

Human Hacking

Die Kunst des Social Engineerings

Human Hacking

Definition und Bedeutung von Social Engineering

- **Denkfehler 1:** „IT-Security kostet, bringt aber nichts ein.“
- Tatsache: Kosten zur **Vermeidung von Schäden**
- **Denkfehler 2:** „Wir haben doch einen Virens Scanner.“
- Tatsache: Schlecht administrierte Tools **nützen nichts**
- **Denkfehler 3:** „Alle Systeme sind top. Problem gelöst.“
- Tatsache: **Mitarbeiter als Schwachstelle** und Ziel
- Social Engineering als Vorstufe zu „Tech-Hack“
- Ausnutzung menschlicher Eigenschaften

Human Hacking

Ausnutzung menschlicher Eigenschaften

- Unerfahrenheit / Naivität
- Gier / Rache
- Angst / Unsicherheit
- Geltungssucht / Mitteilungsbedürfnis
- Hilfsbereitschaft
- Gewohnheit
- Liebe / Zuneigung / Sexualität



Human Hacking

Absichten und Beispiele (nach BSI)

- **Grundprinzip:** Täuschung über Identität und Absicht
- Preisgabe vertraulicher Informationen
- Aushebeln von Sicherheitsfunktionen
- Installation von Schadsoftware auf Firmen-/Privatgerät
- (Spear) Phishing → Vorsicht bei Preisgabe von Daten
- CEO-Fraud → Klare Anweisungen, Skepsis
- BSI-GS: ORP.3 Sensibilisierung und Schulung

Quelle: https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/IT_Sicherheit_am_Arbeitsplatz/SoEng/Social_Engineering_node.html

Human Hacking

Phasen einer Awareness-Kampagne

- Erhebung Ist-Zustand
- Definition Soll-Zustand
- Rahmenbedingungen
- Unternehmenskultur
- Schwerpunkte
- Zielgruppendefinition
- Awareness-Konzept
- Schulungsplanung
- „Kick-off“-Maßnahmen

- Poster / Flyer
- Filme / Clips
- Broschüren
- Mousepads „10 Gebote“
- Live-Hackings
- Trainings / Workshops
- Online-Sensibilisierung
- (Werbe-)Geschenke
- Mitarbeiter des Monats

- Vergleich von Soll & Ist
- Befragung / Interviews
- Feedbacks
- Quizze / „Spielshows“
- Intranet-Zugriffe
- Punktzahl und Versuche
- SE-Pentesting / Phishing

PLANUNG

DURCHFÜHRUNG

MESSUNG

Iterativer Prozess, z.B. durch PDCA-Modell

Danke für Ihre Aufmerksamkeit!

<https://www.mb-informatik.com>

IT-Sicherheit, Training, Datenschutz, Blockchain

MARKUS
BENDER
INFORMATIK