

Theorie und Praxis von Social Engineering Abwehr

Philipp Schaumann
Dipl. Physiker
Erste Bank Group
<http://sicherheitskultur.at/>

Dr. Ulrike Uta Schaumann, MAS
Ärztin für Innere Medizin und
Psychotherapeutische Medizin

philipp.schaumann@erstegroup.com

<http://psymed-schaumann.at/>

1

© 2006, 2007, 2008 Philipp & Ulrike Uta Schaumann

Agenda

- Gegenseitige Vorstellung, gegenseitige Erwartungen und Ziele, Ablauf
- Was ist Social Engineering?
- Die Techniken der Angreifer im Detail
- Selbsteinschätzungen (Test)
- Die Trickkiste des Social Engineers
 - Bedürfnisse, Schwächen, Werthaltungen, Sicherheitsregeln, Konflikte
- Mein Un-Sicherheitsprofil
- Gesprächstaktiken der Angreifer
- Umgang mit (möglichen) Angriffen (Übungen)

2

© 2006, 2007, 2008 Philipp & Ulrike Uta Schaumann

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!)
 - Reverse Social Engineering (Untermenge der klassischen Methode)

DAS Buch zu Social Engineerings:

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



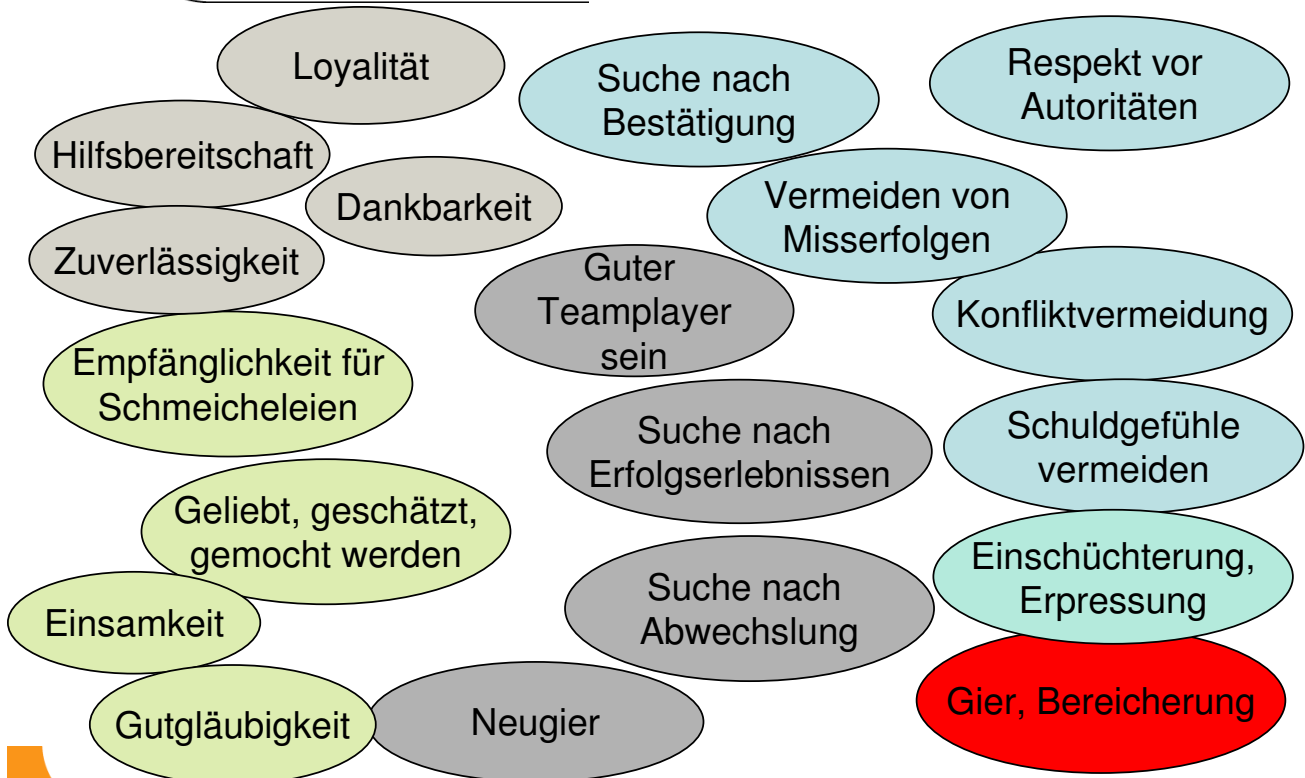
- 1. Telefonat → „Bin Student, mache eine Umfrage, welchen Bonitätsdienst benutzen sie derzeit?“
→ **Trust-Kredit**
- 2. Telefonat → „Ich bin von **Trust-Kredit**, wir machen einen Zufriedenheitsumfrage..... Darf ich fragen, mit welchem von ihren Accounts bei uns Sie eigentlich arbeiten?“ → **Account 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

