



Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften

Kapitel 4: Social Engineering – der Faktor Mensch in der IT-Sicherheit

1. Social Engineering — Begriffsbildung und -abgrenzung

2. Angreifer-Perspektive:

- Ausgewählte Beispiele für Social Engineering
- Kategorisierung und Arten von Social-Engineering-Angriffen

3. Anwender-Perspektive:

- Gegenmaßnahmen für Social-Engineering-Angriffe
- Durchführung von Social Engineering Penetration Tests
- Digitale Sorglosigkeit

Begriffsbildung und Abgrenzung

- Kapitel 3: (Technische) Angriffe auf technische Systeme, z.B. DDoS-Angriff via Botnet, Remote Exploit für Serverdienst

vs.

- Social Engineering (soziale Manipulation): Angriffe richten sich nicht direkt auf technische Systeme, sondern auf ihre Benutzer. Ziele sind z.B.
 - Informationsgewinnung (vs. Vertraulichkeit)
 - Benutzer führt vom Angreifer gewünschte Aktionen aus (vs. Integrität)
 - Betrug oder Abzocke (Geld verdienen)
- Angriffsarten ergänzen sich und können überlappen:
 - Per Massen-E-Mail verschickte Phishing-Versuche
 - Trojanische Pferde locken mit vordergründiger Nutzfunktionalität
 - Schockanrufe - moderner Enkeltrick

- Ausnutzung menschlicher Eigenschaften oder Gefühle, u.a.:
 - **Hilfsbereitschaft** (z.B. Tür aufhalten)
 - **Vertrauen** (z.B. Umgang mit Personen in bestimmten Funktionen)
 - **Angst** (z.B. Drohungen, körperliche Gewalt)
 - **Respekt vor Autorität** (z.B. Wirkung von Uniformen)
 - **Schutzbedürfnis** (z.B. gegenüber der Familie oder Freunden)
 - Neugierde, Faulheit, Überraschungseffekt, Scham, Schuldgefühl, Zorn, Stolz, Neid, Narzissmus, Mitleid, ...
- Jede menschliche Schwäche kann ausgenutzt werden.
- Social Engineering gibt es immer und überall:
 - Eltern, Erzieher, Lehrer, Freundeskreis, Chef und Kollegen, Partner, ...
 - Werbung, Autoverkäufer, gesellschaftliche Normen, ...
- Bei IT-Sicherheit wird oft primär an Technik gedacht, aber zu wenig an den “Faktor Mensch”.

1. Social Engineering — Begriffsbildung und -abgrenzung

2. Angreifer-Perspektive:

- Ausgewählte Beispiele für Social Engineering
- Kategorisierung und Arten von Social-Engineering-Angriffen

3. Anwender-Perspektive:

- Gegenmaßnahmen für Social-Engineering-Angriffe
- Durchführung von Social Engineering Penetration Tests
- Digitale Sorglosigkeit

Beispiele für Social Engineering (1)

Soziale Netzwerke

■ Robin Sage (2010)

- Social Media Profile bei Facebook, LinkedIn, Twitter, ...
- 25 Jahre, Master-Abschluss vom MIT
- IT-Sicherheitsberaterin mit 10 Jahren Berufserfahrung

- Kontaktaufnahme mit 300 Personen:
Andere IT-Sicherheitsexperten, Mitarbeiter von
Rüstungsfirmen und Behörden, hochrangige Offiziere, ...
- Job-Angebote u.a. von Google und Lockheed Martin
- Diverse Aufträge mit Zugang zu vertraulichen Dokumenten, Informationen über Bankkonten, Truppenstandorte,
...
- Diverse Einladungen zum Abendessen ;-)

- Alles ein Fake:
Experiment von Thomas Ryan zur Vertrauensseligkeit in Social Networks
- Operation „Robin Sage“ ist eine vierwöchige Übung für US-Spezialeinheiten („unconventional warfare exercise“).



Foto: ThePOC.net

Beispiele für Social Engineering (2)

Kompromittierte US-Behörde

■ Elektronische Geburtstagsgrußkarte

- Zwei Angestellte erwähnen Geburtstag ihres Chefs auf Facebook.
- Angreifer schickt E-Grußkarte im Namen eines der beiden.
- Link in E-Mail verweist auf Malware; Rechner vollständig kompromittiert.

