Chur, 2. November 2026 – Das Medizinische Zentrum gleis d und die Medi Porta waren Ziel eines Cyberangriffs. Die elektronische Patientendokumentation, die in einer separaten Applikation geführt wird, war vom Angriff nicht betroffen. Tangiert waren Daten auf lokalen Speicherorten. Es wurden umgehend Massnahmen ergriffen, um die identifizierten Sicherheitslücken zu schliessen. Das Zentrum ist voll betriebsfähig und die medizinische Versorgung ist vollumfänglich gewährleistet.

Zusammen mit unserem IT-Partner und externen Cyberspezialisten konnte der Angriff gestoppt und die betroffenen Systeme gesichert werden. Die identifizierten Sicherheitslücken wurden umgehend geschlossen.

Der Angriff hatte keine Auswirkungen auf die Diagnose und die Behandlung von Patienten. Die elektronische Patientendokumentation, die in einer separaten Applikation geführt wird, war vom Angriff nicht betroffen.

Vom Cyberangriff betroffen waren lokale Datenspeicherorte. Ein Datenabfluss konnte trotz kurzer Reaktionszeit nicht vollständig verhindert werden. Nach aktuellem Stand sind Personendaten wie Namen, Adressen, Rezepte und Röntgenbilder abgeflossen. Betroffen sind auch Daten von unseren Mitarbeitenden. Wir stehen mit ihnen in direktem Kontakt.

Es laufen weitere Untersuchungen in enger Zusammenarbeit mit externen Cyberspezialisten. Zudem überprüft unser IT-Partner gemeinsam mit externen Cyberspezialisten aufgrund dieses Vorfalls, ob zusätzlich zu den getroffenen Massnahmen weitere Anpassungen an unseren IT-Sicherheitssystemen nötig sind.

Die Datensicherheit unserer Kunden, Mitarbeitenden, Lieferanten und Partner hat oberste Priorität. Wir bedauern diesen Vorfall ausserordentlich.

Der Vorfall wurde dem Bundesamt für Cybersicherheit (BACS) und dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemeldet sowie Strafanzeige erstattet.

Wir empfehlen folgende Vorsichtsmassnahmen:

- Vorsichtig sein bei ungewöhnlichen Anrufen oder Nachrichten.
- Keine Auskünfte zu persönlichen Daten geben, wenn sich eine Organisation als gleis d oder Medi Porta ausgibt. Gleis d und Medi Porta werden nie per E-Mail, SMS oder Telefon nach sensiblen Informationen wie Passwörtern, Bankdaten oder Zahlungen fragen.
- Rechnungen und Mahnungen sind zu prüfen. Wurde der Kauf getätigt, ist der Rechnungssteller bekannt und sind die Kontodaten korrekt?
- Grundsätzlich keine Passwörter oder Bankdaten preisgeben, wenn jemand danach fragt.
- Keine Rückrufe tätigen, auch wenn die Nummer der Bank, Handyanbieter etc. vertrauenswürdig ausschaut. Die Nummer kann gefälscht sein, um bei einem Rückruf an weitere Daten zu gelangen.
- Passwörter regelmässig ändern.

Welches Risiko besteht generell:

- Phishing: Kennen Kriminelle Name, Adresse oder Telefonnummer einer Person, können sie Betrugsnachrichten verfassen, die täuschend echt wirken.
- Identitätsdiebstahl: Mit den Daten können Kriminelle Profile auf fremden Namen erstellen oder beispielsweise Online-Bestellungen mit falscher Rechnungsadresse auslösen.

Kontakt für Rückfragen:
kontakt@mez-chur.ch und Telefon +41 81 287 70 90.