Phishing für Fortgeschrittene

Marco Krause
Security Engineer

Münster – 20.11.2015
www.ing-diba.de

ING DiBa
Die Bank und Du

Social Engineering
Definition

Beeinflussung der Denkweise eines menschlichen Ziels, sodass dieses eine vom Social Engineer beabsichtigte Handlung als beste Option wahrnimmt.

(Marco Krause)

Social Engineering
Varianten

- **Phishing**
  - Elektronische Kommunikation (E-Mail, Kurznachrichten)
  - Digitale Speichermedien
  - Printmedien
- **Vishing**
  - Telefonischer Kontakt
- **Persönlicher Kontakt**
  - Tailgating
  - Dumpster Diving

Social Engineering
Relevanz

- **2011 RSA**
  - 66 Mio $
  - Lockheed Martin
  - US Bankensektor: 50-100 Mio $
- **2012 Steuerbehörde South-Carolina**
  - 21 Mio $
- **2013 Target Inc.**
  - 252 Mio $
- **2014 Sony Pictures**
  - 35 Mio $
- **2015 „Carbanak“ Cyber-Bankraub**
  - 1 Mrd $

Human Hacking

Betriebssystem

- Entscheidungsprozess
- Motivation

Sicherheitslücken

- Unbewusste Beeinflussung
- Vorhersagbare Irrationalität

Exploit

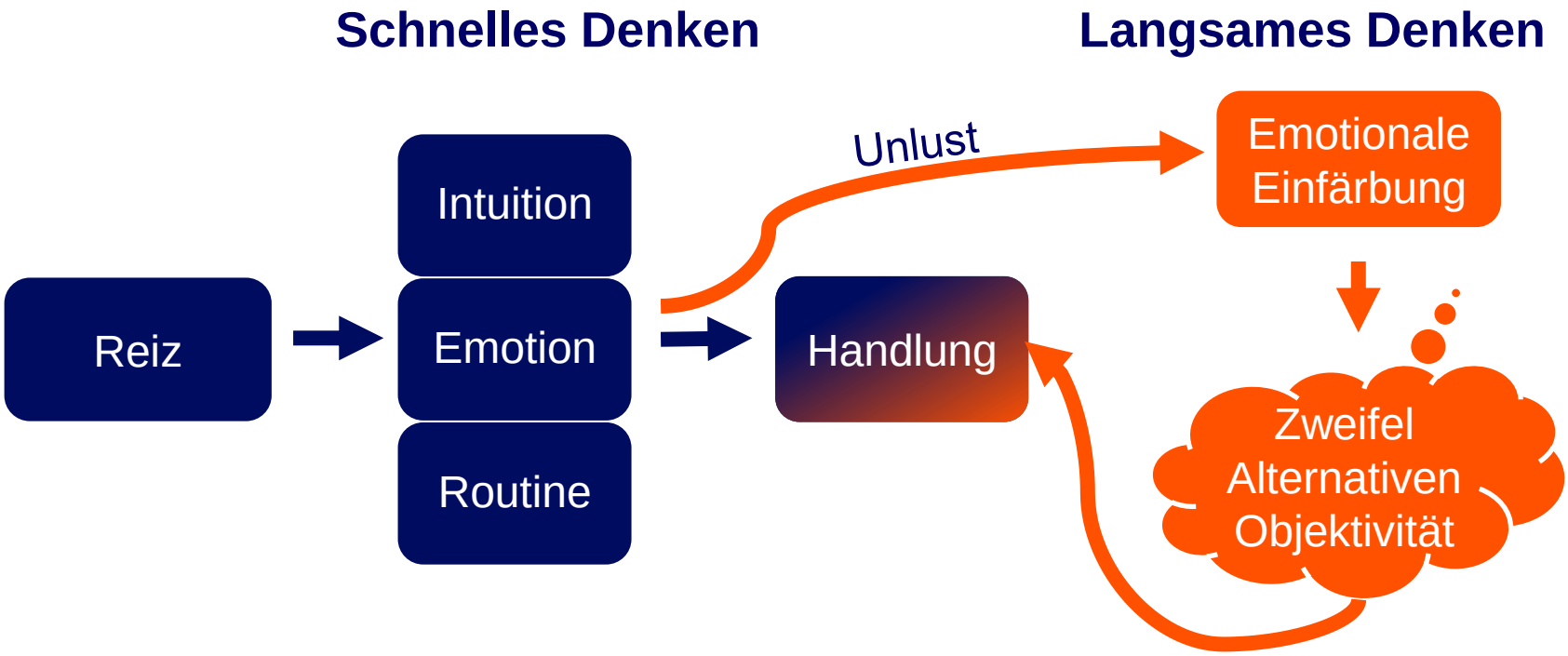
- Ausgefeilte psychologische Tricks
- Konstruktion von Rahmenbedingungen

