To
All employees,
All students,
Professors/instructors,
Service providers,

Subject: Cyber-attack: Information pursuant to article 34 of the GDPR regarding the security incident at the Hamburg University of Applied Sciences (HAW Hamburg)

Dear students and colleagues,

Based on the information available to us from the analysis of the cyber-attack, we know that data have been compromised. We would like to inform you here about the facts of the situation. In doing so, we are fulfilling our obligation to provide information pursuant to article 34 of the GDPR.

HAW Hamburg's official data protection officer is involved. Contact information:
office (at) datenschutz-nord (dot) de; Tel.: 040 5936160400.

What has happened?
The information and communications infrastructure at HAW Hamburg has been targeted by hackers. This was determined on 29 December 2022.

Based on what we know to date, the hackers used decentralised IT systems to manually work their way into HAW Hamburg's central IT and security systems via the network. Using this path, they also obtained the administrative rights for the central storage systems and compromised the central data storage. They then used these administrative rights to begin encrypting various virtualised platforms and deleting stored backups.

What does this mean for you?
As part of the forensic analysis, it has been ascertained that significant amounts of data from various areas were copied and leaked by the hackers.

At the current time, we presume that, at a minimum, the following data have been compromised:

- User names and passwords (cryptographically secured)
- Email addresses
- Stored email addresses, when forwarding to another email was set up, as well as mobile telephone numbers, when call-forwarding was set up
- Employee numbers, student numbers, and internal ID numbers
- Organisational affiliation with university departments/units
- Where applicable: access privileges such as team and group memberships
- Where applicable: additional information in text boxes that can be filled out for self-service functions

It is possible that additional information from areas outside the central university administration (faculties, departments, labs, etc.) have also been saved. This information could include, for example, the IP addresses and details of the individual's computer, as well as other professional or private details that were stored in this context.

A potential risk is that the leaked data could be misused.

6 January 2023

What do you need to do now?
Please stay up to date by checking the HAW Hamburg website created for this purpose each day.

HAW Hamburg: Cyber-attack on IT systems

On this page we will communicate the measures that need to be taken and, in particular, provide you with additional support regarding how you should handle your electronic devices and how the use of HAW Hamburg's IT services is being restored.

Following the restoration or reconstruction of HAW Hamburg's IT environment, we will request that you reset your password.

What is HAW Hamburg doing to deal with the situation?
Due to the attack and in order to prevent further damage or loss of data, all systems have been shut down as a precautionary measure. This has resulted in drastic limitations to critical IT services. These limitations are impacting the entire university.

HAW Hamburg has convened a crisis team and contracted an IT service provider to assist with the forensic analysis and the restoration of the various systems.

Parallel to the analysis and assessment of the incident, the IT services are being restored.

HAW Hamburg has filed a complaint with the cyber-crime division of the Landeskriminalamt. Additionally, the incident has been reported to the Hamburg commissioner for data protection and freedom of information in accordance with article 33 of the GDPR. HAW Hamburg has also notified the Computer Emergency Response Team (CERTnord) for the administrations of the states of Schleswig-Holstein, Hamburg, Bremen and Sachsen-Anhalt, as well as the Computer Emergency and Response Team (DFN-CERT) of the German Research Network.