API

OPEN ACCESS

Publiziert im Februar 2025
DOI: 10.15460/apimagazin.2025.6.1.215

Zeitschriftenartikel

Begutachtet

Begutachtet:

Kristin Ameis
HAW Hamburg
Deutschland

Erhalten: *25. Oktober 2024*
Akzeptiert: *05. November 2024*
Publiziert: *04. Februar 2025*

Empfohlene Zitierung:

JEORGAKOPULOS, Katharina, 2025: Report zur Cyberattacke an der HAW Hamburg. In: *API Magazin* **6**(1) [Online] Verfügbar unter: DOI 10.15460/apimagazin.2025.6.1.215

Report zur Cyberattacke an der HAW Hamburg

Dr. Katharina Jeorgakopulos[1]*

[1] Hochschule für Angewandte Wissenschaften Hamburg, Deutschland
Wissenschaftliche Mitarbeiterin und Lehrende am Department Information und Medienkommunikation

* Korrespondenz: redaktion-api@haw-hamburg.de

Zusammenfassung

Im digitalen Zeitalter sind Cyberangriffe zu einer signifikanten Bedrohung geworden, auch für Bildungseinrichtungen und Hochschulen. Anfang 2023 wird auch die HAW Hamburg Opfer eines Cyberangriffs. Auf Basis von Interviews mit Entscheider*innen der Hochschule dokumentiert der Report sowohl das Einbruchsszenario und die Hackermethode, den Ablauf der internen wie externen Kommunikation, sowie die Chronologie der Wiederherstellung der Systeme bis heute und beschreibt zusammenfassend die psychischen Auswirkungen auf Mitarbeitende, Studierende und Lehrende.

Schlagwörter: Cybersicherheit, Hacking, Hochschule, HAW Hamburg, IT-System

Report on the cyberattack at HAW Hamburg

Abstract

In the digital age, cyberattacks have become a significant threat, including for educational institutions and universities. At the beginning of 2023, Hamburg University of Applied Sciences (HAW Hamburg) was also the victim of a cyberattack. Based on interviews conducted with decision-makers at the university, the report documents the intrusion scenario and the hacking method, the progress of internal and external communication, the chronology of system recovery to date and summarizes the psychological impact on staff, students, and lecturers.

Keywords: Cyber Security, Hacking, University, HAW Hamburg, IT System

DOI: 10.15460/apimagazin.2025.6.1.215

Vorbemerkung

Der ursprüngliche Report zur Cyberattacke auf die IT-Infrastruktur der HAW Hamburg entstand im Rahmen eines Analyseprojektes im 2. Semester des Masterstudiengangs "Digitale Transformation der Informations- und Medienwirtschaft" (DiTra). Zehn Masterstudierende recherchierten und verschriftlichten die gewonnenen Erkenntnisse. Der Report erscheint hier in Kurzform, auf der Publikationsplattform SAIL kann der ausführliche Bericht nachgelesen werden (Abdulai et al. 2024). Alle Erkenntnisse beruhen auf subjektiven Einschätzungen der Interviewten, sodass keine Verantwortung für die Vollständigkeit oder Richtigkeit des Reports übernommen wird.

1 Einleitung

Im digitalen Zeitalter sind Cyberangriffe zu einer signifikanten Bedrohung geworden, insbesondere für Bildungseinrichtungen wie Universitäten und Hochschulen. Knapp zwei Dutzend der rund 300 Hochschulen in Deutschland waren in den Jahren 2022 und 2023 von Cyberangriffen betroffen (Fokken 2023). Diese Institutionen sind aufgrund ihrer umfangreichen Forschungsdaten und der Vielzahl an persönlichen Informationen ein attraktives Ziel für Hacker*innen. Anfang 2023 wird auch die HAW Hamburg Opfer eines Cyberangriffs.[1]

2 Angriffsmethoden und Schutzmaßnahmen

Phishing per E-Mail ist eine gängige Methode, die es Angreifenden ermöglicht, viele Anwender*innen automatisiert zu erreichen. Das Ziel der Hacker*innen ist die Übernahme der IT-Systeme und Server und die Verschlüsselung von Daten (Dreißigacker et al. 2020). Dabei variieren die Motivationen der Angreifenden. Ziel ist die Erpressung von Geld durch Drohungen, Informationen zu veröffentlichen oder Systeme zu verschlüsseln. Ein weiteres Ziel ist Spionage in Forschungseinrichtungen, um Wissensvorteile zu erlangen.

Künstliche Intelligenz (KI) kann beim Hacking unterstützen, indem sie Hinweise auf mögliche Sicherheitslücken gibt, Konfigurationsaufgaben übernimmt und zum Beispiel Phishing-Mails generiert (Müller-Quade et al. 2019). Die eigentliche Ausnutzung von Schwachstellen erfordert bislang noch menschliche Intelligenz. Bisher übernehmen Generative KIs noch die Nebenarbeit; die „Kunst des Hackens“ liegt aber weiterhin beim Menschen (SoSafe 2024). Da es sich um ein sehr dynamisches Feld handelt, kann sich das in Zukunft ändern.

