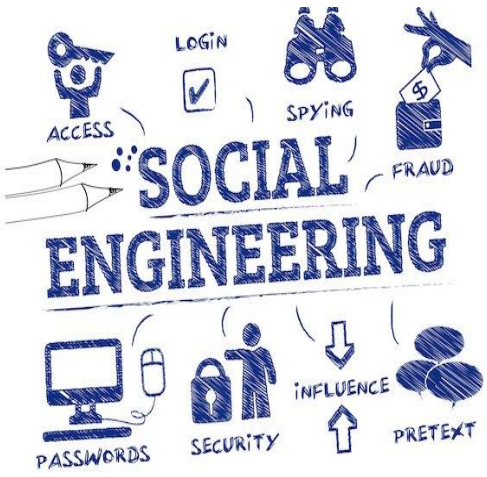

Version 1.1
1.3.2021

conus

www.conus.at

SOCIAL ENGINEERING IM IT BEREICH

EIN GRUNDSÄTZLICHER LEITFADEN FÜR UNTERNEHMEN, ADMINISTRATOREN UND MITARBEITER

Social Engineering - der Mitarbeiter als Angriffsziel

PRODUKTLINK:
https://www.conus.at/submain/links/partner_html_files/social_engineering.pdf

CONUS GmbH.
Kirchstetterngasse 47
1160 Wien
info@conus.at
+41 (0) 1 617 51 44 - 0

GENERELLE BESCHREIBUNG

Social Engineers nutzen menschliche Verhaltensweisen aus, um an Informationen oder Dienstleistungen zu kommen. Zu diesem Zweck spionieren sie zuerst oft das persönliche Umfeld ihres Opfers aus und täuschen falsche Tatsachen oder Identitäten vor.

Ziel der Aktion ist es, die Person zu beeinflussen und ein bestimmtes Verhalten zu erreichen. Das kann zum Beispiel die Preisgabe von vertraulichen Informationen sein, aber auch der Kauf eines Produktes oder die Freigabe von Finanzmitteln. Auch stellt z.B. der bekannte Enkel-Trick ein klassisches Beispiel für Social Engineering dar.

Oft hat diese Vorgangsweise zum Ziel, Zugang in ein fremdes Computersystem zu bekommen, um dort vertrauliche Daten einzusehen. Man spricht dann auch von **Social Hacking.**

Betrüger nutzen verschiedene Kommunikationswege, um einen Betrug durch soziale Manipulation auszuführen:

- Persönlich, telefonisch, postalisch, digital per E-Mail, Messenger, Chat, Einbruch

VORGANGSWEISEN IM IT BEREICH

Meist fokussieren sich Angreifer auf den wichtigsten Teil Ihres Sicherheitssystems: das Passwort, oder es wird ein Virus implantiert, welcher sofort, später oder viel später Daten nach außen sendet und/oder die IT zerstört. Denn damit können die meisten technischen Zugriffsbarrieren und Überwachungssysteme umgangen werden. Haben die Angreifer einmal Zugang zum Unternehmens-Netzwerk, werden dort vertrauliche Unternehmensinformationen abgesaugt: Kundendatenbanken, Verträge und Patente usw.

Die Einzige Abhilfe ist, jeder einzelne Mitarbeiter verwendet sein eigenes, sicheres Passwort und teilt dieses unter keinen Umständen mit anderen. Jeder neue Mitarbeiter (auch Aushilfen für wenige Stunden!) erhält einen eigenen Zugang.

Dieses Passwort darf niemals herausgegeben werden – weder unter Druck eines telefonischen Vorwands (z.B. eines „Supportanrufs“) noch schriftlich (z.B. per e-mail an anfragende „offizielle“ Institutionen), womöglich mittels Sticker am Monitor oder unterm Keyboard. Dies hebelt nicht selten die komplette IT-Sicherheit aus!

Auch scheinbar harmlose und alltäglich benutzte Geräte, E-Mails oder Webseiten stellen ein mitunter massives Sicherheitsrisiko dar.

Beispiele:

Betrüger benutzen USB-Geräte, um sich Zugang zu Netzwerken zu verschaffen. Auf USB Sticks, USB Ladegeräten von E-Zigaretten, sowie allen weiteren USB Geräten können sich versteckte Trojaner befinden, welche im Hintergrund eine Türe ins Netzwerk öffnen, sobald Sie das Gerät anstecken. Oftmals werden Produkte aus China mit solchen Hintergedanken verkauft.

Dasselbe gilt für Anhänge und Links von und in E-Mails. Auch in E-Mails können sich versteckte Trojaner befinden, welche im Hintergrund eine Türe ins Netzwerk öffnen und/oder einen Virus aktivieren, sobald Sie den Anhang öffnen. Man kann davon ausgehen, dass **jedes** e-mail von „seltsamen“ Absendern solche Schadsoftware enthält.

