27.08.2026

Die grösste Sicherheitslücke ist oft der Mensch

Cyberkriminelle setzen heute zunehmend auf psychologische Tricks, um an vertrauliche Informationen zu gelangen. Statt technische Schwachstellen auszunutzen, manipulieren sie gezielt Menschen durch gefälschte E-Mails, Anrufe oder Nachrichten.

Mit überzeugenden Geschichten und psychologischem Druck verleiten Internetbetrüger ihre Opfer dazu, Passwörter preiszugeben, schädliche Links anzuklicken oder sensible Daten weiterzugeben. Diese manipulative Angriffsform wird als Social Engineering bezeichnet.

Die Methoden werden dabei immer raffinierter. Dank künstlicher Intelligenz wirken Nachrichten und Anrufe authentischer denn je. Auch gefälschte Stimmen, Fotos, Videos und Identitäten kommen vermehrt zum Einsatz.

Sensibilisierung und ein gesundes Mass an Misstrauen sind entscheidend, um Social-Engineering-Angriffe frühzeitig zu erkennen und richtig darauf zu reagieren.

Möchten Sie mehr über aktuelle Angriffsmethoden und Schutzmassnahmen erfahren? Dann nehmen Sie an unserem Webinar «Social Engineering – Betrugsmaschen erkennen und sicher handeln» teil. Unsere Expertinnen und Experten zeigen Ihnen anhand praxisnaher Beispiele, wie Sie sich, Ihre Daten und Ihr Vermögen wirksam vor dreisten Betrugsversuchen schützen können:

- Dienstag, 20. Oktober 13:00 Uhr (https://events.teams.microsoft.com/event/1071392a-6e09-4c1a-bcea-13e520e64d77@75a34008-d7d1-4924-8e78-31fea86f6e68)
- Mittwoch, 21. Oktober 19:00 Uhr (https://events.teams.microsoft.com/event/545297b9-ae92-45bc-ac13-5238eaa06794@75a34008-d7d1-4924-8e78-31fea86f6e68)

Jetzt anmelden und Ihre Sicherheitskompetenz stärken!