Angriffsziel Mensch

Quelle: shutterstock

Der Mensch ist das schwächste Glied in der Informationssicherheitskette. Dieser Tatsache bedienen sich so genannte «Social Engineering-Angriffe». Technische Sicherheitsmassnahmen bieten keinen Schutz vor nichttechnischen Angriffen!

WOLFGANG SIDLER

Mit Social Engineering können zwischenmenschliche Beziehungen zur Manipulation genutzt werden, um unerlaubt an Informationen zu gelangen. Das Ziel ist das Ausspionieren des persönlichen Umfeldes eines ausgewählten Opfers. Dies geschieht vielfach mit der Vortäuschung falscher Identitäten oder der Nutzung von Verhaltensweisen, um an geheime Informationen oder gewinnbringende Daten zu gelangen. Meist dient dies dem Einstieg in ein fremdes Computersystem, welches vertrauliche Daten beherbergt. Diesen Vorgang nennt man auch Social-Hacking.

Eine bestens bekannte Form des Social Engineerings ist das Phishing. Das Prinzip: Der Social Engineer sendet dem potenziellen Opfer ein E-Mail und operiert mit dem Schein einer vertrauenswürdigen Seite. Er lässt den Benutzer glauben, dass es zwingend notwendig sei, das Mail zu beantworten. So wird der Empfänger aufgefordert, seine geheimen Zugangsdaten wie Passwörter usw. zu erfassen. Der Angreifer braucht in diesem Fall nichts mehr als die E-Mail-Adresse des Empfängers, ein bisschen Glück und Geduld. Durch die unpersönliche Form des Phishings ist die Wirksamkeit zwar begrenzt, aber nicht minder gefährlich.

Social Engineering kann grob in zwei unterschiedliche Angriffsarten gegliedert werden:

Computer Based Social Engineering

Dieses basiert, wie der Name schon sagt, auf der Verwendung des Computers, um an die gewünschten Informationen zu gelangen. Dazu ein Beispiel: Ein Social Engineer verschickt Massen-Mails, gibt sich als Mitarbeiter des Online-Auktionshauses eBay aus und versucht so, an Kreditkartennummern und andere persönliche Daten heranzukommen. In seiner Massen-Mail bestätigt er den Kauf eines erfundenen Artikels und gibt als Stornierungsseite www.ebay.com.rr.nu an. Auf dieser gefälschten Seite kann der Kauf mit der Eingabe der Kreditkartennummer storniert werden.

Human Based Social Engineering

Bei dieser Variante wird versucht, die gewünschten Informationen direkt von den Opfern zu erhalten, indem der Social Engineer mehr oder weniger geschickt danach fragt. Dazu ein Beispiel: Ein Angreifer gibt sich am Telefon als Mitarbeiter der Informatikabteilung aus und fragt das Opfer nach seinen Passwörtern. Subtiler ist folgende Angriffsart: Der Social Engineer verursacht dem Opfer ein Problem und tritt als Retter in der Not auf. Er verschafft sich so das Vertrauen des Opfers und erhält die gewünschten Informationen. Ein weiteres lohnenswertes Ziel der Social Engineers ist das Durchwühlen von Mülltonnen. Studien zeigen immer wieder, wie sorglos Firmen mit ihrem Müll umgehen. Oft können in Mülltonnen interne Telefonbücher, Kalender, Notizen, Ausdrucke von vertraulichen Dokumenten, Systemhandbücher, Ausdrucke von Benutzernamen mit Passwörtern, Ausdrucke von Source Code, Disketten, Backup Tapes oder alte Hardware gefunden werden. Informationen dieser Art sind für einen Social Engineer äusserst wertvoll und erleichtern ihm den Weg ins System erheblich.

Einfallstor Mensch

Der Mensch als Tor zu sensiblen Informationen. Die sechs typischen Schritte einer Social Engineering-Attacke:

1. Informationen beschaffen (z.B. im Internet, Google, Adressverzeichnisse usw.)
2. Aufbauen eines Vertrauensverhältnisses (Insider, Gewohnheiten usw.)
3. Gezielte Manipulation von Personen, um an die gewünschten Informationen zu gelangen (Lieferanten, Techniker, Journalist, usw.)
4. Aunutzen von menschlichen Eigenschaften, um das Opfer zu bestimmten Aktionen zu verleiten (um Hilfe fragen, Auskunft verlangen usw.)
5. Angriffe auf IT-Systeme oder Diebstahl von Daten und Passwörtern über Menschen (Bestechung, Erpressung, usw.)
6. Personen ohne Fachwissen zu sicherheitsgefährdenden Aktionen bewegen.

