1.5 Transkript Interview Social Engineering 24.06.2019

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 (2) ich hoffe die Aufnahme funktioniert jetzt (1) okay, scheint zu funktionieren. Dann herzlich willkommen zum Interview. Dieses Interview ist freiwillig. Am Anfang jedes Interviews soll ich hinweisen, dass dieses Interview freiwillig ist und aufgenommen wird. Bist du bereit ein Interview zu geben?

(E): ja.

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

(E): Also, generell würde ich Social Engineering als eine Manipulationsmethode bezeichnen. Es kann alles sein (1) ein nettes Gespräch irgendwo auf einer Messe oder im Hotel auf einer Konferenz (2) oder eben eine digitale Methode (1) so was wie eine Phishing Attacke (2) Social Engineers benutzen eigentlich ganz alte Manipulationsmethoden. Die Art und Weiße (2) also wie sie manipulieren und warum hat sich geändert.

(M): Okay, kannst du vielleicht ein Paar Beispiele dazu nennen?

(E): ja natürlich. Wenn früher wollten die Soziale Engineers <lacht> oder Diebe in Besitz von gewissen Objekten kommen, jetzt ist die Besitzung von Informationen eher interessant. Wie kommen sie dazu? Also zum einen können sie natürlich im wahren Sinne des Wortes IT-Systeme hacken (1) gut, das ist ein bisschen kompliziert und benötigt spezielles Wissen. Zum anderen können soziale Engineers oder Hacker tatsächlich Menschen hacken um an die gewisse Informationen ran zu kommen.

(M): okay, ja.

(E): also, die typischen Beispiele sind (1) naja das erste was mir einfällt ist Phishing. Es ist eine Art des Angriffs (2) also wenn der Hacker versucht durch eine E-Mail mit zum Beispiel einem schädlichen Link oder mit einem bösartigen Anhang eine Person oder ein System auf dem Computer zu hacken, so zu sagen. Wir in der IT-Sicherheit unterschieden zwischen einer Phishing-Welle und einer Spear-Phishing-Methode. Was ist dann der Unterschied zwischen den beiden Methoden? Ja, es ist ganz leicht zu erklären. Mit Phishing-Welle versuche ich möglichst viele User zu erreichen und hoffe, dass möglichst viele auf den Link klicken oder den Anhang öffnen. Die Phishing E-Mail in dem Fall ist nicht wirklich personalisiert, fängt mit „Hallo lieber User“ oder „Sehr geehrte Damen und Herren“ solche Geschichten. Der Inhalt

dieser E-Mail dann auch eher generisch, so was wie „Herzlichen Glückwunsch, Sie haben ein Million Euro gewonnen, um Ihre persönlichen Daten zu bestätigen, klicken Sie auf den Link“ <lacht>, oder eine andere E-Mail „Ihr Packet konnte nicht geliefert werden, bitte klicken Sie auf den Link um die Lieferzeit zu bestätigen“ so was (2) Dazu muss man sagen, dass die Hacker verschiedene Manipulationstechniken benutzen (1) Also es könnte wirklich eine Super-Überraschungs-E-Mail sein, wie ich schon gesagt habe, so was wie „Sie haben ein Million Euro gewonnen“ <lacht> oder eine Bedrohungs-E-Mail, wie „Um Ihre Mahnung zu bezahlen klicken Sie hier“ etc (2) Genau. Also solche Geschichten. Klar, wenn ich zum Beispiel weiß, dass ich in der letzten Zeit nicht Lotto gespielt habe <lacht> oder nichts bestellt habe, dann ignoriere ich es. Aber wenn der User nicht sensibilisiert genug ist, dann klickt er oder sie darauf, weil man ist verunsichert (2) ja (2)

(M): ja, also das war quasi Phishing-Welle?

(E): genau ja.

(M): du hast noch eine andere Phishing-Methode erwähnt und zwar Spear-Phishing?

(E): ja habe ich, danke <lacht>

(M): kannst du vielleicht dazu was sagen?

