HIS-HE:Forum
4|2025

Mathias Stein | Maren Lübcke | Harald Gilch (Hrsg.)

Krisenmanagement nach Cyber-Angriffen an Hochschulen – Tagungsband 2024

HIS-Institut für Hochschulentwicklung e. V.
Goseriede 13a | D-30159 Hannover | www.his-he.de

Dr. Mathias Stein
Geschäftsbereich Hochschulmanagement
Tel.: +49 511 169929-27
E-Mail: stein@his-he.de

Dr. Maren Lübcke
Geschäftsbereich Hochschulmanagement
Tel.: +49 511 169929-19
E-Mail: luebcke@his-he.de

Dr. Harald Gilch
Geschäftsbereich Hochschulmanagement
Tel.: +49 511 169929-32
E-Mail: gilch@his-he.de

5. November 2025

ISBN 978-3-948388-48-5

Vorwort

Die Auseinandersetzung mit Cyber-Angriffen auf Hochschulen fiel uns zunächst schwer – dann zunehmend leicht. Schwer fiel sie uns, weil wir anfangs davon ausgingen, es handele sich vorrangig um ein technisches Thema, bei dem es um Firewalls, Serverkonfigurationen und Netzwerksegmentierungen, Verschlüsselungsstandards oder die technische Wiederherstellung von IT-Systemen nach einem Angriff geht. In solchen Fragen, so dachten wir, verfügen andere über die eigentliche Expertise – Fachleute für IT-Sicherheit, Administrator:innen, Spezialist:innen für IT-Infrastrukturen.

Leichter wurde es erst, als wir erkannten, dass Cyber-Sicherheit weit über Technik hinausgeht. Sie betrifft Organisation und Kommunikation ebenso wie Strukturen und Prozesse der Krisenbewältigung und Entscheidungsfindung. Im Kern steht nicht die Frage, welches System geschützt wird, sondern wie eine Hochschule als Organisation auf einen Angriff vorbereitet ist, reagiert, sich neu sortiert – und dabei ihre Handlungsfähigkeit bewahrt.

Seit den ersten überregional bekannt gewordenen Cyber-Angriffen auf deutsche Hochschulen im Jahr 2019 ist die Bedrohungslage kontinuierlich gestiegen und das Thema ist heute allgegenwärtig. Die heterogene, teilweise über Jahrzehnte gewachsene IT-Struktur an Hochschulen begünstigt Angriffe. Und zugleich lässt sich gar nicht so genau sagen, welche sicherheitsrelevanten Vorfälle eigentlich als Cyber-Angriff gewertet werden und wie viele Angriffe es tatsächlich auf Hochschulen bereits gegeben hat. Doch auch wenn die Frage nach der Anzahl von Cyber-Angriffen derzeit nicht pauschal beantwortet werden kann, stellt sich eine weitere wichtige Frage: Was passiert, wenn es passiert ist? Welche Folgen kann ein erfolgreicher Cyber-Angriff auf eine Hochschule haben und vor allem: Wie können sich Hochschulen und Hochschulleitungen auf ein solches Krisenszenario vorbereiten?

Mit diesen Fragen haben wir uns im Jahr 2023 befasst und als Ergebnis unserer Studie eine Handreichung zum „Krisenmanagement nach Cyber-Angriffen“ veröffentlicht wurde. Die Unterstützung für das Vorhaben war bemerkenswert. Wir fanden insbesondere Rückhalt beim Arbeitskreis Digitale Transformation der Vereinigung der Kanzlerinnen und Kanzler der Universitäten Deutschlands; zahlreiche betroffene Hochschulen standen für Interviews zur Verfügung und gaben zahlreiche Hinweise und Tipps für Handlungsempfehlungen. Das große Interesse an der Thematik zeigte sich auch bei der Organisation des Forums „Krisenmanagement nach Cyber-Angriffen an Hochschulen“ im Sommer 2024: Zahlreiche Expertinnen und Experten erklärten sich sofort bereit, einen Beitrag zu leisten, sodass wir ein dichtes Programm zusammenstellen konnten.

Vor diesem Hintergrund freuen wir uns sehr, dass die Beiträge unserer Tagung nun in dieser Publikation vorliegen. Darin skizzieren Eva Wolfangel und René Rehme ihre Erfahrungen als ethische Hacker:innen, die zwischen Weihnachten und Neujahr 2022/2023 eine Reihe von Hochschulen in Deutschland gehackt haben. Der Beitrag zeigt, wie Hacker:innen vorgehen, um die IT-Sicherheit von Hochschulen zu testen und zu durchbrechen. Harald Gilch, Maren Lübcke und Mathias Stein geben in ihrem Beitrag einen Überblick über bisherige Cyber-Angriffe auf Hochschulen, Phasen des Krisenmanagements nach einem Angriffsfall und zeigen Aspekte auf, mit denen sich Hochschulen vor dem Ernstfall befassen sollten. Den konkreten Fall eines Cyber-Angriffs auf eine Hochschule und die Folgen stellen Prof. Dr. Josef von Helden, Präsident der Hochschule Hannover (HsH), und Isabel Kassel vor. Die HsH wurde Ende November 2023 gehackt. Einen

Erfahrungsbericht liefert auch Lisa Dittrich, die über den Cyber-Angriff auf die Justus-Liebig-Universität Gießen berichtet. Als Pressesprecherin der Universität geht es in ihrem Beitrag vor allem um die Krisenkommunikation im Ernstfall.

Christian S. Fötinger gibt auf einer übergreifenden Betrachtungsebene einen Überblick über Maßnahmen und Initiativen im Kontext von Cyber-Sicherheit im Freistaat Bayern. Bayern gehört zu den Bundesländern, die bereits frühzeitig Projekte und Initiativen zur Stärkung der Cyber-Sicherheit an Hochschulen gefördert haben. Einen weiteren Überblick geben Malte Dreyer und Jan K. Köcher in ihren Beiträgen. Malte Dreyer widmet sich den zentralen Schritten zur Vorbereitung auf mögliche Cyber-Angriffe. Abschließend geht Dr. Jan K. Köcher auf die rechtlichen Rahmenbedingungen vor und nach Cyber-Angriffen ein.

Den Autor:innen danken wir für die Ausarbeitung ihrer Vorträge sehr herzlich. Den Leser:innen wünschen wir eine inspirierende Lektüre.

Hannover im Oktober 2025

Mathias Stein, Maren Lübcke und Harald Gilch

Inhaltsverzeichnis

Abbildungsverzeichnis

Eva Wolfangel, René Rehme: Noten und Atteste frei zugänglich: Wir haben die IT-Sicherheit von Unis und Hochschulen getestet

Hinweis: Grundlage für die Beiträge von Eva Wolfangel und René Rehme auf dem Forum Cyber-Security für Hochschulen war eine gemeinsame Veröffentlichung im RiffReporter.de[1] und ein Artikel in der ZEIT. Da die Ergebnisse und Anmerkungen immer noch aktuell sind, drucken wir den Beitrag im RiffReporter.de hier erneut ab.

Immer häufiger werden Hochschulen von kriminellen Hackern angegriffen. Dabei sind nicht nur private Daten in Gefahr, der ganze Betrieb kann lahmgelegt werden. Doch wie reagieren Hochschulen auf Attacken? Wir haben es ausprobiert

Als die Hacker:innen seine Hochschule angreifen, erschrickt Thomas Grünewald. Aber er ist nicht überrascht. „Wir haben bestimmte Risiken gekannt und sie möglicherweise zu Unrecht zu lange hingenommen“, sagt der Präsident der Hochschule Niederrhein, als wir ihn einige Tage später darauf ansprechen.

Es war eine Unaufmerksamkeit, die den Eindringlingen die Tür öffnete – mit potenziell weitreichenden Folgen: Sie bekamen Zugriff auf ein internes System, indem sie eine ungeschützte Schnittstelle ausnutzten. Sie schleusten ein Programm ein, das ihnen half, Dateien auf einem Server auszulesen – unter anderem die Datei „ /etc/passwd“, die Nutzernamen beinhaltet, die auf den Server Zugriff haben.

Der nächste Schritt der Eindringlinge wäre die Suche nach Passwörtern, Konfigurationsdateien und privaten Schlüsseln gewesen. Eine Ransomware-Bande würde es zwar etwas Zeit kosten, aber womöglich wäre sie durch diese Lücke irgendwann in das Herz der universitären Systeme vorgedrungen, hätte Daten gestohlen und schließlich alles verschlüsselt, um dann Lösegeld für eine Freischaltung zu verlangen. So wie es aktuell an der HAW Hamburg[2] geschehen ist.

Zwischen den Jahren schlagen Angreifer besonders gern zu

Der Unterschied: Im Fall der Hochschule Niederrhein waren wir die Eindringlinge. „Rene Rehme, ethischer Hacker, und Eva Wolfangel, Tech-Journalistin“, so stellen wir uns in der E-Mail an den Präsidenten und sein Sicherheitsteam vor, in der wir vor der Sicherheitslücke warnen.

Wir haben die IT-Sicherheit von Deutschlands Universitäten und Hochschulen auf den Prüfstand gestellt, indem wir einige von ihnen von außen angegriffen haben – so wie es kriminelle Angreifer derzeit massiv tun: Eine gute Zeit dafür, Angriffe zu starten, war zwischen Weihnachten und Neujahr, wenn die Aufmerksamkeit von IT-Verantwortlichen niedriger ist als sonst.

[1] https://www.riffreporter.de/de/technik/hacking-datenschutz-ransomware-hochschulen-universitaeten-daten-im-netz-it-sicherheit [18.07.2025].
[2] https://www.forschung-und-lehre.de/management/haw-hamburg-von-hackern-erpresst-5321 [18.07.2025].

So machen das auch böswillige Hacker. Ins Visier genommen haben sie zum Jahreswechsel 2022/23 zum Beispiel die Stadtverwaltung Potsdam, die Westsächsische Hochschule Zwickau[3] und die HAW Hamburg. Kurz zuvor hatte es die Hochschule Heilbronn[4], die Hochschule Ansbach[5], der TH Ulm[6], die FH Münster[7], die Hochschule für Technik, Wirtschaft und Kultur in Leipzig[8] und gleich zwei Mal die Uni Duisburg-Essen getroffen[9], die nun ebenso wie die HAW Hamburg von den Angreifern erpresst wird: Sie drohen damit, die erbeuteten Daten zu veröffentlichen.

Sind Hochschulen begehrte Opfer oder einfach nur schlecht geschützt?

Der Ausgangspunkt unserer Recherche war die Frage: Wenn Universitäten derzeit so stark angegriffen werden, liegt das daran, dass sie attraktive Opfer sind – beispielsweise, weil es interessante Daten gibt? Oder sind sie einfach schlecht geschützt? Nach allem, was wir in den vergangenen Wochen gesehen haben, trifft letzteres auf jeden Fall zu. Wir fanden nicht nur extrem kritische Lücken, sondern teilweise auch Schadcode, den kriminelle Angreifer:innen bereits in den IT-Systemen hinterlassen hatten – unbemerkt von den Unis selbst.

Bei mindestens vier Universitäten und Hochschulen – nämlich der Universität Düsseldorf, der Universität Tübingen, der Uni Bremen und der Hochschule Niederrhein – kamen wir an Stellen, an denen es möglich gewesen wäre, tiefer in interne Systeme einzudringen, an typische Einfallspunkte von Ransomware-Gruppen.

Würden Kriminelle auf solche Schwachstellen stoßen, könnten sie diese ausnutzen, um sich in den Systemen auszubreiten, sich nach und nach weitergehende Rechte zu erschleichen, und schließlich womöglich zentrale Systeme zu verschlüsseln – nicht ohne vorher Daten herunterzuladen, um dann als weitere Erpressungsmaßnahme mit deren Veröffentlichung zu drohen. Vielleicht wären solche Angreifer dann irgendwann aufgehalten worden. Das haben wir nicht getestet, denn das widerspricht den Grundsätzen ethischen Hackings. Sie sehen unter anderem vor, nur so weit wie nötig einzudringen, um die Schwachstelle beschreiben zu können.

Bei mehr als zehn weiteren Unis und Hochschulen konnten wir zudem persönliche und sensible Daten Studierender und Mitarbeitender herunterladen.

---

[3] https://www.tag24.de/nachrichten/regionales/sachsen/zwickau/hacker-angriff-hochschule-in-sachsen-lahmgelegt-2707206 [18.07.2025].
[4] https://www.stuttgarter-nachrichten.de/inhalt.angriff-bestaetigt-hacker-blockieren-hochschule-heilbronn.e3f6f60f-dba5-421b-a3c9-339592a30a85.html [18.07.2025].
[5] https://www.sueddeutsche.de/bayern/hackerangriff-hochschule-ansbach-lka-cyberattacke-1.5678669 [22.11.2024].
[6] https://www.swp.de/lokales/ulm/hacker-angriff-auf-hochschule-ulm-was-zur-cyber-attacke-bislang-bekannt-ist-und-wie-es-weitergeht-67788875.html [18.07.2025].
[7] https://www.fh-muenster.de/de/ueber-uns/newsroom/news/archiv/2022-01-26-cyberangriffe-auf-die-fh-muenster [18.07.2025]
[8] https://www.htwk-leipzig.de/hochschule/aktuelles/newsdetail/artikel/it-sicherheitsvorfall-an-der-htwk-leipzig [18.07.2025].
[9] https://www.spiegel.de/netzwelt/web/universitaet-duisburg-essen-hacker-erpressen-die-hochschule-a-ec8b93b2-8111-417c-bf14-e7e933d47732 [18.07.2025].

Jede fünfte Hochschule wies eine Sicherheitslücke auf

Als wir die Sicherheitslücken meldeten, begegneten wir weiteren Überraschungen: Viele reagierten schnell, aber andere waren kaum zu erreichen. Und während die meisten dankbar und erleichtert waren, dass wir und nicht kriminelle Angreifer:innen die Lücken gefunden hatten, drohten uns zwei mit rechtlichen Schritten: Der Datenschutzbeauftragte der Uni Tübingen erwähnte beiläufig die Paragraphen 202 a, 202 b und 202 c des Strafgesetzbuches[10], die so genannten „Hackerparagrafen", die auch ethische Hacker permanent der Gefahr der Kriminalisierung aussetzen[11]. Die Justiziarin der FH Kiel drohte unverhohlen mit dem Presserecht.

Wir erlebten weitere Überraschungen: Als wir zufällig einige Wochen später bei zwei Universitäten die Sicherheitslücken erneut nachvollzogen, sahen wir, dass die eine Hochschule die Lücke trotz anderslautender Angaben nicht geschlossen hatte und die andere eine weitere, kritische Lücke aufwies. Das ist symptomatisch für diese Recherche, denn wo wir hinschauten, taten sich Probleme auf. Bei zwei Universitäten fanden wir sogar Schadcode früherer Angreifer – echter Krimineller also, die nach der Attacke weitergezogen waren. Die Universitäten hatten weder die Angriffe noch die verbliebenen Hintertüren bemerkt.

Doch von vorne: Vorgenommen hatten wir uns ursprünglich, alle der mehr als 400 deutschen Hochschulen zumindest grob zu testen. Doch nach den ersten 73 (wir gingen grob der Größe nach) lief die Recherche völlig aus dem Ruder: Wir fanden so viele Lücken und Datenlecks, dass uns klar wurde, dass wir aufhören müssen. Schließlich ist es ein großer Aufwand, die Daten zu sichten, die Lücke einzuschätzen und sie den betroffenen Unis zu melden. Jede fünfte Hochschule wies eine Sicherheitslücke auf. Also stoppten wir nach den 73 Größten mit dem mulmigen Gefühl, dass die verbliebenen 350 vermutlich eine ähnliche Quote haben werden.

Kriminelle können Daten herunterladen, verschlüsseln und Lösegeld verlangen

Die schwerste Sicherheitslücke begegnete uns an der Uni Düsseldorf: Dort bekamen wir Zugriff auf mehrere zentrale Dateispeichersysteme der philosophischen Fakultät, die offen im Netz lagen und in denen sowohl der Quellcode diverser Programme abgelegt war als auch eine Dokumentation der gesamten Server-Infrastruktur einer Fakultät sowie zahlreiche Zugangsdaten für verschiedene Systeme. Darin waren mehr als 100 Passwörter von Nutzenden gänzlich unverschlüsselt gespeichert und weitere knapp 500 mit einer veralteten, leicht zu knackenden Methode verschlüsselt.

Zudem bekamen wir Zugang zu mehr als 300 Datenbanken mit vielerlei Information, unter anderem tausende Datensätze von Mitarbeitenden und Studierenden, Moodle-Datenbanken aus vielen Jahren voller Noten, private Chat-Protokolle und anderes.

In einem Versionsverwaltungssystem für Dateien – ein so genanntes Git Repository – waren auch die Zugangsdaten des Root-Users eines zentralen Datenbank-Servers hinterlegt. Das ist der Zugang mit den

[10] https://www.gesetze-im-internet.de/stgb/__202a.html [18.07.2025].
[11] https://www.zeit.de/digital/datenschutz/2021-08/cdu-connect-app-it-sicherheit-lilith-wittmann-forscherin-klage [18.07.2025].

meisten Rechten. Angemeldet als Root-User hätten wir alle Inhalte verändern können – angefangen von Webseiten der Uni bis hin zu den Noten der Studierenden, die in einigen Moodle-Datenbanken abgelegt waren. Wären wir Kriminelle, hätten wir Daten herunterladen und verschlüsseln können, um die Universitäten zu erpressen.

Die Verantwortlichen an der Uni Düsseldorf lehnten ein Interview ab. In einem schriftlichen Statement bestätigte ein Sprecher die Zugriffsmöglichkeit auf ein IT-System der philosophischen Fakultät, die man zwar als „prinzipiell sehr kritisch" beurteile, die aber lediglich „ein begrenztes IT-Subsystem und nicht die komplette HHU-IT-Infrastruktur" betroffen habe.

Was hat Vorrang – Freiheit oder Forschung oder IT-Sicherheit?

Daraus zu schließen, dass die zentrale Infrastruktur der Uni sicher war, ist allerdings voreilig, sagt Matthias Marx, ein IT-Sicherheitsforscher, den wir gebeten haben, die von uns entdeckten Schwachstellen unabhängig zu bewerten. „Der Umfang der hier zugänglichen Daten ist bemerkenswert", sagt Marx, der selbst zum Thema Sicherheit und Datenschutz an Universitäten geforscht hat (Mueller et al., 2018) und im vergangenen Jahr Sicherheitslücken an zehn Universitäten gemeldet hat. Düsseldorf steche heraus: „Hier ist ein großer Teil der Serverinfrastruktur der zweitgrößten Fakultät dokumentiert, was es Angreifern ermöglicht, weitere Schwachstellen zu finden."

Angesichts der Menge an Zugangsdaten wäre es seiner Erfahrung nach wahrscheinlich, dass wir einen Account gefunden hätten, der das gleiche Passwort auch an anderen Uni-Systemen verwendet. „Die Datenbank in Zusammenhang mit dem umfangreichen Quellcode ist eine gute Grundlage für Angreifer", lautet die Einschätzung von Marx.

Zudem ist allein die philosophische Fakultät der Uni Düsseldorf mit ihren 25 Studiengängen und 10.000 Studierenden fast so groß wie die ganze Hochschule Niederrhein mit ihren 13.000 Studierenden. Das Bild eines kleinen dezentralen Systems wankt.

Im Gegensatz zu seinen Kollegen an der Uni Düsseldorf ist es Thomas Grünewald von der Hochschule Niederrhein wichtig, Sicherheitslücken nicht zu verharmlosen, sondern zu klären, wieso sie existieren. „Sie sind als Angreifer richtig in unsere Systeme eingedrungen und hatten die Chance, im internen System etwas zu verändern", sagt er ganz offen im Gespräch mit uns.

Er wolle das nicht verharmlosen. Wer aber behaupte, solche Lücken seien gänzlich vermeidbar, liege falsch. „Das geht nur zu einem gewissen Grad, es wird immer Lücken geben." IT-Sicherheit an Universitäten unterliege einer ständigen Güterabwägung: „Gebe ich der Sicherheit oder der Freiheit den Vorrang?"

Nach strengeren Regeln stellten Mitarbeiter auf Gmail und GMX um

Ganz persönlich sei ihm das Dilemma der Sicherheit an Hochschulen klar geworden, als er versuchte, auf immer neue Sicherheitslücken bei Microsofts Exchange[12] Servern zu reagieren, die 2021 und 2022 vielen Unternehmen, Universitäten und Behörden[13] kriminelle sowie Spionage-Angriffe bescherten, sagt Grünewald.

„Wir haben deshalb damals die Schotten ein Stück weit hochgezogen." Wer von außen auf das Uni-Netz zugreifen wollte, musste sich per VPN verbinden. Dann startete der 63-jährige Hochschulpräsident einen Selbstversuch: „Ich habe als *digital immigrant* selbst versucht, mir die Software für einen VPN-Tunnel zu organisieren." Einfach war es nicht, gibt er zu, ein bisschen Hilfe war dann doch nötig.

Doch dann ging die Sache nach hinten los. Mitarbeitende überlegten sich eigene Lösungen – beispielsweise E-Mail-Weiterleitungen auf private Accounts. Viele Dozent:innen seien komplett ausgewichen auf ihre Gmail- oder GMX-Adressen, und haben die Studierenden umgeleitet: „So erzeugen Sie einen Verkehr an hochschulrelevanten Daten, den Sie nicht mehr abgesichert bekommen."

Dezentrale Systeme sind beliebt – aber unsicher

Seither ist Grünewald auf der Suche nach dem richtigen Weg. „Es ist grenzenlos naiv zu glauben, man könnte die Schotten so hochziehen", sagt er. Es sei ein Kulturprozess zwischen Sicherheitsanforderungen und Forschenden, die stets einen eigenen Kopf haben und aus seiner Sicht für gute Forschung eben auch Freiheit brauchen. „Die Frage ist, wann ziehe ich die Schrauben so eng an, dass mir meine eigenen Leute nicht mehr folgen?"

Dazu komme der Wunsch nach dezentralen Servern, jenen Subsystemen, die auch die Uni Düsseldorf in ihrer Antwort erwähnte. Letztlich gebe es immer Forschungsprojekte und Gruppen, die eigene Server betrieben – das habe er bisher zugelassen, „wir haben dem häuslichen Frieden den Vorrang gelassen", gibt er zu. Gleichzeitig seien diese nicht immer so gut geschützt wie die zentralen Systeme, „das ist salopp gesagt ein Sack Flöhe."