Agenda

- Gegenseitige Vorstellung, gegenseitige Erwartungen und Ziele, Ablauf
- Was ist Social Engineering?
- Die Techniken der Angreifer im Detail
- Selbsteinschätzungen (Test)
- Die Trickkiste des Social Engineers
 - Bedürfnisse, Schwächen, Werthaltungen, Sicherheitsregeln, Konflikte
- Mein Un-Sicherheitsprofil
- Gesprächstaktiken der Angreifer
- Umgang mit (möglichen) Angriffen (Übungen)

Das Ziel der Angreifer ? Menschliche Stärken und Schwächen



7

© 2006, 2007, 2008 Philipp & Ulrike Uta Schaumann

Die Trickkiste: Ausnützen von Bedürfnissen - aktuell und/oder biographisch gewachsen

- **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

8

© 2006, 2007, 2008 Philipp & Ulrike Uta Schaumann

Die Trickkiste: Ausnutzen von Schwächen (kontextbezogen)

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



Die Trickkiste: Ausnutzen von Werthaltungen

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



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

Typische Erziehungsbotschaften

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

Lebensgeschichtliche Prägung

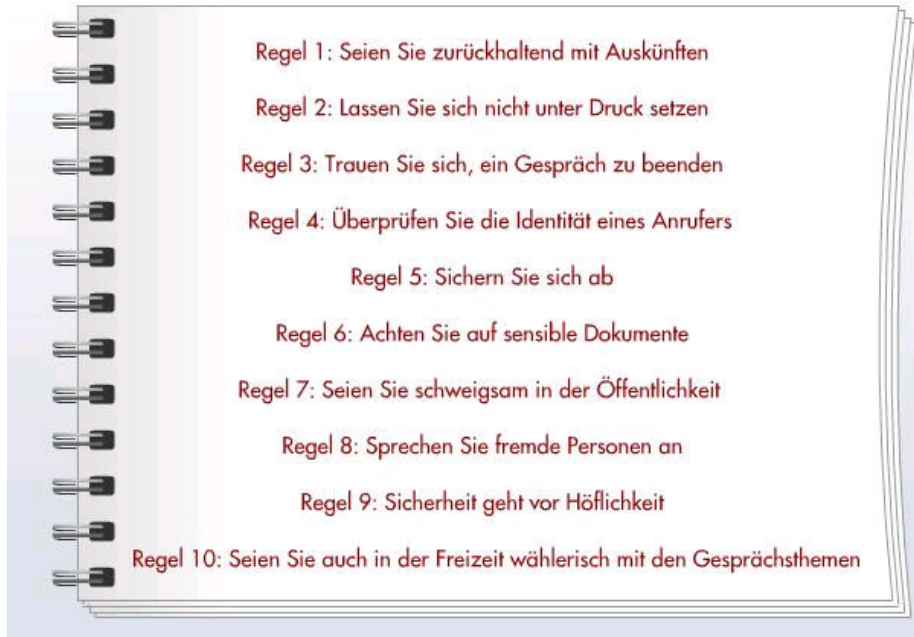
- Lebensgeschichtlich (biographisch) geprägte Bedürfnisse, Schwächen, Werte sind schwer veränderbar und daher leicht angreifbar
- Sie steuern unser Verhalten zumeist auch im Erwachsenenalter
- „Erziehungsbotschaften“ wirken weiter
- Weil auch Angreifer erzogen wurden, haben sie zumeist ein sehr gutes Gespür, wo andere Menschen angreifbar sind

Lösungsweg „Strenge Regeln in der Policy“

- Traditionelle Lösung:
 - Vertrauliche Informationen dürfen nicht weitergegeben werden
 - Jeder Anrufer / Kunde muss authentifiziert werden
 - Auskünfte am Telefon sind nicht erlaubt
 - xxxx braucht die vorherige Genehmigung durch YYYY
 - Eine Passwort-Rücksetzung erfolgt nur nach schriftlicher Information durch den Vorgesetzten
 - Für eine Passwort-Rücksetzung muss der Mitarbeiter persönlich erscheinen

10 goldene Regeln

10 goldene Regeln...