1 Die folgenden Informationen basieren auf den Antworten eines IT-Experten der HAW Hamburg, Prof. Dr. Volker Skwarek, Professor für Technische Informatik an der HAW Hamburg, um die Methoden und Motivationen der Angreifenden zu beleuchten, Sicherheitsmaßnahmen zu analysieren und Empfehlungen zur Verbesserung der Cybersicherheit zu geben.

DOI: 10.15460/apimagazin.2025.6.1.215

Die spezifische Methode des Angriffs auf die HAW Hamburg ist unbekannt, die Befragten vermuten „Phishing“. Angreifende übernehmen zunächst normale Nutzerrechte und bewegen sich innerhalb des Systems, um Schwachstellen zu analysieren. Diese spezialisierten, oft monatelangen Angriffe werden als „Multistager“ bezeichnet. Ein absoluter Schutz vor Cyberangriffen ist bei den großen und teilweise unübersichtlichen Strukturen der IT- Systeme von Bildungseinrichtungen in der Regel unmöglich und ineffizient. Für eine Absicherung gegen Cyberattacken ist die Priorisierung der wichtigsten IT-Systeme wesentlich (Bub 2023). Die Sensibilisierung von Mitarbeitenden und Studierenden durch Fortbildungen kann positive Effekte haben, bietet jedoch keine absolute Sicherheit. Grundlegende Maßnahmen wie automatische Updates von Virenscannern, regelmäßige Backups und die Nutzung sicherer Cloud-Laufwerke können die Risiken minimieren (BSI 2020). Letztendlich ist eine Kombination aus technischer Sicherheit und bewusstem Nutzerverhalten der beste Schutz; so will auch die HAW Hamburg weiter verfahren.

3 Chronologie des Angriffs

Die Hackergruppe Vice Society ist eine finanziell motivierte Ransomware-Hacker*innengruppe, die seit Januar 2021 aktiv mit bestehender Schadsoftware wie HelloKitty und Zeppelin (Adamek und Laufer 2023) arbeitet (Microsoft Threat Intelligence 2022). Ihre Zielgruppe ist hauptsächlich der Bildungssektor. Die Gruppe ist dafür bekannt, Backups anzugreifen, Daten herauszuschleusen und zu verschlüsseln, um Lösegeld zu erpressen (Gumarin 2022). Auch im Fall der HAW Hamburg war es das Ziel, einen zentralen Schaden im IT-Bereich und in der zentralen Verwaltung anzurichten, um dann die Lösegeldforderungen geltend zu machen.[2]

Die Hacker*innen erlangen vor Weihnachten 2022 über dezentrale IT-Systeme Zugriff auf die HAW Hamburg und auf die Administrationsrechte. Mithilfe von Schlüsselbegriffen werden die Systeme nach Daten durchsucht. Mit den Administrationsprivilegien haben die Hacker*innen Zugriff auf das Hauptrechenzentrum und das Backup-Rechenzentrum. Daten werden durch die Hacker exfiltriert und sequentiell verschlüsselt.[3] Die Exfiltration endet am 26.12.2022, Programme zum Löschen von Daten laufen. Der Zugriff erfolgt bewusst über Weihnachten, so dass die Möglichkeit frühzeitig bemerkt zu werden, relativ gering ist. Nachdem zunächst ein technischer Defekt vermutet wurde, wird am 29.12.2022 eine Datei mit verschlüsselten Daten gefunden. Diese enthält ein Dokument mit der Aufforderung zur Zahlung von Löse-

2 Die Informationen zur HAW Hamburg stammen aus einem Interview mit dem IT-Sicherheitsbeauftragten der HAW Hamburg, Prof. Dr. Klaus-Peter Kossakowski. Mehr Informationen über sein laufendes Projekt „Evaluation der Informationssicherheit der HAW Hamburg“ unter https://www.haw-hamburg.de/digitalisierung/digitale-infrastruktur-services/it-projekte/evaluation-der-informationssicherheit-1/.

3 „Exfiltrieren“ bedeutet: Daten werden ohne Wissen des Besitzers aus seinem System oder Netzwerk herauskopiert und an einen externen Ort (z. B. einen Server des Angreifers) übertragen. „Sequentielle Verschlüsselung“ bedeutet: die Daten (z. B. Dokumente, Datenbanken) werden in einer bestimmten Reihenfolge verschlüsselt, sodass sie für den rechtmäßigen Besitzer unzugänglich werden.

