Mittelstand-Digital Zentrum Leipzig-Halle

Bedrohung: Social Engineering

Inhalt: Bedeutung und Arten von Social Engineering, Schutz vor Social Engineering

Social Engineering…

… bezeichnet einen Cyberangriff, der psychologische Manipulation einsetzt, um Zugriff zu Daten oder Systemen zu erhalten

… nutzt menschliche Schwächen (Neugier, Vertrauen, Unsicherheit, Angst etc.) aus

Arten von Social Engineering

Phishing

gefälschte E-Mails oder Nachrichten von vertrauenswürdig wirkenden Absendern, die auf den Erhalt sensibler Daten oder die Implementierung von Schadsoftware abzielen

Bürosocial Engineering

persönliche Interaktionen oder Anrufe, in denen Angreifer sich als vertrauenswürdige und arbeitsrelevante Personen ausgeben, um an sensible Informationen zu gelangen

Technischer Support-Betrug

persönliche Interaktionen oder Anrufe, in denen sich Angreifer als technischen Support ausgeben und Unterstützung anbieten, um Zugang zu Systemen oder sensiblen Informationen zu bekommen

Social Media-Exploitation

personalisierte Angriffe (oft Spear Phishing-Angriffe), die Daten von öffentlich zugänglichen Social Media-Profilen nutzen, um vertrauenswürdig und authentisch zu erscheinen

Schutzmaßnahmen für KMU

- regelmäßige Schulungen und Sensibilisierung zur Identifizierung von Social Engineering
- Implementierung bzw. Beachtung von unternehmensinternen Sicherheitsrichtlinien und –verfahren zum Umgang mit vertraulichen Informationen und Zugängen zu Unternehmenssystemen
- Engagieren von bzw. Zusammenarbeit mit externen IT-Dienstleistern oder Sicherheitsexperten

Hinweis: Social Engineering nutzt gezielt menschliche Schwächen aus, weshalb die Implementierung von Sicherheitslösungen wie Firewalls oder Anti-Malware-Software nicht zum Schutz ausreicht. Wichtiger ist es, das Bewusstsein für diese Art von Cyberangriffen zu stärken.

Mittelstand-Digital

Web Based Training:

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages