IT-Sicherheit spielend lernen: Ein Lernspiel zu Social Engineering

Kristian Beckers Sebastian Pape

Technische Universität München
Goethe Universität Frankfurt

21. Juni 2016

ITSKRITIS

Agenda

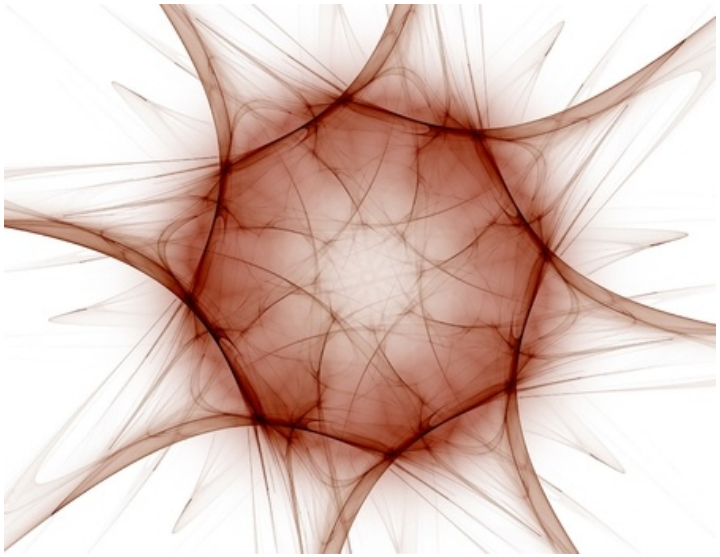
Definition

"Social engineering is the art of utilizing human behavior to breach security without the participant (or victim) even realizing that they have been manipulated. " (Gulati, 2003)

"Any act that influences a person to take an action that may or may not be in their best interest. " (Chris Hadnagy, 2016)

(cybertec-security.com, 2016)

Ablauf



- Informationen sammeln
- Szenario / Geschichte entwickeln
- Beziehung aufbauen
- Beziehung ausnutzen
- Ziel erreichen

Beispiele

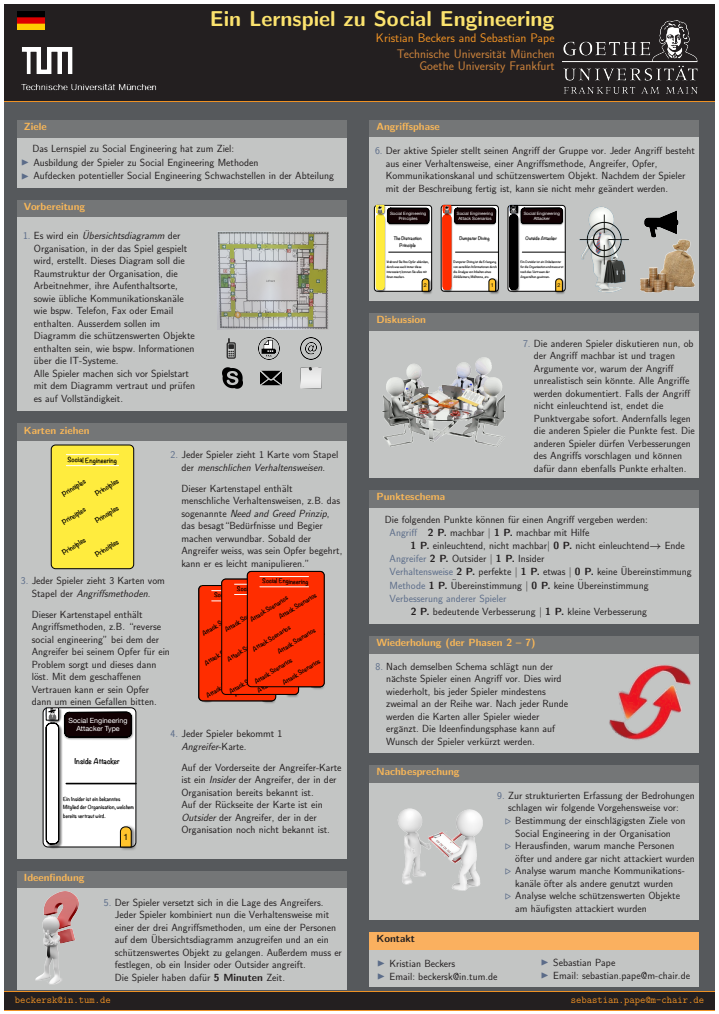
Betrugsmasche aufgewärmt: Falsche Microsoft-Techniker am Telefon