(E): klar <lacht> Also, der einzige Unterschied ist, dass der Hacker die Spear-Phishing Attacke elaborierter gestaltet. Spricht, er haut nicht 100 000 generische infizierte E-Mails raus, sondern untersucht sein Opfer und bereitet diese Attacke schon vor. Sprich, der Hacker untersucht ganz genau, zB in sozialen Medien etc., ob sein Opfer ein Mitglied in einem Sportverein ist, oder gerne reist, oder gerne kocht etc. und benutz die gewonnenen Informationen für die Spear-Phishing Attacke. Davor kann der Hacker z. .B den Kontakt herstellen und mit seinem Opfer telefonieren etc. (2) ja, aber solche Geschichten betreffen eher sage ich jetzt mal, irgendwelche Promis, oder Politiker oder Sportler. Also, wo es sich quasi für den Hacker lohnt, die Zeit und eventuell das Geld für die Vorbereitung reinzustecken (2) ja (2) Aber die psychologischen Methoden, die der Hacker benutz sind die gleichen wie bei der Phishing-Welle. Mein Opfer, sei es irgendein generischer User oder eine definierte Person muss neugierig werden oder vielleicht überrascht werden, damit sie quasi eine E-Mail erstmal öffnen.

(M): Ist es aus deiner Meinung die wichtigste Methode, die social Engineers benutzen?

(E): ja und nein <lacht> ich glaube die Kombination macht schon aus. Vor allem wenn es sich um den Einzelangriff handelt. Sei es eine Person oder eine Organisation (1) Wenn es tatsächlich um so einen Einzelangriff geht, dann muss der Hacker quasi mehrere Methoden benutzen, um erfolgreich zu sein <lacht> Wir in der IT-Sicherheit kennen das. Deswegen sind diese ganzen sage ich jetzt mal blöde Regeln und IT-Systeme mit Firewalls etc. entstanden.

(M): was wären aus deiner Sicht dann die wichtigsten Methoden außer Phishing?

(E): also, eine Phishing-Attacke an ein Unternehmen hat nur dann Erfolg, wenn aus verschiedenen Seiten angegriffen wird. Wenn zum Beispiel es versucht wird, ins Server-Raum reinzukommen (2) deswegen sind die ja meistens <lacht> so besonders geschützt, oder wenn der Hacker versucht einen persönlichen Kontakt herzustellen, per Anruf (1) wie es jetzt heißt (2)

(M): meinst du Vishing?

(E): <lacht> ja genau, Vishing (2) oder wenn man versucht mit fremdfirmen Hardware oder USB-Sticks, die man als „Geschenk“ auf einer Messe bekommen, den Zugang zu einem oder anderem System zu schaffen. Deswegen sind es bei uns so viele Regeln und deswegen soll man bei uns immer mehr Sensibilisierung schaffen, denn obwohl die psychologischen Manipulationsmethoden nicht neu sind, entwickeln sich die ganzen Techniken weiter. Und wenn früher muss der Hacker physisch in einem Server-Raum sein, um den Zugang zu den Systemen zu bekommen, muss der Hacker jetzt nicht im Land sein, um die ganzen Zugänge zu schaffen. Natürlich, ohne Digitalisierung läuft gar nicht das ist ganz klar (2) aber man muss sowohl im privaten Kontext als auch im Beruf vorsichtiger damit umgehen (2) ja.

(M): okay, auf meine nächste Frage hast du schon teilweise geantwortet, aber vielleicht könntest du ein paar Beispiele nennen, wie sieht Social Engineering in fünf Jahren aus?

(E): ja (2) also es wird auf gar keinen Fall weniger <lacht> Drum rum kommen wir da nicht, vor allem hier in der Informationssicherheit, wir sind ja an der Quelle <lacht> Frag mal die Jungs aus CERT, wie viele Anfragen und mit wie vielen Problemen sie jeden Tag zu tun haben <lacht>

(M): ja das stimmt.

(E): ja, also es ist ein bisschen kompliziert jetzt darüber zu philosophieren, welche Techniken etc werden wichtiger und warum.

(M): ja, aber was wäre jetzt diene persönliche Meinung dazu?

