HIS HE
WIR GESTALTEN HOCHSCHULZUKUNFT.

HIS-HE: Handreichung

November 2023

Krisenmanagement nach Cyber-Angriffen – Handlungsempfehlungen

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

Dr. Harald Gilch, Dr. Maren Lübcke, Dr. Mathias Stein
Geschäftsbereich Hochschulmanagement

15. November 2023

ISBN 978-3-948388-31-7

Inhaltsverzeichnis

Acknowledgement

Die vorliegenden Empfehlungen sind neben der Sichtung bestehender Literatur vor allem auf Basis von Interviews und Gesprächen mit betroffenen Hochschulen – der Technischen Universität Berlin, der Universität Duisburg-Essen, der Justus-Liebig-Universität Gießen, der HAW Hamburg und der Hochschule Ruhr West – entstanden. Wir möchten uns sehr für die Zeit bedanken, die sich Kanzler:innen, IT-Verantwortliche, IT-Sicherheitsbeauftragte und Leitende der Presse- und Kommunikationsabteilungen genommen haben, um unsere Fragen zu beantworten und ihre wertvollen Erfahrungen mit Cyber-Attacken zu teilen. Ohne sie wären diese Handlungsempfehlungen nicht möglich gewesen. Zudem möchten wir uns beim Arbeitskreis „Digitale Transformation“ der Universitätskanzler:innen für die Unterstützung des Vorhabens, von dem wir schon früh wertvolle Hinweise bekommen haben, sowie bei den Expertinnen und Experten, die das Dokument kritisch gelesen und uns umfassendes und hilfreiches Feedback gegeben haben, bedanken.

0 Vorbemerkungen

Hochschulen in Deutschland sehen sich zunehmend Cyber-Angriffen ausgesetzt[1], wobei die hohe Anzahl von Nutzer:innen in den zum großen Teil frei zugänglichen Hochschulnetzen und die zunehmende Digitalisierung der Hochschul-IT die Angriffsmöglichkeiten weiter erhöhen. Damit steigt gleichzeitig die Notwendigkeit zum Aufbau entsprechender Abwehr- und Notfallmaßnahmen, um Angriffe zu unterbinden bzw. im Falle einer Attacke schnell handlungsfähig zu sein.

Da die i. d. R. historisch gewachsenen IT-Landschaften der Hochschulen und die möglichen Angriffswege sehr unterschiedlich sein können, unterscheiden sich die Cyber-Attacken und die Folgen für die Hochschulen teilweise sehr deutlich. Im Umkehrschluss bedeutet dies, dass

- sich je nach Schwere des Angriffes und der betroffenen IT-Systeme ein individuelles Krisenszenario entwickelt,
- die Bandbreite an Folgeerscheinungen in der Größe variabel ist (von keinerlei direkten Auswirkungen über Verschlüsselung einzelner Systeme und Datendiebstahl bis hin zur vollständigen Lahmlegung des gesamten Hochschul-IT-Systems) und
- nicht für jedes Krisenszenario eine spezifische Vorbereitung oder Handlungsanweisung erstellt werden kann.

Die folgenden Ausführungen und Empfehlungen sind dementsprechend **Verallgemeinerungen**, die individuell an die Gegebenheiten der jeweiligen Hochschule angepasst werden müssen – abhängig von der jeweils eigenen IT-Landschaft, den vorhandenen Ressourcen sowie der bestehenden (IT-)Governance-Struktur. Zudem ist anzumerken, dass im Rahmen der Erarbeitung dieser Handreichung allein Universitäten und Hochschulen für Angewandte Wissenschaften betrachtet worden sind. Cyber-Angriffe haben sich in den letzten Jahren aber auch gegen Universitätskliniken, außeruniversitäre Forschungseinrichtungen oder Hochschul-Kooperationspartner gerichtet. Die damit verbundenen Besonderheiten und spezifischen Folgen nach einem Cyber-Angriff sind nicht Teil dieser Handreichung.

Im Mittelpunkt der Handreichung steht nicht die Vermeidung und Überwindung einer Cyber-Attacke aus IT-Sicht im Fokus, auch wenn IT-Fragen im Verlauf einer Cyber-Attacke von zentraler Bedeutung sind. **Betrachtungsebene** ist vielmehr die **Gesamtorganisation Hochschule aus Sicht der Hochschulleitung**, da der – wenn auch nur kurzfristige – Ausfall von IT-Systemen gravierende Folgen für die Arbeitsfähigkeit der Hochschulorganisation und damit für die Hochschulsteuerung hat. Die vorliegende Handlungsempfehlung soll eine Hilfestellung sein, um einen Cyber-Angriff möglichst schnell zu beheben und den Schaden so stark wie möglich zu begrenzen. In dem Sinne ist diese Handreichung als Anregung zur internen Diskussion und als erster Leitfaden für mögliche Schritte zur Vorbereitung und Krisenbewältigung gedacht. Ausgehend von dem Krisenfall einer Cyber-Attacke werden anhand der verschiedenen zeitlichen Phasen Maßnahmen und

[1] „Obwohl nicht davon ausgegangen werden kann, dass das vermehrte Angriffsaufkommen das Resultat von fokussierten Kampagnen ist, waren Bildungseinrichtungen 2022 äußerst attraktive Ziele von Cyber-Gruppierungen." (BKA 2023, S. 26)

Handlungsempfehlungen abgeleitet und gezeigt, wie eine Vorbereitung die Bewältigung dieser Phasen unterstützen kann. In Abbildung 1 sind die fünf Phasen

- Detektionsphase Zeitpunkt 0
- Reaktionsphase Tag 1
- Reaktionsphase Woche 1
- Reaktionsphase Monat 1
- Normalisierungsphase

dargestellt, die sich aus den Erfahrungen der im Rahmen dieser Handreichung befragten Hochschulen ergeben und die in den nachfolgenden Kapiteln beschrieben werden.

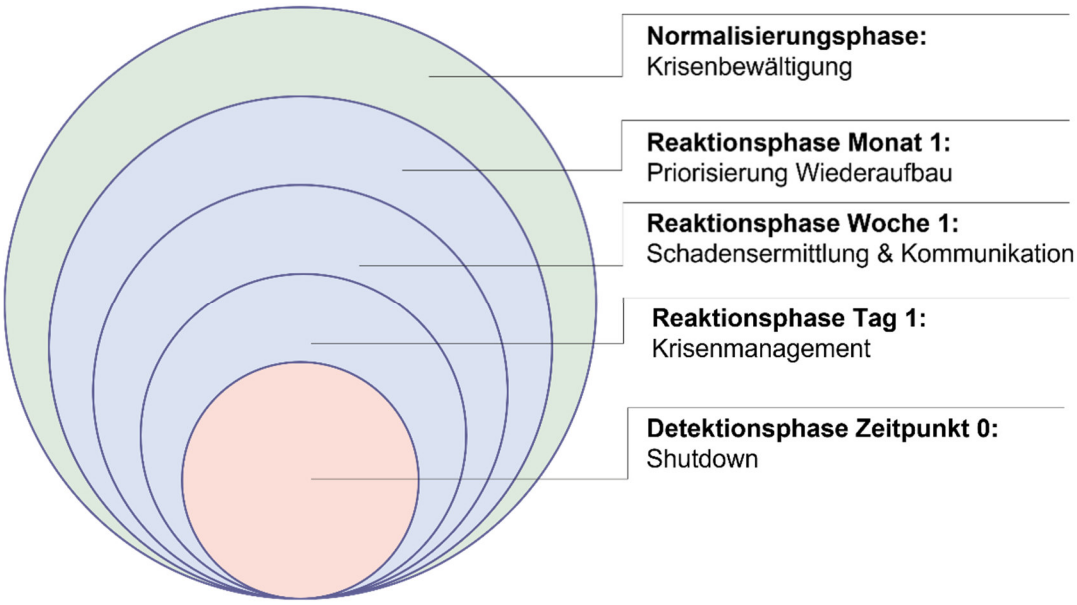

Abbildung 1: 5 Phasen des Krisenmanagements nach einem Cyber-Angriff

Pro Phase bzw. pro Aufgabenbereich sind leitende Fragen formuliert. Im Sinne einer Vorbereitung für den Ernstfall einer Cyber-Attacke können diese Fragen als Ausgangspunkte für eine interne Beschäftigung mit dem Thema genutzt werden. Ausgehend von den einzelnen Fragen ist im Anhang eine Checkliste an Maßnahmen pro Zeitabschnitt beigefügt. Die Vorbereitung auf eine Cyber-Attacke muss als eine neue, permanente Daueraufgabe für Hochschulen und Hochschulleitungen verstanden werden. Es gilt innerhalb der Hochschule die **Awareness** für diese Gefahr hochzuhalten, dass **Kontinuitätsmanagement** der Hochschulsysteme zu gewährleisten und insgesamt die (Krisen-)**Resilienz** der Hochschule zu stärken.

