



Pädagogische Hochschule Freiburg · Kunzenweg 21 · 79117 Freiburg
Rektor

An die Mitglieder und Angehörigen
der PH Freiburg

An die externen Partner der PH Freiburg

Rektorat

Der Rektor
Prof. Dr. Hans-Georg Kotthoff

Tel. +49.(0)761.682-263
Fax +49.(0)761.682-603
kanzler@ph-freiburg.de

bearbeitet von / Aktenzeichen

23. Juni 2022

**Betreff: Cyberangriff - Information zum Sicherheitsvorfall
an der PH Freiburg nach Art. 34 DSGVO**

Sehr geehrte Damen und Herren,
liebe Kolleginnen und Kollegen,
liebe Studierende,

aufgrund der uns vorliegenden Informationen aus den Analysen des Cyberangriffes auf unsere Hochschule wissen wir, dass Daten abgeflossen sind. Hierüber informieren wir Sie im Rahmen unserer Meldepflicht gemäß Art. 34 DSGVO in einem ersten Schritt:

Der behördliche Datenschutzbeauftragte der PH Freiburg, Dr. Bernd Remmele, erreichbar unter datenschutz@ph-freiburg.de wurde eingebunden und steht auch für Sie für Rückfragen zu Ihren abgeflossenen Daten zur Verfügung.

Was ist passiert?

Am 6. Juni 2022 erfolgte ein Cyberangriff auf die Pädagogische Hochschule Freiburg. Der Angreifer hat sich vermutlich über eine Phishing-Attacke Zugang zu unserer IT-Infrastruktur verschafft. Am 06. Juni 2022 entdeckten wir auf unseren Windows-Systemen verschlüsselte Dateien. Daraufhin haben wir unverzüglich alle Systeme heruntergefahren und vom Netz genommen.

Nach derzeitigem Kenntnisstand hat sich der Angreifer mehrere Tage vor diesem Datum in verschiedenen IT-Systemen bewegt, Schadsoftware installiert und umfangreich Daten kopiert. Es ist nicht ausgeschlossen, dass die Angreifer die abgeflossenen Daten unbestimmten Dritten zugänglich machen. Teile dieser Daten sind von erheblicher datenschutzrechtlicher Relevanz.

Was bedeutet das für Sie?

Im Rahmen der forensischen Untersuchung konnte nachgewiesen werden, dass Daten einer zentralen Dateiablage der Mitarbeitenden abgeflossen sind. Weitere Datenabflüsse konnten in der noch andauernden forensischen Untersuchung bisher nicht nachgewiesen werden.

Auf dieser Dateiablage waren Informationen verschiedener Funktionseinheiten der PH Freiburg gespeichert und damit personenbezogene Daten vielfältiger Art. Neben Identitätsdaten wie Name, E-Mail-Adresse, Anschrift, Matrikelnummer, etc. finden sich weitere Informationen von einzelnen Personen, die zu Identitätsdiebstahl und individuellen ausgerichtete Attacken auf Basis dieser Informationen führen können.

Worauf Sie nun achten müssen!

1. Verfolgen Sie die Anweisungen der PH Freiburg in Hinblick auf die Neuvergabe Ihrer Passwörter und dem Aufbau der weiteren Sicherheitsarchitektur für die PH-Dienste.
2. Sollten Sie Ihr bisheriges PH-Passwort bei anderen Diensten verwenden, ändern Sie die Passwörter bei diesen Diensten auf unabhängige Passwörter. Es ist grundsätzlich nicht zu empfehlen, dasselbe Passwort mehrfach oder ähnlich lautende Passwörter zu verwenden. Vermeiden Sie die Nutzung von persönlichen Merkmalen bei der Passwortvergabe.
3. Sollten Sie Passwörter auf der zentralen Dateiablage der PH Freiburg gespeichert haben, ändern Sie diese unbedingt.
4. Achten Sie verstärkt auf Phishing-Kampagnen über E-Mail und andere Kommunikationskanäle, in denen Sie gebeten werden, Login-Daten anzugeben oder auf fremde Seiten umgeleitet werden, auf denen Sie sich unter Angabe Ihrer Daten registrieren sollen. Hinterfragen Sie auch solche Anfragen, die persönliche Informationen von Ihnen enthalten, um vermeintliches Vertrauen aufzubauen.

Was unternimmt die PH Freiburg?

Alle betroffenen Systeme wurden abgeschaltet. Parallel zur forensischen Analyse wurde unter Hochdruck damit begonnen, die zentrale IT-Infrastruktur der PH Freiburg vollständig neu aufzusetzen. Die im Zuge des Vorfalls gewonnenen Erkenntnisse und Empfehlungen des externen Dienstleisters, der Ermittlungsbehörden und der Cybersicherheitsagentur Baden-Württemberg werden dabei hochschulspezifisch in der neuen Sicherheitsarchitektur umgesetzt. Dies bedeutet sowohl technische als auch organisatorische Änderungen. Der Wiederaufbau erfolgt in Etappen und priorisiert. Bis zur vollständigen Wiederherstellung und der Überführung aller IT-Systeme kann es noch mehrere Monate dauern.

Es wurde Strafanzeige erstattet. Gleichzeitig haben wir einen IT-Krisendienstleister engagiert, um uns bei der Aufklärung (sogenannte „Forensik“) und der Bewältigung des IT-Sicherheitsvorfalls zu unterstützen. Weiterhin haben wir den Vorfall dem Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI) gemäß Art. 33 DSGVO gemeldet.



Wir werden Sie weiterhin fortlaufend unter anderem über <https://www.ph-freiburg.de/stoerung> informieren, in allgemeiner Hinsicht sowie auch in Hinblick auf Meldeerfordernisse nach Art. 34 DSGVO.

Mit freundlichen Grüßen

Prof. Dr. Hans-Georg Kotthoff
Rektor der Pädagogischen Hochschule Freiburg