# SOCIAL ENGINEERING – RISIKOFAKTOR MENSCH

**PASCAL C. KOCHER**
B. Sc., E. M. B. L.-HSG, CEO Auditron GmbH Düdingen

Stichworte: Social Engineering, Hacking, Angriffstechniken

Hacker, auch Angreifer genannt, sind an Unternehmensdaten interessiert. Diese gestohlenen Daten werden teilweise öffentlich publiziert, an die Konkurrenz verkauft oder dienen als Grundlage für eine Lösegeldforderung. Zunehmend sind auch kleine und mittlere Unternehmen von solchen Angriffen betroffen. Auch Anwaltskanzleien können davon betroffen sein. Dieser Beitrag widmet sich dem sogenannten Social Engineering – einer spezifischen Angriffsmethode – und wie sich Anwaltskanzleien davor schützen können. Sie werden verstehen, wie Social Engineering den Dow-Jones-Index im Jahr 2013 um 150 Punkte nach unten bewegen und einen geschätzten wirtschaftlichen Schaden von knapp 140 Milliarden Dollar verursachen konnte.

## I. Social Engineering

Social Engineering ist die Kunst, zwischenmenschliche Beziehungen auszunutzen, um an geschützte oder vertrauliche Informationen zu gelangen. Durch verschiedene Methoden gelangt der Social Engineer meist unbemerkt (oder zumindest ohne Verdacht zu erwecken) an sein Ziel. Ein simples Beispiel: Um das Kennwort eines Benutzers zu beschaffen, genügt es, den Benutzer nach seinem Kennwort zu fragen. In den meisten Fällen gibt der Benutzer dem Angreifer das Passwort bereitwillig heraus (falls das Passwort nicht schon im vornherein «123456» oder «password» war).

### *1. Phishing – Informationsbeschaffung per E-Mail*

Die bekannteste Social-Engineering-Technik ist das sogenannte *Phishing.* Wie der Name es verlauten mag, geht es um das Fischen. Spezifisch um das Fischen von Informationen von Hacking-Opfern. Phishing wird in den meisten Fällen per E-Mail durchgeführt. In diesem Fall wird dem Opfer eine möglichst gut gefälschte E-Mail geschickt, in der Hoffnung, dass dieses auf den Anhang oder die enthaltenen Links klicken wird. Auf den ersten Blick können gute Phishing-E-Mails nicht direkt als solche erkannt werden. Sie scheinen von einer bekannten, vertrauenswerten Quelle gesendet zu werden. Der Inhalt der E-Mail ist vielmals so gut gestaltet, dass der User neugierig wird. Beispielsweise kann eine solche E-Mail suggerieren, dass der Absender eine Vertragspartei aus dem IT-Bereich sei und eine Passwortänderung erfolgen müsse, oder kann von einem Bewerber für eine ausgeschriebene Stelle kommen, der ein infiziertes Dokument angehängt hat. In beiden Fällen wird der Computer des Users, sollte dieser der Anleitung folgen, infiziert. In einem solchen Fall hat der Hacker Zugriff auf die ihm fälschlicherweise übertragenen Daten (z. B. Kreditkartendaten) oder er hat uneingeschränkten Zugang zum Computer des Opfers.

Um sich vor Phishing zu schützen, muss man sich jeweils überlegen, in welchen Fällen solche Informationen effektiv angefragt werden könnten. Eine Bank beispielsweise wird nicht via E-Mail (oder Telefon) den Kunden nach seinem Passwort fragen. Geben Sie unter keinen Umständen ihr Passwort via E-Mail oder Telefon an eine Person weiter, auch wenn sich diese Person als IT-Fachmann ausgibt und vorgibt, ein Problem lösen zu wollen. Aus Sicht der IT gibt es kaum einen Grund, warum das Passwort eines Benutzers benötigt wird. Dasselbe gilt auch, wenn eine Person von Ihnen verlangt, Ihr Passwort auf ein vorgegebenes Passwort zu ändern. Wechseln Sie das Passwort nur auf ein ausschliesslich Ihnen bekanntes Passwort. Lassen Sie sich in der Wahl des Passwortes nicht beeinflussen oder gar ein Passwort vorgeben.

