1.6 Interview Social Engineering 08.07.2019

Prosodische Merkmale	Erklärung
(1) (2) (3)	Pause mit Sekundenlänge
[ahja] [mhm]	Redewendungen, die innerhalb des Kommunikationsbeitrags sind
{gleichzeitig}	Gleichzeitige Rede
E	Experte
M	Moderatorin
?	Steigende Endintonation (Frage)
.	Fallende Endintonation
<lacht>, <hustet>	Außersprachliche Handlungen
(unv)	Unverständlich

(M): Okay, dann herzlich willkommen zum Interview. Interview ist freiwillig. Sind Sie bereit ein Interview zu geben?

(E): ja.

(M): Gut, dann meine erste Frage wäre, was sind Ihrer Meinung nach, die wichtigsten Techniken, die Social Engineers benutzen?

(E): also, die erste Frage würde ich sagen, gibt es zwei unterschiedliche Methoden. Einmal eine offene und einmal eine verdeckte Methode. Die offene Methode ist für mich die wichtigste Technik im allgemeinen Bereich, wenn wir gerade nicht die Geheimdienste oder so was sehen. Die verdeckte wäre dann so was wie (1) ich spioniere, ich Telefonate abhöre und so was. Die offene ist im Prinzip Recherche im Internet (1) über social Media (1) und es ist für mich eigentlich so ist das wichtigste (1) dass ich so einfach schaue, welche offene Dinge sind dann vorhanden, zum Beispiel im Netz, im Telefonbuch, und solche Sachen (1) man kann ganz viel ablesen lassen für mich die wichtigsten Techniken des Social Engineering, also, die offenen (1) also, das heißt alle Informationsquellen, die mir offen zur Verfügung stehen. Und da kann ich schon ganz ganz viele Sachen rausbekommen.

(M): okay.

(E): ja, das ist eigentlich schon die erste Frage.

(M): ja, also, die Techniken sind ja nicht neu. Aber jetzt mit digitalen Medien werden sie neu ausgeführt.

(E): ja, genau. Du wirst effektiver, du kannst besser suchen. Jetzt gibt es mehr Digitalisierung. Das ist auf einer Seite schön, auf der anderen nicht. Wenn du alleine auf die Gesellschaften guckst, GmbH oder so (1) ist irgendeine Person als Gesellschaft da eingetragen ist alles digitalisiert, kann ich dir heute sagen stimmt die Ansage, dass er zum Beispiel als Gesellschaftsführer von sonstiges ist, wenn ich Verträge abschließe hat er Insolvenzen, so was kann ich dir sagen heutzutage kann man online rausbekommen. Ich kann SCHUFA-Auskünfte einholen. Im Prinzip hast du schon richtig transparente, gläserne Person, die du dir zusammenstellen kannst. Manches kostet ein bisschen Geld, wie ein SCHUFA Auskunft. Manches kriegst du ja wie gesagt „for free“ (1) zum Beispiel Vereine in diesem Ganzen XING Profil und so. Da brauchst du nur einmal anzuschauen und schon mal (1) oder LinkedIn. Da kannst du ganz viel rauskriegen. Schwierig ist es nur bei älteren Leuten oder so was (1) weil

die nämlich ganz wenig in diesen Profielen drinnen hängen (!) da hast du halt ein Problem ja (1) aber bei jüngeren Leuten, so in deiner Zielgruppe, total easy. Da gibt es wie gesagt, auch Suchtechniken. Da gibt es auch Maschinen, die auch schon die E-Mails weiter gucken. Wenn du in einer E-Mail eine neue generierst, gier was weiß ich was (1) Partnership Sachen das kann ich (2) das machen die Maschinen selber, da kann ich ganz genau sagen, die jetzt gerade was ich weiß ich kann ich nicht so sagen, kenne mich nicht so gut da aus (1) die jetzt gerade in einem Forum drinnen, oder in einem anderen. Kannst du heute mit wenigen Klicks machen. Deswegen sage ich Internet und Social Engineering – offene Medien (1) nichts verdecktes.