DOI: 10.15460/apimagazin.2025.6.1.215

geld. In Deutschland sind Angriffe auf öffentlich-rechtliche Einrichtungen dabei erfolglos, da Lösegeldzahlungen rechtlich unzulässig sind. Auch die HAW Hamburg zahlt kein Lösegeld (Kuss und Neugebauer 2024).

Die Schadensfeststellung läuft an und die gesamte Informations- und Kommunikationsinfrastruktur wird vorsorglich stillgelegt (HAW Hamburg 2022). Die ersten Schritte einer umfassenden IT-Krisenbewältigung werden eingeleitet und die Polizei setzt eine Sonderkommission ein. Am 16. Januar 2023 wird erstmals der Schadensfall vollständig bilanziert. Parallel beginnt der Aufbau einer neuen IT-Struktur. Im Zuge dieser Maßnahmen wird das „Zero Trust"-Konzept"[4] eingeführt (Lobmeyer 2023). Am 05.03.2023 veröffentlichen die Hacker*innen erstmals Daten im Darknet. Die veröffentlichten Daten werden überprüft und Betroffene durch die HAW Hamburg informiert.

4 Externe Kommunikation

Bereits am 30. Dezember 2022, also einen Tag nachdem intern an der HAW Hamburg der Cyberangriff bestätigt werden konnte, erfolgt die Medienberichtserstattung. So berichtet das Hamburger Abendblatt in einer kurzen Meldung von der HAW Hamburg als Opfer eines Hackerangriffs und verweist auf die Homepage der Hochschule (Hamburger Abendblatt 2022). Am 12. Januar 2023 erscheint ein Artikel des SPIEGEL. Der Pressesprecher der HAW Hamburg schildert im SPIEGEL-Interview die aktuelle Lage, das Vorgehen der Hochschule und die Bemühungen, möglichst schnell Lösungen zu finden. Der SPIEGEL befragt dazu Studierende, die Ärger, Verunsicherung, eine schlechte Kommunikation und fehlende Kulanz hinsichtlich der anstehenden Prüfungen seitens der Hochschule äußern (Fokken 2023).

Am 13. Januar 2023 erscheint bei der Tagesschau ein Artikel zum Cyberangriff auf die HAW Hamburg (Adamek und Laufer 2023). Durch eine umfassende Recherche berichtet das ARD-Politikmagazin „Kontraste" detailliert über den konkreten Angriff auf die IT-Systeme der Hochschule, die Hackergruppe und deren Hintergrund sowie über die Folgen und andere betroffene Institutionen. „Kontraste" berichtet, wie die Hackergruppe mit der Hochschule kommuniziert und welche Cyberangriffe Vice Society in Deutschland noch verübte. Mutmaßungen über einen Einstieg in die internen IT-Systeme der HAW Hamburg über Phishing-E-Mails und ein Zusammenhang mit einem vorangegangenen Vorfall in der IT-Abteilung werden ebenfalls beschrieben. Die Angaben des Sprechers zu dem zeitlichen Ablauf des Einstiegs, der ersten internen Reaktion der HAW Hamburg wie auch, dass Daten abgeflossen seien und sich darunter sensible Daten von Studierenden und Beschäftigten befänden, flossen

4 Das „Zero Trust"-Konzept ist ein Sicherheitsmodell, das auf dem Prinzip basiert, keinem Benutzer, Gerät oder System standardmäßig zu vertrauen, unabhängig davon, ob es sich innerhalb oder außerhalb des Unternehmensnetzwerks befindet. Stattdessen erfordert es eine kontinuierliche Verifizierung und die Minimierung von Zugriffsrechten. Quelle u. a.: https://www.pexip.com/whitepaper/optimizing-your-zero-trust-security.

DOI: 10.15460/apimagazin.2025.6.1.215

ebenfalls in die Berichtserstattung ein.

Das Hamburger Abendblatt berichtet am 18. Mai 2023 wiederholt über den Cyberangriff (Jessen 2023), es hatte unter anderem Betroffene interviewt. Der Sprecher wird zitiert, dass aus ermittlungstaktischen Gründen keine weiteren Informationen herausgegeben würden und dass die HAW Hamburg im engen Austausch mit dem Beauftragten für Datenschutz und Informationsfreiheit der Stadt Hamburg stehe.

5 Interne Kommunikation und Reaktionen

Über die Website der HAW Hamburg wird am 28. Dezember 2022 erstmals kommuniziert, dass es einen Cyberangriff gegeben hat. Die Website fungiert in dieser Zeit als primärer Kommunikationskanal, sowohl intern als auch extern. Eine FAQ-Seite zum Cyberangriff informiert Studierende, Beschäftigte und die Öffentlichkeit, dabei liegt der Fokus auf den Studierenden. Sie werden fortlaufend über die Social-Media-Kanäle der HAW Hamburg, insbesondere Instagram, informiert. Ein unabhängiger Analyst für IT-Sicherheit bescheinigt der HAW Hamburg, dass sie eine gelungene unmittelbare Kommunikation durch die betroffene Organisation durchführte (Kondruss 2022).