Falls Sie eine unerwartete E-Mail mit einem Anhang erhalten, seien Sie immer wachsam vor dem Öffnen des Anhanges. Auch wenn der Absender auf den ersten Blick bekannt erscheint (z. B. eine Kollegin oder ein Kollege), kann die E-Mail-Adresse durchaus gefälscht sein. Den Absender können Sie mit einem einfachen Trick prüfen, indem Sie auf «Antworten» klicken und die (jetzt) Empfänger-E-Mail-Adresse genau prüfen. Erscheint in diesem Fall eine Ihnen unbekannte E-Mail-Adresse, können Sie den Anhang ignorieren bzw. sollten Sie diesen löschen.

Auch wenn der Absendertest keine Unregelmässigkeiten aufwies, kann der Anhang trotzdem infiziert sein. In

diesem Falle, falls Sie den Anhang immer noch öffnen müssen, empfiehlt es sich, den Anhang nicht direkt aus dem E-Mail-Programm zu öffnen, sondern erst auf dem PC zu speichern und durch die Antivirensoftware prüfen zu lassen. Bei weiterem Verdacht sollten Sie vor dem Öffnen mit dem Absender des Anhanges telefonisch Kontakt aufnehmen und spezifisch nach dem Anhang fragen. Dies beseitigt in den meisten Fällen sämtliche Missverständnisse.

Bei Links, Buttons und Aufforderungen zum Klicken in E-Mails sollten Sie besonders vorsichtig sein. Bevor Sie auf den Link klicken, zeigen Sie mit dem Mauszeiger darauf und nach kurzer Zeit erscheint die Webseitenadresse des Links. Diese Webseitenadresse muss genau mit der Firma übereinstimmen, die die Webseite betreibt. Sollten Sie Bedenken haben, klicken Sie lieber nicht auf den Link. Insbesondere Wettbewerbe, Anfragen nach Kreditkartendetails, Bankinformationen und Gratis-iPads sollten Ihr Misstrauen wecken. Alternativ können Sie im Internetbrowser auch nach der gewünschten Information suchen, ohne Copy-Paste aus der E-Mail.

Sobald etwas in einer E-Mail ein bisschen Misstrauen weckt, sollten Sie weder Anhänge öffnen noch Links klicken. Sind Sie dennoch auf die Daten angewiesen, fragen Sie am besten ihren Verantwortlichen für die IT-Sicherheit.

### *2. Whaling – Angriff auf die grossen Fische*

Whaling ist eine spezielle Art von Phishing. Das Ziel beim Whaling sind die grossen Fische – typischerweise im höheren Management. Die bekannteste Art von Whaling ist der CEO-Betrug (CEO fraud). In diesen Szenarien erhält ein Mitglied der Geschäftsleitung mit Zahlungsberechtigung eine vermeintliche E-Mail des CEO oder Geschäftspartners mit der Aufforderung, eine Zahlung ins Ausland vorzunehmen. Typischerweise wird in der E-Mail erklärt, die Zahlung sei dringend. In vielen Fällen befindet sich der Absender der E-Mail auch effektiv im Ausland oder gar in den Ferien. Wird dieser Zahlungsaufforderung nun effektiv Folge geleistet, ohne mit dem richtigen Absender der E-Mail Rücksprache zu nehmen, ist das Geld in vielen Fällen verloren.

Spezifisch gegen CEO-Betrug ist es sinnvoll, für Zahlungen ab einem gewissen Betrag das Vieraugenprinzip walten zu lassen, d. h., eine Einzelperson sollte keine Überweisung selbstständig durchführen können. In den meisten Fällen hilft eine kurze telefonische Rückfrage mit dem CEO oder dem Kanzleipartner, ob dieser Geldtransfer tatsächlich vorgesehen sei. Die Höhe der Beträge für solche Überweisungsanfragen liegt im Schnitt bei USD 150 000, d. h. für solche Fälle, sollte der CEO oder Kanzleipartner in den Ferien kurz gestört werden dürfen.

