Cyberangriffe auf Universitäten, Fachhochschulen und deren Bibliotheken – ein unterschätztes Problem?

Stephan Holländer

In regelmäßigen Abständen erscheinen Medienberichte, meist als Kurzmeldungen, über Cyberangriffe auf Hochschulen und ihre Bibliotheken. Sie verschwinden in der Flut der täglichen Berichterstattung so schnell wie sie gekommen sind. Beunruhigend ist die Regelmäßigkeit, mit der solche Nachrichten in verschiedenen Ländern in immer kürzerer Abfolge erscheinen. Sie betreffen nicht nur Hochschulen und Bibliotheken, so waren am letzten Märzwochenende zwei Presseverlage in der Schweiz[1], darunter die Neue Zürcher Zeitung, von einem Cyberangriff betroffen und konnten drei aufeinander folgende Tage nur in einem reduzierten Umfang erscheinen. Ist der Schaden eingetreten, wird versucht, den Betrieb mit Zettelwirtschaft und Notausleihe händisch aufrechtzuhalten, und man fährt die Server und Rechner runter und schließt die betroffene Bibliothek für einige Tage. Außer einer dürren Mitteilung, dass die IT-Systeme wieder hochgefahren wurden und die Kommunikation wieder möglich sei, wird meist nur sehr zögerlich, wenn überhaupt, über den entstandenen Schaden berichtet. Dazu gehören der Abfluss von Daten, verschwundenes Geld oder entwendete Personendaten, die dann wieder im Darknet auftauchen können. Meist ist nach einem solchen Angriff kein Zugriff auf Daten im Hochschulnetz mehr möglich, da diese mittels einer Ransomware-Attacke auf den jeweiligen Servern verschlüsselt wurden

Hackerangriffe sind aus allen deutschsprachigen Ländern bekannt geworden. Unter den betroffenen Hochschulen befinden sich sowohl große Universitäten wie auch Fachhochschulen auf dem Lande. Mitbetroffen sind fast immer auch deren Bibliotheken, die meist in das hochschuleigene IT-Netz eingebunden sind. Im vergangenen Jahr hatten Hacker die Server der Kölner Universitäts- und Stadtbibliothek angegriffen. So auch diejenigen der Justus-Liebig-Universität in Gießen, der Paris Lodron Universität in Salzburg sowie der Universität Neuenburg (frz. Neuchâtel) in der Schweiz. Deren Server wurden unmittelbar nach Bekanntwerden des Angriffs zwar heruntergefahren, aber Dienstleistungen wie Recherche und Ausleihe waren gemäß Mitteilung der Bibliotheken[2] für Tage oder Wochen größtenteils nur noch offline möglich. Allein bereits bestellte und zur Ausleihe bereitgestellte Medien sowie Bücher aus dem Freihandbestand konnten noch als Ausleihen registriert werden. Die Leihfristen wurden unisono bis Ende des Monats verlängert. Bibliothekseigene E-Mail-Adressen waren unbrauchbar geworden[3].

Ähnlich verlief ein Hackerangriff an der Universität Basel sowie an weiteren Schweizer Hochschulen[4]. Auch die Universität Salzburg war Zielscheibe eines solchen Angriffs[5]. Ende März dieses Jahres standen zentrale Systeme für die rund 3.000 Mitarbeitenden während neun Tagen still und gingen dann wieder online. Bezeichnend waren das vielfach betretene Schweigen oder die schmallippigen Statements seitens der verschiedenen Hochschulen, wenn die Medien solche Vorfälle aufgriffen.

Neben einem möglichen Reputationsschaden für die betroffene Hochschule stellt sich die Frage, was Hochschulen und deren Bibliotheken für Hacker so interessant macht? Attraktiv für Hacker ist die Tatsache, dass auf den Servern der Hochschulen viele personenbezogene Daten wie Geburtsdaten, Adressen, Telefonnummern, Mailadressen und Personalausweisdaten gespeichert werden, die für die Anmeldung zum Studium notwendig sind. Hinzu kommen Angaben wie Sozialversicherungsnummern, Bankverbindungen, belegte Vorlesungen und akademische Abschlüsse. Aus all diesen Daten lassen sich Personenprofile erstellen, die für falsche Identitätsprofile und auch für Werbezwecke genutzt werden können.

