

**Zeitschriftenartikel***Begutachtet***Begutachtet:**

Dr. Katharina Jeorgakopulos   
HAW Hamburg  
Deutschland

**Erhalten:** 24. Dezember 2023**Akzeptiert:** 16. Januar 2024**Publiziert:** 30. Januar 2024**Copyright:**

© Sarah Rühmkorf.  
Dieses Werk steht unter der Lizenz  
Creative Commons Namens-  
nennung 4.0 International (CC BY 4.0).

**Empfohlene Zitierung:**

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

## Studieren mit und während der Cyberattacke Erfahrungen zur Cyberattacke an der HAW Hamburg

**Sarah Rühmkorf**<sup>1\*</sup> <sup>1</sup> Hochschule für Angewandte Wissenschaften Hamburg, Deutschland

Studentin im 5. Semester des Bachelorstudiengangs Bibliotheks- und Informationsmanagement

\* Korrespondenz: [redaktion-api@haw-hamburg.de](mailto:redaktion-api@haw-hamburg.de)

### Zusammenfassung

Der Beitrag befasst sich mit der Cyberattacke, die die HAW Hamburg im Dezember 2022 getroffen hat. Nach einer kurzen Einführung über Cyberangriffe im Allgemeinen werden persönliche Eindrücke und Erfahrungen sowohl aus Sicht der Studierenden als auch einer Dozentin geschildert.

**Schlagwörter:** Cyberattacke, Hackerangriff, Studium, HAW Hamburg

## Studying with and during the cyberattack Experiences to the cyberattack at HAW Hamburg

### Abstract

The article deals with the cyberattack that occurred at Hamburg University of Applied Sciences in December 2022. After a short introduction about cyber attacks in general, personal impressions and experiences are described from both the perspective of the students and a lecturer.

**Keywords:** Cyberattack, Hacker Attack, Studies, Hamburg University of Applied Sciences

# 1 Über den Cyberangriff

## 1.1 Definition

„Cyberangriffe sind vorsätzliche Versuche, Daten, Anwendungen oder andere Assets durch unbefugten Zugriff auf ein Netzwerk, ein Computersystem oder ein digitales Gerät zu stehlen, offenzulegen, zu verändern, zu deaktivieren oder zu zerstören“ ([IBM 2023](#)). Cyberkriminelle verschaffen sich unbefugten Zugriff auf digitale Geräte aus verschiedenen Gründen, u. a. um Daten zu stehlen oder zu beschädigen, um Geld mittels Erpressung einzufordern, um ihr Können unter Beweis zu stellen oder um staatliche Institutionen oder Wettbewerbsunternehmen auszuspionieren ([Generali 2023](#); [IBM 2023](#)).

## 1.2 Formen von Cyberattacken

Es gibt drei verbreitete Formen von Cyberattacken:

- Phishing und Spear-Phishing: Hierbei werden seriös wirkende E-Mails von Hacker\*innen verschickt, damit die angegriffenen Personen ihre Daten preisgeben.
- DoS- und DDoS-Attacken: Unter Denial of Service versteht man, dass ein System außer Betrieb gesetzt wird. Dies wird erreicht, indem die Hacker\*innen eine Flut an Anfragen an den Server senden. Häufig bricht somit das System zusammen.
- Schadsoftware (Malware): Das sind Viren, die einen Programmcode beinhalten. Diese heften sich an die Wirtsdaten an, welche sich daraufhin vermehren und einen gewissen Schaden verursachen. Durch die Ransomware wird der Zugriff zum System eingeschränkt, um Lösegeld von den Opfern zu erpressen (engl. „ransom“). Die Gefahr dabei ist, dass die Wiederfreigabe der Daten von den Hackern\*innen ungewiss ist ([Generali 2023](#)).

