sicherheitskultur.at

Social Engineering,
der etwas andere Angriff

Philipp Schaumann

philippschaumann@mailbox.org

Disclaimer:
- Alle hier präsentierten Positionen sind rein privater Natur
- Die technischen Details haben keinen Zusammenhang mit Angeboten oder Software meines Arbeitgebers

Agenda

- Was ist Social Engineering?
- Die Trickkiste des Social Engineers
  - Bedürfnisse, Schwächen, Werthaltungen, Sicherheitsregeln, Konflikte
- Gesprächstaktiken der Angreifer
- Umgang mit (möglichen) Angriffen

Was ist „Social Engineering“

- Eine gefährliche Angriffsmethode zur Erlangung von vertraulichen Informationen, häufig eingesetzt bei Industriespionage.
- Sie nutzt die „Schwachstelle Mensch“ aus

- Häufige Klassifizierung
  - „Human Based“ – die klassische Methode (unser Thema heute)
  - „Computer Based“ – z.B. Phishing Mails, „I love you“-Virus, „Sie haben in der Lotterie gewonnen“ (obwohl sie gar nicht gespielt haben!)

DAS Buch zu Social Engineering:
Kevin Mitnick, The Art of Deception, Wiley Publishing 2002, ISBN 0-471-23712-4

Die „klassische Methode“

- Ein Profi-Angriff ist mehrstufig. Jedes Telefonat oder jeder Kontakt fragt nur eine kleine, „fast öffentliche“ Zusatzinformation ab. Nach einigen Anrufen entsteht Insider-Wissen, das „legitimiert“. Dies wirkt vertrauensbildend.

  - Internet-Recherchen, Presse (Namen von Angestellten, Struktur, Niederlassungen, Außenstellen, …)
  - Urlaubsabwesenheitsnotizen („…bis zum xx.Aug. außer
  - Internes Wissen als Weg zum Vertrauen
  - („wer ist bei Ihnen für xxx zuständig“ - „Ich bin zufriedener Kunde und möchte mich beim Chef bedanken.“)
  - Speiseplan in der Kantine, ……

Beispiel: der Legitimierungskette führt zum Vertrauensverhältnis

- 1. Telefonat → „Bin Student, mache eine Umfrage, welchen Bonitätsdienst benutzen sie derzeit?“ → Trust-Kredit
- 2. Telefonat → „Ich bin von Trust-Kredit, wir machen einen Zufriedensheitsumfrage….. Darf ich fragen, mit welchem von ihren Accounts bei uns Sie eigentlich arbeiten?“ → Account xxxx
- 3. Telefonat → „Ich bin Administrator von Trust-Kredit, es geht um ihren Account xxxx, ich brauche ihr Passwort für eine Account-Verifizierung“. → das Passwort

2002: Kriminelle spiegeln gegenüber Experian vor, Ford Motor Company zu sein und bekommen Kreditreports und Bankinformationen von 13 000 Menschen

Social Engineering – ein alter Hut

Wer von den Profis fällt da heute noch drauf rein?

Facebook-Profil:
Robin Sage, 25 Jahre alt, Absolventin der renommierten Technischen Hochschule in Massachusetts, Analystin für Cybersicherheit der US-Marine samt zehn Jahren Berufserfahrung.

Ergebnis:
An die 300 hochrangige Militärs, Industrielle und Politiker schickten ihr Freundschaftsanfragen und ließen sich nur allzu freimütig vertrauliche Informationen entlocken.

http://diepresse.com/home/meinung/imsucher/585352/Der-virtuelle-Lockvogel?from=simarchiv

Auch bei RSA klappt es

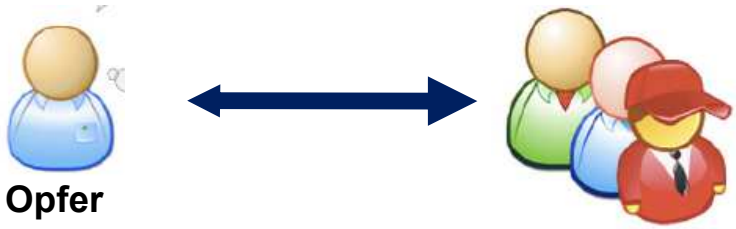
Frühjahr 2011:

Es ist nicht ganz klar, was eigentlich genau passiert ist, aber irgendwie gab es einen Einbruch ins Netz und Angreifer haben wohl Informationen erbeutet.