Patch-Management

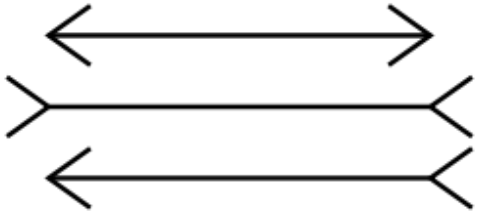
- Kontinuierliches Training
- Ergänzung durch technische Maßnahmen

ING DiBa

Betriebssystem



Sicherheitslücken

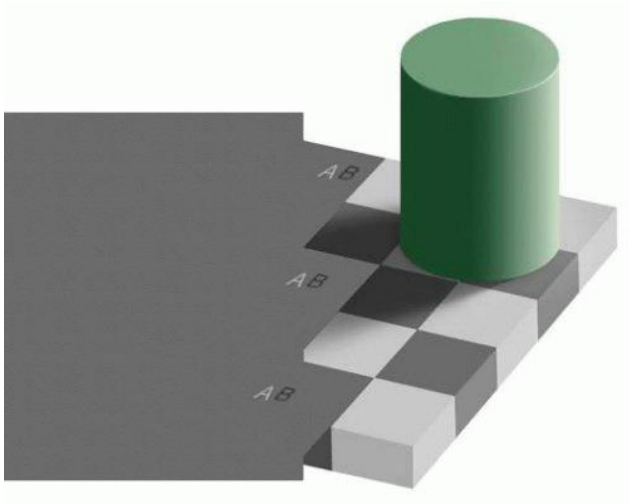


Sicherheitslücken

Anreize für das "Schnelle Denken"

- Leichtigkeit
- Schnelligkeit
- Hohes Maß an Überzeugtheit
- Innerhalb der Wertvorstellung