■ Emily Williams:

- 28 Jahre alt, MIT-Abschluss, 10 Jahre Berufserfahrung
- Eigentlich Kellnerin eines Restaurants in Behördennähe
- Innerhalb von 24h nach Anlegen des Facebook-Profil:
 - 60 Facebook-Freunde
 - 55 LinkedIn-Bekannte
 - Drei Job-Angebote von anderen Firmen
- Emily bewirbt sich bei der Behörde:
 - Wird eingestellt, neue Kollegen helfen ihr mit Berechtigungen
 - Social Media Seiten ergänzt um Link auf Malware-Weihnachtskarte
 - Java-Exploit kompromittiert diverse Clients



Bildquelle / Details: <http://nakedsecurity.sophos.com/2013/11/03/fake-femme-fatale-dupes-it-guys-at-us-government-agency/>

Emily Williams und die kompromittierte US-Behörde

- War “nur” ein bezahlter Penetration-Test:
 - Durchgeführt von Fa. World Wide Technology
 - Abgestimmt mit der Behördenleitung
- Fazit des Testleiters:
 - “[Attractive women can open locked doors in the male-dominated IT industry.](#)” - Paralleltest mit männlichem Fake-Profil war erfolglos.
 - “[People are trusting and want to help others. Unfortunately, \[...\] employees don't always think that they could be targets for social engineering because they're not important enough in the organization. They're often unaware of how a simple action like friending somebody on Facebook, for example, could help attackers establish credibility.](#)”

Quelle: <http://nakedsecurity.sophos.com/2013/11/03/fake-femme-fatale-dupes-it-guys-at-us-government-agency/>

Beispiele für Social Engineering (3)

- USB-Sticks für Bankangestellte
 - Bank beauftragt Security Assessment inkl. Social Engineering
 - Bankangestellte wissen, dass auch der Faktor Mensch getestet wird
 - 20 USB-Sticks mit Malware auf Parkplatz, Weg zur Kantine, etc. „verloren“
 - 15 USB-Sticks werden gefunden, alle 15 werden am Arbeitsplatz ausprobiert
- Kevin Mitnick (Buch: The Art of Deception; Biographie: Ghost in the Wires)
 - Ehemals meistgesuchter Social Engineer der USA
 - „Lieblingswaffe“ Telefon; gibt sich z.B. oft als ranghoher Polizist aus
 - Hacking als Sport:
 - Keine monetäre Motivation; arbeitet nebenher (meist) unauffällig.
 - Kopiert sich interne Dokumente, E-Mails, Sourcecode, ... just for fun
 - Teamwork und Hackerkriege:
 - Mitnick griff oft auf Exploits und Tools befreundeter Hacker zurück
 - Rivalitäten und falsche Freunde führen letztlich zu seiner Verhaftung

Beispiele für Social Engineering (4)

Baiting mit Geschenken (10/2013)

The Telegraph

Search - enhanced by Google

Friday 08 November 2013

Home News World Sport Finance Comment Culture Travel Life Women Fashion Luxury Tech

Dating Offers Jobs

USA Asia China Europe Middle East Australasia Africa Nelson Mandela South America Central Asia

France | Francois Hollande | Germany | Angela Merkel | **Russia** | Vladimir Putin | Greece | Spain | Italy

HOME » NEWS » WORLD NEWS » EUROPE » RUSSIA

Russia 'spied on G20 leaders with USB sticks'

Russia used complimentary 'Trojan horse' pen drives to spy on delegates at G20 summit, it has been reported

By Nick Squires, Rome, Bruno Waterfield in Brussels and Peter Dominiczak
12:13PM GMT 29 Oct 2013

 Russia spied on foreign powers at last month's G20 summit by giving delegations USB pen drives capable of downloading sensitive information from laptops, it was claimed today.

The devices were given to foreign delegates, including heads of state, at the summit near St Petersburg, according to reports in two Italian newspapers, *La Stampa* and *Corriere della Sera*.

Downing Street said David Cameron was not given one of the USB sticks said to have contained a Trojan horse programme, but did not rule out the possibility that officials in the British delegation had received them.

The Prime Minister's official spokesman said: "My understanding is that the Prime Minister didn't receive a USB drive because I think they were a gift for delegates, not for leaders."

Asked if Downing Street staff were given the USBs, he said: "I believe they were part of the gifts for delegates."

More From The Web

Delegations also received mobile phone recharging devices which were also reportedly capable of secretly tapping into emails, text messages and telephone calls.