Lässt sich der noch einfangen? „Ich kann versuchen, den Wissenschaftsbetrieb entgegen seiner Natur so zentralistisch wie möglich zu führen", sagt er. Aber das sei ein Drahtseilakt. Grünewald weiß seit der VPN-Geschichte, wie schnell das schief gehen kann.

Wer die großen Angriffe der vergangenen zwei Jahre analysiert, sieht aber auch: Die Ransomware-Banden finden meist eine Lücke genau in diesen dezentralen Servern und arbeiten sich dann vor in das Herz der Hochschulen. So war es auch aktuell beim Angriff auf die HAW Hamburg.[14]

---

[12] https://www.heise.de/news/Patchday-Microsoft-Attacken-auf-sechs-Luecken-Exchange-Patches-endlich-da-7334213.html [18.07.2025].

[13] https://www.zeit.de/digital/datenschutz/2021-03/microsoft-exchange-server-sicherheitsluecke-bundesbehoerden-datenschutz [18.07.2025].

[14] https://www.haw-hamburg.de/cyberangriff [18.07.2025].

Schwere Lücke an der Uni Tübingen

Auch der Uni Tübingen wurde ein solches dezentrales System zum Verhängnis bei unserem Angriffsversuch. Dort gelang es uns dank eines auf einer Website vergessenen Installationstools einen so genannten „Super-Admin"-Account anzulegen. Damit war es möglich, aus der Ferne ein eigenes Programm auf dem Server laufen zu lassen. Das Fachwort hierfür ist *Remote Code Execution*. Das Programm half uns, uns auf dem Server umzusehen. Auch das hätte ein Einfallstor für eine Ransomware-Gruppe sein können, die dann nach und nach weitere Informationen und Zugänge sammelt.

„Das hätte nicht passieren dürfen", sagt Thomas Walter, *Chief Information Officer* der Uni Tübingen ganz unumwunden. Man habe sofort nach unserer Meldung den entsprechenden Server vom Netz genommen und untersucht, wer darauf Zugriff hatte. Die Lücke sei vor acht Jahren entstanden, als ein Forschungsprojekt eine eigene Webseite erstellt und dabei offenbar das Installationstool nicht entfernt hatte. Man hatte diese Webseite völlig vergessen. Auch er spricht von einem „dezentralen Server", stimmt aber zu, dass Angreifer mit den Informationen von dort möglicherweise ihren Weg in zentrale Systeme finden könnten.

Wenn der Schadcode schon im System schlummert

Matthias Marx ordnet diese Lücke als zweitgefährlichste unserer Entdeckungen ein und bestätigt: „Durch solche vergessenen Entwicklungswerkzeuge oder Installationstools kann man häufig admin-Zugang erlangen." Dieser hat sehr weitgehende Rechte, und wer diese ausnutze, könne beispielsweise Konfigurationsdaten einsehen, Schadcode ins System einschleusen, Nutzende und deren Zugangsdaten ausspähen und sich auf diese Weise Zugriff auf andere Dienste und Server verschaffen.

Als wir einige Wochen später den Vorfall erneut nachvollziehen, finden wir allerdings eine noch kritischere Lücke: Über weitere Applikationen ist es möglich, Zugriff auf den Server zu erlangen.

Dabei stoßen wir auf etwas besonders Erschreckendes: Schadcode anderer Angreifer:innen. Offenbar gab es bereits verschiedene Angriffe Krimineller auf die Infrastruktur. Wir finden mehrere sogenannte *Backdoors*, also Hintertüren, die es den Eindringlingen ermöglichen, Schadsoftware auf den Systemen der Uni auszuführen. Teile davon sind mehrere Jahre alt. Hat die Universität tatsächlich nicht bemerkt, dass sie angegriffen wurde? Können die Verantwortlichen ausschließen, dass dabei Daten abgezogen wurden?

In der Tat habe man die Hintertüren erst nach unserer Meldung bemerkt, bestätigt CIO Thomas Walter. Er stimmt uns zu, dass der Server wohl bereits vor mehreren Jahren von Kriminellen angegriffen wurde, ohne dass es jemand bemerkte. „Wir ermitteln gerade das Ausmaß des Vorfalls", sagt Walter, der den ganzen Bereich umgehend offline genommen hat. Bisher seien keine auffälligen Aktivitäten gefunden worden, „die auf eine Weiterverbreitung oder den gezielten Angriff auf andere Server hinweisen." Ausschließen könne man das aber nicht.

Auch bei der Universität Bremen finden wir alten Schadcode auf einem Server: Eine abgelegte so genannte Webshell, mit der sich Kriminelle eine Hintertür ins System gebaut haben. Auf dem Server ist zudem unter anderem ein Private Key zu finden sowie MySQL Zugangsdaten. Außerdem SMTP Zugangsdaten, mit denen Kriminelle valide E-Mails über eine @uni-bremen.de E-Mail Adresse verschicken könnten. Das könnten sie

für Social Engineering nutzen: Speziell auf die Empfänger:innen zugeschnittene E-Mails, die mit dem validen Absender dann besonders überzeugend wirken.

An der Uni Bremen gibt man sich wortkarg. Auf die Schwachstellenmeldung selbst antwortet niemand, erst als wir diese über das Deutsche Forschungsnetzwerk und deren CERT melden, wird sie Tage später geschlossen. Erst eine Anfrage über die Pressestelle führt zu einer Reaktion: Die Lücke sei nun geschlossen. Über den Schadcode im System und den damit verbundenen älteren Cyberangriff, der offenbar nicht bemerkt worden ist, wolle man sich nicht äußern.

Noten, Zeugnisse und Atteste – private Informationen im Internet

Neben dieser vier für die Universitäten selbst bedrohlichen Lücken haben wir unzählige Datenlecks gefunden. Die betroffenen Hochschulen haben sich selbst damit nicht angreifbar gemacht – sie haben „nur“ die ihnen anvertrauten Daten miserabel geschützt. Das ist besonders tragisch, denn diese Daten gewährten uns – und möglicherweise auch Kriminellen – sehr persönliche Einblicke, zum Beispiel in das Leben von Finn (alle Namen geändert), dem 21-jährigen Wirtschaftsingenieurs-Studenten an der Fachhochschule Erfurt, der nicht gut ist in Mathe (Note 4), oder das der 23-jährigen Melissa, die Bauingenieurin werden will, aber ihre erste Massivbau-Prüfung verhauen hat (Note 5).

Die 22-jährige Lena hat ganz andere Probleme: Sie reicht der FH Erfurt ein Attest einer Psychotherapeutin ein. Der angehende Stadtplaner Peter bewirbt sich als Werkstudent, Florian (35) hat eine Anzeige bei der Polizei gestellt, andere schicken Führungszeugnisse, Fotos vom Sommerfest – oder eine Krankmeldung wie Yasmin (27): Sie ist nicht alleine, im Dezember 2022 haben viele ihr Attest per E-Mail an die FH Erfurt geschickt – und sie damit unwissentlich offen ins Netz gestellt.

Die FH hatte einen Webmailer nicht abgesichert, wodurch E-Mail-Anhänge von Studierenden und Mitarbeitenden und andere Daten öffentlich einsehbar waren. In Erfurt ist man damit nicht allein: Auch die TU Berlin, die TU Dresden, die Uni Kassel, die Hochschule Worms, die Hochschule Trier, die TH Deggendorf und ein Fachbereich der Uni Stuttgart hatten in unterschiedlichem Ausmaß Daten aus ungeschützten Webmailern im Netz. Darin Atteste, Personalausweise, noch unveröffentlichte Forschungsarbeiten mit teils geschützten Daten deutscher Unternehmen, Zeugnisse, Bewerbungen, Motivationsschreiben und vieles mehr.

Sechs Monate später können Angriffe gar nicht mehr nachvollzogen werden

Diese Art von Sicherheitslücken sind einfach zu finden – vor allem aber auch einfach zu vermeiden, wenn man entsprechende Webmailer sorgfältig einrichtet. Alle betroffenen Institutionen nutzen eine freie Software namens *Roundcube* und hatten diese schlicht falsch implementiert: „In der Dokumentation wird eindeutig darauf hingewiesen, dass das sensible Verzeichnisse und Daten sind und dass sie nicht offen im Netz erreichbar sein dürfen“, sagt René Rehme.

Dass dies trotzdem geschieht, spricht für eine gewisse Sorglosigkeit. Einige der betroffenen Hochschulen konnten nicht ausschließen, dass auch Kriminelle Zugriff auf diese Daten hatten. Damit müssen sie rechtlich

alle Betroffenen informieren – also in der Regel alle Hochschulangehörigen. In Trier und Erfurt wurde das umgesetzt, von anderen wissen wir es nicht.

Als wir einige Wochen später erneut einige der Links anklickten, stellten wir erstaunt fest, dass die Uni Stuttgart nur versucht hatte, die Lücke zu schließen – allerdings wenig erfolgreich: Wir hatten weiterhin Zugriff auf hunderte Vorgänge, die zwar nicht den Inhalt der E-Mails verrieten, wohl aber die E-Mail-Adressen der Beteiligten und wann diese an wen eine E-Mail geschickt hatten. Die aktuellste E-Mail war vom gleichen Tag.

Da sich diese Protokolle permanent die aktuellsten E-Mails erfassen, könnten Angreifer:innen theoretisch über Jahre mitgelesen und persönliche Daten gesammelt haben. Dies im Nachhinein festzustellen ist für die betreffende Institution häufig unmöglich, weil entsprechende Logdateien meist nur sechs Monate gespeichert werden. Alles, was vor dieser Zeit geschah, lässt sich nicht rekonstruieren.

Datenschutzbehörden verlangen von Hochschulen Meldungen

Wenn persönliche Daten offen im Netz liegen, müssen die Verantwortlichen die jeweiligen Datenschutzbehörden informieren – aber auch das taten einige der betroffenen Hochschulen und Universitäten nicht. Von der Uni Stuttgart liege auch nach dem nunmehr zweiten Vorfall keine Datenpannenmeldung vor, teilt Jan Wacke, Leitender Beamter beim Landesbeauftragten für den Datenschutz Baden-Württemberg, mit: Man wende sich nun an die Uni, um Genaueres zu erfahren.

„Wenn personenbezogene Daten wie von Ihnen beschrieben online für Unbefugte zugänglich sind, gehen wir zunächst grundsätzlich davon aus, dass dies meldepflichtig ist.“ Angesichts unserer Recherchen werde die Behörde nun zudem auf weitere Hochschulen in Baden-Württemberg zugehen „und uns erklären lassen, ob und inwieweit sie Prüfungen vornehmen, um entsprechende mögliche Sicherheitslücken zu finden und zu schließen.“

Auch die Datenschutzbehörde in Nordrhein-Westfalen meldete sich auf unsere Anfrage hin zurück und teilte mit, dass die Uni Düsseldorf trotz Meldepflicht keine Mitteilung über den Vorfall gemacht habe – man werde nachfragen.

Die Uni Göttingen, die Hochschule Anhalt, die FH Kiel sowie die Humboldt-Universität zu Berlin wiesen ebenfalls Schwachstellen auf, durch die wir an personenbezogene Daten wie Adressen und Rechnungen kamen sowie in Anhalt auch an Zugangsdaten zu internen Systemen, die möglicherweise ein tieferes Eindringen ermöglicht hätten. Das ist bezeichnend vor dem Hintergrund, dass die Hochschule Anhalt bereits im Februar 2022 Ziel eines Hackerangriffs war.[15]

[15] https://www.hs-anhalt.de/hochschule-anhalt/aktuelles/neuigkeit/it-sicherheitsvorfall-die-hochschule-anhalt-ist-erreichbar-1.html [18.07.2025].

Die ganze Uni schien im Winterschlaf zu sein

Die Urlaubszeit zwischen den Jahren machte es uns ebenso wie Kriminellen nicht nur einfacher, in Systeme einzudringen – sie bremste auch die Schutzmaßnahmen. Denn die Sicherheitslücken zu melden, damit sie geschlossen werden können, erwies sich als nächste Herausforderung. Es war schwierig, überhaupt die richtigen Ansprechpartner zu ermitteln. Während manche umgehend antworteten und die angreifbaren Dienste vom Netz nahmen, wie die Uni Tübingen und die Hochschule Trier, ließen sich andere Zeit.

Besonders nervös wurden wir, als die Universität Düsseldorf auch nach 20 Stunden noch nicht reagiert hatte und die Lücke weiterhin offen war. Was, wenn sie nun Kriminelle entdecken? Wer um so eine massive Sicherheitslücke weiß, schläft schlecht, solange sie nicht geschlossen ist.

Unzählige Anrufe führten ins Leere: Die ganze Uni schien im Winterschlaf. Schließlich erreichten wir einen Mann, der reichlich erstaunt war über unseren Anruf: Er sei bereits seit drei Jahren in Rente – auch wenn er einst für IT-Sicherheit zuständig war und sogar manchmal noch aushelfe. Aber woher wir seine Nummer hätten? Sie stand offenbar seit drei Jahren ohne sein Wissen auf der Webseite der Uni Düsseldorf.

Immerhin kommt danach Bewegung in die Sache – offenbar hatte der Rentner noch gute Kontakte: Wenige Stunden nach dem Telefonat wird die Lücke geschlossen. Was war vorher geschehen? War unsere E-Mail übersehen worden? Wir erfahren von einem zusätzlichen Sicherheitsproblem: Die E-Mail-Adresse des Zuständigen für die IT-Sicherheit war nicht erreichbar – offenbar war die betreffende Person im Urlaub. So erfuhren die Verantwortlichen erst mit Verzögerung von der heiklen Sicherheitslücke.

Zeit spielt durchaus eine Rolle, wie andere Vorfälle zeigen. So habe eine der Universitäten, die Opfer der Hackergruppe Conti[16] wurde, das Update für die Lücke in Microsofts Exchange-Servern nur wenige Minuten zu spät aufgespielt, sagt der Tübinger CIO Thomas Walter. Er selbst hat deshalb seit drei Jahren zwischen den Jahren keinen Urlaub mehr genommen: „Das ist eine so kritische Zeit."

Hochschulen sind seit 2019 stärker im Fokus krimineller Banden

Walter erinnert sich noch gut daran, wann er eine Ahnung davon bekam, dass sich die Zeiten für Universitäten ändern würden. Der „Datenpunkt, an dem alle nervös wurden", sei der 8. Dezember 2019 gewesen. Das war der zweite Advent. An diesem Tag wurde die Uni Gießen mit Emotet angegriffen[17] – der Name bezeichnet eine kriminelle Bande ebenso wie eine berüchtigte Schadsoftware. „Das war der Erfolgsdurchbruch für Erpressungssoftware an Universitäten", sagt Walter. Bis dahin habe man vor allem mit Kleinkriminellen zu tun gehabt, doch seither haben es Profis auf die Unis abgesehen. Gleichzeitig sei ihm klar geworden, dass es nahezu unmöglich sein würde, Universitäten vollständig abzusichern.

Die Hochschulen haben sich zwar zusammengetan: Das Deutsche Forschungsnetzwerk, in dem viele Hochschulen Mitglied sind, hat ein eigenes *Computer Emergency Response Team* (CERT), das vor

[16] https://blogs.tu-berlin.de/datenschutz_notizen/2021/10/29/vor-waehrend-nach-einem-cyberangriff-wie-am-besten-reagieren/ [18.07.2025].

[17] https://www.heise.de/news/Uni-Giessen-nach-Cyber-Attacke-groesstenteils-wieder-online-4692730.html [18.07.2025].

Schwachstellen und aktuellen Angriffsmustern warnt. Viele Hochschulen blockieren bekannte IP-Adressen von Ransomwaregruppen.

Aber viele klassische Sicherheitsmaßnahmen versagen: So geben viele Unternehmen ihren Angestellten gesicherte Arbeitscomputer und lassen nur eine übersichtliche Auswahl an Programmen zu, die stets aktuell gehalten sind. Das ginge an der Uni nicht, sagt Walter: „Wir haben die Freiheit der Forschung und Lehre." Es sei kaum möglich, bestimmte Programme oder Geräte vorzuschreiben. „Eine Exzellenz-Uni lebt von der Offenheit, ich kann das Netz nicht so zumachen, wie ich wollte."

60.000 unbetreute Geräte im System – jeden Tag

Allein die 30.000 Studierenden, von denen jeder im Schnitt zwei Geräte mit zur Uni bringt, seien eine Herausforderung. „Ich habe jeden Tag 60.000 unbetreute Geräte in meinem Netzwerk, das ist security-mäßig der Horror." Dazu kommen Spezialgeräte wie teure Elektronenmikroskope in der Medizin. „Die haben teilweise noch Windows XP auf dem Rechner" – ein mehr als 20 Jahre altes Betriebssystem, das seit bald zehn Jahren keine Sicherheitsupdates mehr erhält. „Aber ich kann die ja nicht wegschmeißen, weil der Steuerungs-PC veraltet ist." Also baue er Schutzmaßnahmen drumherum. Neben den klassischen Ransomware-Banden beobachtet Walter zudem verstärkte Spionageangriffe auf die Corona-Forschung in Tübingen. So hätten Personen in diesem Bereich gezielte, auf sie persönlich zugeschnittene Phishing-E-Mails erhalten.

Gibt es also keine Chance? Kann man Unis nicht besser absichern?

IT-Experte Matthias Marx war selbst bis vor kurzem Mitarbeiter an der Uni Hamburg und weiß aus eigener Erfahrung, dass Wissenschaft Freiheit braucht. Dennoch findet er, dass der Konflikt zwischen Freiheit und Sicherheit kleiner ist, als ihn die befragten Unis zeichnen. „Man sollte im Blick haben, welche Infrastruktur man betreibt", kommentiert er die Tübinger Aussage über die „vergessenen Server." Das ließe sich zum Beispiel durch technische Maßnahmen erreichen wie regelmäßiges Scannen der eigenen IP-Adressbereiche – oder durch organisatorische Maßnahmen. Universitäten hätten zwar wegen der vielen befristeten Verträge mehr Fluktuation als etwa Unternehmen: „Das führt häufig dazu, dass Dinge vergessen werden." Helfen würde aber eine gute Dokumentation der Fachbereiche, in der für jeden Server und jedes Projekt klare Verantwortliche benannt werden. „Verlassen diese die Universität, wird die Verantwortung entweder übertragen, oder der Server wird abgeschaltet." Das beeinträchtige nicht die Freiheit der Forschung.

Langsam beginnt ein Umdenken

Auch René Rehme, der ethische Hacker im Team, denkt, dass es besser gehen müsste. „Ich bin verwundert, dass wir in dieser kurzen Zeit so viele offensichtliche Probleme entdeckt haben. Wenn es von außen so einfach ist, massive Sicherheitslücken zu finden, frage ich mich, wieso die Unis diese nicht selbst finden. Es scheint, als haben sie keinen Überblick über ihre eigenen Netzwerke."

In der Tat fallen alle Lücken, die wir gefunden haben, unter die so genannten OWASP-Top10 – die zehn in der Sicherheitsforschung allgemein anerkannten Risiken, die Verantwortliche um jeden Preis vermeiden sollten. Es sind also keine ausgefallenen Angriffe, sondern eher das, was Kriminelle als erstes ausprobieren. Diese

Top-10-Liste wird vom *Open Web Application Security Project* (OWASP) – einer internationalen Non-Profit-Organisation, die sich der Sicherheit von Webanwendungen widmet – regelmäßig aktualisiert.

Vielleicht bewegt sich tatsächlich etwas. Nachdem wir Thomas Walter geschrieben haben, dass wir viele Jahre alte Hintertüren von kriminellen Angreifer:innen in den Netzen der Uni Tübingen gefunden haben, schiebt er Überstunden und baut das Netz grundlegend um. Das hätten er und sein Team ohnehin vorgehabt, nur war immer anderes wichtiger – jetzt ist die Dringlichkeit klar geworden.

Generell beobachtet Walter ein Umdenken: „Die Grenze verschiebt sich gerade von der Freiheit zu Sicherheit." Ein Grund ist die aktuelle Angriffswelle von Ransomware-Banden. Den Hochschulen wird klar, dass es so nicht weitergehen kann. Gleichzeitig werde die Situation mit der fortschreitenden Digitalisierung immer komplexer. „Wir sollten uns besser schützen, aber wir kriegen keine zusätzlichen guten Leute" sagt Walter. Denn es gebe zu wenig Budget für IT-Sicherheit. „Wir fahren da fröhlich weiter auf Wände zu."

***Eva Wolfangel** ist Journalistin und Autorin, Stuttgart.*

***René Rehme** ist Sicherheitsexperte und ethischer Hacker, rehme.infosec, Stuttgart.*

Literatur:

Mueller, T., Herrmann, D., Pridöhl, H., Marx, M., Wichmann, P. (2018). Sicherheit und Privatheit auf deutschen Hochschulwebseiten: Eine Analyse mit PrivacyScor, in: Ude, A. (Hrsg.). Sicherheit in vernetzten Systemen: 25. DFN-Konferenz. https://muelli.cryptobit.ch/paper/2018-02-DFN-PrivacyScore.pdf [18.07.2025].

Harald Gilch, Maren Lübcke, Mathias Stein: Mehr als Technologie: Krisenmanagement nach Cyber-Angriffen – Empfehlungen für das Hochschulmanagement

1 Einführung

Hochschulen weltweit und in Deutschland sehen sich einem zunehmenden Risiko von Cyber-Angriffen ausgesetzt. Dies ist auf mehrere Faktoren zurückzuführen: Sie verfügen über wertvolle Daten (insbesondere Personal- und Forschungsdaten), ihre IT-Struktur ist in der Regel komplex und dezentral, zudem nutzen täglich viele Menschen das IT-System der Hochschule. Folglich ist es nicht die Frage, ob eine Hochschule von einem Cyber-Angriff betroffen sein wird, sondern wann dies geschehen wird. Laut dem „Global Threat Report“ des Sicherheitsunternehmens Crowdstrike ist Cyber-Kriminalität ein globales Problem, von dem verschiedene Sektoren betroffen sind – am stärksten jedoch der Hochschulsektor. Daten aus dem akademischen Bereich werden von Access-Brokern demnach häufiger angeboten als Daten aus den Sektoren Technologie, Industrie oder Finanzen (Crowdstrike, 2023, S. 9). Der Bericht zeigt eine zunehmende Professionalisierung und Arbeitsteilung bei Angriffen auf, bei denen Zugangsdaten im Darknet von sogenannten Access-Brokern angeboten werden. Access-Broker beschaffen und verkaufen den Datenzugang, während der eigentliche Angriff von anderen Akteuren durchgeführt wird. Der Cybercrime-Bericht des Bundeskriminalamtes aus dem Jahr 2023 stellt eine ähnliche Situation dar.