→ Ignoriert Auffälligkeiten



Exploits

Framing

- Konstruierte Rahmenbedingungen
- Lenkung der Denkweise

Emotionen

- Verlustangst
- Neugier

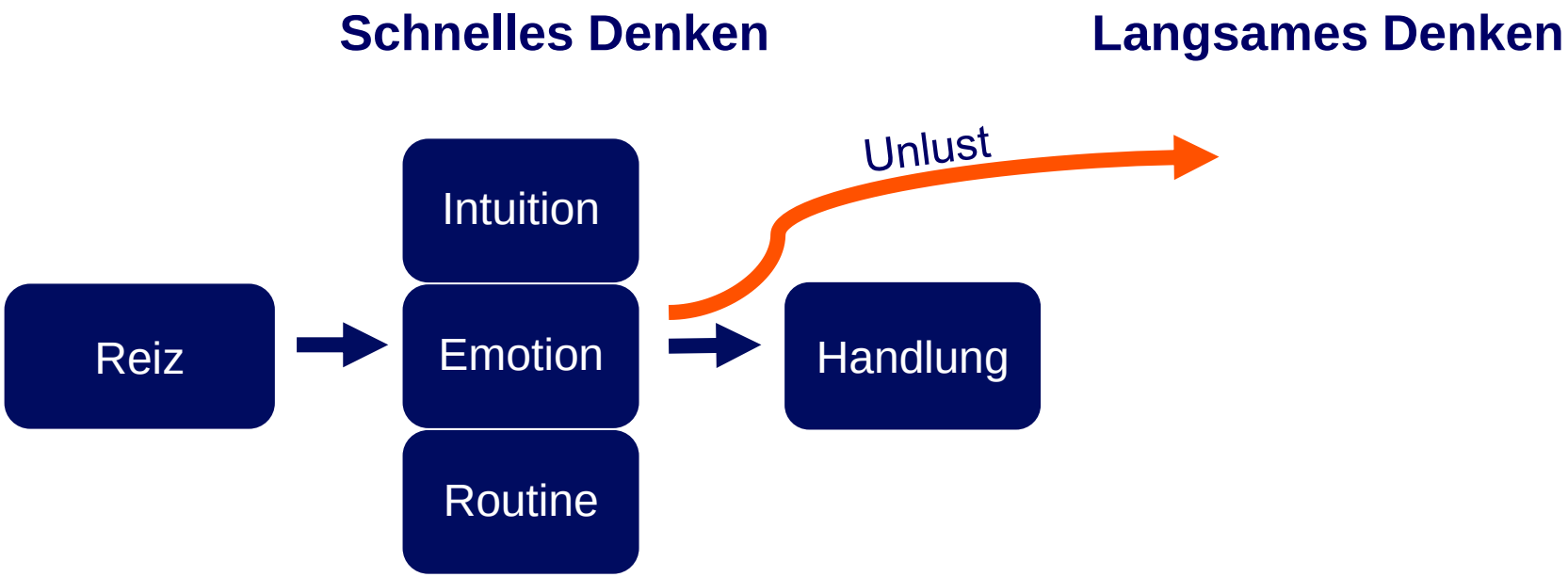
Stress

- Zeitdruck
- Autorität

Auto-Pilot

- Vertraute Aufmachung
- Routine

Exploits


Schnelles Denken
Langsames Denken
Unlust
Intuition
Reiz
Emotion
Handlung
Routine

Beispiel

Guten Tag Marco Krause,

das von Ihnen gespeicherte Bankkonto wurde im Moment der Abbuchung nicht ausreichend gedeckt um die Kontoabbuchung durchzuführen. Sie haben eine offene Forderung bei unseren Mandanten [redacted]

Aufgrund des andauernden Zahlungsausstands sind Sie gezwungen dabei, die durch unsere Beauftragung entstandenen Gebühren von 47,71 Euro zu bezahlen. Die Überweisung erwarten wir bis spätestens 27.11.2015.

Es erfolgt keine weitere Erinnerung oder Mahnung. Nach Ablauf der Frist wird die Angelegenheit dem Gericht und der Schufa übergeben.

Mit freundlichen Grüßen
Abrechnung von Slandersberg Jakob

Beispiel

Beispiel Bank

14. September 2015 16:32 MESZ
Transaktionscode: 02D11937JS973803FC

Guten Tag Marco Krause,

Uns ist eine verdächtige Zahlung über 1.229,00 EUR an Example Elektro SAS (shop@example-elektro.com) aufgefallen.

Eine Prüfung der unten stehenden Transaktion hat ergeben, dass sie möglicherweise nicht durch Sie autorisiert wurde. Daher wurde diese Transaktion zurückgerufen.

Händler	Mitteilung an den Händler
Example Elektro SAS shop@example-elektro.com +33 180503575	Sie haben keine Mitteilung eingegeben.

Beschreibung	Einzelpreis	Anzahl	Betrag
		1	1.229,00 EURO
		Zwischensumme	€ 1.229,00 EUR
		Summe	€ 1.229,00 EUR
		Zahlung	€ 1.229,00 EUR

Zahlungsempfänger shop@example-elektro.com

Rechnungsnummer: 51126091

Um weiten Betrug zu verhindern, wirde Ihr Beispiel-Bank Konto bis auf weiteres eingeschränkt. Wir bitten Sie daher ihr Beispiel-Bank Konto mit nachfolgendem Link zu bestätigen um die Einschränkung Ihres Kontos aufzuheben.

