Social Engineering

Dr. Lukas Feiler, SSCP

Associate, Wolf Theiss Rechtsanwälte GmbH

WOLF THEISS

TOPICS

1. Social Engineering Basics
2. Methoden des Social Engineering
3. Schutzmaßnahmen

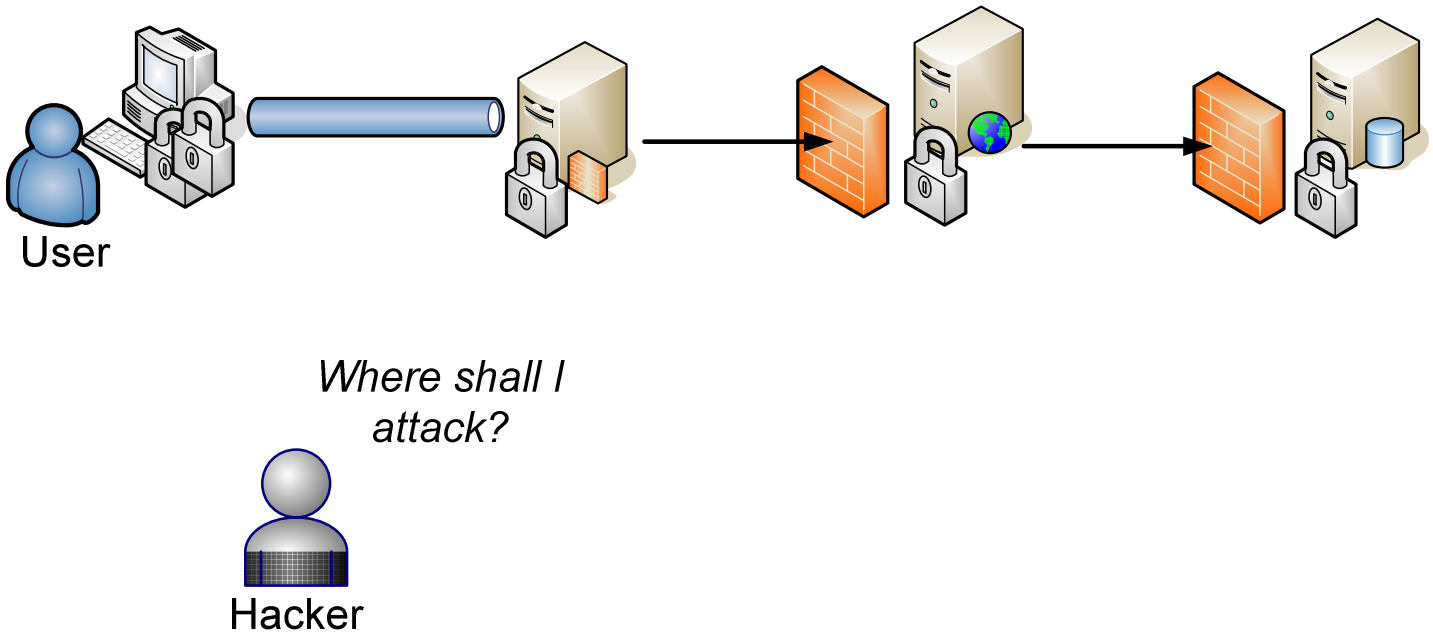
Social Engineering

- *Die Manipulation von Menschen zwecks Beeinträchtigung der Informationssicherheit*
  - zB:
    - E-Mail: “Dear Friend, … please don’t forget to install the new security update available on Microsoft’s website: www.micorsoft.com/critical-update-2012-09-13.exe”