### *3. Fischen mit Speeren – Spear Phishing*

Beim normalen Phishing-Angriff werden die E-Mails breit gestreut, in der Hoffnung ein Opfer zu treffen. Spear Phishing ist identisch mit einem normalen Phishing-Angriff, mit der Ausnahme, dass das Ziel präzise ausgewählt wird. Eine E-Mail kann spezifisch auf eine Firma oder gar auf eine Person abgestimmt werden, sodass dies kaum mehr von normalen Firmen-E-Mail unterschieden werden kann. Diese Art des Angriffes ist besonders heimtückisch, da sich die meisten User kaum Gedanken bei «firmeninternen» bzw. «kanzleiinternen» E-Mails machen. Die Wahrscheinlichkeit eines Erfolges bei diesen Angriffen ist sehr hoch, entsprechend genauer muss der Benutzer auch hinschauen, um nicht in die Falle zu tappen. Die Methoden zur Erkennung von Spear Phishing sind dieselben wie für Phishing.

### *4. Vishing – Telefonverkauf für Hacker*

Wenn der Angriff nicht via E-Mail stattfindet, sondern via Telefonanruf, spricht man von Vishing (Voice Phishing). Bei Telefonanrufen sollten Sie es möglichst vermeiden, zu viele Informationen weiterzugeben. Dies kann einerseits Ihr Passwort betreffen (siehe oben) oder die Ferienabwesenheiten Ihrer Arbeitskollegen. Kommt Ihnen der Telefonanruf verdächtig vor, verlangen Sie eine Rückrufnummer und rufen Sie den Anrufer später zurück.

Dasselbe gilt, wenn Aufforderungen per SMS kommen (Smishing, SMS Phishing). Hinterfragen Sie den Grund der SMS – Ihre Bank beispielsweise schickt Ihnen höchstens Informationen. Sollten Sie eine SMS bekommen, dass Ihre Kreditkarte gesperrt wurde, rufen Sie nicht die Nummer in der SMS an, sondern die Nummer auf der Rückseite Ihrer Kreditkarte.

### *5. Shoulder Surfing – der Feind auf der Schulter*

Shoulder Surfing ist ein Social-Engineering-Angriff, bei dem der Angreifer Ihnen über die Schulter auf Ihrer Tastatur schaut. Geschieht dies während Sie Ihr Passwort eingeben, ist dem Angreifer dieses oder Teile davon bekannt. Speziell bei der Nutzung von Smartphones oder Tablets im öffentlichen Raum sollten Sie besonders vorsichtig sein. Die Geräte haben die Tendenz, dass die gedrückten Tasten des PIN-Codes noch eine kurze Zeitlang nachleuchten. Lange genug, damit der Angreifer hinter Ihnen im Tram sich den PIN-Code merken kann.

Arbeiten Sie mit einem Computer oder Tablet, stellen Sie sicher, dass niemand zuschauen kann, während Sie Ihr Passwort eintippen. Wählen Sie auf Tablets und Smartphone möglichst auch ein längeres Passwort und nicht einen vierstelligen PIN-Code. Sollten Sie das Sitzungszimmer kurzzeitig verlassen, sperren Sie jeweils Ihren Computer oder lassen Sie diesen nicht unbeaufsichtigt bei unbekannter oder neuer Klientel.

### *6. Eavesdropping – das Mithören von Gesprächen*

Kanzleien sind bei Diskussionen über Fälle und Klienten von Berufs wegen bereits vorsichtig. Andere Branchen sind in diesen Fällen weniger vorsichtig. Die Erfahrung macht jeder, der zu Stosszeiten in der 1. Klasse im Zug von Bern nach Zürich fährt. Dennoch gibt es auch für Kanzleien Bedrohungsszenarien, in denen potenzielle Informationen mitgehört werden können.

Diese Szenarien treten meist dort auf, wo sich die Gesprächspartner unbeobachtet fühlen. Das klassische Beispiel ist die Toilette. Kurz zuvor war noch eine hitzige Ver-

handlung im Sitzungszimmer im Gange und nun gibt es eine kurze Pause. Denken Sie daran, bevor Sie die Debatte auf der Toilette weiterführen, dass die Toilette potenziell nicht leer sein könnte.