Klicken Sie hier zum Bestätigen Ihrer Daten

- Branding + Aufmachung
- Personalisierte Begrüßung
- Plausibler Inhalt + Verlustangst
- Rechtschreibung + Grammatik nahezu fehlerfrei
- Gefälschter Absender

Von	Betreff	Erhalten
info@beispiel-bank.de	Verdächtige Zahlung	Montag, 14.09.2015 16:35

- Getarnter Link

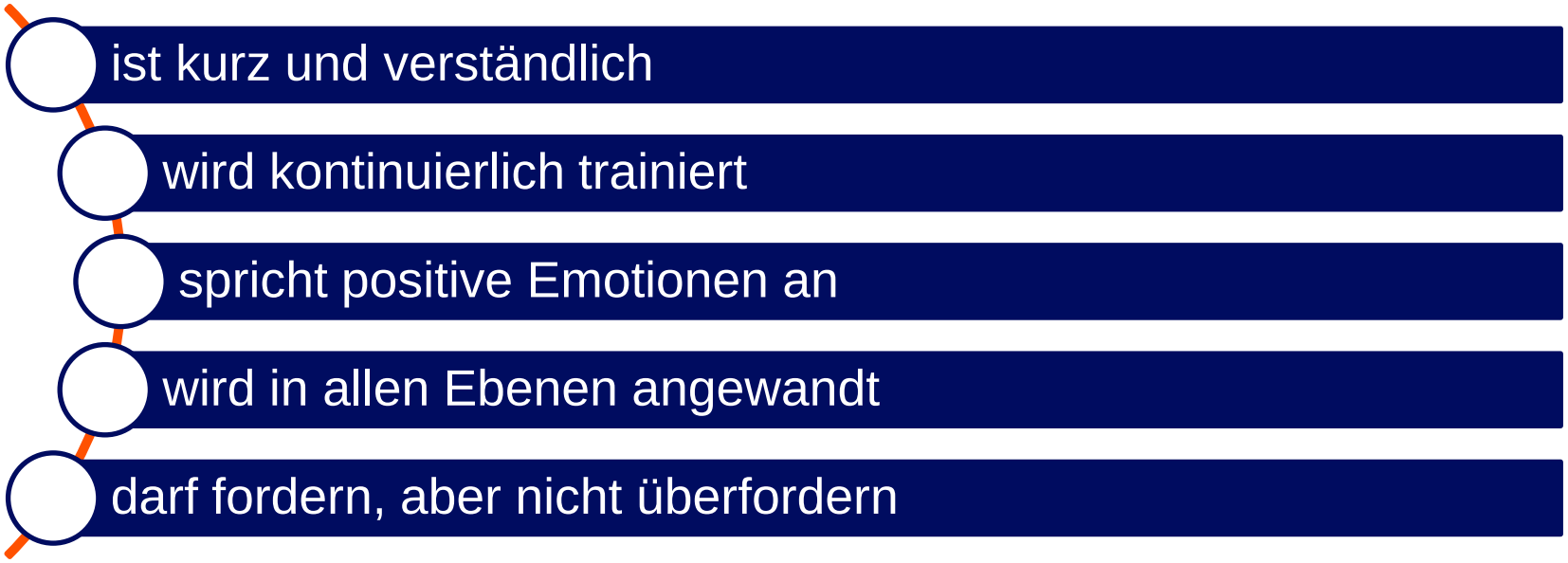
Klicken Sie hier zum Bestätigen Ihrer Daten