Quelle: <http://www.secorvo.de/video/video-social-engineering-goldene-regeln.jpg>

Psychologischer Hintergrund, warum wir, obwohl wir die Regeln kennen, sie oft nicht befolgen

- Biographisch gebahntes und geprägtes Verhalten ist schwer veränderbar
- Erziehungsbotschaften sind tief verwurzelt
- Weil auch Angreifer erzogen wurden, haben sie zumeist ein sehr gutes Gespür, wo andere Menschen angreifbar sind
- Konflikte setzen die Entscheidungsfähigkeit herab

Ausnutzen 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



Erkennen von Konflikten

- Welche Konflikte kennen Sie?
- Haben Sie sich schon einmal zwischen 2 einander widersprechenden Anforderungen, Erwartungen, Möglichkeiten entscheiden müssen?
 - Zwischen welchen? (Umfrage, Gruppenarbeit)

Umgang mit Konflikten

- **a) Vermeidung**
- **b) Entscheidung**— ist die Abwägung von Handlungsalternativen und deren Folgen- diese ist beeinträchtigt
- Der Mitarbeiter wird also entweder, um den Konflikt zu vermeiden, auf die Wünsche des Angreifers eingehen, oder eine meist spontane Entscheidung treffen.
- Die Entscheidung wird immer zugunsten des Parts, der sich schwerer unterdrücken lässt, fallen!
Es sei denn, der Mitarbeiter erkennt, dass ein Konflikt vorliegt und schafft es, aus der Distanz heraus zu entscheiden! (Training)

Umgang mit Konflikten

- Trachten Sie, Konflikte eher zu vermeiden oder betrachten Sie sie als Herausforderung?
- Versuchen Sie, Konflikte zu schlichten? Haben Sie ein großes Harmoniebedürfnis?
(Rollenspiele, Gruppenarbeit, Umfrage)



Abwehrtraining- Strategien und Techniken (auch unter Berücksichtigung des psychologischen Hintergrunds)

- **Abwehr durch geeignete Kommunikationsstrategien und Supervision**
- Gesprächstechniken - kundenfreundlich UND regelbewusst!!
 - Wie sage ich kundenfreundlich Nein?
 - Zeitgewinn
- Rollenspiele an Hand konkreter Beispiele;
 - z.B. Telefonzentrale
Wie gehe ich um mit: Aggression, emot. Erpressung, Einschüchterung, Schuldzuweisung, forderndem Verhalten, Bestechung, Schmeicheleien, Zeitdruck, Überrollen, Overload, Verwirrung etc...

Verhalten in unterschiedlichen kritischen Situationen

Psychologischer Hintergrund, warum wir, obwohl wir die Regeln kennen, sie oft nicht befolgen

- Biographisch gebahntes und geprägtes Verhalten ist schwer veränderbar
- Erziehungsbotschaften sind tief verwurzelt
- Weil auch Angreifer erzogen wurden, haben sie zumeist ein sehr gutes Gespür, wo andere Menschen angreifbar sind
- Konflikte setzen die Entscheidungsfähigkeit herab
- Emotionalisierung setzt die Entscheidungsfähigkeit herab

