Wie Hacker unsere Psyche entschlüsseln…

Über E-Mails, den sozialen Medien, Websites, aber auch über das Telefon oder persönlich wird immer wieder versucht, uns zu beeinflussen und an unsere Informationen zu gelangen, damit sich Angreifer einen Vorteil verschaffen = *Social Engineering (Soziale Manipulation mit dem Ziel, bei Personen bestimmte Verhaltensweisen (z.B. Preisgabe von vertraulichen Informationen, Freigabe von Finanzmitteln) zu bewegen).*

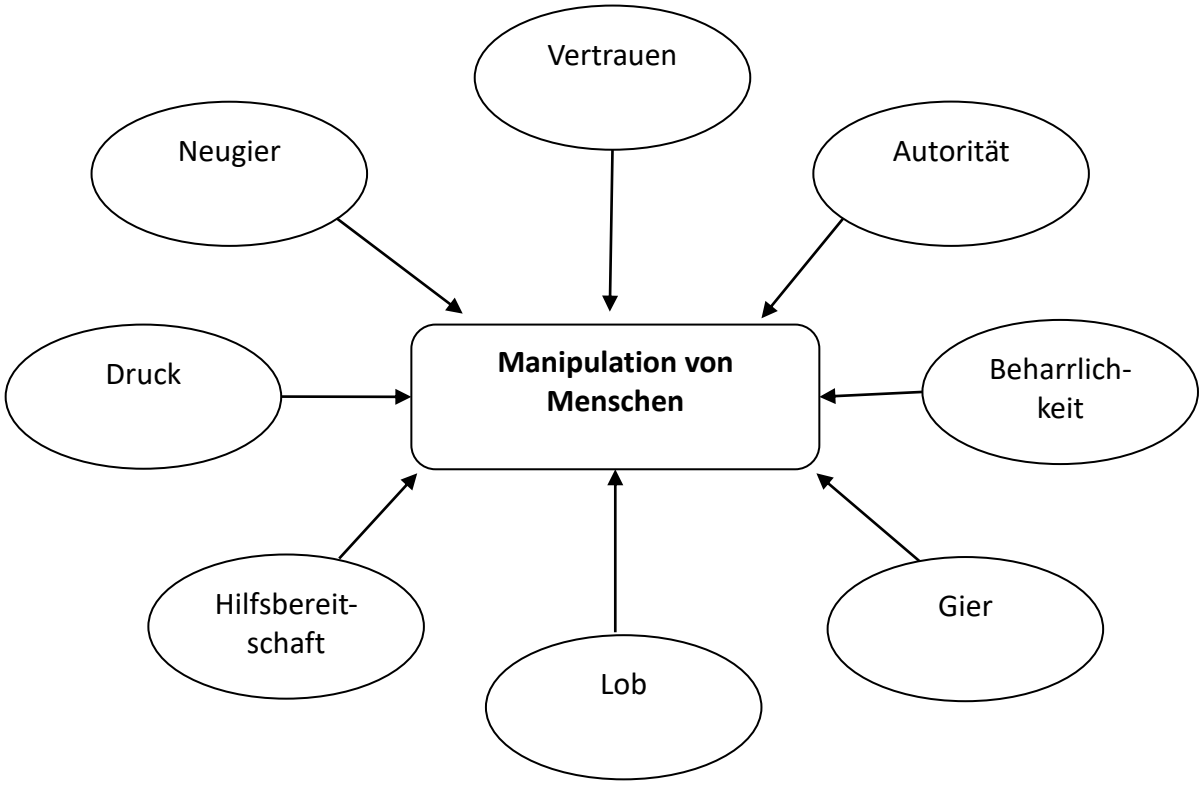

Abbildung: Anreize zur Manipulation von Menschen (Social Engineering)
Quelle: Eigene Darstellung in Anlehnung an Beißel 2019

Dabei zielen Angreifer darauf ab, uns auf psychologischer Ebene zu beeinflussen. Die Anreize in der obigen Abbildung werden genutzt, damit wir eine Beeinflussung zulassen und auf die Anweisungen eines Angreifers eingehen. Nachstehend sind die Anreize tiefgehend beschrieben.

Druck
Unsere Angst wird geschürt, wenn ein Angreifer z.B. negative Konsequenzen in Aussicht stellt, falls nicht gehandelt wird (z.B. Mahngebühren in einer falschen Rechnungs-E-Mail) oder künstlicher Zeitdruck wird erzeugt („Handeln Sie jetzt oder ein wichtiges Projekt ist in Gefahr“).

Neugier/Interesse
Die Neugier ist grundsätzlich eine starke und treibende Kraft, die uns oft zu unvorsichtigem Handeln und zur Verharmlosung von Gefahren führt. So werden z.B. interessante Informationen in Aussicht gestellt (z.B. eine Excel-Datei mit dem Titel

„Gehaltsdaten-2024.xlsx“) oder spannende Inhalte werden angedeutet („Bist Du das auf dem Video?“)

Gier
Unsere Gier wird in der Regel dadurch ausgenutzt, dass ein hoher Geldbetrag in Aussicht gestellt wird. Angreifer versenden Nachrichten, die vermeintlich von Banken, anderen Finanzdienstleistern oder Lotteriegesellschaften kommen. („Sie haben 10 Mio. € gewonnen…“)

Vertrauen
Unser Vertrauen wird ausgenutzt, wenn z.B. ein Angreifer vortäuscht, dass er einer allgemein bekannten und vertrauenswürdigen Organisation (z.B. einer Behörde) angehört oder es bereits einen Kontakt gibt. Vermeintliche Gemeinsamkeiten werden angeführt, um zusätzliches Vertrauen zu erzeugen (z.B. „Wir haben doch kürzlich zu diesem Thema gesprochen“).

