Landesamt für Sicherheit in der Informationstechnik

Gib „Manipulation“ keine Chance!

Was ist Social Engineering?

Bei **Social Engineering** handelt es sich um eine Form der **Manipulation**. Der Angreifer nutzt psychologische Tricks und Täuschungen um **menschliche Schwachstellen**, wie z.B. Hilfsbereitschaft oder Angst auszunutzen.

Mögliche Motive

- Zugangsdaten abgreifen
- Schadsoftware einschleusen
- Mitarbeiter zu falschen Geldüberweisungen veranlassen

Ablauf eines Angriffs

1. Informationsbeschaffung über das Opfer
2. Vertrauensaufbau zum Opfer (z.B. durch gefälschte Identität)
3. Manipulation des Opfers
4. Erfolg oder Misserfolg des Täters

Beliebte Taktiken

- Im Namen einer vertrauenswürdige Marke auftreten
- Im Namen einer staatlichen Stelle auftreten
- Erzeugung von Handlungsdruck beim Opfer
- Appellieren an die Hilfsbereitschaft des Opfers

Arten von Social Engineering-Angriffen (1/2)

Phishing	Spear Phishing	Identitäts-diebstahl	Baiting
Angreifer täuscht vor, eine vertrauenswürdige Person oder Organisation zu sein, um sensible Informationen wie Benutzernamen oder Passwörter zu stehlen	Angreifer verwendet maßgeschneiderte und personalisierte Nachrichten, um gezielt Einzelpersonen oder Organisationen anzugreifen	Der Angreifer gibt sich als Autoritätsperson oder Vertrauensperson aus, um sensible Informationen zu sammeln	Opfer wird mit verlockenden Angeboten gelockt im Gegenzug für sensible Informationen (z.B. vorgetäuschtes Gewinnspiel)

Arten von Social Engineering-Angriffen (2/2)

Pretexting

Der Angreifer erfindet eine überzeugende Geschichte, um das Vertrauen des Opfers zu erschleichen, damit das Opfer sensible Informationen preisgibt

Tailgaiting

Angreifer folgt dem Opfer unbemerkt (auch digital) in geschützte Bereiche

Scareware

Software, die dem Opfer Angst machen soll, damit es sensible Informationen preisgibt (z.B. gefälschter Bescheid einer Strafverfolgungsbehörde)

Watering-Hole-Angriff

Einschleusen von Schadcode auf einer legitimen, vom Opfer oft besuchten Internetseite

Social Engineering?

Anzeichen

- Unbekannte/ungewöhnliche Anfragen oder beigefügte verdächtige Anhänge und Links
- Anfragen mit hoher Dringlichkeit oder Zeitdruck
- Abfrage vertraulicher Informationen
- Versprechen von Belohnungen oder anderer Vorteile ein
- Vermeintliche vertrauenswürdige Kommunikationspartner bitten Sie, von Ihrer gewöhnlichen Verhaltensweise abzuweichen

Schutzmaßnahmen

- Persönliche Daten nicht leichtfertig auf sozialen Netzwerken preisgeben
- Passwörter und Zugangsdaten nicht per Telefon oder E-Mail an andere weitergeben
- Lassen Sie bei Mails von unbekannten Absendern besondere Vorsicht walten. Im Zweifelsfall die Identität des Absenders durch einen zweiten Kanal verifizieren (bspw. einen Anruf)
- Mehr-Augen-Prinzip, bitten Sie eine weitere Person um Ihre Meinung, ob es sich hier um Social Engineering handelt
- Vorsicht bei Anfragen, die Dringlichkeit oder Zeitdruck suggerieren

Monats-Challenge

Gehen Sie folgende Fragen für sich durch:

- Haben sie bereits Phishing Mails erhalten?
- Kennen Sie solche Situationen? (Schockanrufe, Enkeltrick)
- Kollegen fragen, ob ihnen bereits ähnliches passiert ist.
- Wie haben Sie in dieser Situation reagiert?