Aber auch Bibliotheken verfügen über Daten, die potentiell für Hacker interessant sein könnten. Darunter fallen Forschungsdaten, die die Bibliotheken im Auftrag ihrer akademischen Einrichtungen speichern und verwalten. Dazu kommen auch die Zugangsdaten zu Dienstleistungen der Bibliotheken, die auch Personen, die nicht Angehörige der Hochschulen sind, zugänglich gemacht werden können. Diese Zugangsdaten enthalten auch den

1 https://www.srf.ch/news/schweiz/cyberangriff-auf-nzz-hackerangriff-trifft-verschiedene-systeme-der-nzz-und-ch-media

2 https://hochschulforumdigitalisierung.de/de/blog/Hackerangriff-Universitaet-Gießen
https://salzburg.orf.at/stories/3149476/
https://www.watson.ch/digital/ransomware/519378360-universitaet-in-neuchatel-von-cyberangriff-betroffen

3 https://www.forschung-und-lehre.de/politik/cyberangriff-auf-uni-bibliothek-koeln-2835/

4 https://www.forschung-und-lehre.de/politik/hacker-stehlen-gehalt-von-schweizer-hochschulen-3160

5 https://kurier.at/chronik/oesterreich/cyberangriff-auf-universitaet-salzburg-offenbar-beendet/401963651

Foto: © iStock-1144604245

Firewalls, Intrusion-Detection- und Intrusion-Prevention-Systeme sowie die VPN-Technologie sind zur Sicherheit der Netze gegen Cyberangriffe unumgänglich.

Status, ob es sich bei der registrierten Person um einen Hochschulangehörigen oder Auswärtigen handelt. Bei Hochschulangehörigen können diese Daten auch mit den Immatrikulationsdaten gekoppelt sein.

Damit wird dem «Identitätsbetrug» Tür und Tor geöffnet

Spricht man mit Kolleginnen aus Bibliotheken im In- und Ausland, dann ist das Bewusstsein bei Mitarbeitenden und Nutzenden der Bibliotheken zur Möglichkeit von Cyberangriffen auf Bibliotheken nicht sehr präsent, da man kein kommerzielles Interesse an den dort gespeicherten Daten und Informationen sieht. Dieses Verhalten lässt mehr auf ein Bewusstsein wie vor 30 Jahren schließen, als Bibliotheken mit ihren Bibliothekssystemen noch nicht so vernetzt mit der übrigen IT-Infrastruktur ihrer Hochschulen waren. Bibliothekssysteme liefen damals auf Mainframe-Computern und konnten von Terminals in den Bibliotheken bedient werden. Mit den nun zunehmend eingeführten Bibliothekscloudsystemen sind diese Systeme wesentlich exponierter für mögliche Cyberangriffe, da sie einerseits sehr vernetzt sind und von vielen Nutzenden über das World Wide Web genutzt werden und andererseits die Bibliotheken zu großen, bis zu landesweiten Verbünden zusammengeschlossen sind, was in der Konsequenz die damit verbundene mögliche Ausbreitung eines Cyberangriffs wesentlich erhöht.

Hochschulen bieten verschiedene Angriffspunkte mit ihren unzähligen Zugangsmöglichkeiten, ihren unterschiedlichen IT-Richtlinien in den verschiedenen Instituten und mit einer großen Anzahl von angeschlossenen Benutzern unter Dozierenden sowie wissenschaftlichen Mitarbeitenden und Studierenden. Akademische Einrichtungen weisen nicht die gleichen restriktiven Zugangsregulierungen wie die IT-Infrastrukturen beispielsweise der Finanzbranche auf und bieten daher viele Schwachstellen und Einfallspunkte, die leicht für einen Hackerangriff genutzt werden können. Vielfach herrscht auch die weitverbreitete Ansicht, dass Cybersicherheit die ausschließliche Aufgabe der IT-Abteilung der betreffenden Hochschule sei. Dies ist nicht korrekt, denn im englischen Sprachgebrauch wird zu Recht ein Unterschied zwischen Cyber-Security im Sinne von Sicherheit und Cyber-Safety mit der Bedeutung von Schutz gemacht.