- Informationssicherheit:
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit

  von Informationen

Sicherheitsarchitektur aus Sicht des Angreifers

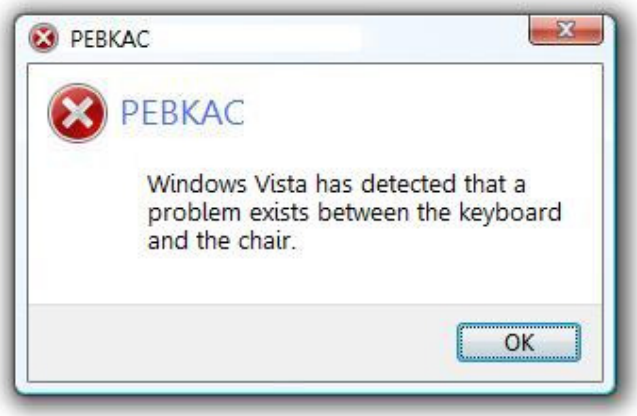


- Problem: Die Maschine muss mit Menschen interagieren; diese sind das schwächste Glied in der Kette

Schwachstelle Mensch

- „People often represent the weakest link“

  Bruce Schneier, Secrets and Lies (2000)
- PEBKAC Errors



- “Error in OSI Layer 8”

Methoden des Social Engineering

- Autorität wird vorgetäuscht
  - zB Täter ruft neuen IT-Mitarbeiter an, stellt sich als Sektionschef Müller vor und verlangt, dass sein Passwort zurückgesetzt wird, aber pronto
- Hilfsbereitschaft wird ausgenützt
  - zB Täter ruft bei älterer Mitarbeiterin an, stellt sich als neuer Außendienstmitarbeiter vor und fragt, ob sie ihm kurz ihr Passwort „borgen“ kann
- Zuneigung wird ausgenützt
  - zB Hackerin flirtet auf einer Fachmesse mit Systemadministrator eines Unternehmens und bringt ihn dazu, über die Schwachstellen in seinen Systemen zu erzählen

Methoden des Social Engineering #2

WOLF THEISS

- Glücksgefühl wird ausgenützt
  - Ein 50 GB USB-Stick wird verschenkt mit folgendem Inhalt
    - D:\malware.exe
    - D:\autorun.inf

      [autorun]

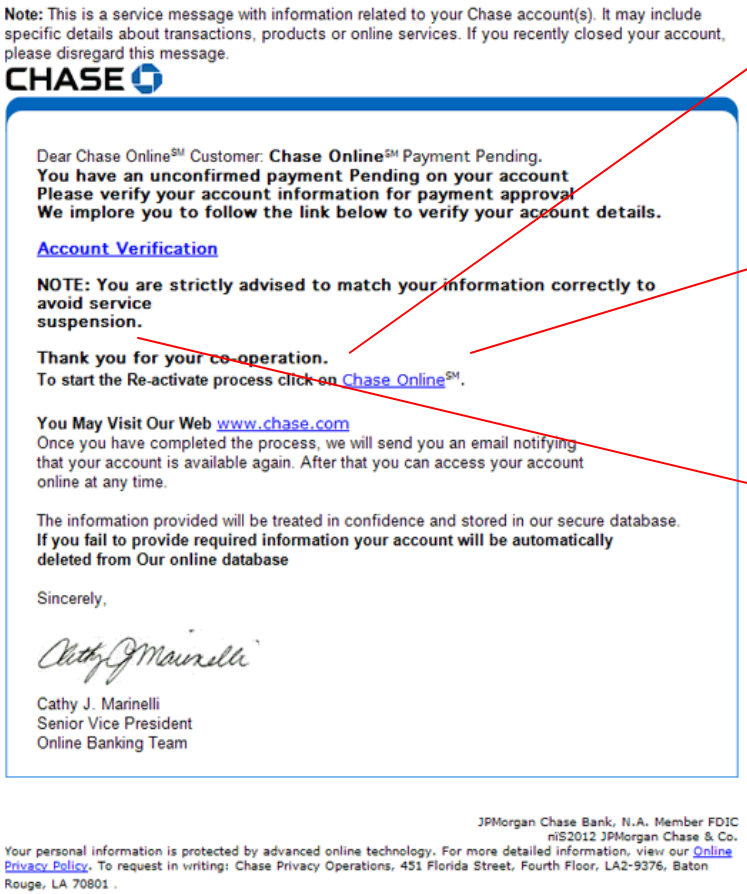
      open=malware.exe
  - „You can‘t cheat an honest man“

Erscheinungsformen: Manipulation des Gesprächspartners per Telefon

WOLF THEISS

- Täter will zB
  - Die Herausgabe eines Passworts
  - Die Vornahme einer Konfigurationsänderung
  - Die Herausgabe von Information, die dabei hilft einen Dritten zu täuschen
- In der Praxis selten – aber gefährlich!

