Neustadt an der Weinstraße, 15. März 2019

Social Engineering: Die Kunst der Täuschung

Im digitalen Zeitalter ist Hacking die wohl am weitesten verbreitete Form von Cyberkriminalität. Glücklicherweise ermöglichen verschiedene Technologien, wie Antivirenprogramme oder Firewalls, den Schutz von Smartphones, Tablets, Computern und Co. – allerdings bieten sie keinen Schutz für den Menschen. Und das, obwohl das sogenannte „Human Hacking" in Form von Social Engineering immer weiter zunimmt. SpardaSurfSafe, eine Initiative der Stiftung Bildung und Soziales der Sparda-Bank Baden-Württemberg, hat sich angeschaut, wie genau Social Engineers bei ihren Angriffen vorgehen.

Unter Social Engineering versteht man eine Form des Betrugs mit dem Ziel, bei Personen bestimmte Handlungsweisen hervorzurufen. Durch zwischenmenschliche Beeinflussung und Manipulation bringen Betrüger ihre Opfer dazu, vertrauliche Informationen preiszugeben, Produkte zu kaufen oder Geld zu überweisen. Im Internet findet das Social Engineering seinen Ursprung meistens per E-Mail oder per Nachricht über einen Social-Media-Kanal. Betrüger schlüpfen dafür in die Rolle eines Bekannten, geben sich als ein Unternehmen aus, bei dem man z. B. ein Abo abgeschlossen hat, oder kontaktieren einen im Namen einer Behörde oder eines Vorgesetzten. So gewinnen sie schnell das Vertrauen ihrer Opfer und können sie gezielt ausnutzen, um unbemerkt an sensible Daten zu gelangen. Im IT-Bereich spricht man deshalb auch vom „Human Hacking", da statt eines Computers die Psyche eines Menschen gehackt wird.

„Social Engineering tritt überall dort auf, wo Menschen einen Schlüssel für Geld oder Informationen darstellen", erklärt Götz Schartner vom Verein Sicherheit im Internet e. V., einem Mitveranstalter von SpardaSurfSafe. Potenzielle Opfer sind folglich vor allem staatliche Einrichtungen, Behörden und Konzerne, aber auch Privatpersonen geraten oftmals ins Visier von Betrügern. „Ein Reinfall auf eine solche Masche darf allerdings nicht als Naivität verstanden werden, da Kriminelle gezielt die Berechenbarkeit des menschlichen Denkens und Verhaltens ausnutzen. Gegen solche Psycho-Taktiken kann man sich nur schwer schützen", so der Experte.

Die Angreifer bedienen sich bei ihrem Vorgehen tief verwurzelter Mechanismen der menschlichen Psyche, wie beispielsweise Vertrauen und Gemeinsamkeiten. Vor der ersten Kontaktaufnahme werden Informationen zu den Opfern gesammelt, die wichtige Kontakte, Interessen oder die aktuelle Lebenssituation betreffen. Dann wird eine Mail im Namen eines Bekannten verschickt, in die Einzelheiten eingebaut werden, die theoretisch nur das Opfer und der Absender kennen. Die Betroffenen denken somit nicht weiter über eine mögliche Falle nach und geben unbemerkt Informationen preis. Ein weiterer wirkungsvoller Mechanismus ist vermeintliches Detailwissen. Opfer werden von Angreifern mit konkretem und meist persönlichem Detailwissen konfrontiert und erpresst. Es wird also mit Druck und Angst der Opfer gespielt. Durch künstlichen Zeitdruck und das Androhen von Konsequenzen beim Nichthandeln drängen die Angreifer zur schnellen Durchführung ihrer Forderungen. Zuletzt sind Neugier und Interesse Mechanismen, derer sich Betrüger gerne bedienen. Durch das Versprechen von Belohnungen oder persönlichen Vorteilen spielen sie mit der Gier der menschlichen Natur.

Mit anderen Worten: Social Engineers instrumentalisieren Menschen für ihre Zwecke. Eine erschreckende Erkenntnis, die im digitalen Zeitalter jedoch keine Seltenheit mehr darstellt. Aufklärungskampagnen wie SpardaSurfSafe wollen deshalb vermitteln, wie man sich gegen Cyberkriminalität schützen kann. Im Rahmen von Social Engineering legt Sicherheitsexperte Schartner deshalb nahe: „Es ist immer ratsam, kritisch zu überdenken, mit wem ich private Inhalte teile." Dies gilt besonders für Social-Media-Plattformen und E-Mails. Grundsätzlich gilt: Wen ich nicht kenne, dem vertraue ich keine intimen Daten an. Deshalb ist es empfehlenswert, eine Datenweitergabe vorab persönlich oder telefonisch abzuklären. Auch bei Gewinnspielen und weitergeleiteten Links sollte man Vorsicht walten lassen und zuerst sicherstellen, dass es sich um seriöse Nachrichten handelt. Auf verdächtige SMS, E-Mails oder Anrufe sollte man gar nicht erst reagieren. Eine gesunde Portion Skepsis kann also dabei helfen, sich vor Social Engineering zu schützen.

8com GmbH & Co. KG | Europastraße 32 | 67433 Neustadt an der Weinstraße
Telefon: +49 6321 / 484 46 - 0 | info@8com.de
Vertretungsberechtigte: Götz Schartner, Sandra Schartner

Steuer- Nr. DE 238115883
Handelsregistereintragung Ludwigshafen am Rhein HRA 60853 LU
Gerichtsstand: Neustadt an der Weinstraße

Über SpardaSurfSafe – eine Initiative der Stiftung Bildung und Soziales der Sparda-Bank Baden-Württemberg

Veranstalter und Träger von SpardaSurfSafe ist die Stiftung Bildung und Soziales der Sparda-Bank Baden-Württemberg, die gemeinsam mit dem Kultusministerium Baden-Württemberg, dem Verein Sicherheit im Internet e. V. und dem Landesmedienzentrum Baden-Württemberg das Großprojekt bereits im achten Jahr durchführt. In Kooperation mit den IT-Sicherheitsexperten der 8com GmbH & Co. KG wurde ein Konzept entwickelt, das die Schüler im Rahmen des Unterrichts im Umgang mit den Neuen Medien aufklärt. „Wir haben das Konzept in den vergangenen Jahren erfolgreich in 26 verschiedenen Städten in Baden-Württemberg durchgeführt und haben mittlerweile über 350.000 Besucher erreicht. Dafür bekommen wir durchweg positives Feedback von den Teilnehmern, ob Schüler, Eltern oder Lehrer", erklärt Patrick Löffler vom Verein Sicherheit im Internet e. V.

Ansprechpartner:

Presse
Quadriga Communication GmbH
Martje Christin Lutterbeck
030-303 080 89-15
lutterbeck@quadriga-communication.de

Projekt „SpardaSurfSafe"
8com GmbH & Co. KG
Eva-Maria Nachtigall
06321-48446-0
info@8com.de