Hochschule Biberach
Karlstrasse 11
D - 88400 Biberach
Deutschland

30.06.2026

Benachrichtigung über eine Datenschutzverletzung gemäß Art. 34 DSGVO: Kompromittiertes E-Mail-Postfach vom 16.06.2026 | CaseID#576328

Am 16.06.2026 10:00 wurde uns folgende Datenschutzverletzung bekannt, über welche wir Sie fristgerecht informieren.

Art der Verletzung

Im Rahmen eines Angriffs auf ein E-Mail-Konto eines Hochschulangehörigen (Studierender) haben sich unberechtigte Dritte Zugriff auf ein E-Mail-Postfach der Hochschule Biberach verschafft. Die erlangten Zugangsdaten wurden unter anderem dazu genutzt, über dieses Konto Phishing- bzw. Spam-E-Mails zu versenden. Durch den unberechtigten Zugriff auf das E-Mail Postfach kann nicht ausgeschlossen werden, dass personenbezogene Daten, die im Rahmen der E-Mail-Kommunikation verarbeitet wurden, von den Angreifern eingesehen oder gesichert wurden. Typischerweise können dabei insbesondere folgende Datenarten betroffen sein:

- Persönliche Identifikationsdaten (z. B. Namen, Funktionsbezeichnungen)
- Kommunikationsdaten (E-Mail-Adressen)
- Inhalte der E-Mail-Kommunikation einschließlich projekt- oder studienbezogener Informationen
- E-Mail-Anhänge, die organisatorische, verwaltungsbezogene oder projektbezogene Inhalte enthalten

Potentiell betroffene Personen:

- Mitglieder und Angehörige der Hochschule
- Externe Personen, mit denen über das betroffene E-Mail-Konto kommuniziert wurde
- Externe Empfänger der versandten Phishing-/Spam-E-Mails

Der Vorfall endete am 16.06.2026 16:00.

Name und Kontaktdaten des/der Verantwortlichen:

Name	Rektor Professor Dr.-Ing. Matthias Bahr
Anschrift	Hochschule Biberach Karlstrasse 11 D - 88400 Biberach
E-Mail	info@hochschule-bc.de
Telefonnummer	+49 (0) 7351 582-0

Name und Kontaktdaten des/der Datenschutzbeauftragten

Name:	Benedict Lenz
Anschrift:	EXACON Prüf- und Sachverständigengesellschaft mbH Untere Gallusstr. 34 D - 88677 Markdorf
E-Mail:	datenschutzbeauftragter@hochschule-bc.de
Telefonnummer:	+49 (0) 7544 912982

Folgende Maßnahmen wurden zur Abmilderung bzw. Behebung der Datenschutzverletzung gesetzt:

Bezeichnung	Beschreibung
Benachrichtigung der Betroffenen	Die betroffenen Personen werden über den Datenschutzvorfall informiert. Zudem erfolgt eine Sensibilisierung der Hochschulangehörigen für Phishing- und Social-Engineering-Angriffe sowie Hinweise zu sicheren Verhaltensweisen im E-Mail-Verkehr, um mögliche Folgerisiken zu reduzieren.
Meldung des Vorfalls an die zuständige Datenschutzaufsichtsbehörde	Der Datenschutzvorfall wurde an die zuständige Datenschutzaufsichtsbehörde gemeldet. Dadurch wurde sichergestellt, dass der Vorfall transparent dokumentiert ist und durch die Aufsichtsbehörde geprüft werden kann.
Sperrung des kompromittierten E-Mail-Kontos und Vergabe neuer Zugangsdaten	Das Passwort des kompromittierten E-Mail-Kontos wurde geändert, um einen weiteren Zugriff auf dieses durch die Hacker zu verhindern.
Technische Analyse des betroffenen E-Mail-Postfachs	Das betroffene E-Mail-Postfach wurde technisch überprüft, um den Umfang des Vorfalls besser einschätzen zu können und festzustellen, ob und in welchem Umfang unberechtigte Zugriffe erfolgt sind. Die Analyse diente zudem dazu, weitere Sicherheitsrisiken auszuschließen.

Eine Analyse hat ergeben, dass voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen besteht:

☑	Risiko Identitätsdiebstahl oder -betrug
☑	Risiko Rufschädigung
☑	Risiko Kontrollverlust

Mögliche Folgen für betroffene Personen:

Es kann nicht ausgeschlossen werden, dass unberechtigte Dritte vor der Unterbindung des Zugriffs Inhalte der kompromittierten E-Mail-Postfächer eingesehen oder gesichert haben. Dadurch besteht die Möglichkeit, dass personenbezogene Daten oder Dokumente weiterhin unbefugt verwendet werden.

Ein denkbares Szenario ist insbesondere die Nutzung dieser Informationen für weitere gezielte Angriffe, etwa durch täuschend echt wirkende E-Mails („Spear-Phishing“), die inhaltlich an frühere Kommunikation oder

persönliche Kontexte anknüpfen. Darüber hinaus besteht das Risiko, dass über den Versand von Spam- oder Phishing-Nachrichten schadhafte Links oder Inhalte verbreitet werden, über die beim Anklicken Schadsoftware auf den Endgeräten der betroffenen Personen installiert werden könnte.

Diese Risiken können insbesondere dann erhöht sein, wenn betroffene Personen

- schadhafte Links oder Dateianhänge in E-Mails öffnen oder
- Zugangsdaten oder Passwörter ungewollt gegenüber Dritten preisgeben.

Sonstige Informationen für Betroffene:

Betroffenen wird empfohlen, im täglichen E-Mail-Verkehr erhöhte Wachsamkeit walten zu lassen. Insbesondere sollte auf ungewöhnliche oder unerwartete Nachrichten, abweichende Absenderadressen sowie auf ungewohnte Formulierungen oder Inhalte geachtet werden.

Bei Unsicherheiten sollte stets geprüft werden, ob der angezeigte Name des Absenders zur tatsächlichen Absender-E-Mail-Adresse passt. Abweichungen oder unplausible Kombinationen können ein Hinweis auf einen betrügerischen Versand sein. Auch E-Mails, die einen ungewöhnlichen Kontext haben oder sich nicht eindeutig einer bekannten Kommunikation zuordnen lassen, sollten kritisch hinterfragt werden.

Typische Merkmale von Phishing- oder Social-Engineering-Angriffen sind unter anderem:

- Aufforderungen zu sofortigem Handeln („Bitte klicken Sie umgehend…“, „Ihr Konto wird gesperrt…“),
- das Erzeugen von Zeitdruck oder Dringlichkeit,
- die Aufforderung, Links zu öffnen, Dateien herunterzuladen oder Zugangsdaten preiszugeben.

Links oder Dateianhänge aus verdächtigen E-Mails sollten nicht geöffnet werden. Zugangsdaten, Passwörter oder sonstige vertrauliche Informationen sollten grundsätzlich nicht per E-Mail weitergegeben werden.

Sofern Zweifel an der Echtheit einer Nachricht bestehen oder Auffälligkeiten festgestellt werden, wird empfohlen, die E-Mail nicht zu beantworten und den Vorfall an die zuständigen Stellen der Hochschule zu melden.

Diese Hinweise dienen der Sensibilisierung für Phishing- und Social-Engineering-Angriffe sowie der Reduzierung möglicher Folgerisiken im Zusammenhang mit dem beschriebenen Vorfall.