Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation UVEK

Social Engineering
Der Mensch im Fokus

Referent

Urs Maurer
Wissenschaftlicher Mitarbeiter
Diplomingenieur Informatik / EMBA
NDS Informatiksicherheit / Informationsschutz

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation UVEK
Bundesamt für Verkehr
Abteilung Sicherheit, Sektion Schifffahrt

Mühlestrasse 6, 3063 Ittigen, CH-3003 Bern
Tel. +41 58 480 89 77
urs.maurer@bav.admin.ch
www.uvek.admin.ch

Was ist "Social Engineering"?

"...the art and science of getting people to comply with your wishes.“

Harl, People Hacking

Grundsatz von Social Engineering

Ausnützen von menschlichen Eigenschaften und stereotypischem Verhalten (Fixed Action Patterns):

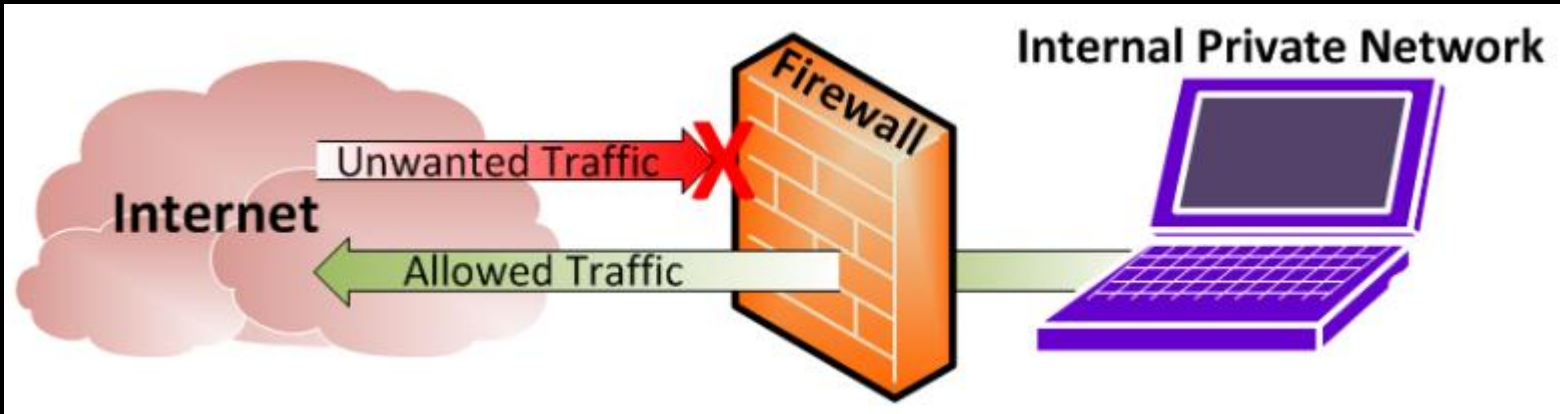
Konrad Lorenz * 07.11.1903 in Wien; † 27.02.1989

- Hilfsbereitschaft
- Vertrauen
- Angst
- Respekt vor Autorität
- Neugierde, Faulheit, Überraschungseffekt, Scham, Schuldgefühl (Commitment und Konsistenz), Zorn, Stolz, Neid, Narzissmus, Mitleid, Sympathie, Knappheit, Soziale Bewährtheit… etc.

Urteilsheuristiken* unterstützen stereotypes Verhalten

* Eine Denkstrategie, die die Problemlösung vereinfacht, Daniel Kahneman und Amos Tversky

IT-Sicherheit / Cybersicherheit heute



Bildquelle: https://www.tunnelsup.com

«Unsere Systeme sind sicher»
«Sowas passiert nur anderen»
«Wer soll sich schon für unsere Daten interessieren?»
«Man kann sowieso nichts dagegen machen»

If they can't hack you, they'll fool you (2018, Cormac Bracken)

Angriffsziele bei SCADA* Systemen

- Verunsicherung
- Betriebsstörung
- Rufschädigung
- Datenzugriff / Manipulation von Daten
- Veröffentlichung von Informationen
- Spionage
- Absichtliche oder unabsichtliche Herbeiführung von Unfällen
- Erpressung

Durchschnittliche Dauer bis ein Angriff bemerkt wird: 200 Tage (2017, KPMG)

* Wikipedia: Unter Supervisory Control and Data Acquisition (SCADA) versteht man das Überwachen und Steuern technischer Prozesse mittels eines Computer-Systems.

Angriffswerkzeuge / Methoden

- Phishing (Zugangsdaten für Systeme)
- Ransomware (Ein «Töölchen» installieren, welches mir dann z. B. alle Daten verschlüsselt)
- Business Email Compromise (BEC) Scams (E-Mails von “wichtigen” Absendern)
- Friendshipness (Kontaktanfragen attraktiver Damen oder Herren)
- Water-Holing (Angriff über beliebte Webseiten)
- Baiting (USB-Sticks, CD-Disks, Flash-Drives)

Timing und Kontext müssen immer stimmen!!!

* Wikipedia: Unter Supervisory Control and Data Acquisition (SCADA) versteht man das Überwachen und Steuern technischer Prozesse mittels eines Computer-Systems.

Beispiele… Robin Sage, lebte 30 Tage

Die Mata Hari des Cyberspace:
25 Jahre alt, attraktiv
Absolventin MIT
Analystin für Cybersicherheit der US-Marine
10 Jahre Berufserfahrung

Erfunden von Thomas Ryan

- Zugang zu vertraulichen Regierungsinformationen
- Zugang zu diversen E-Mail- und Bankkonten
- Kannte auf Grund GPS-Positionsangaben zugeschickter Fotos geheime Truppenstützpunkte der USA
- Wer mit wem im exklusiven Sicherheitsmilieu der USA verkehrt
- Bekam mehrere Jobangebote, sogar als Referentin für Google und dem weltgrößten Rüstungskonzern Lockheed Martin

Ein späterer Test mit einem attraktiven Mann als Lockvogel funktionierte bei Frauen nicht!

