

# IT-Sicherheit spielend lernen: Ein Lernspiel zu Social Engineering

Kristian Beckers    Sebastian Pape

Technische Universität München  
Goethe Universität Frankfurt

21. Juni 2016

ITSKRITIS

# Agenda

- 1 Social Engineering
  - Definition
  - Funktionsweise
  - Beispiele
- 2 Das Spiel
  - Idee
  - Anleitung



# Definition

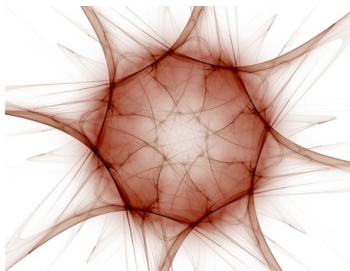
“Social engineering is the art of utilizing human behavior to breach security without the participant (or victim) even realizing that they have been manipulated. ” (Gulati, 2003)

“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



**Ein Lernspiel zu Social Engineering**  
Mitteil-Stunden 45 Minuten

Technische Universität München  
Goethe-Universität Frankfurt



---

**Ziele**

Das Lernspiel zu Social Engineering hat zwei Ziele:

- 1. Vermittlung der Spielern zu Social Engineering Methoden.
- 2. Aufklärung möglicher Social Engineering Schwachstellen in der Abteilung.

**Verständigung**

Es wird ein Übersichtsdiagramm der Organisation, in der das Spiel gespielt wird, erstellt. Dieses Diagramm soll die Hierarchie der Organisation, die Abteilungen, den Rollenstellungen, sowie alle Kommunikationskanäle wie Intranet, Telefon, Fax oder Email enthalten. Ressourcen sollen im Diagramm die verschiedenen Diagramme enthalten sein, wie Intranet, Informationen über das IT-System.

Alle Spieler machen sich vor Spielstart mit dem Diagramm vertraut und gehen es auf Vollständigkeit.

**Karten ziehen**

Jeder Spieler zieht 1 Karte vom Stapel der unentdeckten Verhörschritten.

Diese Kartenregel stellt menschliche Verhaltensweisen, z.B. die regelmäßige Mail und Google-Prüfung, das häufige Surfen und Blogs, mobiles Smartphone, Social Media, Angewandte, usw. dar. Diese Karten werden verwendet, um die Angriffe von den Spielern zu ziehen, um sie zu identifizieren.

Jeder Spieler zieht 1 Karte vom Stapel der Angriffskarten.

Diese Kartenregel stellt Angriffsmethoden, z.B. "Intranet social engineering" dar, die das Angewandte im selben Spiel für die Spieler zeigt und diesen dazu hilft. Mit dem geschlossenen Verhörschritt kann ein Spieler die Angriffe identifizieren.

Jeder Spieler bekommt 1 Angewandte-Karte.

Auf der Vorderseite der Angewandte-Karte ist ein Intranet der Angewandte, das in der Organisation benutzt ist. Auf der Rückseite der Karte ist ein Überblick der Angewandte, die in der Organisation noch nicht bekannt ist.

**Identifizierung**

Das Spiel versucht sich in die Lage der Angewandte, Jeder Spieler konzentriert sich die Verhaltensweisen mit denen die Angewandte, um eine der Personen auf dem Übersichtsdiagramm angeordnet wird als verschiedenen Diagramm zu identifizieren. Aufklärung muss es bestätigen, ob ein Intranet oder Intranet angeht. Die Spieler können 10 Minuten Zeit.

**Angriffskarten**

Die ersten Spieler stellen können Angriff die Gegner vor. Jeder Angriff besteht aus zwei Verhaltensweisen, einer Angewandte, Angewandte, Qualitätskontrollen und schützenden Diagramm. Nachdem der Spieler mit der Beschreibung fertig ist, kann es nicht mehr geändert werden.

**Überprüfen**

Die anderen Spieler diskutieren sich, ob die Angriff realistisch ist und Intranet Angewandte von, wenn die Angriff unentdeckt sein könnte. Alle Angriffe werden dokumentiert, falls der Angriff nicht identifiziert ist, endet die Prüfung ab. Identifiziert Intranet die anderen Spieler die Punkte hat. Die anderen Spieler dürfen Verhaltensweisen die Angriffe bestätigen und können dafür dann ebenfalls Punkte erhalten.

