

Update zum Datenschutzvorfall

29.9.2026 - | Ludwig-Maximilians-Universität München

Die LMU ist Ziel eines Angriffs auf ihre IT-Systeme geworden. Hier informiert die Hochschulleitung nach Art 34 DS-GVO über die bisher bekannten Details.

Seit dem 16. September ist die LMU mit maximalem zeitlichem und personellem Einsatz damit befasst, den unbefugten Cyberangriff auf eines ihrer IT-Systeme abzuwehren und aufzuklären. Unmittelbar nach den ersten Anzeichen wurden umfangreiche Gegenmaßnahmen ergriffen. Das betroffene IT-System wurde heruntergefahren; die Daten wurden gesichert. Vorsorglich wurden weitere nicht betroffene Systeme vom Netz genommen und sicherheitstechnisch überprüft. Die zuständigen Aufsichts- und Ermittlungsbehörden wurden informiert; mit Unterstützung von internen und externen IT-Sicherheitsexperten wurde unverzüglich eine umfassende Analyse des Vorfalls gestartet.

Weitere Erkenntnisse aus der Datenanalyse

Nach den neuesten forensischen Erkenntnissen steht inzwischen fest, dass der gesamte Datensatz im Zulassungs-System betroffen war, dem System, in dem sämtliche Daten aktueller und ehemaliger Studierender verarbeitet werden. Der dortige Bestand umfasst somit Immatrikulationsdaten, die ca. 50 Jahre zurückgehen. Hinsichtlich der Betroffenen ist von ca. 600.000 Datensätzen auszugehen.

Die betroffenen Kategorien sind sehr unterschiedlich; der Umfang nimmt je nach Alter der Daten stetig ab. So enthalten die Datensätze bis einschließlich 1994 ausschließlich Stammdaten und die Semesterhistorie; ab 2005 liegen umfangreichere Angaben darunter teilweise auch Bankdaten vor. Ansonsten haben die Analyseergebnisse die am 19. September bereits kommunizierten betroffenen Datenkategorien bestätigt. Dazu gehören Identitäts-, Kontakt- und Bankdaten, soweit entsprechende Angaben gemacht wurden, sowie je nach Einzelfall weitere Informationen zum Studienverlauf und Angaben zu Beurlaubungsgründen.

Ausdrücklich nicht betroffen sind weiterhin Passwörter, sensible Daten in größerem Umfang sowie Prüfungsinformationen der LMU oder konkrete Angaben zu Studieninhalten und individuellen Leistungen.

Als öffentliche Institution ist die LMU verpflichtet, bestimmte Studieninformationen zur Erfüllung ihrer hoheitlichen Aufgaben und nach Maßgabe der gesetzlichen Vorgaben langfristig zu verarbeiten. Die Daten werden beispielsweise für Nachweise gegenüber der Rentenversicherung oder zur Ermittlung der Hochschulsemester benötigt. Vielfach stellt die LMU den ehemaligen und aktuellen Studierenden die Daten häufig auch erst kurz vor Renteneintritt zur Verfügung. Für die langfristige Speicherung dieser Daten orientiert sich die LMU an der im Hochschulwesen üblichen Aufbewahrungsfrist von rund 50 Jahren. Die Angabe einer Aufbewahrungsdauer von „bis zu“ 100 Jahren in der allgemeinen Datenschutzhinweise für Studierende auf unserer Website kam nicht zum Tragen und war in diesem Zusammenhang missverständlich; die Information wurde zwischenzeitlich präzisiert.

Die LMU konzentriert sich mit professioneller externer, sowie amtlicher zuständiger, Unterstützung neben der Aufklärung des Vorfalls auch weiterhin auf ein engmaschiges Monitoring des Darknets, um – sofern möglich – zu prüfen, ob die Daten veröffentlicht wurden. Nach bisherigen Erkenntnissen gibt es hierfür weiterhin keine Anhaltspunkte, weder für eine Veröffentlichung noch eine anderweitige missbräuchliche Verwendung.