Konflikte reduzieren die Entscheidungsfähigkeit

Konflikte erzeugen Stress

Der Cortisolspiegel steigt

Das deklarative Gedächtnis wird beeinträchtigt

Die Entscheidungsfähigkeit sinkt



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

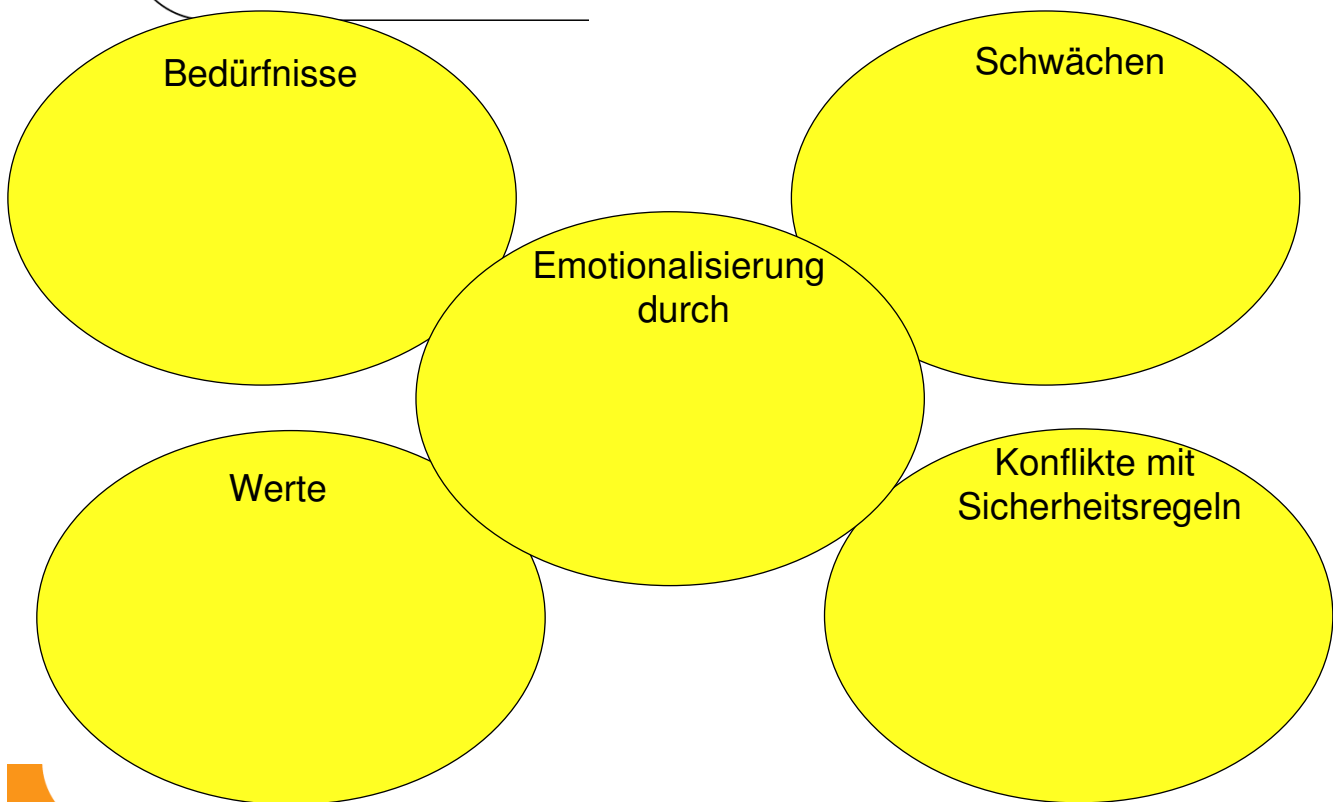
- Gefühlswechsel von positiv zu negativ und zurück verwirrt noch mehr

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 „....“

Mein Un-Sicherheitsprofil



Agenda

- Gegenseitige Vorstellung, gegenseitige Erwartungen und Ziele, Ablauf
- Was ist Social Engineering?
- Die Techniken der Angreifer im Detail
- Selbsteinschätzungen (Test)
- Die Trickkiste des Social Engineers
 - Bedürfnisse, Schwächen, Werthaltungen, Sicherheitsregeln, Konflikte
- Mein Un-Sicherheitsprofil
- Gesprächstaktiken der Angreifer
- Umgang mit (möglichen) Angriffen (Übungen)

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!!

Bei verdächtigem Verhalten Abstand nehmen und überlegen

- Wer ist es, der mich da um einen Gefallen bittet? Kenne ich ihn? In welchem Verhältnis stehen wir zueinander?
- Was ist das genau, was ich tun soll? Eine Arbeit, ein Gefallen, soll ich etwas geben?
- Welche Berechtigung hat der Anrufer, diese Information zu erfragen?
- Ist er der, der er vorgibt zu sein?
- Warum wendet er sich gerade an mich? Bin ich die richtige und einzige Ansprechperson?
- Welche Folgen könnte mein JA haben?