1 Detektionsphase - Zeitpunkt 0

Im Falle eines Cyber-Angriffs ist der **Faktor Zeit** entscheidend, d. h. eine frühzeitige Reaktion innerhalb von Minuten bzw. wenigen Stunden ist dringend erforderlich, um den Schaden am IT-System zu minimieren. Je schneller Gegenmaßnahmen – u. a. vom Netz trennen des IT-Systems – ergriffen werden, desto wahrscheinlicher ist es, dass die verschiedenen Komponenten vor einer Infektion geschützt werden und dass das IT-System schneller und einfacher wieder in den Betrieb genommen werden kann. Da die Angriffe zum Großteil gezielt am oder zum Wochenende bzw. an Feiertagen erfolgen, kann der Angriff schneller bemerkt werden, wenn es eine dauerhafte Systemüberwachung und Reaktionsmöglichkeiten auch außerhalb der Kernarbeitszeiten gibt. Folgende Fragen sind deshalb im Vorfeld zu klären:

- □ Ist die Überwachung der IT-Systeme auf Angriffe und Unregelmäßigkeiten auch außerhalb der Kernarbeitszeiten gewährleistet?
- □ Wer trifft (kurzfristig) die finale Entscheidung, Teile oder notfalls auch das gesamte IT-System der Hochschule vom Netz zu trennen? Bedarf es einer gemeinsamen Leitungsentscheidung oder hat z. B. die Leitung des Rechenzentrums die Möglichkeit, die Abschaltung eigenverantwortlich vorzunehmen?
- □ Welche Schritte sind operativ für eine IT-Abschaltung notwendig?
- □ Welche Zugänge zu den Räumlichkeiten sind für die Kappung und den Abschluss der Rechner notwendig?
- □ Welche Einrichtungen sind mit den Netzen der Hochschule u. U. noch verbunden (z. B. Universitätskliniken, An-Institute, Kooperationspartner)?
- □ Welche/r externe Dienstleister ist bzw. sind zur Krisenbewältigung der Cyberattacke vorgesehen und zu informieren?

Ein Großteil dieser Fragen lässt sich bereits im Vorfeld und unabhängig von einer konkreten Cyber-Attacke abstimmen. So unter anderem die Frage, wer (kurzfristig) die Entscheidung zum Trennen des IT-Systems der Hochschule vom Netz und zu einem möglichen Shutdown treffen darf. Eine pauschale Beantwortung dieser Frage ist nur bedingt möglich, da sich (aus juristischer Sicht) einerseits die Verantwortlichkeiten für eine solche weitreichende Entscheidung aus den einschlägigen Hochschulgesetzen ergeben. Andererseits liegt (aus fachlicher Sicht) die Expertise über das Vorliegen einer Cyber-Attacke und die möglichen Auswirkungen bzw. die Notwendigkeit zur kurzfristigen Trennung unter Umständen auf Fach- und nicht auf Leitungsebene. Ggf. kann die Entscheidung über das Trennen vom Netz und das Herunterfahren der Systeme mit externen Expert:innen vorab diskutiert werden. Die befragten Hochschulen berichten, dass sie hier sehr unterschiedlich vorgegangen sind: Trennung nach Beschluss der Hochschulleitung und nach Empfehlung der Fachabteilung bzw. Trennung durch die Fachabteilung und Information/Bestätigung der Hochschulleitung im Nachgang. Diese Grundfrage sollte daher jede Hochschule in Vorbereitung auf eine mögliche Cyber-Attacke intern abstimmen und beantworten. Unabhängig von der jeweiligen Entscheidung muss das Hauptziel sein, eine schnelle Reaktions- und Handlungsfähigkeit zu ermöglichen.

Vorbereitung Zeitpunkt 0:

Wichtig ist die **durchgängige Überwachung der IT-Systeme** zur Detektion sicherzustellen, damit **auch am Wochenende, Feiertagen und in Randzeiten** ein Angriff so schnell wie möglich festgestellt werden kann. Ist dies nicht mit eigenem Personal zu gewährleisten, muss diese Überwachung ggf. an externe Dienstleister vergeben werden.

Im Vorfeld ist es notwendig, **Entscheidungs- und Kommunikationswege** zu klären, die im Falle des Cyber-Angriffs genutzt werden können. Zu klären ist weiterhin, wer unmittelbar beim Entdecken eines Angriffs informiert werden muss. Wer kann und muss die Einschätzung, dass es sich um einen Cyber-Angriff handelt, bestätigen? Festgelegt werden muss auch, wer die Entscheidungen über den **Shutdown der IT-Systeme und das Trennen der Systeme vom Netz treffen** kann. Nur wenn dies schnell geschieht, kann eine Verbreitung und eine Infektion anderer Systemteile verhindert werden.

Unabhängig davon sollte der – bereits vorab festgelegte – **IT-Krisenstab (im Folgenden IT-Kernteam genannt)** seine Tätigkeit aufnehmen, um die notwendigen Maßnahmen abzustimmen und einzuleiten. Dazu sind die Mitglieder des IT-Kernteams bestimmt bzw. Vertretungsregelungen etabliert. Es gibt Listen mit privaten Telefonnummern und E-Mailadressen, um die Erreichbarkeit sicherzustellen. Die Hochschulleitung ist frühzeitig einzubinden bzw. ein übergeordneter Krisenstab (siehe Tag 1 in Kap. 2.1) einzuberufen.

2 Reaktionsphase

2.1 Tag 1

Im Idealfall hat das interne **IT-Kernteam** bereits zum Zeitpunkt 0 die Tätigkeit aufgenommen bzw. spätestens im Verlaufe des Tags 1 nach dem Cyber-Angriff. Parallel sollte der **zentrale Krisenstab** zusammenkommen. Die Trennung von IT-Kernteam und einem zentralen, übergeordneten Krisenstab empfiehlt sich, um das IT-Kernteam weitestgehend von Steuerungs- und Koordinierungsmaßnahmen sowie Kommunikationsaufgaben zu entlasten. Die Ermittlungsbehörden (Polizei, Landeskriminalamt) sollten frühzeitig eingeschaltet und Strafanzeige gestellt werden. Was für die Strafverfolgung benötigt wird, ist abhängig von der Art und dem Umfang des Angriffes. In Folge einer Cyber-Attacke ist ein erhöhter Kommunikationsaufwand notwendig. Folgende Fragen sind deshalb im Vorfeld zu klären:

- □ Wer gehört zum IT-Kernteam, wer gehört zum zentralen Krisenstab? Welche weiteren Krisenstäbe für Notfälle generell sind u. U. bereits etabliert und können kurzfristig einberufen bzw. umgewidmet werden?
- □ Liegen die aktuellen (auch privaten) Kontaktdaten der für das Krisenmanagement wichtigen Personen (Mitglieder von IT-Kernteam, zentralem Krisenstab und weiteren Krisenstäben, IT-Admins, Hochschulleitung, Hochschulkommunikation, …) vor? Sind alternative Kommunikationswege vorbereitet?
- □ Besteht eine Vertretungsregelung? Welche Personen/Vertretungen sind unbedingt notwendig und müssen ggf. bei Abwesenheit (u. a. Urlaub) sofort eingebunden bzw. zurückgeholt werden?
- □ Welche räumlichen Möglichkeiten inkl. IT-Notfall-Versorgung stehen permanent zur Verfügung?
- □ Welche externen Stellen wie Aufsichtsbehörde/Ministerien, Polizei/Landeskriminalamt, Kooperationspartner etc. müssen informiert werden?
- □ Liegt u. U. eine Kontaktaufnahme durch die Angreifer und ein Erpressungsversuch vor? Muss eine schnelle Einbindung der Polizei und der zuständigen Stellen (z. B. Cyber-Abwehr der Landeskriminalämter) erfolgen?
- □ Ist eine Verletzung des Schutzes personenbezogener Daten möglich oder absehbar, so dass die Datenschutzbehörde informiert und eingebunden werden muss?
- □ Sind auch dezentrale Strukturen und IT-Systeme betroffen, so dass die Fakultäten/Fachbereiche entsprechend eingebunden werden müssen? Welche dezentralen Ressourcen (Personal, IT-Struktur etc.) stehen zur Verfügung und können genutzt werden?
- □ Wer koordiniert die Schadensaufnahme?

Unabhängig von der Schwere des Angriffes ist eine rasche **Kommunikation** in die Hochschule hinein und nach extern notwendig. Zunächst ist zu klären, welche Kommunikationskanäle noch zur Verfügung stehen und welche Personen Zugriff darauf haben. In Fällen von umfassenden Angriffen kann es zum Ausfall aller klassischen Kommunikationswege (inkl. E-Mail, Telefon, Intranet, Homepage) kommen, so dass auf alternative Kommunikationsmittel (insb. private E-Mail-Accounts, Messenger Dienste, Social Media-Accounts) ausgewichen werden muss. Zudem muss geprüft werden, ob Handlungsnotwendigkeiten bezüglich der

Hochschulgebäude (z. B. Schließanlagen für den Gebäudezugang, Klimaanlagen für kritische Labore und Instrumente, Aufzüge etc.) bestehen. Folgende Fragen sind deshalb im Vorfeld zu klären:

- □ Hat das für Kommunikations- und Öffentlichkeitsarbeit zuständige Referat einen Krisenplan? Wer übernimmt die Krisenkommunikation hochschulintern und nach außen? Wer übernimmt die zentrale Sprecher:innenfunktion – Präsident:in/Rektor:in, zuständige:r Vizepräsident:in/Kanzler:in, Pressesprecher:in? Wer übernimmt im Bedarfsfall die Vertretung?
- □ Welche Vorlagen und Textbausteine für eine erste Krisenkommunikation stehen zur Verfügung? Wer hat darauf Zugriff?
- □ Steht eine sichere, technische Notfallinfrastruktur zur Verfügung? Gibt es nicht kompromittierte Laptops, Drucker, Telefonanschlüsse? Welche Alternativen stehen jeweils zur Verfügung? Wer hat die Zugänge?
- □ Welche Räume sind von einem Ausfall elektronischer Schließsysteme betroffen, welche nicht?