> *„Obwohl nicht davon ausgegangen werden kann, dass das vermehrte Angriffsaufkommen das Resultat von fokussierten Kampagnen ist, waren Bildungseinrichtungen im Jahr 2022 äußerst attraktive Ziele von Cyber-Gruppierungen.“ (Bundeskriminalamt, 2023, S. 26)*

Die ersten registrierten Cyber-Angriffe auf deutsche Hochschulen fanden 2019 statt, darunter ein Angriff auf die Justus-Liebig-Universität Gießen (Kost, Loibl, Reuter & Stenke, 2022). Seitdem sind Universitäten und Hochschulen wiederholt Ziel von Cyber-Angriffen geworden. Offizielle Aufzeichnungen über die Anzahl dieser Angriffe oder zentrale Statistiken gibt es derzeit jedoch nicht. Das Portal KonBriefing.com bietet jedoch einen Einblick in öffentlich bekannte Hackerangriffe auf Universitäten und Hochschulen an (siehe Abbildung 1). KonBriefing verzeichnet für das Jahr 2023 elf Hackerangriffe auf deutsche Hochschulen und 30 Angriffe in Europa sowie für das Jahr 2024 sechs Angriffe in Deutschland und 14 in Europa. Es ist wahrscheinlich, dass die tatsächliche Zahl der Cyber-Angriffe deutlich höher ist als die der öffentlich bekannt gewordenen Fälle.

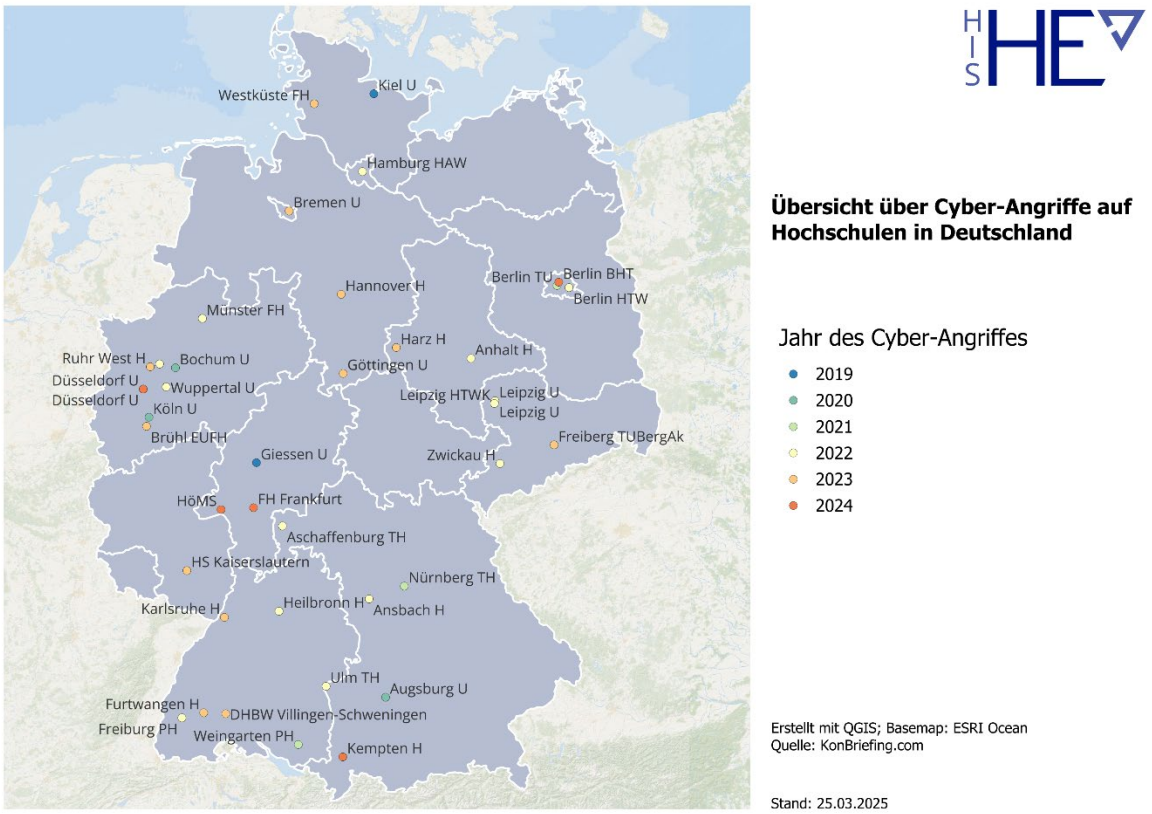

Abbildung 1: Übersicht über Cyber-Angriffe auf Hochschulen zwischen 2019 und 2024

Vor diesem Hintergrund gibt es seit einigen Jahren zunehmend Initiativen auf staatlicher Ebene, um dieser Bedrohung zu begegnen. So riefen die Staats- und Regierungschefs der Europäischen Union (EU) im Oktober 2020 dazu auf, die Fähigkeit der EU zu verbessern, sich gegen Cyber-Bedrohungen zu schützen. Im Dezember 2020 legte die EU-Kommission eine neue Cybersicherheitsstrategie vor, um die Widerstandsfähigkeit Europas gegenüber Cyber-Angriffen zu stärken. Im Jahr 2004 gründete die EU die Europäische Agentur für Netz- und Informationssicherheit, die 2019 als „Agentur der Europäischen Union für Cybersicherheit“ (ENISA) umbenannt wurde und ihren Sitz in Athen hat. Bereits im Jahr 2022 hat das Bundesministerium des Innern und für Heimat mit der Veröffentlichung der Cybersecurity-Agenda die zentralen Leitlinien in Deutschland neu definiert. Hauptziel ist es, das Bundesamt für Sicherheit in der Informationstechnik (BSI) als zentrale Stelle zu stärken, um eine bessere Abstimmung zwischen Bund und Ländern zu ermöglichen. Der Schwerpunkt liegt dabei auf technischen Aspekten zur Verbesserung der Sicherheit von IT-Infrastrukturen und -Prozessen. Um dieses Ziel zu erreichen, hat das BSI kürzlich das Nationale IT-Lagezentrum eingerichtet und damit die BSI-Initiative „Cybernation Deutschland“ gestartet.[18] Darüber hinaus wurden in Deutschland mehrere Forschungszentren für Cyber-Sicherheit eingerichtet, wie zum Beispiel das Nationale Forschungszentrum für Angewandte Cybersicherheit (Athene) in Darmstadt. Es wurde 2019 in seiner

[18] Vgl. u. a. den Blog des BSI zum Thema unter https://www.bsi.bund.de/DE/Das-BSI/Cybernation/cybernation_node.html [18.07.2025].

heutigen Form gegründet und ist inzwischen das „größte Forschungszentrum für Cybersicherheit und Privatsphärenschutz in Europa“[19].

In den letzten Jahren haben sich neben übergeordneten staatlichen Stellen und der Forschung auch Universitäten und Hochschulen verstärkt mit dem Thema Cyber-Sicherheit beschäftigt. Bereits im Jahr 2018 veröffentlichte die Hochschulrektorenkonferenz (HRK) ihre erste Empfehlung „Informationssicherheit als strategische Aufgabe der Hochschulleitung“ (Hochschulrektorenkonferenz (HRK), 2018). Weitere wichtige Publikationen zu diesem Thema stammen vor allem vom Zentrum für Kommunikation und Informationsverarbeitung (ZKI) e. V., darunter das IT-Grundschutzprofil für Hochschulen (ZKI e. V., 2022) und die Handreichung zur Vorbereitung auf Informationssicherheitsvorfälle (Dreyer, Kühnlenz, & Brandel, 2023). Der Fokus liegt dabei auf der Verbesserung der eigenen IT-Sicherheit, um mögliche Angriffe zu erschweren.

Bislang wurden die Auswirkungen eines Cyber-Angriffs auf Hochschulorganisationen nur teilweise analysiert und Empfehlungen ausgesprochen. Mit der zunehmenden Bedrohung durch Cyber-Angriffe wächst der Bedarf an geeigneten Notfallmaßnahmen. HIS-HE hat hierzu im November 2023 Handlungsempfehlungen zum „Krisenmanagement nach Cyber-Angriffen“ (Gilch, Lübcke & Stein, 2023) veröffentlicht. Der Fokus des Papiers liegt nicht auf technischen Aspekten, sondern auf der Frage: „Was muss geschehen, wenn es passiert ist?“ Ziel dieses Leitfadens ist es, das Hochschulmanagement dabei zu unterstützen, auf Cyber-Angriffe umgehend zu reagieren und den daraus resultierenden Schaden zu minimieren. Basierend auf den Erfahrungen bereits betroffener Hochschulen wurde ein Fragenkatalog entwickelt, der als Leitfaden dienen kann. Er soll zur internen Diskussion anregen und einen ersten Rahmen für die Vorbereitung und Bewältigung von Cyber-Krisen bieten. Im Rahmen dieses Beitrags wollen wir einen kurzen Überblick über die in der Handreichung genutzte Methode, die Phasen eines Cyber-Angriffes sowie zentrale Aspekte geben.

2 Methode

Die Untersuchung stützt sich auf eine Analyse von fünf Hochschulen darunter drei Universitäten und zwei Hochschulen für Angewandte Wissenschaften, die Opfer von Cyber-Angriffen wurden.

Abbildung 2 gibt einen Überblick über die ausgewählten Fälle. Für jeden Fall wurde eine Dokumentenanalyse durchgeführt und öffentlich verfügbare Informationen über den jeweiligen Cyber-Angriff geprüft. Mithilfe von Leitfadeninterviews wurden die Fälle rekonstruiert und Fragen zur Prävention, Reaktion, Bewertung und Folgen gestellt. In jeden Fall wurden Interviews mit der/dem Kanzler:in der Hochschule und – soweit möglich – Gespräche mit IT-Manager:innen und den Leitungen der Kommunikationsabteilungen geführt. Die Interviews fanden zwischen Mai und August 2023 statt. Anschließend erfolgte die Analyse der Fälle im Hinblick auf Gemeinsamkeiten und Unterschiede sowie darauf aufbauend die Entwicklung eines Phasenmodell für das Krisenmanagement bei Cyber-Angriffen. Das Phasenmodell und die damit verbundenen Handlungsempfehlungen wurden mit IT-Sicherheitsexpert:innen und IT-Arbeitsgruppen deutschsprachiger Hochschulen validiert.

[19] https://www.athene-center.de/ueber-athene [18.07.2025].

Hochschultyp	Größe[20]	Jahr des Vorfalls	Merkmale und Folgen des Cyber-Angriffs
Universität	Groß	2019	Unterbrechung der Internetverbindung, Abschaltung von Servern, Kompromittierung von zahlreichen Systemen
Technische Universität	Groß	2021	die zentralen IT-Dienste konnten nicht genutzt werden, aber dezentrale Dienste und der Lehrbetrieb waren verfügbar
Universität	Groß	2022	wiederholte Angriffe zur Blockierung von Wiederherstellungsmaßnahmen
Hochschule für Angewandte Wissenschaften	Groß	2023	Der Angriff konnte sich über einen längeren Zeitraum erstrecken und das gesamte IT-System lahmlegen.
Hochschule für Angewandte Wissenschaften	Mittel	2023	rechtzeitige Erkennung von Angriffen, präventive Systemabschaltung

Abbildung 2: Übersicht Fallbeispiele

Da die Folgen eines Cyber-Angriffs je nach Hochschuleinrichtung sehr unterschiedlich sein können, basiert die Handreichung auf einer Verallgemeinerung. Die Folgen eines IT-Ausfalls können von kurzfristigen Systemausfällen bis hin zur kompletten Lahmlegung der gesamten Hochschul-IT für mehrere Monate reichen – u. a. in Abhängigkeit der Schwere des Angriffs, aber auch der Beschaffenheit der IT-Landschaft, der verfügbaren personellen, technischen und finanziellen Ressourcen zur Bewältigung der Auswirkungen des Angriffs sowie der Erfahrungen der Einrichtung mit dem Management von Krisensituationen. Zudem bezieht sich die Studie schwerpunktmäßig auf Hochschulen. Gleichwohl ist in den vergangenen Jahren auch eine Zunahme von Cyber-Angriffen auf Universitätsklinika, außeruniversitäre Forschungseinrichtungen sowie wissenschaftliche Kooperationspartner festzustellen. Allgemeine Empfehlungen sind sicherlich auf diese Einrichtungen übertragbar, wobei die Maßnahmen auf die jeweiligen Spezifika der Organisation anzupassen wären.

Die Interviews konzentrierten sich auf die Gesamtorganisation aus Sicht der Hochschulleitung. Denn jeder Ausfall von IT-Systemen, auch wenn er nur vorübergehend ist, kann gravierende Auswirkungen auf die Funktionsfähigkeit der Hochschule und somit auf die Hochschulleitung haben.

[20] Kategorien in Anlehnung an den HSI-Monitor. https://www.hsi-monitor.de/methodik/hochschulcluster/ [18.07.2025].

3 Phasen eines Cyber-Angriffs

Je nach Schwere eines Cyber-Angriffs lassen sich verschiedene Phasen definieren. Die drei zentralen Phasen sind die Erkennungsphase, die Reaktionsphase und die Normalisierungsphase. Die Reaktionsphase kann wiederum in weitere Unterphasen unterteilt werden. Die Phasen sind in Abbildung 3 aufgeführt.

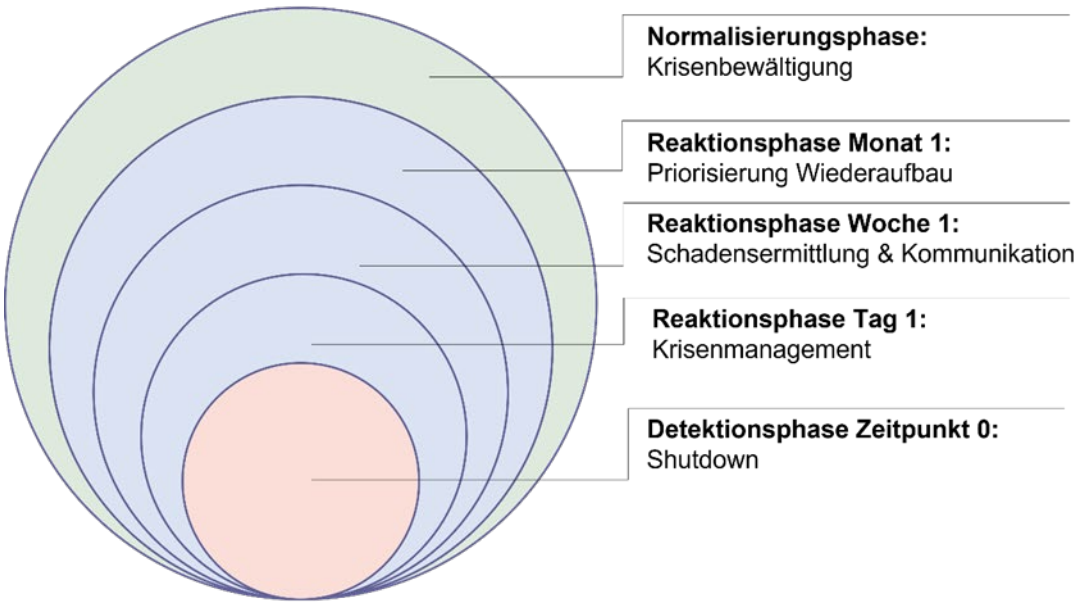

Abbildung 3: Fünf Phasen des Krisenmanagements nach einem Cyber-Angriff

Zu beachten ist, dass die Dauer und Komplexität der einzelnen Phasen stark von der Art des Angriffs, der Reaktion der Organisation und anderen Faktoren abhängen. Die Auswirkungen eines Cyber-Angriffs können – je nach individuellem Krisenszenario – zu unterschiedlichen Zeitpunkten im Phasenmodell auftreten, sodass es auch zu entsprechenden Verschiebungen kommen kann.

a) Detektionsphase – Zeit 0

Im Falle eines Cyber-Angriffs ist die Zeit entscheidend. Eine schnelle Reaktion innerhalb von Minuten oder Stunden kann das weitere Eindringen von Angreifern verhindern und den Schaden am IT-System minimieren. Zu einer schnellen Reaktion gehört, einen Angriff zu erkennen und die Systeme bei Bedarf herunterzufahren, um die Ausbreitung von Malware zu verhindern. Eine kontinuierliche Systemüberwachung kann dabei helfen, Angriffe schneller zu erkennen, da viele Angriffe an Wochenenden oder Feiertagen stattfinden. Wenn dies nicht durch eigenes Personal gewährleistet werden kann, muss die Überwachung möglicherweise an externe Dienstleister vergeben werden.

Um in dieser Phase optimal vorbereitet zu sein, müssen die folgenden Fragen (Auswahl) beantwortet werden:

- Ist die Überwachung der IT-Systeme auf Angriffe und Unregelmäßigkeiten auch außerhalb der regulären Arbeitszeiten gewährleistet?

- Wer trifft die endgültige Entscheidung (kurzfristig), Teile oder ggf. das gesamte IT-System vom Netz zu trennen?
- Welche operativen Schritte sind notwendig, um das IT-System herunterzufahren und abzuschalten?

Diese Fragen sollten im Vorfeld intern abgestimmt werden, um im Falle eines Cyber-Angriffs ein schnelles Handeln zu ermöglichen. Die Entscheidung hierüber muss für jede Hochschule individuell getroffen werden. Dies betrifft auch die Frage, ob die Hochschulleitung – aus rechtlicher Sicht – allein die Entscheidung für eine Systemabschaltung treffen kann oder ob die IT-Leitung – aus technischer Sicht – unabhängig handeln sollte, um eine schnelle Reaktion zu ermöglichen. Die Interviews haben gezeigt, dass die Hochschulen diesbezüglich sehr unterschiedliche Ansätze verfolgen. Es ist daher nicht möglich, eine allgemeine Empfehlung zu geben.

Neben der kontinuierlichen Überwachung der IT-Systeme ist es von entscheidender Bedeutung, im Vorfeld Entscheidungs- und Kommunikationskanäle einzurichten. Es muss festgelegt werden, wer informiert werden muss, sobald ein Angriff entdeckt wird. Wer kann zudem bestätigen, dass ein Cyber-Angriff stattfindet, und wer sollte die Entscheidung über das Herunterfahren und Trennen von IT-Systemen treffen? Unabhängig davon sollte das im Vorfeld gebildete IT-Kernteam mit der Koordinierung und Einleitung der notwendigen Maßnahmen beginnen. Die Teammitglieder wurden bereits benannt und es wurden Stellvertreterregelungen getroffen. Private Telefonnummern und E-Mail-Adressen sind vorhanden, um die Erreichbarkeit zu gewährleisten. Die Hochschulleitung sollte frühzeitig eingebunden werden oder es sollte ein übergeordneter Krisenstab (siehe Tag 1 in Abschnitt 3.1) einberufen werden. In den Gesprächen mit den betroffenen Hochschulen zeigte sich, dass zwar in der Regel Krisenpläne und Kontaktlisten vorhanden waren, diese aber im konkreten Krisenfall jedoch nicht abgerufen werden konnten (z. B. aufgrund des fehlenden IT-Zugangs), keine ausgedruckte Version vorhanden war oder die aufgeführten Ansprechpartner:innen nicht mehr an der Hochschule tätig waren.

b) Reaktionsphase

TAG 1

Um ein effektives Krisenmanagement während eines Cyber-Angriffs zu gewährleisten, empfiehlt es sich, neben dem IT-Kernteam einen separaten zentralen Krisenstab einzurichten. Durch diese Trennung wird die IT-Abteilung von Koordinations- und Kommunikationsaufgaben entlastet. Die Kommunikation ist ein entscheidender Faktor während eines Cyber-Angriffs, sowohl intern mit den Mitgliedern der Institution als auch extern mit staatlichen Behörden und Sicherheitsorganisationen. Um in dieser Phase optimal vorbereitet zu sein, müssen folgende Fragen (Auswahl) beantwortet werden:

- Wer ist Mitglied des IT-Kernteams, wer ist Mitglied des zentralen Krisenstabs?
- Welche Vertretungsregelungen gibt es?
- Welche Räumlichkeiten, einschließlich IT-Notfallversorgung, sind vorhanden?
- Welche externen Organisationen müssen informiert werden?

Es empfiehlt sich, die Situation offen und zeitnah zu kommunizieren. Klären Sie zunächst, welche Kommunikationskanäle noch verfügbar sind. Bei umfangreichen Angriffen können herkömmliche

Kommunikationskanäle wie E-Mail, Telefon, Intranet und Website nämlich ausfallen. Daher müssen alternative Kommunikationsmittel wie private E-Mail-Konten, Messenger-Dienste und soziale Medien genutzt werden. Darüber hinaus sollten alle Leitungspersonen umgehend informiert werden, damit sie die Entscheidungen der Krisenstäbe wirksam kommunizieren und Bedenken der Hochschulmitgliedern aufnehmen und weiterleiten können. Dies wirft mehrere Fragen auf, darunter:

- Ist eine externe Homepage bei Bedarf sofort verfügbar und wird sie laufend aktualisiert?
- Welche alternativen Kommunikationskanäle (z. B. Gruppenchats, Social-Media-Kanäle) sind verfügbar und können kurzfristig genutzt werden?

Je nach Schwere des Angriffs kann es notwendig sein, frühzeitig externe IT-Experten hinzuzuziehen, die bei der Abwehr, der forensischen Analyse oder der Wiederherstellung des IT-Systems helfen. Aufgrund des kurzfristigen Bedarfs an Fachwissen und Personal im IT-Bereich ist es wichtig, diese Punkte im Vorfeld zu klären.

- Welche Notfallunterstützung ist verfügbar? Gibt es bereits externe Dienstleistungsverträge oder kann im Rahmen der Zusammenarbeit der Institutionen Unterstützung eingeholt werden?
- Welche personellen Ressourcen sind in den Einrichtungen vorhanden, beispielsweise in den Fakultäten und Abteilungen, die zentral Unterstützung leisten können?

Zu berücksichtigen ist die überdurchschnittlich hohe Arbeitsbelastung insbesondere in den Bereichen IT und Kommunikation. Zudem können Ausfälle von IT-Systemen in anderen Bereichen der Hochschule den ordnungsgemäßen Betrieb von Abteilungen und Bereichen behindern. Daher kann es notwendig sein, Personal kurzfristig umzuverteilen, um den Betrieb der Hochschule unmittelbar nach einem Cyber-Angriff aufrechtzuerhalten.

Wenn die Angreifer Kontakt aufnehmen und ein Lösegeld fordern, sollten spätestens jetzt staatliche Stellen eingeschaltet werden. Lösegeldforderungen sollten nicht erfüllt werden, da dies die Finanzierung krimineller Aktivitäten unterstützt. Zudem gibt es keine Garantie, dass die Täter im Falle einer Zahlung die Entschlüsselung ermöglichen.