Cybersecurity ist der Schutz von Netzwerken, Computersystemen, cyber-physischen Systemen und Robotern vor Diebstahl oder Beschädigung ihrer Hard- und Software oder der von ihnen verarbeiteten Daten sowie der Schutz vor Unterbrechung oder Missbrauch der angebotenen Dienste und Funktionen mittels technischer Maßnahmen wie zum Beispiel einer Firewall aus Hard- und Software. Bei den bedrohten Daten handelt es sich einerseits um persönliche, andererseits um betriebliche oder persönliche Daten.

Cybersafety umschreibt das sichere Verhalten beim Navigieren in Netzwerken und im World Wide Web. Dies betrifft nicht nur die Vorkehrungen und Hilfeleistungen der akademischen Institutionen, aber auch das sichere Verhalten der Nutzenden in den Netzwerken und im World Wide Web. Cybersafety erfordert eine andauernde Sensibilisierung der entsprechenden Nutzergruppen auf mögliche Gefahren, z.B. durch die Zusendung gefälschter E-Mails, die zu einer Handlung wie das Aufrufen einer gefälschten Webseite oder der Weitergabe der Zugangsdaten der Nutzenden zur angeblichen Identifikation auffordern.

Eine der einfachsten Möglichkeiten für Hacker, in ein

Netzwerk einzudringen, besteht darin, Studenten ins Visier zu nehmen. Studenten verbringen mehr Zeit online als jede andere Gruppe von Internetnutzenden. Wenn sie eine höhere Ausbildung beginnen, müssen sie sich eine große Anzahl von Anmeldedaten und Passwörtern merken. Cyberkriminelle wissen, dass Studenten in dieser Zeit verwundbar sind, was sie zum idealen Ziel für einen Online-Angriff macht.

Es gibt zwei weitverbreitete Arten des Cyberangriffs:

1. Der Phishing-Angriff. Unter Phishing versteht man die unrechtmäßige Beschaffung von persönlichen Daten über gefälschte Websites, E-Mails oder Kurznachrichten mit dem Ziel, das Konto des Bestohlenen zu plündern und ihm auch anderweitig persönlich zu schaden. Phishing ist ein englisches Kunstwort, das sich aus «password harvesting» (Passworte sammeln) und «fishing» (Angeln, Fischen) zusammensetzt und somit das Angeln nach Passwörtern mit Ködern bedeutet.
2. Business-E-Mail Compromise (BEC) ist die Ausnutzung einer möglichen Schwachstelle im Unternehmensnetz, bei dem sich ein Angreifer Zugriff auf ein geschäftliches oder ein akademisches E-Mail-Konto verschafft und die Identität des Kontoinhabers imitiert, um das Unternehmen und seine Mitarbeitenden oder seine Partner zu betrügen. Häufig erstellt ein Angreifer dafür ein Konto mit einer E-Mail-Adresse, die mit einer Unternehmens-E-Mail fast identisch ist und setzt dabei darauf, dass ein Opfer diesem E-Mail-Konto vertraut.

Mit der fortschreitenden digitalen Transformation in Bibliotheken werden die Cyberangriffe zahlreicher und vielseitiger. Hier einige weitere Beispiele für die bekanntesten Cyberangriffsmethoden:

a) Maleware

Malware (Schadprogramme) steht im Zusammenhang mit Software, die vom Benutzer unerwünschte und unter Umständen schädliche Aktionen hervorruft. Diese Aktionen tauchen während der PC-Benutzung unbemerkt auf, da die Schadprogramme oft im Hintergrund ablaufen.