Schwieriger wird es bei der Nutzung von Mobiltelefonen bei vertraulichen Gesprächen. Ohne das Mobiltelefon aktiv zu nutzen, kann – sollte dieses vorher infiziert worden sein – durch einen Angreifer das Mikrofon aktiviert und der Raum belauscht werden. Die Mobiletelefone sind die neuen Wanzen, sogar vom Abgehörten selbst mitgebracht.

Das Einfachste ist es, Mobiletelefone grundsätzlich aus den Sitzungszimmern mit vertraulichen Inhalten zu verbannen. Möchten Sie oder ein Teilnehmer jedoch einen wichtigen Anruf nicht verpassen, können Sie die Mobiltelefone in Konfitürengläser einschliessen und vor ihnen auf dem Sitzungstisch in Sichtweite zu deponieren. Dies erlaubt es Ihnen Anrufe und SMS auf dem Telefon zu sehen, der Angreifer jedoch wird Schwierigkeiten haben, aus dem Konfitürenglas heraus etwas verstehen zu können.

#### *7. Der physische Zugang*

Ein Angreifer mit physischem Zugang zu den Büros oder Servern hat grundsätzlich ein leichtes Spiel. In vielen Fällen wird der Zutritt zu den Büros in Unternehmen durch Sicherheitstüren und Vereinzelungsanlagen geschützt, die Unberechtigten den Zugang erschweren. In Anwaltskanzleien existieren solche Zutrittsbarrieren jedoch äusserst selten. In einer Kanzlei ist der primäre Angriffspunkt das Sitzungszimmer. In vielen Fällen werden die Gäste in diesen Zimmern für eine gewisse Zeit unbeaufsichtigt gelassen, bis das Sekretariat die Anwältin oder den Anwalt informiert hat. Falls ein Sitzungszimmer mit Netzwerkanschlüssen ausgestattet sein sollte, müssen diese besonders gesichert werden. Der Angreifer kann in diesem Falle entweder den nicht gesicherten Netzwerkanschluss nutzen, um mit seinem Laptop auf Kanzleidaten zuzugreifen, oder er steckt beispielsweise hinter der Verschalung ein Gerät an das Netzwerk, das ihm nachträglich noch Zugang ermöglicht.

Besonders vorsichtig sollten Sie sein, wenn Sie einen USB-Stick (oder einen anderen Datenträger) bekommen mit Daten, beispielsweise Dokumente oder Verträge zum Ausdrucken. Prüfen Sie diese Datenträger immer zuerst mit Ihrer Antivirensoftware. Falls Sie den USB-Stick auf dem Parkplatz gefunden haben sollten, stecken Sie diesen erst gar nicht ein. Aus unserer Erfahrung werden gefundene USB-Sticks von der Hälfte der Finder in den Computer eingesteckt – eine verheerende Statistik.

Nach getaner Arbeit im Sitzungszimmer, begleiten Sie den potenziellen Mandanten bis zur Eingangstüre, denn auf dem Weg dahin gibt es für einen Angreifer – falls unbeobachtet – viele Verlockungen. Hierbei kann auch das sensibilisierte Sekretariatspersonal Wunder bewirken.

#### *8. Reverse Social Engineering*

Ein bekanntes Szenario ist auch das Reverse Social Engineering, d. h. das umgekehrte Social Engineering. In diesem Fall wird eine Situation geschaffen, in der das Opfer selbstständig auf den Angreifer zugeht. Hierzu gibt sich beispielsweise der Angreifer als Computerfachmann aus und stellt sicher, dass das Opfer diese Rolle auch bewusst wahrnimmt. Im zweiten Schritt stellt der Angreifer sicher, dass das Opfer ein Problem mit seinem Computer bekommt, z. B. durch das unbeobachtete Entfernen der Netzwerkverbindung. Da das Opfer nun nicht mehr Arbeiten kann und Hilfe benötigt, ist die Wahrscheinlichkeit gross, dass es sich an den Angreifer wendet, um Hilfe zu bekommen. Hier schliesst sich der Kreis und der Angreifer bekommt so Zugang zum Computer des Opfers.