Die kurze Zusammenfassung: Jemand bei RSA hat ein Mail mit einem Spreadsheet mit dem Namen
„2011 Recruitment plan.xls“
bekommen, in dem eine neue (0-day) Flash Vulnerability ausgenutzt wurde.

http://blogs.rsa.com/rivner/anatomy-of-an-attack/

Fake President Fraud – CEO Betrug



Opfer

Ablauf

- Täter kontaktiert Opfer in der Regel per Email im Namen des Chefs und verlangt eine Überweisung auf ein bestimmtes Konto - Grund z.B. Anzahlung auf geheime Firmenübernahme oder Ankauf eines Kunstwerks

- Der Chef ist meist wirklich auf Dienstreise und die Anfrage nicht unplausibel

- Oft kombiniert mit der Möglichkeit, bei einem Anwalt o.ä. Rückfragen zu stellen

CEO-Betrug

futurezone TECHNOLOGY NEWS Netzpolitik B2B Produkte Digital Life Science Meinung Ga

CYBERCRIME

FACC-Betrug: Finanzvorständin muss gehen

03.02.16, 10:13 Mail an die Redaktion

Der oberösterreichische Luftfahrtzulieferer FACC wurde Betrugsopfer - Foto: APA/DANIEL SCHARINGER

CYBERCRIME

FACC-Betrug: Finanzvorständin muss gehen

Der Luftfahrtzulieferer FACC verlor 50 Millionen Euro durch Online-Betrug. Die Finanzabteilung fiel auf eine falsche Identität herein. Ihre Vorständin muss nun gehen.

Auf Kriminelle reingefallen

Der Betrug erfolgte, indem der Finanzbuchhaltung von Außenstehenden eine falsche Identität vorgespiegelt wurde. Das gab das Unternehmen unter Berufung auf den derzeitigen Stand der forensischen und kriminalpolizeilichen Untersuchungen bekannt.

Bei dieser Betrugsmasche, die den Sicherheitsbehörden unter verschiedenen Bezeichnungen bekannt ist - "Fake President Fraud", "CEO Fraud" oder "Business E-Mail Compromise" - wird der Finanzabteilung in Mails täuschend echt vorgespiegelt, ein Vorgesetzter gebe die Anweisung Geld zu überweisen. Im Fall von FACC ging es auf Konten in Asien und eines in der Slowakei, insgesamt rund 50 Millionen Euro. Die IT-Infrastruktur, Datensicherheit, IP-Rechte sowie die operativen Bereiche von FACC seien von den kriminellen Aktivitäten nicht betroffen, teilte FACC mit. Es seien keine Hinweise auf Malware identifiziert worden.

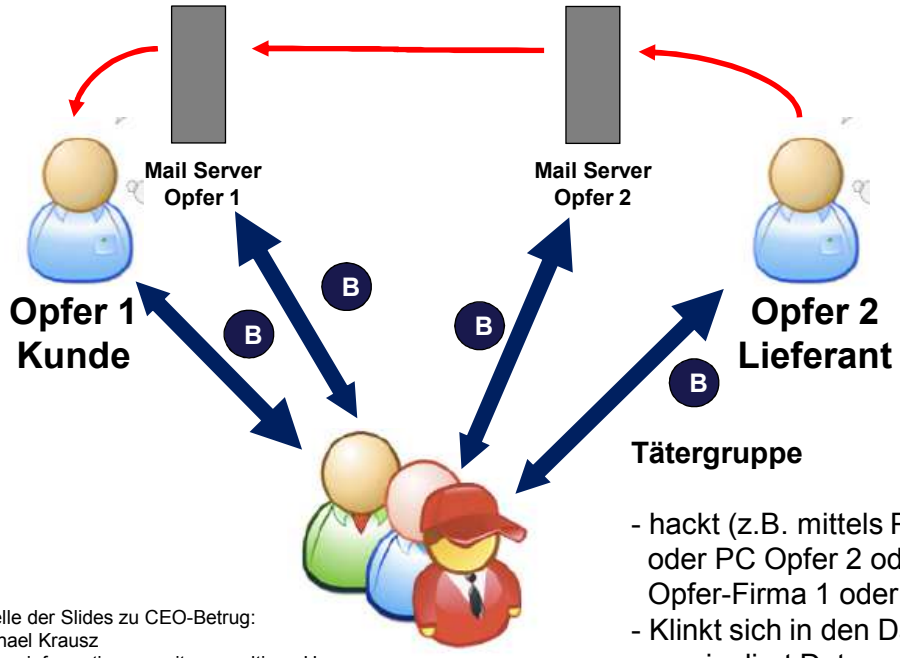
https://futurezone.at/b2b/facc-betrug-finanzvorstaendin-muss-gehen/178.785.380