heise online 19.06.2015 18:16 Uhr

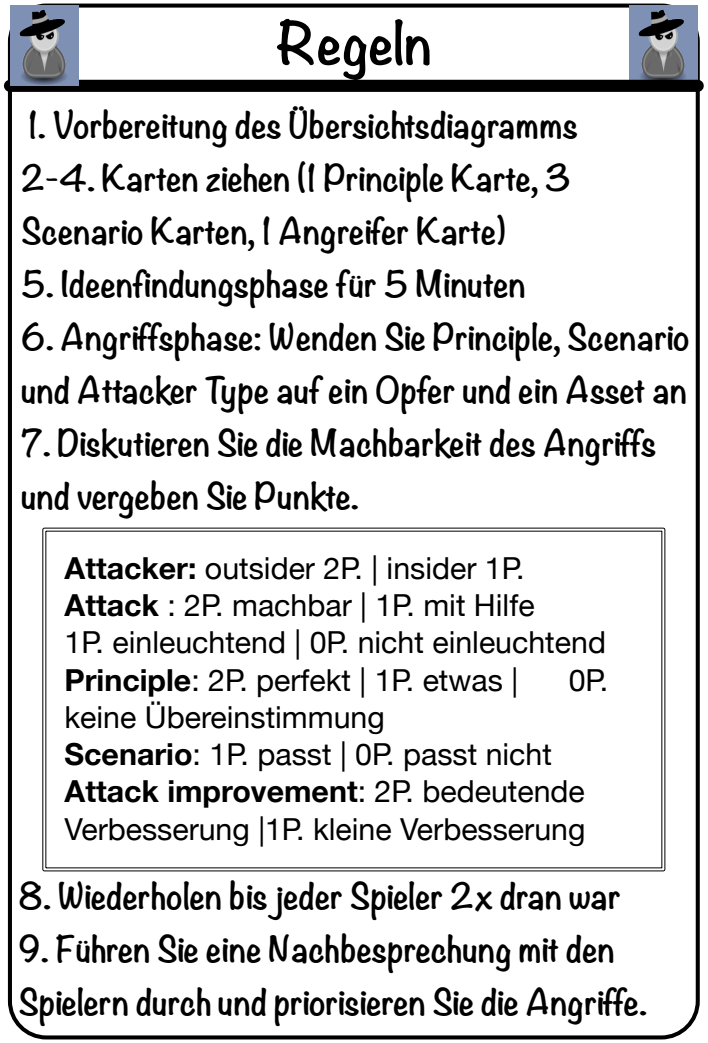
(Bild: dpa, Marc Müller/Symbolbild)

Idee: Serious Gaming

- Spielern Social Engineering Techniken vermitteln, Bewusstsein schärfen
- Mögliche Social Engineering Schwachstellen / Angriffe identifizieren