Wiederinbetriebnahme weiterer IT-Systeme

Die LMU wird einzelne, nach dem IT-Sicherheitsvorfall nicht betroffene, aber vorsorglich heruntergefahren abgeschaltete Systeme nach einer umfassenden sicherheitstechnischen Überprüfung schrittweise wieder in Betrieb nehmen. Das zentrale Online-Vorlesungsverzeichnis (LSF) der Ludwig-Maximilians-Universität München (LMU) ist am Mittwoch, 30. September 2026, für Studiengangskordinatorinnen und -koordinatoren ab 9:00 Uhr und für Studierende ab 15:00 Uhr wieder erreichbar.

Zunächst stehen die wichtigsten Funktionen für den Semesterstart zur Verfügung: Veranstaltungen können angepasst und belegt sowie Notenspiegel abgerufen werden. Noch fehlende Noteneinträge werden zeitnah nachgetragen. Weitere LSF-Funktionen folgen schrittweise nach dem 30. September.

Aus Sicherheitsgründen ist der Zugang zu LSF zunächst nur im Münchner Wissenschaftsnetz und im LMU-Verwaltungsnetz möglich. Außerhalb der LMU ist eine VPN-Verbindung erforderlich. Für das Münchner Wissenschaftsnetz nutzen Sie bitte Edu-VPN; Hinweise finden Sie unter www.lmu.de/vpn.

Die Systeme für Feedback- und Prüfungsprozesse EvaSys und EvaExam stehen ab Montag, 28. September 2026, um 12:00 Uhr in beiden Netzen wieder zur Verfügung. Die sicherheitstechnischen Überprüfungen von OpenCampus und Apte (u.a. Eignungsfeststellungsverfahren) dauern an. Über deren Wiederinbetriebnahme informiert die LMU so schnell wie möglich.

Parallel wird die fortlaufende Einführung des geplanten neuen Systems CampusOnline mit Hochdruck fortgeführt. Ab Dezember 2026 wird es flächendeckend digitale Studienbewerbungen und Immatrikulationen auf sicherer Cloud Basis ermöglichen.

Hinweise für Betroffene

Es gibt derzeit weiterhin keine Anhaltspunkte dafür, dass Daten aus dem Angriff veröffentlicht oder anderweitig missbräuchlich verwendet wurden. Sollten sich aus dem zusätzlich eingerichteten Monitoring oder der fortlaufenden Aufklärung entsprechende Hinweise ergeben, informieren wir die Betroffenen unverzüglich. Wir raten zu besonderer Aufmerksamkeit und empfehlen die üblichen allgemeinen Vorsichtsmaßnahmen. Zum eigenen Schutz sollte insbesondere dies beachtet werden:

- Auch in vermeintlich persönlich adressierten E-Mails keine Anhänge oder Links – weder von unbekannten noch von bekannten Absendern – ohne genaue Prüfung öffnen.
- Besondere Aufmerksamkeit gegenüber verdächtigen Kontaktversuchen per E-Mail, Telefon oder Nachricht, insbesondere, wenn ein Bezug zur LMU oder dem Studium hergestellt wird. Keine Bankdaten oder Passwörter preisgeben.
- Unterlagen und Mitteilungen mit Bezug zur LMU oder dem Studium besonders sorgfältig prüfen.
- Weitere Hinweise zum Schutz vor Betrugsversuchen und zur sicheren Verwendung von Passwörtern finden sich auf der Internetseite des Bundesamts für Sicherheit und Informationstechnik unter www.bsi.bund.de.

Sämtliche neueren Informationen zum Vorfall und zur Wiederverfügbarkeit einzelner Dienste werden fortlaufend hier im Newsroom in den FAQs veröffentlicht.

Bei Rückfragen können sich Betroffene jederzeit an cybersicherheit@lmu.de wenden.

<https://www.lmu.de/de/die-lmu/struktur/zentrale-universitaetsverwaltung/presse-und-kommunikation-puk/press-room/pressemitteilung/update-zum-datenschutzvorfall-71c6c19a.html>