(M): ja (2) wie sieht Social Engineering in 5 Jahren aus?

(E): viel viel leichter als heute. Wegen der Digitalisierung. Ich glaube die Menschen werden keine besondere Resistenz bezüglich des Social Engineering entwickeln und ich glaube die Technik entwickelt sich schneller (1) also die Technik geht schneller voran als die Sicherheit. Im Vorgespräch hast du ein schönes Beispiel, hast du schon eine Antwort gegeben. Und zwar hast du einen Beispiel genannt mit Autofahren. Und erst dann kommen die Gesetzte, wenn schon z.B. ein Umfall passiert ist. Und in diesem Vakuum, bis die Gesetze da sind, und bis man das vielleicht technisch hinbekommt hat man ganz viel Potenzial (2) ich sage mal (1) ich sage jetzt ein Beispiel mit diesen ganzen Partnerbörsen. Das geht mir so auf den Senkel, wenn ich Fernseher gucke, und dann siehst du jede 5 Minuten Parship irgendwie so was aber das sind ja alles keine richtig geschützte Dinge! Da steht zwar Datenschutz drauf, aber vom Prinzip brauchst du dich nur einzuloggen und in Profil zu gehen und zu suchen. Die Suchmaschinen sind ja da! Also, das ist total (1) oder mit einem Bot, die machen das automatisch, da brauche ich kein Schutz, da hat sich auch keiner Gedanken gemacht, wie schütze ich denn da eigentlich die Zugänge, deswegen in 5 Jahren, das wird immer transparenter, außer bei den Leuten, die jetzt sagen, ich verzichte radikal auf Digitalisierung. Also, für mich es ist immer so, dass ich über Person gehe (1) also, ich verurteile die Medien nicht. Ich nutze sie selber. Aber ich gucke manchmal auch, gerade, wenn ich irgendwelche Anfragen von Personen kriege, ob die mich belügen oder nicht. Und das kriegt man eigentlich relativ gut und leicht raus.

(M): ja. okay, zu dem Punkt kommen wir dann später, wenn wir über Schutzmaßnahmen sprechen. Meine nächste Frage wäre, welche Techniken werden dann wichtiger und warum?

(E): meinst du jetzt, wie ich mich vor Social Engineering schütze, oder welche Techniken werden Social Engineers in der Zukunft entwickeln?

(M): ja, entwickeln.

(E): Ja, also, die Frage ist, wie wird sich dann Social Engineering weiter entwickeln. Welche Techniken werde wichtiger?

(M): also, ja, ich denke, dass Social Engineering Technik in wenigen Bereichen noch die verdeckte stattfinden wird. Also, ich kenne es nur aus meiner vergangenen Tätigkeiten, wir mussten mehrmals die Geschäftsleitung auswechseln, weil sie im Hotels kompromittiert worden waren, dann wurden sie erpresst (2) dann denke ich Mal in solchen Ebenen, wenn es um wirtschaftlichen starken Interessen geht, dann wird dann auch diese verdeckte mit Honeypot und wie man das so alles nennt, wird aber im allgemeinen um schnell an Geld zu kommen, oder um die Leute zu überzeugen eine Waschmaschine zu kaufen auf ihrem Portal (1) [mhm] da kann man auch Werbung machen auf der Seite und so was (2) also, in der Zukunft wird elektronisch ganz viel gemacht werden. In dem ich einfach das Konsumverhalten [mhm]

Phishing, oder es wird ja dann auch Anbieter geben, dass ich dann auch das Konsumverhalten voraus einschätzen kann, gibt es schon was, macht Google, musst dann einfach auf die Seiten gehen und da siehst du, wo du gerade auf die Seiten warst. Das gibt das Protokoll schon her. So ein Übertragungsprotokoll wo war vorher und so. Solche Sachen werden dann wichtiger, und dann würde ich gezielt in Konsum animiert. Das nenne ich auch Social Engineering. Also, nicht unbedingt um jemandem zu schaden, sondern hier geht's um Masse, um Produkte, auch mal um schlechte Produkte an einen Menschen zu bringen und zu verkaufen.

