu, deren Anfragen rasch und umfassend beantwortet werden mussten. Noch am Abend des 8. Dezember 2019 wurden erste Meldungen im Hessischen Rundfunk gesendet; bereits im Dezember berichtete unter anderem auch die BBC über den Vorfall. Bei einer gut besuchten Pressekonferenz am 10. Januar 2020 wurden die Medien nach der Weihnachtspause auf den aktuellen Stand gesetzt.

5 Krisenmanagement im Bibliothekssystem

Die Auswirkungen der Cyber-Attacke vom 8. Dezember 2019 und die eingeleiteten Maßnahmen seien im Folgenden am Beispiel des universitären Bibliothekssystems geschildert. Das Bibliothekssystem der Justus-Liebig-Universität mit einem Gesamtbestand von ca. 3,7 Millionen Bänden und 111 Stellen (VZÄ) ist funktional einschichtig organisiert und bestand zum Zeitpunkt der Cyber-Attacke aus der Universitätsbibliothek, vier Zweigbibliotheken, die am elektronischen Ausleihsystem teilnehmen, sowie sieben dezentralen Fachbibliotheken ohne Ausleihverbuchung. Als lokales Bibliothekssystem ist im Rahmen von hebis LBS4 von OCLC im Einsatz, das vom Hochschulrechenzentrum betrieben wird.

Einen umfassenden Notfallplan für einen derart umfassenden IT-Ausfall gab es im Bibliothekssystem nicht, die bisherigen Erfahrungen erstreckten sich lediglich auf einen temporären und/oder lokal begrenzten Ausfall einzelner IT-basierter Dienste. In enger Abstimmung mit dem Krisenstab der Universität und dem HRZ wurde daher ad hoc ein Maßnahmenkatalog entwickelt, bei dem die möglichst rasche Wiedereinführung der Benutzungsdienste (insbesondere die Ausleihe und der Zugang zum digitalen Angebot) im Vordergrund stand. Parallel mussten die Voraussetzungen für einen funktionierenden internen Betrieb geschaffen werden. Im Einzelnen gehörten dazu vor allem die im Folgenden erläuterten Maßnahmen.

Bereits wenige Tage nach dem Cyber-Angriff konnte von der Universitätsbibliothek ein Ausleihverfahren mittels konventioneller Ausleihzettel, die von Hand auszufüllen waren, angeboten werden. Die Ausleihzettel stammten aus altem Bestand der UB und der Fachbibliotheken, der nicht entsorgt worden war, um ggf. im Notfall zur Verfügung zu stehen. Der Online-Katalog JUSTfind war zwar noch erreichbar, da er in der hebis-Verbundzentrale gehostet wird, aber die Signaturanzeige war durch die Trennung des LBS4-Servers vom Internet nicht mehr möglich. Signaturen mussten daher im Karlsruher Virtuellen Katalog (KVK) recherchiert werden. Dies war für einige Studierende nicht ganz leicht, das Bibliotheksper-

Abb. 6: Computer bitte nicht einschalten (Foto: JLU/Katrina Friese)

sonal konnte aber weiterhelfen. Die Ausleihe per Leihschein wurde weitergeführt, bis die elektronische Ausleihverbuchung wieder funktionierte. Für die Bücher, die per Leihschein entliehen wurden, wurde das Rückgabedatum auf einem beigelegten Fristzettel notiert. Die Bücher mussten in der Bibliothek zurückgegeben werden, in der sie ausgeliehen wurden. Mahngebühren wurden in großzügigem Umfang erlassen, da eine nachträgliche Überführung der konventionellen Ausleihen in das elektronische Verbuchungssystem zu aufwändig gewesen wäre, zudem war nicht absehbar, wie lange die konventionelle Ausliehe würde aufrechterhalten werden müssen. Bis zum Beginn der Weihnachtspause erfolgten täglich gut 500 Ausleihen auf diesem Weg.

