Der Landesbeauftragte für
DATENSCHUTZ und
INFORMATIONSFREIHEIT
Mecklenburg-Vorpommern

PRESSEMITTEILUNG

Schwerin, den 08. August 2025

Achtung Phishing! Wenn Emails zur Falle werden.

Aktuell häufen sich Phishing-Kampagnen mit gefälschten E-Mails, bei denen gezielt gefälschte Bank- oder Providerseiten eingesetzt werden, um an persönliche Daten zu gelangen. Der Landesdatenschutzbeauftragte, Sebastian Schmidt, mahnt deshalb zur Vorsicht.

„Nach wie vor ist Phishing eine der größten digitalen Bedrohungen. Die Angriffsmethoden haben sich jedoch erheblich weiterentwickelt“, wie Schmidt in Schwerin erklärt. KI-generierte E-Mails, perfekt imitierte Stimmen in Sprachnachrichten oder täuschend echte Deepfakes machen es selbst Profis schwer, Betrugsversuche zu erkennen. Kombiniert mit ausgeklügeltem Social Engineering zielen diese Angriffe nicht nur auf technische Schwächen ab, sondern direkt darauf, menschliches Verhalten zu beeinflussen. Dabei wird etwa Neugier geweckt oder psychischer Druck aufgebaut. „Die Folgen für die Betroffenen können erheblich sein“, wie der Landesdatenschutzbeauftragte anfügt. Gelangten die Angreifer an personenbezogene Daten, könnten sie Identitätsdiebstahl begehen, finanzielle Schäden verursachen oder sensible Informationen veröffentlichen. Für Unternehmen und Behörden bedeutet ein erfolgreicher Phishingvorfall nicht nur ein Vertrauensverlust und finanzielle Schäden, sondern auch mögliche rechtliche Konsequenzen im Rahmen der Datenschutz-Grundverordnung (DSGVO).

„Institutionen benötigen deshalb Sensibilisierungen zum Thema Phishing, die über klassische Schulungen, wie Rundschreiben mit Hinweisen und Regeln oder einmalige jährliche Pflichtschulungen, hinausgehen“, erklärt Schmidt weiter. Es braucht kontinuierliche Awareness-Programme, in denen simulierte Phishing-Angriffe eingebettet sind. Das trainiere Erkennen und Abwehren von Phishing-Attacken und trägt dazu bei, das Risiko zu minimieren, Opfer von Angriffen zu werden. „Mit entsprechenden Sicherheitsmaßnahmen lässt sich die Wahrscheinlichkeit für Jedermann, Opfer einer Phishing-Attacke zu werden, deutlich reduzieren“, so Sebastian Schmidt weiter. Dazu zählt erstens, immer vorsichtig zu sein. Beim Erhalt von unerwarteten Nachrichten, vor allem dann, wenn zur Eingabe persönlicher Daten aufgefordert wird. Zweitens sollten enthaltene Links überprüft werden, indem etwa mit der Maus über den Link gefahren wird. Dadurch werde die tatsächliche Internetadresse angezeigt, die dann entsprechend verifiziert werden kann. Wer sich das nicht zutraut, kann die Internetadresse auch mit Link-Checker bzw. URL-Checker prüfen lassen. Gerade bei Bank-Links sollten lieber die verifizierten Links als Favoriten bzw. Lesezeichen im Browser angelegt und immer nur über diese die entsprechenden Seiten angesteuert werden.

„Sichere Authentifizierungsmethoden, wie etwa die Zwei-Faktor-Authentifizierung (2FA), sind ebenfalls ein wichtiger Schutz für Konten und Daten“, wie Schmidt abschließend erläutert. Diese sollten wann immer möglich eingerichtet werden. Diese Zwei-Faktor-Authentifizierung erfordert dabei neben dem Passwort einen zweiten, unabhängigen Identitätsnachweis, wie z.B. einen Code aus einer App, eine Push-Benachrichtigung oder einen biometrischen Scan. Mit diesen Maßnahmen kann man seinen Schutz bereits erheblich verbessern.

Kontakt

Telefon: 0385 59494-56
E-Mail: presse@datenschutz-mv.de