(M): ja. Alles klar. ja. Ich würde gerne über das Social Engineering in Bezug auf das Unternehmen sprechen. Wir haben schon ein bisschen darüber gesprochen. Aber was meinst du, welchen Einfluss bzw. wie wird Social Engineering in Bezug auf das Unternehmen ausgeführt.

(E): ja, also, Social Engineering in Allgemeinen (1) werde ich als „immer geringer" bezeichnen, es sei denn (1) die Länder schotten sich mehr ab, kann ich sagen mehr geringer, weil wir teilen sowieso schon alles: Aktien, Anteile werden von ausländischen Stakeholdern, Regierungsstakeholdern, wir kaufen Unternehmen ab, oder das KUKA ist, oder sonstiges. Deutsche Unternehmen, französische Unternehmen, aber die Besitzer sind alle ausländische Investoren. Und ich sage so mal, die haben Zugänge zu allen Informationen, da brauche ich nicht nochmal irgendwelche Geheimnisse, irgendwelche Sachen geheim zu haben, weil das sind meine Besitzer, meine Eigentümer. Das einzige, wo ich mir Social Engineering vorstellen könnte, ist wenn ein (1) ich spinne mal einfach ein Fall. Hat mir der Realität nichts zu tun, aber wenn ein Unternehmen, zum Beispiel neue Märkte erobern möchte, wie zum Beispiel in Russland. Da gehen natürlich Leute hin, machen Scouting, oder Verhandeln auch wegen Grundstücke mit Bürgermeistern oder mit Landesfürsten, und das kann ich mir schon vorstellen, in solchen prekären Situationen, dass da persönliches Social Engineering betrieben wird, wie gesagt, weil man da die Leute erpressen kann für Verträge oder Vertragsabschlüsse. Genau (1) eine ist allgemeine Wirtschaft und das andere ist skizielte Verträge und da wird es sicherlich über Social Engineering, XING und sonst was nachgeguckt, was macht man privat, wofür interessiert man sich? Geht man wandern, ist er im Wanderverein? Dann gehe ich auch zum Wanderverein, schicke dann auch hübsches Mädel hin und da ist das gleiche Spiel, und das wird immer so sein. Aber im Einzelfall.

(M): okay, ja. Also, das war jetzt so eine Perspektive von Oben. Welche Techniken werden eingesetzt um Unternehmen zu hacken, im Sinne um jeden einzelnen mit dem Angriff zu erreichen.

(E): ich glaube das wird keine Rolle mehr spielen. Weil früher waren die Unternehmen nicht so vernetzt. Wenn ich alles zentralisiere, dann kriege ich alles einfacher, wenn ich große Systeme habe, die habe ich zentralisiert. Ich habe, wie gesagt, keine dezentrale Systeme. Und wenn ich erstmal Eigentümer bin, dann es ist mir egal, ob ich die Unterlage (1) ob es Herr Müller erstellt hat, oder Frau Müller oder wie auch immer. Das liegt sowieso zentral in einer großen Datenbank, ich muss mir nur bedienen und wenn ich die Firma gekauft habe, kann ich mich jeder Zeit (unv) und wenn ich da noch externe einstelle als Manager, die das für mich schaffen, weil ich kann so einen einstellen, weil ich der Eigentümer bin. Also, es ist ganz einfach, wir brauchen überall Schutz im Unternehmen, in der Form, wenn wir gerade nicht im militärischen Bereich handeln, vergiss es (1) für mich gibt es kein Schutz. Alles komplett transparent. Da brauchen wir über Social Engineering in der Form nicht zu reden. Ich glaube viel mehr, dass die spätere Rolle im Unternehmen so sein wird, einzelne Leute zu

