An
alle Beschäftigten
alle Studierenden
Lehrbeauftragten
Dienstleister

Betreff: IT-Angriff: Information nach Art. 34 DSGVO zum Sicherheitsvorfall an der Hochschule für Angewandte Wissenschaften Hamburg (HAW Hamburg)

Sehr geehrte Damen und Herren,

aufgrund der uns vorliegenden Informationen aus den Analysen des IT-Angriffs wissen wir, dass Daten abgeflossen sind. Hiermit möchten wir Sie über den Sachverhalt informieren. Damit kommen wir unserer Informationspflicht laut Art. 34 DSGVO nach.

Der behördliche Datenschutzbeauftragte der HAW Hamburg ist involviert. Kontaktdaten:
office (at) datenschutz-nord (dot) de; Tel.: 040 5936160400.

Was ist passiert?

Die technische Informations- und Kommunikationsinfrastruktur der HAW Hamburg ist angegriffen worden. Dies wurde am 29. Dezember 2022 festgestellt.

Nach derzeitigem Kenntnisstand haben sich die Angreifer ausgehend von dezentralen IT-Systemen über das Netzwerk manuell bis in die zentralen IT- und Sicherheitskomponenten der HAW Hamburg vorgearbeitet. Über diesen Angriffspfad haben sie auch administrative Rechte auf den zentralen Storage-Systemen erlangt und damit die zentrale Datenhaltung kompromittiert. Mit den erlangten administrativen Rechten wurde abschließend die Verschlüsselung diverser virtualisierter Plattformen und das Löschen gespeicherter Backups gestartet.

Was bedeutet das für Sie?
Im Rahmen der forensischen Untersuchung konnte nachgewiesen werden, dass signifikante Datenmengen aus verschiedenen Bereichen durch den Angreifer kopiert wurden und abgeflossen sind.

Wir gehen zum aktuellen Zeitpunkt davon aus, dass mindestens folgende Daten abgeflossen sind:

- die Benutzer*innennamen und Passwörter (kryptographisch gesichert),
- E-Mail-Adressen,
- hinterlegte E-Mail-Adressen, soweit eine externe E-Mail-Weiterleitung besteht, desgleichen hinterlegte Mobilfunk-Nummern,
- Personalnummern der Beschäftigten, Matrikelnummern der Studierenden sowie interne Kennungen,
- organisatorische Zugehörigkeiten zu Hochschul-Bereichen,
- ggf. erhaltene Berechtigungen wie Team-Zugehörigkeiten und Gruppenmitgliedschaften,
- ggf. weitere Informationen in Textfeldern, die durch Self-Services gefüllt werden konnten.

Möglicherweise sind in dezentralen Bereichen (Fakultäten, Departments, Labore etc.) weitere Informationen gespeichert worden. Solche Informationen können z.B. die IP-Adresse und Details der Rechner der betroffenen Person sein, aber auch weitere dienstliche oder private Details, die in diesem Zusammenhang abgelegt wurden.

Ein mögliches Risiko ist, dass die abgeflossenen Daten missbräuchlich genutzt werden.

Was müssen Sie nun unternehmen?
Informieren Sie sich tagesaktuell über die dafür eingerichtete Web-Seite der HAW Hamburg unter:

HAW-Hamburg: Angriff auf die IT-Infrastruktur

Dort werden wir alle zu treffenden Maßnahmen kommunizieren und Ihnen insbesondere weitere Unterstützung liefern, wie Sie konkret weiter mit Ihren Endgeräten umgehen sollen bzw. wie die Nutzung der IT-Dienste der HAW Hamburg anläuft.

Nach der Wiederherstellung bzw. dem Neuaufbau der IT-Umgebung der HAW Hamburg werden wir Sie auffordern, ein neues Passwort zu setzen.

Was unternimmt die HAW Hamburg?

Aufgrund des Angriffs und um weiteren Schaden zu vermeiden, wurde die gesamte Kommunikationsinfrastruktur vorsorglich stillgelegt. Dies hat drastische Einschränkungen bei kritischen IT-Services zur Folge. Die Einschränkungen betreffen die gesamte Hochschule und alle ihre Bereiche.

Die HAW Hamburg hat einen Krisenstab einberufen und einen IT-Dienstleister eingebunden, der bei der forensischen Aufklärung und der Wiederinbetriebnahme der verschiedenen Dienste unterstützt.

Parallel zur Analyse und Auswertung des Vorfalls werden die Dienste sukzessive wiederhergestellt.

Die HAW Hamburg hat beim Landeskriminalamt, Abteilung Cyber-Kriminalität, Anzeige erstattet. Außerdem wurde der Vorfall gem. Art. 33 DS-GVO dem Hamburger Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) gemeldet. Auch erfolgte eine Meldung an das CERTnord, das"Computer Emergency Response Team" für die Verwaltungen der Länder Schleswig-Holstein, Hamburg, Bremen und Sachsen-Anhalt, sowie das DFN-CERT, das Computer Emergency and Response Team des Deutschen Forschungsnetzwerks.

Stand:06.01.2023