Malware tritt in verschiedenen Varianten auf:

- Ein Computervirus ist ein Programmcode, der sich selbstständig oder automatisiert weiterverbreiten kann, indem er Dateien infiziert.
- Ein Computerwurm ist ein eigenständiges Computerprogramm oder Skript, das sich selbstständig oder automatisiert weiterverbreitet.
- Ein Trojanisches Pferd ist ein eigenständiges Programm, das als Haupt- oder Nebenfunktion schädlichen Code enthält, sich aber nicht selbstständig oder automatisiert weiterverbreiten kann.

b) Man-in-the-Middle-Angriff (MitM),

Als Man-in-the-Middle-Attack (MITM) oder Mittelsmannangriff wird eine Methode bezeichnet, bei der sich ein Hacker in den Datenverkehr zweier Kommunikationspartner einklinkt und beiden Parteien vorgaukelt, sie hätten es mit dem jeweils anderen Kommunikationspartner zu tun. Früher erfolgten solche Angriffe durch eine Manipulation des physischen Kommunikationskanals. In Zeiten gemeinsam genutzter öffentlicher Kommunikationsnetze tritt der unbefugte Dritte meist logisch zwischen zwei oder mehr Kommunikationspartner. Ziel des Angreifers ist es, die Kommunikation zwischen Opfer und Internetressource abzufangen, mitzulesen oder unbemerkt zu seinen Gunsten zu manipulieren.

c) Denial-of-Service-Angriff (DDoS)

Eine geläufige Form des DoS wird „Distributed Denial of Service“ (DDoS) genannt. Cyberkriminelle agieren bei dieser Variante nicht von einem einzelnen Angriffscomputer aus, sondern belasten die Zielsysteme durch Anfragen mehrerer Rechner, die zu gigantischen Bot-Netzen zusammengeschlossen sein können und die Server der Zielsysteme zum Absturz bringen. Durch einen solchen Rechnerverbund lässt sich deutlich mehr Datenverkehr generieren als bei einfachen DoS-Angriffen, die nur von einem einzigen System aus durchgeführt werden. Da beim DDoS-Angriff die Anfragen von einer Vielzahl von Quellen ausgehen, ist es nicht möglich, den Angreifer zu blockieren, ohne die Kommunikation mit dem Netzwerk komplett einzustellen.

d) SQL-Einschleusung

Die SQL-Einschleusung ist das Ausnutzen einer Sicherheitslücke in Zusammenhang mit SQL-Datenbanken, wie sie in Bibliothekssystemen enthalten sind. Die Sicherheitslücke entsteht durch einen Programmierfehler in einem Programm, das auf die Datenbank zugreift. Die Einschleusung von SQL-Befehlen ist ein Angriff, bei dem Schadcode in Zeichenfolgen eingefügt wird, die später zur Analyse und Ausführung an eine Instanz des SQL-Servers übergeben werden. So sollten sie jede Prozedur, die SQL-Anweisungen erstellt, auf Anfälligkeiten überprüfen, denn der SQL-Server führt alle empfangenen und gültigen Abfragen ohne weitere Prüfung aus.

e) Zero-Day-Schwachstelle

Zero-Day ist ein allgemeiner Begriff und steht für neu entdeckte Sicherheitslücken, über die Hacker Systeme angreifen können. Der englische Ausdruck „Zero-Day“ bezieht sich auf die Tatsache, dass ein Hersteller oder Entwickler gerade erst von diesem Fehler erfahren hat und damit „Null Tage“ Zeit hat, ihn zu beheben. Man spricht von einem Zero-Day-Angriff, wenn Hacker die Schwachstelle ausnutzen können, bevor die Entwickler sie feststellen und beheben können.

f) DNS-Tunneling

Das Domain Name System (DNS) ist eines der zentralen Protokolle des Internets. Die Aufgabe dieses Protokolls ist es, Domainnamen in IP-Adressen umzuwandeln. Es han-

Kirstin Grantz

Sachbücher des politisch rechten Spektrums in Öffentlichen Bibliotheken

Handlungsempfehlungen zum Umgang mit umstrittenen Werken

Die vorliegende Studie untersucht die aktuellen Herausforderungen im Umgang mit rechten Sachbüchern und arbeitet Handlungsempfehlungen für einen fachlich begründeten und transparenten Umgang mit rechten Sachbüchern in Öffentlichen Bibliotheken heraus. Neben der grundsätzlichen Frage, welcher Umgang empfehlenswert ist, wird die Kontextualisierung als Lösungsansatz, im Bestandsaufbau Neutralität zu wahren und gleichzeitig in Bereichen wie der Veranstaltungsarbeit eine eindeutige demokratische Positionierung einzunehmen, genauer beleuchtet.