Weiterhin sollten alle **Führungskräfte** der Hochschule informiert werden, da je nach Schwere der Cyber-Attacke unterschiedlichen Folgen auf die jeweiligen Arbeitsbereiche und Organisationseinheiten zukommen können. Zudem sind die Führungskräfte die zentralen Multiplikator:innen sowie erste Ansprechpersonen im Krisenfall. Gleiches gilt für die verschiedenen Leitungsgremien der Hochschule auf zentraler und dezentraler Ebene, die ebenfalls frühzeitig einzubinden sind. Folgende Fragen sind deshalb im Vorfeld zu klären:

- □ Stehen die Kontaktdaten aller Führungskräfte zur Verfügung – auch wenn unter Umständen die Kommunikationswege und -systeme der Hochschulen ausgefallen sind?
- □ Bestehen Handlungsanleitungen für die einzelnen Führungskräfte in (Cyber-)Krisenfällen?
- □ Welche Mittel stehen zur Verfügung, um alle Mitglieder der Hochschule zu informieren und bei Bedarf zu koordinieren (um z. B. das Einschalten technischer Geräte zu verhindern)?

Vorbereitung Tag 1:

Die **Mitglieder des IT-Kernteams und des zentralen Krisenstabs** sind bestimmt. Es gibt Listen mit privaten Telefonnummern und E-Mailadressen, um die Erreichbarkeit sicherzustellen, wenn u. a. der E-Mail- und Telefon-Service der Hochschule ausgefallen ist. Zudem stehen **Räumlichkeiten** zur Verfügung, die über eine entsprechende Ausstattung für die Krisenbewältigung verfügen. Ebenso ist festgelegt, zu welchen festen Tageszeiten (z. B. täglich um 8:00 Uhr sowie um 17:00 Uhr) die Krisenstäbe zusammenkommen.

Des Weiteren kann die interne und externe Kommunikation im Falle eines Cyber-Angriffs vorbereitet werden, wie etwa der **Aufbau und laufende Aktualisierung einer externen Homepage.** Diese kann sofort aktiviert werden, um zentrale Informationen für die Öffentlichkeit aber auch für die Hochschulmitglieder bereitzustellen. Ggf. können auch mit dem Hosting der externen Homepage zusammen Reserve-E-Mails oder Notfallinformationen auf Social-Media-Kanälen vorbereitet werden. Vorbereitet werden kann auch die Information vor Ort für Mitarbeiter:innen und Studierende (z. B. Regelung von Druckmöglichkeiten bzw. von Alternativen). Grundsätzlich dient die Vorbereitung dazu, schnell alle Statusgruppen der Hochschule zu erreichen und bei Bedarf **alternative Kommunikationswege** (z. B. zentraler Telefondienst, Gruppenchats, Social Media-Kommunikation) zu etablieren.

Die Zugriffsmöglichen und Zugänge für die **Hochschulgebäude** sind zumindest in einem ersten Überblick geregelt bzw. es beginnen etablierte Notfallverfahren (z. B. Schließanlagen für den Gebäudezugang, Klimaanlagen für kritische Labore und Instrumente). Gleichfalls ist etabliert, ob und wie Hochschulangehörige Hochschulgebäude betreten können und diese entsprechend auch informiert sind (z. B. Ausfall von Aufzügen, Störung der Notrufsysteme).

Der **Einsatz von externen IT-Expert:innen** ist unbedingt ratsam. Diese können beispielsweise bei der Abwehr des Angriffes, bei der Forensik oder beim Wiederaufbau der IT-Systeme unterstützen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt hier eine Liste von Firmen zur Verfügung, die diese **Notfallunterstützung** leisten. Da der Markt an IT-Sicherheitsberatung begrenzt und oftmals eine kurzfristige Unterstützung zeitlich nicht möglich ist, ist es umso wichtiger, bereits im Vorfeld **externe Serviceverträge** abzuschließen. Bei der Auswahl externer Dienstleister ist auf Kenntnisse von Hochschulen, ihrer Organisation und ihrer IT-Infrastruktur zu achten. Unabhängig davon ist es zentral, auch innerhalb der eigenen Organisation die vorhandene IT-Expertise (u. a. dezentrale Einheiten, Kooperationspartner) zu kennen und bei Bedarf einzubinden.

Weiterhin sollte in Abstimmung mit den Ermittlungsbehörden rasch die **forensische Sicherung**, d. h. das Isolieren und Sichern von möglichen Beweismitteln erfolgen. Alle Maßnahmen sollten dokumentiert werden, um rückwirkend (z. B. bei Datenschutzfragen) entsprechend auskunftsfähig zu sein. Die Dokumentation des Angriffes sowie der eingeleiteten Maßnahmen ist parallel wichtig für mögliche **Rechtsfragen**. Die Ermittlungsbehörden sollten frühzeitig eingeschaltet und Strafanzeige gestellt werden.

2.2 Woche 1

Es empfiehlt sich, einen **zweiten, erweiterten Krisenstab** zu etablieren, an dem auch Leiter:innen beispielsweise der Fachbereiche/Fakultäten sowie wichtiger zentraler Einrichtungen, Leitungsgremien und Statusgruppen beteiligt sind, um eine gute Krisenbewältigung über die gesamte Hochschule zu organisieren. Wenn einzelne Bereiche der Hochschule durch den Angriff besonders stark betroffen sind, kann es sinnvoll sein, einen Krisenstab mit einem besonderen Fokus auf diese Bereiche (z. B. auf Verwaltung) einzurichten. Hierbei ist aber abzuwägen: einerseits zwischen einer breiten Einbindung von Entscheidungsträger:innen und Multiplikator:innen sowie andererseits hinsichtlich einer notwendigen Begrenzung, um die Handlungs- und Entscheidungsfähigkeit zu sichern. Zugleich sollte die Anzahl an Schnittstellen und die Anzahl an Gremiensitzungen beschränkt werden – auch um die Arbeitsbelastung der zentralen Akteur:innen nicht unnötig zu erhöhen. Klare Entscheidungsstrukturen helfen die Handlungsfähigkeit zu gewährleisten. Bei der Besetzung der Krisenstäbe ist es zudem notwendig, die „Übersetzungsleistung“ z. B. zwischen IT-Expert:innen und Verwaltungsstrukturen zu berücksichtigen. Folgende Fragen sind deshalb zu beantworten:

- □ Wer gehört zum erweiterten Krisenstab? Wer kann eine zentrale „Übersetzer“- und Mittlerrolle übernehmen?
- □ Wie ist das Zusammenspiel von zentralem Krisenstab und erweiterten Krisenstab (informierend, beratend, unterstützend)?
- □ Wer übernimmt die Schnittstelle zwischen IT-Kernteam, zentralem und erweiterten Krisenstab?
- □ Sind bereits etablierte Verbindungen z. B. zwischen IT- und Kommunikationsabteilung vorhanden, die entsprechend genutzt werden können?

Sollte eine Kontaktaufnahme durch die Angreifer und ein **Erpressungsversuch** vorliegen, müssen spätestens jetzt staatliche Stellen wie Polizei, Landeskriminalamt bzw. die zuständigen Stellen für Cyber-Kriminalität und die Staatsanwaltschaft eingebunden werden – soweit dies nicht schon sofort nach Feststellung des Cyber-Angriffes erfolgt ist. Die Kommunikation mit möglichen Erpressern sollte nur in Abstimmung mit oder direkt über die staatlichen Stellen erfolgen. Im Falle von Lösegeldforderungen sollten diese nicht erfüllt werden. Vielmehr rät das Bundesamt für Sicherheit in der Informationstechnik (BSI) ausdrücklich von einer Lösegeldzahlung bei Cyber-Angriffen ab. Zum einen führe dies zur Finanzierung krimineller Aktivitäten, die – da erfolgreich – zu einer Fortsetzung und Ausweitung von Cyber-Attacken führen kann (vgl. u. a. Bodden, E. et al. 2022).[2] Zum anderen besteht keine Garantie, dass die Täter im Falle einer Zahlung die Entschlüsselung wirklich ermöglichen bzw. zu einem späteren Zeitpunkt nicht erneut angreifen. Abgesehen davon kann eine Lösegeldzahlung eine Strafbarkeit begründen – von einer Verletzung der Sorgfaltspflicht über Unterstützung einer kriminellen Vereinigung bis hin zum Risiko der Terrorismusfinanzierung.

