HELPDESK

Social Engineering – trau schau wem

Jede Woche beantworten Sicherheitsexperten Leserfragen und geben Ratschläge, wie sich die Sicherheit in einem Unternehmen erhöhen lässt.

ILLUSTRATION: CW/THÜ

Frage: Wie können sich Unternehmen wirkungsvoll vor den Folgen von Social Engineering schützen?

Problem: Social Engineering bezeichnet Angriffsmethoden, bei welchen Prozesse mittels gezielten Ausnutzens menschlicher Schwächen angegriffen werden. Das Arsenal der Angriffsmethoden beinhaltet Täuschung, Bestechung, Erpressung, Einschüchterung, Bedrohung, Appellieren an die Hilfsbereitschaft oder Ausnutzen der Arglosigkeit des Opfers. Das Ziel des Angreifers ist es, dabei möglichst viele für seine Zwecke entscheidende Informationen zu erlangen. Oftmals werden so von den einzelnen Opfern Informations-Puzzlesteine gesammelt, welche den Angreifer an anderer Stelle als vertrauenswürdig «authentifizieren». So erhält ein Anrufer beispielsweise durch die Nennung eines Namens und der zugehörigen falschen, da geratenen Direktwahlnummer von der hilfsbereiten Telefonistin im Nu die richtige Direktwahlnummer und die Information, dass die entsprechende Person bis nächsten Monat im Urlaub sei, obwohl dies eigentlich per Policy verboten wäre. Mit diesen Informationen kann sich der Angreifer nun bei einem anderen Opfer auf ein fiktives Gespräch mit dem in den Ferien Weilenden beziehen um bestimmte Informationen wie beispielsweise eine Passwortliste oder den Marketingplan zu erschleichen, da eine Nachprüfung bis zur Rückkehr der «Referenzperson» unwahrscheinlich ist.

«Social Engineering wird aus wirtschaftlichen Gründen oft einer technischen Hackerattacke vorgezogen.»

Je nach Einsatzgebiet erscheint der Angreifer persönlich beim Opfer oder nutzt Medien wie Telefon, E-Mail oder SMS. Traditionelle Briefpost kommt weniger in Frage, weil da das Überraschungsmoment wegfällt. Im Gegensatz zu traditionellen technischen Hackerattacken benötigen die Angreifer keine besonderen technischen Kenntnisse. Somit ist die Gruppe der potenziellen Angreifer ungleich grösser. Aus wirtschaftlichen Gründen wird die Informationsbeschaffung mittels Social Engineering oftmals einer aufwändigen Hackerattacke mit ungewissem Ausgang vorgezogen.

Massnahmen: Menschenverstand gepaart mit einer gesunden Portion Misstrauen und ausgeprägtem Sicherheitsbewusstsein (Security Awareness) sind die wirkungsvollsten Mittel zum Schutz vor Social Engineering. Restriktive Berechtigungsmodelle oder Sicherheitsrichtlinien, in welchen beispielsweise definiert wird, dass Altpapier nicht in für Fremde zugänglichen Bereichen gesammelt wird, dienen allenfalls als Ergänzung. Bei Verdacht sollte nicht vorschnell gehandelt werden, weil Angreifer, welche Social Engineering betreiben, oft nicht vor körperlicher Gewalt zurückschrecken, um nicht gefasst zu werden. Ausserdem können so Peinlichkeiten wie die nicht gerechtfertigte Festsetzung eines Besuchers, welcher seine Wartezeit mit einem zugegebenermassen etwas unglücklich angegangenen Smalltalk mit der Empfangsdame verkürzen wollte, vermieden werden. Bei Verdacht sollen die Sicherheitsverantwortlichen oder die Vorgesetzten informiert werden. In öffentlichen Räumen oder Verkehrsmitteln dürfen im Gespräch über vertrauliche Themen keine relevanten Einzelheiten erwähnt werden. Wer proaktiv agieren möchte, kann selbst eine Social Engineering-Attacke im eigenen Unternehmen in Auftrag geben. So zeigt sich schnell, ob es Sinn machen würde, das Sicherheitsbewusstsein der Mitarbeiter gezielt zu schulen, oder ob eine vorhergegangene Schulung den erwünschten Effekt hatte. Bei derartigen Tests ist darauf zu achten, dass die Rechte der geprüften Mitarbeiter nicht verletzt werden. Aus diesem Grund müssen Social Engineering Tests nach OSSTMM (Open Source Security Testing Methodology Manual) mit nicht geschulten «Opfern» – aber nur dann – anonymisiert werden. Trau schau wem.

Der Autor
Christoph Baumgartner ist Senior Consultant bei der Sicherheitsberaterin One-Consult, Thalwil, www.one-consult.com

Unsere Experten beantworten Ihre Fragen. Schreiben Sie uns: it-security@computerworld.ch

Ein Archiv der Helpdeskartikel finden Sie im Internet: www.computerworld.ch