kompromittieren, dass man sich Leute fügig macht. Das habe ich persönlich mehrfach erlebt. Das man gegen Leute geht, um andere Interessen durchzusetzen. Und nicht unbedingt wirtschaftliche, sondern auch persönliche Interessen. Stellenbesetzung ist so ein Thema. Das ich dann zum Beispiel sage, dem Kollegen, ich möchte den gerne mit Social Engineering beglücken, da kriegt man vielleicht den raus. Also, Machtposition ausbauen. Also, ich kenne auch Leute im Unternehmen, so wie ich es im Vorgespräch gesagt habe, gucke ich, dass es bei mir sich einer meldet, wo kann ich den zuordnen, lügt er mich an, und andere, die gehen in Gespräch rein, wenn sie auch innerhalb des Unternehmens sprechen, was macht er. Social Engineering fängt zum Beispiel an, wenn ich zum Beispiel beim Herrn Prof. so und so im Büro bin, und sehe dann auf dem Schrank sehe ich da eine Golffigur. Dann weiß ich schon, wie ich mit dem rede, was er für Hobbies hat, was er eigentlich macht, was Profis machen. Auch bei uns im Unternehmen, ich kenne einige, sie lassen sich erstmal einen Vortermin geben, sie gehen ins Büro, sie wissen ganz genau pass auf, die hat die und die Hobbies, ob es Familie ist, ob er ein Wander-Spack ist, ob das China ist, und so bauen ihr die Gespräche auf. Das ist schon ein verdecktes Social Engineering. Das ist schon Manipulation. Es geht immer um die Vorteilsschaffung. Und da sehe ich dieses Social Engineering, diese Bewusste sich ein Vorteil gegen anderes zu verschaffen. Macht eine andere Person zu steuern. Das ist für mich Social Engineering.

(M): Okay, dann gehen wir weiter (1) meine nächste Frage ist, wie kann ein ganz normaler User kein Opfer von Social Engineering werden? Privat und dann auch im Arbeitsleben?

(E): ich werde so ein Standartantwort geben. Eine Standartantwort wäre für mich erstmal zu überlegen, in welchen Foren, auf welchen Seiten muss ich mich rumtreiben. Muss ich jetzt zum Beispiel offene Gruppen nutzen, oder muss ich geschlossene Gruppen nutzen. Ob es WhatsApp ist, ob es Facebook ist, ob es verschiedenste andere Sachen sind, weil ich kann immer Communities aufbauen. Und ich würde mir immer überlegen, ob ich irgendeiner Community beiträte oder nicht. Ich kenne es selber. Ich habe LinkedIn, ich habe da auch ein Profil (1) ich kriege permanent irgendwelche Anfragen in LinkedIn oder XING, ist genau das gleiche. Wo ich schon immer sage, das geht gar nicht, ich habe da schon Profile gelöscht, da sieht man schon ganz genau, der arbeitet da, der macht das, der hat die Rolle und dann schreibe ich dahin. Das heißt auch bewusstes Umgehen auch mit Social Media. Und ganz allgemein, sage ich jetzt, bewusst, wenn du nicht die Person des öffentlichen Interessen bist, wie ein Schauspieler, oder Wirtschaftsboss, oder so dann wird dich diese verdeckte Vermittlung nicht erwischen, dass einer deiner Papierkörbe durchkramt, nicht weil du bist zu wichtig, hier geht es darum, bei Social Media , wo treibe ich mich rum. Weil eins kam auch immer wieder, auch in der Vergangenheit. Das sage ich zum Beispiel bei meinen Kindern auch. Die stellen auch zu viele Bilder von ihren Freundinnen und dann haben sie eine neue Freundin oder wie auch immer, oder auch die Mädels, die kommen immer rein bei uns, machen das Ding an und teilen erstmal mit ihrer Familien, wie wir leben. Da kriege ich Pickel. Die schmeiße ich raus! Weil so was geht gar nicht. Weil du siehst dann ganz genau, in welchem Lebenszustand oder Wohnzustand du gerade bist, und du weißt gar nicht, wer das alles kriegt. Und so was komplett weg.