The latest claims of international espionage come on the heels of allegations that the United States' National Security Agency spied on friendly European powers, including Germany, France, Spain and Italy, by covertly monitoring tens of millions of telephone calls.

The alleged attempts by Moscow to access secret information from foreign powers at the G20 came at a time of high tension between the US and Russia, in particular over Syria and the Russian granting of asylum to former NSA systems analyst Edward Snowden.

Suspicions were first raised about the Russian spying campaign by Herman Van Rompuy, the President of the European Council, according to *Corriere della Sera*, which carried the story on its front page.

He ordered the USB pen drives and other devices received by the delegates in St Petersburg to be analysed by intelligence experts in Brussels, as well as Germany's secret service.

1. Social Engineering — Begriffsbildung und -abgrenzung

2. Angreifer-Perspektive:

- Ausgewählte Beispiele für Social Engineering
- Kategorisierung und Arten von Social-Engineering-Angriffen

3. Anwender-Perspektive:

- Gegenmaßnahmen für Social-Engineering-Angriffe
- Durchführung von Social Engineering Penetration Tests
- Digitale Sorglosigkeit

■ Grundlegend zu unterscheiden:

- Passive Angriffe** (keine Interaktion mit dem Opfer), u.a.
 - Belauschen von Gesprächen
 - Beim Tippen „über die Schulter schauen“ (**shoulder surfing**)
 - Durchsuchen von Papiertonnen (**dumpster diving**)
 - Liegenlassen präparierter USB-Sticks (**baiting**)
- Aktive Angriffe**, u.a.
 - Am Telefon als Mitarbeiter der IT-Abteilung oder guter Bekannter/Assistent des Chefs ausgeben (**pretexting**)
 - Kontaktaufnahme per E-Mail (**phishing**)
 - Internet-Bekanntschaften, z.B. über fingiertes Facebook-Konto

■ Etablierte Kategorien:

- Human-based Social Engineering** (ohne technische Hilfsmittel)
- Computer-based Social Engineering** (mit technischen Hilfsmitteln)
- [Reverse Social Engineering]** (Opfer wendet sich freiwillig an Angreifer)

Kategorie Human-based Social Engineering

- **Dumpster Diving**
 - Klausurentwürfe in der Papiertonne?
- **Shoulder Surfing**
 - Notebook-Nutzung im Hörsaal?
- **Tailgating**
 - PIN-Code gesicherte Türen
- **Badge Surveillance**
 - Selbstgedruckte Mitarbeiterausweise?
- **Pretexting**
- **Quid pro quo**
 - Schokolade für Hausaufgabenblätter?
- **People Watching**
- **Diversion Theft**

Kategorie Computer-based Social Engineering

■ Phishing

- Clone phishing (“Update” echter E-Mails)
- Spear phishing (personalisiertes Phishing)
- Whaling (Phishing z.B. gegen hochrangigen Mitarbeiter)
- CEO Fraud (Manipulation zur Überweisung von Geld)
- Vishing (Voice Phishing; Ziel: Opfer ruft Angreifer an)
- Evil Twins (rogue WiFi access points)

■ Baiting

- Im Hörsaal verlorener USB-Stick?

■ Forensic analysis (“Dumpster diving” für Elektronik)

■ Electronic badges (Duplizieren elektronischer Schlüssel)

Typische Eigenschaften von erfolgreichen Social Engineers

■ Können gut mit Menschen kommunizieren

- Harmlose Unterhaltung - Angriff wird gar nicht bemerkt
- Vortäuschen diverser Stimmungslagen (hektisch, ärgerlich, traurig, ...)
- Fachjargon des Opfers und seiner Umgebung wird beherrscht
- Glaubliche Vertrauensgewinnung oder Positionierung als Autorität

■ Sind geduldige Schauspieler

- Vorgespielte Person muss authentisch wirken:
 - Junge Menschen gehen selten als CEOs von Großkonzernen durch.
 - Wer behauptet, in München geboren zu sein oder studiert zu haben, sollte bayerisch verstehen/sprechen oder Uni-Alltag beschreiben können.
- Auskundschaften und Vertrauen aufbauen kann dauern.
- Flexibilität und Anpassungsfähigkeit, gutes Faktengedächtnis.