Rechnungsfraud
Normaler Ablauf eines Geschäfts

Quelle der Slides zu CEO-Betrug:
Michael Krausz
i.s.c. – information security consulting eU
Cumberlandstraße 63/2c
1140 Wien
http://www.i-s-c.co.at

Kontakt: inquiries@i-s-c.co.at

Einklinken in Zahlungsverkehr bei Lieferant ODER Kunde



Tätergruppe

- hackt (z.B. mittels Phishng) PC Opfer 1 oder PC Opfer 2 oder Mailserver von Opfer-Firma 1 oder 2
- Klinkt sich in den Datenverkehr ein und manipuliert Datenverkehr
- mit oder ohne telefonischer Kommunikation möglich

Quelle der Slides zu CEO-Betrug:
Michael Krausz
i.s.c. – information security consulting eU
Cumberlandstraße 63/2c
1140 Wien
http://www.i-s-c.co.at

Kontakt: inquiries@i-s-c.co.at

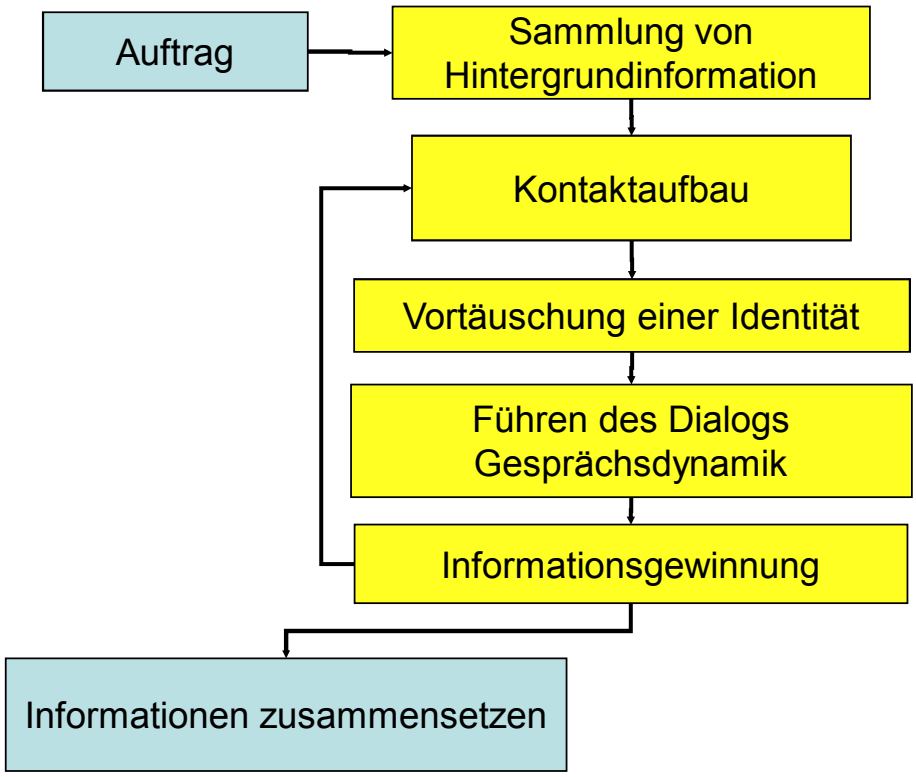
Agenda

- Was ist Social Engineering?
- Die Trickkiste des Social Engineers
  - Bedürfnisse, Schwächen, Werthaltungen, Sicherheitsregeln, Konflikte
- Gesprächstaktiken der Angreifer
- Umgang mit (möglichen) Angriffen

Die klassische Methode

- Gründliche Recherche über das Unternehmen
- Planung des Angriffswegs
- Plausibler Auftritt als Kunde oder Lieferant oder Wartungstechniker oder Mitarbeiter einer andere Niederlassung oder …
- Kontakt per Telefon, Email oder persönlich mit Darlegung eines plausiblen Anliegens (das gegen Regeln verstößt)
- Nächster Kontakt auf der Basis der neuen Informationen