## 1.3 Cyberattacke auf die HAW Hamburg

„Im Dezember 2022 wurde die technische Informations- und Kommunikationsinfrastruktur der HAW Hamburg durch Cyberkriminelle angegriffen. Ursächlich war eine zunächst unbemerkte Phishing-Attacke sowie eine vermutlich unzureichend segmentierte Systemarchitektur, die es den Hacker\*innen ermöglicht hat, sich verschiedene Systemberechtigungen und Adminrechte zu verschaffen. Damit konnten sie Daten und Plattformen verschlüsseln sowie gespeicherte Backups löschen. Die HAW Hamburg hat daraufhin eine Anzeige beim Landeskriminalamt der Abteilung Cyberkriminalität erstattet. Der Vorfall wurde aber darüber hinaus dem Hamburger Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) gemäß Art. 33 DSGVO (Datenschutz-Grundverordnung) sowie dem CERT Nord gemeldet, dem Computer Emergency Response Team für die Verwaltungen der Länder Schleswig-Holstein, Hamburg, Bremen und Sachsen-Anhalt. Betroffene Personengruppen wurden nach Art. 34 DSGVO informiert. Nachdem die Hochschule auf die Lösegeldforderungen der Hacker\*innen nicht eingegangen ist, wurden am 05.03.2023 personenbezogene Daten im Darknet veröffentlicht. ([HAW Hamburg 2023](#)).

## 2 Auswirkungen der Cyberattacke auf das Studium

### 2.1 Befragung einer Studentin des 5. Semesters (Bibliotheks- und Informationsmanagement)

#### **Wann und wie haben Sie von der Cyberattacke erfahren?**

Ich wollte zwischen Weihnachten und Neujahr meinen Notenspiegel auf dem My-HAW-Portal herunterladen und musste feststellen, dass die Seite nicht erreichbar war. Ich glaube, ich habe dann noch andere Seiten der HAW versucht aufzurufen. Auf jeden Fall habe ich dann in Google nach so etwas wie „HAW Website nicht erreichbar“ oder „HAW technische Probleme“ gesucht und bin dann auf die Instagram-Posts gestoßen. Oder erst auf die Zeitungsartikel? So genau weiß ich das nicht mehr.

#### **Wo waren Sie, als Sie von der Cyberattacke erfahren haben? (Uni? Praktikum? Sonstiges?)**

Im Praktikum.

#### **Wie haben Sie die Cyberattacke wahrgenommen? Was haben Sie dabei empfunden?**

Zuerst habe ich mich etwas erschreckt und war froh, dass ich gerade im Praktikum und nicht auf EMIL angewiesen war. Dann hatte ich die Befürchtung, dass alle meine Prüfungsnachweise weg sind. Leider hatte es recht lange gedauert, bis die letzte Note aus dem vorigen Semester eingetragen wurde, daher hatte ich nur einen Auszug aus der Notenübersicht vom 1. Semester, bei der dann natürlich viele Noten fehlten. Außerdem war es praktisch unmöglich, auf Literatur zugreifen zu können, was für den Praktikumsbericht von Nachteil war.

#### **Welche Maßnahmen der HAW Hamburg wurden Ihrer Meinung gut umgesetzt?**

Moodle wurde zum nächsten Semester hin eingerichtet und irgendwann konnten dann auch die Office Produkte wieder genutzt werden. Als die Website wieder lief wurden dort auch IT-Sicherheitshinweise veröffentlicht.

#### **Welche Maßnahmen der HAW Hamburg wurden Ihrer Meinung nach nicht gut umgesetzt und wie könnten diese in Zukunft verbessert werden?**

Es gibt leider immer noch keine Möglichkeit die Rechner vor Ort mit einem eigenen Benutzeraccount zu nutzen, so dass eigene Geräte mitgebracht werden müssen. Die Semesterunterlagen wurden zwei Semester lang auf Papier verschickt und es gab zunächst keine elektronische Immatrikulationsbescheinigung für den Arbeitgeber, was in meinem Fall einiges Hin und Her verursacht hat. E-Mail-Verteiler rasch wieder einzurichten, hätte uns im Projektsemester geholfen und wäre vermutlich auch für die Dozent\*innen sehr hilfreich gewesen.

## 2.2 Befragung einer Dozentin aus dem Studiengang Bibliotheks- und Informationsmanagement

### **Wann und Wie haben Sie von der Cyberattacke erfahren?**

Die Ahnung, dass die IT ein Problem hat, hatte ich bereits zwischen Weihnachten und Neujahr, da die Server nicht mehr erreichbar waren. Anfang des Jahres stand es dann auf der Webseite.

### **Wo waren Sie, als Sie von der Cyberattacke erfahren haben?**

In der vorlesungsfreien Zeit im Home-Office.

### **Wie haben Sie die Cyberattacke wahrgenommen? Was haben Sie dabei empfunden?**

Unsicherheit, Ohnmacht, Wut – den Verursachern gegenüber. Bildungseinrichtungen anzugreifen ist einfach mies.