■ Sind sich nicht zu gut

- Dumpster Diving macht nicht unbedingt Spaß.
- Tarnung als Reinigungspersonal impliziert entsprechende Tätigkeit. ;-)

1. Social Engineering — Begriffsbildung und -abgrenzung

2. Angreifer-Perspektive:

- Ausgewählte Beispiele für Social Engineering
- Kategorisierung und Arten von Social-Engineering-Angriffen

3. Anwender-Perspektive:

- Gegenmaßnahmen für Social-Engineering-Angriffe
- Durchführung von Social Engineering Penetration Tests
- Digitale Sorglosigkeit

Typische Merkmale in der „Story“ von SE-Angriffen

- Gefühl der Dringlichkeit erzeugen
- Stress erzeugen
- Drohen mit negativen Konsequenzen
- Fragen nach Bypass-Verfahren bzw. Ausnahmen
- Viele/Hohe Berechtigungen erbitten
- Sehr neugieriges Nachfragen
- Unnötig viel Fachjargon verwenden
- Schwammige Angaben machen
- „Zu gut um wahr zu sein“
- Der Ton ist ungewöhnlich



Skeptisch werden!

■ Pretexting - Sich für jemand anderen ausgeben

- Am Telefon als Mitarbeiter der IT-Abteilung oder guter Bekannter/Assistent des Chefs ausgeben
- Anruf der Polizei
- Pressevertreter
- Enkeltrick / Schockanrufe

⇒ Gesundes Maß an Misstrauen und Vorsicht

⇒ Gespräch beenden und zurückrufen oder Kanal wechseln

⇒ Bei Zweifeln Kollegen zu Rate ziehen

- **Kanal wechseln**
- **Raus aus dem Gespräch**
- Sie rufen zurück!
- Anruf, Message, Chat bei Familienangehörigen
- Mit jemandem darüber sprechen
- Polizei verständigen

- Wenn Sie **zwei oder mehr Fragen** mit „JA“ beantworten,
wählen Sie 110
 - Wurden Sie angerufen?
 - Soll heute noch Geld oder Wertsachen übergeben werden?
 - Wurden Sie zu Stillschweigen aufgefordert?
 - Hat sich der Anrufer als Familienangehöriger, Polizist, Arzt, Notar oder Richter ausgegeben?
 - Sollen Sie Geld an eine Ihnen unbekannte Person übergeben?
 - Sollen Sie etwas überweisen oder Geldwertkarten kaufen?

Gegenmaßnahmen

- Gutes Social Engineering funktioniert immer. ;-)
- Beispielmaßnahmen:

Technisch:

- Dumpster Diving**: Aktenvernichtung / Papiertonnen abschließen
- Shoulder Surfing**: Sichtschutzfolien für Notebook-Displays
- Tailgating**: Wachdienst, Vereinzelungsanlagen, Tür vor der Nase schließen
- Baiting**: Systeme einschränken, z.B. USB-Ports deaktivieren

Organisatorisch:

- Sensibilisieren** durch Schulungen, Plakate, Übungen, ...
- Klare Anweisungen** z.B. zu Auskünften am Telefon
- Meldepflicht** für verdächtige Vorkommnisse inkl. Tests