Die Arbeitsbelastung vor allem in den Bereichen IT und Kommunikation ist in Folge eines Cyber-Angriffs überdurchschnittlich hoch, während andere Bereiche aufgrund des Ausfalls der notwendigen IT-Systeme unter Umständen nicht arbeitsfähig sind. Eine kurzfristige **Personal(um-)steuerung** ist notwendig, um die Arbeitsfähigkeit im direkten Nachgang zu einer Cyber-Attacke zu erhalten. Zu prüfen ist, wie zusätzliches Personal

[2] Fast 100 führende IT-Sicherheitsexpert:innen haben einen offenen Brief gegen Lösegeldzahlungen bei Ransomware-Attacken veröffentlicht: „Lösegeldzahlungen sind jedoch bei Ransomware die Wurzel allen Übels.“ (ebenda)

insbesondere im Bereich der IT und der Kommunikation eingebunden werden kann (z. B. externe Dienstleister, Fachkräfte aus anderen Verwaltungsbereichen und den Fachbereichen/Fakultäten, Abordnungen von kooperierenden Hochschulen). In Vorbereitung auf diese Situation können **Kooperationsvereinbarungen** mit anderen Hochschulen (z. B. an einem gemeinsamen Standort/Campus oder in übergreifenden Projektstrukturen) zur gegenseitigen Unterstützung getroffen werden. Allerdings sollte diese unter strengen Sicherheitsabwägungen erfolgen, um nicht fremde IT-Systeme zu kompromittieren. Folgende Fragen sind deshalb zu beantworten:

- □ Wer kann ressourcentechnisch (Hardware, Software, Räume, Personal) unterstützen? Welche Systeme oder Anwendungen können unter Umständen an andere Hochschulen bzw. an externe Dienstleister ausgelagert bzw. alternativ – unter Berücksichtigung der nötigen Sicherheitsvorgaben – genutzt werden? Zu den wichtigsten Systemen zählen hier sicherlich Learning Management, Campus Management sowie Personal- und Finanzverwaltung, die für die Lehre und den Betrieb der Hochschule essenziell sind. Für eine solche alternative Nutzung sind tägliche Back-Ups der zentralen Dienste auf externen Servern unverzichtbar, um einen Datenverlust so gering wie möglich zu halten.
- □ Gibt es die Möglichkeit, externe Dienstleister zur Unterstützung einzubinden?
- □ Gibt es Arbeitsbereiche, die durch Systemausfall nicht arbeitsfähig sind, die aber mit ihren Personalkapazitäten bei der Krisenbewältigung unterstützen können?

In der ersten Woche nach einem Cyber-Angriff müssen auch **Prioritäten zur Wiederherstellung der Systeme** entschieden und abgestimmt werden. Je nach Schwere des Angriffes sowie des Zeitpunktes im Semesterverlauf gilt es, entsprechend abzuschichten: ein Angriff in der vorlesungsfreien Zeit hat andere Folgen, als wenn dies in der Bewerbungs-, Einschreibungs- oder Prüfungsphase erfolgt. Weiterhin gilt es zu bedenken, welche sekundären Folgeerscheinungen u. U. auftreten können – wenn z. B. aufgrund eines Ausfalls der Finanz-IT-Systeme Gehaltsauszahlungen nicht mehr erfolgen können oder aufgrund einer außer Betrieb genommenen Gebäudetechnik kritische Experimente oder Forschungsanlagen nicht fortgesetzt bzw. betrieben werden können. Folgende Fragen sind deshalb zu beantworten:

- □ Welche Systeme sind wie stark vom Angriff betroffen?
- □ Wie ist die Wiederherstellung der Systeme zu priorisieren? Welches Kerngeschäft ist in der aktuellen Phase, in der sich die Hochschule befindet, absolut prioritär zu behandeln?
- □ Wer dokumentiert die Schäden und wie werden diese dokumentiert? Wer wird mit der Berichtslegung beauftragt?

Im kritischsten Fall muss davon ausgegangen werden, dass keine internen Kommunikationsmittel mehr zur Verfügung stehen und nur noch öffentliche Kommunikationskanäle (zum Beispiel Social Media) als Alternative genutzt werden können. Die **Kommunikation** kann damit nicht mehr zielgruppenspezifisch gelenkt und angepasst werden. Die Mitteilung über den Fortschritt bei der Wiederherstellung der IT-Systeme (was im Sinne einer internen Kommunikation gewünscht ist) kann u. U. dazu führen, dass diese (extern) von den Angreifern beobachtet wird. Findet eine Cyberattacke mit Lösegeldforderungen statt, so ist es durchaus möglich, dass die Angreifer den Druck beispielsweise durch gezielte Angriffe auf die Notfallwebseite der

Hochschule erhöhen. Damit wird die Kommunikation über den Vorfall hochsensibel und sollte bei Bedarf professionell extern begleitet werden. Folgende Fragen sind zu beantworten:

- □ Funktionieren die alternativen Kommunikationswege in die Hochschulöffentlichkeit oder muss nachgesteuert werden?
- □ Reichen die eigenen Kompetenzen und Ressourcen zur Organisation der Kommunikation aus?
- □ Ist die Kommunikation zwischen IT-Kernteam und Kommunikations- und Öffentlichkeitsarbeit etabliert? Wer gibt die Meldungen frei, wer kann bei Bedarf unterstützen, wenn IT-Fachfragen in allgemein verständliche Meldungen „übersetzt“ werden müssen?
- □ Wer übernimmt die Übersetzung der wichtigsten Meldungen mindestens ins Englische? Steht eine Notfall-Homepage mit Informationen in deutscher und englischer Sprache zur Verfügung?
- □ Wie wirkt sich der aktuelle Stand der IT-Systeme auf die verschiedenen Statusgruppen der Hochschule aus und wie können diese regelhaft darüber informiert werden?
- □ Wie können Nachfragen der Hochschulmitglieder erfasst und kanalisiert werden? Steht z. B. ein zentrales Info-Telefon zur Verfügung?
- □ In welcher „Berichtsperiodizität“ sollte intern und extern über die Entwicklung informiert werden? Welche externen Partner (z. B. Ministerien) sollten regelhaft über den Fortschritt informiert werden?

Da Hochschulen personenbezogene Daten verarbeiten, sind sie verpflichtet, **Datenschutzvorfälle** zu melden. Gemäß Artikel 33 der Datenschutz-Grundverordnung (DSGVO) müssen Hochschulen bei einer Verletzung des Datenschutzes von personenbezogenen Daten die zuständigen Behörden innerhalb von 72 Stunden nach Bekanntwerden der Sicherheitsverletzung informieren. Teil der Meldung ist eine präzise Beschreibung, welche Art von Datenschutzverletzung vorliegt, und wie viele Datensätze betroffen sind. Die Hochschule muss eine Abschätzung abgeben, welche Folgen durch die Datenschutzverletzung eintreten. Nach Artikel 34 der DSGVO muss die Hochschule betroffene Personen zudem unverzüglich informieren, sofern mit der Datenschutzverletzung ein hohes Risiko für die persönlichen Rechte und Freiheiten dieser Personen einhergeht. Bei Cyber-Angriffen mit Ransomware ist daher eine rasche Analyse der genauen technischen Umstände des jeweiligen Angriffs erforderlich, um zu klären, ob tatsächlich persönliche Informationen entwendet worden sind. Wenn bei einem Cyber-Angriff mit Ransomware Daten nur verschlüsselt worden sind, ohne dass persönliche Informationen entwendet wurden, liegt nicht zwangsläufig eine meldepflichtige Datenschutzverletzung vor. Erst im Anschluss einer solchen Analyse lässt sich entscheiden, ob jeweils eine interne Dokumentation der Datenschutzverletzung, eine Meldung an die zuständigen Behörden und eine Information der betroffenen Personen (oder mehrere dieser Punkte zugleich) erforderlich ist.

Vorbereitung Woche 1:

Wichtig ist die **Vorbereitung** eines dauerhaften **Krisenmanagements**, um neben dem zentralen Krisenstab auch einen erweiterten Krisenstab bzw. bei Bedarf verschieden Krisenstäbe einberufen zu können. Die Besetzung der Krisenstäbe kann im Vorfeld definiert sowie Zuständigkeiten und Abstimmungsprozesse festgelegt werden. Es geht darum, eine stringente **Krisenkommunikation** aufzubauen und schnelle Entscheidungsprozesse zu etablieren, um handlungsfähig zu sein. Auch ist zu überlegen, ob im Vorfeld Verträge mit externen Spezialisten für Krisenkommunikation abgeschlossen werden, die zum einen die Organisation sowie die Arbeit der Krisenstäbe und zum anderen bei der Krisenkommunikation unterstützen.

Sollte ein **Erpressungsversuch** vorliegen, sollten spätestens jetzt unbedingt die Polizei, das Landeskriminalamt bzw. die zuständige Stelle für Cyber-Kriminalität und die Staatsanwaltschaft eingebunden werden. Auch wenn zu Beginn einer Cyber-Attacke noch kein Erpressungsversuch vorliegt, empfiehlt sich die zügige Einbindung der staatlichen Stellen. Reaktionen auf Lösegeldforderung und die Kommunikation mit den Erpressern sollte immer in Abstimmung mit Polizei und/oder LKA erfolgen. Die Zahlung von Lösegeld ist keine Option, da es einerseits zur Finanzierung krimineller Aktivitäten führt und andererseits Strafbarkeitsrisiken bestehen. Weiterhin ist abzuschätzen, inwieweit durch die Cyber-Attacke eine **Verletzung des Datenschutzes** vorliegt. Innerhalb von 72 Stunden müssen die zuständigen Behörden nach Bekanntwerden der Sicherheitsverletzung informiert werden.