2021, ISBN 978-3-9821824-4-5, Brosch.,
240 Seiten, € 29,50

Picture by Samuel Ferrara on Unsplash

PETER LANG
INTERNATIONAL ACADEMIC PUBLISHERS

SEIT MEHR ALS 50 JAHREN AUF HÖCHSTEM QUALITÄTSNIVEAU

Ihr Fachverlag der Geistes- und Sozialwissenschaften

Entdecken Sie
unsere E-Book-Pakete:

PICK & CHOOSE (PICK & MIX),
THEMEN-/ FACHGEBIETSSAMMLUNGEN,
DIREKTKAUF, ABONNEMENTS,
EVIDENCE BASED SELECTION/ EVIDENCE BASED ACQUISITION

Erhalten Sie einen Überblick über unsere angebotenen Titel und Fachgebiete auf

WWW.PETERLANG.COM

GERN ERSTELLEN WIR IHNEN EIN INDIVIDUELLES ANGEBOT. KONTAKTIEREN SIE UNS DAZU UNTER
sales@peterlang.com

Peter Lang Group • Place de la Gare 12, 1003 Lausanne, CH • sales@peterlang.com • Folgen Sie uns


Foto: © iStock-954538188

Hacker verschlüsseln Dateien und veröffentlichen Daten nach vergeblichen Erpressungsversuchen im Darknet.

delt sich also um einen Dienst, der eine bestimmte Domain einer IP-Adresse zuordnet und damit einem Server zuweist, beziehungsweise erst die Verbindung zum Server ermöglicht.

Im Normalfall ist die Anfrage an den DNS-Server in einem einheitlichen Format gehalten. Gleichzeitig sind die Anfragen und Antworten sehr kurz. Auf eine Domainanfrage antwortet der DNS-Server mit der dazugehörigen IP-Adresse. Weitere Inhalte sind bei den Anfragen nicht vorgesehen. Die eigentliche Kommunikation zwischen dem Client und dem Server, also beispielsweise zwischen einem Browser und dem Webserver, läuft dann über ein anderes Protokoll.

Bei einer DNS-Anfrage findet also eine Kommunikation zwischen zwei Rechnern statt. Hacker machen sich diese Eigenschaft zunutze: Jeder hat die Möglichkeit, einen eigenen Webserver im Internet zu betreiben. Die Konfiguration der DNS-Einträge obliegt dann dem Betreiber dieser Webseite, die unter einer Domain gehostet wird. Beim DNS-Tunneling dienen vor allem Subdomains für solche Angriffe.

g) Ransomware

Ransomware sind Schadprogramme, die den Computer sperren oder darauf befindliche Daten verschlüsseln. Die Täter erpressen ihre Opfer, indem sie deutlich machen, dass der Bildschirm oder die Daten nur nach einer Lösegeldzahlung wieder freigegeben werden.

In der Regel ist der blockierte Bildschirm oder der Erpresserbrief, der sich nicht mehr schließen lässt, das Erste, was der Nutzer von der Ransomware mitbekommt. Einige Ransomware-Varianten haben eine Ansteckungszeit. Das heißt, dass die schädliche Wirkung erst eintritt, wenn sich der User nicht mehr daran erinnern kann, wann und wo er sich eventuell einen Erpressungstrojaner eingefangen haben könnte. Der Faktor «Mensch» spielt eine wichtige Rolle bei Ransomware-Attacken. Durch Unachtsamkeit der User oder der Mitarbeitenden in der Bibliothek kann es immer und immer wieder zu erfolgreichen Ransomware Attacken kommen.