Beispiele

Awareness-Poster



www.mita.gov.mt/securityaware

Quelle: Malta Information Technology Agency



Quelle: ENISA

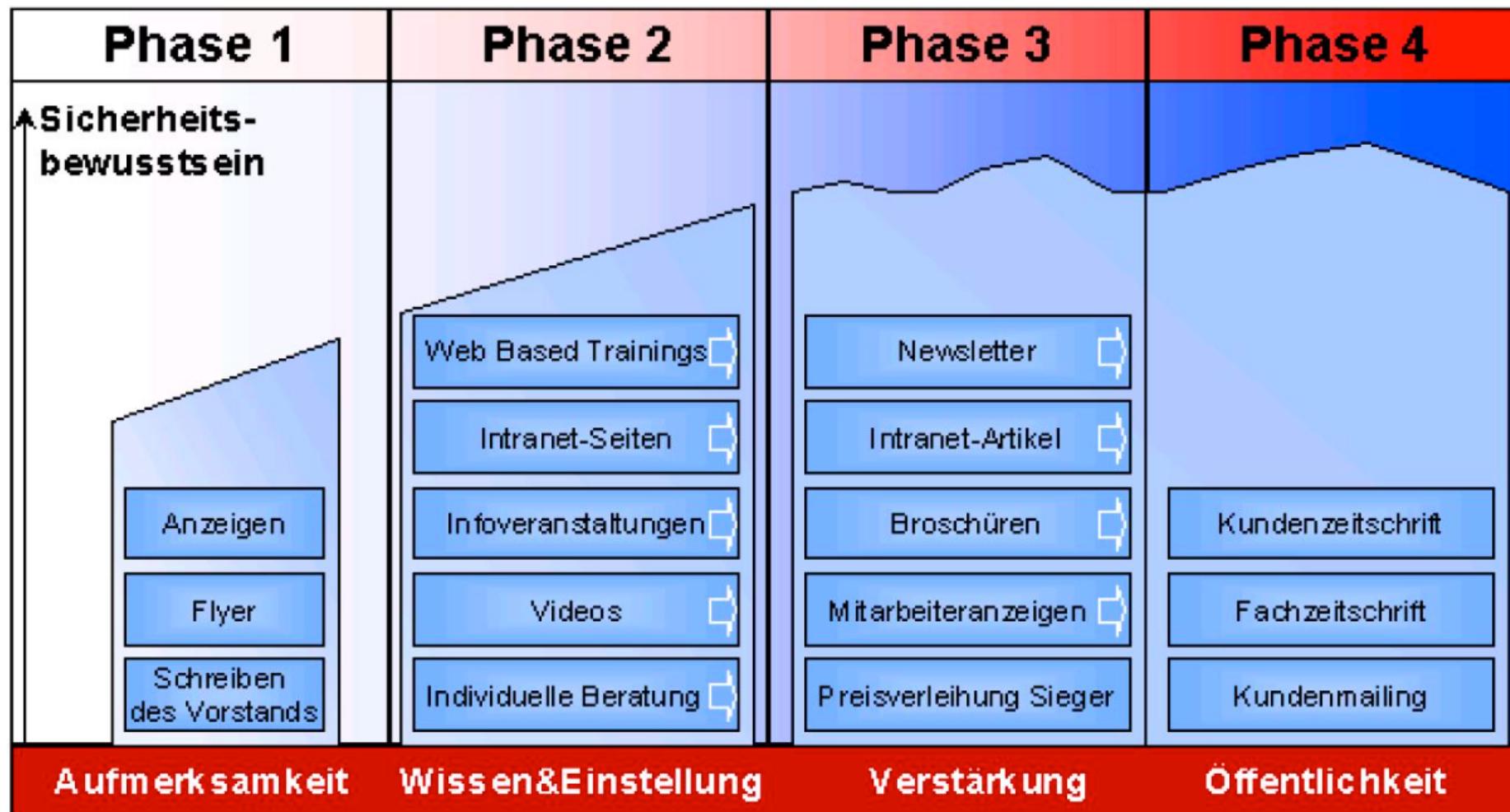
- Wie alles rund um IT-Sicherheit auch eine Budgetfrage:
 - Personal- und Zeitbedarf für Schulungen
 - Awareness verhindert Schaden, erwirtschaftet aber keinen Gewinn
- Organisatorische Randbedingungen:
 - Schutzziele und Schulungsprioritäten müssen definiert sein
 - Inhaltliche, didaktische und mediale Aufbereitung erfordern ein interdisziplinäres Team
 - Kontinuität und Erfolgskontrolle
- Kombination verschiedener Ansätze:
 - Präsenzveranstaltungen vs. Computer-based Training
 - Poster, Flyer, Newsletter, Intranet-Webseiten, ...
 - Bestätigte Kenntnisnahme, Teilnahmezertifikate, Gewinnspiele, ...

- **Slow down!**
- Halte Dich an die Verfahren.
Vermeide Shortcuts & Ausnahmen!
- Erkenne ungewöhnliche oder unangemessene Anfragen!
- Protokolliere und melde verdächtige Vorgänge
- Üben, üben, üben!
→ Rollenspiele, Szenariotrainings, Feedback, ...

Es ist völlig in Ordnung, (im Moment) Unberechtigten
den Zutritt zum RG zu verwehren!