5.1 Interne Kommunikation

Die interne Kommunikation erlangt während der Zeit des Cyberangriffs eine zentrale Rolle. Es funktionierten anfangs weder Telefone noch Rechner und es gab nur wenige private Kontaktdaten von Mitarbeitenden. So wird ein erstes Notfallkommunikationsnetz über handschriftliche Nachrichten sowie private Kommunikationskanäle wie Signal-Gruppen und private E-Mail-Adressen aufgebaut. Verantwortliche Personen werden zu einem Krisenstab vereint, um Informationen zu sammeln und zu verteilen.

Zügig wird eine FAQ-Seite auf der Website der HAW Hamburg eingerichtet, um grundlegende Informationen bereitzustellen. Parallel dazu wird die Kommunikation mit den Studierenden über Instagram aufgebaut. Im Januar 2023 wird eine Veranstaltung als Informationsplattform genutzt, um Beschäftigten ihre Fragen zu beantworten. Die kontinuierliche Kommunikation mit den Mitarbeitenden erfolgt über Microsoft Teams (MS Teams), nachdem der dortige Kanal wiederhergestellt war.

Zu den wichtigsten Informationen gehörten ein laufendes Update zum Stand des Cyberangriffs, Informationen zur Nutzung der Dienst-Laptops, die Wiedereinrichtung von Funktionspostfächern sowie das Vorgehen im Verdachtsfall von Datendiebstahl. Diese Informationen werden laufend zentral auf der FAQ-Seite der Website bereitgestellt, die die Abteilung Presse und Kommunikation (PK) unterhält. PK ist ebenfalls zuständig für den Instagram-Kanal der Hochschule. Studierende nutzen dazu die FAQ-Seite und die Video-Botschaften auf der Website, sowie den Insta-

DOI: 10.15460/apimagazin.2025.6.1.215

gram-Kanal als interaktives Austauschformat.[5]

5.2 Reaktionen der Studierenden

Die Studierenden und Lehrenden waren von der Cyberattacke besonders betroffen. Die Studierenden reagieren auf dem zentralen Instagram-Account der HAW Hamburg mit vielfältigen Emotionen. Viele äußern Frust über mangelnde Kommunikation und Transparenz. Es herrscht Verwirrung über widersprüchliche Informationen zu Prüfungsverschiebungen (HAW-Studierende 2022). Herausforderungen wie der fehlende Zugang zu Plattformen wie MS Teams, MyHAW und Moodle werden thematisiert.

Besondere Herausforderungen für die Studierenden ergeben sich aus der schlechten Vorbereitung auf Prüfungen in den Weihnachtsferien, denn der Cyberangriff geschah kurz vor der Prüfungsphase. Unterschiedliche Regelungen bezüglich Freiversuchen und einer zweiten Prüfungsphase je nach Department stiften Verwirrungen. Die Vizepräsidentin für Studium und Lehre führt mit den Fachschaftsräten Gespräche, zeigt Verständnis und versucht Lösungen zu finden.

5.3 Perspektive der Lehrenden

Die Reaktion der Lehrenden fällt gemischt aus, während einige wenig Verständnis für die Ausnahmesituation zeigen, reagieren andere verständnisvoll. Die erste Wahrnehmung der IT-Probleme führt zu einer erheblichen Verunsicherung bei den Lehrenden, insbesondere da die Cyberattacke unmittelbar vor den Prüfungen erfolgte. Fragen wie „Wie kann ich meine Studierenden erreichen?“ und „Wie organisiere ich die Prüfung?“ stehen im Vordergrund.

Die zentrale Unterstützung der HAW Hamburg wurde als zu langsam befunden, während auf Fakultäts- und Departmentsebene schnell konkrete Hilfen angeboten wurden (HAW Hamburg 2023c). Viele Lehrende zeigten dabei große Eigeninitiative bei der Wiederherstellung der Kommunikationsstrukturen. Sie entwickelten Alternativen zur schnellen Bereitstellung von Lehrmaterialien und nutzten private Kontakte wie Telefonnummern und E-Mails, um den Informationsfluss aufrechtzuerhalten. Zur Koordination richteten sie Taskforces und Krisenstäbe auf Departmentsebene ein. Um die Prüfungen sicherzustellen, griffen sie auf diverse, datenschutzkonforme Messengerdienst wie Signal zurück und organisierten analoge Treffen (Rühmkorf 2024).

5 Siehe dazu die Instagram-Kanäle der HAW Hamburg und des Departments Medizintechnik an der HAW Hamburg: https://www.instagram.com/hawhamburg/ und https://www.instagram.com/medizintechnik_hawhamburg/.