Abb. 7: Screenshot Twitter

Die Sicherheitsprüfungen der ca. 200 windowsbasierten Endgeräte, die pro Gerät zwei separate, mehrstündige Prüfroutinen erforderten, konnten Anfang Januar 2020 abgeschlossen werden. Unter diese Geräte fielen neben den PCs der Mitarbeiterinnen und Mitarbeiter auch die in Selbstverbuchern, Rücknahmeautomaten und Kassenautomaten eingebauten Systeme. Um die Prüfroutinen möglichst stark parallelisieren zu können, wurden die vom HRZ zur Verfügung gestellten USB-Sticks zunächst mehrfach geklont. Lediglich acht Geräte waren befallen und wurden ausrangiert bzw. neu aufgesetzt. Alle anderen Geräte wurden als überprüft gekennzeichnet und konnten zunächst offline benutzt werden, d. h. bei gezogenem Netzwerkkabel. Programme zur Textverarbeitung und Tabellenkalkulation wie Microsoft Word und Excel konnten somit lokal genutzt werden. In jeder Abteilung, Zweig- und Fachbibliothek wurde ein lokaler USB-Drucker eingerichtet, sofern der Bedarf bestand. Anschließend wurden die PCs der Mitarbeiterinnen und Mitarbeiter für die Anbindung ans Netz vorbereitet. Dafür mussten jeweils neue lokale Nutzer mit dem Nachnamen und neuem Passwort eingerichtet, ein neuer Virenscanner installiert, aktuelle Windows-Updates eingespielt sowie verschiedene Sicherheitseinstellungen in Outlook vorgenommen werden. Nur wenn alle Endgeräte eines Netzwerkbereichs (des so genannten Subnetzes) geprüft waren, erfolgte zunächst eine Freischaltung für das JLU-interne Intranet. Sofern das HRZ in dem Subnetz in den folgenden Tagen keine Auffälligkeiten feststellen konnte, wurde auch der Internetzugriff wiederhergestellt. In einigen Zweig- und Fachbibliotheken, die sich die Netzwerkbereiche oft mit den Fachbereichen teilen, wurde zusätzlich auf geprüfte Laptops zurückgegriffen, da das WLAN eduroam bereits wieder erreichbar war. Auf diese Weise konnte die elektronische Ausleihverbuchung auch in den Zweigbibliotheken ermöglicht werden, obwohl noch nicht alle Geräte in den Subnetzen geprüft waren. Diese Arbeiten im Bibliothekssystem wurden zügig umgesetzt und waren im Januar im Wesentlichen abgeschlossen. Damit gehörten die Bibliotheken zu den sog. Netzsegmentpiloten.

Anfang Januar hatten auch die LBS-Server die vom HRZ vorgegebenen Sicherheitsprüfungen positiv überstanden. Sie wurden am 8. Januar 2020 wieder in Betrieb genommen.

Die elektronische Ausleihe war ab dem 13. Januar 2020 zunächst nur im Subnetzbereich der UB wieder möglich, auch die Selbstverbucher und der Rückgabeautomat in der UB konnten ab diesem Zeitpunkt wieder genutzt werden. Die seit der Cyber-Attacke zurückgegebenen Bücher wurden sukzessive zurückgebucht und die Ausleihkonten der Nutzerinnen und Nutzer nach und nach bereinigt. Um Zugriff auf das Konto zu erhalten, wurde allerdings ein neues Passwort benötigt, welches mit Hilfe der Uni-E-Mail-Adresse gesetzt werden konnte. Nutzerinnen und Nutzer, die noch keinen Zugriff auf ihre E-Mail-Konten hatten, konnten sich an der Ausleihtheke in der UB ein neues Passwort setzen lassen. Alle vor der Cyber-Attacke elektronisch entliehenen Medien, deren Leihfrist abgelaufen war, mussten bis spätestens Mittwoch, 26. Februar 2020, zurückgegeben werden. Ab diesem Zeitpunkt wurden zu spät zurückgegebene Medien wieder regulär gemahnt. Das

Ende der Rückgabefrist konnte dem persönlichen Ausleihkonto entnommen werden.

Für die Mitarbeiterinnen und Mitarbeiter des Bibliothekssystems wurden die neuen LBS4-Passwörter seit Anfang Januar 2020 sukzessive verteilt. Mit der Einarbeitung der ACQ-Rechnungen 2019 konnte in der UB in der zweiten Januarwoche 2020 begonnen werden.

Durch die Freigabe der LBS-Server am 8. Januar 2020 waren diese auch für die drei betreuten Mandanten (Hochschul- und Landesbibliothek Fulda, Bibliothek der Technischen Hochschule Mittelhessen, Bibliothek des Priesterseminars Fulda) wieder erreichbar. Aufgrund der Trennung der LBS-Server vom Internet waren die Mandanten im LBS von den Auswirkungen der Cyber-Attacke ebenso betroffen und mussten für ihre Arbeitsabläufe in Ausleihe und Erwerbung auf Interimslösungen zurückgreifen.

