Komplett offline

Rückblick auf den Cyberangriff an der Universität Gießen

| IM GESPRÄCH | **Die Universität Gießen war 2019 als eine der ersten Hochschulen in Deutschland von einem Cyberangriff betroffen. Wie verlief das Krisenmanagement im Rückblick? Welche Lehren zieht die Universität aus dem Hackerangriff? Fragen an die Kanzlerin.**

Forschung & Lehre: Frau Kraus, was ging Ihnen als erstes durch den Kopf, als Sie von dem Cyberangriff erfahren haben?

Susanne Kraus: Mein erster Gedanke am Nachmittag des 8. Dezember 2019 galt der Sorge um die Forschungsdaten der Wissenschaftlerinnen und Wissenschaftler, die Prüfungsdaten der Studierenden und auch die in der Verwaltung vorhandenen und für die Leitung einer Universität erforderlichen Informationen – etwa im Bereich Personal und Finanzen. Nicht auszudenken, wenn diese unwiederbringlich verloren gewesen wären und welche Auswirkungen dies auf die Zukunft der Universität Gießen gehabt hätte.

Foto: JLU / Rolf K. Wegst

Susanne Kraus *ist Kanzlerin der Universität Gießen.*

F&L: Welche Forderungen haben die Angreifer gestellt?

Susanne Kraus: Eine explizite Lösegeldforderung wurde nicht gestellt. Wir wurden nicht erpresst und gehen davon aus, dass der Angriff rechtzeitig gestoppt werden konnte.

F&L: Konnten Sie unmittelbar auf vorhandene Notfallpläne zurückgreifen?

Susanne Kraus: Wir verfügen bzw. verfügten über diverse Notfallpläne – damals aber noch nicht für diesen speziellen Fall. Der Angriff erfolgte an einem Sonntag und fiel auf, weil es in der IT der Veterinärmedizin zu Unregelmäßigkeiten kam. Um Schlimmeres zu vermeiden, hat ein Notfallteam des Hochschulrechenzentrums (HRZ) in Abstimmung mit dem Präsidium die Universität umgehend vom Internet getrennt und die Server- und Speichersysteme kontrolliert heruntergefahren. Gegen 18 Uhr war die Universität Gießen komplett offline. Noch am selben Tag haben wir die zuständigen Stellen des Landes informiert und Kontakt zu fachlich ausgewiesenen Firmen aufgenommen. Bereits am Sonntagabend kam der zentrale Krisenstab unter der Leitung des Präsidenten zusammen; dazu gehörten die Mitglieder des Präsidiums, die Leitung des HRZ, der IT-Sicherheitsbeauftragte, verschiedene Verwaltungsangehörige und die Pressestelle. Letztere hatte eine wesentliche Rolle in der Krisenbewältigung, da es sowohl innerhalb als auch außerhalb der Universität einen enormen Bedarf an verlässlichen und transparenten Informationen gab. Während sich ein zweiter Krisenstab im HRZ (unter der Leitung des für die IT zuständigen Vizepräsidenten) ganz auf die technische Krisenbewältigung konzentrieren konnte, wurden die wesentlichen Management- und Kommunikationsentscheidungen im zentralen Krisenstab getroffen. Um die Mitglieder der Universität mit Informationen zu versorgen und Anweisungen im Hinblick auf die IT-Sicherheit weiterzugeben, musste der zentrale Krisenstab neue Kommunikationswege finden: Dazu gehörten neben den sozialen Medien eine Behelfshomepage, eine Telefonhotline und mehrere große Informationsveranstaltungen in der Aula, in der die Präsidiumsmitglieder und HRZ-Verantwortlichen teilweise stundenlang die Fragen von Studierenden und Beschäftigten beantworteten.

F&L: Welche Maßnahmen mussten zur Wiederherstellung der digitalen Infrastruktur ergriffen werden und in welcher Reihenfolge?