DOI: 10.15460/apimagazin.2025.6.1.215

6 Maßnahmen zur Wiederinbetriebnahme der IT-Infrastruktur und -dienste

Abb. 1: Maßnahmen der Wiederinbetriebnahme der IT-Infrastruktur/IT-Dienste (Quelle: Abdulai et al. 2024, S. 20)

Nach dem Cyberangriff stehen der HAW Hamburg zwei externe IT-Dienstleister beratend zur Seite, die ihre Expertise in unterschiedliche Aufgabenbereiche einbringen. Ein externer Dienstleister unterstützt bei der technischen Umsetzung des Notbetriebes, dem Errichten von Datenspeicherungssystemen und der Kommunikation mit dem Software-Dienstleister Microsoft. Zwei Wochen nach dem Vorfall übernimmt eine weitere externe Firma die Begleitung des Krisenmanagements. Zu ihren Aufgaben gehören die Errichtung und Betreuung eines IT-Krisenstabes, die Planung des IT-Notbetriebes zur Sicherstellung des Lehrbetriebes und der Aufbau einer neuen IT-Infrastruktur (Lobmeyer 2023).

6.1 Sicherstellung eines Notbetriebes der IT-Basisdienste

Zuerst wurden wesentliche Programme zur Aufrechterhaltung von Verwaltung und Lehre in Betrieb genommen. Zu diesem Zweck wurde ein vorläufiges MS Teams etabliert. Des Weiteren wurde eine neue WLAN-Verbindung ohne Identitätssystem eingerichtet. Zur Aufrechterhaltung der Lehre wurde in Zusammenarbeit mit dem hochschulinternen Projekt KOMWEID und dem Informationstechnik Service Center (ITSC) eine vorläufige Kursplattform (Übergangsmoodle) eingerichtet. Hierzu wurde das auf den Servern der Universität Hamburg befindliche Moodle-System für die Hochschulmitglieder der HAW Hamburg bereitgestellt (HAW Hamburg 2023a).[6] Für die laufende Bewerbungsphase wurde ein eingeschränktes Bewerbungs- und Studierendenportal (myHAW) errichtet. Hierfür stellte die Technische Universität Hamburg der HAW Hamburg Serverkapazitäten zur Verfügung.

6 Inzwischen ist die Rückführung des Moodle-Systems zum Wintersemester 2024/25 erfolgt. Tägliche, kurzfristige Sicherheitsupdates soll Moodle u. a. gegen Hackerangriffe sichern. Deren Veröffentlichung erfolgt unregelmäßig und ohne Vorankündigung (Stand 10/2024).

 DOI: 10.15460/apimagazin.2025.6.1.215

6.2 Aufbau der IT-Basisinfrastruktur

Bevor neue Laufwerke erstellt und zentrale IT-Dienste in Betrieb genommen werden konnten, musste eine neue IT-Infrastruktur errichtet werden. Dazu wurde ein verbessertes Netzwerkkonzept erarbeitet und sukzessive umgesetzt. Vom ITSC wurden virtuelle Server-Strukturen bereitgestellt, um Ressourcen für eine Vielzahl von Servern (Telefon, E-Mail, Verwaltung etc.) zur Verfügung zu haben. Zusätzlich wurde ein neues Identitätsverwaltungssystem eingeführt. Die Authentifizierung mittels HAW-Kennung ermöglichte die Zuweisung von Berechtigungen für IT-Ressourcen auf Basis eines Rechte- und Rollenkonzepts (HAW Hamburg 2024).

Die Nutzerlaufwerke wurden nach dem Cyberangriff forensisch untersucht (HAW Hamburg 2023d), auf neue Server migriert und zur Prüfung der Berechtigung weitergegeben. Die verschlüsselten Datenbereiche anbietender Server konnten aus den Backups wiederhergestellt werden. Im Rahmen der Wiederinbetriebnahme wurden zentrale IT-Dienste integriert. Für zahlreiche Anwendungen und Einrichtungen, darunter Office365, HIBS und myHAW, war die Implementierung einer 2-Faktor-Authentifizierung als zusätzliche Sicherheitsmaßnahme von entscheidender Bedeutung. Dafür versendete die HAW Hamburg mehr als 17.000 Schreiben per Post. Zudem wurde jeder HAW-Account mit einer randomisierten W-Kennung[7] gekoppelt, um bei Wiederherstellungsmaßnahmen die alten Identifier-Accounts von den neuen zu unterscheiden. Ein sicherer Zugang zum WLAN wurde mittels eines Single-Sign-On-Verfahrens über den Anbieter Easyroam ermöglicht (HAW Hamburg 2023b).[8]

7 Psychologische Auswirkungen durch die Cyberattacke

Studien zu Cyberattacken auf Unternehmen zeigen, dass diese nicht nur technische und finanzielle Folgen haben, sondern auch psychologische Auswirkungen auf die betroffenen Mitarbeitenden. Diese umfassen unter anderem Stress und Angst, ob persönliche und berufliche Daten kompromittiert wurden, das Gefühl der Unsicherheit und Verwundbarkeit des Unternehmens sowie Vertrauensverlust in die Führung. Hinzu kommen Schuldzuweisungen und Stigmatisierung von Mitarbeitenden, die für die IT-Sicherheit verantwortlich sind, wie auch Burnout und Erschöpfung durch oftmals intensiven Arbeitseinsatz (NortonLifeLock 2021; SoSafe 2024; IBM 2023).

