Fraunhofer
ACADEMY

SEMINAR

IHRE VORTEILE AUF EINEN BLICK

Nach dem Seminar können Sie …
… Social Engineering Angriffe abwehren.
… Angriffsvektoren analysieren und beurteilen.
… den Umgang mit Ihren Daten bewerten, um einem Social Hacking-Angriff vorzubeugen.

Dieses Seminar bietet Ihnen …
… eine Sensibilisierung für die Gefahren durch Social Engineering.
… zahlreiche Praxisbeispiele der Strategien und Taktiken von Social Hackern.
… Spielraum zur Selbstreflexion und Analyse eigener Schwachstellen.
… Vorschläge für eine sichere Daten- und Personalstruktur.

Melden Sie sich gleich an!
In Kooperation mit PAN-Seminare:
www.cybersicherheit.fraunhofer.de/cybercrime-vs-unternehmen

VIELEN DANK FÜR IHRE DATEN – CYBERCRIME VS. OFFENES UNTERNEHMEN

Gefahren erkennen – Schutzmaßnahmen ergreifen

Die Herausforderung: Angriff von Personen und Unternehmen durch Social Engineering

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.

Die Lösung: richtiger Datenumgang schützt vor Hackern

Der Schutz vor Social Hackern erfordert vor allem Awareness 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 IM ÜBERBLICK

Kurs: Vielen Dank für Ihre Daten
Voraussetzungen: Problemloser Umgang mit dem PC, Verständnis für die IT-Grundprozesse
Dauer: 1 Tag Präsenz (9–17 Uhr), auch als Inhouse-Schulung möglich
Kurssprache: Deutsch
Teilnehmerzahl: max. 10 Teilnehmer
Veranstaltungsort: Mittweida
Kosten: 690 €
Veranstaltet durch:

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

Die Inhalte

Digitale Informationsgewinnung

- Vorgehensweisen von Human Hackern
- Vorstellung von Human-Hacker-Werkzeugen: Welche Informationen zu Personen und Unternehmen lassen sich finden?
- Anwenden der vorgestellten Human-Hacker-Werkzeuge. Die Teilnehmenden versetzen sich in die Rolle eines Angreifers. Dieses Vorgehen schärft das Gefühl, für die Funktionsweise von Social Engineering.

Schutz vor Social Engineering

- Kommunikationsmodelle aus Sicht eines Social Engineers, Persönlichkeitstest
- Angriffsvektoren des Social Engineering. Hierbei werden aktuelle Bedrohungen und deren Erkennung aufgezeigt.
- Sie lernen unter anderem, wie Sie gefälschte von authentischen E-Mails unterscheiden und schädliche URLs identifizieren können.

Die Lernziele

- Sensibilisierung für die Gefahren von Social Engineering-Angriffen und Datendiebstahl für den einzelnen und ganze Unternehmen
- Kenntnisse über die Werkzeuge, mit denen Human Hacker personenspezifische sensible Daten aus sozialen Netzwerken ableiten
- Verstehen, wie diese personenspezifischen Daten genutzt werden können, um gezielt in unternehmensinterne Prozessketten einzugreifen
- Anwenden von Schutzmaßnahmen gegen Social Engineering-Angriffe

Die Zielgruppe

- öffentlich wirksame Personen
- Führungskräfte
- Selbstständige

UNSERE REFERENTEN

Prof. Dr. rer. nat. Dirk Labudde
Professor für Bioinformatik und Forensik mit Forschungsschwerpunkten in Algorithmen und Berechnungsmethoden in der (digitalen) Forensik und der strukturellen Bioinformatik.

Markus Straßburg und Martin Klöden
Wissenschaftliche Mitarbeiter der Hochschule Mittweida und im Fraunhofer Lernlabor Cybersicherheit.

Das Lernlabor Cybersicherheit: Weiterbildung für die IT-Sicherheitsexperten von morgen

Das Lernlabor Cybersicherheit ist eine Zusammenarbeit zwischen Fraunhofer und ausgewählten Fachhochschulen, um aktuelle Erkenntnisse auf dem Gebiet der Cybersicherheit in Weiterbildungsangebote für Unternehmen zu überführen. Fach- und Führungskräfte aus Industrie und öffentlicher Verwaltung erhalten an zahlreichen Standorten in Deutschland eine kompakte Qualifizierung in hochwertigen Laboren mit aktueller IT-Infrastruktur.

HABEN SIE NOCH FRAGEN ZU…

… Vielen Dank für Ihre Daten
Prof. Dr. rer. nat. Dirk Labudde
Hochschule Mittweida
Telefon +49 3727 58-1469
dirk.labudde@hs-mittweida.de

… Anmeldung, Organisation oder weiteren Angeboten?
Adem Salgin | Fraunhofer Academy
Telefon +49 89 1205-1555
cybersicherheit@fraunhofer.de