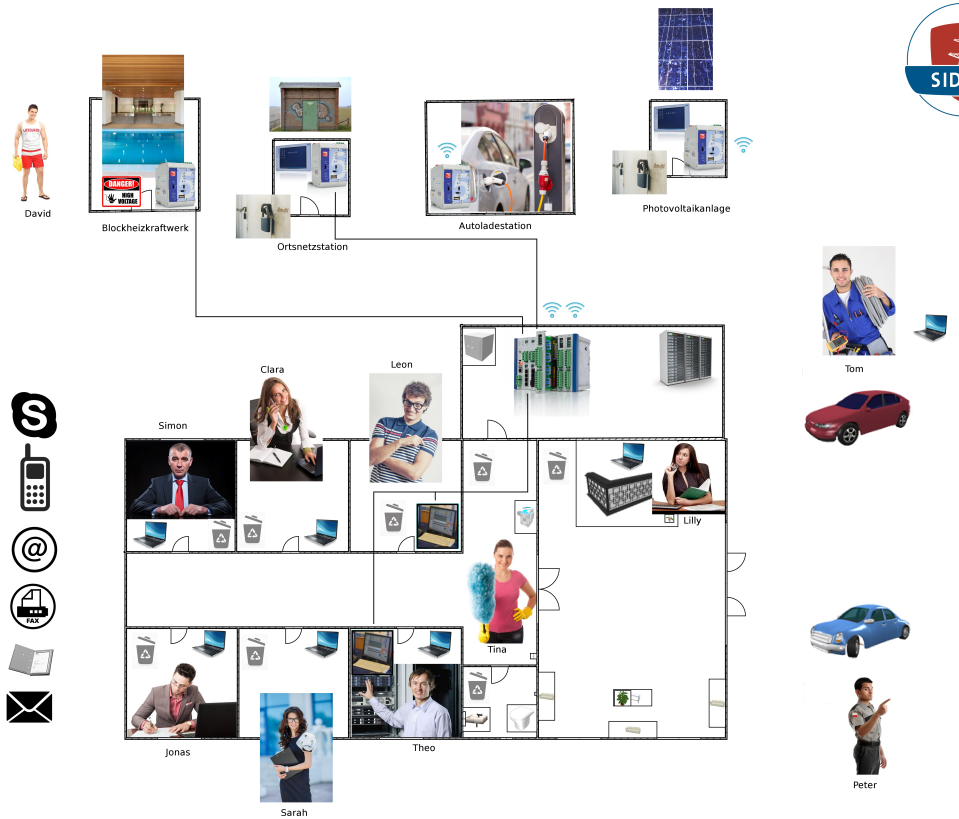


Regelübersicht

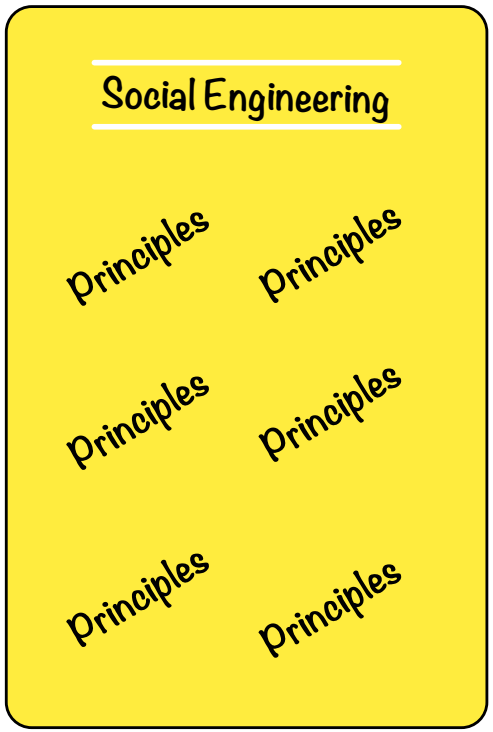


Vorbereitung

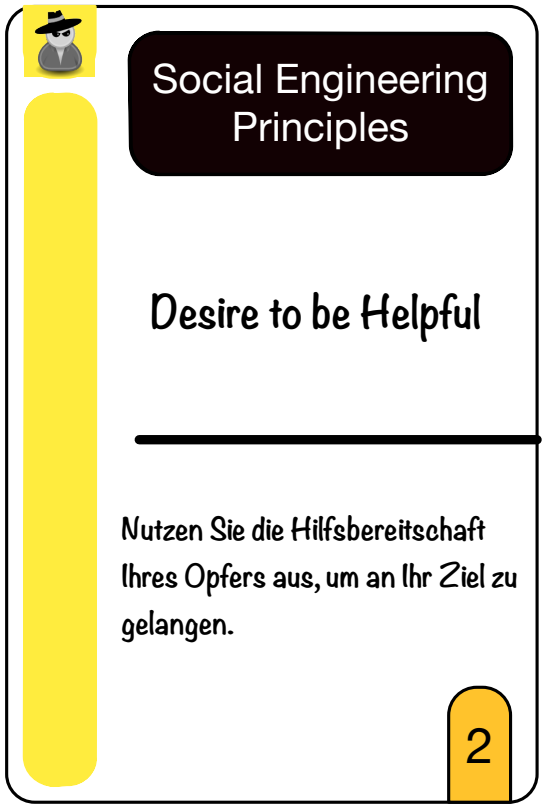
1. Übersichtsdiagramm
   - Raumstruktur der Organisation
   - Mitarbeiter und ihre Büros
   - Kommunikationskanäle