Social-Engineering-Attacken werden immer raffinierter und nehmen zu. Ein gekonntes und autoritäres Auftreten macht es möglich. Besonders so genannte kommerzielle Spionage-Software (Spyware, Trojaner) bzw. Überwachungsprogramme werden heute in Kombination mit Social-Engineering-Attacken eingesetzt. Viele dieser Spionage-Programme und Kniffs werden von den Antiviren-Scannern nicht erkannt. Einige nichttechnische Beispiele aus der Praxis:

► Mitlaufen in einer Gruppe Mitarbeiter, welche das Gebäude betreten.
► Beschäftigt telefonierend in den Aufzug marschieren und warten, bis dieser von jemandem in ein oberes Stockwerk gerufen wird.
► Beschäftigt telefonierend an anderen Zu- oder Ausgängen warten, bis jemand die Tür öffnet und diese dann für den unberechtigten Zutritt nutzen.
► Als z.B. Getränke-Lieferant getarnt sich Zugang verschaffen.
► Guten Tag Frau Müller, hier ist Herr Meier von der IT. Wir haben gerade ein grosses Systemproblem und brauchen unbedingt Ihre Hilfe. Wie lautet Ihr Passwort?
► Beim Personaleingang: Entschuldigen Sie, ich habe meinen Badge vergessen.
► Ein Social Engineer wartet in der Toilette, bis die Belegschaft in ihren wohl verdienten Feierabend geht.
► Zum Reinigungspersonal: Entschuldigen Sie, ich habe meinen Aktenkoffer im Büro liegen gelassen und den Schlüssel im Auto.

Erfahrungen aus der Praxis zeigen, dass Social-Engineering-Attacken sehr erfolgreich bei ungenügender Sensibilisierung der Mitarbeitenden sind. Bei Passwort-Phishing per E-Mail liegt die Erfolgsquote zwischen 30 und 50%. Bei Passwort-Klau per Telefon bei 50 bis 80%. Und Zutritt in gesicherte Räume bei 50%.

Tipps:

Seien Sie kritisch und haben Sie ein gesundes Mass an Misstrauen.
► Begleiten Sie eine externe oder unbekannte Person an den Bestimmungsort.
► Fragen Sie eine Ihnen nicht bekannte Person freundlich nach Name, Kontaktperson und Auftrag.
► Alle Mitarbeiter und Besucher sollten einen Badge gut sichtbar tragen.
► Achten Sie darauf, dass Sie keine vertraulichen Dokumente auf Ihrem Arbeitsplatz unbeaufsichtigt liegen lassen (Clear Desk).
► Speichern Sie vertrauliche Informationen auf mobilen Geräten immer verschlüsselt ab.
► Transportieren Sie vertrauliche Daten nur geschützt.
► Senden Sie vertrauliche E-Mails nur verschlüsselt.
► Wählen Sie ein komplexes Passwort von mindestens acht Zeichen Länge und behalten Sie es für sich.
► Sprechen Sie nie in der Öffentlichkeit (Zug, Tram, Bus, Restaurant, Raucherecke, Toilette) über geschäftsinterne und vertrauliche Angelegenheiten. Lassen Sie andere nicht mithören!
► Schliessen Sie keine USB-Sticks mit unbekannter Herkunft an Ihren Computer an.
► Schliessen Sie Ihren USB-Stick nicht an einem Ihnen unbekannten Computer an.
► Legen Sie keine CD-ROM ein, von der Sie nicht wissen, woher sie stammt.
► Installieren Sie keine Gratissoftware unbekannter Herkunft. Viele Gratis-Programme sind getarnte Spionage-Programme.
► Lassen Sie Notebook, Handy oder PDA nie unbeaufsichtigt. Das gilt auch für Aktentaschen oder Papier-Agenden.
► Lassen Sie keine vertraulichen Dokumente auf dem zentralen Drucker/Fax/Kopierer liegen.
► Entsorgen Sie Datenträger und vertrauliche Dokumente sicher (Shredder).
► Entfernen Sie nach jeder Sitzung die Skizzen und Notizen auf dem Whiteboard bzw. entfernen Sie die Flip-Chart-Notizen.