(M):Okay, danke. Meine nächste Frage ist, haben Sie jemals einen Social Engineering-Angriff erlebt bzw. gemacht? Könnten Sie bitte über diese Erfahrung erzählen?

(E): ja, also gemacht nicht, aber miterlebt schon. Auf einer Arbeitskonferenz, wo auch verschiedene Lieferanten und so weiter miteingeladen wurden, haben wir super viele Geschenke und Kleinlichkeiten bekommen, diverse Booklets, Kugelschreiber, was weiß ich

was alles. Und eben unter anderem ein Paar USB Sticks, ohne Logo ohne gar nichts, von einer sage ich jetzt mal Fremdfirma, es war eine chinesische Firma. Diese USB-Sticks und der ganze Kramm habe nicht ich bekommen, sondern ein anderer Kollege an einem Stand. Mit dem haben wir auch früher zusammen gearbeitet damals und ich habe selber die Sensibilisierung-Schulungen unter anderem auch gemacht. Auf jeden Fall kommt der Kollege zu mir und sagt zu mir (1) du, pass auf, ich habe echt viel Kramm gescheckt bekommen, auch irgendwelche USB-Sticks. Ich habe das Gefühl, man muss die erstmal bei Werkschutz oder so was überprüfen lassen, bevor wir die überhaupt benutzen. Dann habe ich gesagt, ja, aber wir dürfen so was überhaupt nicht nutzen, die USB-Sticks sind das unsicherste überhaupt. Wir lassen die checken, bei Werkschutz oder CERT oder keine Ahnung wo, aber wir benutzen die nicht.

(M): okay. Waren die USB-Sticks dann tatsächlich unsicher oder kompromittiert?

(E): ja na klar. Die Firma haben wir auch dann nie wieder getroffen. Ich weiß nicht, ob Rechtsschutz sie sogar angeklagt hat. Fakt ist – egal was man auf so einer Veranstaltung bekommt, ob es ein USB-Stick ist, oder ein Präsenter oder keine Ahnung was. Man darf es nicht benutzen, nicht mal auf der Arbeit, nicht privat. Wenn es natürlich interne Sachen sind, dann es ist eine andere Frage. Jedoch mit diesem USB-Anschluss muss man schon vorsichtig sein.

(M): Okay ja. Meine letzte Frage wäre, welche Maßnahmen sollten ergriffen werden, um das Awareness für Social Engineering zu fördern?

(E): das sage ich immer wieder, wir müssen unsere Systeme patchen. Also, jetzt zurzeit geht es nicht darum, dass wir alle Angriffe verhindern und beheben, es geht darum, dass wir schwache bis mittlere Angriffe verhindern, denn richtig also ich sage jetzt richtig gute externe Hacker, die wirklich vorhaben einen Schaden ins Unternehmen zu bringen, finden immer einen Weg. Und natürlich Sensibilisierung ist eine große und wichtige Frage. Wir machen eigentlich viel zu wenig für unsere Mitarbeiter und wir kommen sogar mit der ganzen Information Sicherheit nicht hinterher. Es ist alles schon veraltet wir können nicht diverse Zielgruppen einfach zu dem Thema abholen. Wir müssen echt regelmäßig verpflichtend die Schulungen anbieten und die Mannschaft richtig schulen, mit Spielen oder mit Unterweisungen oder mit allem zusammen. Aber wir müssen es machen, und je mehr wir es machen desto besser.

(M): vielen Dank, hast du vielleicht etwas, was du zu dem Thema hinzufügen könntest?

(E):...nein, ich glaube ich habe alles gesagt, ja wir müssen jetzt zu einem anderen Termin.

(M): stimmt. Vielen Dank für deine Zeit und ich werde dich auf dem Laufenden halten, was meine Promotion betrifft.

(E):Danke, darauf freue ich mich.