   - Schützenswerte Objekte



Karten ziehen (Verhaltensweisen)

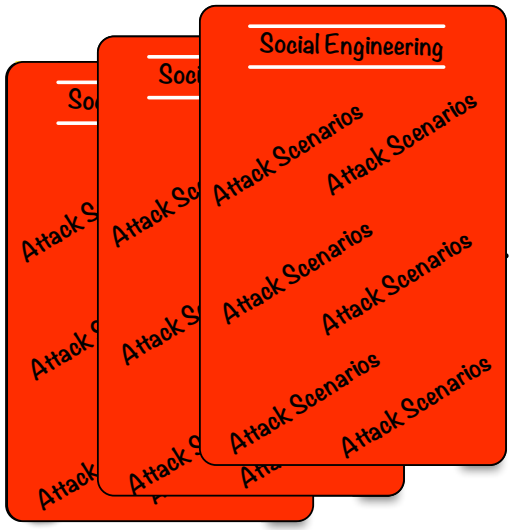


2 Jeder Spieler zieht 1 Karte vom Stapel der *menschlichen Verhaltensweisen*.
z.B.

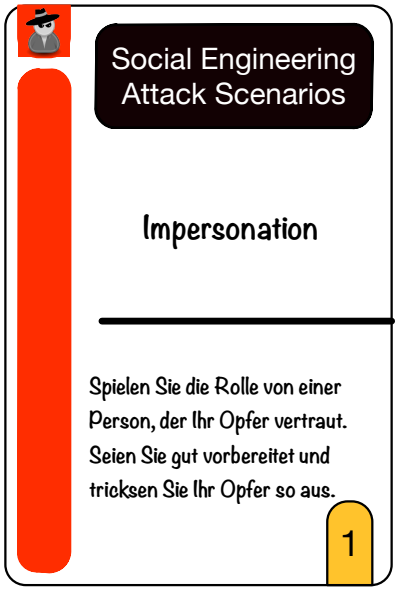


Karten ziehen (Angriffstechniken)