WOCHE 1

Nach einer ersten Bewertung des Cyber-Angriffs und seiner Folgen wird die Einführung eines laufenden Krisenmanagements auf der Grundlage zuvor festgelegter Maßnahmen und Verantwortlichkeiten empfohlen. Je nach Schwere des Angriffs kann es außerdem notwendig sein, zusätzliche Krisenstäbe für bestimmte Themen oder Abteilungen wie beispielsweise Fakultäten oder Standorte einzurichten. Das oberste Ziel besteht darin, eine transparente Krisenkommunikation und schnelle Entscheidungsprozesse zu etablieren, um die Handlungsfähigkeit zu wahren. Neben der Abwehr des Cyber-Angriffs ist es entscheidend, frühzeitig Entscheidungen über die Prioritäten für die Wiederherstellung der betroffenen Systeme festzulegen. Ein definierter Zeitplan kann helfen, zentrale Hochschulprozesse zu priorisieren. Die konkrete Umsetzung hängt von der Schwere des Angriffs und dem individuellen Krisenszenario und dem Zeitpunkt des Angriffs während des Semesters ab. In der Prüfungsphase können sich die Prioritäten deutlich von denen in der Immatrikulationsphase unterscheiden. Daher sind die folgenden Aspekte (Auswahl) zu berücksichtigen:

- Wie wirkt sich der Zustand der IT-Systeme auf die verschiedenen Statusgruppen der Hochschule aus? Wie können sie regelmäßig informiert werden?
- Welche Systeme sind betroffen und in welchem Umfang? Wie soll die Wiederherstellung der Systeme priorisiert werden?
- Welches Kerngeschäft sollte in der aktuellen Phase, in der sich die Hochschule befindet, priorisiert werden?

Es ist wichtig, rechtliche Fragen, wie beispielsweise eine mögliche Verletzung des Datenschutzes, zu berücksichtigen. Gemäß der geltenden Datenschutzbestimmung müssen die zuständigen Behörden innerhalb von 72 Stunden nach Bekanntwerden einer Sicherheitsverletzung informiert werden. Parallel dazu muss die Kommunikation kontinuierlich angepasst und aufrechterhalten werden. Wenn die internen Kommunikationsmittel nicht mehr zur Verfügung stehen, müssen im kritischsten Fall öffentliche Kanäle wie soziale Medien genutzt werden. Wenn es zu einem Erpressungsversuch kommt und die Angreifer die Situation weiter beobachten, kann jede öffentliche Kommunikation über den Vorfall äußerst sensibel sein und ebenfalls externe Unterstützung erfordern.

MONAT 1

In den ersten Wochen nach einem Cyber-Angriff ist es wichtig, das Ausmaß des Schadens zu bewerten und die betroffenen Systeme zu identifizieren. Es ist von entscheidender Bedeutung festzustellen, welche ausgefallenen Dienste ersetzt werden müssen und welche Aufgaben mit alternativen Mitteln bewältigt werden können. Für Hochschulen sind insbesondere die Ermöglichung von Bewerbungs- und Einschreibungsprozessen, die Durchführung von Prüfungen und die Verarbeitung von Zahlungen besonders wichtig. Eine kontinuierliche Priorisierung der anstehenden Aufgaben ist unerlässlich. Deshalb sind folgende Aspekte zu berücksichtigen:

- Welche Aufgaben sind für die Grundfunktion der Hochschule prioritär? Welche Aufgaben können aufgeschoben werden?
- Wie kann die Rückkehr zum Regelbetrieb gelingen?
- Welche Testläufe und Simulationen stehen zur Verfügung, um die Folgen einer Abschaltung oder eines Neustarts von Systemen abzuschätzen?

Unter bestimmten Umständen ist es möglich, die Datensicherung und die Wiederherstellung von IT-Systemen, wie beispielsweise Campus-Management-Systeme, aus Backup-Systemen im Vorfeld zu testen. In dieser Phase des Krisenmanagements ist es wichtig, ein Gleichgewicht zwischen der Notwendigkeit einer schnellen Wiederherstellung und der Bedeutung einer sicheren, wenn auch längeren Reorganisation der IT-Landschaft zu finden. Dabei ist nicht nur die Wiederherstellung der Systeme, sondern auch die langfristige Überwachung des Personalmanagement wichtig, um die zugrundeliegenden Folgen einer Cyber-Krise, wie Arbeitsüberlastung und Krisenerfahrung, zu ermitteln. Dies hängt mit dem Problem einer „wellenartigen“ Arbeitsbelastung zusammen, die sich noch verschlimmern kann, wenn offene Arbeitsstände nicht gelöst werden und Überstunden bzw. Überlastung nach der Rückkehr zum Normalbetrieb nicht abgebaut werden

können. Wie bei jeder Krisenerfahrung können auch hier langfristige, unterschwellige Folgen auftreten. Offene Fragen können hier u. a. sein:

- Welche Möglichkeiten zur Entlastung des Personals gibt es? Welche zusätzlichen Personalressourcen stehen zur Verfügung, um dies zu kompensieren?

Die Folgen eines Cyber-Angriffs können eine Reihe von Folgeschäden nach sich ziehen. Diese können sich beispielsweise auf den Forschungssektor auswirken, etwa durch die Nichtverfügbarkeit von Labors und die erschwerte Durchführung von Experimenten. Auch die Berichterstattung an Drittmittelgeber kann beeinträchtigt werden, wenn Daten nicht mehr verfügbar sind. Neben der Wiederherstellung der relevanten Daten, Berichtsformate oder Systeme ist es auch wichtig, mögliche Fristverletzungen und Folgemaßnahmen zu überwachen.

c) Normalisierungsphase

Ein Cyber-Angriff stellt sowohl für die Hochschule als Organisation als auch für alle Hochschulangehörigen eine einschneidende Krise dar. Während der Beginn eines solchen Angriffs meist klar definierbar ist, gestaltet sich die Rückkehr zum Normalbetrieb deutlich komplexer. Die Wiederherstellung erfolgt nicht einheitlich, sondern in unterschiedlichen Geschwindigkeiten und Intensitäten, je nachdem, welcher Bereich betroffen ist. Selbst wenn die zentralen IT-Systeme und Anwendungen bereits wieder funktionsfähig sind, können in anderen Bereichen weiterhin Beeinträchtigungen oder Folgeeffekte auftreten. Ein eindeutiger Abschluss der Krise lässt sich daher nur schwer bestimmen – vielmehr handelt es sich um einen graduellen Prozess der schrittweisen Normalisierung. Die Bewältigung der unterschwelligen Folgen der Cyber-Krise – wie Überlastung oder innere Kündigung – erfordert langfristige Personalmanagementmaßnahmen und die Betreuung der einzelnen Mitarbeitenden. Dies ist eine besondere Herausforderung in einem Umfeld, das bereits durch einen Fachkräftemangel gekennzeichnet ist. Bislang gibt es nur wenige Studien zu den Folgen eines Cyber-Angriffes (vgl. u. a. Northwave, 2022).

Die Krise durch den Cyber-Angriff sollte auch als Lernerfahrung genutzt werden. Neben der kurzfristigen Wiederherstellung der Handlungsfähigkeit bietet sie die Chance, die gesamte IT-Struktur und IT-Governance langfristig zu überdenken und neu zu organisieren. Je nach Schwere des Angriffs ist jedoch mit Widerständen zu rechnen, da die Krisenerfahrung auch zu einem Vertrauensverlust in die Bereiche IT und Digitalisierung führen kann. Zu berücksichtigen sind auch weitere Auswirkungen wie Vertrauensverlust bei Kooperationspartner:innen, Studierenden oder Studieninteressierte.

4 Zusammenfassung und weiteres Vorgehen

Die vorgestellten Fragen und Maßnahmen bieten einen ersten Überblick über das Thema, wobei der Fokus auf der Bewältigung eines Cyber-Angriffs liegt. Die Bedeutung von Prävention sowie technische Aspekte wie Netzwerksegmentierung, Backups oder Recovery-Strategien sind mindestens genauso wichtig. Sie standen jedoch nicht im Fokus der Untersuchung, da sich diese nicht an IT-Fachleute, sondern an die Hochschulleitung richtete. Dennoch haben die Interviews gezeigt, dass neben den technischen Aspekten auch die Vorbereitung auf das Krisenmanagement nach einem Cyber-Angriff wichtig ist. Auch wenn die Folgen eines solchen Angriffs

sehr unterschiedlich sein können und individuelle Krisenszenarien auftreten können, hat jeder Cyber-Angriff Konsequenzen für die Hochschule. IT-Sicherheit, Vorbereitung auf das Krisenmanagement und Stärkung der Resilienz sind daher neue, permanente Aufgaben für Hochschulen und deren Hochschulleitung. Hochschulen können bereits im Vorfeld Maßnahmen ergreifen, um ihre Widerstandsfähigkeit zu erhöhen. Die Weiterentwicklung des Business Continuity Managements (BCM) hilft dabei, alternative Prozesse für wichtige Abläufe zu definieren und Systeme entsprechend ihrer Relevanz für die Hochschule wiederherzustellen. Ein Notfallplan für die wichtigsten IT-gestützten Prozesse ist insbesondere in den Bereichen Studium und Lehre sowie in der zentralen Verwaltung unerlässlich. Zudem sollte die IT-Sicherheit als Daueraufgabe betrachtet werden. Die Ernennung eines Chief Information Security Officers (CISO) auf strategischer Ebene sowie von IT-Sicherheitsbeauftragten auf operativer Ebene kann bei der Entwicklung von IT-Sicherheitsrichtlinien, dem Aufbau eines Sicherheitsmanagementsystems und der Durchführung von Schutzbedarfsanalysen unterstützen. Von entscheidender Bedeutung ist es, das Bewusstsein und die Sensibilität für dieses Thema in der gesamten Hochschule zu schärfen und eine Kultur der Fehlermeldung zu fördern, in der das Melden von Sicherheitsvorfällen wertgeschätzt wird. Ein Cyber-Angriff ist eine Krise, die einen angemessenen Umgang seitens der Hochschule erfordert. Neben der Wiederherstellung der IT-Systeme und der organisatorischen Funktionalität muss die Hochschule auch das Krisenmanagement, das Personalmanagement, die Arbeitssicherheit und das Gesundheitswesen berücksichtigen.

***Dr. Harald Gilch** ist Senior-Berater und Projektmanager für HIS-HE, Hannover.*

***Dr. Maren Lübcke** ist Geschäftsbereichsleitung im Bereich Hochschulmanagement für HIS-HE, Hannover.*

***Dr. Mathias Stein** ist Berater und Projektmanager für HIS-HE, Hannover.*

Literatur:

Bundeskriminalamt (2023). Cybercrime. Bundeslagebild 2022. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2022.pdf?__blob=publicationFile&v=4 [18.07.2025].

Bundesministerium des Innern und für Heimat (2022). Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat. Ziele und Maßnahmen für die 20. Legislaturperiode. Berlin. https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.html [18.07.2025].

Crowdstrike (2023). Global Threat Report 2023. Der Bericht wird jährlich aktualisiert und veröffentlicht unter: https://www.crowdstrike.com/global-threat-report/ [18.07.2025].

Dreyer, M., Kühnlenz, F. & Brandel, B. (2023). Handreichung zur Vorbereitung auf Informationssicherheitsvorfälle. Herausgegeben durch den ZKI e. V. https://doi.org/10.5281/zenodo.10122533 [18.07.2025].

Gilch, H., Lübcke, M. & Stein, M. (2023) Krisenmanagement nach Cyber-Angriffen – Handlungsempfehlungen. Hannover: HIS-HE. https://medien.his-he.de/publikationen/detail/krisenmanagement-nach-cyber-angriffen-handlungsempfehlungen [18.07.2025].

Hochschulrektorenkonferenz (HRK) (2018). Informationssicherheit als strategische Aufgabe der Hochschulleitung. Empfehlungen der 25. Mitgliederversammlung der HRK am 06. November 2018 in Lüneburg. https://www.hrk.de/fileadmin/redaktion/hrk/02-Dokumente/02-01-Beschluesse/HRK_MV_Empfehlung_Informationssicherheit_06112018.pdf [18.07.2025].

Kost., M., Loibl, B., Reuter, P. & Stenke, M. (2022). #JLUoffline. Der Cyber-Angriff auf die Justus-Liebig-Universität Gießen im Dezember 2019. ABI Technik, 42(1), 43-54. https://doi.org/10.1515/abitech-2022-0005 [18.07.2025].

Northwave (2022). After the crisis comes the blow - the mental impact of ransomware attacks. https://26168787.fs1.hubspotusercontent-eu1.net/hubfs/26168787/Northwave-Research-After-the-crisis-comes-the-blow-The-mental-impact-of-ransomware-attacks-1.pdf [18.07.2025].

ZKI e. V. (Hrsg.) (2022). IT-Grundschutz-Profil für Hochschulen. Berlin. https://www.zki.de/fileadmin/user_upload/Downloads/IT_Grundschutz_ZKI_2022_Final.pdf [18.07.2025].

Josef von Helden, Isabel Kassel: Lessons Learned aus dem Cyber-Angriff auf die Hochschule Hannover

„Die Frage ist nicht, ob wir ‚erfolgreich' angegriffen werden, die Frage ist nur, wann."

1 Die Hochschule Hannover

Die Hochschule Hannover (HsH) bietet an fünf Standorten in Hannover über 60 Studienangebote verschiedenster Fachrichtungen in fünf Fakultäten an. Mit etwa 9.000 Studierenden, 290 Professuren, rund 640 Mitarbeiter:innen sowie ca. 460 Lehrbeauftragten ist die HsH die drittgrößte Hochschule für Angewandte Wissenschaften in Niedersachsen. Die technische Infrastruktur wird in einer Mischung aus zentralen und dezentralen Angeboten in den Fakultäten betrieben. Sie ist damit geprägt durch eine große Heterogenität in Software und Hardware. Im Vergleich zu einem stark zentralisierten IT-Betrieb ist damit auch die Komplexität im Umgang mit einem Cyberangriff deutlich erhöht.

2 Anatomie des Cyber-Angriffs auf die Hochschule Hannover

Der Angriff auf die HsH wurde am Montag, den 30. Oktober 2023 entdeckt – einem sogenannten Brückentag, da der 31.10. in Niedersachsen ein Feiertag ist. Die späteren forensischen Analysen ergaben, dass der Angriff bereits am Abend des 27.10.2023 (einem Freitag) gestartet wurde, als ein unberechtigter Zugriff über den VPN-Zugang eines Hochschul-Accounts erfolgte. Am Samstag, den 28.10.2023 wurden die Rechte eines Domain-Admins erlangt und am Abend des 29.10.2023 (Sonntag) wurde mit der Verschlüsselung des Domain Controllers (DC) begonnen. Im schlechtesten Fall hätte es durch den Brückentag also passieren können, dass der Angriff erst am Mittwoch, 01.11.2023 entdeckt worden wäre.

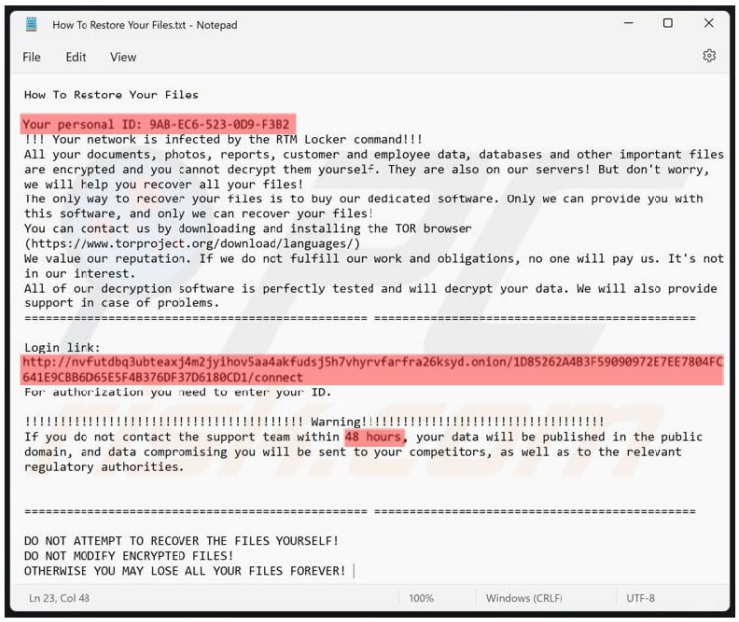

Abbildung 4: Information der Angreifer

Bei dem Angriff handelte es sich primär um eine Verschlüsselung des DC; der Einsatz von sich selbst verbreitender Schadsoftware konnte später nicht festgestellt werden. In den eingeschleusten Datenbeständen fand sich jedoch eine Textdatei „How to Restore Your Files" mit dem Hinweis, dass die (gestohlenen) Daten innerhalb von 48

Stunden veröffentlicht werden, wenn keine Kontaktaufnahme mit den Angreifern erfolgt. Der Angriff wurde von der RTM-Locker-Gruppe durchgeführt, die sich von Beginn an als Verursacher zu erkennen gab.

Die Entscheidung, wie mit diesem Erpressungsversuch umgegangen werden soll, musste erfolgen, ohne zu wissen, was genau die Angreifer tatsächlich im System beschädigt hatten und welche Art von Daten ggf. abgeflossen waren. Die HsH entschied sich, so schnell wie möglich alle Server der Hochschule vom Netz zu nehmen, um eine zu befürchtende Ausbreitung von Schadcodes einzudämmen. Der Angriff hatte somit weitreichende Folgen für die fünf Fakultäten sowie die gesamte zentrale Verwaltung. Nahezu alle digitalen Kommunikations- und Arbeitsprozesse waren blockiert und grundlegende Funktionen waren betroffen, was zu erheblichen Einschränkungen für Studierende und Mitarbeiter:innen führte.

3 Umgang, Auswirkungen und Herausforderungen

3.1 Erste Schritte und Herausforderungen

Das Herunterfahren der Server bzw. die Trennung vom Netz hatten zur Folge, dass eine ganze Reihe von Systemen, die für den Ablauf alltäglicher Prozesse sowie für die Kommunikation innerhalb der Hochschule zentral sind, nicht mehr zur Verfügung standen. Betroffen waren insbesondere

- die gesamte E-Mail-Kommunikation,
- VoIP-Telefonie,
- das Intranet,
- die Lehr- und Lern-Plattform Moodle,
- die Zugänge zu Diensten der GWDG (z. B. academic cloud),
- EvaSys/EvaExam (zur Durchführung von Umfragen, Evaluationen und Prüfungen),
- die Erstellung der Campus Card für Studierende bzw. von Dienstausweisen,
- die Nutzung der Netzwerkdrucker,
- die Zeiterfassung,
- das Backup von Dateien,
- der VPN-Zugang sowie
- die Zugänge zu SAP und HIS-Produkte.

SAP sowie die HIS-Produkte selbst waren nicht betroffen, da diese auf externen Servern und nicht von der Hochschule selbst betrieben werden. Hier waren lediglich die Zugänge nicht mehr verfügbar.

Parallel dazu funktionierten eine Reihe von Systemen – teilweise aber mit Einschränkungen – weiter. Dies waren insbesondere die Webseiten der HsH, die Strom- und Klimatechnik, die Zugänge zu den Räumen und Gebäuden, WLAN inkl. eduroam, Teams, Zoom sowie der Zugriff auf die Rechner mit lokalem Profil.

Zur Bewältigung der Krise wurden zunächst ein strategischer und ein operativer Krisenstab eingerichtet.

Der strategische Stab bestand aus Mitgliedern des Präsidiums, Kolleg:innen aus den Bereichen Kommunikation und Marketing, einem Sprecher des operativen Krisenstabs sowie externen Kolleg:innen, die

die HsH mit ihrer Fachexpertise unterstützten. Zentrale Aufgabe dieses Krisenstabes war die strategische Steuerung und die Kommunikation ohne Zugriff auf die regulären Instrumente zur Kommunikation innerhalb der Organisation.

Ein zweiter (operativer) Krisenstab bestand aus einer Person aus der Leitung der Hochschul-IT, Mitarbeiter:innen aus der Personal- und Organisationsentwicklung der HsH sowie 4 Kolleg:innen aus unterschiedlichen Hochschulen und Wissenschaftseinrichtungen – eine zentrale Unterstützung, die kurzfristig durch das LANIT[21] ermöglicht wurde. So standen schnell zusätzliche Personen mit Fachexpertise und Projektmanagement-Skills zur Verfügung, die wesentlich zur erfolgreichen Steuerung der ersten Schritte nach dem Angriff beitrugen.

Zu diesen ersten Schritten gehörten die Schadensanalyse und die forensische Analyse aller Systeme der Hochschule. Parallel dazu begannen Maßnahmen zur Kommunikation nach innen und außen und zur Priorisierung der nächsten Schritte. Neben den (externen) Meldungen an die Polizei, den Verfassungsschutz, das Niedersächsische Ministerium für Wissenschaft und Kultur und den Datenschutz musste vor allem die (interne) Kommunikation neu organisiert werden. Insbesondere der Wiederherstellung der Kommunikationskanäle wurde hohe Priorität eingeräumt und eine erste Notfall-Website sowie alternative Kommunikationskanäle eingerichtet. Neben den weiter verfügbaren Social-Media-Kanälen gehört hierzu der Aufbau von Gruppen-Chats über den Messenger-Dienst „Signal“ sowie innerhalb weniger Tage die Errichtung eines speziellen Bereichs auf der Internet-Seite der Hochschule. Dieser wurde später kontinuierlich mit FAQs ausgebaut, um so den Informationsfluss zu den Studierenden und den Beschäftigten sicherzustellen.

Durch das Umsteigen auf einen cloudbasierten Dienst standen nach nur 10 Tagen die persönlichen E-Mail-Adressen der HsH für Beschäftigte und Studierende wieder zur Verfügung. Der Versand von Massen-E-Mails zur schnellen Information für viele war jedoch noch über Wochen nur mit enormem Aufwand möglich, da Funktionsadressen, Aliase und Verteilerlisten kurzfristig noch nicht wieder eingerichtet werden konnten.

Zur Beantwortung von technischen und praktischen Fragen zum Cyber-Angriff allgemein, und zur Wiedereinrichtung von Diensten im Speziellen, konnten innerhalb der ersten beiden Wochen zudem ein zentraler Helpdesk aufgebaut werden, bei dem zahlreiche Kolleg:innen aus der gesamten HsH einsprangen, um Fragen per E-Mail individuell zu beantworten.