Ein Link kann auf Webseiten weiterleiten, welche zu Zweck haben, Informationen, wie z.B. Kontonummern, Passworte oder Logindaten zu erlangen. Oft gelangen Sie auf „offizielle“ Webseiten renommierter Unternehmen, welche zwar genau so aussehen, wie ihre Originale, jedoch nur gut nachempfundene Fallen darstellen. Jede, auf diesen Webseiten eingegebene Information wird zukünftig für Einbruch und Diebstahl benutzt. Oder es wird im Hintergrund ein Schadprogramm installiert, welches jede Aktion und jeden Tastenanschlag Ihres Arbeitsplatzes protokolliert, und diese Informationen an Betrüger übersendet.

DEFINITIONEN

Begriff	Methode
Phishing (abgeleitet von to fish, deutsch: fischen)	Massenhafte Versenden von betrügerischen Schreiben oder E-Mails, um an geschützte (private) Informationen zu erhalten z. B. PINs, Bankinformationen, Zugangsdaten
Spear Phishing (deutsch: speerfischen)	Gezielte Phishing-Angriffe auf ausgewählte Personen(gruppen), um Trefferquote zu erhöhen
Vishing (Kofferwort aus voice fishing)	Fingierte Telefonanrufe mithilfe von Voice over IP-Telefonie
CEO-Fraud/ CEO-Betrug	Gezielter Angriff auf Entscheider und Führungskräfte, auch Whaling genannt (deutsch: Walfang, dicke Fische angeln)
Pharming (Kofferwort aus phishing und farming, deutsch: züchten)	Manipulation von DNS-Anfragen von Webbrowsern Computer des Opfers wird so manipuliert, dass die Fake-Version einer häufig besuchten Website aufgerufen wird, auf der sich Opfer mit geschützten Zugangsdaten einloggen
Pretexting (deutsch: Vorwand verwenden)	Verwenden eines erfundenen Vorwands oder Szenarios, um Informationen vom Betrugsopfer zu erhalten, die es unter normalen Umständen nicht preisgeben würde z. B. fingierte E-Mails und Anrufe von Behörden, Polizei, Chef, Bank, Versicherer, Arbeitskollegen, Familienmitgliedern
Quid pro Quo (Gegenleistung einfordern)	Betrugsmasche, bei dem der Täter dem Opfer etwas anbietet und dann eine kleine Wiedergutmachung einfordert z. B. IT-Support bietet Hilfe, benötigt aber Passwort zur Verifizierung
Water holing (deutsch: Wasserloch-Strategie)	Opfer wird zu Fake-Version einer Website umgeleitet, die sie sehr häufig nutzen, dort werden private Daten erfragt oder zum Link-Klick aufgerufen Betrug basiert auf der Annahme, dass Nutzer auf vertrauten Websites viel bereitwilliger Informationen preisgeben oder Anweisungen folgen
Baiting (deutsch: ködern)	Opfer wird mit einem Köder (USB-Stick, CD, SD-Karte von vertrauenswürdiger Quelle oder Werbegeschenk) dazu gebracht, Datenträger zu verwenden, der Malware enthält
Tailgating (deutsch: Dichtes Auffahren-Strategie)	Höflichkeit des Opfers wird ausgenutzt, um Zugang zu einem abgesicherten Bereich zu erlangen z. B. Tür aufhalten, Handy ausleihen
Dumpster Diving (deutsch: tauchen im Müllcontainer)	Buchstäbliches Durchsuchen von Mülltonnen und Abfalleimern, um Informationen zu erhalten oder Anhaltspunkte für eine erfolgreiche Betrugsmasche zu finden

MASSNAHMEN FÜR UNTERNEHMEN UND ADMINISTRATOREN

Aufklärung der Mitarbeiter über das Risiko von Social Engineering! Motivieren Sie Ihre Mitarbeiter, in Sicherheitsbelangen auf Ihr „Bauchgefühl“ zu achten und einfach rückzufragen, wenn ihnen eine Situation komisch oder verdächtig vorkommt.

Definieren Sie, was alles vertraulich ist, und auch wo keinesfalls über vertrauliche Dinge gesprochen werden sollte. Ein belanglosens Plaudern im Kaffee an der Ecke kann schnell durch einfaches Mitlauschen durch Dritte zum Risiko werden.

Wiederholtes Lernen, Aufklären und Warnen - nur so können Menschen **dauerhaft für die Bedrohung von Social Engineering sensibilisiert** werden. Je größer das Bewusstsein für die Bedrohungslage, desto wahrscheinlicher ist die Entwicklung von Automatismen bei der Bewältigung der Arbeit.