### II. Massnahmen gegen Social Engineering

Social Engineering ist eine Angriffsmethode, die an allen technischen Sicherheitslösungen vorbei funktioniert. Keine Firewall und kein Antivirusprodukt, d. h. keine technische Massnahme kann Social Engineering erkennen oder verhindern. Das Angriffsziel ist immer der Mensch – als schwächstes Glied in der Kette der Sicherungsmassnahmen.

#### *1. Social Engineering und Dow Jones*

Im Jahr 2013 erhielten Mitarbeiter der Associated Press folgenden E-Mail. Dazu ist zu sagen, dass Pressebüros permanent E-Mails bekommen, um auf News aufmerksam zu machen.

Sent: Tue 4/23/2013 12:12 PM
From: [Ein AP Mitarbeiter]
Subject: News
Hello,
Please read the following article, it's very important:
http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/23/
[Ein anderer AP Mitarbeiter]
Associated Press
San Diego
mobile [entfernt]

Schauen Sie sich die E-Mail genau an und überlegen Sie sich, ob Sie diesen wichtigen Artikel lesen möchten. Die Webseitenadresse sieht korrekt aus. Einziges Detail ist, dass der Absender der E-Mail und die Signatur in der E-Mail nicht übereinstimmen. Wer auf den Link geklickt hatte, wurde auf eine täuschend echte Seite geleitet und wurde aufgefordert die Login-Informationen anzugeben, um die Informationen lesen zu können.

Ziel des Angriffes war das Twitter-Konto der Associated Press. Sobald die Angreifer diese Login-Informationen hatten, wurde folgende, falsche Twitter-Meldung auf dem Konto der Associated Press publiziert. *«Breaking: Two Explosions in the White House and Barack Obama is injured».* Dieser Tweet wurde um 13.07 Uhr versendet. Um 13.10 Uhr stabilisierte sich der Dow-Jones-Index 150 Punkte tiefer als drei Minuten zuvor. In diesen drei Minuten wurden knapp 140 Milliarden US-Dollars «vernichtet». Diese schnelle

Reaktion auf den Tweet liegt unter anderem auch an der Hochautomatisierung der Handelssysteme, die neben vielen anderen Kanälen auch Twitter überwachen.

### *2. Ein Update für den Menschen – nicht nur für die Maschine*

Im Social Engineering wird grundsätzlich mit Ausreden oder speziellen Vorwänden gearbeitet, um das Opfer zu einer Aktion zu verleiten. Dies wird in einem Szenario zusammengestellt, um möglichst effizient an die entsprechenden Daten heranzukommen. Speziell, wenn mit Zeitdruck gearbeitet wird, d. h. es wird von Ihnen unmittelbar eine Aktion verlangt, sollten Sie misstrauisch werden. Dasselbe gilt für ungewöhnlich viel Lob und Charme. Der Mensch ist ein einfaches Ziel für Social Engineering, weil man freundlich ist; man hält der nachfolgenden Person die Türe auf. Ob diese Person aber wirklich durch die Türe darf, wird in vielen Fällen – gerade morgens bei Eingang in das Bürogebäude – selten hinterfragt.

Um den Menschen gegen Social Engineering sicher zu machen, muss auch hier jeweils ein «Update eingespielt» werden. Das heisst, der Benutzer muss regelmässig daran erinnert werden, dass Social Engineering existiert und dass er vorsichtig sein soll. In der Praxis wird dies durch interne oder externe Sensibilisierungskampagnen erreicht. Die Benutzer werden in Schulungen (auch online) jeweils regelmässig daran erinnert, vorsichtig zu sein und auf ihren Bauch zu hören. Ebenfalls regelmässige Tests erhöhen die Sensibilität der Mitarbeiter. Testweise verschickte Phishing-Kampagnen dienen einerseits dazu, den Nutzen der Schulungen zu messen, und andererseits hilft dies jedes Mal auch bei der Sensibilisierung der Mitarbeiter.

Grundsätzlich kann man sagen, dass, wenn etwas faul erscheint, es dies in den meisten Fällen auch ist. Lassen Sie sich nicht unter Druck setzen und hören Sie auf Ihren Bauch. Dieser ist das beste Mittel gegen Social Engineering. Wenn sich eine Situation komisch anfühlt und Sie misstrauisch werden, kann dies durchaus seinen Grund haben.