Da zunächst kein Zugriff auf das elektronische Angebot bestand, wurde das Angebot der UB Marburg, den Studierenden der JLU einen Gast-Account einzurichten, mit dem vor Ort das WLAN sowie die elektronischen Medien der UB Marburg genutzt werden konnten, seitens der Gießener Studierenden dankbar angenommen.

Abb. 8: Good News auf Twitter

Der Zugriff auf E-Medien im Bibliothekssystem (E-Books, elektronische Zeitschriften und Datenbanken) war seit dem 13. Januar 2020 wieder möglich, da der EZ-Proxy-Server nach den entsprechenden Serverprüfroutinen wieder zugänglich war. Mit der individuellen Kennung und dem neuen Passwort konnten so die im Discovery-System JUSTfind nachgewiesenen E-Medien aus den freigegebenen Subnetzen oder über anderweitige Internetzugänge (Heimnetz, mobile Netze) aufgerufen werden. Eine VPN-Verbindung wurde nicht benötigt. Der Zugriff auf das Hochschulschriftenrepositorium (Gießener Elektronische Bibliothek, GEB) und die digitalen Sammlungen (DIGISAM) war ab Ende Januar wieder möglich.

Ab Anfang Januar waren auch viele Basisdienste wieder zugänglich, u. a. die Homepage der JLU, Stud-IP, JLUbox, FlexNow (intern) und ILIAS. Auch die Server für die Gleitzeiterfassung konnten wieder in Betrieb gehen (bis dahin mussten die Arbeitszeiten im Bibliothekssystem händisch notiert werden). Die öffentlichen Rechner in der Universitätsbibliothek sollten aus Sicherheitsgründen erst im Verlauf des Sommersemesters wieder zur Verfügung stehen, da die dafür benötigte Server-Infrastruktur neu aufgebaut werden musste. Durch die Nutzungseinschränkungen, die im Zuge der COVID-19-Pandemie erforderlich wurden, wurden diese Arbeiten jedoch verschoben.

6 Schlussfolgerungen aus dem IT-Sicherheitsvorfall

6.1 Anpassung der IT-Sicherheitsmaßnahmen

Die JLU hatte bereits vor dem Cyberangriff einen umfassenden Prozess zur Weiterentwicklung ihrer IT-Gesamtstrategie angestoßen. Aus dem IT-Sicherheitsvorfall konnten zusätzliche und teils weitreichende Schlussfolgerungen zur Anpassung der IT-Sicherheitsmaßnahmen gezogen werden. So wurde die Chance genutzt, die Windows-Serverinfrastrukturen beim Wiederaufbau unter aktuellsten Sicherheitsgesichtspunkten neu zu konzipieren und auch im Netzwerk strukturelle Änderungen zur Verbesserung der Sicherheit vorzunehmen. Weitere Maßnahmen betreffen u. a. die Verbesserung des Schutzes vor E-Mails, mit denen Schadsoftware verbreitet werden soll, und den verbesserten Schutz von Endgeräten. Durch den Sicherheitsvorfall trafen die Maßnahmen bei den Mitgliedern und Angehörigen der JLU auf großes Verständnis, wodurch der Einführungsprozess beschleunigt und die Akzeptanz der getroffenen Vorkehrungen erhöht werden konnten.

6.2 Entwicklung einer neuen IT-Governance- und Sicherheitsarchitektur

Im Vergleich zu späteren Cyber-Attacken auf öffentliche Einrichtungen wie z. B. die vom September 2020 auf das Uniklinikum Düsseldorf, bei der sogar ein Todesopfer zu beklagen war,[12] ist der nachhaltige Schaden für die JLU verhältnismäßig gering gewesen. In einer im Jahr 2020 universitätsintern durchgeführten Erhebung wurden systematisch alle zentral und dezentral verbuchten Kosten, die direkt der Schadensbewältigung zuzuordnen waren, ermittelt. Im Ergebnis belaufen sich die zur Schadensbewältigung der Cyber-Attacke zuzurechnenden Kosten

12 *Handesblatt*, 18.09.2020.

hochschulweit auf ca. 1,7 Millionen Euro.[13] Der Angriff hat aber sehr deutlich und nachhaltig gezeigt, in welchem Ausmaß das Leben einer Universität in allen Bereichen digital geprägt ist und vom einwandfreien Funktionieren entsprechender Dienste und Anwendungen abhängt. Entsprechend groß waren anfangs die Befürchtungen: Studierende fürchteten den Verlust ihrer elektronisch dokumentierten Studien- und Prüfungsleistungen und Wissenschaftlerinnen bzw. Wissenschaftler den Verlust von Daten aus Untersuchungen und Forschungsreihen und den Verlust der Anschluss- und Wettbewerbsfähigkeit. Die Befürchtungen haben sich nicht bestätigt, und in gewissem Sinn ist die JLU sogar gestärkt aus der Krise hervorgegangen, da die Sensibilität im Umgang mit den digitalen Diensten innerhalb und außerhalb der Universität stark zugenommen hat.