### **Welche Maßnahmen der HAW Hamburg wurden Ihrer Meinung gut umgesetzt?**

Die Situation war schwierig, die zentrale Unterstützung sehr langsam. Immerhin gab es auf Fakultäts- und Departmentsebene konkrete Unterstützung. Wir haben uns vor allem selbst geholfen, um zum Beispiel Kommunikationsstrukturen wieder aufzubauen.

### **Welche Maßnahmen der HAW Hamburg wurden Ihrer Meinung nach nicht gut umgesetzt und wie könnten diese in Zukunft verbessert werden?**

Kommunikation muss schneller und konkreter sein. Die schnelle Einrichtung von Kommunikationsstrukturen ist wichtig.

## 3 Persönliche Erfahrungen

### 3.1 Erste Kenntnisse der Cyberattacke

Tatsächlich habe ich erst von der Cyberattacke im neuen Jahr erfahren. Zuvor hatte ich aber schon von einigen Studierenden aus dem Semester gehört, dass sie Probleme hatten, ihr HAW-Mailkonto zu öffnen. Daraufhin habe ich selbst versucht, mein Mailkonto zu öffnen, woran ich ebenfalls gescheitert bin. Meine erste Kenntnis der Cyberattacke erhielt ich durch einen Newsbeitrag vom NDR, welcher am 03.01.2023 in eine der Semestergruppen auf WhatsApp gestellt wurde ([NDR 2023](#)).

Zu dem Zeitpunkt der Cyberattacke befand ich mich im Praktikum. Ansonsten wäre ich wahrscheinlich schon früher auf die Attacke hingewiesen worden, durch die tägliche Nutzung der E-Learning-Plattform „EMIL“ und des E-Mail Accounts der HAW Hamburg. Diese fielen für mich während des Praktikums weg bzw. verringerten sich, durch die Aufgaben in der Praktikumeinrichtung.

### 3.2 Wahrnehmung der Cyberattacke

Zu Beginn der Cyberattacke habe ich mich hilflos gefühlt, da man keinen direkten Kontakt zu seinen Dozent\*innen herstellen konnte. Vor allem in Bezug zu Aufgaben, Treffen, Abgabe der Semesterarbeit und die Entscheidung der Wahlpflichtkurse. Aber auch die generelle Ungewissheit, weil man nicht viele Informationen zum Thema hatte.

Am 14.01.2023 wurde der zweite Newsbeitrag in dieselbe WhatsApp-Gruppe gestellt. Dieser war von der Tagesschau, worin die Hintergründe der Cyberattacke erläutert wurden. In dem Zusammenhang machte sich ein anderes Gefühl breit. Ich würde es schon fast als Angst bezeichnen, aufgrund von den Schlagworten, die man im Artikel lesen konnte. Dies umfassten Worte und Meldungen wie „Hackergruppe“, „Vice Society“, „droht sie, erbeutete Daten zu veröffentlichen“, „Angreifer in Russland“, „All Ihre Dateien wurden von der 'Vice Society' verschlüsselt“, „Wenn Sie uns nicht innerhalb von sieben Tagen kontaktieren, werden wir die Dateien ins Darknet hochladen“, „Mitteilung des FBI zufolge konzentriert sich die Gruppe "unverhältnismäßig stark auf den Bildungssektor"“(Tagesschau 2023).

### 3.3 Gut umgesetzte Maßnahmen der HAW Hamburg

Wenn man an den Unialltag denkt, war für mich am wichtigsten: die Benutzung einer Plattform, worin die Aufgaben formuliert werden sowie wo das Ablegen von Materialien, Präsentationen und die Anmerkungen von Dozenten\*innen möglich ist. Es wurde die Übergangs-Plattform „Moodle“ angelegt, die in Vielem der alten Plattform „EMIL“ ähnelte. So konnten wir uns relativ leicht umstellen. Denn ohne eine Plattform zur Ablage von Informationen sehe ich nicht, wie man effizient im betroffenen Semester hätte arbeiten können.

Die Einrichtung der Updates über die Webseite der HAW Hamburg waren sehr hilfreich, sodass man Informationen erhalten hat, welche Maßnahmen ergriffen werden und wie die Kommunikation organisiert ist. Teilweise habe ich mehrfach täglich auf die Webseite geschaut, ob weitere Neuigkeiten enthalten sind ([HAW Hamburg 2023](#)).

### 3.4 Weitere Kommunikationswege

Über Social Media, besonders via Instagram, wurde man über aktuelle Änderungen und Neuigkeiten auf dem Laufenden gehalten. Bezüglich der Kommunikation dort wurde z. B. angegeben, an welche Dozenten\*innen man sich für welches Department wenden soll. Dazu wurden die Beiträge benutzt, aber vor allem durch die Stories des Accounts konnte man relevante Informationen erhalten.