In Folge einer Cyber-Attacke kann es in einzelnen Bereichen zu einer starken Arbeitsbelastung führen, so dass entsprechend eine **Personal(um-)steuerung** notwendig ist. Parallel kann zur Unterstützung einer schnellen Krisenbewältigung wie auch hinsichtlich zusätzlicher (Personal-)Ressourcen helfen, im Vorfeld **Kooperationsmöglichkeiten mit anderen Hochschulen oder externen Dienstleistern** zu sondieren. Im Falle der Krise kann dadurch kurzfristig mit IT-Personal ausgeholfen, den Mitarbeitenden der eigenen Hochschule Räumlichkeiten zur Verfügung und/oder zentrale IT-Systeme (bspw. Learning Management-, Campus-Management- ERP-Systeme) als Backups zur Verfügung gestellt werden. Ein täglicher Datenaustausch zu solchen Backup-Systemen ist zentral, wobei die Backups außerhalb der eigenen Hochschule bereitgehalten werden sollten. Eine Nutzung der ausgelagerten und nicht kompromittierte Backups muss immer auch einer Risikoabschätzung vorrausgehen, um eine Ausweitung des Angriffs auf andere IT-Systeme von Kooperationspartnern wie z. B. anderen Hochschulen zu verhindern.

Um möglichst zügig Entscheidungen über die **Prioritäten zur Wiederherstellung** der betroffenen Systeme zu treffen, kann im Vorfeld ein zeitliches Schema erstellt werden, dass die Priorität der zentralen Prozesse einer Hochschule im zeitlichen Verlauf darstellt. Die laufende Priorisierung ist abhängig von der Schwere des Angriffes sowie vom Zeitpunkt im Semesterverlauf.

2.3 Monat 1

Im Laufe der ersten Woche(n) kann mit hoher Wahrscheinlichkeit abgeschätzt werden, wie weitreichend der durch den Cyber-Angriff entstandene Schaden ist und welche Systeme betroffen bzw. nicht betroffen sind. In Folge gilt es zu klären, welche zentralen, ausgefallenen Dienste zu ersetzen sind, aber auch welche Aufgaben alternativ umgesetzt werden müssen. Besonders wichtig für die Hochschulen sind sicherlich, Bewerbungs- und Immatrikulationsprozesse zu ermöglichen, Prüfungen durchzuführen und Zahlungen vornehmen zu können (möglichst nicht durch das manuelle Ausfüllen von Papier-Überweisungsträgern und Ein- und Auszahlungsscheinen). Je nach Schwere des Angriffes und des Zeitpunktes im Studienjahr müssen die anstehenden **Aufgaben fortwährend priorisiert** werden. Folgende Fragen sind deshalb zu beantworten:

- □ Welche Aufgaben sind für die Grundfunktionen der Hochschule prioritär und welche Aufgaben können verschoben werden – in den einzelnen Verwaltungs- und Struktureinheiten wie auch in der Abwägung von Lehre und Forschung sowie der dazugehörigen IT-Systemlandschaft?
- □ Welche Workarounds stehen zur Verfügung?
- □ Wie kann die Rückkehr in den Regelbetrieb gelingen? Welche Systeme/Anwendungen müssen prioritär wieder zur Verfügung stehen, bei welchen Systemen/Anwendungen kann die Wiederherstellung verschoben werden?

Die weitere Entwicklung ist abhängig vom jeweiligen Krisenfall und der tatsächlichen Beeinträchtigung der IT-Systeme. Datensicherungen und der **Wiederaufbau von IT-Systemen** aus Backup-Systemen (z. B. für Standardsysteme wie Campus Management) kann u. U. bereits ohne einen konkreten Anlass oder Cyber-Angriff vorab erprobt werden. In dem Sinne kann auch das Herunterfahren bzw. das Trennen vom Netz sowie die Auswirkungen innerhalb der gesamten IT-Systemlandschaft ohne konkreten Ernstfall simuliert und in schrittweisen Testläufen durchgeführt werden. Dies ist umso wichtiger, um einschätzen zu können, was beim Abschalten bzw. beim Wiederanfahren der Systeme mögliche Folgeerscheinungen sein können. Folgende Fragen sind deshalb zu beantworten:

- □ Welche Testläufe und Simulationen bestehen bereits, um die Folgen des Abschaltens bzw. der Wiederaufnahme von Systemen einschätzen zu können? Welche möglichen Kettenreaktionen bestehen?
- □ Welche externe IT-Verbindungen bestehen z. B. mit Kooperationspartnern oder Systemanbietern, die in den Wiederaufbau mit eingebunden werden müssen?

Je nach Schwere des Angriffes können die **Folgen für die Hochschul-IT-Landschaft** sehr unterschiedlich sein: von der raschen Wiederaufnahme einzelner Systeme mit Hilfe vorhandener, gesicherter Backups bis hin zum vollständigen (langwierigen) Neuaufbau der gesamten IT-Landschaft. In der Zeit der Krisenbewältigung und des Wiederaufbaus der IT-Systeme ist die Hochschule – vor allem im Fall von Erpressungsversuchen und einer möglichen externen Beobachtung – sehr angreifbar. In dem Sinne gilt es abzuwägen zwischen einem schnellen Wiederaufbau der IT-Systeme und einem sicheren, aber längeren Neuaufbau der Systeme bzw. der IT-Landschaft abzuwägen. In dem Sinne kann der Wiederaufbau auch als Chance verstanden werden, die gesamte IT-Struktur der Hochschule neu auszurichten und z. B. die Maßnahmen für die IT-Sicherheit zu stärken. Folgende Fragen sind deshalb zu beantworten:

- □ Welche Grundidee ist konsensfähig und soll umgesetzt werden: rascher Wiederaufbau der IT-Systeme oder (langsame) Neuausrichtung und Verbesserung der IT-Struktur?
- □ Liegen aktuelle Pläne für eine Aktualisierung der IT-Landschaft sowie der IT-Sicherheitsmaßnahmen vor?

Neben der Wiederherstellung der Systeme geht es auch darum, die (langfristige) **Personalsteuerung** im Blick zu behalten, um unterschwellige Folgen einer Cyber-Krise (z. B. Arbeitsüberlastung, Krisenerfahrung) zu adressieren. Damit verbunden ist der Aspekt einer „wellenartigen" Arbeitsbelastung, die sich verstärken kann, wenn nach der Rückkehr in den Normalbetrieb offene Arbeitsstände nachbearbeitet sowie Überstunden/Überlast nicht abgebaut werden. Wie bei jeder Krisenerfahrung können langfristige, unterschwellige Folgen auftreten. Folgende Fragen sind deshalb zu beantworten:

- □ Welche Möglichkeiten bestehen, um Personal zu entlasten? Welche zusätzlichen Personalressourcen stehen kurzfristig zu Verfügung (zum Beispiel durch strukturelle Unterlast in Abteilungen, die nicht arbeitsfähig sind, aber anderweitig unterstützen können)?

Abhängig von den Folgen des Cyber-Angriffes und den Auswirkungen auf die IT-Landschaft kann es u. U. zu einer ganzen Reihe von **Sekundärschäden** kommen. Dies kann beispielsweise den Forschungsbereich betreffen, wenn u. a. Labore bzw. einzelne Laborausstattungen nicht mehr zur Verfügung stehen und Experimente oder Versuchsreihen zeitweise nicht mehr durchgeführt werden können. Es kann aber auch Folgen für die Berichtslegung z. B. gegenüber Drittmittelgebern haben, wenn z. B. Datenbestände und Forschungsergebnisse nicht mehr zur Verfügung stehen. Neben der Wiederherstellung der jeweiligen Daten, Berichtsformate oder Systeme ist es ebenfalls wichtig, mögliche Fristverletzungen, Berichtspflichten oder Anschlussfolgen mindestens im Blick zu behalten.

Vorbereitung Monat 1:

Um in der akuten Krisensituation die Entscheidungslast zu reduzieren, ist es hilfreich, im Rahmen eines **Kontinuitätsmanagement** die Aufgaben und Funktionen der Verwaltung zu priorisieren. Es geht darum Strategien, Pläne und Handlungen zu entwickeln, um für die zentralen Prozesse alternative Abläufe so schnell wie möglich zur Verfügung zu stellen. Eine vorbereitende Definition der zentralen Aufgaben, um den hochschulischen Betrieb aufrechtzuerhalten, kann helfen, die Handlungsfähigkeit schnell herzustellen. Dies dient der Priorisierung der Vielzahl der Aufgaben.

Gleichzeitig ermöglicht eine solche Planung entscheiden zu können, welche Systeme bzw. welche Prozesse und Anwendungen in welcher Reihenfolge wiederhergestellt werden müssen. Dabei sind verschiedene zeitliche Szenarien zu berücksichtigen, die auch mit dem Zeitpunkt des Angriffs zu tun haben (z. B. Bewerbungsfristen, Prüfungszeiträume).