Die Erfahrungen der JLU aus dem Cyber-Angriff wurden intensiv mit dem Hessischen Ministerium für Wissenschaft und Kunst (HMWK) diskutiert, damit auch alle anderen Landeseinrichtungen davon profitieren können. Die Erfahrungen aus #JLUoffline flossen zudem in die Anpassung der Krisenmanagementsysteme der JLU mit Blick auf IT-Störfälle und Notfallpläne ein. Darüber hinaus wurde im Rahmen eines vom Ministerium für Wissenschaft und Kunst bereitgestellten Förderbudgets zur Stärkung der Strategiefähigkeit hessischer Hochschulen die Umsetzung einer nachhaltigen und an den Bedarfen von Forschung, Lehre und Verwaltung ausgerichteten IT-Governance- und -Sicherheitsstrategie schon bald nach der Cyber-Attacke in Angriff genommen. Besondere Berücksichtigung fanden dabei die Ergebnisse und Empfehlungen aus der im Januar 2020 erfolgten Evaluation des Hochschulrechenzentrums, welche durch das Präsidium der JLU bereits Anfang 2019 initiiert worden war. In Zusammenarbeit mit externer Beratung durch die KPMG AG (IT-Governance) und xivconsult GmbH (IT-Sicherheit) wurde der Status quo evaluiert, um auf Basis dieser Ergebnisse eine zukunftsfähige IT-Governance- und -Sicherheitsstrategie mit expliziten Handlungsempfehlungen zu entwickeln. Die Umsetzung der Strategie, die 2020 bereits begonnen hat, soll sich ausdrücklich auf die gesamte interne Prozesslandschaft auswirken und hat Einfluss auf alle universitären Bereiche, vom Hochschulrechenzentrumsbetrieb über die Hochschulverwaltung bis hin zu den universitären Fachbereichen und Zentren.

Der Cyber-Angriff hat die Entwicklung der bereits im Aufbau befindlichen, neuen IT-Governance-Strategie intensiviert und beschleunigt. Basierend auf Design-Prinzipien, die im Rahmen von abteilungs- und fachbereichsübergreifenden Workshops definiert wurden, wird sie sukzessive umgesetzt. Bezogen auf die Organisation gehört hierzu nicht nur die neue Ablauforganisation, sondern auch eine veränderte Steuerung des dezentralen IT-Supports.

Im Bereich der IT-Sicherheit wurden mehrere Ziele und die flankierenden Governance-Strukturen formuliert, die den künftigen Handlungsrahmen und die strategische Leitlinie der JLU im Bereich IT-Sicherheit bilden werden. Prioritär ist dabei der Aufbau einer Organisationsstruktur, die zur Förderung und Durchsetzung des Informationssicherheitsprozesses erforderlich ist. Dazu wird insbesondere die Position einer/eines Informationssicherheitsbeauftragten (ISB; W2-Professur) als unabhängige Stelle beim Präsidium geschaffen. Hinzu kommt ein/e Informationssicherheitsmanager/in (ISMS Manager/in) zur Unterstützung der/des ISB im Sicherheitsprozess. Die/der ISB wird nicht einer IT-Abteilung zugeordnet sein, um eine Funktionstrennung und Unabhängigkeit zu erzielen. Die/der ISB soll Sicherheitsrichtlinien für die gesamte JLU erstellen, in denen strikte Vorgaben für die Informationssicherheit geregelt werden, und für deren Durchsetzung verantwortlich sein. Mit Hilfe eines Risikomanagements sollen risikobasierte Entscheidungen für die Sicherheit getroffen und nachhaltig dokumentiert werden. Durch die Neuorganisation fungiert die/der ISB künftig zudem als zentrale/r Ansprechpartner/in für Sicherheitsfragen. Für operative Sicherheitsaufgaben wurden im HRZ zusätzliche Stellen geschaffen. Diese Personen sollen auch in operative Prozesse der anderen Abteilungen eingebunden sein, um dort aktuelle Gefährdungen zu identifizieren, umzusetzende Sicherheitsanforderungen zu bestimmen und sicherheitsrelevante Entscheidungen im Tagesgeschäft mit beeinflussen zu können.