Die Wiederherstellung bzw. der Neuaufbau von Diensten blieb dabei nicht ohne Widerstände und Rückschläge. Die Einrichtung neuer Accounts, einer neuen Accountverwaltung sowie einer Multi-Faktor-Authentifizierung für mehr als 11.000 Accounts stellte für die IT und für die Beschäftigten einen massiven Kraftakt dar, der noch dazu ohne Vorbereitung und erst mit zeitlicher Verzögerung mit begleitenden Schulungen durchgeführt werden konnte. Zudem musste für die Umsetzung der Multi-Faktor-Authentifizierung auf private Telefone zurückgegriffen werden, da die dienstlichen Telefone nicht oder nur eingeschränkt zur Verfügung standen. Der Datenzugriff auf Gruppenlaufwerke konnte zwar relativ schnell

[21] Landesarbeitskreis Niedersachsen für Informationstechnik/Hochschulrechenzentren (LANIT) https://www.lanit-hrz.de/ [18.07.2025].

wiederhergestellt werden, war jedoch nur aus dem Netzwerk der Hochschule möglich, nicht aus dem Home Office. Auch gab es vereinzelte Rückschläge wie Datenverluste auf einzelnen Laufwerken.

Herausforderungen waren neben dem Wiederaufbau der Kommunikationskanäle und der Priorisierung insbesondere die Härtung der relevanten Systeme sowie die Krisenorganisation für Aufbau- und Ablauforganisation der Hochschule. Für die forensische Analyse des Angriffs und die Härtung der betroffenen Systeme wurde dabei auf externe Unterstützung zurückgegriffen. Diese lief parallel zu den Wiederaufbauarbeiten und für die Mehrheit der Beschäftigten und Studierenden unbemerkt. Für die Frage, welche Systeme neu aufgestellt und welche ggf. wieder aus den Back-ups an den Start gebracht werden können, waren die Ergebnisse jedoch von zentraler Bedeutung. Mit wachsender Sicherheit, dass „nur“ ein Domain Controller (DC) verschlüsselt worden war und so gut wie keine Daten abgeflossen waren, wuchs das Vertrauen darin, die Krise relativ schnell überwinden zu können. Wichtiger Meilenstein war die Erkenntnis, dass auf einem nicht am Netz befindlichen Server noch eine Back-up Kopie des DC vorhanden war, die zur Wiederherstellung der Zugänge genutzt werden konnte.

Als erstes Zwischenziel wurde somit die Erreichung eines stabilen Notbetriebs bis Ende des Jahres 2023 ausgegeben.

3.2 Der Weg zum stabilen Notbetrieb und zum „Normalbetrieb“

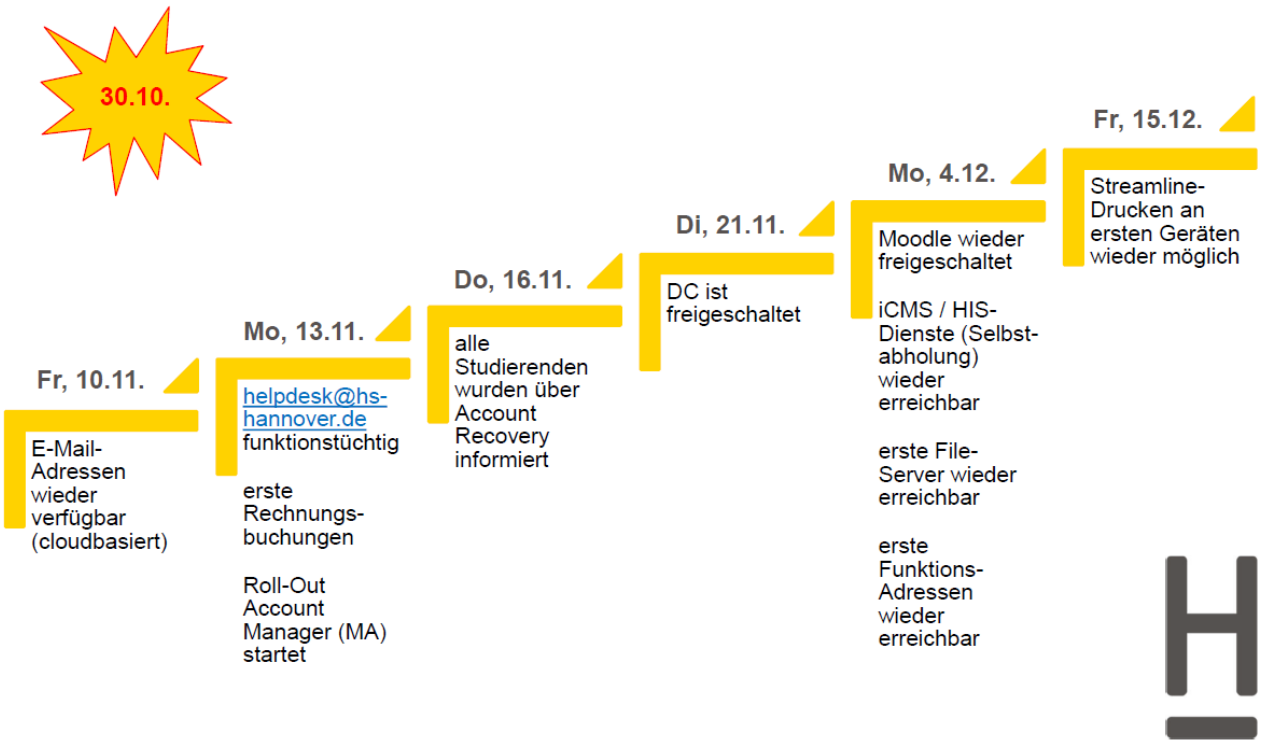

Abbildung 5: Der Weg zum stabilen Notbetrieb

Aufbauend auf Planungen um Umsetzungen zur Erreichung eines stabilen Notbetriebs erfolgten parallel die Planungen für einen neuen „Normalbetrieb“. Für die in Abbildung 5 aufgezeigten Teilschritten und Erfolge

waren eine Reihe von Arbeiten und Abstimmungen im Hintergrund notwendig. So handelt es sich beispielsweise beim Wechsel zu einem cloudbasierten Dienst für den Aufbau der E-Mail-Kommunikation um eine zustimmungspflichtige Organisationsmaßnahme, die schnell und ohne die sonst üblichen ausführlichen Beratungen und Vorbereitungen getroffen werden musste.

Während an vielen Stellen also schnell Erfolge erzielt wurden und zentrale Dienste bis Ende 2023 wieder verfügbar waren, zeigten sich praktische Auswirkungen noch bis weit ins Jahr 2024. Exemplarisch kann hier das Thema Campus Card bzw. Dienstausweis herangezogen werden. Neuausstellungen oder Änderung bei Campus Card und Dienstausweisen waren auch zum Start des Sommersemesters 2024 noch nicht automatisiert möglich. Dies führte z. B. dazu, dass Studierende auf anderem Weg nachweisen mussten, dass sie eingeschrieben sind und den Beitrag für den Verkehrsverbund gezahlt hatten. Für neue Kolleg*innen musste u. a. die Zugangsberechtigung zu Büroräumen händisch bearbeitet werden.

Abbildung 6 gibt einen Überblick über die weiteren Meilensteine zur Erreichung des neuen „Normalbetriebs“.

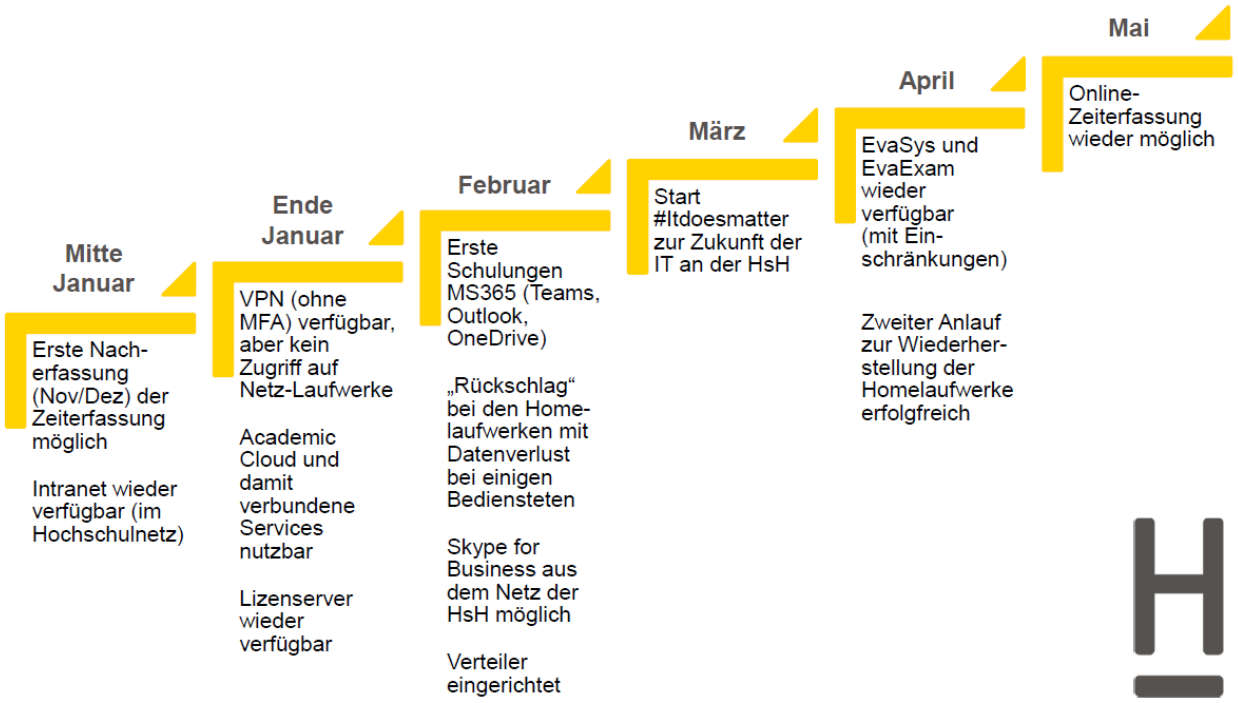

Abbildung 6: Der Weg zum neuen "Normalbetrieb" 2024

4 Lessons Learned

Der Angriff machte vor allem deutlich, wie wichtig eine funktionierende Krisenorganisation und ein klares Krisenhandbuch sind. Auch die Abhängigkeiten zwischen den verschiedenen Diensten und die Bedeutung einer dezentralen, aufeinander abgestimmten redundanten IT-Struktur wurde mit jedem Dienst, der wiederhergestellt oder neu aufgesetzt werden sollte, deutlicher. Last but not least hat sich gezeigt, dass die Resilienz sowohl einzelner Beschäftigter, also auch der verschiedenen Organisationseinheiten, unterschiedlich stark ausgeprägt ist. Im Einzelnen lassen sich für die Bereiche Kommunikation und

Organisation, aber auch für das Land Niedersachsen, die auf den folgenden Seiten näher beschriebenen Erkenntnisse ableiten.

4.1 Lessons Learned – Kommunikation

Die interne und externe Kommunikation war entscheidend für die Aufrechterhaltung des Vertrauens und die Koordination der Wiederherstellungsprozesse. Aufgrund des Ausfalls der E-Mail-Kommunikation mussten alternative Kanäle geschaffen werden. Die Notfall-Website bzw. schnell auch wieder der eigentlichen Internet-Auftritt der HsH und ein zentraler Helpdesk erwiesen sich als wertvolle Ressourcen für die Bereitstellung von Informationen und die Bündelung von Anfragen. Da die sonstigen Kommunikationskanäle ausgefallen waren, mussten alternative Wege gefunden werden, um insbesondere eine „Massenkommunikation ohne Verteiler“ zu ermöglichen.

Ein weiterer zentraler Aspekt in der Kommunikation sind die notwendigen Übersetzungsleistungen. Zum einen sollten die Informationen zumindest ins Englische oder in andere notwendige Sprachen übersetzt werden. Zum anderen bedarf es einer „Übersetzung“ zwischen IT und den Anwender:innen, um die in technischer Sprache ausgedrückten Informationen in allgemein verständliche Informationen sowie in praktisch anwendbare Handlungsanweisungen für die Anwender:innen zu „übersetzen“. In diesem Sinne ist es besonders wichtig, darauf zu achten, was von technischer Seite nicht gesagt wurde, da es als Selbstverständlichkeit gesehen wird – und auch daraus allgemein verständliche Handlungsanweisungen für Anwender:innen ohne IT-Kenntnisse zu formulieren. Dies zeigte sich an der HsH beispielhaft am lange fehlenden Back-up neu erstellter Dateien nach dem Cyber-Angriff. So lange Dienste und Dateien aus Back-up Servern wiederhergestellt werden, können dort keine neuen Back-ups erstellt werden – für IT-ler:innen eine Selbstverständlichkeit, für Anwender:innen über einige Zeit ein trügerisches Sicherheitsgefühl.

Zusammenfassend hat der Vorfall aufgezeigt, wie wichtig eine klare, transparente und verständliche Kommunikation im Krisenfall ist. Dies gilt einerseits für die interne Kommunikation, andererseits für die externe Kommunikation mit Partnerorganisation der Hochschule sowie mit einzelnen externen Projektbeteiligten. Als gute Vorbereitung für einen solchen Krisenfall empfiehlt es sich sehr, alternative Kommunikationskanäle präventiv einzurichten und vorzuhalten.

4.2 Lessons Learned – Organisation

Auch für die Organisation und Verwaltung der Hochschule konnten Lehren aus dem Cyber-Angriff gezogen werden. So wurde die Notwendigkeit eines sofort einsetzbaren Notfall- oder Krisenhandbuchs offenkundig, das im Kern über Informationen darüber verfügt, wer innerhalb der Hochschule was tut und wer was tun darf, wie Entscheidungsträger:innen erreichbar sind, welche Meldeketten einzuhalten sind oder welche Alternativen für verschiedenen Szenarien offenstehen. Außerdem ist eine Darstellung der für die Hochschule wichtigsten Services und Dienste inkl. einer Priorisierung zur Wiederherstellung der Verfügbarkeit wichtig. Die Priorisierung kann dabei in Abhängigkeit des Zeitpunkts eines Angriffs bzw. des Wiederaufbaus variieren, z. B. Prüfungs-, Bewerbungs- oder Einschreibezeitraum sowie Semesterbeginn. Ein Krisenhandbuch sollte hier für unterschiedliche Szenarien angepasste Maßnahmen ausweisen.

Weiterhin sollten Kernprozesse priorisiert und für unverzichtbare Kernprozesse möglichst Alternativen vorgehalten werden. Im Zuge des Cyber-Angriffs hat es sich etwa als sehr vorteilhaft erwiesen, dass einzelne Dienste extern betrieben werden (insbesondere SAP, HIS, Gehaltsabrechnung).

Zur Vermeidung von Verzögerungen sollte auch die Möglichkeit ausgebaut werden, Verbünde mit anderen Hochschulen einzugehen (vgl. Hilfestellung durch den LANIT für die HsH, Kapitel 4.3). Da gerade für kleinere Hochschule nicht alle Dienstleistungen und Szenarien mit hinreichend Personal hinterlegt werden können, besteht die Gefahr von Kopf-Monopolen. Gemeint sind einzelne Beschäftigte, bei denen bestimmte Aufgaben und Kenntnisse zusammenfließen, so dass diese im Notfall wie ein Flaschenhals wirken, der schnell verstopft und ein schnelles Handeln behindert.

Ebenso sind die regelmäßige Sensibilisierung und Schulung der Mitarbeiter:innen im Bereich IT-Sicherheit unerlässlich. Die Hochschule Hannover hat nach dem Angriff beschlossen, ihre Sicherheitsstandards weiter zu erhöhen, eine Multi-Faktor-Authentifizierung für zentrale Dienste einzuführen und die Nutzer:innen regelmäßig zu sensibilisieren. Diese Maßnahmen sollen das Risiko des „Erfolgs“ von Cyber-Angriffen langfristig minimieren.

Mit Blick auf die Organisation Hochschule hat sich außerdem gezeigt, dass nicht nur die Betroffenheit, sondern insbesondere die Resilienz der einzelnen Bereiche sehr unterschiedlich war. Viele Bereiche haben erfinderisch und effizient auf die Herausforderungen reagiert, einige wenige waren durch den Cyber-Angriff zunächst wie gelähmt, wieder andere waren bereits nach kurzer Zeit zurück im „Normalbetrieb“. Die Belastung war also sehr unterschiedlich. Den Führungskräften in der Organisation kommt dabei die Aufgabe zu, die (Über-)Beanspruchung rechtzeitig zu erkennen und bei Bedarf entsprechende Unterstützung anzubieten bzw. einzufordern. Dies kann sowohl eine Organisationseinheit und ihre Aufgaben insgesamt betreffen als auch einzelne Beschäftigte und deren individuelle Gesunderhaltung.

Last but not least lassen sich für die IT-Organisation und IT-Architektur klare Erkenntnisse gewinnen. So sind die Erstellung und Pflege eines Notfallhandbuches speziell für die IT-Organisation unerlässlich. Hierbei ist insbesondere der Umgang mit Intrusion Detection und Intrusion Prevention zu überprüfen und bei Bedarf auszubauen. Auch Abhängigkeiten zwischen verschiedenen Diensten sind zu klären und zu berücksichtigen, um diese Abhängigkeiten für einen ggf. notwendigen Wiederaufbau entsprechend berücksichtigen zu können. Für die übergreifende IT-Architektur der Hochschule ist es wichtig, die gesamte Hochschul-IT gemeinsam zu betreiben und dabei in einer verteilten IT-Architektur zentral und dezentral betriebene IT-Systeme und deren Verantwortlichkeiten zu definieren und zu dokumentieren. Die Vor- und Nachteile verschiedener Ausprägungen einer verteilten IT-Architektur sind zu analysieren und entsprechend umzusetzen bzw. anzupassen. Redundanzen sollten systematisch und gezielt aufgebaut werden, um das Risiko eines Totalverlusts kritischer Daten und Dienste zu minimieren bzw. Datenverluste zu vermeiden.

4.3 Lessons Learned – Niedersachsen

Die beiden Krisenstäbe der HsH wurden von externe Kolleg:innen unterstützt, die vor allem über den LANIT kurzfristig als Unterstützung gewonnen werden konnten. Gerade die Zusammenarbeit und die Abrufbarkeit von Expert:innen innerhalb des LANIT haben sich als großes Plus in der Krisenbewältigung erwiesen.

Zukünftig sollte die enge Zusammenarbeit der niedersächsischen Hochschulen in diesem Bereich noch besser strukturiert werden. Finanziert mit Mitteln aus Hochschule.digital Niedersachsen[22] wird 2024/2025 das Verbundprojekt „Sicherung der Resilienz“ zur Stärkung der IT-Sicherheit der niedersächsischen Hochschulen mit einem Volumen von rund 10 Mio. € auf den Weg gebracht. Parallel dazu wird ein gemeinsamer IT-Strategieprozess durchgeführt und es sollen sinnvolle landesweite bzw. länderübergreifende IT-Strukturen und Services entwickelt werden.

5 Fazit

Cyber-Angriffe können nicht vollständig verhindert werden, eine gute Vorbereitung auf verschiedene Szenarien ist jedoch möglich – und unerlässlich, um den Schaden zu minimieren. Der Cyber-Angriff auf die HsH und seine Folgen haben deutlich gemacht, dass IT-Sicherheit und Krisenmanagement dynamische Aufgaben sind, die einer kontinuierlichen Weiterentwicklung und Schulung bedürfen. Eine Aufgabe, die am besten gemeinsam gelöst werden kann. Nur durch ein proaktives, resilient aufgestelltes IT- und Krisenmanagement sowie durch enge Kooperation und Wissensaustausch können Hochschulen den Herausforderungen durch Cyber-Bedrohungen effektiv begegnen.

Hochschulen müssen – wie andere Organisationen auch – die Vorbereitung auf Cyber-Angriffe als Daueraufgabe anerkennen und entsprechend agieren.

Denn: Nach dem Angriff ist vor dem Angriff.

Prof. Dr. Josef von Helden *ist Präsident der Hochschule Hannover.*

Isabel Kassel *ist Referentin Personal- und Organisationsentwicklung in der Stabsabteilung Strategische Hochschulentwicklung (S1) der Hochschule Hannover*

[22] https://hochschuledigital-niedersachsen.de/home/ [18.07.2025].

Lisa Dittrich: Krisenkommunikation im Ernstfall. Cyberattacke auf die Universität Gießen

Die Ersten zu sein – gerade bei einer so existenziellen Krise, wie wir sie erlebt haben – hat Vor- und Nachteile. Vor mittlerweile fünf Jahren wurde die Justus-Liebig-Universität Gießen (JLU) von einer Cyberattacke getroffen, die es in diesem Ausmaß an einer großen deutschen Universität zuvor noch nicht gegeben hatte. Der Nachteil: Es gab keine Vorbilder, an denen wir uns orientieren konnten. Und was es wirklich bedeuten würde, als Universität über Wochen offline zu sein, konnten wir zu Beginn nicht wissen. Der Vorteil: Einen ausgeklügelten Schritt-für-Schritt-Notfallplan für genau diesen Fall hat auch niemand von uns erwartet. Anscheinend ist uns der Umgang mit der Krise aber trotzdem gelungen – zumindest werden wir seitdem sehr oft darum gebeten, unsere Erfahrungen zu teilen.

Am Sonntag, 8. Dezember 2019, mitten in der besinnlichen Adventszeit, fielen in den Tierkliniken der Universität, wo auch am Wochenende gearbeitet wird, Unregelmäßigkeiten in den Datenbanken auf. Dann ging alles sehr schnell: Das Hochschulrechenzentrum wurde informiert, als Ursache der Unregelmäßigkeiten ein Verschlüsselungstrojaner ausgemacht, der auch auf anderen Systemen aktiv ist und in Absprache mit dem Präsidium die JLU vollständig vom Netz getrennt. Alle Systeme wurden kontrolliert heruntergefahren. Das war der Startschuss für #JLUoffline, die Cyberattacke auf die Universität Gießen. Dank der schnellen Reaktion der JLU konnte das Schlimmste – nämlich Verluste von Forschungsdaten, Noten oder Verwaltungsdokumenten – verhindert werden. Erst einige Tage später sollte sich im Zuge der Ermittlungen des Landeskriminalamts herausstellen, dass die JLU Opfer einer bis dahin unbekannten Variante der Schadsoftware Ryuk geworden war.

Der Krisenstab aus Präsidium, Hochschulrechenzentrum, Pressestelle und Verwaltung – umgehend vom Präsidenten einberufen – nahm noch am selben Abend seine Arbeit auf. Die ersten Meldungen auf Twitter und Instagram wurden gegen 22.30 Uhr veröffentlicht.