Hilfsbereitschaft
Menschen möchten anderen Menschen gerne helfen. Dies nutzen Angreifer aus, indem sie Verhalten anregen, dass jemandem vermeintlich geholfen werden soll (z.B. „Kannst du mir kurz helfen?“.)

Autorität
Hierbei nutzt der Angreifer die Hierarchien in einem Unternehmen aus (z.B. indem er sich als Vorgesetzter oder Behörde ausgibt „Ihr CEO braucht dringend die Informationen zu…“).

Lob / Schmeichelei
Immer wieder werden wir umschmeichelt, um unsere wertvollen Informationen preiszugeben (z.B. in Form einer Interviewanfrage „…Sie als Expert*in auf diesem speziellen Feld“)

…und wie wir uns davor schützen können:

Im beruflichen/ehrenamtlichen Kontext sind die IT-Abteilungen angesichts der ständigen Angriffe und Bedrohungen gut gewappnet und versuchen uns mit technischen Möglichkeiten so gut es geht zu schützen und fangen einen Großteil der Angriffe ab. Trotzdem bleibt dort und auch im Privaten ein Risiko, dem nur durch persönliche Aufmerksamkeit entgangen werden kann.

Was können wir also tun?

Software aktuell halten!
Es ist wichtig, auf allen Geräten (privat und beruflich) automatische Updates zu aktivieren oder regelmäßig selbst upzudaten, damit der technische Schutz aktuell und somit bestmöglich bleibt.

Wachsam bleiben!
Seien Sie vorsichtig bei ungewöhnlichen Anfragen – insbesondere, wenn Sie die oben genannten Manipulationsanreize wiedererkennen! Wird in E-Mails direkt nach Geld

oder Passwortdaten gefragt, ist dies zudem ein sicherer Hinweis auf Phishing (=das "Abfischen" von Zugangsdaten, Geschäftsgeheimnissen etc. über präparierte E-Mails, Nachrichten oder Anrufe). Achtung aktuell ist auch Phishing per Briefpost unterwegs, in dem per QR-Code auf gefälschte Zugangsseiten geleitet wird.

Nicht unter Druck setzen lassen!
Geben Sie niemals interne oder vertrauliche Informationen preis! Auch nicht, wenn vermeidliche Behörden, Vorgesetzte oder Autoritäten hinter einer Anfrage stehen. Versichern Sie sich immer genau, worum es geht, und fragen Sie – wenn möglich – Ihre IT-Abteilung, was sie von der Anfrage hält. Sätze wie „Handeln Sie jetzt!“ und „Nur noch wenige Stunden verfügbar“ oder „Wenn Sie jetzt nichts machen, sperren wir Ihren Account!“ sollten Sie stutzig machen! Versichern Sie sich daher immer genau, worum es geht.

Jeden Absender verifizieren!
Wenn auch nur ein leichter Zweifel besteht, prüfen Sie den Absender und die Adresse genau, beispielsweise indem sie die Adresse genau anschauen (Ist es die Adresse, die Sie kennen oder erwarten?) oder indem sie den Absender auf einem anderen Weg (Anruf) oder in einer gesonderten E-Mail kontaktieren. Bleiben Zweifel bestehen, lieber löschen und auf keinen Fall Anhänge öffnen oder Links klicken.

Vorsicht in sozialen Medien!
Je mehr wir über uns veröffentlichen, desto leichter wird es auch, Informationen über uns oder unser Unternehmen oder unsere Organisation zu sammeln. Achten Sie also auf das, was Sie im Internet hinterlassen (wollen) und passen Sie gegebenenfalls Ihre Einstellungen zur Privatsphäre an.

Informiert bleiben!
Halten Sie sich auf dem Laufenden, was aktuelle Betrugs- oder Phishingwellen angeht. Ihr Arbeitgeber/Ihre Hilfsorganisation bietet u.U. aktuelle Informationen überlaufende Phishing-Angriffe oder besitzt eine eLearning-Plattform zu Sicherheitsthemen. Vielleicht haben Sie solche Schulungen bereits absolviert. Eine gute Möglichkeit sich aktuell zu halten ist der Newsletter des Bundesamtes für Sicherheit in der Informationstechnik (BSI), den Sie unter: https://www.bsi.bund.de/DE/Service-Navi/Abonnements/Newsletter/newsletter.html abonnieren können.

Weitere Informationen:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html

www.allianz-fuer-cybersicherheit.de

https://sosafe-awareness.com/de/ressourcen/reports/human-risk-review/

Beißel, S. Evaluation von Security-Awareness-Maßnahmen, *Datenschutz und Datensicherheit* **43**, 287–291 (2019). https://doi.org/10.1007/s11623-019-1109-3

Erstellt im Projekt deFenSIO (www.defensio.de), stand 2024