http://www.beispiel-bank.de

http://www.beispiel-bank.de-r-betrug.com/2015

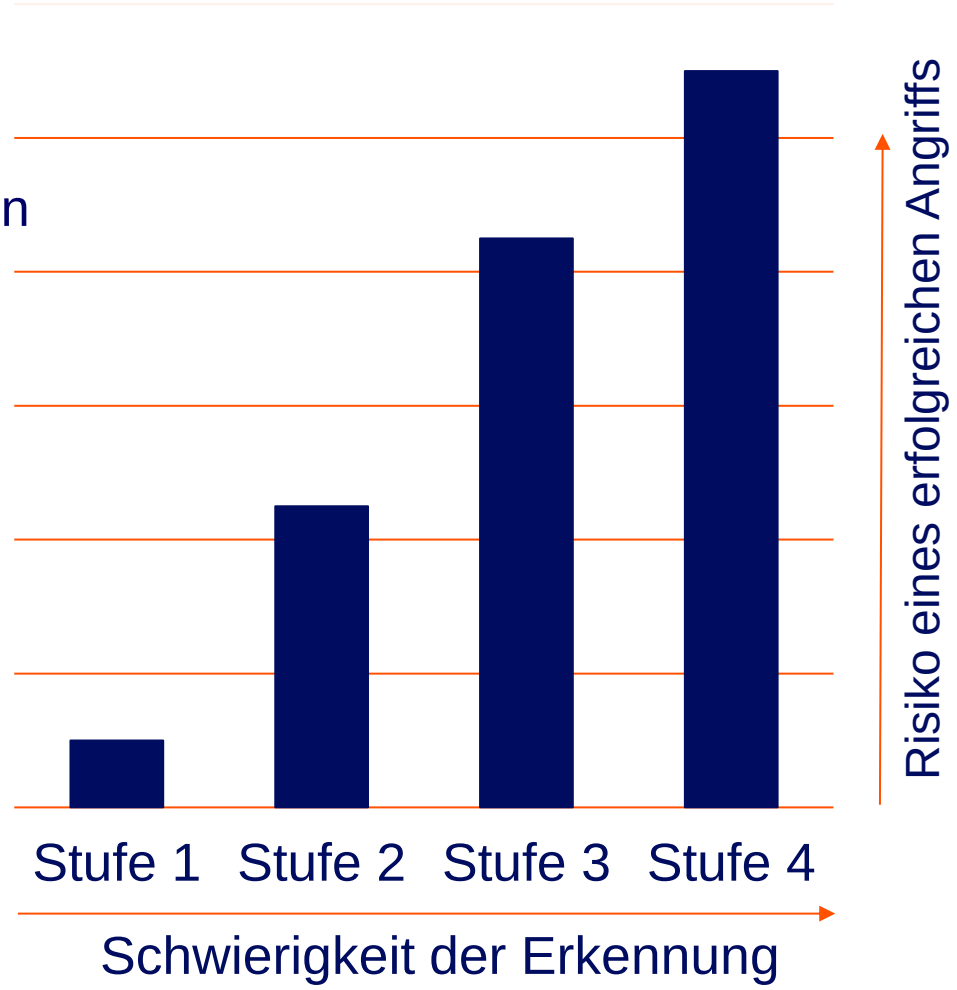
Patch Management

Ein gutes Security Awareness Programm…



Phishing Einstufung

- Personalisierter Kontext
- Tarnung von Links / Anhängen
- Personalisierte Begrüßung
- Tarnung des Absenders
- Korrekte Grammatik
- Korrekte Rechtschreibung
- Plausibilität des Inhalts
- Auslösen von Emotionen



Beispiel

Spear Phishing

Von: Web Master [webmaster@personalberatung.bsp]
Betreff: Übersicht der Anstellungen 2011
Anhang: Übersicht der Anstellungen 2011.xls

Ich leite dir diese Datei zur Überprüfung weiter. Bitte öffnen und ansehen.

Technische Maßnahmen - Mitarbeiter

E-Mail

- Verhaltens-Analyse
- Anhang-Filterung mit Sandbox Lösung
- Automatisiertes Öffnen in einer abgeschotteten Umgebung

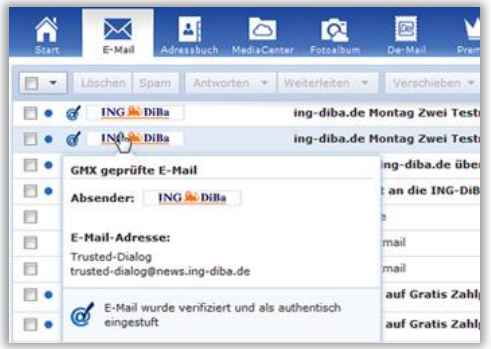
Web-Zugriff

- Whitelisting
- Gezielte Freigabe geschäftsrelevanter Webseiten
- Abgeschotteter Browser für reine Informationsbeschaffung