Umsetzung:

- Warnungen zu aktuellen Betrugsmaschen versenden
- Schulungen zum Thema Social Engineering (verpflichtend) anbieten
- Klare Sicherheitsvorschriften und -richtlinien für die konkrete Umsetzung im Alltag aufsetzen
- Unangekündigte Simulationen durchführen

Die technischen IT-Sicherheitsmaßnahmen sollten Hand und Hand mit der Sensibilisierung der Mitarbeiter gehen:

- Striktes Zugangsmanagement für Anwendungen und Systeme
- Erforderliche Passwortänderungen in festgelegten Intervallen
- Update- und Patch-Management
- Monitoring von Logdaten
- Netzwerksegmentierung

Basierend auf einem Regelwerk prüft und reglementiert eine gut strukturierte, konfigurierte und gewartete Firewall in Echtzeit alle Daten-Pakete, die ausgetauscht werden und warnt im Falle von **Anomalien im Datenverkehr**. Außerdem können über eine Blacklist bekannte Phishing-Seiten standardmäßig gesperrt, oder über Whitelist Seiten geöffnet werden.

MASSANAHMEN FÜR MITARBEITER

Diese Maßnahmen betreffen alle Mitarbeiter und Geräte, welche wie auch immer Kontakt mit Daten und dem Netzwerk eines Unternehmens haben.

- Kennen Sie den Absender einer E-Mail nicht, sollten sie stets misstrauisch sein. Öffnen Sie dieses E-Mail nicht, oder fragen Sie gegebenenfalls **vorher** beim Absender nach.
- Öffnen Sie niemals Anhänge von E-Mails, die Sie nicht erwarten oder Ihnen „seltsam“ vorkommen. Weitere Indizien sind Rechtschreib- und oder Grammatikfehler, oder Links auf Webseiten, die Sie nicht kennen.
- Bei Anrufen dürfen wichtige Daten nicht an unbekannte Personen weitergegeben werden. Aber auch scheinbar unwichtige Daten („Der Kollege ist im Urlaub“) sollten nicht sorglos an Unbekannte weitergegeben werden. Sie können diese Informationen für weitere Angriffe nutzen.
- Seriöse Unternehmen oder Personen, die Sie nicht kennen, fragen telefonisch oder in E-Mails niemals nach vertraulichen Daten oder Netzwerkdaten (wie z.B. Anmeldedaten). Beantworten Sie Fragen dieser Art niemals!
- Geben Sie keine Mobiltelefonnummer oder Durchwahl von Vorgesetzten oder Mitarbeiter/innen an unbekannte Personen weiter. Bieten Sie stattdessen an, dass zurückgerufen wird.
- Bei Antworten auf eine E-Mail-Anfrage sollten unter keinen Umständen persönliche oder zahlungsrelevante Daten preisgegeben werden, egal von wem die Nachricht zu kommen scheint.
- Klicken Sie nicht auf Links aus E-Mails, die die Eingabe persönlicher Daten verlangen. Hinter der sichtbaren Adresse befindet sich oft eine andere Adresse! Geben Sie stattdessen die URL selbst im Browser ein. So vermeiden Sie gefälschte Websites. Weiters können Sie davon ausgehen, dass Webseiten, welche im URL nicht mit http**s**:// sondern mit http:// beginnen, und die Eingabe von Daten verlangen, betrügerische Webseiten sind. Darunter finden sich oft vermeintliche Webseiten namhafter und bekannter Unternehmen oder Banken.
- Bei Unklarheit über die Echtheit des Absenders oder die Authentizität der E-Mail, fragen Sie telefonisch nach. Die Rückrufnummer sollte aus einer unabhängigen Quelle stammen (Telefonbuch) und nicht aus dem vorangegangenen E-Mail oder Anruf.
- Sperren Sie konsequent den Bildschirm beim Verlassen des Arbeitsplatzes damit Betriebsfremde, die sich Zutritt zum Gebäude erschlichen haben, keinen Zugriff auf das Firmennetzwerk haben.
- Konsequentes Abräumen der Schreibtische am Ende des Arbeitstags
- Zugangspassworte werden nur dann zurückgesetzt, wenn der unmittelbare Vorgesetzte dies anordnet oder der Mitarbeiter persönlich beim Helpdesk vorspricht.
- Alle Mitarbeiter tragen deutlich sichtbar ihre Firmenausweise, Fremde sind leicht zu erkennen und alle Mitarbeiter nutzen, falls vorhanden, ihre elektronischen Zugangskarten.
- Alle Besucher werden beim Empfang abgeholt und sind nie unbeaufsichtigt im Gebäude oder auf dem Firmengelände.
- Benutzen Sie niemals USB-Sticks, bzw. schließen Sie keine Geräte an USB-Ports an. Generell ist das Benutzen von USB zu vermeiden.
- Senden oder empfangen Sie niemals Daten über Datendienste oder soziale Netzwerke. Wenn Firewalls nicht für diese Anwendungen konfiguriert sind, ist diese Art der Datenübertragung nicht sicher!