wohnungsgenossenschaft neukölln eg

gegründet 1901

Berlin, 23.04.2026

Liebe Mitglieder, liebe Mieter,

sehr geehrte Damen und Herren,

wir möchten Sie hiermit informieren, dass es in der Wohnungsgenossenschaft Neukölln eG zu einem Datenschutzvorfall gekommen ist, der auch Daten betrifft, die wir im Rahmen der Genossenschaftstätigkeit zu Ihnen verarbeiten.

Was ist passiert?

Am 18.04.2026 haben unbekannte Täter unser IT-System durch eine Cyberattacke angegriffen. Dabei wurden Teile unserer Systeme (durch sogenannte „Ransomware“) verschlüsselt, um uns zu erpressen. Zusätzlich wurde gedroht Teile unseres Datenbestandes zu veröffentlichen.

Das bedeutet: Die Täter haben nicht nur unsere Daten auf den Systemen unzugänglich gemacht, sondern auch Teile davon kopiert – darunter auch Unterlagen zu unseren Mietgliedern und Geschäftspartnern.

Dies ist trotz bereits bestehender und umfassender Sicherheitsmechanismen wie z.B. Multi-Faktor-Authentifizierung, Berechtigungsstrukturen, Firewalls, Absicherung durch Dienstleister (Ausgelagert auf Spezialisten) etc. gelungen.

Unmittelbar nach dem Vorfall haben wir mit den zuständigen Cybercrime Spezialisten der Strafverfolgungsbehörden sowie externen IT-Sicherheitsspezialisten Kontakt aufgenommen, um unsere Daten wiederherzustellen, die Täter zu ermitteln, unsere IT-Sicherheit weiterzuentwickeln und uns vor einem erneuten Vorfall bestmöglich zu schützen.

Der Vorfall wurde sowohl dem LKA Berlin als auch der zuständigen Datenschutz-aufsichtsbehörde gemeldet. Aktuell wird daran gearbeitet die IT-Systeme wiederherzustellen und die Daten wieder verfügbar zu machen.

Welche Daten sind betroffen?

Nach aktuellem Stand betrifft der Vorfall insbesondere folgende Kategorien von Daten:

- Auf unseren Systemen verarbeitete Mieter-/Mitgliederdaten
- Unternehmens und Ansprechpartnerdaten unserer Geschäftspartner
- Vereinbarungen und Dokumente im Rahmen der Zusammenarbeit mit Geschäftspartnern

Welche Folgen könnte das haben?

Die entwendeten Daten könnten durch die Angreifer missbraucht werden. Mögliche Risiken sind unter anderem:

- Veröffentlichung im Internet (z. B. im „Darknet“), um Druck auf unser Unternehmen auszuüben.
- Phishing oder Betrugsversuche: Angreifer könnten die bekannten Kontaktdaten nutzen, um täuschend echt wirkende Nachrichten zu versenden, die vermeintlich von unserem Unternehmen oder von Ihnen stammen.
- Reputationsschäden: Durch die Veröffentlichung oder den Missbrauch unserer Daten könnte das Vertrauen in die Genossenschaft beschädigt werden.

Welche Maßnahmen haben wir ergriffen?

- Unmittelbar nach Bekanntwerden des Angriffs haben wir die betroffenen Systeme vom Netz genommen und externe IT-Sicherheits- und Forensikexperten hinzugezogen.
- Strafverfolgungsbehörden (Polizei/LKA Cybercrime) wurden eingeschaltet.
- Wir arbeiten intensiv daran, die betroffenen Systeme wiederherzustellen und unsere Sicherheitsmaßnahmen erneut zu verstärken.
- Wir haben den Vorfall an die zuständige Datenschutzaufsichtsbehörde gemeldet.

Was können Sie selbst tun?

- Seien Sie bitte besonders aufmerksam bei E-Mails oder Nachrichten, die ungewöhnlich erscheinen oder unaufgefordert personenbezogene Daten oder Zahlungen verlangen.
- Prüfen Sie sorgfältig den Absender und den Inhalt von Nachrichten, auch wenn diese auf den ersten Blick vertrauenswürdig wirken.
- Geben Sie keine vertraulichen Informationen preis, wenn Sie nicht sicher sind, dass die Kontaktaufnahme von einer echten und bekannten Person ausgeht.
- Auch wenn uns derzeit keine Hinweise auf den Diebstahl von Bankdaten vorliegen, überprüfen Sie bitte regelmäßig Ihre Kontoauszüge und achten Sie auf ungewöhnliche oder nicht autorisierte Buchungen.
- Sollten Sie Hinweise auf einen Missbrauch der betroffenen Daten feststellen, bitten wir um sofortige Mitteilung an uns.

Unsere Ansprechpartner für Sie

Für weitere Informationen oder bei Rückfragen steht Ihnen unser Krisenstab zur Verfügung:

krisenmanagement.gwn@gmx.de