Die aufgezählten Angriffsvarianten müssen in ihren vielfältigen Varianten von der IT-Abteilung der Bibliotheken oder der Hochschulen überwacht und mit geeigneten Sicherheitsmaßnahmen bekämpft werden. Eine geeignete Sicherheitsmaßnahme ist die Zwei-Faktor-Authentifizierung (2FA) beim Zugang zu den Benutzer- und E-Mail-Konten. Eine weitere Maßnahme ist der Aufbau eines Sicherungskonzepts in konzentrischen Kreisen. Im innersten Kreis befinden sich die Nutzenden der Bibliothek und deren Zugangsdaten, in einem zweiten Kreis die Mitarbeitenden der Bibliothek. In einem weiteren Kreis dann die weiteren Personengruppen, die ein Zugangskonto zum Netzwerk der Bibliothek haben, wie beispielsweise Dienstleister. Es empfiehlt sich das Netzwerk durch Diagnostiksoftware und Filtersysteme überwachen zu lassen. Ist ein Bibliothekscloudsystem im Einsatz, dann muss der Datenverkehr von und zum Provider des Cloudsystems überwacht werden. Wichtig ist auch ein Sicherungskonzept mit bis zu drei Sicherungskopien des gesamten Bibliotheksystems: eine Kopie online, eine Kopie near line und eine Kopie offline, die alle regelmäßig aktualisiert werden.

Eine wichtige Aufgabe in der Sensibilisierung der Nutzenden und Bibliotheksmitarbeitenden kommt den Bibliotheken zu. Vielfach fehlt aber bereits ein Handlungskonzept, das beschreibt, was zu tun ist, bevor es zu einem Cyberangriff kommt. Das Krisenmanagement muss aber bereits vor einem Cyberangriff geplant und eingeübt werden. Gerade die Corona-Krise hat viele Bibliotheken dazu geführt, ihr digitales Angebot auszuweiten und breiter zugänglich zu machen. Eine Auswertung von Fachartikeln zu Cyberangriffen auf Hochschulen und deren Bibliotheken vor allem während der Corona-Pandemie zeigte auf, dass der überwiegende Anteil deutscher Hochschulen vor einem Cyberangriff kein adäquates Krisenmanagement für den Eventualfall bereithielt. Nachdem sie sich durch die Pandemie durchgehangelt haben, wägen sich zudem viele Hochschulbibliotheken in falscher Sicherheit, über genügend Flexibilität und Anpassungsfähigkeit zu verfügen, damit sie auch gegen einen Cyberangriff gewappnet sind.

Wie die Analyse und Nachbereitung von erfolgten Cyberangriffen an Hochschulen ergeben haben, findet ein Hackerangriff fast nie ausschließlich auf die IT-Infrastruktur der Bibliothek statt. Meist ist die gesamte IT-Infrastruktur der Universität oder Hochschule betroffen und der Angriff breitet sich intern sehr schnell aus.

Bibliotheken sollten sich gemeinsam mit den Leitungsstrukturen ihrer Hochschulen frühzeitig auf derartige Szenarien vorbereiten, indem sie organisatorische Vorkehrungen treffen und Maßnahmen von der Risikokommuni-

kation bis zur Schadensbewältigung vorbereiten und vor allem ihre Mitarbeitenden diesbezüglich intern ausbilden und sie verschiedenste Szenarien üben lassen. Neben wenigen spezialisierten Sachverständigenbüros, die sowohl Risikoanalysen und Sicherheitsaudits als auch Schulungen für Krisen- und Notfallmanager, Pandemiemanager, Stabsmitglieder und Coachings für Hochschulleitungen oder auch Stabsübungen anbieten, stehen ihnen hierbei meist die IT-Abteilung der entsprechenden Hochschule technisch zur Seite.

Vorbereitung, bevor ein Cybervorfall eintritt

Die Hochschulführung unter Einbeziehung der Bibliotheksleitung sollte sich frühzeitig überlegen, mit welcher Strategie man einem möglichen Cybervorfall begegnen möchte. Wichtig dabei sind die Bildung und das Vorhandensein eines einsatzbereiten Krisenstabs unter Einbeziehung der Verantwortlichen für Kommunikation und Recht. Die Zuständigkeiten und Verantwortungsbereiche müssen klar definiert sein und der Krisenstab muss mit den notwendigen Ressourcen und Kompetenzen ausgestattet sein. Die Kontaktdaten der Mitglieder wie auch der externen technischen Sachverständigen zur Schadensbewältigung müssen sofort greifbar sein.

