PRODATIS®

The eBusiness Solution Company.


# Social Engineering – was Sie dazu wissen müssen

Beim Social Engineering erschleichen Angreifer das Vertrauen der Opfer, indem sie eine falsche Identität vortäuschen. Die Opfer geben im guten Glauben vertrauliche Daten oder den Zugang zu den Daten weiter. Rein technische Datenschutz-Maßnahmen reichen als Gegenreaktion nicht aus. Die psychologischen Tricks der Angreifer zu kennen, muss hinzukommen.

**Wie sieht Social Engineering aus?**

Social Engineering kommt immer wieder in einem neuen Gewand daher. Es gibt aber einige typische Erscheinungsformen, meist in Form von sogenannten Phishing Mails:

- die angebliche E-Mail vom eigenen Systemadministrator, der alle Passwörter zurücksetzen muss
- der gefälschte Urlaubsgruß des Freunds, der gleich einige (verseuchte) Bilddateien mitschickt
- die scheinbare Nachricht des tatsächlich zuständigen Finanzamts mit Fragen zur finanziellen Situation, die über einen Einblick in das Online-Konto überprüft werden soll
- der vorgetäuschte Vorsitzende des eigenen Sportvereins, der die Spielberichte des letzten Monats schickt. In Wirklichkeit aber ist die Word-Datei ein Trojaner, der Daten stehlen soll.

**Wie funktioniert Social Engineering?**

Der Report „Exploring the Psychological Mechanisms used in Ransomware Splash Screens“ von Cyber-Psychologe Dr. Lee Hadlington von der De Montfort Universität veranschaulicht, wie Cyberkriminelle Social-Engineering-Taktiken – von Angst über Autorität bis zu Zeitdruck und Humor – einsetzen, um Menschen zu manipulieren.

Dabei haben die Wissenschaftler unter anderem die sprachliche Ausdrucksweise und die Optik von 76 Angriffen analysiert.

Die wichtigsten Ergebnisse der Analyse:

- **Kritischer Faktor Zeit:** Bei mehr als der Hälfte der Stichproben (57 %) setzte eine ablaufende Uhr die betroffenen User unter Druck. Die gewährten Fristen beliefen sich dabei auf Zeitspannen zwischen zehn und 96 Stunden.

- **Negative Folgen:** In den meisten Fällen drohten die Angreifer den Opfern an, dass sie den Zugang zu ihren Daten verlieren und die Daten für immer gelöscht werden.
- **„Anwenderfreundlichkeit“**: 51 Prozent der Mitteilungen über die Attacke waren dabei relativ anwenderfreundlich gestaltet. Sie gaben den Opfern etwa genaue Anweisungen oder enthielten eine Liste häufig gestellter Fragen (FAQ). In einem Fall bekamen die Opfer sogar angeboten, mit „einem Mitarbeiter“ zu sprechen.
- **Bildsprache:** Bei der Untersuchung des eingesetzten Bildmaterials fiel auf, dass in einigen Fällen offizielle Markenzeichen und Embleme zum Einsatz kommen. So auch das Wappen des FBI. Das soll den betroffenen Personen Autorität und Glaubwürdigkeit vermitteln.

**Welche Tricks nutzen die Angreifer?**

Auch die Studie „Hacking die Human OS“ von McAfee gibt hilfreiche Hinweise.

Zum einen ist wichtig, zu wissen, dass die Angreifer sich zunehmend Mühe geben, die Opfer kennenzulernen, also Angriffspunkte und Zugangswege zu finden.

Hier bieten die Profile in den sozialen Netzwerken meist genug Material, um eine für das Opfer passende Geschichte zu erfinden. Sie bildet die Basis der Attacke.

Die Hebel, die die Angreifer dann auf das Opfer anwenden, sind insbesondere:

- ein angeblicher Gefallen, den der Absender dem Opfer gegenüber erweist,
- eine künstliche Verknappung der Zeit, damit der Empfänger schnelle, unüberlegte Entscheidungen trifft,
- ein Hinweis auf eine angebliche Verpflichtung des Opfers,
- das Ausnutzen von scheinbarer Attraktivität und Sympathie,
- das Vorspielen von Autorität gegenüber dem Opfer und
- der Hinweis darauf, dass alle anderen etwas Bestimmtes tun, das das Opfer ebenfalls tun sollte.