Erscheinungsformen des Social Engineering – Phishing



Note: This is a service message with information related to your Chase account(s). It may include specific details about transactions, products or online services. If you recently closed your account, please disregard this message.

CHASE

Dear Chase Online℠ Customer: **Chase Online℠ Payment Pending.**
You have an unconfirmed payment Pending on your account
Please verify your account information for payment approval
We implore you to follow the link below to verify your account details.

Account Verification

NOTE: You are strictly advised to match your information correctly to avoid service suspension.

Thank you for your co-operation.
To start the Re-activate process click on Chase Online℠.

You May Visit Our Web www.chase.com
Once you have completed the process, we will send you an email notifying that your account is available again. After that you can access your account online at any time.

The information provided will be treated in confidence and stored in our secure database.
If you fail to provide required information your account will be automatically deleted from Our online database

Sincerely,

Cathy J. Marinelli
Senior Vice President
Online Banking Team

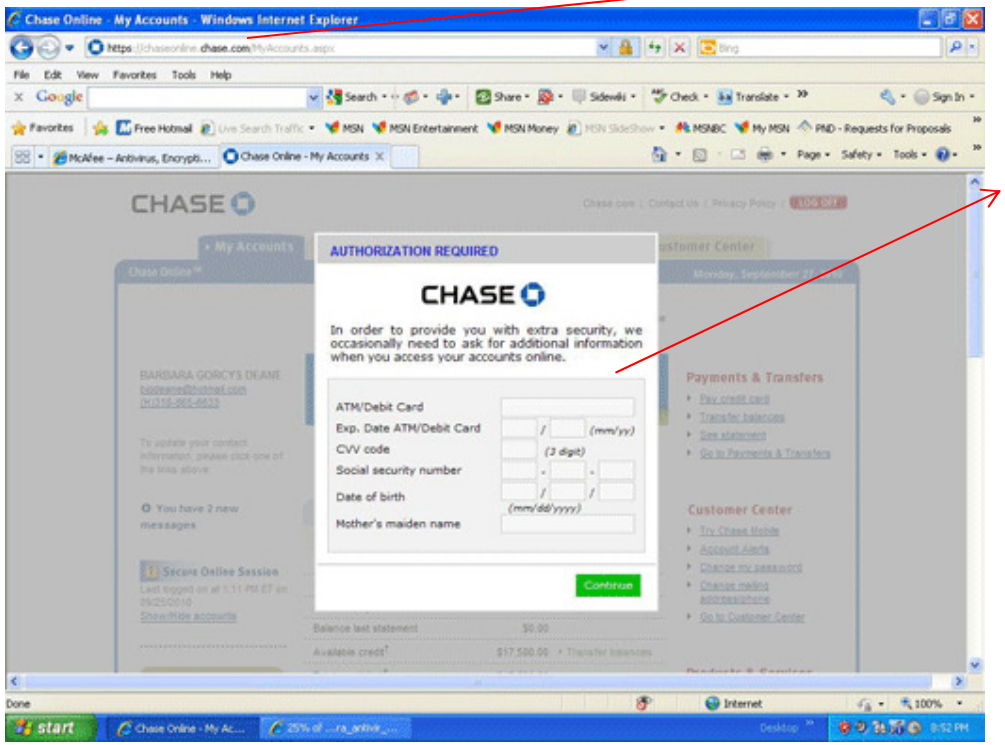
JPMorgan Chase Bank, N.A. Member FDIC
niS2012 JPMorgan Chase & Co.
Your personal information is protected by advanced online technology. For more detailed information, view our Online Privacy Policy. To request in writing: Chase Privacy Operations, 451 Florida Street, Fourth Floor, LA2-9376, Baton Rouge, LA 70801 .