Nach einigen Wochen wurde sich dann dazu entschieden, Briefpost an die Studierenden zu verschicken. Das war eine gute Lösung, da so die zeitbegrenzten Benutzernamen und Passwörter vergeben wurden sowie die Einleitung zur Einrichtung der

Accounts. Damit hatte man wieder Zugriff auf sein MS-Teams, aber auch auf das MS Office Paket und kurze Zeit später auch auf Outlook für die E-Mails. Dadurch gingen jedoch zuvor gespeicherte Daten verloren und man musste sich neue Dokumente anlegen und E-Mails verfassen. Mit der Briefpost wurden seitdem auch die Semesterunterlagen verschickt, welche z. B. den Studierendenausweis und die HVV-Karte beinhaltete. Die lagen den Studierenden somit nur in Papierform vor. Das Positive an der Briefpost ist, dass man komplett von den technischen Geräten abgegrenzt und „analog“ ist, was Sinn macht bei einer Cyberattacke. Das bringt mich aber zugleich auch zum negativen Punkt. Durch die Briefpost sehe ich einen starken Rückgang in Bezug auf die Digitalisierung, die Benutzung von technischen Geräten. Während der Corona-Pandemie waren wir dazu gezwungen diese auszubauen, z. B. durch die Verwendung von ZOOM. Nun gingen wir wieder einen Schritt zurück zur Benutzung von Papier und der Briefpost, die als überwunden galt. Es ist keine ideale Lösung, aber es ist die, die zu diesem Zeitpunkt von Nutzen war.

#### 4 Fazit

Für mich stellen die Computer in den Lehrräumen jetzt eher eine Gefahr als eine Hilfe dar. Zu Beginn des Studiums habe ich fast nur die Computer in den Lehrräumen benutzt. Nach der Cyberattacke bringe ich meinen eigenen Laptop in die Uni mit. Nach meinem Wissen kann man sich noch nicht wieder in seinen eigenen Account einloggen außer in „Student\*in“ oder „Gast“. Die Arbeit an den Computern vor Ort ist möglich, aber unpersönlicher, da sich theoretisch jede\*r Student\*in über das Konto einloggen kann. Ich sehe dadurch ein Problem, weil man heute auf die Technik angewiesen ist, um mit ihr effizienter arbeiten zu können, besonders im Studium, wo die Digitalität für uns jeden Tag eine wichtige Rolle spielt.

Die Cyberattacke stellte sowohl die Studierenden als auch die Dozent\*innen, sowie alle an der Hochschule insgesamt vor eine große Herausforderung. So ist es verständlich, dass noch nicht alles wieder so funktioniert wie vor der Cyberattacke. Ich finde dabei jedoch wichtig, dass wir die Cyberattacke nicht vergessen, sondern von ihr lernen können, welche Verbesserungen vorgenommen werden müssen, um einen sicheren Uni-Alltag zu schaffen.

## Literatur

GENERALI, 2023. *Die wichtigsten Maßnahmen beim Verdacht auf einen Hackerangriff* [online]. [Zugriff am 23.12.2023]. Verfügbar unter: <https://www.generali.de/journal/die-wichtigsten-massnahmen-beim-verdacht-auf-einen-hackerangriff>

HAW HAMBURG, 2023. *HAW-Hamburg: Angriff auf die IT-Infrastruktur* [online]. [Zugriff am 19.12.2023]. Verfügbar unter: <https://www.haw-hamburg.de/cyberangriff/>

IBM, 2023. *Was ist ein Cyberangriff?* [online]. [Zugriff am 19.12.2023]. Verfügbar unter: <https://www.ibm.com/de-de/topics/cyber-attack>

NDR, 2023. *Hamburg: Studierende kritisieren HAW wegen Cyberangriff* [online]. [Zugriff am 19.12.2023]. Verfügbar unter: <https://www.ndr.de/nachrichten/hamburg/Hamburg-Studierende-kritisieren-HAW-wegen-Cyberangriff,hacker446.html>

TAGESSCHAU, 2023. *Hamburger Hochschule wird von Hackern erpresst* [online]. [Zugriff am 19.12.2023]. Verfügbar unter: <https://www.tagesschau.de/investigativ/rbb/hackernangriff-haw-vice-101.html>