

PHISHING-ANGRIFFE: ALLTÄGLICHE BEDROHUNG MIT HOHEN RISIKEN

12. Januar 2026 Erstellt von Danilo Gimbel, Datenschutzbeauftragter



Durch eine weitreichende Phishing-Kampagne wurde der Zugriff auf einzelne Microsoft-365-Konten des Paritätischen Sachsen kompromittiert. Dabei besteht das Risiko, dass personenbezogene Daten Unbefugten zugänglich wurden. Betroffene werden hiermit informiert und erhalten Hinweise zum Schutz ihrer Daten.

Im November 2025 kam es beim Paritätischen Sachsen zu einem Phishing-Angriff, bei dem missbräuchlich versendete E-Mails im Umlauf waren. Die Nachrichten enthielten präparierte Anhänge, die als legitime Sprachnachrichten getarnt waren. Auch Mitgliedsorganisationen sowie andere Organisationen und Personen im verbandlichen Netzwerk waren betroffen.

Durch das Öffnen solcher Anhänge konnten Angreifer Zugriffsdaten abgreifen und auf zwei unserer Microsoft 365-Konten zugreifen. Diese Konten wurden anschließend zum Versand weiterer Phishing-Mails an insgesamt rund 1000 Adressaten genutzt, darunter Mitarbeitende des Paritätischen Unternehmensverbundes, seiner Mitgliedsorganisationen und Dienstleister bzw. Kooperationspartner, von Einsatzstellen der Paritätischen Freiwilligendienste gGmbH sowie Freiwilligendienstleistende und vereinzelt auch Privatpersonen, die sich mit Informationsanfragen an den Paritätischen gewendet haben.

Welche Daten können betroffen sein?

Nach derzeitiger Analyse kann nicht ausgeschlossen werden, dass im Rahmen des Zugriffs auch personenbezogene Daten v.a. aus den E-Mail-Postfächern der kompromittierten Konten einsehbar waren. Betroffen sein könnten insbesondere:

- Stammdaten (z. B. Namen, Kontaktdaten, E-Mail-Adressen)
- Beschäftigtendaten und Mitgliedsdaten

- Finanz- und Abrechnungsdaten
- Korrespondenzen mit Mitgliedsorganisationen, Behörden und Partnern
- vereinzelt auch besonders schützenswerte Daten nach Art. 9 DSGVO (z. B. Gesundheits- oder Sozialdaten im Rahmen von Verwaltungs- oder Personalvorgängen)

Die Schätzung der mittelbar betroffenen Personen liegt zwischen rund 5000 und 8500, überwiegend Mitarbeitende sozialer Einrichtungen sowie Teilnehmende im Freiwilligendienst.

Ein tatsächlicher Datenabfluss konnte bislang nicht nachgewiesen werden. Aufgrund der Art des Angriffs ist ein solcher Zugriff jedoch nicht mit letzter Sicherheit auszuschließen.

Welche Maßnahmen wurden ergriffen?

Unmittelbar nach Bekanntwerden des Vorfalls wurden der illegitime E-Mail-Versand gestoppt und alle betroffenen Konten abgemeldet sowie Kennwörter organisationweit geändert. Darüber hinaus erfolgten:

- forensische Analysen durch den IT-Dienstleister des Paritätischen Sachsen,
- Meldung an die Datenschutzaufsichtsbehörde und Strafverfolgungsbehörden,
- Information an alle Empfänger der betrügerischen Nachrichten,
- Überprüfung und Anpassung der E-Mail-Sicherheitsrichtlinien,
- Vorbereitung der Einführung einer Zwei-Faktor-Authentifizierung und erweiterter Maßnahmen zum Zugriffsschutz und zur E-Mail-Sicherheit.

Nach Einschätzung des IT-Dienstleisters ist der Angriff eingedämmt und es liegen keine Hinweise auf fortlaufende Zugriffe oder Datenabflüsse vor.

Welche möglichen Folgen gibt es und welche Vorsichtsmaßnahmen werden empfohlen?

Für betroffene Personen kann ein Risiko bestehen, dass ihre Daten für weitere Phishing-Kampagnen, Erpressungsversuche oder Identitätsdiebstahl missbraucht werden.

Wir empfehlen Ihnen daher:

- Seien Sie besonders wachsam gegenüber unerwarteten E-Mails oder Anrufen,
- öffnen Sie keine verdächtigen Anhänge oder Links,
- nutzen Sie starke, einzigartige Passwörter und ändern diese regelmäßig,
- aktivieren Sie – falls möglich – eine Zwei-Faktor-Authentifizierung, zumindest für wichtige Konten,
- melden Sie verdächtige Nachrichten sofort an Ihre IT.

Kontakt

Bei Fragen bzw. für weitere Informationen zum Vorfall wenden Sie sich bitte zunächst an unseren Datenschutzbeauftragten:

Datenschutzbüro Gaß und Gimbel
Bernsdorfer Straße 10
01945 Ruhland

Tel.: 035752 - 940 790

Handy: 0175 - 515 10 18

Mail: [datenschutz\(at\)gassundgimbel.com](mailto:datenschutz(at)gassundgimbel.com)

Internet: www.gassundgimbel.com

Diese Information erfolgt gemäß Art. 34 Datenschutz-Grundverordnung (DSGVO). Die Veröffentlichung bleibt für mindestens vier Wochen online, um sicherzustellen, dass alle möglicherweise betroffenen Personen informiert werden.