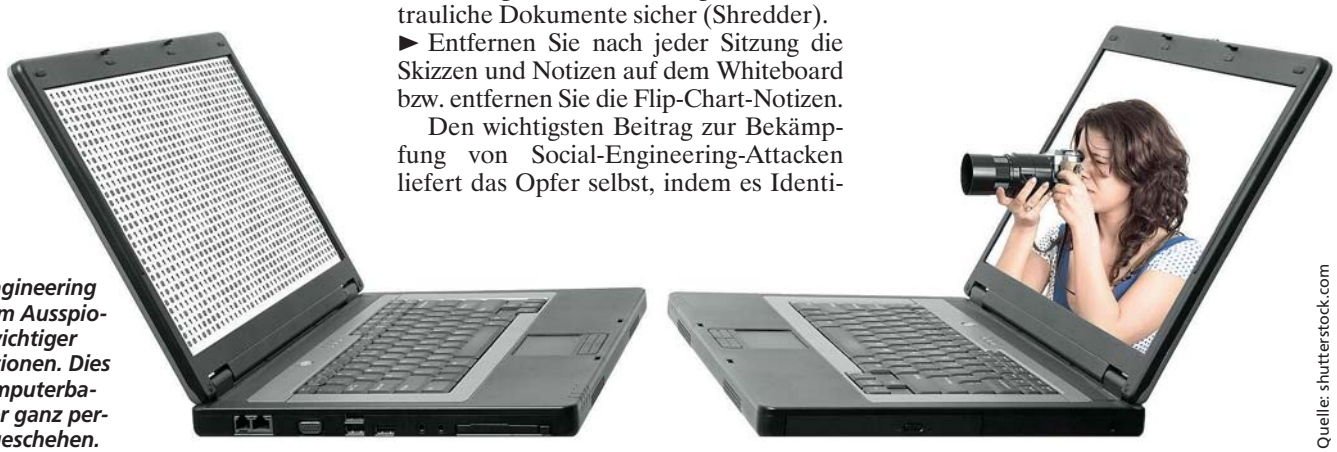
Den wichtigsten Beitrag zur Bekämpfung von Social-Engineering-Attacken liefert das Opfer selbst, indem es Identität und Berechtigung des Ansprechenden zweifellos sicherstellt, bevor es weitere Handlungen vornimmt. Bereits die Rückfrage nach Name und Telefonnummer des Anrufers kann schlecht informierte Angreifer enttarnen. Auch scheinbar geringfügige und nutzlose Informationen sollten Unbekannten nicht offengelegt werden, denn sie könnten in folgenden Kontaktaufnahmen zum Aushorchen anderer missbraucht werden oder zusammen mit vielen anderen für sich genommen nutzlosen Angaben zum Abgrenzen eines grösseren Sachverhalts dienen. Wichtig ist eine schnelle Warnung aller potenziellen weiteren Opfer; erste Ansprechpartner sind die Sicherheitsabteilung des Unternehmens, die Kontaktadresse des E-Mail-Providers und Mitmenschen und Institutionen, deren Angaben zur Vorspiegelung falscher Tatsachen missbraucht wurden.

Social Engineering Audit

Im Rahmen eines Social Engineering-Audits stellt man fest, wie es um das Sicherheitsbewusstsein der Mitarbeiter steht. Durch den persönlichen Kontakt werden dem Mitarbeiter vertrauliche Informationen entlockt – meist eine User ID und ein Passwort. Der Social Engineer als Angreifer täuscht dem Mitarbeiter eine bestimmte glaubwürdige Identität vor, um an die gewünschten Informationen zu gelangen. Ein solches Audit basiert auf den bekannten Angriffsmethoden des Social Engineerings. Die einzelnen Angriffsarten können je nach Kundenbedürfnis beliebig kombiniert werden. Folgende Ziele werden in einem solchen Audit verfolgt:

► Überprüft das Sicherheitsbewusstsein der Mitarbeiter effektiv.
► Erkennt Schwachstellen im Sicherheitsverständnis und Sicherheitsdispositiv.
► Liefert erprobte und praxisnahe Ansätze zur Risikominimierung.
► Eine wirkungsvolle Art, die Effektivität einer Awareness-Kampagne zu messen.
► Sinnvoll ist ein Audit vor und nach der Awareness-Kampagne.

Der Autor: Wolfgang Sidler ist Senior Security Consultant bei der InfoGuard AG und Security-Projektleiter EMEA bei der Crypto AG. Mitautor «Sicherheitshandbuch für die Praxis» (www.sihb.ch)



Social Engineering dient dem Ausspionieren wichtiger Informationen. Dies kann computerbasiert oder ganz persönlich geschehen.

Quelle: shutterstock.com