Vier-Phasen-Modell nach Fox/Kaun



Quelle: Dirk Fox, Sven Kaun: Security-Awareness-Kampagnen; 9. IT-Sicherheitskongress des BSI, 2005

1. Social Engineering — Begriffsbildung und -abgrenzung
2. Angreifer-Perspektive:
 - Ausgewählte Beispiele für Social Engineering
 - Kategorisierung und Arten von Social-Engineering-Angriffen
3. Anwender-Perspektive:
 - Gegenmaßnahmen für Social-Engineering-Angriffe
 - Durchführung von Social Engineering Penetration Tests
 - Digitale Sorglosigkeit

■ **Pentests (allgemein)** als Dienstleistung:

- **Ziel:** White-Hat Hacker identifizieren und melden bis dato unbekannte Sicherheitslücken, bevor böswillige Angreifer erfolgreich sind.
- Untersuchung beziehen sich auf **Organisationsspezifika**, z.B.:
 - Eigenentwickelte / dedizierte Software
 - Zusammenstellung / Konfigurationen von IT-Diensten
 - Physische Sicherheit
- Je nach bereitgestellten Unterlagen (z.B. Quelltexte):
Blackbox- vs. Whitebox-Test

■ **Social Engineering Pentests** als Aufträge an Externe:

- Know-How und Routine oft nicht organisationsintern vorhanden.
- “Neue Gesichter” wichtig für Angriffe mit persönlichem Kontakt.
- Fokus auf Perspektive “externer Angreifer” (nicht: “Innentäter”).

- SE-Pentest = **Projekt mit fünf Phasen:**

1. Planung und Zielfestlegung (zusammen mit dem Auftraggeber)
2. Informationsakquise und Auskundschaften
3. Spezifikation der durchzuführenden Angriffe ("Szenarien")
4. Angriffe (unbemerkt) durchführen
5. Ergebnisbericht und Kundenberatung

- Unterschiede zu richtigen Angriffen:

- **Bezahlung:** Pentesting-Team kostet pro Kopf und Tag — wirkt sich auf Dauer und somit Breite und Tiefe der Tests aus.
 - Ethische Aspekte: Oft **Ausklammerung bestimmter Angriffswege**, z.B.
 - Privatleben des Personals ist tabu
 - Keine Angriffe, die bei Missglücken oder im Anschluss demotivieren
 - **Keine Beschädigungen**, z.B.
 - keine Gewaltanwendung (Fenster einschlagen, Türen aufbrechen)
 - kein Entwenden von Gegenständen (Notebooks, Dokumente, ...)

- Festlegung des Testumfangs:
 - **Beratung:** Auftraggeber wissen oft nicht, was sinnvoll zu testen ist.
 - Budget- und Ethikrandbedingungen, Ziele und Deliverables
 - **Testzeitraum und -orte** (z.B. nur tagsüber, nicht an bestimmten Tagen oder in bestimmten Bereichen, nicht bestimmte Systeme/Personen)
 - **Werkzeugwahl**, z.B. Telefon, E-Mail, Dietriche, ...; **Vorabinformationen**
- Vertragliche Regelungen:
 - **Dienstleistungsvertrag** auf Basis des definierten Testumfangs
 - (Mindestens zwei) Ansprechpartner und **“Get out of jail free”-Karten** für Notfälle (Personal/Werkschutz ruft Polizei o. ähnl.)
 - **Schriftliche Erlaubnis** zur Dokumentenfälschung (Ausweise, ...), zum Eindringen in Gebäude/IT-Systeme, Verwenden von Uniformen (z.B. des Wach- oder Reinigungspersonals), ... soweit relevant.
 - **Art der Erfolgsnachweise:** Videos/Fotos zulässig? Gegenstände entfernen oder z.B. mit Aufkleber versehen?
 - **Berichtsmodalitäten**, z.B. wöchentlich oder nur nach Abschluss

- Per Internet (OSINT):
 - Organigramme
 - Jahresberichte, Stellenanzeigen, Firmengeschichte und Leitbild
 - Mitarbeiternamen mit E-Mail-Adressen und Telefonnummern
 - Aktuelle Projekte, Produkte, Presseerklärungen, Kunden, Dienstleister
 - Jargon (Fachbegriffe, Abkürzungen, ...)
 - Beiträge in Diskussions-/Support-Webforen mit Firmen-E-Mailadresse
 - Ggf. Social-Network-Profile des Personals
- Vor Ort:
 - Personal: Typische Kleidung, Arbeits- und Pausenzeiten, Ausweise, Kommunikations-/Raucherbereiche, Anliefer-/Besucherverkehr, ...
 - Gebäude: Raumpläne, überwachte Bereiche (Kameras/Wachpersonal), Zugangskontrollsysteme, Dienst- und Schichtpläne, Funktionsräume (Drucker-/Post-/Serverraum, Lager, ...), Toiletten, Papiertonnen, ...