Für die Weiterentwicklung und Etablierung eines umfassenden Sicherheitskonzepts[14] soll zudem eine Strukturanalyse durchgeführt und der Schutzbedarf für die Geschäftsprozesse, die dabei zu verarbeitenden Infor-

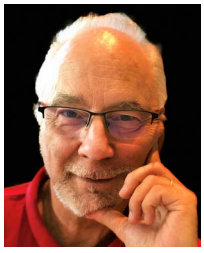
13 Davon entfallen 1,1 Millionen Euro auf das HRZ und ca. 600 000 Euro auf die übrigen Einrichtungen. Nach Kostenarten differenziert sind ca. 900 000 Euro Personalkosten und 700 000 Euro Sachkosten angefallen (Mitteilung zur Sitzung des Senats der Justus-Liebig-Universität Gießen vom 7. Juli 2021). Die indirekten Kosten – die Verzögerungen etwa in laufenden, insbesondere empirischen und experimentellen Forschungsprojekten – lassen sich quantitativ nicht ermitteln.

14 Gemäß ISO 27001 auf der Basis *IT-Grundschutz* des Bundesamts für Sicherheit in der Informationstechnik (BSI).
Die IT-Sicherheitsrichtlinie der JLU aus 2014 (gemäß der Informationssicherheitsrichtlinie für die Hessische Landesverwaltung vom Januar 2010) befand sich zum Zeitpunkt des Cyber-Angriffs bereits in Überarbeitung mit dem Ziel einer Anpassung an den BSI-Standard. Zum 1. Dezember 2017 war ein Abteilungsleiter im HRZ zum IT-Sicherheitsbeauftragten für die JLU bestellt worden.

mationen und die eingesetzte IT-Infrastruktur festgelegt werden. Geeignete Sicherheitsanforderungen und darüber umzusetzende Maßnahmen sollen identifiziert werden. Eine nachgelagerte Risikoanalyse für Zielobjekte mit hohem oder sehr hohem Schutzbedarf entscheidet über das Ausmaß der noch umzusetzenden Maßnahmen. Diese werden entsprechend priorisiert und deren Umsetzung geplant. Der Aufbau eines Notfallmanagements inklusive der Erstellung einer Leitlinie zum Notfallmanagement, eines Rahmenkonzeptes, eines Notfallvorsorgeplans sowie eines Notfallhandbuches soll noch weiter vorangetrieben und forciert werden.

Die Cyber-Attacke vom Dezember 2019 hat in vielerlei Hinsicht gezeigt, dass alle Mitarbeitenden in den Sicherheitsprozess und dessen Hintergründe einbezogen werden müssen. Zur Steigerung der Sensibilisierung der Nutzerinnen und Nutzer sind verschiedene Maßnahmen geplant, um die Sicherheitsmaßnahmen nutzungsgerecht für den Arbeitsalltag zu erklären und deren Anwendung zu stärken. Angesichts des tendenziell weiter steigenden Bedrohungspotentials und immer ausgefeilterer Angriffsmethoden steht auch die JLU vor der dauerhaften Aufgabe, ein ausreichendes Sicherheitsniveau mit angemessenen Maßnahmen zu gewährleisten, ohne dabei die Arbeitsfähigkeit und Effektivität in Verwaltung, Forschung und Lehre zu sehr einzuschränken. In dieser Hinsicht ist es unbedingt erforderlich, dass alle Mitarbeitenden Verantwortung tragen, die Sicherheit an der Universität aktiv mitzugestalten.

Autoreninformationen



Dr. Michael Kost
Direktor des Hochschulrechenzentrums
Justus-Liebig-Universität Gießen
Ludwigstraße 23
35390 Gießen
michael.kost@hrz.uni-giessen.de

Bastian Loibl, M.A.
Stabsabteilung für wissenschaftliche Infrastruktur
Justus-Liebig-Universität Gießen
Ludwigstraße 23
35390 Gießen
bastian.u.loibl@admin.uni-giessen.de

Dr. Peter Reuter
Direktor der Universitätsbibliothek
Justus-Liebig-Universität Gießen
Ludwigstraße 23
35390 Gießen
peter.reuter@bibsys.uni-giessen.de
orcid.org/0000-0001-5039-2020

Dr. Matthias Stenke
Abteilungsleiter Basisdienste und Service im Hochschulrechenzentrum
Justus-Liebig-Universität Gießen
Ludwigstraße 23
35390 Gießen
itsicherheit@uni-giessen.de