Vishing

Weitere Bezeichnungen: Voice Phishing, Telefon-Phishing, Sprach-Phishing

Rubrik: IT-Sicherheit

Vishing (Voice Phishing) ist eine Form des Phishings, bei der Betrüger Telefonanrufe oder Sprachnachrichten nutzen, um an vertrauliche Informationen zu gelangen oder ihre Opfer zu Zahlungen zu bewegen. Dabei geben sie sich beispielsweise als Bankmitarbeiter, Polizeibeamte oder Mitarbeiter des IT-Supports aus.

Eine zunehmende Gefahr stellt der Einsatz von künstlicher Intelligenz (KI) dar. Mithilfe von KI-generierten Stimmen und Voice Cloning können Angreifer Stimmen täuschend echt nachahmen. So kann ein Anruf scheinbar von einem Familienmitglied, Vorgesetzten oder einer anderen vertrauten Person stammen. Auch die angezeigte Telefonnummer kann manipuliert sein (Call-ID-Spoofing).

Ziel solcher Angriffe ist häufig die Herausgabe von Passwörtern, Zugangsdaten oder TANs, die Freigabe einer Überweisung oder die Installation schädlicher Software. Typisch sind erfundene Notfälle, Zeitdruck und die Aufforderung, sofort zu handeln.

Schutz vor Vishing: Bei verdächtigen Anrufen sollten keine vertraulichen Daten weitergegeben und keine Zahlungen freigegeben werden. Besonders wichtig ist es, die Identität des Anrufers über eine unabhängig überprüfte Telefonnummer zu bestätigen. Auch eine vertraut klingende Stimme ist heute kein zuverlässiger Identitätsnachweis mehr.

Weiterführende Informationen

Phishing, Smishing, Social Engineering, Voice Cloning, Deepfake, Künstliche Intelligenz, Call-ID-Spoofing, Identitätsdiebstahl, Telefonbetrug, TAN