- **Welche Angriffe sind erfolgversprechend?**
 - Rollen / Zuständigkeiten im Team definieren
 - “Drehbuch” / Personenbeschreibungen erstellen
- Reihenfolge und Zeitplan festlegen
- Im Zusammenspiel mit dem Auftraggeber:
 - Gewählte Szenarien genehmigen lassen
 - Abbruchkriterien definieren
 - Vertragliche und gesetzliche Erlaubnis prüfen
 - Ggf. Dritte einbeziehen (z.B. Wachdienst-Firma, Gebäudevermieter)
- Requisiten beschaffen / Material vorbereiten:
 - Uniformen
 - Ausweise, Dokumente
- Üben, üben, üben, ...

- Per E-Mail: Abschicken und abwarten. ;-)
- Per Telefon: Notizen machen, lokale Störungen vermeiden
- Vor Ort:
 - Üblicherweise Teamarbeit (zwei Personen, eine steht Schmiere)
 - Wartezeiten sinnvoll nutzen
- **Wichtig: Nichts tun, was man nicht darf!**
 - Gesetze beachten:
 - Z.B. Polizeiuniformen verwenden oder amtliche Lichtbildausweise fälschen ist fast überall ein No-Go!
 - Relevante Gesetze können sich pro Land unterscheiden
 - Vertragliche Vereinbarungen einhalten
 - Soweit möglich an den Plan halten, aber nicht mehr testen als vereinbart

- Weniger spannend, aber für den Auftraggeber das Wichtigste
- Schriftlich und/oder als Präsentation/Diskussion
- Struktur ähnlich zu technischen Pentest-Reports:
 - Methode und Szenario (Angriffsplan) beschreiben
 - Durchführung und Ergebnis dokumentieren, ggf. Beweise beifügen
 - Handlungsoptionen aufzeigen, ggf. Empfehlungen aussprechen
- Möglichst **keine Schuldzuweisungen an Einzelpersonen**
- Auf Überbleibsel hinweisen, z.B.
 - geöffnete, nicht mehr verschlossene Schlosser, z.B. an Schränken
 - mit Stickern als Anwesenheitsnachweis beklebte Geräte
 - beim Angriff eingebrachte Geräte (WLAN-Accesspoints, Keylogger, ...)

1. Social Engineering — Begriffsbildung und -abgrenzung

2. Angreifer-Perspektive:

- Ausgewählte Beispiele für Social Engineering
- Kategorisierung und Arten von Social-Engineering-Angriffen

3. Anwender-Perspektive:

- Gegenmaßnahmen für Social-Engineering-Angriffe
- Durchführung von Social Engineering Penetration Tests
- Digitale Sorglosigkeit

Digitale Sorglosigkeit

ZDF/dpa-Meldung 13.01.2015:

[...] "Viele Nutzer und Firmen merken gar nicht, wenn sie Opfer einer Cyberattacke werden", so Hange. Zum Teil fehle es an Kompetenz, Gefahren zu erkennen und für genügend Schutz zu sorgen. [...]