Susanne Kraus: In den ersten Wochen mussten alle an der Universität verwendeten Computer, Laptops und Tablets auf einen möglichen Virenbefall geprüft werden; es ging um mehr als 6.000 Windows-basierte Endgeräte. Gleichzeitig war das HRZ damit beschäftigt, die IT-Infrastruktur wieder aufzubauen. Um die IT-Dienste wie z.B. E-Mail wieder nutzen zu können, mussten sich sämtliche Nutzerinnen und Nutzer der Universität Gießen – 28.000 Studierende und mehr als 5.700 Beschäftigte – neue Passwörter abholen und dazu persönlich in der Turnhalle unseres Sportcampus erscheinen. An dieser gigantischen Abholaktion, die

von einem Team der Verwaltung organisiert wurde, haben 200 Personen mitgewirkt. Noch vor Weihnachten konnten die allermeisten Universitätsmitglieder wieder auf ihre E-Mails zugreifen. Ab Januar waren bereits viele Basisdienste wieder zugänglich, wie zum Beispiel die Homepage der Universität Gießen, das Prüfungsverwaltungssystem FlexNow, Stud.IP oder der Zugriff auf die E-Medien im Bibliothekssystem. Das HRZ, dessen Mitarbeiterinnen und Mitarbeiter in den ersten Wochen und Monaten extremen Belastungen ausgesetzt waren, hat die Chance genutzt und die Systeme ganz neu strukturiert und weitere IT-Sicherheitsstandards etabliert.

»Wir haben den Cyberangriff zum Anlass genommen, unsere IT-Governance und -Sicherheitsstruktur neu aufzustellen.«

F&L: Konnten Sie bei der Lösung der Probleme ausschließlich auf Fachleute aus Ihrer Universität zurückgreifen oder haben Sie auch Expertise von außen eingeholt?

Susanne Kraus: Die Bewältigung einer solchen Krise ist ganz auf sich gestellt nicht zu schaffen, da die personellen Ressourcen des HRZ dafür nicht annähernd ausreichen, auch wenn Fachkräfte aus den dezentralen Bereichen das HRZ sehr stark unterstützt haben. Daher waren wir auf externe Unterstützung angewiesen – etwa durch Institutionen aus dem universitären Umfeld und Fachfirmen. Ich bin auch den anderen hessischen Hochschulen sehr dankbar, die uns durch die Entsendung von einschlägig ausgewiesenen Mitarbeiterinnen und Mitarbeitern tatkräftig unterstützt haben, wie zum Beispiel bei den sehr zeitaufwändigen Überprüfungen der Endgeräte. Teilweise haben uns benachbarte Hochschulen auch Arbeitsplätze zur Verfügung gestellt, damit zum Beispiel Buchungen vorgenommen werden konnten, die für den Jahresabschluss wichtig waren.

»Die Präsidiumsmitglieder befanden sich – wie der komplette Krisenstab – jeden Tag vor neuen Herausforderungen.«

F&L: Welche Aufgaben musste die Hochschulleitung übernehmen?

Susanne Kraus: Wie bereits erwähnt, waren alle fünf Präsidiumsmitglieder Teil des Krisenstabs. Im Rahmen unserer jeweiligen Ressortzuständigkeit mussten wir die Auswirkungen von #JLUoffline auf so gut wie alle Bereiche der Universität in den Blick nehmen und die notwendigen Maßnahmen einleiten. Im Bereich der Lehre haben wir beispielsweise großzügig Fristen verlängert, um die Folgen der Cyberattacke für die Studierenden abzufedern. Mit dem Wissenschaftsministerium war zu klären, wie sich die Rückmeldefristen der Studierenden für das Sommersemester gestalten und wie Bewerbungen für das Sommersemester erfolgen sollten, da die digitalen Wege noch nicht zur Verfügung standen. Die Präsidiumsmitglieder befanden sich – wie der komplette Krisenstab – jeden Tag vor neuen Herausforderungen, auf die wir schnell und unbürokratisch reagieren mussten. Daneben gab es es noch das Tagesgeschäft, das wir auch nicht ruhen lassen konnten. Ich kann mich gut daran erinnern, dass wir genau in dieser Zeit den derzeit laufenden Hochschulpakt mit dem Land verhandelt haben.

F&L: Wann wurde die Polizei eingeschaltet? Konnte die Polizei die Täter ermitteln?

Susanne Kraus: Wir haben unmittelbar nach der Entdeckung des Cyberangriffs – bereits am Montag, 9. Dezember 2019 – Anzeige erstattet. Im Anschluss haben wir uns ganz auf die Bewältigung der Krise konzentriert. Für Fragen zum Ausgang der Ermittlungen wäre das Landeskriminalamt der richtige Ansprechpartner.

F&L: Wie lange hat es im Endeffekt gedauert, bis alle Schäden wieder behoben waren?