Der **Wiederaufbau der IT-Systeme** und das Trennen bzw. das Wiederhochfahren von Systemen kann unabhängig von einer konkreten Cyber-Attacke simuliert werden. Ziel ist es, in schrittweisen Testläufen mögliche Folgeerscheinungen und Kettenwirkungen einzuschätzen. Parallel gilt es abzuwägen, inwieweit welche IT-Systeme bzw. Anwendungen rasch wieder zur Verfügung stehen müssen oder ob perspektivisch der (langfristige) Neuaufbau inkl. Verbesserung der IT-Sicherheitsstrukturen umgesetzt werden soll.

Ein weiteres Thema ist die (langfristige) **Personalsteuerung**, um Effekte einer „wellenartigen" Arbeitsbe- und -entlastung zu adressieren und vor allem mögliche Folgen der Krisenerfahrung (z. B. Arbeitsüberlastung) zu bewältigen. Auch mögliche **Sekundärschäden** gilt es zu beachten (z. B. gegenüber Drittmittelgebern, Forschungsprojekten oder Kooperationspartnern).

3 Normalisierungsphase

Notwendig ist es anzuerkennen, dass es sich bei einem Cyber-Angriff um eine Krisenerfahrung für die Hochschule als Organisation sowie auch alle Hochschulmitglieder als Personen handelt. Eine Krisenerfahrung, die einen eindeutigen Anfang hat und in dem Sinne einen Abschluss sowie eine Rückkehr in den Normalbetrieb benötigt. Abhängig von den Folgeerscheinungen von Cyber-Angriffen ist dieser „eindeutige Abschluss" aber umso schwieriger, da es zu Ungleichzeitigkeiten kommt. Während bspw. der Großteil der IT-Systeme und der Anwendungen schon wieder einsatzfähig ist, kann es parallel in einzelnen Bereichen noch zu Beeinträchtigungen oder Folgeerscheinungen kommen. Damit verbunden sind Aufgaben der langfristigen **Personalsteuerung und Fürsorgepflicht** für die einzelnen Mitarbeiter:innen, um unterschwellige Folgen der Cyber-Krise (z. B. Überlastung, innere Kündigung) zu adressieren (vgl. Northwave 2022). Dies gilt umso mehr, da die Überlastung bereits in einem vom Fachkräftemangel stark gekennzeichneten Umfeld stattfindet. Die Frage der Überlast betrifft nicht nur die Bereiche IT und Kommunikation, sondern auch andere Bereiche, in denen es zunächst eine strukturelle Unterlast in Folge von Systemausfällen gegeben hat und die dann, nach erfolgreicher Wiederherstellung, die liegengebliebenen Aufgaben nacharbeiten müssen (z. B. Papierbuchungen nachdigitalisieren etc.). Folgende Fragen sind deshalb zu beantworten:

- Wie können Überstunden kompensiert werden? Gibt es die Möglichkeit, diese abzubauen bzw. teilweise auszuzahlen? Dies ist eine zentrale Aufgabe der jeweiligen Führungskräfte hier individuelle Wünsche und Vereinbarungen zu treffen. Es ist aber sinnvoll verschiedene Modellvarianten abzustimmen.
- Sind der Arbeitsschutz und das Gesundheitsmanagement eingebunden?

Zudem gilt es, die **Krise als Lernerfahrung** zu nutzen, wobei es neben der Verbesserung der IT-Struktur auch um die Weiterentwicklung der Krisenfähigkeit der Hochschulorganisation geht. Es ist empfehlenswert, neben der kurzfristigen Wiederherstellung der Handlungsfähigkeit den Cyber-Angriff auch als Chance zu verstehen, die IT-Struktur und IT-Governance in ihrer Gesamtheit zu überarbeiten und langfristig neu aufzustellen. Je nach Massivität des Angriffs muss jedoch mit Widerständen gerechnet werden, da die Krisenerfahrung auch zu einem Vertrauensverlust in die IT und die Digitalisierung führen kann. Darüber hinaus gibt es ggf. auch noch andere Effekte, die zu berücksichtigen sind, wie etwa ein Vertrauensverlust bei Wirtschaftspartnern, bei Verbundpartnern, bei den Studierenden.

Generell jedoch sollte das Krisenmanagement nach Cyber-Attacken in das grundlegende **Krisenmanagement** der Hochschule eingebunden werden. Die Hochschulen können hierfür die etablierten Instrumente und Methoden nutzen und im Detail ergänzen. Es sollte bereits im Vorhinein eine Kohärenz zwischen IT-Notfallplan und allgemeinem Krisenmanagement angestrebt werden, um Vertrauen und Handlungssicherheit zu gewährleisten. Darüber hinaus kann die Situation eines Cyber-Angriffes auch dazu genutzt werden, um grundsätzliche Überlegungen zu den Umgehungslösungen (Workarounds) in der Verwaltung anzustellen und festzulegen.

Vorbereitung der Normalisierungsphase

Es können im Vorfeld durch den Arbeits- und Gesundheitsschutz Maßnahmen konzipiert werden, die auf die **Bewältigung einer Krisenerfahrung** abzielen. Zudem können **Regelungen** vorbereitet und abgestimmt werden, wie mit Phasen von **starker Über- und Unterlast** umgegangen wird und ob z. B. für die hochüberlasteten Mitarbeitenden auch finanzielle Kompensationen der Überstunden vorgehalten werden können.

Zudem ist es wichtig, **Prozesse des organisationalen Lernens** zu etablieren, um diese Krisenerfahrung auswerten zu können und daraus Handlungshinweise für zukünftige Krisenereignisse zu generieren. Die Wiederherstellung der IT-Systeme kann eine Chance sein, die IT-Landschaft insgesamt neu aufzustellen und die IT-Sicherheit im speziellen auszubauen.

Generell sollte das Krisenmanagement nach Cyber-Attacken als **Thema in das Krisenmanagement** der Hochschule aufgenommen und integriert werden. Etablierte Instrumente und Methoden können hierfür genutzt und in die bestehenden Verfahren bzw. Zuständigkeiten eingebunden wurde. Die Themen IT-Sicherheit und die Gefahr einer Cyber-Attacke sind neue, permanente Daueraufgaben für Hochschulen und Hochschulleitungen und sollten entsprechend dauerhaft adressiert werden.

Ein Cyber-Angriff und die möglichen Folgen sind eine Krisenerfahrung für die Hochschule und sollten im weitesten Sinne einen **Abschluss** erfahren – um die individuelle und institutionelle Bewältigung sowie den Übergang in den Normalbetrieb zu erleichtern. Mögliche Instrumente hierfür sind insbesondere eine offene Kommunikation über die Führungsstrukturen sowie eine „Abschlussveranstaltung“.

4 Zusammenfassung und weitere Präventionsmaßnahmen

Auch wenn die konkreten Folgen eines Cyber-Angriffs sehr unterschiedlich ausfallen und sich für jede Hochschule sehr individuelle Krisenszenarien entwickeln können, so bleibt doch jeder Cyber-Angriff nicht ohne Wirkung. In der Regel führen diese mindestens zu einer Überprüfung oder sogar zu einer Anpassung und Weiterentwicklung der IT-Sicherheitsstruktur und damit der IT-Struktur insgesamt sowie der damit verknüpften (IT-)Governance. Im Extremfall kann bei der Wiederherstellung der IT-Systeme bzw. beim Wiederaufbau der gesamten IT-Landschaft auf eine angriffssichere Architektur (z. B. Zentralisierung, verbesserte Back-Up-Struktur) hingearbeitet werden. Hierbei ist abzuwägen, welche Systeme rasch wieder zur Verfügung gestellt werden müssen und inwieweit ein langsamerer dafür aber gründlicher Wiederaufbau langfristig von Vorteil ist. IT-Sicherheit, die Vorbereitung auf einen möglichen Cyber-Angriff und die Entwicklung eines (Cyber-)Krisenmanagements sind neue, permanente Daueraufgaben für Hochschulen und Hochschulleitungen. Im Endeffekt gilt: „Nach dem Angriff ist vor dem (nächsten) Angriff“. Es ist keine Frage mehr, ob ein solcher Angriff erfolgt, sondern eher eine Frage, wann und wie erfolgreich dieser ist.

