Cyberkriminelle und ihre psychologischen Tricks: Die häufigsten Social Engineering-Angriffe

Social Engineering gilt heute als eine der grössten Sicherheitsbedrohungen für Unternehmen. Im Gegensatz zu traditionellen Hacking-Angriffen können Social Engineering-Angriffe auch nicht-technischer Natur sein und müssen nicht zwingend eine Kompromittierung oder das Ausnutzen von Software- oder System-Schwachstellen beinhalten. Im Erfolgsfall ermöglichen viele Social-Engineering-Angriffe einen legitimen, autorisierten Zugriff auf vertrauliche Informationen. Die Social Engineering-Strategie von Cyberkriminellen fusst auf starker zwischenmenschlicher Interaktion und besteht meist darin, das Opfer dazu zu verleiten, Standard-Sicherheitspraktiken zu missachten. Und so hängt der Erfolg von Social-Engineering von der Fähigkeit des Angreifers ab, sein Opfer so weit zu manipulieren, dass es bestimmte Aktionen ausführt oder vertrauliche Informationen preisgibt. Da Social-Engineering-Angriffe immer zahlreicher und raffinierter werden, sollten Organisationen jeder Grösse eine intensive Schulung ihrer Mitarbeiter als erste Verteidigungslinie für die Unternehmenssicherheit betrachten.

Die Strategie der Cyberkriminellen: Trickbetrüger des digitalen Zeitalters

Social Engineering-Angreifer sind letztlich eine moderne Spielart der klassischen Trickbetrüger. Häufig verlassen sich diese Kriminellen auf die natürliche Hilfsbereitschaft von Menschen: Zum Beispiel rufen sie bei ihrem Opfer an und geben ein dringendes Problem vor, das einen sofortigen Netzwerkzugang erfordert.
Social Engineering-Angreifer nutzen gezielt bestimmte menschliche Schwächen wie Unsicherheit, Eitelkeit oder Gier aus und verwenden Informationen, die sie aus Lauschangriffen oder dem Ausspionieren sozialer Medien gewonnen haben. Dadurch versuchen sie, das Vertrauen autorisierter Benutzer zu gewinnen, damit ihre Opfer sensible Daten preisgeben, mit Malware infizierte E-Mail-Anhänge öffnen, oder sie deren Zugangsdaten für Computernetzwerke oder Datenspeicher stehlen können. Auch durch den Aufbau eines Schreckensszenarios wie einem angeblichen Sicherheitsvorfall können sie ihre Zielperson dazu bewegen, beispielsweise als Antiviren-Software getarnte Malware zu installieren und auszuführen.

Häufige Social Engineering-Methoden im Ãœberblick

Technologielösungen wie E-Mail-Filter, Firewalls und Netzwerk- oder Daten-Ãœberwachungs-Tools helfen zwar, Social Engineering-Attacken abzuschwächen, doch eine gut geschulte Belegschaft, die in der Lage ist, Social Engineering zu erkennen, ist letztlich die beste Verteidigung gegen diese Art Angriffe. Unternehmen sollten ihre Mitarbeiter deshalb umfassend über die gängigen Arten von Social-Engineering aufklären. Im Folgenden daher ein Ãœberblick zu verschiedenen Angriffstechniken, deren Ãœbergänge teilweise fliessend sind und von Kriminellen auch in Kombination eingesetzt werden.

Pretexting: Geschicktes Vortäuschen falscher Tatsachen

Beim Pretexting schützt ein Angreifer geschickt falsche Tatsachen vor, um ein Opfer dazu zu bringen, ihm Zugang zu sensiblen Daten oder geschützten Systemen zu gewähren. Beispielsweise gibt ein Krimineller vor, Bankdaten zu benötigen, um die Identität des Empfängers zu bestätigen. Oder er tarnt sich als Mitarbeiter der IT-Abteilung, um sein Opfer dazu zu verleiten, Login-Daten preiszugeben oder einen Computerzugang zu gewähren. Angreifer führen Köderangriffe durch, indem sie ein mit Malware infiziertes Gerät wie ein USB-Flash-Laufwerk, an einem bestimmten Ort im Unternehmen zurücklassen, an dem es wahrscheinlich gefunden wird. Wenn ein Mitarbeiter den Datenträger mit seinem Computer verbindet, um beispielsweise zu sehen, was sich darauf befindet, wird der Rechner heimlich mit Malware infiziert. Einmal installiert, erlaubt die Malware dem Angreifer, in das System des Opfers einzudringen.

Phishing: Von gefälschten Geschäftsemails bis zum vermeintlichen Spendenaufruf

Bei einem Phishing-Angriff tarnen Cyberkriminelle sich als vertrauenswürde Quelle und nehmen eine betrügerische Kommunikation mit ihrem Opfer auf, um es dazu zu verleiten, Malware zu installieren oder persönliche, finanzielle oder geschäftliche Informationen herauszugeben. E-Mail ist der beliebteste Vektor für Phishing-Angriffe, aber Phishing kann auch Chat-Anwendungen, Social Media, Telefonanrufe (auch Vishing oder Voice Phishing genannt) oder gefälschte Websites verwenden. Einige besonders perfide Phishing-Angriffe täuschen gezielt wohltätige Zwecke vor dem Hintergrund aktueller Naturkatastrophen oder anderen tragischen Vorfällen vor. So nutzen sie den guten Willen ihrer Opfer aus, um durch einen Spendenaufruf an persönliche Daten oder Zahlungsinformationen gelangen.

Watering-Hole-Attacke

Bei einer Watering-Hole-Attacke (Auflauern am Wasserloch) wählt der Angreifer sorgfältig eine bestimmte Website aus, von der er weiss, dass seine Opfer diese häufig besuchen, und infiziert die Homepage mit Malware. Zielpersonen sind

meist Mitarbeiter von grossen Unternehmen oder Regierungsstellen. Ein Beispiel wäre die Webseite eines lokalen Restaurants, in denen Mitarbeiter ihre Pause verbringen, beispielweise regelmässig das Tages- oder Wochenangebot abrufen oder den Lieferservice in Anspruch nehmen.

Spear-Phishing: Gezieltes Ausspähen und Angreifen eines Opfers

Spear-Phishing ist eine sehr gezielte Art von Phishing-Angriff, die sich auf eine bestimmte Person oder Organisation konzentriert. Spear Phishing-Angriffe verwenden persönliche Informationen, die spezifisch auf das Opfer zugeschnitten sind, um Vertrauen zu gewinnen und besonders legitim zu erscheinen. Oftmals werden diese Informationen aus den Social Media-Accounts der Opfer oder anderen Online-Aktivitäten entnommen. Durch die Personalisierung ihrer Phishing-Taktiken haben Spear-Phisher höhere Erfolgsquoten, wenn es darum geht, ihre Opfer dazu zu bringen, Zugang zu Systemen gewähren oder sensible Informationen wie Finanzdaten oder Geschäftsgeheimnisse preiszugeben.
Social Engineering ist eine anhaltende Bedrohung für viele Organisationen. Mitarbeiterschulungen sind deshalb die erste und wichtigste Massnahme, um zu verhindern, dass Unternehmen Opfer von Angreifern werden, die immer ausgefeiltere Methoden einsetzen, um Zugang zu sensiblen Daten zu erhalten. Durch Sensibilisierung der Mitarbeiter in Kombination mit entsprechenden Security- und Datensicherheitstechnologien kann dieses Risiko erheblich minimiert werden.