Susanne Kraus: Ein annähernder Normalbetrieb war im ersten Quartal 2020 wieder möglich. Bis zum Herbst des Jahres war das HRZ noch mit den Aufräumarbeiten beschäftigt – was durch die Coronapandemie ab März 2020, die weitere Digitalisierungsaufgaben mit sich brachte, zusätzlich erschwert wurde. Wir haben zudem den Cyberangriff zum Anlass genommen, unsere IT-Governance und -Sicherheitsstruktur neu aufzustellen, um künftig vor solchen Angriffen besser geschützt zu sein. Bereits vor der Cyberattacke hatten wir einen Prozess zur Weiterentwicklung der IT-Gesamtstrategie angestoßen. Aus dem Sicherheitsvorfall konnten dafür weitere Schlussfolgerungen gezogen werden, die uns in den letzten Jahren beschäftigt haben.

F&L: Können Sie im Rückblick sagen, welche Maßnahmen, die im Vorfeld ergriffen wurden, besonders wichtig waren?

Susanne Kraus: Wir waren die erste Universität in Deutschland, die in diesem Ausmaß von einer Cyberattacke getroffen wurde. Um eine solche Krise zu bewältigen, braucht es eine starke Führung, kurze Entscheidungswege, unkonventionelle Lösungen sowie eine kontinuierliche und transparente Kommunikation. Ich denke, wir können für uns in Anspruch nehmen, dass uns das beim #JLUoffline-Krisenmanagement weitgehend gelungen ist. Mit im Vorfeld getroffenen Maßnahmen hat das zunächst nichts zu tun – es handelt sich aber um Faktoren, die in jeder Krise von Bedeutung sind.

F&L: Wie wirkt sich die Sorge oder auch Angst vor zukünftigen Hackerangriffen auf die tägliche Arbeit der Hochschulangehörigen aus?

Susanne Kraus: Wir versuchen, bei der Sensibilisierung für sicherheitsrelevante Themen alle Mitglieder und Angehörigen mitzunehmen. Dies beginnt bereits beim Arbeitsbeginn im Rahmen des Onboardings sowie beim Ausscheiden aus der Universität, indem Zugriffsberechtigungen gelöscht werden. Aufgrund der hohen Fluktuation sowohl bei Beschäftigten als auch bei Studierenden ist dies eine stetige Aufgabe. Unser HRZ hat in Zusammenarbeit mit externen Partnern ein vielfältiges Angebot an Awareness- und Weiterbildungsmaßnahmen geschaffen. Dazu zählen ein PocketGuide zur IT-Sicher-

Kurze Chronologie der Ereignisse

8. Dezember 2019:
Hacker dringen in die Netzwerke der Universität ein. Die Universität fährt ihre Server aus Sicherheitsgründen herunter.

9. Dezember 2019:
Extern gehostete Notfall-Homepage geht online. Krisenhotline wird für Fragen der Studierenden und Beschäftigten eingerichtet.

12. Dezember 2019:
Die Universität setzt sämtliche Passwörter für alle rund 38 000 E-Mail-Konten zurück. Die Studierenden und Beschäftigten müssen sich die neuen Passwörter persönlich abholen.

13. Dezember 2019:
Die Verteilung von Virenscanner-Sticks beginnt, um alle Windows-basierten Endgeräte der Beschäftigten zu überprüfen.

19. Dezember 2019:
Es wird bekanntgegeben, dass bei dem Hackerangriff eine Schadsoftware namens "Ryuk" verwendet wurde.

20. Dezember 2019:
Die E-Mail-Kommunikation der Mitglieder und Angehörigen ist über ihre universitären Konten wiederhergestellt.

6. Januar 2020:
Reguläre Webseite und Lehrveranstaltungssystem Stud.IP gehen wieder online.

20. Januar 2020:
WLAN Eduroam ist für Studierende wieder zugänglich, wenige Tage später auch für Beschäftigte.

17. Februar 2020:
JLU-Verwaltungsnetz ist wieder online.

6. März 2020:
Alle großen Subnetze der JLU sind wieder online.

Kosten bis einschließlich Mai 2020: 1,7 Millionen Euro.

heit oder eine aktuelle Online-Schulungskampagne. Dabei dürfen wir eines nicht vergessen: Die strengen IT-Sicherheitsbedarfe mit der Freiheit von Forschung und Lehre sowie mit der offenen Kommunikationskultur an einer Hochschule zu vereinbaren, ist nicht immer ganz einfach. Die meisten akzeptieren aber strengere Regelungen, auch wenn dadurch Kommunikationsabläufe erschwert oder verlangsamt werden.