Vorgehen des Social Engineers in Schritten – die klassische Methode



Die Trickkiste:
Ausnützen von Bedürfnissen

- **Abwechslung** (eintönige Tätigkeit)
- **Gespräch, Kontakt** (den ganzen Vormittag allein im Büro)
- **Bequemlichkeit** („warum soll ich mir den Stress eines Rückrufs antun?“)
- **Erhöhung des Selbstwerts (Lob und Anerkennung)**
  - **Bedürfnis gebraucht zu werden, wichtig zu sein**
  - **private Anerkennung** (Kompliment, Flirt**)**
  - **berufliche Anerkennung** („Nur Sie können mir helfen“)
- **Zugehörigkeit, Teamplayer sein**
  - „ein Projekt, das sehr wichtig für die Abteilung ist“
  - „Unser Unternehmen hat gute Chancen ……

Die Trickkiste:
Ausnützen von Schwächen

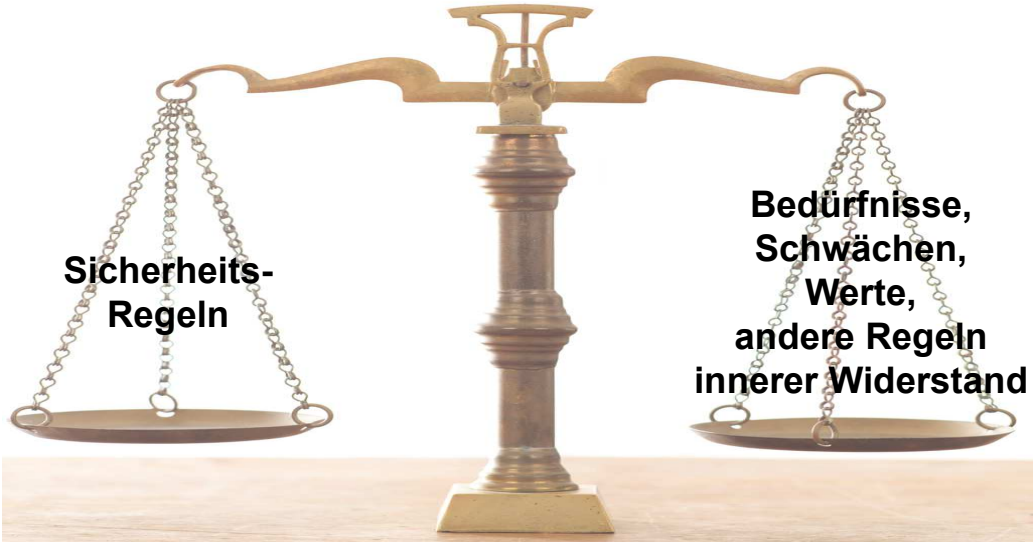
- Nicht-Neinsagen-können
  - Unsicherheit, Schüchternheit
  - Autoritätsabhängigkeit
  - Aggressionsvermeidung, Konfliktscheu
  - Emotionale Erpressbarkeit
- Unerfahrenheit
- Eitelkeit
- Neugier
- Profilierungswunsch
- Machtgier
- Bereicherungsabsicht
- ……

Die Trickkiste:
Ausnutzen von positiven Werthaltunge

- Hilfsbereitschaft
- Solidarität, Loyalität
- Andere moralische und ethische Grundsätze
  - *Versprechen muss man halten*
  - *Geschenke verpflichten*
  - *Dankbarkeit ist eine hohe Tugend*

Das Ziel der Angreifer ?
Menschliche Stärken und Schwächen

Ausnützen von Konflikten



Die Trickkiste:
Ausnutzen von Konflikten

- Sicherheitsregeln können Mitarbeiter in Konflikt bringen wenn sie..

- eigenen Bedürfnissen, Überzeugungen oder Werten zuwiderlaufen
- mit den eigenen Schwächen kollidieren
- mit anderen Regeln kollidieren
- wenn sie innere Widerstände hervorrufen
  - weil sie negativ assoziiert sind
  - weil ihr Sinn nicht nachvollziehbar ist
  - weil sie unklar formuliert sind
  - weil es keine Unterstützung bei ihrer Durchführung gibt

Agenda

- Was ist Social Engineering?
- Die Trickkiste des Social Engineers
  - Bedürfnisse, Schwächen, Werthaltungen, Sicherheitsregeln, Konflikte
- Gesprächstaktiken der Angreifer
- Umgang mit (möglichen) Angriffen

Techniken im Detail: Heftige Gefühle auslösen

- Gefühle behindern die rationale Entscheidung
- **Freude, Zorn, Wut, Mitleid, Angst, Panik, Bedrohung, Schmeichelei, Überraschung, Stolz, Sympathie, Empathie, Neugierde, Überforderung, Verwirrung, …..**

  alles kann funktionieren
- Gefühlswechsel von positiv zu negativ und zurück verwirrt noch mehr

Angriffstechniken, Angriffstaktiken (2) : Emotionalisierung

Gefühle schränken unsere rationale Entscheidungsfähigkeit ein.