| Psychologischer Hebel der Datendiebe | Beispiel |
|---|---|
| **Methode „Herdentrieb“:** Alle machen dies, Du musst dies auch tun. | Angebliche E-Mail des Administrators: Alle anderen Mitarbeiter haben fristgerecht ihr Passwort geändert. Machen Sie dies nun auch (endlich)! |
| **Methode „Autorität“:** Du musst gehorchen. Dabei setzen die Angreifer auch entsprechende Logos und Bilder ein. | Angebliches Fax der Bank: Es gibt ein Problem mit einer Überweisung. Rufen Sie eine (gefälschte) Nummer an und wiederholen Sie den Zahlungsvorgang. |
| **Methode „Attraktivität“:** Ich mag Dich, vertrau mir. | Angebliche E-Mail einer Verehrerin: Ich habe Dein Facebook-Profil gesehen und will Dich heiraten. Aber ich brauche Deine Hilfe … |
| **Methode „Pflichtbewusstsein“:** Als guter Bürger musst Du dies tun. | Angeblicher Brief der Stadtverwaltung: Jeder Bürger muss auf Bankeinzug umstellen, faxen Sie uns die Bankverbindung mit diesem Formular. |
| **Methode „Keine Zeit“:** Du musst sofort reagieren. | Angebliche Gewinn-Benachrichtigung: Melden Sie sich sofort als Gewinner zurück, sonst ist es zu spät. |
| **Methode „In der Schuld sein“:** Ich habe Dir geholfen, nun bist Du dran. | Angebliche Nachricht des Schulkameraden: Ich habe Dir in der Schule geholfen, jetzt brauche ich Deine Hilfe. |
| **Methode „Drohung“:** Ich veröffentliche Vertrauliches über Dich. | Nachricht des Angreifers, dass er vertrauliche Daten über das Opfer verbreiten werde, wenn es nicht dieses oder jenes tut (Online-Erpressung). |
| **Methode „Hilfsbereitschaft“:** Mache das, ich zeige Dir, wie es geht. | Nachricht des Angreifers, die eine genaue Anleitung und sogar eine FAQ-Liste enthält, die es dem Opfer leichter machen soll. |

**Die Top 10 der Täuschungen**

Der IT-Sicherheitsanbieter KnowBe4 berichtete vor Kurzem über die Top-10-Themen von Täuschungen, die Angreifer im 4. Quartal 2018 am häufigsten als E-Mail verschickt und die die Opfer angeklickt haben.

Fünf Kategorien von Betreffzeilen tauchten von Quartal zu Quartal im Laufe des Jahres 2018 immer wieder auf:

- Lieferungen
- Passwörter
- Unternehmens-Richtlinien
- Urlaub
- IT-Abteilung

Zu den Top-10-E-Mail-Betreffzeilen im 4. Quartal 2018, die die Opfer weltweit am häufigsten anklickten, gehören:

- Passwort-Überprüfung sofort erforderlich / Änderung des Passworts umgehend erforderlich (19 %).
- Ihre Bestellung bei Amazon.com / Ihre Amazon-Bestellbestätigung (16 %).
- Ankündigung: Änderung des Urlaubsplans (11 %).
- Frohe Feiertage! (10 %).
- Problem mit Ihrem Bankkonto (8 %).
- Deaktivierung der [[E-Mail]] im Prozess (8 %).
- IT-Abteilung (8 %).
- Überarbeitete Urlaubs- und Krankheitsrichtlinie (7 %).
- Letzte Erinnerung: Bitte antworten Sie sofort (6 %).
- UPS Etikettenversand (6 %).

**Wie hängen Social Media und Social Engineering zusammen?**

Wer sich bei einem sozialen Netzwerk oder in mehreren sozialen Netzwerken anmeldet, muss erstaunlich viele Details zu seiner Person und Persönlichkeit beantworten.

Diese Angaben im Online-Profil helfen nicht nur dabei, passende Kontakte oder Gruppen zu finden. Sie dienen auch als Grundlage für Angriffe.

Neben den Online-Profilen lassen sich dabei auch die bestehenden Kontakte und die Angaben zu persönlichen Vorlieben (wie „Gefällt mir“ bei Facebook) auswerten.

Das soziale Netzwerk Twitter liefert ein Beispiel für die zusätzliche Kategorisierung von Statusinformationen (Tweets).