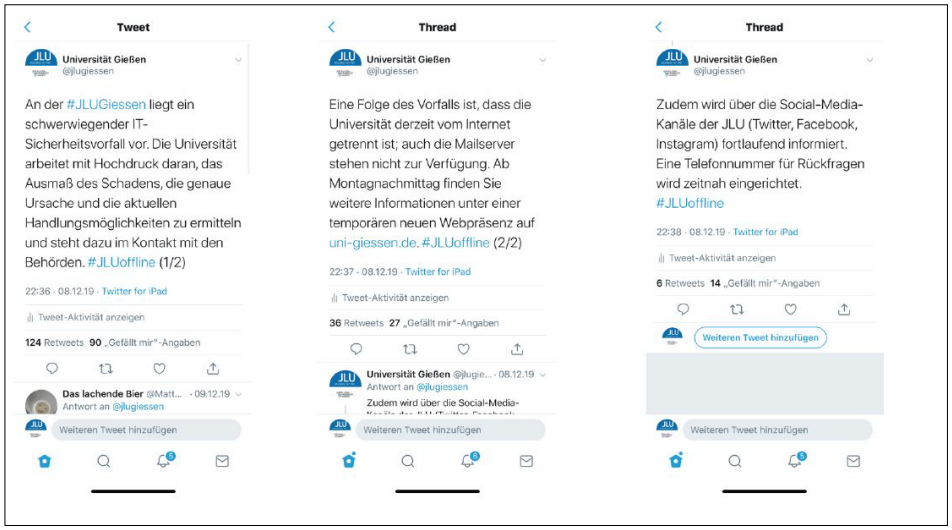

Abbildung 7: Die ersten Meldungen zu #JLUoffline bei Twitter

Von Anfang an war klar: Mit Ursachenforschung konnte sich der Krisenstab nicht lange aufhalten – vor allem galt es, den Lehr-, Forschungs- und Verwaltungsbetrieb im Wintersemester aufrechtzuerhalten. Dafür war eine transparente und schnelle Kommunikation essenziell.

Bereits am Montag, 9. Dezember 2019, konnte die erste Pressemitteilung über einen rudimentär wiederhergestellten Presseverteiler verbreitet werden – mangels Dienstrechnern über iPads, private Handys und eigenes Datenvolumen. Es gab einen O-Ton des Präsidenten vor Kameras, eine temporäre Homepage und alternative E-Mail-Adressen für die Kernbereiche. Die JLU-Mitglieder wurden zu einer ersten Infoveranstaltung am 10. Dezember 2019 eingeladen. Wichtigstes Kommunikationstool für interne Abstimmungsprozesse innerhalb des Krisenstabs war eine eigens eingerichtete Messenger-Gruppe.

Abbildung 8: Erster O-Ton des damaligen JLU-Präsidenten Prof. Joybrato Mukherjee am 9. Dezember 2019 (Foto: JLU/Charlotte Brückner-Ihl)

Abbildung 9: Hotline für Rückfragen der JLU-Mitglieder (Foto: JLU/Katrina Friese)

Eines der wichtigsten Ziele des #JLUoffline-Krisenmanagements: Das Kernteam im Hochschulrechenzentrum sollte sich ganz auf den Wiederaufbau konzentrieren können. Die IT-Beschäftigten wurden nicht von Kamerateams behelligt und auch nicht für Interviews vermittelt. Neben der Schadensbekämpfung hatte die transparente Krisenkommunikation oberste Priorität – das Präsidium hatte schnell erkannt, dass verlässliche und schnelle Informationen für die Stimmung unter den JLU-Mitgliedern und damit für die Resilienz der

Universität zentral waren. Ermöglicht wurde dies durch kurze Entscheidungswege und eine Krisenstabsstruktur, die gleichzeitig eine Abschirmung des IT-Kernteams und einen permanenten Austausch zwischen Präsidium, Hochschulrechenzentrum und Pressestelle sicherstellte (Abbildung 10). Nach der Akutphase im Dezember wurde der Krisenstab nach und nach um weitere universitäre Einrichtungen erweitert. Während gerade zu Beginn schnelle Entscheidungen und schlanke Strukturen unerlässlich waren, wurde es im weiteren Verlauf immer wichtiger, die verschiedenen JLU-Einrichtungen und Statusgruppen aktiv in Entscheidungen einzubinden.

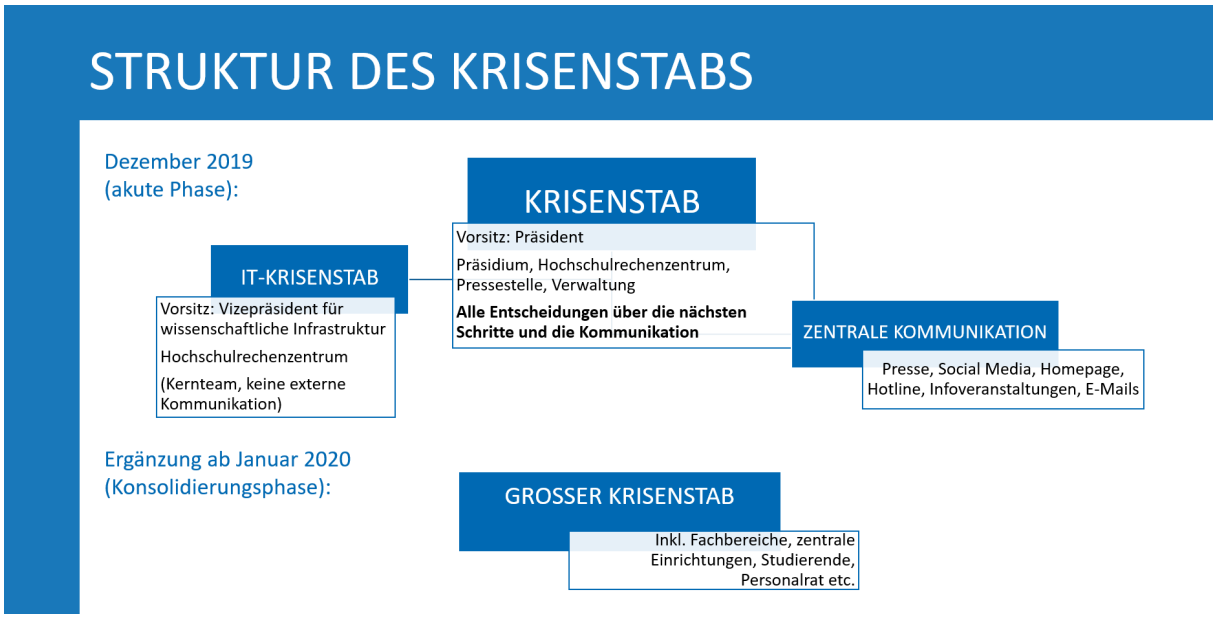

Abbildung 10: Struktur des #JLUoffline-Krisenstabs (Grafik: JLU/Lisa Dittrich)

Erstes Ziel des Krisenstabs war es, die Kommunikationsfähigkeit der Studierenden und Beschäftigten wiederherzustellen. Die Passwörter aller über 35.000 Studierenden und Beschäftigten wurden zuvor zurückgesetzt und mussten in einer bemerkenswerten Verteilaktion, die es sogar in die internationalen Medien wie BBC und NY Times schaffte, persönlich abgeholt werden, bevor das Mailsystem wieder genutzt werden konnte (Abbildung 11). Nach und nach folgten weitere Komponenten wie die Homepage, FlexNow, Stud.IP oder die digitalen Systeme der Universitätsbibliothek. Mitte Januar 2020 konnten die Studierenden wieder über WLAN ins Netz; die Beschäftigten hatten einige Tage später wieder Zugriff auf Eduroam. Besonders viel Geduld war bei der Wiederherstellung der Netzlaufwerke gefragt: Der Angriff hatte zwar nicht zu Datenverlusten geführt, allerdings musste das System der Nutzerberechtigungen ganz neu aufgebaut werden.

Abbildung 11: Abholung der neuen Passwörter (Foto: JLU/Katrina Friese)

Die Kosten des Cyberangriffs beliefen sich bis Mitte Mai 2020 nach einer Erhebung der Verwaltung in den insgesamt 50 Organisationsbereichen der JLU auf rund 1,7 Millionen Euro. Auch unabhängig von den finanziellen Konsequenzen hat die Krise den Studierenden und Beschäftigten sehr viel abverlangt. Dabei wurde schmerzlich bewusst, wie abhängig eine moderne Universität von einer funktionierenden digitalen Infrastruktur ist.

#JLUoffline war aber gleichzeitig gekennzeichnet von einer großen Bereitschaft, mit Pragmatismus, Einfallsreichtum und auch Galgenhumor das Beste aus der Situation zu machen. So hatte etwa die Universitätsbibliothek die alte Zettelausleihe wiederbelebt, und die Lehrenden stellten wie in den 90er-Jahren Semesterapparate zum Kopieren für die Studierenden bereit. Unzählige Hilfsangebote auch der anderen hessischen Universitäten wirkten zusätzlich belebend. Der Umgang mit der Krise war geprägt von einer konstruktiven und pragmatischen Stimmung, Shitstorms blieben aus. Wichtig an dieser Stelle: Die Corona-Pandemie begann erst nach #JLUoffline. Wenn die Cyberattacke nach den zahlreichen Krisen der letzten Jahre auf eine erschöpfte Universitätsgemeinschaft getroffen wäre, wären sicher noch ganz andere Herausforderungen auf das Krisenmanagement zugekommen.

Abbildung 12: Pragmatische Lösung: Wiederbelebung der alten Zettelkästen in der Universitätsbibliothek
(Foto: JLU/Katrina Friese)

Trotzdem gehen wir davon aus, dass die transparente Kommunikation zu dem Wir-Gefühl während der Krise beigetragen hat. Da gerade am Anfang nur die Social-Media-Kanäle der JLU und die temporäre Homepage für die Kommunikation mit den Beschäftigten zur Verfügung standen, mussten wir zwangsläufig in aller Öffentlichkeit die relevanten Details kommunizieren. Die Homepage stellte Informationen auf Deutsch und Englisch bereit und verfügte über eine stetig aktualisierte FAQ-Liste. Die bereitgestellten Informationen hatten absolut verlässlich zu sein, und wir mussten Widersprüche und Unklarheiten unverzüglich aufklären. Dabei galt es, sich auf Wesentliches zu konzentrieren: Social-Media-Kommentarspalten (etwa auf Facebook) erwiesen sich gerade im späteren Verlauf und bei dünner Personaldecke eher als Zeitfresser und als Risiko für das Aufkommen von Fehlinformationen. Daher haben wir diese Aktivitäten mit der Zeit deutlich eingeschränkt und verstärkt auf Instagram-Stories als Kommunikationsformat gesetzt. Nachdem die E-Mails wieder funktionierten, konnten wir die Betroffenen zudem mit internen Rundmails auf dem Laufenden halten.

Abbildung 13: Unterstützung aus der Universität für die Arbeit des Krisenstabs (Foto: JLU/Charlotte Brückner-Ihl)

Wie eingangs bemerkt: Eine perfekte Vorbereitung auf diese Krise und alle auftretenden Eventualitäten hat seinerzeit niemand von uns erwartet – weil wir als Erste getroffen wurden. Danach waren andere Hochschulen gewarnt und mussten sich zwangsläufig sehr sorgfältig für ähnliche Szenarien wappnen. Wir konnten beobachten, dass Kolleginnen und Kollegen viel Zeit in Krisenkommunikationspläne oder in perfekt gestaltete Schatten-Homepages investiert haben – ob das gerade für die Kommunikation in dieser Detailtiefe notwendig und sinnvoll ist, kann aber mit einem Fragezeichen versehen werden.

Unabhängig davon, dass die sehr schnell verfügbare temporäre Homepage in der Rückschau eines unserer kleinsten Probleme war: Krisenmanagement und vor allem Krisenkommunikation bestehen im Wesentlichen daraus, sich unverzüglich ein Bild der Lage zu machen, schnelle Entscheidungen zu treffen und diese nachvollziehbar und transparent zu kommunizieren. Notfallübungen und kurze Kommunikationswege zwischen potenziellen Krisenstabsmitgliedern sind für die Vorbereitung sehr sinnvoll, und auch Krisenpläne für bestimmte Szenarien können hilfreich sein. Allen Beteiligten sollte aber klar sein, dass auch die detailliertesten Roadmaps keine Garantie für eine gelungene Krisenkommunikation sind. *One-fits-all*-Schablonen kann es nicht geben, denn keine Krise gleicht der anderen: Es wird höchstwahrscheinlich zu Situationen kommen, die niemand vorhersehen konnte. In diesen Fällen helfen nur Flexibilität, Schnelligkeit, eine klare Führung und transparente Kommunikation.

***Lisa Dittrich** ist Pressesprecherin der Justus-Liebig-Universität Gießen.*

Ausführlicher Bericht zum Cyberangriff auf die JLU:

Kost, Michael, Loibl, Bastian, Reuter, Peter and Stenke, Matthias. "#JLUoffline. Der Cyber-Angriff auf die Justus-Liebig-Universität Gießen im Dezember 2019: Verlauf, Krisenmanagement, Konsequenzen" ABI Technik, vol. 42, no. 1, 2022, pp. 43-54. https://doi.org/10.1515/abitech-2022-0005 [18.07.2025]

Christian S. Fötinger: Cyber-Sicherheit an den Hochschulen in Bayern – Maßnahmen und Initiativen

Vorspann

Seit 2016 unterstützt die Stabsstelle Informationssicherheit der bayerischen staatlichen Hochschulen und Universitäten[23] diese beim Aufbau eines Informationssicherheitsmanagements. Nach etlichen Angriffen auf europäische, deutsche und bayerische Hochschulen ist das Thema Notfallprävention 2022 in den Vordergrund gerückt und der hochschulübergreifende IT-Service Informationssicherheit (HITS IS) durch den Digitalverbund Bayern etabliert.

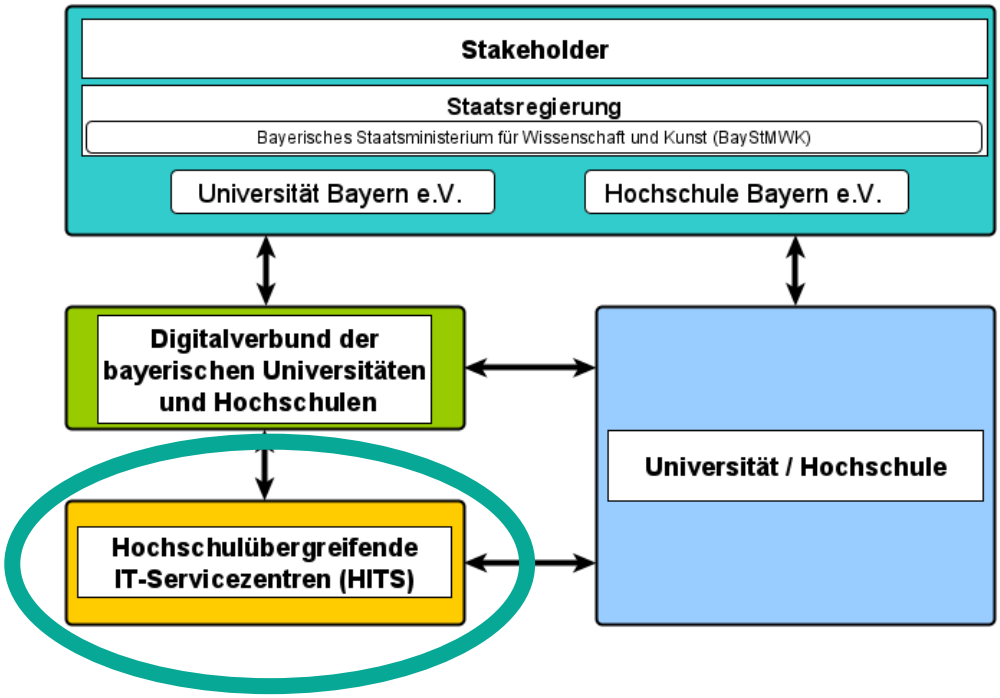

Abbildung 14: schematische Darstellung des Digitalverbund Bayern mit dem HITS IS

Der HITS IS bietet den bayerischen Hochschulen und Universitäten unter anderem Dienste in der Prävention und Bewältigung von Cyberangriffen an.

Zur Abwehr von Cyberangriffen relevante Dienste:

1) Schwachstellenscans

[23] https://www.tha.de/Rechenzentrum/Informationssicherheit/Stabsstelle-Informationssicherheit.html [18.07.2025]

In regelmäßigen Abständen werden die Einrichtungen überprüft. Dabei werden öffentlich erreichbare Dienste erkannt und auf bekannte Schwachstellen hin untersucht. Damit soll die Angriffsfläche für Cyberangriffe reduziert werden. Neben den Stichtagsaufnahmen der Angriffsfläche können täglich Berichte aus öffentlich bekannten an Hochschulen vorkommenden Schwachstellen bezogen werden.

2) Vorbereitung auf einen Cyberangriff

Das HITS IS stellt im Bereich präventives Notfallmanagement unterschiedliche Dienste bereit. Fokus des präventiven Notfallmanagements ist die prozessgestützte Vorbereitung zur schnellen Wiederherstellung eines geregelten und gesicherten IT-Betriebs.

Aus Sicherheitsvorfällen resultierende Notfall- und Krisensituationen erfordern zusätzliche Maßnahmen aus dem Notfallmanagement und die prozessübergreifende Abstimmung mehrerer Personen und Teams, sowie eine zielgerichtete Kommunikationsstrategie. Durch die zentrale Organisation werden einheitliche Prozesse etabliert, die kontinuierlich verbessert werden. Das Ziel ist die Unterstützung der bayerischen Hochschulen bei der Einführung und Verbesserung ihres Business Continuity Management Prozesses nach BSI Standard 200-4.[24]

Um den Einstieg in das Thema „Business Continuity Management“ zu erleichtern, bietet das HITS IS in unregelmäßigen Abständen Workshops an.

Workshop (Pilot)	Inhalte
BCM und Krisenkommunikation	Überblick über BCM Vorgehensweise mit Fokus auf BSI 200-4, inkl. Musterdokumente und Übungen zur Krisenkommunikation (Dauer ca. 6h)
BCM – Erste Schritte im BCM-Tool	Überblick über BCM Vorgehensweise im BCM-Tool (Dauer ca. 4h)
BCM in Kürze	Präsentation für Leitungsebene, Kurzüberblick (Dauer ca. 1h)

Abbildung 15: Dienste des HITS IS zur Notfallbewältigung

In Initial Workshops werden mit bestehenden Notfallteams Dokumente zur Notfallbewältigung überarbeitet, um einen adäquaten Notfallplan zu erhalten.

[24] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html [18.07.2025].

Aber was macht einen guten Notfallplan aus? Ein guter Plan ist ‚klug'...

... konkret, d.h. passend zur jeweiligen Situation bzw. an diese anpassbar,

... lesbar - d.h. jederzeit auf unterschiedlichen Geräten und standortunabhängig abrufbar,

... umfassend – d.h. er deckt möglichst alle Bereiche des notwendigen Betriebs ab und stellt alle nötigen Informationen zur Verfügung

... getestet: am Schreibtisch (mehrerer Personen) und in Teilen live durchgespielt und aktuell.

Ein kluger Notfallplan gibt den Beteiligten die Sicherheit, das Richtige zu tun und hilft, panikartige Reaktionen zu verhindern. Verlassen Sie sich nicht auf die Kenntnisse des verfügbaren Personals, nicht immer sind die besten Mitarbeiter:innen verfügbar und einer Krise intuitiv zu begegnen kann großen Schaden anrichten.

Einen klugen Notfallplan gibt es nicht „von der Stange". Er umfasst die gesamte Organisation mit Beteiligung aller Mitarbeiter:innen und Führungskräfte. Unterschätzen Sie nicht den Aufwand der Vorbereitung, bis die gesammelten und beschriebenen Maßnahmen das erste Mal am Schreibtisch getestet werden können. Integrieren Sie alle Änderungen in die Dokumentations- und regelmäßigen Überprüfungsprozesse ihrer Organisation (gemäß einem PDCA-Zyklus[25]), denn ohne die kontinuierliche Modernisierung der in der Entwicklung befindlichen Dokumente sind diese am Ende veraltet.

Wann und wie sich ein Störfall zu einer Störung, Ausnahmesituation, einem Notfall oder einer Krise entwickelt und welche Unterscheidungen getroffen werden, bleibt der Bewertung der jeweiligen Organisation überlassen. Langjährige Erfahrungen des Autors zeigen, dass es leichter ist, über ein „Unternehmensgedächtnis" zu einer für das Unternehmen passende Abstufung zu finden. Der Grad der Auswirkung ermisst sich demnach darin, wie viele Mitarbeiter:innen über den Vorfall wie lange sprechen. In Beratungsgesprächen analysieren Experten daher Vorfälle der Vergangenheit bzw. Szenarien nach folgender Abstufung:

1. Stufe	**2. Hinweise**	**3. Gedächtnis**
4. Störungen	5. Vorfälle werden im kleinen Kreis, einer Abteilung oder einem Team erkannt, behandelt und korrigiert.	6. wenige Wochen
7. Ausnahmesituationen oder größere Unterbrechungen	8. Betreffen mehrere Gruppen oder Abteilungen. Geschäftsprozesse funktionieren nicht mehr wie gewohnt und interne Spezialisten und Spezialistinnen vereinbaren mit leitenden Angestellten Korrekturmaßnahmen, die aus dem regulären Budget umgesetzt werden können.	9. wenige Monate

[25] PDCA Zyklus, ein von Walter Shewhart und W. Edwards Deming entwickelter 4 phasiger Zyklus zur kontinuierlichen Verbesserung (Plan-Do-Check-Act) von Prozessen.