Michael Hange
Präsident des Bundesamts für Sicherheit in der Informationstechnik



Photo: BSI

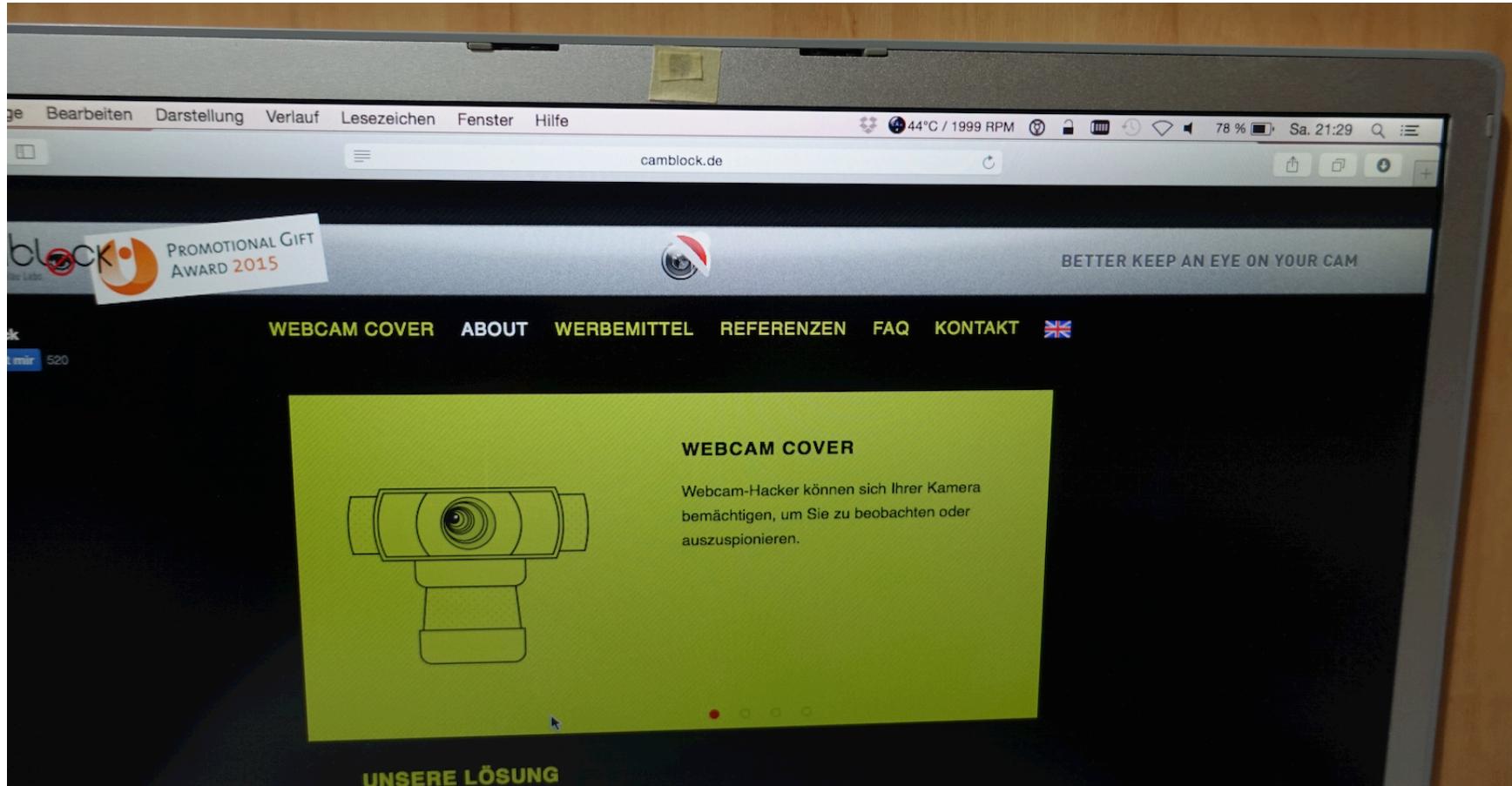
Quelle: <http://www.heute.de/bundesamt-beklagt-digitale-sorglosigkeit-cyberkriminelle-ruesten-auf-36708906.html>

■ Hauptproblem mangelnder Awareness:

- “Sowas passiert nur anderen.”
- “Warum sollte sich jemand für mich und meine Daten interessieren?”
- “Man kann sowieso nichts dagegen machen.”

Problem 1

Symptome statt Ursachen bekämpfen



Notebook-Webcam verdecken – eine gute Idee?

Problem 2

Alles kostenlos, alles ausprobieren

Warum braucht ein Smartphone-Spiel Zugriff auf Geräte-Id, WLAN, Kamera, Mikrofon, Kontakte, Kalender, GPS-Position und SMS-Versand?



Bildquelle: www.mirror.co.uk / Rex Features



Bildquelle: wundergroundmusic.com

Zusammenfassung



- Je nach Zielsetzung und Fähigkeiten eines Angreifers können Social-Engineering-Angriffe einfacher und effektiver sein als technische Angriffe.
- Einteilung in **human-based**, **computer-based** und **reverse Social Engineering**
- Teilweise gibt es **technische Gegenmaßnahmen**; ansonsten sind **Awareness-Maßnahmen** der beste bekannte Ansatz.
- SE-Pentests sind hilfreich, aber aufwendig und teuer
(Fünf-Phasen-Modell)

Gute gemachte Social-Engineering-Angriffe funktionieren immer.

Beispiel für Social Engineering

Microsoft is calling



- **Wer von Ihnen wurde noch nicht von Micorsoft angerufen?**