- Druck, Schuldzuweisung
  - *„Dann wird das Projekt eben nicht rechtzeitig fertig, das müssen Sie aber selbst dem Chef sagen, dass es nicht an mir gelegen ist“)*
- Einschüchterung
- Auslösen von Mitgefühl (Tränen!)
- Emotionale Erpressung
  - *„Ich hätte nicht gedacht, dass Sie mich da so hängen lassen, das hätte ich von einer Kollegin nicht erwartet. Ihretwegen werde ich möglicherweise jetzt meinen Job verlieren“*
- Lob, Schmeicheleien
  - *„möchte mich beim Chef bedanken…“, „Ich bewundere Sie, wie schnell Sie das erledigen „….*

Techniken im Detail: Wechsel auf die persönliche Ebene

- Kommunikationstricks wie z.B. Wechsel von der sachlichen auf die persönliche Ebene
  - *„Wie lange arbeiten sie schon in diesem Unternehmen? Gefällt es Ihnen? Wenn ich Ihnen weiterhelfen kann…*

Wechsel auf die persönliche Ebene dient häufig als Test,
ob Mitarbeiter hellhörig sind!
Reagiert sie/er neutral, startet der Angreifer die heikle Frage!!

Agenda

- Was ist Social Engineering?
- Die Trickkiste des Social Engineers
  - Bedürfnisse, Schwächen, Werthaltungen, Sicherheitsregeln, Konflikte
- Gesprächstaktiken der Angreifer
- Mein Unsicherheitsprofil
- Umgang mit (möglichen) Angriffen (Übungen)

Lebensgeschichtliche Prägung

- Lebensgeschichtlich (biographisch) geprägte Bedürfnisse, Schwächen, Werte sind schwer veränderbar und daher leicht angreifbar
- Sie steuern unser Verhalten zumeist auch im Erwachsenenalter
- „Erziehungsbotschaften“ wirken weiter

Erziehungsbotschaften ausnutzen

- Erziehungsbotschaften sind tief verwurzelt
  - Man/frau darf nicht unhöflich sein,
  - Man/frau darf nicht widersprechen,
  - Man/frau muss ausreden lassen,
  - Man/frau darf nicht unterbrechen,
  - Erwachsene haben immer recht,
  - Man/frau ist hilfsbereit, lehnt eine Bitte nicht ab,
  - Bestimmt aufzutreten ist unweiblich,
  - Man/frau redet nur, wenn man gefragt wird,
  - Man/frau antwortet, wenn man gefragt wird!
  - ……

Agenda

- Was ist Social Engineering?
- Spezialfälle Rechnungsbetrug und CEO-Betrug
- Die Trickkiste des Social Engineers
  - Bedürfnisse, Schwächen, Werthaltungen, Sicherheitsregeln, Konflikte
- Gesprächstaktiken der Angreifer
- Mein Un-Sicherheitsprofil
- Umgang mit (möglichen) Angriffen

Woran erkennt der Mitarbeiter den Angriff? - Mögliche Hinweise

- Kann nicht an der hinterlegten Nummer zurückgerufen werden, auch sein Chef ist nicht erreichbar
- Benutzt Rufnummer-Unterdrückung oder ruft nicht von der hinterlegten Nummer an
- Beruft sich auf jemanden, der nicht erreichbar ist - oder zu viel Name-Dropping
- Ist übermäßig neugierig
- Ist sehr flirtend und sehr schmeichelnd
- Warum erzählt mir der Kunde so viel von sich selbst, und ist es nicht eigenartig, dass in unseren Interessen so viel Gemeinsamkeiten sind?