Technische Maßnahmen - Kunden

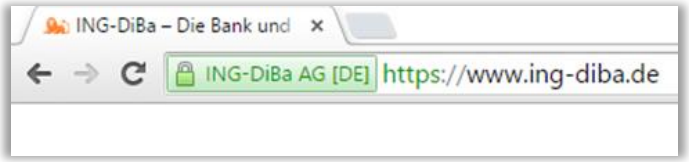
E-Mail

- SPF, DMARC, DKIM (DNS)
- Trusted Dialog



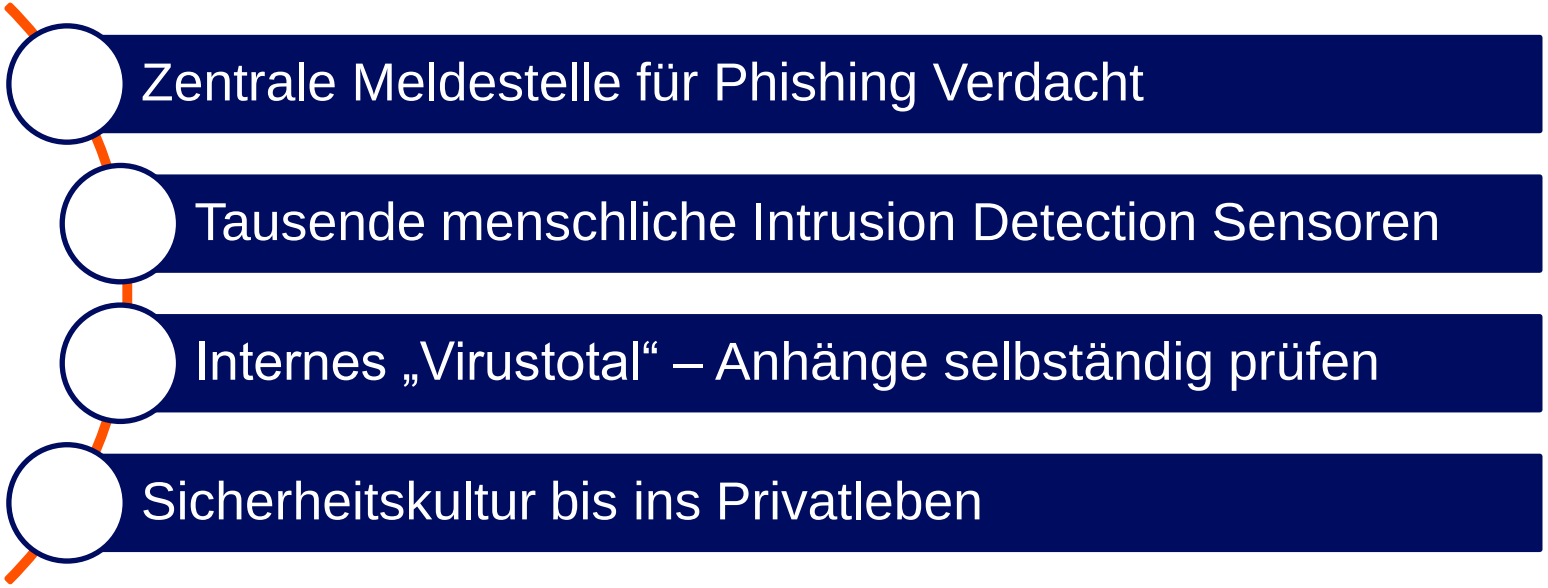
Web-Zugriff

- Extended Validation
  SSL Zertifikat



Security Empowerment

Besseres Zusammenspiel Mensch – Technik



Vielen Dank für Ihre Aufmerksamkeit

ING DiBa

Die Bank und Du

Social Engineering
Ausblick

Menschliche Bedürfnisse / Tendenzen

- Bedürfnis nach Bewunderung
- Sympathie für Ähnlichkeit
- Reziprokes Verhalten
- Hilfsbereitschaft
- Beständigkeit
- Autorität