Woran erkenne ich den Angriff? Mögliche Hinweise (1)

- 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?

Verteidigungstechnik 1: Bei Information Overload



1. Innerlich STOPP sagen
2. Kunden höflich unterbrechen
3. Gezielte Fragen stellen (siehe nächste Folie)
4. Falls 2 und 3 nicht möglich ist und Rückfragen übergeht → Versuchen, Zeit zu gewinnen (siehe später)

Rückfragen stellen, auf Antworten bestehen

- „Wie war noch mal ihr Name?“
- „Von welcher Organisation sind Sie? Können Sie das bitte buchstabieren?“
- „Hat die Firma eine Website? Dort finde ich bestimmt die Telefonnummer, auf der ich sie rückerufen kann / die Telefonnummer ihres Chefs.“
- „Wofür benötigen Sie diese Informationen? Ich habe das nicht genau verstanden.“
- „Wer hat Ihnen gesagt, ich könnte Ihnen diese Auskunft geben, ich muss mich dort vergewissern. Vertraulichkeit ist sehr wichtig für uns.“

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.“

Verteidigungstechnik 2: Verhalten bei Emotionalisierung



1. Innerlich STOPP sagen, Abstand gewinnen
2. Häufig ist Zeitgewinn erforderlich (siehe vorher)
3. Gezielte Fragen stellen, um sich auf eine sachliche Ebene zurückzubringen
4. Pacing - Leading

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


Antwortbeispiele für

- **Zeitdruck, forderndes Verhalten**
 - „Ich fühle mich im Moment unter Druck gesetzt, weil Sie eine sofortige Entscheidung verlangen, geben Sie mir um, dann kann ich Ihnen mehr sagen/ kann ich Ihnen besser helfen.“
 - „Ich verstehe, dass sie in Zeitnot sind, aber unsere Sicherheitsregeln erlauben keine Ausnahmen, das werden Sie verstehen“
 - „Ich fühle mich im Moment unter Druck gesetzt, weil Sie eine Entscheidung verlangen, die ich nicht geben kann. Ich werde dafür sorgen, dass“
- **Bestechung**
 - „Wollen Sie mich testen, ob ich bestechlich bin?“
 - „Ich nehme grundsätzlich keine Geschenke an, das müssen Sie verstehen“

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



- Darf ICH diese Informationen weitergeben?
- Weiß ich, welche Legitimierungen 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?

Projektlauf-Vorschlag (1)

- Umfrage / Brainstorming mit den betroffenen Mitarbeitern:
 - welche Situationen im Kundenkontakt bringen Sie persönlich in einen Konflikt zwischen den Vorschriften und dem, was Sie für den Kunden gern tun würden?
 - in welchen Situationen werden Kunden durch die Vorschriften frustriert
 - bei welchen Situationen mit Kunden haben Sie persönlich ein „komisches Gefühl“ („das kommt mir sehr komisch vor“, „ob das wohl wirklich stimmt?“)
 - Haben Sie die Möglichkeit, im Anschluss an „eigenartige“ Situationen dies zu vermerken, weiterzugeben?
 - was würde Ihnen in solchen Situationen helfen? z.B.
 - ein technisches Werkzeug, z.B. Informationen über die Kunden-Geschichte,
 - eine Stelle, an die Sie weiterleiten könnten
 - eine klarere Definition, wo „Kundenfreundlichkeit“ enden soll

Projekttablauf-Vorschlag (2)

- (optional) Fokusgruppe mit Kunden über ihre Wünsche zu mehr Sicherheit oder mehr Flexibilität
 - was frustriert die Kunden?
 - welche der vielen möglichen Verbesserungsideen werden positiv aufgenommen?
- Erstellung einer Risikostudie
 - Was sind die Bedrohungen?
 - Was sind sensible Informationen?
 - Was ist unsere schwächste Stelle?
 - Was sind höchsten Bedrohungen für uns oder die Kunden?
 - Was sollte die höchste Priorität haben?