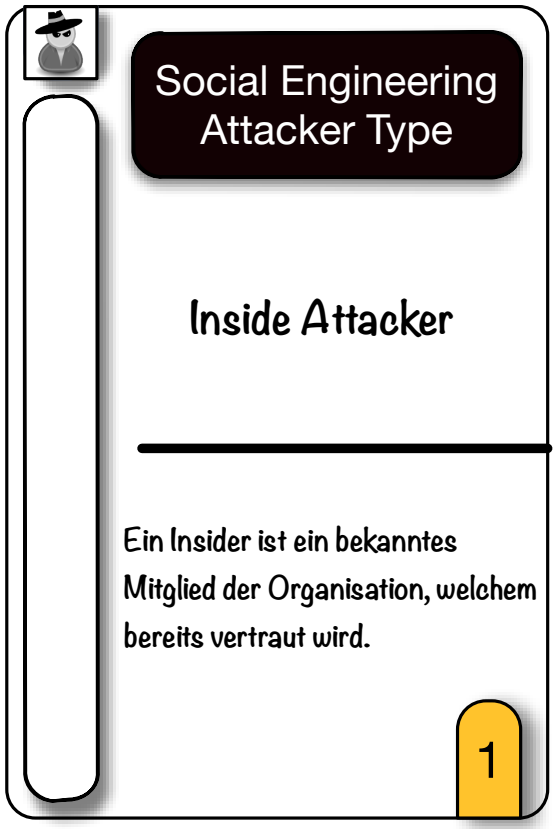
3 Jeder Spieler zieht 3 Karten vom Stapel der *Angriffsmethoden*.



3



Karten ziehen (Angreifer)



3 Jeder Spieler bekommt 1 *Angreifer*-Karte.

Ideenfindung

4. Der Spieler versetzt sich in die Lage des Angreifers.

   Kombination menschlicher Verhaltensweise mit einer der drei Angriffsmethoden

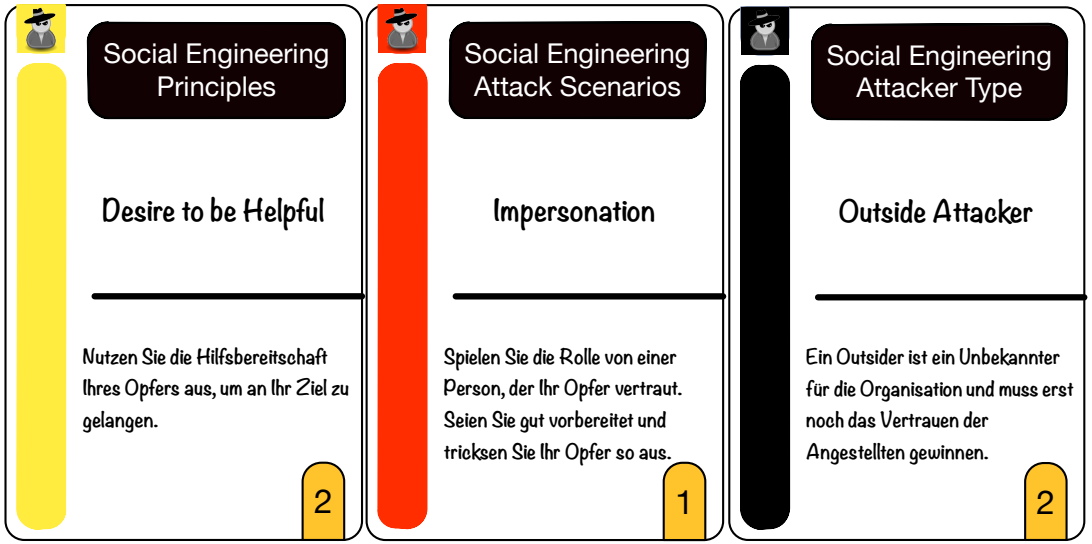
   Asset, Kommunikationskanal

   Opfer, Angreifer (Insider oder Outsider)

   Die Spieler haben dafür **5 Minuten** Zeit.