10. Notfälle	11. Ganze Gebäude oder Standorte sind betroffen, Abteilungen kommen zum Stillstand und das Tagesgeschäft wird für einen längeren Zeitraum unterbrochen. Die Situation kann nicht ohne externe Hilfe bewältigt werden. Das Topmanagement wird regelmäßig über die aktuelle Situation informiert und wahrscheinlich nimmt die Presse bereits Notiz von dem Ereignis. Die Erinnerung an den Vorfall wird von den Medien durch Vergleiche mit ähnlichen Vorfällen bei anderen Organisationen wachgehalten.	12. Jahre
13. Krise	14. Ein Krisenstab mit wesentlicher Beteiligung des Topmanagements tauscht sich regelmäßig über die aktuelle Lage aus und erteilt Anweisungen für den weiteren Betrieb. Bei großräumigen oder marktspezifischen Ereignissen helfen vor allem Solidaritätseffekte – „alle sitzen im selben Boot“ – den Wiederanlauf und Fortbestand zu sichern.	15. Viele Jahre, unvergesslich

Abbildung 16: Abstufung von Vorfällen und wie lange diese in Erinnerung bleiben (Erfahrungswerte aus Beratungsgesprächen des Autors)

Die folgende Grafik veranschaulicht die Tragweite einzelner Notfallmaßnahmen und zeigt auf, dass professionelles Notfallmanagement tatsächlich eine Aufgabe für das leitende Unternehmens-Management ist:

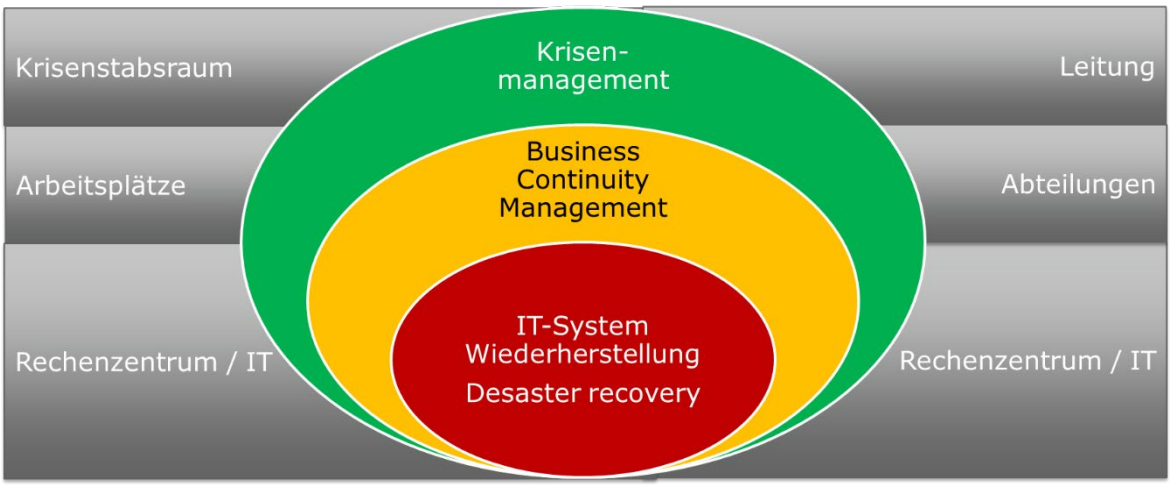

Abbildung 17: Tragweite, Organisationseinheiten und Begriffe zum Notfallmanagement (Christian S. Fötinger, 2012)

Die Grafik zeigt Bedarfe der am Notfallmanagement Beteiligten und veranschaulicht die Zuständigkeitsebenen zur Erstellung von Plänen zur Aufrechterhaltung des Geschäftsbetriebs. Die IT

verantwortet im Notfall eine Basisinfrastruktur während Abteilungsleiter den Bedarf an Arbeitsplätzen und anderen Ressourcen zur Aufrechterhaltung von Geschäftsprozessen planen. In der Krise wird die Leitung in die aktuelle Situation einbezogen und eine Stabsorganisation zur Bewältigung installiert.

Jede Eskalationsstufe verlangt spezifische Organisationsstrukturen und Ressourcen, um die Lage zu bewältigen. Je weiter der Vorfall eskaliert, umso weitergehend müssen reguläre Funktionen, Rollen und Berichtsstrukturen durch Stabsarbeit ersetzt werden, um die kurzfristige Einbeziehung des Top-Managements zu gewährleisten. Routineabläufe des Tagesgeschäfts machen Maßnahmen vorbereiteter Pläne Platz und werden konsequent zugewiesen und abgearbeitet. Abweichung sind nur in Ausnahmefällen erlaubt. Rasches Handeln ersetzt die Suche nach der perfekten Lösung.

„Besser die zweitbeste Entscheidung zur rechten Zeit, als die optimale zu spät!“
Bruno Hersche

Die ersten Schritte im Notfall dienen der Lageklärung und Verfahren der Kommunikation und der Eskalation. Präzise vorbereitete und passende Teams zur Beherrschung unterschiedlicher Situationen müssen zeitnah organisiert werden. Ein Schema zur Lageeinschätzung sehen Sie in der Darstellung rechts (Fötinger, 2011).

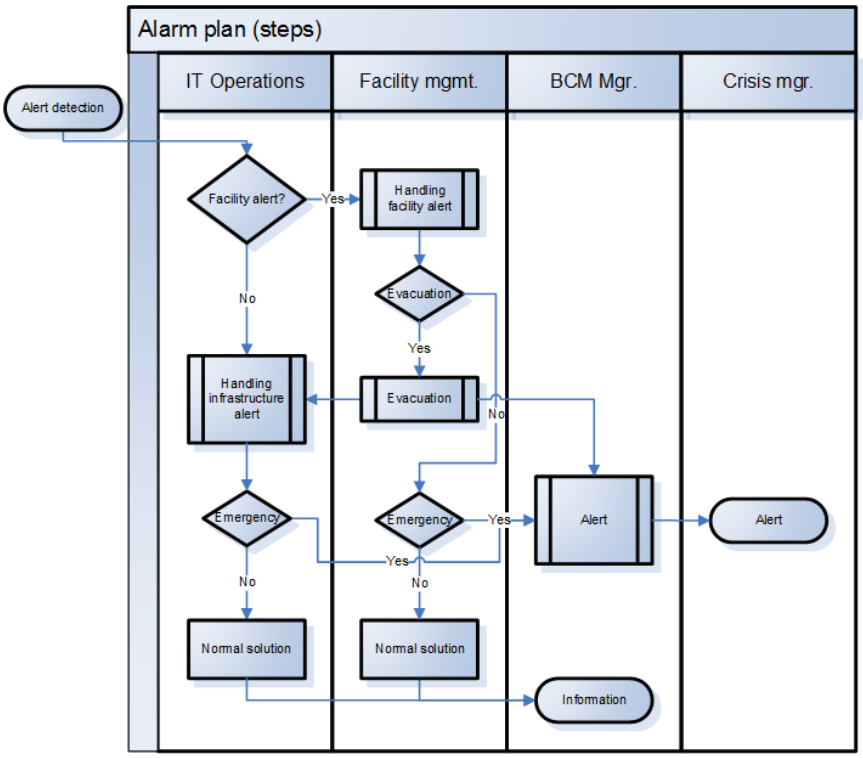

Abbildung 18: Prozessplan Notfallmanagement

Der BSI 200-4 Standard geht bei der Planerstellung von der Gefährdung bzw. dem Schutzbedarf aus, um danach die Folgen für die Organisation zu betrachten. In der Folge werden Maßnahmen und Pläne zur Bewältigung der beschriebenen Situationen entwickelt. Für die Entscheider eines IKT-Servicezentrums dienen diese Pläne als Roadmap im Krisenfall sowie für die Aufrechterhaltung bzw. den Wiederanlauf wichtiger Informationstechnologien zum Betrieb zentraler Geschäftsprozesse.

Prinzipiell haben prozessorientierte Organisationen Vorteile bei Aufbau und Integration eines Notfallmanagements, da Ressourcen und Ziele implizit beschrieben sind. Entsprechend lässt sich in der Zusammenarbeit zwischen dem Notfall- und dem Prozessverantwortlichen ein Teil-Notfallplan entwickeln, der in dem betroffenen Bereich theoretisch sofort anwendbar ist. Die schrittweise Ausdehnung auf alle Geschäftsprozesse vervollständigt sukzessive die Dokumentation zum Notfallmanagement.

Die Krise selbst erfordert eine gute und generische Vorbereitung. Durch die Außergewöhnlichkeit lassen sich kaum Vorhersagen über den Verlauf abschätzen. In bestimmten Krisen, etwa im Fall eines Cyberangriffs, ist die Kommunikation mit den Medien entscheidend. Entsprechend kann dazu ein Leitfaden (1 Seite) mit der Kommunikationsabteilung vorbereitet werden. Dieser berücksichtigt psychodynamischen Besonderheiten (wie Emotionalisierung, Schuld, Zeitdruck, Ventilfunktion, Freunde und Feinde, Tunnelblick) in der Krisensituation.

Es ist unabdingbar, dass der Zugriff auf Planungen über Hierarchien hinweg zu jeder Zeit und an jedem Ort möglich ist.

Ein kontinuierlicher Verbesserungsprozess bedingt die regelmäßige Überprüfung und Anpassung an dynamische Geschäftsprozessen und sich verändernde Sicherheitslagen. Erst der Test zeigt, ob ein Plan im Notfall seine Wirksamkeit entfaltet und ein Unternehmen den Notfall ohne großen Schaden überlebt. Während in einer Krise die Kommunikation und die Zusammenarbeit des Krisenstabs im Vordergrund stehen, können für Notfälle mögliche ‚work-around' Szenarien der Geschäftsprozesse durchdacht (Schreibtischtest) und in selteneren Abständen durchgespielt (Real-Life Test) werden. Regelmäßig sollten auch Wiederherstellungstests der Infrastruktur (IT, Kühlung, Strom, Schließsystem, etc.) durchgeführt werden.

Die Ergebnisse dienen dem Krisenstab (Notfallmanager und relevante Bereichsleiter) zur Verbesserung und Anpassung der jeweiligen Notfallpläne oder Notfallprozesse und geben Budget dafür frei.

3) eduCSIRT – Einsatztruppe

Wenn's doch passiert?

Das HITS IS stellt sofort ein Team zur Verfügung, dass bei der Analyse des Cyberangriffs unterstützt und weitere Schritte empfiehlt. Das Team übernimmt im Bedarfsfall den Kontakt zum Landesamt für Sicherheit in der Informationstechnik (LSI Bayern) und dem Ministerium.

Im Bedarfsfall kann sofort eine Notfallinfrastruktur für folgende Zwecke bereitgestellt werden:

- Begrenzte Anzahl an Mailadressen,
- Filesystem,
- Chatprogramm,
- Notfallwebseite (zum Bloggen).

Außerdem stellt das Staatsministerium den Hochschulen ein Sofortbudget zur Bewältigung zur Verfügung.

Fazit

Hochschulen, die sich auf Vorfälle vorbereiten, überleben Notfälle und Krisen wahrscheinlicher und mit geringerem Schaden.

„Krisen meistert man am besten, indem man ihnen zuvorkommt.“ -
Walt Whitman Rostow

***Christian S. Fötinger** ist Leiter des hochschulübergreifenden IT-Service Informationssicherheit (HITS IS) – Governance, c/o Technische Hochschule Augsburg.*

Weitere Literatur und Standards:

ISO/IEC 22301; Sicherheit und Schutz des Gemeinwesens – Business Continuity Management System Anforderungen (ISO 22301:2012); Deutsche Fassung EN ISO 22301:2014.

ISO-Standard 22301:2012 “Societal security – Business continuity management systems – Requirements”.

BSI-Standard 200-4; 2022.

Hilfsmittel zum BSI-Standard 200-4: Weiterführende Aspekte zur Bewältigung, 2022. https://bsi.bund.de/dok/200-4-hilfsmittel [18.07.2025].

BCI Good Practice Guidelines des britischen Business Continuity Institute. https://thebci.org [18.07.2025].

BSI (British Standards Institute) 17091:2018 Crisis management. Guidance for developing a strategic capability.

Fötinger, C. S. (2011), Notfallhandbuch im Finanzsektor.

Malte Dreyer: Zentrale Schritte zur Vorbereitung auf mögliche Cyber-Angriffe. Ein Überblick

Hinweis: Grundlage für den Beitrag von Malte Dreyer auf dem Forum Cyber-Security für Hochschulen war die „Handreichung zur Vorbereitung auf Informationssichervorfälle“, die er zusammen mit Dr. Frank Kühnlenz und Bernhard Brandel verfasst hat und die vom ZKI e.V., Arbeitskreis Strategie und Organisation herausgegeben worden ist.[26] Im Nachgang zur Veranstaltung wurde die Handreichung leicht überarbeitet und um neue Punkte ergänzt. Hier abgedruckt ist die aktualisierte Fassung.

Zielsetzung der Handreichung

Diese Handreichung soll Hochschul- und IT-Leitungen mit konkreten Handlungsempfehlungen dabei unterstützen, sich besser auf IT-Sicherheitsvorfälle vorzubereiten. Sie zielt dabei im Kern nicht auf die systematische Erhöhung der Reife des Informationssicherheitsmanagementsystems (ISMS), wie sie an den meisten Hochschulen bereits durch Informations- bzw. IT-Sicherheitsbeauftragte adressiert wird. Sie zeigt vielmehr kurzfristige Handlungspunkte mit signifikanter Wirkung auf, die sukzessive durch die Leitung bearbeitet werden können, um einen Einstieg in ein systematisches Notfallmanagement zu ermöglichen.

Hintergrund

Ein Notfall im Fokus der hier beschriebenen Handreichung ist ein Schadensereignis, bei dem IT-gestützte Prozesse oder Ressourcen der Institution nicht wie vorgesehen funktionieren, wie bspw. nach einem erfolgreichen Angriff auf die IT-Infrastruktur. Die Verfügbarkeit der entsprechenden Prozesse oder Ressourcen kann innerhalb einer im normalen Betrieb üblichen Zeit nicht wiederhergestellt werden. Der Geschäftsbetrieb ist stark beeinträchtigt bzw. überwiegend nicht mehr möglich. Es entstehen beträchtliche bis existenzbedrohende Schäden, die sich signifikant und in nicht akzeptablem Rahmen auf den Haushalt oder die Aufgabenerfüllung auswirken. (IT-)Notfälle können nicht mehr im allgemeinen Tagesgeschäft abgewickelt werden, sondern erfordern eine gesonderte Notfallbewältigungsorganisation.

[26] https://www.zki.de/fileadmin/user_upload/Downloads/Final_zki_Informationssicherheitsvorfaelle_2023_Geringeres_Datenvolumen.pdf [18.07.2025].

Phasen eines IT-Notfalls

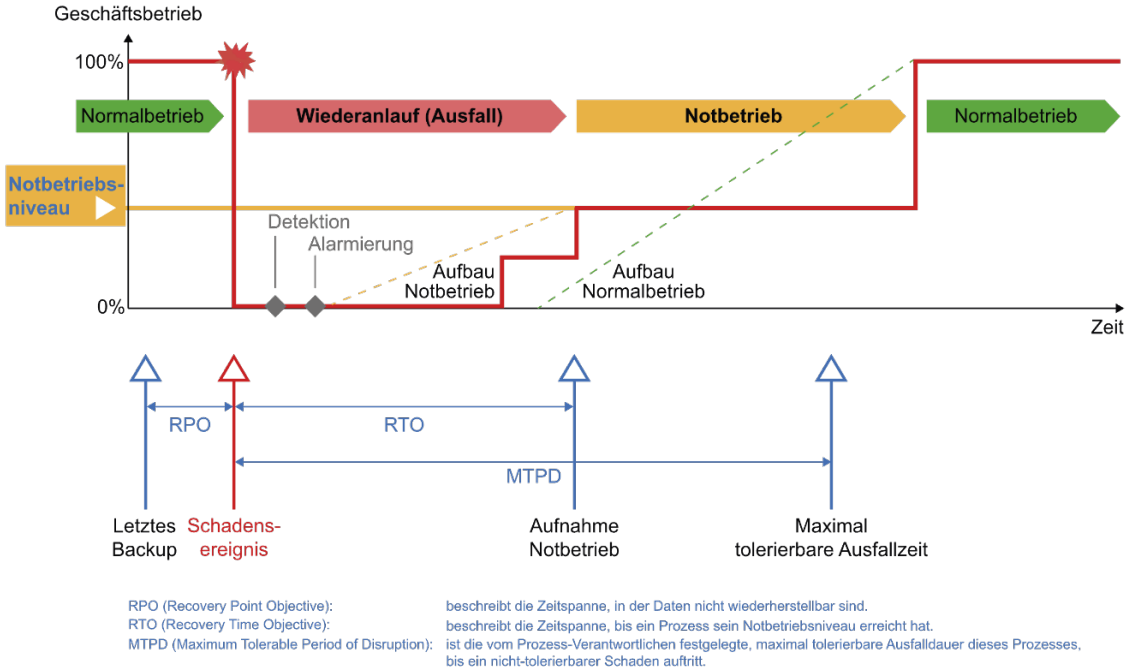

Abbildung 19: Phasen eines IT-Notfalls mit Erläuterung wichtiger Kenngrößen (MTPD, RTO, RPO, Notbetriebsniveau)

Sobald das Schadensereignis eintritt, endet der Normalbetrieb und wird auf ein besorgniserregendes, undefiniertes Niveau des normalen Geschäftsbetriebs reduziert. Erst mit der Detektion des Schadensereignisses und der anschließenden Alarmierung (siehe Abschnitt „Mehrstufiger Krisenstab und Meldeketten“) beginnt eine Reaktion der Hochschule, um die Kontrolle zurückzugewinnen und Maßnahmen zum Wiederanlauf einzuleiten, die einen definierten Notbetrieb herstellen. Verzögert, aber parallel beginnt die Wiederherstellung des Normalbetriebs.

Zeitpunkt des Vorfalls

Für eine angemessene Einordnung des Vorfalls ist der genaue Zeitpunkt im akademischen Jahr von Bedeutung. Hier sind drei Zeitbereiche zu unterscheiden:

- direkt vor oder während der Bewerbungsphase
- direkt vor oder während der Prüfungsphase
- während des Semesters

Je nach Zeitpunkt sind unterschiedliche Schwerpunkte für die ersten Reaktionen zu legen und auch leicht unterschiedliche Personenkreise zu etablieren. Vor der Bewerbungsphase ist ein Schwerpunkt auf die Kommunikation und die Systeme zur Ermöglichung von Bewerbungen und Einschreibung zu setzen. Während der Prüfungsphase liegt ein zusätzlicher Schwerpunkt auf der sorgfältigen Kommunikation mit den Studierenden und der Bereitstellung entsprechender Systeme. Während des Semesters ist der Semesterbetrieb bestmöglich zu unterstützen.

Angriffe werden häufig erst durch bestimmte finale Aktionen der Akteure bemerkt, deren Ziel es ist, möglichst viel Druck auf die Angegriffenen aufzubauen. Solche Aktionen finden daher oft an Wochenenden, Feiertagen und Ferienzeiten statt. Sie orientieren sich zudem an der Situation der Angegriffenen – somit könnten diese Aktionen auch zu besonders kritischen Zeiten des Hochschuljahres stattfinden.

TO DO: Diskutieren Sie intern die Auswirkungen der unterschiedlichen Zeitpunkte im akademischen Jahr, um die verschiedenen Effekte deutlicher zu identifizieren.

Weiterführend: BSI: 7.1.2 Festlegung der BIA-Parameter und betrachteten Zeithorizonte (Business Continuity Management, BSI-Standard 200-4)

Mehrstufiger Krisenstab und Meldeketten (Leitung, Kommunikation, IT)

Im Laufe der Reaktion auf IT-Sicherheitsvorfälle müssen unterschiedliche Personengruppen informiert und für Entscheidungen einbezogen werden. Zusätzlich ist eine gesteuerte Kommunikation nach außen notwendig. Für diese Zwecke werden meist mehrere Krisenstäbe eingerichtet.

Das Hauptziel bei der Etablierung von Krisenstäben ist eine hohe Effizienz der Abstimmungsprozesse und die Freihaltung größtmöglicher Arbeitskapazität für diejenigen, die an der Wiederherstellung der IT-Dienste arbeiten.

Krisenstäbe müssen schwierige Entscheidungen zeitnah auf Basis unvollständiger Informationen innerhalb eines dynamischen Angriffsgeschehens treffen. Es ist während eines IT-Notfalls damit zu rechnen, dass die Angreifer weitere kontinuierlich Maßnahmen ergreifen, um den Leidensdruck zum Erreichen ihrer Forderungen zu erhöhen.

Die Erfahrungen der Hochschulen zeigen, dass die Einrichtung von drei Krisenstäben empfehlenswert ist:

- Krisenstab IT – zur Abstimmung der IT-bezogenen Themen
- Krisenstab Leitung – zur Abstimmung mit der Hochschulleitung
- Krisenstab Kommunikation – für eine gut abgestimmte und gesteuerte Kommunikation der Effekte des IT-Notfalls

Die Teilnehmenden dieser Stäbe überlappen sich hierbei teilweise und werden mindestens durch die Teilnahme des IT-Sicherheitsbeauftragten/CISO und der IT-Leitung an allen Stäben koordiniert. Auch die Einbeziehung des Datenschutzes und möglichst aller Status-Gruppen[27], inkl. der Studierenden, sollte sichergestellt sein.

Die Teilnehmenden der Krisenstäbe müssen vorab bestimmt und auch für den Fall erreichbar sein, dass die IT-Infrastruktur der Hochschule nicht mehr in Betrieb ist. Hierfür sind Lösungen außerhalb der Hochschule zu organisieren, zu etablieren und einzuüben, wie z. B. externe Messenger-Gruppen (bspw. in Signal oder

[27] Zielgruppen sind vielfältig, intern und extern, z. B. Mitarbeitende (in besonderen Positionen), Stellenbewerber:innen, Studierende, Studienbewerber:innen, Partner (Dienstleister, Kooperationen, Verbünde, Hochschule als Service-Provider), offizielle Stellen (Aufsichtsbehörden, Landesdatenschutz, Polizei, BSI) usw.

Threema) oder zumindest die Verteilung (und Aktualisierung) der benötigten Telefonnummern der Teilnehmenden der Krisenstäbe. Krisenstäbe müssen insbesondere auch außerhalb der regulären Arbeitszeiten tätig werden. Darauf müssen die Teilnehmenden vorbereitet sein.

TO DO: Etablieren Sie drei Krisenstäbe, testen Sie deren Funktionsfähigkeit und achten Sie darauf, ob alle Status-Gruppen intern und extern adressiert werden.

Weiterführend: BSI: 13.3 Erstellung einer Jahresübungsplanung (Business Continuity Management, BSI-Standard 200-4)

Externe IT-Ressourcen

Für den Fall der Fälle sollte unbelastete IT-Kapazität bereitstehen. Hierzu empfiehlt es sich, bereits vorab entsprechende längerfristige Kapazitäten auszuschreiben, um einzelne Dienste unabhängig von der kompromittierten eigenen Infrastruktur aufsetzen zu können. Auch ein Modell des Austauschs mit anderen Hochschulen kann in Betracht gezogen werden, wird jedoch von vielen Hochschulen aufgrund der möglichen Wechselwirkungen eher kritisch gesehen. Möglicherweise kann jedoch Fachpersonal temporär zur Verfügung gestellt werden, ohne selbst in die Schusslinie der Angreifer zu geraten.

