Kasseler Verkehrs- und
Versorgungs-GmbH

Pressemitteilung

- **Unbekannte haben Internetseiten der KVV-Gruppe manipuliert**
- **Nutzerinnen und Nutzer sollten Schutz ihrer Computer prüfen**
- **Weitere Systeme der KVV-Gruppe sind nach aktuellem Kenntnisstand nicht betroffen**

Kassel, Am 23. September 2026 ist es zu einem IT-Sicherheitsvorfall auf mehreren Internetseiten der Kasseler Verkehrs- und Versorgungs-GmbH gekommen. Nach aktuellem Stand der internen Ermittlungen haben unbekannte Dritte am frühen Mittwochmorgen mehrere Seiten manipuliert und einen Schadcode eingebettet. Nach jetzigen Erkenntnissen sind die eigentlichen IT-Systeme der KVV-Gruppe nicht betroffen. Daher gibt es derzeit keine Hinweise darauf, dass Kundendaten durch den Schadcode betroffen sind.

Nach aktuellem Stand der Erkenntnisse wurde einem Teil der Besucherinnen und Besucher beim Aufruf einer der Internetseiten, unter anderem von kvvks.de, kvg.de, netzplusservice.de und den Seiten der Bäder, eine zusätzliche Aufforderung angezeigt. Wer dieser betrügerischen Aufforderung zur Installation, Aktivierung und Veränderung am Computer gefolgt ist, könnte unbeabsichtigt Schadsoftware auf sein Gerät geladen haben.

Der Schadcode wurde am Mittwochnachmittag erkannt, von den Internetseiten entfernt und vorsorglich wurden – wie für einen solchen Fall vorgesehen – die Internetseiten durch eine vorübergehende, reduzierte Präsenz mit den wichtigsten Kontaktdaten ersetzt.

Ob und wie viele Besucherinnen und Besucher der Webseiten im Laufe des Mittwochs von der Aufforderung betroffen waren und diese auch ausgeführt haben, ist unklar.

Gleichwohl nimmt die KVV-Gruppe diesen Vorfall sehr ernst und hat unverzüglich die Ermittlungsbehörden und das Bundesamt für die Sicherheit in der Informationstechnik über den Vorfall informiert. Zugleich wird der Vorfall an die Hessische Datenschutzaufsichtsbehörde gemeldet.

Mit Unterstützung externer Dienstleister unter anderem für IT-Forensik wird untersucht, wie genau die Internetseiten von mutmaßlichen Kriminellen manipuliert werden konnten.

Auch wenn die eigentlichen IT-Systeme der KVV nach aktuellem Kenntnisstand nicht betroffen sind, besteht jedoch die Möglichkeit, dass Endgeräte wie PCs oder Laptops der Besucherinnen und Besucher betroffen sein könnten. Die KVV-Gruppe hat sich

deshalb entschieden, frühzeitig und transparent die Öffentlichkeit über den Vorfall und mögliche Risiken für Betroffene zu informieren.

Allen Besucherinnen und Besuchern der Internetseiten gibt die KVV-Gruppe bereits jetzt und vorsorglich Hinweise zum Schutz vor den möglichen, noch unbekannten Folgen des Vorfalls:

- **Überprüfen Sie das Gerät mit einer aktuellen Sicherheitssoftware** (Antiviren- und Antibedrohungsschutz). Stellen Sie sicher, dass Betriebssystem, Browser und Virenschutz auf dem aktuellen Stand sind. Hierzu gibt das Bundesamt für Sicherheit (BSI) in der Informationstechnik gute Anleitungen: https://www.bsi.bund.de/dok/6596284
- Das Bundesamt für Sicherheit (BSI) empfiehlt in einem solchen Fall, **Passwörter zu ändern**, sollte das Risiko eines unbefugten Zugriffs oder eines installierten Schadcodes bestehen. Dazu zählen **insbesondere Passwörter von E-Mail-Konten, OnlineBanking, Online-Shops und anderen wichtigen Benutzerkonten**. Verwenden Sie hierfür möglichst ein anderes, nicht betroffenes Gerät und folgen Sie den amtlichen Empfehlungen des BSI: https://www.bsi.bund.de/dok/6701116
- **Nutzen Sie grundsätzlich sogenannte Zwei- oder Mehr-Faktor-Authentifizierungen** zum Schutz eventuell betroffener Zugangsdaten. Auch hierzu gibt es eine amtliche Empfehlung mit entsprechenden Erklärungen: https://www.bsi.bund.de/dok/509176
- **Sollten Sie anschließend ungewöhnliche Aktivitäten feststellen** – beispielsweise unbekannte Anmeldungen, Passwortänderungen oder auffällige Transaktionen – **wenden Sie sich unverzüglich an den jeweiligen Diensteanbieter bzw. bei Bank- oder Depotkonten an Ihr Kreditinstitut**.

Weitergehende Informationen zu dem Thema bietet das BSI auf seinem Informationsportal für Verbraucherinnen und Verbraucher:

https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Buergerinnen-und-Buerger/buergerinnen-und-buerger_node.html

Sobald es neue, wesentliche Erkenntnisse zum Vorfall gibt, wird die KVV-Gruppe unaufgefordert informieren.

(Stand 24.09.2026 12:00 Uhr)

Pressekontakt

Ute Orgir
Leiterin der Unternehmenskommunikation
KVV-Gruppe

Mobil +49 170 187 3234
presse@kvvks.de