F&L: Sind die Universitäten finanziell gut genug ausgestattet, um sich vor Cyberkriminalität zu schützen?

Susanne Kraus: Wenn der IT-Bereich nicht mehr funktioniert, steht die Hochschule still. Deshalb kann ich jeder Hochschule nur raten, an der IT-Sicherheit als elementarer Aufgabe nicht zu sparen. Es handelt sich eben nicht um eine Aufgabe von vielen, sondern ist das digitale Herz jeder Institution. In Hessen bekommen die Hochschulen ein Globalbudget aufgrund des hessischen Hochschulpaktes, welches bis zum Jahr 2025 um vier Prozent jährlich steigt. Wie viele Mittel daraus für IT-Sicherheit aufgewendet werden, bleibt den Hochschulen überlassen. Hinzu kommt in Hessen der „Digitalpakt Hochschulen“, aus welchem zusätzlich zum Globalbudget auch Mittel für IT-Sicherheit zur Verfügung stehen.

F&L: Welche Erwartungen haben Sie an die zuständigen Ministerien oder an die Hochschulrektorenkonferenz?

Susanne Kraus: Ich würde mir wünschen, dass von den zuständigen Stellen Kooperationen und zentrale Beratungsangebote zu IT-Sicherheit im Wissenschaftsbereich stärker als bisher gefördert werden. Diese könnten Themen wie Prävention, Analyse und Hilfe bei der Behebung des Schadens umfassen. Hier könnten im Sinne von Best-Practice-Beispielen auch die Erfahrungen betroffener wissenschaftlicher Einrichtungen eingebracht werden. Denn die Erfahrungen, die wir in Gießen und nach uns weitere Hochschulen gemacht haben, sollten für andere wissenschaftliche Institutionen nutzbar gemacht werden.

F&L: Welche Bilanz, welche Lehren können Sie aus dem Hackerangriff ziehen?

Susanne Kraus: Die Erfahrungen aus #JLUoffline haben gezeigt, dass wir resilienter gegen die Gefahren durch Cyberangriffe werden müssen. Vor diesem Hintergrund strukturieren wir unsere IT-Governance und Sicherheitsarchitektur neu. Dazu gehören gezielte Maßnahmen wie etwa die Einrichtung eines oder einer professoralen Informationssicherheitsbeauftragten, der oder die direkt beim Präsidium angesiedelt sein wird. Ferner wurden die personellen Ressourcen im Bereich der IT-Sicherheit ausgebaut. Außerdem gibt es Vorgaben für ein universitätsweites einheitliches und angemessenes Sicherheitsniveau, das mittlerweile etabliert wurde.

F&L: Die Universität Gießen war als eine der ersten von einem Cyberangriff betroffen. Haben Sie danach mit weiteren angegriffenen Hochschulen in Kontakt gestanden und Ihre Erfahrungen weitergeben können?

Susanne Kraus: Ja, betroffene Hochschulen haben sich in vergleichbaren Situationen an uns gewandt, und es gab immer wieder Kontakte auf verschiedenen Ebenen: Sowohl die Präsidiumsmitglieder als auch unsere IT- oder Kommunikationsverantwortlichen haben bei verschiedenen Gelegenheiten ihre Erfahrungen weitergegeben. Bei mir selbst war das im Rahmen einer Veranstaltung für Kanzlerinnen und Kanzler der Fall.

F&L: Hat die Vielzahl der bisherigen Hackerangriffe auf Hochschulen zu einer Zusammenarbeit der Hochschulen in puncto Cybersicherheit geführt?

Susanne Kraus: Im Rahmen des Digitalpakts Hochschulen findet zu einzelnen IT-Sicherheitsthemen eine Zusammenarbeit hessischer Hochschulen statt. Darüber hinaus tauschen sich die Hochschulen im Akutfall eines Cyberangriffs aus, und es gibt auf Arbeitsebene – etwa im Bereich der Kommunikation – Workshops und Weiterbildungsmaßnahmen. Eine institutionalisierte Zusammenarbeit findet bisher noch nicht statt.

Die Fragen stellte Ina Lohaus.