Angriffsphase

5 Der aktive Spieler stellt seinen Angriff der Gruppe vor.

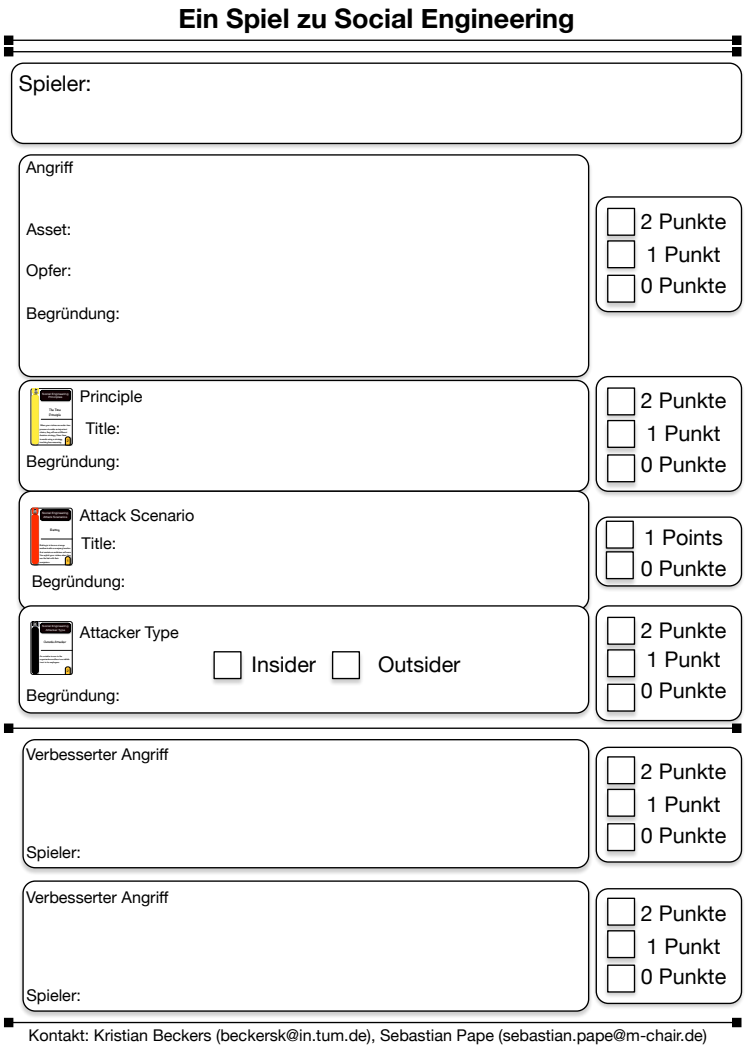


Diskussion

6

- Die anderen Spieler diskutieren nun, ob der Angriff machbar ist
- Alle Angriffe werden dokumentiert.
- Falls der Angriff nicht einleuchtend ist, endet die Punktvergabe sofort.
- Andernfalls legen die anderen Spieler die Punkte fest.
- Die anderen Spieler dürfen Verbesserungen des Angriffs vorschlagen und können dafür dann ebenfalls Punkte erhalten.

Dokumentation



Ein Spiel zu Social Engineering

Spieler:

Angriff

Asset:

Opfer:

Begründung:

☐ 2 Punkte
☐ 1 Punkt
☐ 0 Punkte

Principle

Title:

Begründung:

☐ 2 Punkte
☐ 1 Punkt
☐ 0 Punkte

Attack Scenario

Title:

Begründung:

☐ 1 Points
☐ 0 Punkte

Attacker Type

☐ Insider ☐ Outsider

Begründung:

☐ 2 Punkte
☐ 1 Punkt
☐ 0 Punkte

Verbesserter Angriff

Spieler:

☐ 2 Punkte
☐ 1 Punkt
☐ 0 Punkte

Verbesserter Angriff

Spieler:

☐ 2 Punkte
☐ 1 Punkt
☐ 0 Punkte

Kontakt: Kristian Beckers (beckersk@in.tum.de), Sebastian Pape (sebastian.pape@m-chair.de)

Wiederholung (der Phasen 2 – 7)

7. nächster Spieler
   Wiederholung bis jeder Spieler
   mindestens zweimal an der Reihe war.

Kontakt

Fragen, Anregungen, Feedback an:

- Kristian Beckers
- beckersk@in.tum.de
- Sebastian Pape
- sebastian.pape@m-chair.de

R. Gulati. The threat of social engineering and your defense against it. *SANS Reading Room*, 2003.