Dirk Fox

Social Engineering

Hintergrund

Unter „Social Engineering" werden Techniken der Beeinflussung von Menschen verstanden, die insbesondere dazu eingesetzt werden, um unberechtigt an Daten oder Informationen zu gelangen oder ein regelwidriges Verhalten zu bewirken. „Social Engineers" täuschen eine falsche Identität vor, versuchen ihre „Opfer" unter Druck zu setzen oder sie durch Charme für sich zu gewinnen [1].

Social Engineering ist eine akute Bedrohung moderner Unternehmen. In stark vernetzten Unternehmen erhöhen immer schnellere Informationsflüsse und Änderungen in Prozessabläufen die Zahl der Angriffspunkte für Social Engineering – und damit möglicher unerwünschter Informationsabflüsse. Dabei spielt die Nutzung neuer Kommunikationstechnologien eine wichtige Rolle: der Informationsaustausch über elektronische Medien erfolgt immer öfter zwischen Menschen, die sich nicht persönlich kennen.

Zentral für alle Arten von Angriffen durch Social Engineering ist, dass eine in der Regel dem Angegriffenen nicht persönlich bekannte Person versucht, zunächst das Vertrauen des „Opfers" zu gewinnen.

Social Engineering 2.0

Im Zeitalter so genannter „Sozialer Netzwerke" ergeben sich ganz neue Ansatzpunkte für Social Engineers. So geben Mitarbeiter in Sozialen Netzen nicht nur ihr Kontaktnetzwerk preis, sondern verraten darüber auch, wie gut sie im eigenen Unternehmen vernetzt sind. Zudem sind Soziale Netzwerke eine perfekte Plattform für „Legendenbildung": Ein fremder Name, ein Foto, ein glaubwürdiger Lebenslauf, und schon gibt es eine neue Identität, über die ein Kontakt angebahnt werden kann. Ein zunehmend „digital vernetztes" Leben und Arbeiten ist daher besonders anfällig für Social Engineering.

Manchmal gelingt es Social Engineers Menschen zum „Klicken" auf präparierte E-Mail-Anhänge oder Internet-Links zu verleiten, über die entweder deren IT-System mit Schadsoftware infiziert oder sie zur Preisgabe sicherheitskritischer Informationen bewegt werden (Phishing [2]).

Begünstigende Faktoren

Social Engineering nutzt typische menschliche Verhaltensmuster, die im Zusammenhang mit der Entwicklung sozialen Vertrauens greifen. Zu diesen zählen insbesondere die folgenden [3]:

- *Erfahrung*: Tritt nach einem riskanten Verhalten wiederholt keine negative Konsequenz ein, sinkt die Vermeidungshemmung. Der Effekt wird verstärkt, wenn man beobachten kann, dass auch andere (insbesondere erfahrenere oder sozial höhergestellte) Personen sich so verhalten.
- *Sympathie*: Einem sympathischen Menschen werden ungewöhnliche Wünsche eher erfüllt oder eigenartige Begründungen geglaubt.
- *Autorität*: Insbesondere in von Autorität geprägten Unternehmenskulturen gelten Anordnungen von (vermeintlichen) Autoritätspersonen oft vor Regeln – insbesondere, wenn bekannt ist, dass jene selbst gegen Regeln verstoßen.
- *Gegenleistung*: Ist man jemandem einen Gefallen „schuldig", steigt die Bereitschaft, bestehende Regeln zu überschreiten, um ihn einzulösen.
- *Zeitdruck*: Häufig rechtfertigt die Dringlichkeit eines (vermeintlich) wichtigen Vorgangs, geltende Regeln zu übertreten.

Aber auch der (zu Recht) wachsende Stellenwert der Kundenorientierung und (wünschenswerter) menschlicher Eigenschaften wie Hilfsbereitschaft, Höflichkeit oder Freundlichkeit begünstigen Social Engineering-Angriffe: Mitarbeiter geben Anrufern und Fremden in der Regel einen Vertrauensvorschuss, glauben das, was diese ihnen mitteilen, ohne Überprüfung oder halten schwer beladenen Personen die Sicherheitstüren auf.

Schutzmaßnahmen

Schützenswerte Informationen dürfen in Unternehmen nur dann weitergegeben werden, wenn ein *begründetes* Vertrauen zum Adressaten besteht. Zwar lässt sich ein Unternehmen als Ganzes nicht vollständig vor Social Engineering schützen. Die Bedrohung kann jedoch wesentlich reduziert werden, wenn die Mitarbeiter aufgeklärt und auf einfache Verhaltensregeln hingewiesen werden, die Social Engineering in der Praxis erheblich erschweren. Dafür müssen Mitarbeiter wirksam sensibilisiert werden [4].

Maßnahmen zum Schutz vor Social Engineering sind zudem immer auch im Kontext anderer Themen des Informationsschutzes (Gebäudezugang, Vergabe und Entzug von Zugriffsberechtigungen, Umgang mit Besuchern und externen Mitarbeitern, Verschluss sensibler Dokumente, Entsorgung von Dokumenten und Datenträgern etc.) zu sehen.

Die Gefahr durch Social Engineering-Angriffe muss auch beim Entwurf und der Gestaltung von Web-Anwendungen berücksichtigt werden. Denn Angriffe über einen „Man in the Browser" (einen Trojaner, der das Erscheinungsbild der Web-Anwendung beim Benutzer manipuliert) können das Vertrauen, das einer Web-Anwendung entgegengebracht wird, zu Gunsten des Angreifers missbrauchen. Die Herausforderung liegt hier darin, die Angriffsfläche der Anwendung zu verringern (z. B. durch die Nutzung unabhängiger „Kanäle" wie bspw. mobile TANs) und ein gesundes Misstrauen beim Benutzer zu schaffen („Wir fordern Sie nie zur Eingabe von TANs zu Testzwecken auf und schicken Ihnen auch keine E-Mails"), ohne zugleich das Vertrauen in die Web-Anwendung zu beeinträchtigen.

Literatur

[1] Mitnick, Kevin: *Die Kunst der Täuschung*. Mitp Verlag, 2003.
[2] Fox, Dirk: *Phishing*. DuD 6/2005, S. 365.
[3] Weßelmann, Bettina: *Maßnahmen gegen Social Engineering*. DuD 9/2008, S. 601-604.
[4] Lardschneider, Michael: *Social Engineering*. DuD 9/2008, S. 574-578.