**Punkteberechnung**

Die folgende Punkte können für einen Angriff vergeben werden:

- Angewandte: 2 P, Intranet: 1 P, Intranet: 1 P.
- 1 P, Intranet, nicht Intranet: 0 P, nicht Intranet: -1 Ende
- Angewandte: 2 P, Intranet: 1 P, Intranet: 1 P.
- Verständigung: 2 P, Intranet: 1 P, Intranet: 1 P, keine Übersichtsdiagramm
- Verständigung: 1 P, Intranet: 1 P, Intranet: 1 P, keine Übersichtsdiagramm
- Verständigung: 1 P, Intranet: 1 P, Intranet: 1 P, keine Übersichtsdiagramm
- Verständigung: 1 P, Intranet: 1 P, Intranet: 1 P, keine Übersichtsdiagramm

**Wiederholung (für Phase 2 - 7)**

Nach dem ersten Teilzeit solligt sich mit dem anderen Spielern einen Angriff von, dies und wiederholt, bis jeder Spieler einen Intranet an der Seite war. Nach jeder Runde werden die Karten aller Spieler wieder gegeben. Die Identifizierung kann auf Wunsch die Spieler wiederholen.

**Wiederholung**


Zur vollständigen Erläuterung der Behinderungen, sollten sie folgende Verhaltensweisen vor:

- 1. Bestimmung der unentdeckten Ziele von Social Engineering in der Organisation.
- 2. Identifizieren, warum mehrere Personen (Intranet und andere) nicht identifiziert werden.
- 3. Analyse warum mehrere Kommunikationskanäle über die andere genutzt werden.
- 4. Analyse welche schützenden Diagramme am häufigsten identifiziert werden.


**Kontakt**

- 1. Klausur Beantworten
- 2. Email: kontakt@goe.de
- 3. Intranet: kontakt@goe.de
- 4. Intranet: kontakt@goe.de

# Regelübersicht



## Regeln



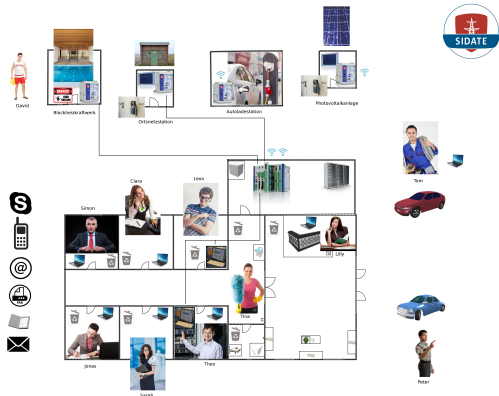
1. Vorbereitung des Übersichtsdiagramms
- 2-4. Karten ziehen (1 Principle Karte, 3 Scenario Karten, 1 Angreifer Karte)
5. Ideenfindungsphase für 5 Minuten
6. Angriffsphase: Wenden Sie Principle, Scenario und Attacker Type auf ein Opfer und ein Asset an
7. Diskutieren Sie die Machbarkeit des Angriffs und vergeben Sie Punkte.

**Attacker:** outsider 2P. | insider 1P.  
**Attack :** 2P. machbar | 1P. mit Hilfe  
1P. einleuchtend | 0P. nicht einleuchtend  
**Principle:** 2P. perfekt | 1P. etwas | 0P. keine Übereinstimmung  
**Scenario:** 1P. passt | 0P. passt nicht  
**Attack improvement:** 2P. bedeutende Verbesserung | 1P. kleine Verbesserung
8. Wiederholen bis jeder Spieler 2x dran war
9. Führen Sie eine Nachbesprechung mit den Spielern durch und priorisieren Sie die Angriffe.

