Schutz vor Social Engineering

Sie entwickeln ein Bewusstsein für die Gefahren durch Social Engineering. Anhand zahlreicher Praxisbeispiele bekommen Sie Einblicke in die Strategien und Taktiken von Social Hackern.

Wie sicher sind meine Daten – und wie sicher ist mein Unternehmen?

Heutzutage kann der unbedachte Umgang mit sensiblen Informationen, vor allem in sozialen Netzwerken, Gefahren ungeahnten Ausmaßes für ein Unternehmen hervorrufen. Denn beim Social Engineering werden personenspezifische Informationen aus sozialen Netzwerken abgeleitet, in Relation gesetzt und schließlich dazu genutzt, um gezielt in unternehmenspezifische Prozessketten einzugreifen.

Im Bereich des CEO--Frauds war es Angreifern im Jahr 2016 gelungen, über 40 Millionen Euro auf ausländische Konten zu transferieren. Mitarbeiter eines Unternehmens wurden im Glauben gelassen, die gefälschten E--Mails – mit Transaktionsaufforderungen – seien von der Geschäftsführung.

Der Schutz vor Social Hackern erfordert vor allem Bewusstsein zu diesem Thema und das Wissen darüber, wie Angreifer vorgehen und welche Schwachstellen sie ausnutzen. Darüber hinaus trägt die überlegte Freigabe von Daten erheblich dazu bei, Sie persönlich als Nutzer oder als Verantwortlicher für Daten im Unternehmen vor Angriffen zu schützen.

Wie Sie mit Ihren Daten richtig umgehen, um Hackern nicht zum Opfer zu fallen, erfahren Sie in unserem eintägigen Seminar anhand von zahlreichen Praxisbeispielen.

Informationen	Inhalte	Nutzen
Voraussetzungen Problemloser Umgang mit dem PC, Verständnis für die IT-Grundprozesse **Dauer** 1 Tag Präsenz (9-17:00 Uhr) **Teilnehmerzahl** Max. 20 Personen **Veranstaltungsort** Mittweida, auch vor Ort im Unternehmen möglich **Kosten** 600 € pro Person **Experten** Prof. Dr. rer. nat. Dirk Labudde, Hochschule Mittweida Markus Straßburg, Fraunhofer Learnlab Martin Klöden, Fraunhofer Learnlab	**Session 1** Informationsgewinnung zur eigenen Person und Möglichkeiten zur Analyse **Session 2** Kommunikationsmodelle, Körpersprache und Persönlichkeitstest **Session 3** Social Engineering Beispiele und Warnzeichen für Social Engineering; aktuelle Bedrohungen und deren Erkennung werden aufgezeigt **Session 4** Maßnahmen zum Schutz vor Social Engineering; Wie unterscheide ich gefälschte von authentischen E-Mails? Wie identifiziere ich schädliche URLs?	**Sie werden lernen:** • die Gefahren von Social Engineering-Angriffen und Datendiebstahl leichter zu erkennen • durch welche Werkzeuge Human Hacker personenspezifische, sensible Daten aus sozialen Netzwerken ableiten • wie personenspezifische Daten genutzt werden können, um gezielt in unternehmensinterne Prozessketten einzugreifen • wie Sie Schutzmaßnahmen gegen Social Engineering-Angriffe einsetzen können

Zielgruppe

- Führungskräfte
- Selbstständige
- Öffentlich wirksame Personen