Pressemitteilung

Schwerin, 05.03.2026

Vorsicht – Falsche IT-Hilfe als Betrugsmasche!

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV), Sebastian Schmidt, warnt vor falschem IT-Support, dem sogenannten Tech-Support-Scam. Zuletzt kommt es vermehrt zu Sicherheitsvorfällen, bei denen sich Kriminelle durch diese Betrugsmasche Zugang zu den Daten von Privatpersonen, Unternehmen und öffentlichen Stellen im Land verschaffen.

Tech-Support-Scam erkennen

Bei diesem Vorgehen geben sich Kriminelle als Mitarbeitende von IT-Firmen bzw. bekannten Softwarefirmen oder als IT-Kundendienst aus und nehmen unaufgefordert Kontakt auf. Durch aufdringliche Anrufe, aber auch per E-Mail, SMS oder Warnmeldungen auf dem Computer beim Besuch bestimmter Webseiten sollen Unsicherheiten und Ängste bei den Nutzerinnen und Nutzern geschürt werden. Behauptet wird, dass ein vermeintlich schwerwiegendes Sicherheitsproblem oder eine IT-Schwachstelle, z. B. durch einen Virus- bzw. Cyberangriff, umgehend behoben werden müsse. Ziel sei laut LfDI MV in diesen Betrugsfällen jedoch der Zugriff auf die Geräte, um auf diesem Weg in den Besitz der Nutzerdaten zu gelangen oder Zugangsdaten auszuspähen.

„Es wird ganz gezielt versucht, Druck aufzubauen, um entsprechende Freigaben von den betroffenen Personen zu erhalten. Durch den Zugriff auf die Nutzerdaten können dann Nutzerkonten gesperrt werden, um Geld zu erpressen oder an sensible personenbezogene Daten zu gelangen“, fasst Sebastian Schmidt die Folgen zusammen und ruft zur Vorsicht auf. Seriöse IT-Unternehmen rufen nie unaufgefordert an und wenden sich bei Organisationen in der Regel unter Einhaltung der Verifikationsvorgaben direkt an die internen IT-Verantwortlichen. Zudem erfolgen die Support-Leistungen durch die tatsächlich beauftragten IT-Anbieter in den allermeisten Fällen unbemerkt im Hintergrund.

Was tun bei einem Betrugsversuch

Generell gilt, so Schmidt: „Bleiben Sie ruhig und geben Sie in keinem Fall Zugangsdaten, Passwörter, TANs oder persönliche Daten heraus. Installieren Sie auch keine Fernzugriffssoftware und erteilen Sie keine Freigaben durch das Klicken auf externe Links oder Anhänge. Beenden Sie etwaige Anrufe sofort, wenn Ihnen etwas komisch vorkommt.“ Privatpersonen und Organisationen sollten bei einem Betrugsversuch die Internetverbindung nach Möglichkeit sofort trennen, Passwörter ändern sowie einen Virenscan durchführen und in jedem Fall Anzeige bei der Polizei erstatten. Wurden darüber hinaus auch Zahlungsdaten herausgegeben, ist umgehend die zuständige Bank zu informieren. „Im privaten Bereich ist es besonders ratsam, auch Angehörige über diese Betrugsmasche oder etwaige Betrugsversuche zu informieren, um bestmöglichen Schutz der eigenen Daten zu gewährleisten“, so der LfDI MV abschließend.