7 Die randomisierte W-Kennung bezieht sich auf eine zufällig generierte Identifikationsnummer (Kennung), die für bestimmte Zwecke verwendet wird, um die Privatsphäre zu schützen oder spezifische Operationen zu ermöglichen. Randomisiert bedeutet in diesem Zusammenhang: Die Kennung wird zufällig erzeugt, typischerweise durch einen Algorithmus wie einen Zufallszahlengenerator. Randomisierte Kennungen sind zeitlich begrenzt, d. h., sie ändern sich regelmäßig, um Tracking oder Missbrauch zu verhindern. Weitere Informationen: https://www.haw-hamburg.de/haw-account/.

8 Am 11.11.2024 wurde an der HAW Hamburg für den HAW-Account eine neue Passwortrichtlinie umgesetzt. Künftig können nur Passwörter mit mindestens 10 Zeichen vergeben werden. Mit dieser Änderung entfällt die Notwendigkeit, regelmäßig ein neues Passwort für den HAW-Account vergeben zu müssen. Das automatische Ablaufen der Passwörter wurde damit abgeschaltet. Im Projekt „HAW2030“ widmet sich die Hochschule in einem eigenen Entwicklungsfeld der weiteren Optimierung der IT-Organisation. Hier geht es insbesondere um die Schnittstellen- und Dienstleistungsdefinition sowie um die Organisationsstruktur der Rechenzentren insgesamt.

DOI: 10.15460/apimagazin.2025.6.1.215

Nach Einschätzung des Personalrats der HAW Hamburg gab es durch den Cyberangriff zwar keinen Einbruch in der Motivation der Mitarbeitenden. Dennoch traten nachgelagert zahlreiche Gefährdungsanzeigen von Beschäftigten aller Bereiche auf, die sich auf schlechte Arbeitsbedingungen, Fehlerquellen und Überlastungen durch den Cyberangriff bezogen.

An der Fakultät Design, Medien Information (DMI) sorgte die fehlende digitale Kommunikation und der Verlust der Daten für große Verunsicherung, vor allem in der Verwaltung (Fakultätsservicebüro) und den Bereichen Personal, Finanzen und Schließsysteme. An der Fakultät Wirtschaft und Soziales (W&S) gab es laut Dekan einen erhöhten Bedarf an Mitarbeitergesprächen in Bezug auf die Organisation des Lehrbetriebes ohne IT-Systeme mit erhöhtem Arbeits- und Abstimmungsaufwand. Die Fakultät Life Science (LS) konnte recht schnell ein alternatives Kommunikationssystem aufsetzen unter aktiver Einbindung der Studierenden. So konnten nach Ansicht der Dekanin psychische Folgen abgewendet werden. Der Dekan der Fakultät Technik und Informatik (TI) berichtet, dass nach einer ersten Phase der Orientierungslosigkeit, die Ärmel hochgekrempelt und angepackt wurde. Auch wenn sich die Lage inzwischen stabilisiert habe, gebe es bis heute Nachwirkungen.

Zur Frage von Schulungsangeboten für Mitarbeitende und Lehrende hinsichtlich Gesundheitsförderung und Cybersicherheit (Bagley 2024) gingen die einzelnen Fakultäten ebenfalls unterschiedliche Wege. Der Kanzler der Hochschule verweist auf die Datenschutzschulungen durch das hochschulinterne Projekt KOMWEID[9] und die hochschulübergreifende Einrichtung des Multimedia Kontor Hamburg[10] und berichtet, dass Awareness-Schulungen vorbereitet würden. Als Learning aus der Cyberattacke schlägt der Sprecher der Hochschule vor, besser aufeinander zu achten, und dass Kolleg*innen in so einem Krisenfall füreinander einspringen sollten: denn so eine Krise würde viel Energie kosten.

9 Projekt KOMWEID: https://www.haw-hamburg.de/qualitaet-in-der-lehre/komweid/.
10 MMKH Multimedia Kontor Hamburg: https://www.mmkh.de/index.html.