(E): ja okay (2) [mhm] (3) auf jeden Fall das Ziel der Hacker wird der Diebstahl der persönlichen Daten sein. Sei es, mein Bankkonto, oder meine Fingerabdrücke <lacht> oder meine Passwörter bei der Smart-Home App. Also, alles was meine Persönlichkeit betrifft wird als Ziel definiert, meiner Meinung nach. Wir werden digitaler, wir werden vernetzter, und somit wenn der Hacker ein Passwort von irgendeinem App kennt, ist es quasi so, dass er ganz schnell den Zugang zu meiner Arbeits- oder Privat-E-Mail hat oder Zugang zu meinem Online Banking so was. An sich interessiert den Hacker nicht, wie viele physische Scheine hat man im Portemonnaie <lacht> ich habe übrigens nie Bargeld.

(M): ich auch nicht, ich glaub ich habe nicht mal 2 Euro Bargeld für den Einkaufswagen im Supermarkt.

(E): ja bei mir auch genauso <lacht> genau, also zurzeit wird der Dieb nicht dein Portemonnaie klauen, denn da gibt es kein Geld <lacht> sondern er ist mehr sagen wir an deinem Laptop oder an deinem Handy interessiert, denn da hast du so gesagt dein Geld, deine Apps, deine Informationen. Und diese Informationen kann der Hacker schon in reales Geld konvertieren. Deswegen denke ich mal, dass es in der Zukunft mehr Angriffe auf der digitalen persönlichen Ebene sein wird. Schon nicht mal „Klicken Sie auf den Link“, es werden bösartigen Programme geben, die aktiviert werden, selbst wenn man eine Phishing E-Mail aufmacht so was. Und natürlich die Angriffe werden elaborierter, weil die meisten Menschen mit der Zeit einfach ein gewisses Level von der Sensibilisierung haben werden. Deswegen werden die Hacker gezwungen, die Angriffe so zu gestalten, dass sie einerseits das Interesse wecken und anderseits dass das Grundvertrauen trotzdem da ist. Dass der User quasi interessiert ist, aber die innere Alarm nicht angeht. Welche Methoden dazu benutz werden (2) das kann ich leider nicht sagen. Aber dass die persönlichen Informationen angegriffen werden, das ist 100 % (3)

(M): okay, also meine nächste Frage lautet (2) welche Techniken werden wichtiger und warum, vielleicht kannst du ganz kurz zusammenfassen, welche Techniken deiner Meinung nach werden wichtiger und warum?

(E): ja (2) also, wir benutzen jetzt E-Mails, diverse Messengers und Handys als Kommunikationstools, und ich glaube es bleibt erstmal so. Deswegen meiner Meinung nach, werden diese Kommunikationstools auch bei den Hackern benutz, um an die diverse Informationen ranzukommen. Sprich, es wird eine Art weiter Phishing geben (2) Vishing und Spam-Nachrichten in Messengers geben. Das ist meine Meinung (2) Natürlich werden die Hacker versuchen nicht nur weiter die Menschen zu hacken, sondern auch die IT-Seite also IT-Systeme zu hacken. Aber das ist dann ein anderes Gespräch <lacht>

(M): okay, also deiner Meinung nach, bleibt die Phishing oder Vishing Methode als Hauptmethode der Social Engineers?

(E): ja, genau (2) und auch natürlich werden die ganzen Messengers angegriffen.

(M): okay, danke für die ausführliche Antwort, gehen wir weiter (2) so, meine nächste Frage wäre, in welchem Bezug steht Social Engineering zu einem oder besser gesagt zu unserem Unternehmen?