Um die Resilienz der Hochschulen zu stärken, können einige Maßnahmen bereits im Vorfeld ergriffen werden. So geht es darum, ein Krisenmanagement aufzubauen und zu etablieren, um schnell handlungs- und entscheidungsfähig zu sein. Ein im Vorfeld entwickeltes Kontinuitätsmanagement hilft dabei, Alternativprozesse für zentrale, hochrelevante Vorgänge zu definieren und die Systeme entlang der Relevanz für die Hochschule wiederherzustellen. Auch wenn dies nicht im Fokus dieser Handreichung steht, so gilt doch grundsätzlich, für die verschiedenen digitalen administrativen Prozesse eine entsprechende Notfallplanung zu entwickeln bzw. anzupassen. Es bedarf mindestens eines Notfallplans für die wichtigsten IT-unterstützten Fachverfahren – insbesondere im Bereich Studium und Lehre (u. a. Learning Management- und Campus-Management-Systeme) sowie in zentralen Verwaltungsbereichen (Personal- und Finanzsysteme). Inwieweit hierbei auch Forschungssysteme prioritär mit einbezogen werden sollen, sollte jede Hochschule intern bereits vorab klären. Mit diesen Maßnahmen soll insgesamt die Arbeitsfähigkeit der Hochschulen in den zentralen Bereichen gesichert werden, wofür eine Priorisierung der Aufgaben und Systeme notwendig ist. Damit verbunden sind technische Aspekte wie externe Backups, Standby-Systeme bzw. Standby-IT-Infrastrukturen sowie allgemein eine IT-Notfallplanung. Aufgrund der zunehmenden Vernetzung der IT mit der Gebäude- und Betriebstechnik generell wie auch im speziellen mit den überwachungsbedürftigen Anlagen gilt es ebenfalls, mögliche Folgen für diesen Bereich zu beachten. An dieser Stelle sei darauf hingewiesen, dass unter der Federführung des Vereins „Zentren für Kommunikation und Informationsverarbeitung“ (ZKI) bereits ein „IT-Grundschutz-Profil für Hochschulen“ (ZKI 2022) entwickelt und veröffentlicht wurde. Um die verschiedenen Risiken eines Cyber-Angriffes zu adressieren, ist die Beschäftigung mit diesem IT-Grundschutz-Profil als vorbereitende Maßnahmen zu empfehlen.

Das Thema der IT-Security sollte unbedingt als dauerhaftes Thema behandelt werden. Die Etablierung eines Chief Information Security Officer (CISO) auf strategischer Ebene sowie der/die IT-Sicherheitsbeauftragte/n auf operativer Ebene können sich z. B. um die Entwicklung, Anpassung, Umsetzung und Kontrolle von IT-Sicherheitsrichtlinien, den Aufbau eines Sicherheitsmanagements und Durchführung von Schutzbedarfsanalysen kümmern. Es geht darum, in der gesamten Hochschule Aufmerksamkeit und Sensibilität für dieses

Thema zu erzeugen. Dazu gehört auch die Vermittlung einer Fehlerkultur, die das Melden von Fehlhandlungen (z. B. versehentliches Anklicken von Phishing-Mails) nicht ahndet, sondern die schnelle Anzeige positiv bewertet. Denn nur, wenn Fehler oder wahrgenommene Unregelmäßigkeiten im System unverzüglich gemeldet werden, kann ein gutes IT-Notfallmanagement greifen und die größten Schäden verhindern. In diesem Sinne ist es auch zu überlegen, ob parallel zu anderen Krisenerscheinungen ebenfalls Übungsszenarien bzw. Stresstests entwickelt und erprobt werden sollten, um möglichst schnell reagieren zu können.

Unabhängig davon ist ein Cyber-Angriff – je nach Schwere des Angriffes – eine Krisenerfahrung für die Hochschule, die im Sinne Verarbeitung und Überwindung entsprechend auch adressiert werden muss. Die Wiederherstellung der IT-Systeme und damit der Arbeitsfähigkeit als Organisation sind vordergründig sicherlich die zentralen Aufgaben. Für die Organisation Hochschule müssen aber im Nachgang auch Aspekte wie Krisenbewältigung, Personalsteuerung und Fürsorgepflicht sowie Arbeitsschutz und Gesundheitsfürsorge beachtet werden. Die Gefahr einer Cyber-Attacke muss entsprechend auch im Arbeitsschutz und der Betriebssicherheit betrachtet werden. Es können zudem eine ganze Reihe von Folgeerscheinungen auftreten – u. a. (externer) Reputationsverlust, (internes) Misstrauen gegenüber IT und Digitalisierung allgemein, Vertrauensverlust gegenüber der Führungsstruktur und/Krisenfähigkeit der Hochschule.

5 Literatur

Alle Links wurden zuletzt am 09.11.2023 abgerufen:

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

Bodden, E. et al. (2022). Lösegeldzahlungen bei Ransomware-Angriffen: ein geostrategisches Risiko.
https://ransomletter.github.io/.

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.

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

Anlagen

Anlage 1 Checkliste zur Vorbereitung der einzelnen Phasen

Checkliste für „Tag 0“:

- □ Die Überwachung der IT-Systeme auf Angriffe und Unregelmäßigkeiten ist auch in den Randzeiten (nachts, Wochenende, Feiertage) gewährleistet. Ggf. sind zur Sicherstellung Verträge mit externen Dienstleistern abgeschlossen worden.
- □ Es ist festgelegt, wer (kurzfristig) die finale Entscheidung, das gesamte IT-System (oder Teile) der Hochschule vom Netz zu trennen, trifft.
- □ Die Schritte für die IT-Abschaltung sind definiert und festgeschrieben.
- □ Die Zugänge zu den Räumlichkeiten, die für die Kappung vom Netz und den Abschluss der Rechner bereitstehen, sind geregelt.
- □ Das IT-Kernteam ist bestimmt.
- □ Aktuelle Kontaktdaten (auch private Daten außerhalb der Hochschulnetze) liegen vor. Vertretungsregelungen sind bestimmt. Es ist definiert, wer ggf. bei Abwesenheit zurückgeholt werden muss.
- □ Ein externer Dienstleister zur Krisenbewältigung der Cyberattacke ist ausgewählt, über einen Rahmenvertrag verpflichtet und kann umgehend informiert werden.
- □ Eine Liste mit Kontaktdaten der Notfallstellen der mit den Netzen der Hochschulen verbundenen Einheiten (z. B. Universitätskliniken, An-Institute, Kooperationspartner) ist aktuell und steht zur Verfügung.

Checkliste für „Tag 1“:

- □ Der zentrale Krisenstab ist bestimmt. Auch hierzu liegen aktuelle Kontaktdaten (auch private Daten außerhalb der Hochschulnetze) vor und Vertretungsregeln sind festgelegt.
- □ Es stehen Räume für das IT-Kernteam sowie für den zentralen Krisenstab zur Verfügung, die mit einer sicheren, technische Notfallinfrastruktur wie etwa Rechner, Drucker sowie Telefonanschlüsse ausgestattet sind.
- □ Die Zusammenarbeit des Krisenstabs und des IT-Kernteams ist festgelegt.
- □ Eine Liste mit externen Stellen wie Aufsichtsbehörde/Ministerium, Polizei/Landeskriminalamt, Kooperationspartner ist erstellt und den Mitgliedern des Krisenstabs bekannt.
- □ Im Falle eines Erpressungsversuches liegen die Kontaktdaten der zu informierenden staatlichen Stellen (Polizei, Landeskriminalamt bzw. Cyber-Abwehr des LKA, Staatsanwaltschaft) vor.
- □ Die Kontaktdaten der Datenschutzbehörde liegen ebenfalls vor, falls eine Verletzung personenbezogener Daten absehbar ist.
- □ Die Einbindung der dezentralen Strukturen und Fakultäten/Fachbereiche ist geregelt. Es ist bekannt, welche dezentralen Ressourcen (Personal, IT-Struktur etc.) im Krisenfall zur Verfügung stehen.
- □ Die Schadensaufnahme ist koordiniert und definiert.
- □ Ein ausgearbeiteter Krisenplan des Referats für Kommunikations- und Öffentlichkeit liegt vor. Es ist abgestimmt, wer die Krisenkommunikation hochschulintern und nach Außen übernimmt und die

zentrale Sprecherfunktion wahrnimmt (z. B. Präsident:in, zuständige:r Vizepräsident:in/Kanzler:in, Pressesprecher:in)
- □ Für die Krisenkommunikation liegen Vorlagen und Textbausteine vor, die auf verschiedenen Medien zugänglich sind.
- □ Eine sichere, technische Notfallinfrastruktur steht zur Verfügung. Die Zugänge sind geregelt und Alternativen z. B. Laptops, Drucker, Telefonanschlüsse stehen ebenfalls bereit.
- □ Eine extern gehostete Notfallhomepage steht zur Verfügung und ist aktuell. Notfallmeldungen mit Verweis auf die Notfallhomepage sind für Social-Media-Kanäle vorbereitet.
- □ Es ist bekannt, welche Räume von einem Ausfall elektronsicher Schließsysteme betroffen sein könnten.
- □ Die Kontaktdaten aller Führungskräfte der Hochschule stehen zur Verfügung. Für die Führungskräfte stehen zudem Handlungsanleitungen in (Cyber-)Krisenfällen bereit.
- □ Kommunikationswege für alle Statusgruppen sind festgelegt. Es ist bekannt, welche Statusgruppen welche Informationen über den Zustand welcher Systeme haben müssen (z.B. um das Einschalten von Systemen zu verhindern, Informationen zu Zugängen zu Gebäuden zu geben etc.).