Zeitgewinn

- Verhalten und Tricks am Telefon – Wie gewinne ich z.B. Zeit und kann in Ruhe nachdenken und mich beraten
  - „Augenblick bitte, bleiben Sie am Apparat“
  - „Können Sie mir das alles noch mal bitte als E-Mail senden?“
  - „Kann ich Sie zurückrufen?“
  - „Können Sie bitte in 1 Stunde noch mal anrufen?“
  - „Diese Informationen können bei uns grundsätzlich nicht über Telefon weitergegeben werden.“
  - „Ich leite ihre Kontaktdaten gern an die zuständigen Kollegen weiter.“
  - „Hallo, hallo, ich die Verbindung wird immer schwächer, bitte rufen Sie später wieder zurück.“

Das „sanfte“ NEIN
Pacing - Leading

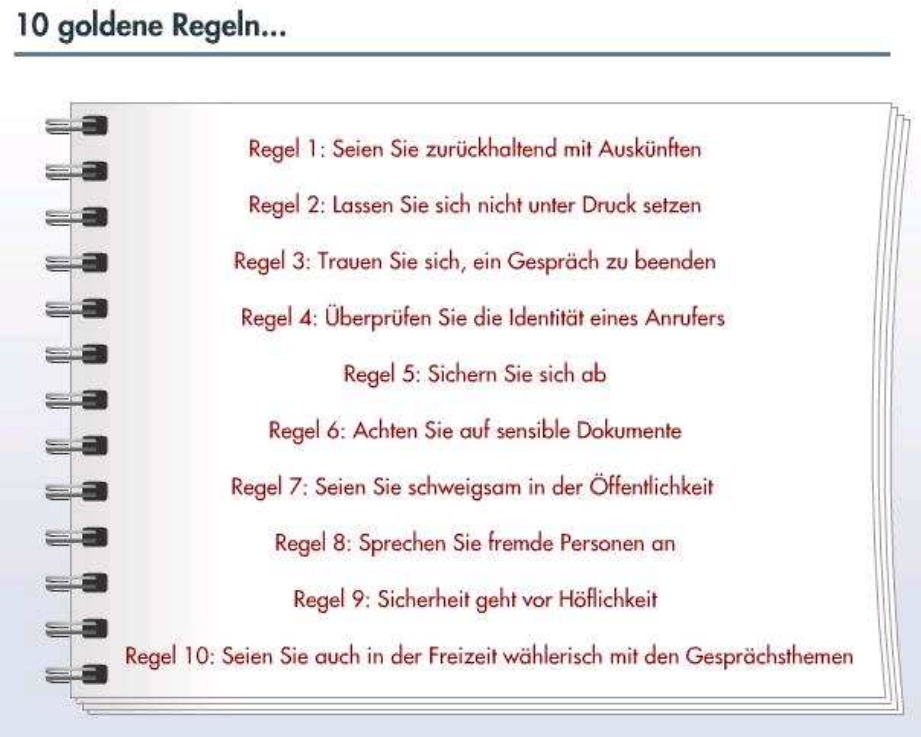
- „Ich verstehe, dass Sie ….., aber (unsere Regeln / derzeit / ….)“
- „Ich sehe ein, dass Sie in Zeitnot sind, aber ……“
- „Ich kann ihre Situation verstehen, aber Sie haben bestimmt Verständnis, dass wir zum Schutz unserer Kunden ….
- „Ihr Lob freut mich sehr, aber trotzdem …..“

Das „sanfte“ NEIN

- “Nein” – und dann ein Hilfsangebot
  - “Können wir Sie später zurückrufen?”
  - „Leider nein, aber ich werde mich erkundigen und sie morgen zurückrufen“
  - „ ich werde mit meinem Chef sprechen, ob in ihrem Fall …..“
- Rückzug hinter die Firmenrichtlinie
  - „Sie haben bestimmt Verständnis, dass wir zum Schutz unserer Kunden …. „

Und dann
sich auf keinen Fall weiter verstricken

10 goldene Regeln



Quelle: https://www.secorvo.de/publikationen/videos.html

Notizen eines „hell-wachen“ IT-Mitarbeiters/Portiers/Rezeptionist/...

- Darf ICH diese Informationen weitergeben?
- Weiß ich, welche Legiti-mierungen notwendig sind?
- Wie kann ich die genannten Legitimierungen überprüfen?
- Wie sicher bin ich, dass er/sie ist, was er vorgibt?
- Warum fragt er gerade mich danach?
- warum kann ich nicht zurückrufen?

- Was könnte mit diesen Informationen in falschen Händen passieren?
- Was wären die Folgen?
- Wen kann ich (um diese Uhrzeit) um Hilfe bitten?
- Passiert etwas schlimmes, wenn ich zum “Kunden” erst mal Nein sage?
- Sollte ich diese Anfrage an jemanden berichten, an wen?

Habe ich ein sicheres Gefühl bei diesem Anrufer?

Danke

Philipp Schaumann

philippschaumann@mailbox.org

Skripten zu diesen Fragen und Literaturtipps auf meiner Website:
http://sicherheitskultur.at/social_engineering.htm