Beispiele…

```
void FC6084(arg2,arg4,arg6,arg8)
{
    case 6: //Write recorded values from dyn. DBs to INPUT process i
    {
       if(DB8061.D16 <> 1) // D16==1: dynamic DBs successfully create
             return;
       ar1 = P#L36                              // points to local dat
       ar2 = P#L46                              // points to local dat
       [ar1] = [ar2] = 0x1002;                  // ANY pointer, data t
       [ar1+2] = [ar2+2] = DB8061.DBD8;         // # of recorded bytes
       if(arg4 >= 0x15 || arg4 < 0x0)           // param validation (max. 21 seconds)
             return;
       [ar1+4] = arg4 / 3 + 0x1F80;             // DB number (DB8064..DB8070)
       [ar1+6] = (((arg4 % 3 + 0x1F80 >> 16 * [ar1+2]) + 4)<<3) | 0x84000000;
                                                // source is DB
       [ar2+4] = 0;                             // dest isn't DB
       [ar2+6] = P#E.0;                         // dest is input process image
       BlklMov(ar1, result, ar2);               //(src, result, dest)
       arg6 = result;                           // error handling
       if(result <> 0) return;
       arg6 = 0;
       return;
    }
}
```

Quelle: Bericht Langner zu Stuxnet, 2017

Stuxnet Virus – Einsatz in Natanz (Standort der iranischen Zentrifugen zur Urananreicherung)

Beispiele… Timing muss stimmen

15
Aug

As Expected: Robin Williams 'Goodbye Video' Facebook Phishing Message

Stu Sjouwerman

Tweet Share Like 0 Share

The scammers are at it, as expected. There is now a Facebook phishing message that invites users to click a link and see an "exclusive" video of Robin Williams saying goodbye through his cell phone. Of course there is no video, and the link leads to a bogus BBC news page which tries to trick you into clicking on other links that lead to scam online surveys.

The surveys will try to get you to provide your personal information or sign up to extremely expensive SMS 'services'. The information you provide will be shared with unscrupulous Internet marketers and may later be used to inundate you with unwanted phone calls, emails, and junk mail.

U. a. Herunterladen von virenverseuchten Toolbars und Plugins

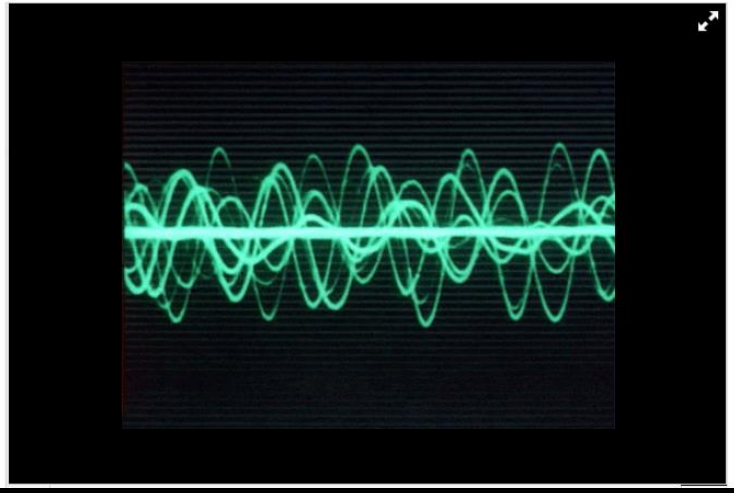
Beispiele… Voice Phishing

Am Telefon

09. Juli 2019 15:27; *Akt: 09.07.2019 15:48*

Betrüger gibt sich als Chef aus und klaut Millionen

Betrüger fälschen Stimmen und machen so hohe Beute. Sie geben sich am Telefon als CEO aus und lassen Millionen transferieren.



Teures Training

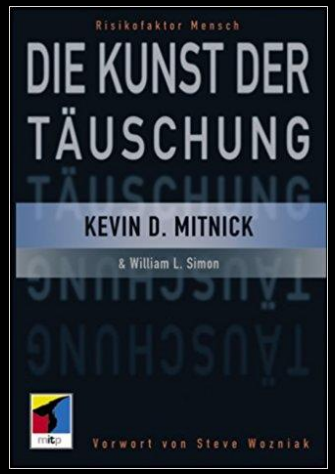
Im Gegensatz zu Video-Deepfakes ist es verhältnismässig einfach, Audio-Fakes zu erstellen. Es sei aber dennoch eine beträchtliche Investition an Zeit und Geld vonnöten, um gute Audio-Fakes zu produzieren, erklärt Alexander Adam, Datenwissenschaftler bei der Londoner Firma Faculty, der BBC. Das Unternehmen hat sich auf künstliche Intelligenz spezialisiert.

Technischer Angriff, Methode: Autorität, Knappheit

Massnahmen

- Regelmässige Sensibilisierung der Mitarbeitenden und Vorgesetzten (Awareness Kampagnen, Präsenzveranstaltungen vs. Flyer)
- Kommunikation auf unterschiedlichen Kanälen
- Klare Verantwortungen schaffen
- Need to Know- und Vieraugen-Prinzip
- ⇒ the proof of the pudding is the eating

DANKE



- Führt Leser in Denk- und Handlungsweise von Hackern ein
- Betrugsszenarien und folgenschwere Konsequenzen werden beschrieben
- Perspektive des Angreifers wie auch des Opfers
- Gründe für die erfolgreichen Angriffe
- Schutzmassnahmen