

digitalfabriX GmbH | Hansastraße 16 | 80686 München

Kundinnen und Kunden der digitalfabriX GmbH

Hansastraße 16
80686 München

Telefon: 089 5404408-0
info@digitalfabrix.de
www.digitalfabrix.de

27. Oktober 2026

Information zum DDoS-Angriff auf die Web-Infrastruktur der digitalfabriX vom 20. bis 25. Oktober 2026

Sehr geehrte Damen und Herren,

mit diesem Schreiben möchten wir Sie offen und umfassend über den Cyberangriff informieren, der in der vergangenen Woche unsere Web-Infrastruktur getroffen hat. Vorab das Wichtigste: Nach aktuellem Kenntnisstand wurden keine Daten entwendet oder manipuliert. Sämtliche Anwendungen stehen seit Freitag, 23. Oktober 2026, wieder uneingeschränkt zur Verfügung.

Was ist passiert?

In der Nacht zum 21. Oktober 2026 (Mittwoch) wurde die Web-Infrastruktur der digitalfabriX Ziel eines sogenannten Distributed-Denial-of-Service-Angriffs (DDoS). Bei einem solchen Angriff wird ein System durch eine extrem hohe Zahl gleichzeitiger Anfragen gezielt überlastet. Ziel ist die Störung der Erreichbarkeit, nicht das Ausspähen von Daten.

Der Angriff verlief in mehreren Wellen und erreichte seinen Höhepunkt am Vormittag des 22. Oktober 2026 (Donnerstag). Er flaute erst am 25. Oktober 2026 (Sonntag) ab.

Nach Angaben des Bayerischen Landesamts für Sicherheit in der Informationstechnik (LSI) zählen DDoS-Angriffe zu den häufigsten Angriffen auf die Verfügbarkeit von IT-Systemen.

Vorübergehend eingeschränkt waren insbesondere:

- Bürgerserviceportal
- komXformularcenter und Online-Anträge
- Ratsinformationssystem und SessionNet
- die Webauftritte der digitalfabriX sowie der Verwaltungen, die ihren Internetauftritt in dieser Infrastruktur betreiben

Welche Maßnahmen wurden ergriffen?

Unser Team IT Operations hat unmittelbar nach den ersten Auffälligkeiten mit der Analyse begonnen. Gemeinsam mit Firewall- und Netzwerkspezialisten sowie dem Support der Telekom wurde die Ursache eindeutig identifiziert.

1. **Sofortschutz:** Die vorhandenen Sicherheitsmechanismen griffen automatisch. Die betroffenen Leitungen wurden deaktiviert und sämtliche Anwendungen kontrolliert gestoppt. Dadurch war zu keinem Zeitpunkt ein Zugriff auf Daten oder Anwendungen möglich.
2. **Erweiterter Schutzschirm (22. Oktober):** Zusätzliche Schutzmaßnahmen wurden aktiviert und ein erweiterter Schutzschirm eingerichtet.
3. **Vorgelagerter DDoS-Schutz (23. Oktober):** Am Freitagvormittag wurde ein weiterer, vorgelagerter Schutzschirm über die gesamte Web-Infrastruktur gespannt. Er filtert schädlichen Datenverkehr, bevor dieser unsere Systeme erreicht. Ab etwa 14 Uhr konnten alle Anwendungen wieder uneingeschränkt gestartet werden.

An der Bewältigung des Vorfalls waren folgende Partner beteiligt:

Partner	Rolle
AKDB	Hauptpartner für Anwendungen und Verträge; Abstimmung und Cybersecurity
Telekom	Support der Cloud-Infrastruktur (Open Telekom Cloud / T Public Cloud) einschließlich des Standard-DDoS-Schutzes
Base IT roosi	Web Application Firewall Barracuda
MYRA Security	Zusätzlicher, vorgelagerter DDoS-Schutz
Base.IT	Unterstützung im Bereich Cybersecurity

Sind Ihre Daten sicher?

Nach aktuellem Stand wurden keine Daten entwendet oder manipuliert. Der Angriff richtete sich ausschließlich gegen die Verfügbarkeit der Systeme.

- **Getrennte Datenhaltung:** Ihre Daten liegen nicht in der öffentlich erreichbaren Web-Oberfläche, sondern in tiefer liegenden Schichten der Systemarchitektur. Sie sind durch Firewalls und restriktive Zugriffsregeln geschützt.
- **Kein Zugriff während des Angriffs:** Da Leitungen deaktiviert und Anwendungen gestoppt wurden, bestand während des Vorfalls kein Zugang zu Daten oder Anwendungen.
- **Georedundante Backups:** Aktuelle Sicherungen werden georedundant, also an räumlich getrennten Standorten und unabhängig von der angegriffenen Infrastruktur, vorgehalten.
- **SessionNet:** SessionNet ist kein eigenständiges System. Die dort angezeigten Daten werden ausschließlich aus dem Kernsystem der jeweiligen Verwaltung gespiegelt und liegen dort weiterhin vollständig vor. Ein gesondertes fachliches Backup ist daher nicht erforderlich.

Aktueller Stand und weiteres Vorgehen

Alle Anwendungen laufen seit dem 23. Oktober 2026 wieder stabil. Der zusätzliche, vorgelagerte DDoS-Schutz bleibt dauerhaft aktiv und stärkt die Widerstandsfähigkeit unserer Infrastruktur gegenüber künftigen Angriffen. Der Vorfall wurde umfassend dokumentiert und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldet.

Unser Notfallkonzept hat sich bewährt: Abstimmung, interne und externe Kommunikation sowie die Zusammenarbeit mit der AKDB und allen Partnern funktionierte reibungslos. Die gewonnenen Erkenntnisse fließen in die weitere Optimierung unserer Sicherheitsmaßnahmen ein.

Besonderen Dank an unsere Interne IT und die beteiligten Partner für die besonnene, professionelle Arbeitsweise in einem Sicherheitsvorfall.

Wir bedauern die entstandenen Einschränkungen und danken Ihnen für Ihr Verständnis und Ihre Geduld. Für Rückfragen stehen wir Ihnen jederzeit zur Verfügung.

Mit freundlichen Grüßen

A handwritten signature in blue ink, appearing to read 'Thomas Schweizer'.

Thomas Schweizer
Chief Operating Officer (COO)