DOI: 10.15460/apimagazin.2025.6.1.215

Literatur

ABDULAI, Vanessa et al., 2024: *Cyberattacken und KI – am Fallbeispiel der HAW Hamburg.* [online] *Report*. 10.10.2024 [Zugriff am 19.06.2024]. Verfügbar unter: https://hdl.handle.net/20.500.12738/16572

ADAMEK, Sascha und LAUFER, Daniel, 2023. *Hamburger Hochschule wird erpresst.* Hamburg: Norddeutscher Rundfunk. [online] 13.01.2023 16:56 Uhr. [Zugriff am 19.06.2024]. Verfügbar unter: https://www.tagesschau.de/investigativ/rbb/hacker-nangriff-haw-vice-101.html

BAGLEY, Drew, 2024. *Achieving Ecosystem-level Cybersecurity* [online]. *A U.S. Policy Perspective.* Austin, TX: CrowdStrike Holdings, Inc. [online] 11.06.2024 [Zugriff am 19.06.2024]. Verfügbar unter: https://www.crowdstrike.com/en-us/blog/next-steps-for-ecosystem-level-cybersecurity/

BSI BUNDESAMT FÜR SICHERHEIT DER INFORMATIONSTECHNIK, 2020. *Informationssicherheit mit System: Der IT-Grundschutz des BSI.* Bonn: BSI. BSI-Bro20/333. [online] 11.2020. [Zugriff am 07.06.2024]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/sonstiges/Informationssicherheit_mit_System.pdf?__blob=publicationFile&v=3

BUB, Nina, 2023. Wie Universitäten mit Hackerangriffen umgehen. In: *Frankfurter Allgemeine Zeitung*, Frankfurt. [online] 28.09.2023. [Zugriff am 07.06.2024]. Verfügbar unter: https://www.faz.net/aktuell/rhein-main/wie-universitaeten-mit-hacker-angriffen-umgehen-19199400.html

DREIßIGACKER, Arne, VON SKARCZINSKI, Bennet und Gina Rosa WOLLINGER, 2020. *Cyberangriffe gegen Unternehmen in Deutschland: Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019.* Hannover: Kriminologisches Forschungsinstitut Niedersachsen e.V. Forschungsbericht Nr. 152. ISBN: 978-3-948647-00-1. Verfügbar unter: https://kfn.de/wp-content/uploads/Forschungsberichte/FB_152.pdf

FOKKEN, Silke, 2023. Wenn ein Cyberangriff eine Hochschule ausknockt. In: *DER SPIEGEL* [online]. 12.01.2023. [Zugriff am 25.06.2024]. Verfügbar unter: https://www.spiegel.de/panorama/bildung/digitalisierung-wenn-ein-cyberangriff-eine-hochschule-ausknockt-a-0a81da2b-3e7f-465c-8066-7e53b8b40c08

GUMARIN, J. R., 2022. *Vice Society: Profiling a Persistent Threat to the Education Sector.* Santa Clara, CA: Unit42, Palo Alto Networks. [online] 06.12.2022. [Zugriff am 07.06.2024]. Verfügbar unter: https://unit42.paloaltonetworks.com/vice-society-targets-education-sector/

 DOI: 10.15460/apimagazin.2025.6.1.215

HAMBURGER ABENDBLATT, 2022. *HAW Hamburg Opfer eines Hackerangriffs.* Hamburg: FUNKE Medien Hamburg GmbH, dpa:221230-99-56891/3. [online] 30.12.2022 [Zugriff am 07.06.2024]. Verfügbar unter: https://www.abendblatt.de/hamburg/article237258901/HAW-Hamburg-Opfer-eines-Hackerangriffs.html

HAW Hamburg, 2024. *Online-Services* [online]. *Ihr HAW-Account / M365 und Ihre E-Mail-Adresse.* Hamburg: HAW Hamburg. [Zugriff am 19.06.2024]. Verfügbar unter: https://www.haw-hamburg.de/haw-account

HAW Hamburg, 2023a. *Angriff auf die IT-Infrastruktur* [online]. *Aktuelle Meldungen und Hinweise.* Hamburg: HAW Hamburg, 07.03.2023 [Zugriff am 09.06.2024] Archiviert als: https://web.archive.org/web/20230307233418/https://www.haw-hamburg.de/cyberangriff/

HAW Hamburg, 2023b. *Angriff auf die IT-Infrastruktur* [online]. *Aktuelle Meldungen und Hinweise.* Hamburg: HAW Hamburg, 20.01.2023 [Zugriff am 14.06.2024]. Archiviert als: https://web.archive.org/web/20230120165636/https://www.haw-hamburg.de/cyberangriff/

HAW HAMBURG, 2023c. *Cyberangriff auf die IT-Infrastruktur* [online]. *Statements aus der Hochschule.* Hamburg: HAW Hamburg, 10.06.2024 [Zugriff am 07.06.2024]. Verfügbar unter: https://www.haw-hamburg.de/cyberangriff/statements-aus-der-hochschule

HAW HAMBURG, 2023d. Prof. Dr. Olga Burkova zum Cyberangriff auf die HAW Hamburg. In: *YouTube* [online]. 20.02.2023 [Zugriff am 07.06.2024]. Verfügbar unter: https://www.youtube.com/watch?v=AMOXybKjwgQ;