TO DO: Beschaffen Sie rechtzeitig externe IT-Kapazitäten.

Website der Hochschule für den Notfall

Bei Informationssicherheitsvorfällen ist eine zeitnahe und umfassende Information unerlässlich. Die Notfallwebsite ist dabei das zentrale Kommunikationsmedium. Hierfür gilt es, Technologien, Design und Pflegemodelle vorab bereits abzustimmen und zu testen. Oftmals wird eine Notfallwebsite gezielt attackiert (z. B. Denial of Service), um den Leidensdruck zu erhöhen, sodass zusätzliche Absicherungen notwendig sind.

TO DO: Klären und testen Sie, wo und wie Sie eine Notfallwebsite betreiben und pflegen.

Vertrag mit Incident-Response-Dienstleister

Im Notfall benötigen Sie externe Unterstützung, um die Angriffe zu analysieren, Spuren zu sichern und die Schäden möglichst zu begrenzen. Hierfür gibt es eine Reihe von Dienstleistern, die „Incident Response"-Leistungen anbieten. Das BSI bietet hierfür eine Liste mit qualifizierten Dienstleistern an. Je mehr diese Dienstleister bereits vorab über Ihre Organisation wissen, desto effizienter können sie bei Notfällen Hilfe leisten. Deshalb sollte auch das Onboarding des Dienstleisters die notwendige Aufmerksamkeit bekommen. Je nach Komplexität der IT-Strukturen kann die Einführung auch größere Zeitanteile von mehreren Teams binden und sich über mehrere Monate erstrecken.

TO DO: Schließen Sie einen Incident-Response-Vertrag und betreiben Sie das Onboarding mit der nötigen Zeit und Aufmerksamkeit.

Weiterführend: BSI: Liste der qualifizierten APT-Response-Dienstleister

Trennung vom Internet

Eine komplette temporäre Trennung des Netzwerkes vom Internet ist zur Schadenseindämmung und -bewertung bei großen IT-Notfällen häufig geboten. Dabei soll jegliche Kommunikation von außen nach innen, aber auch von innen nach außen unterbunden werden. Diese Maßnahme muss insbesondere kommunikativ begleitet werden, denn sie erzeugt große Aufmerksamkeit bei allen Zielgruppen.

TO DO: Prüfen und dokumentieren Sie, was eine Trennung vom Internet für Ihre IT-Strukturen bedeutet und wie diese durchzuführen ist.

IT-Assetmanagement

Im Fall der Fälle muss rasch identifiziert werden, welche IT-Systeme der Vorfall umfasst und welche Auswirkungen sich daraus ergeben. Welche Geräte und Server beteiligt sind und in welchen Netzbereichen sich diese befinden, muss möglichst schnell zu klären sein. Dies ist nur möglich, wenn ein umfassender Überblick zu den IT-Assets besteht, der nicht nur die physischen Aspekte von Hardware abdeckt, sondern auch die logischen Zusammenhänge, wie die Namensauflösungen für IP-Adressen, Zuordnungen zu Ports und beschrifteten Kabeln, Funktionen von Geräten, die jeweiligen Ansprechpartner:innen und auch Architekturbeschreibungen, um Zusammenhänge zwischen Geräten und Diensten nachvollziehen zu können. Liegen diese Informationen nicht vor und sind die dafür nötigen IT-Systeme im Notfall nicht verfügbar, kann die genaue Aufklärung des Vorfalls sehr zeitintensiv und umständlich sein.

TO DO: Verschaffen Sie sich einen Überblick zum Stand des IT-Assetmanagements an der Einrichtung, prüfen Sie stichprobenartig, wie umfangreich und aktuelle die Daten gepflegt sind und stellen Sie einen Zugriff für Notfälle sicher.

Weiterführend: BSI: DER.2.2 Vorsorge für die IT-Forensik

Eine gute Notfallbewältigung erfordert eine klare Steuerung

Ein IT-Sicherheitsvorfall erzeugt viele Aufgaben und Aktivitäten, die bearbeitet werden müssen. In der Summe kann dies bedeuten, Hunderte kleinere und größere Aufgaben zeitkritisch zu steuern und im Blick behalten zu müssen. Dabei muss zu jeder Zeit der Überblick gewahrt werden, welche Aktivitäten durch wen bis wann bearbeitet werden und was das erwartete Ergebnis ist. Einige Aktivitäten werden neue Erkenntnisse hinsichtlich möglicher Ursachen und Mitigationsmaßnahmen bieten, andere schaffen die Voraussetzungen für weitere Schritte. Um einen solchen Notfall zu managen, sind deshalb ganz klare Bearbeitungs- und Statuserhebungsstrukturen unerlässlich, die den Beteiligten bekannt sein müssen. Die hierfür notwendigen Steuerungsstrukturen weichen von den üblichen Managementgepflogenheiten ab und können bereits vorab in den möglichen Auswirkungen besprochen werden. Zu beachten ist dabei insbesondere, dass etablierte Kommunikationskanäle bzw. Monitoring-Werkzeuge voraussichtlich nicht zur Verfügung stehen. Sind sie dennoch verfügbar, muss besonders geprüft werden, ob Angreifer sich dazu Zugang verschafft haben könnten. Vorbereitend kann neben der Auswahl von Werkzeugen auch bereits festgelegt werden, welche Personen sich am besten für eine solche Steuerung eignen könnten.

TO DO: Besprechen Sie vorab, wie eine Steuerung und Statuserhebung umgesetzt werden kann und welche Personen dafür infrage kommen.

Weiterführend: 4.3 Definition der BC-Aufbauorganisation (Business Continuity Management, BSI-Standard 200-4)

Isolation von Netzsegmenten

Bei Vorfällen, die nicht die gesamte IT-Struktur betreffen, werden einzelne Teile bzw. Segmente abgeschottet, z. B. eine Fakultät oder ein Netz für Geräte, um eine Ausbreitung über Netzgrenzen hinweg zu verhindern.

TO DO: Prüfen und dokumentieren Sie die Strukturen und Steuerungsprozesse der Netzwerksegmentierung Ihrer IT-Strukturen.

Weiterführend: BSI: Netzwerkarchitektur und -design (2023)

Wiederaufsetzplan für Rückkehr zum Normalbetrieb

Was kann vorbereitet werden, um die gesamte IT-Infrastruktur ggf. von Grund auf neu aufzubauen? Welche Kernkomponenten gibt es dafür zu berücksichtigen? Typischerweise wird neue Infrastruktur parallel zur bestehenden aufgebaut. Teile der alten Infrastruktur können nur übernommen werden, wenn das Risiko IT-forensisch, z. B. durch den Incident-Response-Dienstleister, geklärt wurde.

TO DO: Entwickeln Sie Pläne und dokumentieren Sie diese, um die Verfügbarkeit von unkompromittierter Infrastruktur zur Administration sicherzustellen.

Weiterführend: BSI: Wiederanlaufparameter bestimmen

Wiederanlauf in den Notbetrieb

Der Wiederanlauf beschreibt alle Maßnahmen, um strukturiert in einen vorab geregelten Notbetrieb wechseln zu können. Er beschreibt nicht die Wiederherstellung eines Normalbetriebs. Hierfür muss ein Notbetriebsniveau für IT-Dienste definiert werden, die als grundlegend für einen Notbetrieb gesehen werden, wie z. B. die Betriebsfähigkeit des Netzwerkes, von Telefonen oder E-Mails.

TO DO: Entwickeln und dokumentieren Sie das gewünschte Niveau für den Notbetrieb.

Vergabe neuer Passwörter

Ab einem bestimmten Grad der Kompromittierung ist die Vergabe neuer Passwörter an alle rechtmäßigen Account-Inhaber:innen notwendig. Alle kompromittierten Accounts sind somit zu sperren. Die initiale Vergabe neuer Passwörter, deren Ausgabe und Versand danach stellen in vielerlei Hinsicht eine große Herausforderung dar, insbesondere auch aufgrund der ggf. hohen Anzahl von Personen. Es empfiehlt sich

deshalb, Rahmenbedingungen und die konkrete Ausführung eines solchen Prozesses bereits vorab zu klären und konkrete Verfahren bzw. auch Dienstleister auszuwählen.

TO DO: Gestalten und prüfen Sie einen Prozess zur Vergabe und Ausgabe neuer Passwörter.

Prioritäten für die IT-Dienste

Das Wiederaufsetzen einer komplexen IT-Struktur, wie sie Hochschulen üblicherweise betreiben, benötigt Zeit und Ressourcen. Deshalb sollte bereits vorab klar sein, in welcher Reihenfolge bzw. mit welchen Prioritäten einzelne Dienste oder Kategorien von Diensten versehen werden. Die Festlegung einer solchen Prioritätenliste geschieht in enger Abstimmung zwischen IT-Zentrum und Hochschulleitung.

Nicht jeder Dienst benötigt einen Notbetrieb: Eine Reduzierung auf das Wesentliche ermöglicht schnelleres Handeln mit den begrenzten Ressourcen. Neben den Prioritäten für den Wiederanlauf in den Notbetrieb sollten gleichzeitig Prioritäten für die Wiederherstellung des Normalbetriebs definiert werden.

TO DO: Erstellen Sie eine Tabelle mit Prioritäten oder Prioritätenklassen für die Bereitstellung von Diensten nach einem Notfall und stimmen Sie diese zwischen IT-Zentrum und Hochschulleitung ab.

Weiterführend: BSI: Geschäftsprozesse priorisieren

Belastungen für die Beschäftigten

Notfälle der hier beschriebenen Größenordnung sind eine ungewöhnlich hohe Belastung für die beteiligten Mitarbeitenden. Diese Belastungen dauern meist mehrere Monate nach Eintreten des Schadensereignisses an. Sie entstehen z. B. durch den hohen Zeitdruck oder auch wenn Beschäftigte das Gefühl haben, an dem erfolgreichen Angriff eine Mitschuld zu tragen. Mitarbeitende sind nicht selten eng verbunden mit bspw. den durch sie betreuten IT-Diensten und finden sich somit in einer zusätzlich belastenden Stresssituation wieder.

Aufgrund der Fürsorgepflicht des Arbeitgebers gegenüber seinen Mitarbeitenden sollte in solch einer Notfallsituation eine besondere Aufmerksamkeit auf der Anerkennung und dem Erhalt der Arbeitskraft liegen. Hierbei können bereits einfache Maßnahmen höchst wirkungsvoll sein, wie bspw. regelmäßiges Essen anzubieten, auf Pausenzeiten zu achten und wertschätzend zu agieren. Möglicherweise klingt dies ungewöhnlich in einer Notsituation – tatsächlich ist es aber von großer Bedeutung: Eines der größten Risiken im Notfall ist der Ausfall von Schlüsselpersonal.

TO DO: Führen Sie sich bereits vorab vor Augen, welche Belastungen durch solche Notfälle für die Beschäftigten entstehen, und bereiten Sie entsprechende Maßnahmen vor.

Malte Dreyer *ist Direktor des Computer- und Medienservices der Humboldt-Universität zu Berlin.*

Weitere Quellen:

BSI: Ersthilfe/Linksammlung
https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/unternehmen.html?nn=133680&cms_pos=1 [18.07.2025]

BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.pdf?__blob=publicationFile&v=3 [18.07.2025]

BSI: Qualifizierte APT-Response-Dienstleister
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.pdf?__blob=publicationFile&v=16 [18.07.2025]

BSI-Standard 200-4 Business Continuity Management (BCM)
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html [18.07.2025]

BSI: Qualifizierte DDoS-Mitigation-Dienstleister
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister-DDos-Mitigation-Liste.pdf?__blob=publicationFile&v=5 [18.07.2025]

DFN.Security (im Aufbau): Mehr als DoS-Basisschutz und DFN-CERT
https://www.dfn.de/dfn-security-ein-dach-fuer-it-sicherheit/ [18.07.2025]

Jan K. Köcher: Rechtliche Rahmenbedingungen vor und nach Cyber-Angriffen

Die Zunahme von Cyberangriffen stellt Organisationen und Behörden vor erhebliche Herausforderungen, denen durch geeignete technische und organisatorische Schutzmaßnahmen begegnet werden muss. Diese zum Teil aufwändigen Maßnahmen liegen im Eigeninteresse der jeweiligen Organisation, da sie Funktionsfähigkeit und Integrität der Verarbeitungen gewährleisten sollen. Daneben gibt es verpflichtende gesetzliche Vorgaben zu Maßnahmen im Vorfeld möglicher Angriffe, um es Angreifern möglichst schwer zu machen. Ebenso bestehen rechtliche Vorgaben, die nach einem erfolgten Angriff einzuhalten sind, damit Auswirkungen begrenzt und mögliche weitere Betroffene möglichst frühzeitig gewarnt werden können. Im Folgenden soll auf diese Vorgaben näher eingegangen werden.

Rechtliche Rahmenbedingungen zur Prävention vor Cyberangriffen

Um es den Angreifern möglichst nicht zu einfach zu machen, bestehen in verschiedenen Bereichen gesetzliche Vorgaben für präventive Maßnahmen. Um hier das Feld nicht zu sehr zu erweitern, konzentriere ich mich im Folgenden auf die Vorgaben an Hochschulen.

Prävention Datenschutz

Vorgaben zur Prävention ergeben sich zunächst aus der Datenschutz-Grundverordnung (DS-GVO). Hier ist aber wichtig zu wissen, dass sich der Anwendungsbereich auf den Schutz personenbezogener Daten beschränkt. D.h. die Vorgaben zur Prävention aus Sicht des Datenschutzes betreffen nur Verarbeitungen, die personenbezogene Daten zum Gegenstand haben. Gemäß Art. 32 DS-GVO muss die für die Verarbeitung verantwortliche Stelle „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen“ treffen, „um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“. Das Gesetz schreibt somit keine konkreten Maßnahmen vor. Es legt abstrakt die Anforderungen für solche Maßnahmen fest, die sich wie folgt systematisieren lassen:

Geeignete Schutzmaßnahmen: Eine konkrete Maßnahme muss von ihrer Wirkung geeignet sein das Ziel des Schutzes zu fördern. Zudem muss diese Maßnahme dem Stand der Technik entsprechen.

Angemessenheit: Der Aufwand der geeigneten Maßnahmen wird ins Verhältnis zum Schutzbedarf (Risiko und Schadenhöhe) gestellt, um die für den konkreten Fall richtige Maßnahme auszuwählen.

Nachhaltigkeit: Es genügt nicht den Schutz einmalig herzustellen. Es bedarf Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit (Art. 32 Abs. 1 Buchstabe b) und somit ein Managementansatz.

Verantwortlichkeit: Die Verantwortlichkeit liegt bei der Organisation und damit bei ihren gesetzlichen Vertretern.

Neben den Regelungen der DS-GVO gibt es ergänzende Regelungen im Bundesdatenschutzgesetz (BDSG) für Bundesbehörden und Unternehmen und in den Landesdatenschutzgesetzen für die öffentlichen Stellen der Länder, wie z. B. Hochschulen. Das geschilderte Grundprinzip aus der DS-GVO wird hierdurch aber nicht berührt.

Prävention Informationssicherheit

Die gesetzlichen Vorgaben zur Informationssicherheit betreffen alle Daten einer Organisation und sind somit nicht wie der Datenschutz auf den Schutz personenbezogene Daten beschränkt. Hier sind insbesondere die Vorgaben durch die europäische NIS2-Richtlinie[28] zu nennen. Als EU-Richtlinie gilt sie grundsätzlich nicht direkt, sondern muss zunächst in das deutsche Recht umgesetzt werden. Die Umsetzung erfolgt im Wesentlichen durch die hierdurch erforderlich werdenden Änderungen im BSI-Gesetz[29]. Die Umsetzung hätte bis Herbst 2024 erfolgen sollen und ist nunmehr frühestens Anfang 2025 zu erwarten.

In seiner bisherigen Fassung richtet sich das BSI-Gesetz mit seinen Anforderungen in erster Linie an Bundesbehörden und die Betreiber Kritischer Infrastrukturen (KRITIS). Durch die Umsetzung der Anforderungen der NIS2-Richtlinie werden durch das BSI-Gesetz darüber hinaus besondere Anforderungen an „Besonders wichtige Einrichtungen“ und „Wichtige Einrichtungen“ (§ 28 BSIG-neu) gestellt. Der bisherige Kreis der zu Maßnahmen Verpflichteten wird hierdurch deutlich ausgeweitet. Allerdings werden Länder und Kommunen und somit auch die Hochschulen als öffentliche Landeskörperschaften hierdurch nicht direkt reguliert, da dies in die Zuständigkeit der Bundesländer fällt. Der IT-Planungsrat hat für die föderale Ebene ein Identifizierungskonzept entwickelt, welches eine einheitliche Umsetzung in den Ländern gewährleisten soll. Dabei wurde empfohlen, dass die NIS2-Richtlinie aktuell keine Anwendung auf Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene oder auf Bildungseinrichtungen finden soll.[30]

Einige Bundesländer haben aber dennoch IT-Sicherheitsgesetze, die aber in der Regel die Anforderungen aus der NIS2-Richtlinie nicht gänzlich erfüllen. Das Cyber-Sicherheitsgesetz in Baden-Württemberg[31] hat beispielsweise eine eigene Cybersicherheitsagentur mit umfassenden Befugnissen etabliert. Hier sind Rechtsverordnungen zur Konkretisierung und flächendeckender Umsetzung einheitlicher Standards geplant. Das Hessische IT-Sicherheitsgesetz[32] statuiert in § 3 eine Pflicht zu angemessenen technischen und organisatorischen Maßnahmen nach dem Stand der Technik. Außerhalb des kommunalen Bereichs haben sich die Stellen dabei an der IT-Grundschutzmethodik des BSI zu orientieren und ein Informationssicherheitsmanagement umzusetzen. Wichtig ist hier, dass mit der Pflicht zur Orientierung an

[28] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:02022L2555-20221227 [18.07.2025]
[29] https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html [18.07.2025]
[30] 42. Sitzung vom 3.11.2023, Beschluss 2023/39, https://www.it-planungsrat.de/beschluss/beschluss-2023-39 [18.07.2025]
[31] https://www.landesrecht-bw.de/bsbw/document/jlr-CSGBWrahmen [18.07.2025]
[32] https://www.rv.hessenrecht.hessen.de/bshe/document/jlr-ITSiGHErahmen [18.07.2025]

der IT-Grundschutzmethodik keine Pflicht zur Zertifizierung gemeint ist. In vielen öffentlichen Bereichen bestünden überhaupt nicht die technischen und baulichen Voraussetzungen hierfür. Gesetze mit vergleichbaren Anforderungen bestehen noch im Saarland (IT-SiG SL) und in Sachsen (SächsISichG). Die anderen Länder sind noch nicht so weit.

Prävention aus anderen Rechtsgrundlagen

Neben den Datenschutz- und IT-Sicherheitsgesetzen sind das Onlinezugangsgesetz (OZG)[33] sowie diverse E-Government-Gesetze von Relevanz. Die genannten Gesetze regeln den elektronischen Zugang zur Verwaltung und fordern entsprechende angemessene Sicherheitsmaßnahmen. Ferner werden in Förderbedingungen, welche von öffentlichen Geldgebern vorgegeben werden, häufig Standards definiert, welche eine bestimmte Sicherheitsarchitektur oder Sicherheitsstandards vorschreiben. Ebenso können vertragliche Verpflichtungen zur Informationssicherheit bestehen, beispielweise im Rahmen von Service-Level-Agreements, welche Sicherheitsmaßnahmen zum Schutz von Daten und Systemen verlangen.

Rechtliche Rahmenbedingungen nach Cyberangriffen

Kommt es trotz aller Präventionsmaßnahmen zu einem Cyberangriff, greifen spezifische Melde- und Informationspflichten.

Meldepflichten Datenschutz

Die Meldepflichten aus dem Datenschutz beschränken sich auf Vorfälle, bei denen personenbezogene Daten betroffen sind. Die Datenschutz-Grundverordnung (DS-GVO) statuiert in Artikel 33 eine Meldepflicht an die Aufsichtsbehörde, welche innerhalb eines Zeitraums von 72 Stunden nach Bekanntwerden des Datenschutzvorfalls zu erfolgen hat. Die Meldung muss unter anderem Angaben zur Art des Vorfalls, den betroffenen Datenkategorien, der Zahl der betroffenen Personen sowie zu den geplanten Abhilfemaßnahmen enthalten. Gemäß Artikel 34 besteht die Verpflichtung zur Information der Betroffenen, sofern durch den Vorfall ein hohes Risiko für deren Rechte und Freiheiten besteht. Sinn und Zweck der Vorschrift ist, dass Betroffene gewarnt sind und sich gegen mögliche Folgeangriffe wappnen können.

Meldepflichten Informationssicherheit

Informationssicherheitsgesetze der Länder, wie beispielsweise das Sächsische Informationssicherheitsgesetz[34], verlangen darüber hinaus eine Meldung an das Sicherheitsnotfallteam, sobald erhebliche Beeinträchtigungen in der Informationssicherheit auftreten. Dies beinhaltet zudem die statistische Erfassung und Protokollierung der betroffenen Systeme und Prozesse. Ziel ist hier ein möglichst

[33] https://www.gesetze-im-internet.de/ozg/ [18.07.2025].
[34] https://www.revosax.sachsen.de/vorschrift/18349-Saechsisches-Informationssicherheitsgesetz [18.07.2025].

schneller Meldeweg, damit mögliche weitere betroffene Stellen möglichst frühzeitig gewarnt werden können.

Fazit:

Die rechtlichen Anforderungen an Datenschutz und Informationssicherheit legen großen Wert auf geeignete und angemessene präventive Maßnahmen sowie die kontinuierliche Überprüfung ihrer Wirksamkeit. Es besteht eine klare Verpflichtung für Organisationen hierbei den Stand der Technik zu wahren und damit ein hohes Sicherheitsniveau zu gewährleisten. Diese Verantwortung liegt bei den gesetzlichen Vertretern der Organisationen, die eine kontinuierliche Überprüfung und Anpassung der Sicherheitsmaßnahmen sicherstellen müssen. Die rechtlichen Rahmenbedingungen tragen somit zu einem nachhaltigen Schutz vor Cyberangriffen und zur Stärkung der Widerstandsfähigkeit von Organisationen und Institutionen bei.

Dr. iur. Jan K. Köcher *ist als Prokurist Mitglied der Geschäftsleitung der DFN-CERT Services GmbH für die Bereiche Recht, Compliance und Personal.*