1) Bad English

2) Fordert dazu auf, einen Link zu klicken

3) Drohung

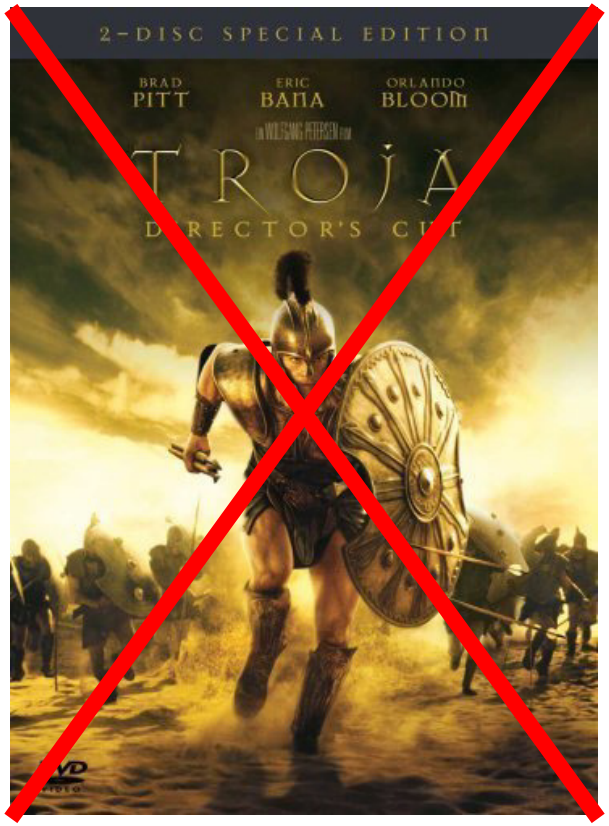
Erscheinungsformen des Social Engineering – Phishing



1) URL ist oft merkwürdig

2) Fordert dazu auf, Daten preiszugeben, die sonst nicht abgefragt werden; zB hier Kreditkarten-Nr., Ablaufdatum & CVV code

Erscheinungsformen: Trojaner/ trojanische Pferde



Welches Bild passt zur Malware?

Erscheinungsformen: Trojaner/ trojanische Pferde #2

- Nutzer installiert Software freiwillig
- Wird jedoch über die Neben-Funktionen der Software getäuscht
- zB
  - Gratis-Computerspiel, das einen Keylogger integriert hat
  - „Sicherheits-Update“, das Kreditkartendaten ausspioniert

Erscheinungsformen: „Identity Theft“

WOLF THEISS

- Was ist Identity Theft / Identitäts-Diebstahl?
  - Täter gibt vor, jemand zu sein, der er nicht ist
  - um sich einen Vorteil zu verschaffen
  - → Wird die Identität hierbei wirklich „gestohlen“?
    Hinweis: Stehlen = Jemandem anderen eine Sache wegnehmen
  - Treffendere Bezeichnung: Impersonation Fraud

Was tun gegen Social Engineering?

WOLF THEISS

- Ein Grundverständnis des Problems hilft:
  - In den meisten Fällen täuscht der Täter über seine Identität oder das Ausmaß seiner Berechtigung (wer ist er & was darf er?)

- Allgemeines Problem der Informations/IT-Sicherheit:
  - Wer bist du?
  - Welche Berechtigung hast du?

  → Man unterscheidet drei Konzepte:
    - Identification
    - Authentication
    - Authorization

Identification

- Prozess, in dem der Nutzer eine bestimmte Identität behauptet; zB
  - Eingabe eines Username
  - Eingabe einer E-Mail-Adresse
  - Nennen eines Namens am Telefon

Authentication

- Prozess der Überprüfung der behaupteten Identität
- Wie kann man eine Identitätsbehauptung prüfen?