Verhalten beim Eintreten des Schadensfalls

Kommt es zu einem Cyberangriff, muss sehr rasch gehandelt werden. Die Abläufe zur Abwehr möglicher Eskalationen müssen über gut eingespielte Prozesse und Konzepte bereits gut eingeübt sein, um die Kontrolle über den Vorfall zu behalten. Wird eine Hochschule akut angegriffen, ist es notwendig, sich auch mit externen technisch versierten Sachverständigen von Bund, Bundesland und Kanton telefonisch zu verständigen. Der/die entsprechende Mitarbeitende braucht zwingend die interne Freigabe vom Krisenstab, um diese Kontakte in die Wege zu leiten. Die Melde- und Analysestelle des Bundes oder des Bundeslandes hilft einzuschätzen, von welcher Schadsoftware die Hochschule befallen ist und ob neben der eigenen Bibliothek noch weitere Bibliotheken eines Verbundes betroffen sind. Eine wichtige Aufgabe ist die unverzügliche Information der Hochschulangehörigen sowie aller anderen Nutzenden der Bibliothek, damit im günstigen Fall ihre Rechner vor möglichen Schäden bewahrt werden können und sich die Schadsoftware nicht weiter ausbreiten kann.

Nachbereitung nach einem Schadensfall

Eine systematische Nachbereitung von Schadenfällen (oder auch von Fast-Schadensfällen, bei denen der Angriff gerade noch abgewehrt werden konnte) sind Pflicht. Dies dient der potenziellen Verbesserung der präventiven Abläufe, wie gut und zeitnah ein Vorfall erkannt werden konnte. Des Weiteren muss analysiert werden, wie schnell das Schadensausmaß und das Risiko des Schadens eingeschätzt werden konnte. Es gilt auch festzustellen, ob alle fälligen Sofortmaßnahmen zur Eindämmung des Schadenausmaßes gegriffen haben und die eigentlichen Ursachen und Schwachstellen erkannt und behoben werden konnten. Gelang es, Maßnahmen und Hilfsmittel zur Aufrechterhaltung eines angemessenen Notbetriebs während der Vorfallbewältigung zu aktivieren? War eine effektive Kommunikation nach innen und außen gewährleistet? Ein aktiver Erfahrungsaustausch bezüglich Vorfallbewältigung mit anderen Hochschulen in der gleichen Region und auch mit ähnlichen Institutionen im In- und Ausland sind ein wichtiges Instrument zur effektiven Nachbearbeitung. Die erworbenen Erkenntnisse sollen systematisch in die Qualitätsverbesserung der internen Prozesse einfließen. Damit wird die Prävention vor dem nächsten Vorfall wesentlich verbessert.

Fazit

Mit den heutigen, stark vernetzten und integrierten IT-Infrastrukturen sind die Hochschulen meist in ihrer Gesamtheit betroffen, wie entsprechende Vorfälle in Deutschland, Österreich und der Schweiz gezeigt haben. Der angerichtete Schaden umfasst Ausfallzeiten, die einige Tage oder mehrere Wochen dauern können, und beispielsweise gestohlene Forschungsdaten, die ins Darknet gestellt wurden. Die vorgängige Planung und wiederholte Beübung für die institutionelle Gefahrenabwehr und die Krisenmanagementstufenplanung sind sehr wichtig. Der diesbezügliche subsidiäre Struktur- und Maßnahmenaufbau für den Notfall gegen eine Cyberattacke ist eine unabdingbare Notwendigkeit. Gerade weil die Hochschulen ihre IT nicht so restriktiv reglementiert haben wie die Finanz- oder Versicherungsbranche, da für ihre Forschenden die offene Kommunikation untereinander unerlässlich ist, sind die Bibliotheken mit ihren Bibliothekscloudsystemen besonders vulnerabel. Cyberangriffe betreffen nicht nur die eigene Hochschulbibliothek, sondern oft auch gleich die gesamte Hochschule, ja unter gewissen Umständen auch einen ganzen Bibliotheksverbund. Daher sind Bibliotheksleitungen und alle Mitarbeitenden aufgerufen, sich für den Schutz ihres Arbeitsinstruments wirksam und nachhaltig einzusetzen.

Stephan Holländer
Lehrbeauftragter, Basel
stephan@stephan-hollaender.ch