Projekttablauf-Vorschlag (3)

- Erstellung eines Lageberichts
- Erarbeitung von Verbesserungsvorschlägen
 - Überarbeitung von Regelungen
 - neue Trainingsvorschläge
 - Erarbeitung von Werkzeugen für die Mitarbeiter (z.B. Verbesserungen im CRM-System)
- Implementierungen

Trainingsvorschläge (1)

■ Alle Mitarbeiter:

- Was ist bei uns „vertraulich“?
- Wer darf vertrauliches erhalten?
- Welche Legitimierung akzeptieren wir?
- Was ist zwar nicht „vertraulich“, wird aber trotzdem nicht (am Telefon) ohne Legitimierung öffentlich bekannt gemacht (z.B. Handynummern, Zuständigkeiten)

Trainingskonzept - psychologischer Teil (1)

- Angreifer- und Opferpsychologie
- Sensibilisierung für die Angreiferstrategien
 - woran erkenne ich verdächtiges Verhalten am Telefon, im direkten Kontakt?
- Sensibilisierung für die eigenen Verwundbarkeiten
 - Selbsteinschätzungsfragebogen
 - „Bin ich manipulierbar?“
 - Selbsterfahrung (Gruppen- und Einzelarbeit)
 - „Wo bin ich angreifbar?“ (Schwächen, Bedürfnisse, Werte, Konflikte)

Trainingsinhalte - psychologischer Teil (2)

- Kommunikation und Gespräch
(Rollenspiele, Supervision eigener Situationen)
 - Kundenfreundlich Neinsagen
 - Reaktion auf typische Phrasen
 - Reaktion auf typisches Angreiferverhalten
 - „Wie verhalte ich mich, wenn..?“
 - Umgang mit Konflikten
 - Verhalten bei Emotionalisierung
 -

Abwehrtraining- Strategien und Techniken (auch unter Berücksichtigung des psychologischen Hintergrunds)

- Sensibilisierung für die eigenen Verwundbarkeiten
 - Fragebogen, Gruppenarbeit-Erziehungsbotschaften
- Woran kann ich verdächtiges Verhalten erkennen? - Erkennen der Täterstrategie
 - Beispiele
Zeitdruck, Überrollen, Overload, Verwirrung.....
- Erkennen eines möglichen, vom Täter geschaffenen Problems
 - Brainstorming; Beispiele der Referenten
- Erkennen von Konflikten
 - Rollenspiele, Gruppenarbeit, Umfrage

Trainingskonzepte (1) Widerstands-Boot Camp

■ Abhärten durch „Exponierung“

Im Rollenspiel Antworten auf typische Problemstellungen üben

die Exponierung gegenüber einer „Geschichte“ nimmt den Neuheitscharakter, ein ganz neuer „Schmäh“ bleibt allerdings ein Problem

Trainingskonzepte (2) Widerstands-Boot Camp

■ Vorwarnung

bzgl. der

- kriminellen Absichten und
- Der verwendeten emotionalen Tricks

■ Erinnerung daran, dass nicht alle Anrufer ehrlich sein müssen.

■ Mehr Vorsicht bei emotionalen Situationen (auch eigenem Zorn, Freude, Überraschung, etc.)

Trainingskonzepte (3)

Widerstands-Boot Camp

■ Erhöhung der Selbstsicherheit - Unsicherheit verunsichert

Mehr Sicherheit in Bezug auf

- Kenntnis der Abläufe (wer ist wofür zuständig?, wo kann ich Hilfe bekommen?),
- Kenntnis der Regeln, Vorschriften und Gesetze (wer darf was?),
- Kenntnis der Zusammenhänge (was ist eigentlich vertraulich?),
- Darf ich im Unternehmen Schwächen zugeben, „dumme“ Fragen stellen, mich rückversichern?
- Darf ich NEIN sagen ohne Angst vor „großen Tieren“?
- etc.

Trainingskonzepte (4)

Widerstands-Boot Camp

■ Realitätstraining

- Menschen vertrauen auf ihre Menschenkenntnis, sie glauben, dass sie nicht reinfallen würden. Hier hilft nur ein lehrreicher Schock.
- Menschen gehen immer davon aus, dass sie verschont bleiben, dass gewisse Risiken sie selbst nicht betreffen.

■ Risikobewusstsein

- Wissen um die Existenz des Risikos
- Erkennen, dass andere betroffen sein könnten
- Erkennen, dass man selbst betroffen sein könnte – dies geht nur über eigenes Erleben, nicht über einen Vortrag

Fragen bitte



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