  Drei mögliche Faktoren

  – Etwas, das der User weiß
  – Etwas, das der User hat
  – Etwas, das der User ist

Authentication: Factor 1 – Something You Know

- Beispiele?
  - Ein Passwort
  - Ein PIN
  - Die Sozialversicherungsnummer?
  - Der Mädchenname der Mutter?

- Welche Eigenschaften hat ein guter „Authenticator“?
  - Etwas, das nur der Nutzer weiß
  - Etwas, das schwer zu erraten ist
  - Etwas, das leicht zu merken ist
  - Etwas, das geändert werden kann, wenn es kompromittiert wird

Authentication: Factor 2 – Something You Have

- Beispiele?
  - Ein Schlüssel
  - Eine Magnetkarte / eine Chip-Karte
  - Ein Ausweis mit Namen
  - Ein Mobiltelefon
    - Variante 1: User wird angerufen/erhält ein SMS
    - Variante 2: User ruft an/sendet ein SMS

- Welche Eigenschaften hat ein guter „Authenticator“?
  - Etwas, das nur der Nutzer hat
  - Etwas, das schwer nachzumachen ist
  - Etwas, das geändert werden kann, wenn es kompromittiert wird

Authentication: Factor 3 – Something You Are

- Beispiele?
  - Iris-Scanner
  - Fingerprint-Reader
  - Sprach-Authentifizierung
  - Gesichts-Authentifizierung

- Welche Eigenschaften hat ein guter „Authenticator“?
  - Fälschlich positive Authentifizierung (False Positives) gering
  - Fälschlich negative Authentifizierung (False Negatives) gering

Authentication: Multi-Factor Authentication

- Ein Authentifikations-Faktor ist für viele Fälle zu schwach
- Häufig: Two-Factor Authentication
  - Amtliche Lichtbildausweis
    - Something you *have* (den Ausweis)
    - Something you *are* (Gesichtsmerkmale)
  - Chip-Karte mit PIN
    - Somthing you *have* (Chip-Karte)
    - Something you *know* (PIN)
  - E-Banking mit SMS-Tan
    - Something you *know* (Kundenkennwort zum Login)
    - Somthing you *have* (Mobiltelefon mit entsprechender Tel.Nr.)

Authorization

- Prozess der Ermittlung der Berechtigungen eines (authentifizierten) Nutzers
- Beispiele?
  - UNIX file permissions: read, write, execute (rwx)
  - Eine Person hat sich mit einem Lichtbildausweis authentifiziert; steht sie auch auf der Gästeliste (dh darf sie hinein)?

Beispiele für Identification, Authentication & Authorization

	Identifi-cation	Authenti-cation	Authori-zation
Zugang zu U.S. Federal Buildings nur mit amtlichem Lichtbildausweis	X	X	
Schlüssel zu Bankschließfach		X (1F)	
Username	X		
Passwort		X (1F)	
Ausweiskontrolle im Kino, um Altersbeschränkung durchzusetzen	X	X (2F)	X
„Bitte geben Sie Ihren Namen & Ihr Geburtsdatum ein, um sich einzuloggen“	X		
Sicherheitsfrage statt Passwort: Wie lautet der Mädchenname Ihrer Mutter?		X (~1F)	

Beispiele für Identification, Authentication & Authorization #2

	Identifi-cation	Authenti-cation	Authori-zation
Ich suche übers Internet eine Wohnung; potentielle Vermieterin bittet um eine Anzahlung; zuerst schickt sie mir eine Kopie ihres Reisepasses per E-Mail	X		
Access-Token meiner Kanzlei	(X)	(X)	X
Jemand, den ich nicht kenne, will (ohne, dass er einen Access-Token vorweist) mit mir in die Kanzlei. Ich frage: Wie heißt denn dein Chef?		X (1F)	X

Danke für die Aufmerksamkeit!

KONTAKTADRESSE

Dr. Lukas Feiler, SSCP

Wolf Theiss Rechtsanwälte GmbH
Schubertring 6, 1010 Wien

Tel: (+ 43 1) 515 10 5090
Fax: (+ 43 1) 515 10 665090

e-mail: lukas.feiler@wolftheiss.com

www.wolftheiss.com