Checkliste für „Woche 1“:

- □ Der erweiterte Krisenstab ist festgelegt. Spezifische Rollen wie z. B. „Übersetzer“ und Mittlerrolle sind festgelegt.
- □ Das Zusammenspiel von zentralem Krisenstab und erweiterten Krisenstab ist definiert und abgestimmt.
- □ Die personelle Schnittstelle zwischen IT-Kernteam, zentralem und erweiterten Krisenstab ist bestimmt.
- □ Etablierte Verbindungen z. B. zwischen IT und Kommunikationsabteilung sind vorhanden.
- □ Es sind Vereinbarungen mit anderen Hochschulen und/oder externen Dienstleistern geschlossen, um ressourcentechnisch (Hardware, Software, Räume, Personal) unterstützen zu können. Dazu können unter Berücksichtigung der nötigen Sicherheitsvorgaben unter Umständen Teilsysteme an andere Hochschulen/externe Dienstleister ausgelagert bzw. alternativ (z. B. als SaaS) genutzt werden (z. B. Moodle, HISinOne, SAP bzw. die entsprechenden Systeme andere Hersteller).
- □ Die Möglichkeit, externe Dienstleister zur Unterstützung einzubinden, ist geregelt.
- □ Die Leistungsfähigkeit der hochschuleigenen Kommunikationsabteilung im Krisenfall ist bestimmt und es sind Rahmenvereinbarungen mit externen Dienstleistern zur Unterstützung der Kommunikation abgeschlossen.
- □ Es ist definiert, welche Systeme in welcher Phase (vorlesungsfreie Zeit, Prüfungszeit, Jahreswechsel, Einschreibefristen) prioritär zu behandeln sind.
- □ Die Dokumentation der Schäden (Schadensaufnahme) ist gesichert und die Beauftragung zur Berichtslegung ist geregelt.
- □ Alternative Kommunikationswege intern und extern sind etabliert. Bei Bedarf steht externe Unterstützung bzw. Beratung zur Verfügung.
- □ Im Sinne einer einheitlichen Sprachregelung ist geregelt, wer die Meldungen frei gibt und wer bei der „Übersetzung“ von IT-Fachfragen in leicht verständliche Pressemitteilungen unterstützen kann.
- □ Die Übersetzung der wichtigsten Meldungen bzw. der Homepage mind. ins Englische ist geregelt.

- □ Für die interne Erfassung und Weiterleitung von Nachfragen der Hochschulmitglieder steht ein eigener Kanal (z. B. Info-Telefon) zur Verfügung.
- □ Die „Berichtsperiodizität“ z. B. gegenüber externen Partnern ist festgelegt.

Checkliste für „Monat 1“:

- □ Ein detaillierten Kontinuitäts- und Widerherstellungsplan liegt vor, indem festgelegt ist, welche Systeme und Prozesse für die Grundfunktionen als Hochschule prioritär sind und bei welchen Aufgaben die Widerherstellung verschoben werden kann.
- □ Für wichtige Prozesse sind alternative Abläufe festgelegt und definiert.
- □ Für die Rückkehr in den Regelbetrieb stehen Ablaufpläne und Informationsmaterialien zur Verfügung.
- □ Um auf das Abschalten bzw. das Wiederhochfahren der Systeme vorbereitet zu sein, sind Simulationen und schrittweise Testläufe durchgeführt.
- □ Es ist absehbar, welche möglichen Folgen bzw. welche IT-Verbindungen zur Kooperationspartnern oder Systemanbietern bestehen.
- □ Aktuelle Pläne für eine Aktualisierung der IT-Landschaft sowie der IT-Sicherheitsmaßnahmen liegen vor und sind bekannt.
- □ Szenarien und Pläne für den Wiederaufbau der IT-Landschaft inkl. einer Verbesserung der IT-Sicherheitsstrukturen liegen vor und können kurzfristig umgesetzt werden.
- □ Für die Personalplanung gibt es in den Abteilungen Einschätzungen zu Über- und Unterlast der Beschäftigten im Falle von Systemausfällen und erste Überlegungen zu möglichen Unterstützungen und Umschichtungen.

Checkliste „Normalisierungsphase“:

- □ Modelle zur Überstundenkompensation sind entwickelt, abgestimmt und den Leitungspersonen bekannt.
- □ Arbeitsschutz und das Gesundheitsmanagement sind auf die Krisenbewältigung vorbereitet und haben entsprechende Angebote und Programme entwickelt.
- □ Modelle und Prozesse des organisationalen Lernens sind entwickelt, um die Krisenerfahrung auswerten zur können und die Verbesserungen für folgende Krisenereignisse zu gewinnen.
- □ Es gibt ein aktualisiertes Maßnahmenpaket zur Awareness-Schulungen der Mitarbeitenden und Studierenden.
- □ Die Einbindung des Themas IT-Sicherheit/Cyber-Angriffe in das bestehende Krisenmanagement der Hochschule (thematisch, personell und strukturell) ist umgesetzt.

Anlage 2 Weiterführende Literatur

Ergänzend zu der in der Handreichung verwendeten Literatur (Kap. 5) sind im Folgenden weiterführende Leseempfehlungen angegeben.

Alle Links wurden zuletzt am 09.11.2023 abgerufen:

BITKOM (2016). Kosten eines Cyber-Schadensfalles. Leitfaden. https://www.bitkom.org/sites/main/files/file/import/160426-LF-Cybersicherheit.pdf.

Bundesministerium des Innern (BMI) (2014). Leitfaden Krisenkommunikation. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/leitfaden-krisenkommunikation.pdf?__blob=publicationFile&v=4.

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

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.

Europäische Agentur für Sicherheit und Gesundheitsschutz am Arbeitsplatz (2022). Einbeziehung des Arbeitsschutzes in die Bewertung von Risiken im Bereich der Cybersicherheit. https://osha.europa.eu/sites/default/files/Cybersecurity-and-OSH_EN.pdf.

European Union Agency for Network and Information Security (enisa) (2014). Report on Cyber Crisis Cooperation and Management. https://www.enisa.europa.eu/publications/ccc-study/@@download/fullReport.

Schwartmann, R., Ritter, S. (2020). Wer haftet beim Verlust von Forschungsdaten? Forschung & Lehre, 2020 *https://www.forschung-und-lehre.de/recht/wer-haftet-beim-verlust-von-forschungsdaten-2998.*

Shulman, H., Waidner, M. (2023). Forschung muss besser geschützt werden. *Forschung & Lehre.* https://www.forschung-und-lehre.de/management/forschung-muss-besser-geschuetzt-werden-5449.

Verwaltungs-Berufsgenossenschaft (VBG) (2022). Umgang mit Bedrohung und Notfällen. Risiken kennen und angemessen handeln. https://www.vbg.de/SharedDocs/Medien-Center/DE/Broschuere/Themen/Arbeitsschutz_organisieren/Umgang_mit_Bedrohungen_und_Notf%C3%A4llen_VBG_Fachwissen.pdf;jsessionid=166F36057361581E12998379BBED33C5.live2?__blob=publicationFile&v=1.

Anlage 3 Nützliche Adressen

Alle Links wurden zuletzt am 09.11.2023 abgerufen:

Bundeskriminalamt (BKA), Wiesbaden, www.bka.de

- Übersicht Cybercrime inkl. Adressen der Polizeien der Bundesländer, der Abteilung Cybercrime im BKA sowie dem Nationalen Cyber-Abwehrzentrum https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html.

Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, www.bsi.bund.de

- BSI-Standard 200-4 Business Continuity Management 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.
- Qualifizierte Dienstleister (externe Berater) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Qualifizierte-Dienstleister/qualifizierte-dienstleister_node.html.
- IT-Notfallkarte https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/it-notfallkarte_node.html.

Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAUA), www.baua.de

- Technische Regel für Betriebssicherheit (TRBS 11115-1): Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen https://www.baua.de/DE/Angebote/Regelwerk/TRBS/TRBS-1115-Teil-1.html.

Deutsches Forschungsnetz (DFN), www.dfn.de

- DFN-CERT GmbH: Dienstleister für Sicherheit im Internet https://www.dfn-cert.de/index.html.

European Union Agency for Cybersecurity (enisa), https://www.enisa.europa.eu/

- Cyber Crisis Management https://www.enisa.europa.eu/topics/cyber-crisis-management.

Zentren für Kommunikation und Informationsverarbeitung e.V. (ZKI), www.zki.de

- ZKI-Arbeitskreis Informationssicherheit https://www.zki.de/ueber-den-zki/arbeitskreise/arbeitskreis-informationssicherheit/.

Weitere Initiativen und Projekte (Auswahl):

- Allianz für Cyber-Sicherheit (BSI) https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/home_node.html.
- Nationales Forschungszentrum für Angewandte Cybersicherheit (Athene) https://www.athene-center.de/.
- Digitale Hochschule NRW: Informationssicherheit und Datenschutz https://www.dh.nrw/diskurse/Informationssicherheit%20und%20Datenschutz-13 https://www.mkw.nrw/hochschule-und-forschung/digitalisierung-hochschule-und-wissenschaft/cybersicherheit.
- Stabsstelle Informationssicherheit bayrischer Hochschulen und Universitäten https://www.tha.de/Rechenzentrum/IT-Sicherheit/Stabsstelle-Informationssicherheit.html.
- Landesarbeitskreis Niedersachsen für Informationstechnik / Hochschulrechenzentren (LANIT) https://www.lanit-hrz.de/aktuelles.