HAW HAMBURG [@hawhamburg], 2022. Update vom 30.12.2022: Wie das ITSC bereits auf dem Telegram-Kanal bekannt gegeben hat, steht der Grund für die Ausfälle der IT-Dienste und Services der zentralen Infrastruktur jetzt fest: Die technische Informations- und Kommunikationsinfrastruktur der HAW Hamburg ist angegriffen worden. In: *Instagram* [online], Post vom 28.12.2022, letztes Update 03.01.2023. [Zugriff am 07.06.2024] Verfügbar unter: https://www.instagram.com/p/CmtzmiVq6rB/

HAW-STUDIERENDE, 2022. *Server-Ausfall an der HAW: Verschiebung der Klausurenphase & Fristen oder Zweittermine* [online]. San Francisco, CA: Change.org. 30.12.2022 [Zugriff am 07.06.2024]. Verfügbar unter: https://www.change.org/p/server-ausfall-an-der-haw-verschiebung-der-klausurenphase-fristen-oder-zweittermine.

DOI: 10.15460/apimagazin.2025.6.1.215

IBM, 2023. *IBM Report* [online]. *Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs.* Armonk, NY: IBM, 24.07.2023 [Zugriff am 07.06.2024]. Verfügbar unter: https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs

JESSEN, Elisabeth, 2023. Nach Cyberangriff: Daten von HAW-Studierenden im Darknet. In: *Hamburger Abendblatt* (online). Hamburg: Funke Medien Hamburg GmbH. 18.05.2023 13:00 Uhr [Zugriff am 19.05.2024]. Verfügbar unter: https://www.abendblatt.de/hamburg/hamburg-nord/article238435203/Nach-Cyberangriff-Daten-von-HAW-Studierenden-im-Darknet.html

KONDRUSS, Bert, 2022. *Cyberangriffe auf Universitäten: Ransomware, DDoS, Datendiebstahl* [online]. Möglingen: KonBriefing Research UG. O.D. [Zugriff am 24.06.2024]. Verfügbar unter: https://konbriefing.com/de-topics/cyber-angriffe-universitaeten.html

KUSS, Christian und NEUGEBAUER, Franziska, 2021. *Die rechtliche Zulässigkeit von Lösegeldzahlungen.* München: CIO, IDG Tech Media GmbH. [online] 04.03.2021. [Zugriff am 07.06.2024] Verfügbar unter: https://www.cio.de/a/die-rechtliche-zulaessigkeit-von-loesegeldzahlungen,3728833

LOBMEYER, Lisa, 2023. *HAW Hamburg: Incident Response und IT-Krisenmanagement nach einem Ransomeware-Angriff*. Berlin: HiSolutions AG. [online] 03.07.2023 [Zugriff am 07.06.2024]. Verfügbar unter: https://www.hisolutions.com/detail/haw-ir-ransomware

MICROSOFT THREAT INTELLIGENCE, 2022. *DEV-0832 (Vice Society) opportunistic ransomware campaigns impacting US education sector.* [online] Redmond, WA: Microsoft Corporation. 25.10.2022. [Zugriff am 07.06.2024]. Verfügbar unter: https://www.microsoft.com/en-us/security/blog/2022/10/25/dev-0832-vice-society-opportunistic-ransomware-campaigns-impacting-us-education-sector/?msocki-d=15aeaea0972d6e090c41bd1296f06ff1

MÜLLER-QUADE, J. et al., 2019. *Künstliche Intelligenz und IT-Sicherheit: Bestandsaufnahme und Lösungsansätze.* [online] 04.04.2019. [Zugriff am 07.06.2024]. Verfügbar unter: https://www.acatech.de/publikation/kuenstliche-intelligenz-und-it-sicherheit-bestandsaufnahme-und-loesungsansaetze/download-pdf?lang=de

NORTONLIFELOCK, 2021. *Norton Cyber Safety Insights Report 2021* [online] *Germany, US.* Tempe, AZ: NortonLifeLock Inc. o.D. [Zugriff am 07.06.2024]. Verfügbar unter: https://www.nortonlifelock.com/de/de/newsroom/press-kits/2021-norton-cyber-safety-insights-report/

DOI: 10.15460/apimagazin.2025.6.1.215

RÜHMKORF, Sarah, 2024. Studieren mit und während der Cyberattacke: Erfahrungen zur Cyberattacke an der HAW Hamburg. In: *API Magazin*, 5(1). [Online] Verfügbar unter: https://doi.org/10.15460/apimagazin.2024.5.1.190

SOSAFE, 2024. *Cybercrime Trends 2024: Die größten Angriffstrends und Best Practices für mehr Sicherheit.* [Online, Zugriff am 07.06.2024]. Verfügbar unter: https://sosafe-awareness.com/de/ressourcen/reports/cybercrime-trends/