Social Engineering – Lösungen

Leicht

Aufgabe 1
«Social Engineering findet nur im Internet statt.» Ist diese Aussage korrekt?

a) Ja
b) Nein

Lösung: Nein. Social Engineering geschieht sowohl in der analogen, realen Welt, also in der direkten Begegnung mit Personen, wie auch in der digitalen Welt, wenn man online kommuniziert (bspw. E-Mails).

Aufgabe 2
Welche Methode des Social Engineering ist besonders verbreitet und geschieht meist via E-Mail?

Lösung: Phishing

Mittel

Aufgabe 3
Was ist der Unterschied zwischen «Phishing», «Smishing» und «Vishing»?

Lösung: Mit sogenannten Phishing-E-Mails versuchen Social Engineers, an Passwörter zu gelangen oder Viren / Malware (Schadprogramme) zu verbreiten. Phishing geschieht meistens per E-Mail, kann aber auch per SMS oder per Anruf geschehen. Bei SMS spricht man von «Smishing», bei Anrufen von «Vishing».

Aufgabe 4
Was ist unter dem «CEO-Betrug» zu verstehen?

Lösung: Der CEO-Betrug ist eine Betrugsmasche. Angestellte einer Firma werden bspw. per E-Mail angeschrieben und der Absender gibt sich als CEO (Chief Executive Officer) aus und bittet «seine» Angestellten, ihm einen Gefallen zu tun oder eine dringende Angelegenheit zu erledigen. Der Manipulationsversuch rechnet damit, dass die Angestellten reagieren, was diese aber keinesfalls tun sollten.

Aufgabe 5
Nenne drei Massnahmen, wie du dich wirksam vor Social Engineering schützen kannst!

Lösung:

Die wirksamsten Schutzmassnahmen vor Social Engineering sind:

- Prüfe alle Kontaktaufnahmen und Nachrichten kritisch (E-Mail, Anrufe, SMS)!
- Gib deine Zugangsdaten nie weiter und achte darauf, dass dir beim Eintippen eines Passwortes niemand zuschaut!
- Klicke nie auf Links in E-Mails oder SMS, die dir verdächtig vorkommen! Öffne keine Anhänge!
- Falls du per E-Mail oder SMS zu einer Zahlung aufgefordert wirst, prüfe die Anfrage sorgfältig mit dem Empfänger, der Empfängerin und kontaktiere ihn, sie über die offizielle Telefonnummer!
- Achte darauf, dass deine Geräte und deine Software immer auf dem neuesten Stand sind!
- Wähle sichere Passwörter!
- Mache Sicherheitskopien / Back-ups von wichtigen Dateien!
- Besuche nur vertrauenswürdige Webseiten!
- Bei diesen und ähnlichen Betreffzeilen in E-Mails solltest du vorsichtig sein: «Passwort-Überprüfung sofort erforderlich», «Problem mit Ihrem Bankkonto», «Letzte Erinnerung: Bitte antworten Sie sofort», «Ihre Bestellung bei Amazon.com».

Schwer

Aufgabe 6
Aus welchen Elementen besteht ein sicheres Passwort?

Lösung: Beachte folgende Kriterien, wenn du ein Passwort wählst. So machst du es Angreifern schwer, sich Zugang zu deinen Daten zu verschaffen.

- Lang (mind. 8 Zeichen, besser sind 12 oder mehr Zeichen.)
- Vielfältig (Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen.)
- Zufällig (Keine allgemeinen Begriffe, besser sind Zeichenfolgen, die keinen Sinn ergeben.)
- Einmalig (Verwende für jedes Login ein anderes Passwort!)

Aufgabe 7
Wie erkennst du unter anderem, ob eine Website sicher ist?

Lösung:

- Prüfe, ob eine Website mit einem SSL-Sicherheitszertifikat gesichert ist. Wenn in der Adressleiste ein kleines Schloss zu finden ist und die Adresse mit https:// (anstatt http://) beginnt, dann handelt es sich eher um eine sichere Website.
- Du kannst Browsererweiterungen wie bspw. «Web of Trust» verwenden, die dir anzeigen, wie sicher eine Website ist. Allerdings kann die Browsererweiterung dein Nutzungsverhalten komplett einsehen.