# Vorbereitung

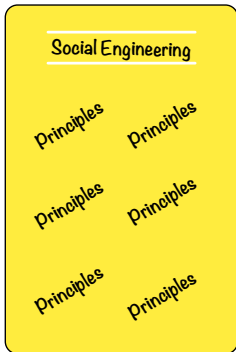
## 1 Übersichtsdiagramm

- Raumstruktur der Organisation
- Mitarbeiter und ihre Büros
- Kommunikationskanäle
- Schützenswerte Objekte

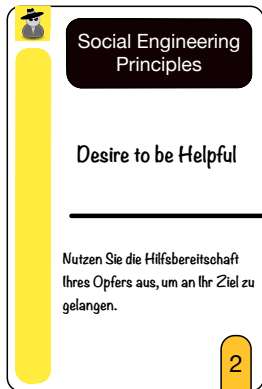




# Karten ziehen (Verhaltensweisen)

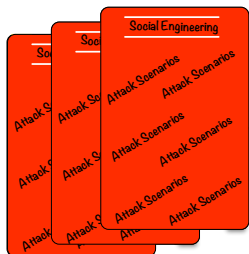


- 2 Jeder Spieler zieht 1 Karte vom Stapel der *menschlichen Verhaltensweisen*.  
z.B.



# Karten ziehen (Angriffstechniken)

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



3

**Social Engineering Attack Scenarios**

**Baiting**

Beim Baiting wird ein Speichermedium so präpariert, dass es bei der Benutzung den Rechner mit Malware infiziert. Platzieren Sie das Speichermedium an einer prominenten Stelle.

1

**Social Engineering Attack Scenarios**

**Tailgating**

Erfinden Sie einen Vorwand um hinter einem Mitarbeiter durch eine Tür zu treten. Erlangen Sie so physischen Zugang zu einem Sicherheitsbereich.

1

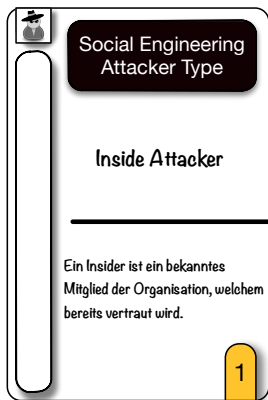
**Social Engineering Attack Scenarios**

**Impersonation**

Spielen Sie die Rolle von einer Person, der Ihr Opfer vertraut. Seien Sie gut vorbereitet und trickosen Sie Ihr Opfer so aus.

1

# 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.

 2	 <b>Social Engineering Principles</b>  Desire to be Helpful  Nutzen Sie die Hilfsbereitschaft Ihres Opfers aus, um an Ihr Ziel zu gelangen.
 1	 <b>Social Engineering Attack Scenarios</b>  Impersonation  Spielen Sie die Rolle von einer Person, der Ihr Opfer vertraut. Seien Sie gut vorbereitet und tricksen Sie Ihr Opfer so aus.
 2	 <b>Social Engineering Attacker Type</b>  Outside Attacker  Ein Outsider ist ein Unbekannter für die Organisation und muss erst noch das Vertrauen der Angestellten gewinnen.






# 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:	<input type="checkbox"/> 2 Punkte
Opfer:	<input type="checkbox"/> 1 Punkt
Begründung:	<input type="checkbox"/> 0 Punkte
 Principle	<input type="checkbox"/> 2 Punkte
Title:	<input type="checkbox"/> 1 Punkt
Begründung:	<input type="checkbox"/> 0 Punkte
 Attack Scenario	<input type="checkbox"/> 1 Points
Title:	<input type="checkbox"/> 0 Punkte
Begründung:	
 Attacker Type	<input type="checkbox"/> 2 Punkte
<input type="checkbox"/> Insider <input type="checkbox"/> Outsider	<input type="checkbox"/> 1 Punkt
Begründung:	<input type="checkbox"/> 0 Punkte
Verbesserter Angriff	
	<input type="checkbox"/> 2 Punkte
	<input type="checkbox"/> 1 Punkt
Spieler:	<input type="checkbox"/> 0 Punkte
Verbesserter Angriff	
	<input type="checkbox"/> 2 Punkte
	<input type="checkbox"/> 1 Punkt
Spieler:	<input type="checkbox"/> 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.