Mit sogenannten Hashtags, die mit „#“ beginnen, lassen sich die Twitter-Nachrichten einem bestimmten Thema zuordnen. Die Nutzer wählen also die passenden Keywords oder Schlagworte zu der Nachricht aus.

Das ist recht praktisch, wenn andere Nutzer sich für gewisse Themen interessieren und alle Informationen dazu nachverfolgen möchten. Allerdings können auch Angreifer die Hashtags für Social Engineering gezielt auswerten.

**Hashtags zeigen Interessen und Vorlieben**

Ein Nutzer, der einem bestimmten Thema oder Hashtag folgt, interessiert sich dafür und ist wahrscheinlich für passende Werbung zugänglicher.

Deshalb sind die Hashtags nicht nur für die Nutzer hilfreich. Datendiebe füllen ihre Datenbanken mit Nutzernamen und bevorzugten Hashtags. Gerade für Social Engineering, also Attacken, die das Vertrauen der Opfer erschleichen, lässt sich dies nutzen.

Verfolgt ein Nutzer etwa alles zum Thema „Formel 1“, sind manipulierte Twitter-Nachrichten mit diesem Hashtag bei ihm besonders erfolgreich.

Die Wahrscheinlichkeit ist hoch, dass dieser Nutzer den Kurzlink im entsprechenden Tweet anklickt, der auf verseuchte Webseiten führt, aber ein tolles Formel-1-Foto verspricht.

**Wie gegen Social Engineering schützen?**

Anders als bei den meisten sonstigen Angriffsformen der Datendiebe ist ein Unternehmen bei Social Enginee-

ring auch dann gefährdet, wenn das Netzwerk sowie alle Server und Endgeräte vollständig und optimal abgesichert sind.

Social Engineering nutzt eher menschliche Eigenschaften als technische Schwachstellen aus, etwa Eigenschaften und Reaktionen wie

- Neugierde,
- Hilfsbereitschaft,
- Kollegialität,
- Kundenfreundlichkeit und
- Angst.

Gegen die psychologischen Tricks der Datendiebe hilft deshalb in erster Linie, über die Methoden der Social Engineers aufzuklären.

Darüber hinaus ist es wichtig, Mitarbeiter dafür zu sensibilisieren, dass digitale Identitäten, gleich bei welchem Kommunikationskanal, grundsätzlich gefälscht sein könnten, sofern keine technischen Zusatzmaßnahmen die Identitäten kontrollieren.

Social Engineering nutzt zwar hauptsächlich die sogenannte Schwachstelle Mensch. Aber besteht die Gefahr, dass ein Angriff Rechner verseucht oder ein Lauschangriff personenbezogene Daten abgreift, kann zusätzlich die Technik helfen:

- Für Webbrowser und E-Mail-Clients gibt es Anti-Phishing-Filter.
- Online-Scanner überprüfen Links, bevor sie jemand öffnet.

**Wie für Angriffe sensibilisieren?**

Viele IT-Sicherheitsforscher halten die Nutzer für die „größte Schwachstelle“ überhaupt. Denn „Sicherheitslücken“ bei den Nutzern lassen sich nicht automatisch beheben, indem man Patches einspielt. Stattdessen ist es entscheidend, Nutzer beziehungsweise Mitarbeiter zu sensibilisieren.

In eine Datenschutz-Unterweisung gehört deshalb unbedingt auch das Thema Social Engineering.

Die Angriffsmethode, das Vertrauen der Nutzer auszunutzen, die Anwender ungewollt zu einer Datenweitergabe zu verleiten, wird immer beliebter unter den Datendieben. Und zwar deshalb, weil sich der Nutzer nicht so einfach automatisch absichern lässt, wie dies bei Hardware und Software zumindest teilweise möglich ist.

Social Engineering funktioniert nicht nur über E-Mails und Webseiten, sondern auch über Chat-Dienste, über das Telefon, über Fax-Nachrichten, mit der klassischen Briefpost und sogar von Angesicht zu Angesicht.

Angreifer könnten die Mitarbeiterinnen und Mitarbeiter also auch am Telefon oder per Brief dazu verleiten, vertrauliche Daten oder Wege zu diesen preiszugeben.

Informieren Sie daher in Ihrer nächsten Schulung zum Datenschutz die Kollegen über die Tricks der Angreifer.

Quelle:
www.datenschutz-praxis.de