Angriffsziel Mensch

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 wird dies über den Einstieg in ein fremdes Computersystem erreicht, das vertrauliche Daten beherbergt. Diesen Vorgang nennt man auch Social-Hacking.

Das meist verwendete Grundmuster des Social-Engineerings wird in Form von Telefonanrufen gehandhabt. Der Social-Engineer ruft einen Mitarbeiter eines Unternehmens an und gibt sich fälschlicherweise z. B. als Techniker aus. Mit Hilfe dieses Deckmantels gelangt er an vertrauliche Zugangsdaten, weil er unmissverständlich kundtut, dass er seine Arbeit sonst nicht abschliessen könne. Gelingt ihm dies auf Anhieb nicht, wird er es wieder und wieder versuchen und wird in Kombination von vorgängig konsultierten öffentlichen Quellen und mit Informationsfetzen und Teilen der gescheiterten Anrufe sein Ziel der Manipulation früher oder später erreichen. Der Angreifer beeindruckt sein Opfer, das ihm meist technisch unterlegen ist, einerseits mit Charme und andrerseits mit Fachjargon und erntet Sympathie und Autorität. Wer wird da nicht weich? Zudem kann es schwierig sein, der Androhung, dass der Chef kontaktiert wird, wenn die Information nicht gegeben wird, zu widerstehen. Und vielleicht liegt tatsächlich ein technisches Problem vor und man wartet auf einen Anruf.

Eine andere Form des Social-Engineerings ist das Phishing. Das Prinzip ist dasselbe, wie herkömmliches Social-Engineering über fingierte Telefonanrufe, mit dem Unterschied, dass es sich um eine unpersönliche Variante via E-Mail handelt. Die E-Mails operieren mit dem Schein einer vertrauenswürdigen Seite und lassen den Benutzer glauben, dass es zwingend notwendig ist, 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 basiert, wie der Name schon sagt, auf die Verwendung des Computers, um an die gewünschten Informationen zu gelangen. Dazu ein Beispiel: Ein Social-Engineer verschickt Massenmails, gibt sich als Mitarbeiter des Online-Auktionshauses eBay aus und versucht so, an Kreditkartennummern und andere persönliche Daten heranzukommen. In seiner Massenmail 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.

Mittels Human Based Social Engineering 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.

Der Mensch als Tor zu sensiblen Informationen. Die 6 typischen Schritte einer Social-Engineering-Attacke:

1. Informationen beschaffen (z. B. im Internet, Google, Adressverzeichnisse usw.)
2. Aufbauen eines vermeintlichen Vertrauens (Insider, Gewohnheiten usw.)
3. Gezielte Manipulation von Personen, um an die gewünschten Informationen zu gelangen (Lieferant, Techniker, Journalist usw.)
4. Ausnutzen 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.

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

- Mitlaufen mit einer Gruppe Mitarbeitern, 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 wartend, bis jemand die Tür öffnet und diese dann für den unberechtigten Zutritt benutzt.
- Als Getränkelieferant getarnter Mitarbeiter verschafft sie sich Zugang.

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 50–80%. Und Zutritt in gesicherte Räume bei 50%.

Tipps

Seien Sie kritisch und haben Sie ein gesundes Mass an Misstrauen.

- Begleiten Sie eine externe Person an den Bestimmungsort.
- Fragen Sie eine Ihnen nicht bekannte Person freundlich nach Name, Kontaktperson und Auftrag.
- Alle Mitarbeiter und Besucher sollen einen Badge sichtbar tragen.
- Achten Sie darauf, dass Sie keine vertraulichen Dokumente auf Ihrem Arbeitsplatz unbeaufsichtigt liegen lassen (Clear Desk).
- Schliessen Sie Ihren USB-Stick nicht an einen Ihnen unbekannten Computer an.
- Legen Sie keine CD-ROM ein, von der Sie nicht wissen, woher sie stammt.
- Installieren Sie keine Gratissoftware mit unbekannter Herkunft. Viele Gratisprogramme sind getarnte Spionage-Programme.
- Lassen Sie Notebook, Handy oder PDA nie unbeaufsichtigt. Das gilt auch für Aktentaschen oder Papieragenden.
- Lassen Sie keine vertraulichen Dokumente auf dem zentralen Drucker/Fax/Kopierer liegen.
- Entsorgen Sie Datenträger und vertrauliche Dokumente sicher (Schredder).
- 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

- Guten Tag Herr Muster, hier ist Frau Meier von der IT-Abteilung. Wir haben gerade ein Systemproblem und brauchen unbedingt Ihre Hilfe. Wie lautet ihre User-ID und Passwort?
- Beim Personaleingang: Ein Mitarbeiter der Reinigungsfirma reinigt den Personaleingang. Entschuldigen Sie, ich habe meinen Badge vergessen.
- Ein Social-Engineer wartet in der Toilette, bis die Mitarbeiter in den Feierabend gehen.
- Reinigungspersonal: Entschuldigen Sie, ich habe meine Aktenkoffer im Büro liegen gelassen.
- Durchsuchen von Altpapier und Müll (Dumpster Diving).

- 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 mind. 8 Zeichen 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.

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 offen gelegt 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 weiterer potenzieller 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.

Ein «Social-Engineering-Audit» ist eine sehr gute Methode, das Sicherheitsbewusstsein in einer Unternehmung effektiv zu messen.

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, welche vorher beschrieben wurden. Die einzelnen Angriffsarten können je nach Kundenbedürfnis beliebig kombiniert werden. Folgende Ziele werden in einem solchen Audit verfolgt:

- Überprüft effektiv das Sicherheitsbewusstsein der Mitarbeiter.
- 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 einer Awareness-Kampagne.

Fazit

Diverse Rezepte haben in der Praxis gezeigt, dass die Sicherheitskultur durchaus positiv beeinflusst werden kann. Sogenannte Aha-Effekte bei Zuhörern sind langen Erklärungen über Sinn und Zweck vorzuziehen, da sie wesentlich besser und nachhaltiger aufgenommen werden. Beispielsweise das Knacken eines Passwortes, eines Notebooks oder das Fälschen eines E-Mails während einer Sensibilisierungs-Präsentation z. B. in Form eines Info-Lunch zeigen die Risiken eindrücklich auf. Der Hinweis auf eine mögliche, ja sogar sinnvolle Nutzung der Verhaltenshinweise auch im Umgang mit dem privaten PC erhöht die Aufmerksamkeit des Publikums merklich. So hat sich die Verknüpfung der Informationen mit privatem Nutzen als Erfolg versprechend erwiesen: Im Rahmen einer unternehmensweiten Informationssicherheit Awareness-Aktion wurde eine CD «Vertrauen ist gut, Kontrolle ist besser! Wie Sie Ihren Home-PC schützen können» mit einem Virus-Scanner und anderen Tools inkl. Booklet mit Internet-Tipps allen Mitarbeitern abgegeben, damit sie zu Hause ihren PC sicher und kontrolliert betreiben können. Besonders heute mit der Verwendung von USB Memory-Sticks ist das Risiko, einen Virus oder andere schädliche Programme einzuschleusen, sehr hoch. Das Feedback der Mitarbeiter war durchwegs positiv, zumal sie einen aktuellen Viren-Scanner mit Update-Abo und Tipps für das korrekte Verhalten im Internet kostenlos bekommen haben. Ziel ist, das Verhalten aller Mitarbeiter nachhaltig in Bezug auf die Informationssicherheit zu ändern. ■