(E): ja, eine interessante Frage <lacht> ich glaube, dass soziales Engineering ist eher uninteressant und nicht so präsent in Bezug auf unseren Unternehmen. Wir arbeiten so eng mit anderen Marken (1) und anderen Unternehmen, dass ich glaube im großen und ganzen ist der Mitarbeiter an sich nicht so betroffen von social Engineering (2) Was aber betroffen sein kann ist natürlich das Image vom Unternehmen. Und somit dann natürlich der jeweilige Mitarbeiter oder Manager (2) wenn sage ich jetzt mal, irgendwelche Strategie-Geheimnisse oder Preise oder irgendwelche steuerliche Sachen nicht ganz sauber waren (2) wenn so was rauskommt, dann es ist natürlich Image-Schaden und Image-Verlust fürs Unternehmen (2) oder wenn Kundendaten betroffen sind. Nehmen wir an, da ist es ein Datenleak im System, und 10 000 Kundendaten (1) Passwörter, E-Mail Adressen, VINs, etc. (2) das ist auch eine Art social Engineering, wo quasi wir als Unternehmen betroffen sind.

(M): okay (1) ja.

(E): also, meiner Meinung nach, sind wir dann als Unternehmen betroffen, nur wenn wir ein Image-Schaden haben. Im Kontext von einem ganz normalen Mitarbeiter ist es auch meiner Meinung nach erstmal nicht so präsent.

(M): ja, verstehe. Dann gehen wir weiter (2) wie kann ein durchschnittlicher User kein Opfer von Social Engineering werden (privat und im Arbeitsleben)?

(E): ja, auf jeden Fall Passworthygiene muss sein <lacht> also, sprich man benutz nicht dasselbe Passwort oder ähnliches Passwort für alle Systeme oder Portale. Man benutz kein Fremdfirmenhardware. Ja, und natürlich das Thema Phishing. <lacht> also, eigentlich alles was wir an Rechtlinien haben muss man schon beachten. <lacht>

(M) Kannst du vielleicht das ein bisschen detaillierter erklären?

(E): ja, klar (1) also, nehmen wir das Thema Phishing. Wie kann ein User kein Opfer von einem Phishing-Scam werden? Erstens muss man schauen, wer ist der Absender. Wenn die E-Mail von (2) nehmen wir an, wenn die E-Mail von Telekom kommt, aber in der Absender-Adresse

kein Telekom steht, oder wenn die Absender-Adresse irgendwelche komischen Zahlen, Namen etc beinhaltet, dann könnte es das erste Zeichen einer Phishing E-Mail sein. Zweitens, der Inhalt der E-Mail (2) also, worum geht es, wenn es generisch und unpersonalisiert (2) wie man schön uncustomized sagt und (1) ich sage jetzt (1) kurz vorkommt, dann ist es auch (1) höchstwahrscheinlich eine Phishing-Email. Die selben Regeln gelten halt für privat (1) und beruflich. (2) ja, was noch (1) Auf gar keinen Fall soll man auf verdächtige Links in solchen E-Mails klicken, oder irgendwelche Anhänge aufmachen (2) Wenn der Inhalt schon nicht stimmt, oder verdächtig ist, dann sind Links und Anhänge garantiert auch nicht vertrauenswürdig. Ja.

(M): gibt es noch irgendwelche Wege über die einen die social Engineers erreichen können? Privat oder beruflich?

(E): ja, vielleicht noch das Thema Informationsschutz an sich (2) und need-to-know-Prinzip. Das heißt ich schütze die Informationen zu den ich Zugriff habe.

(M): inwiefern?

(E): ja, ich schütze Informationen zu denen ich den Zugriff habe, indem ich die Informationen nach der Klassifizierungsstufen behandle (2) Wenn ich Zugang zu den sensiblen Informationen habe, behandle ich diese Informationen entsprechend, zum Beispiel ich verschlüssle meine E-Mails (2) ich erzähle davon nicht in meinem Freundeskreis etc. (2) ich fotografiere diese Infos nicht und poste sie nicht in meinen sozialen Netzwerken. Abgesehen davon, haben wir überhaupt einen Foto-Verbot auf dem Werksgelände <lacht> und man muss sich eine Genehmigung holen, um ein Foto machen dürfen <lacht> Also, solche Sachen, ich bin vorsichtig was meine privat Sphäre und meine eigenen sensiblen Daten angeht.

(M): ja, verstehe. Hast du noch was zu dem Thema?

(E): nein (2) glaube ich nicht. Also, meiner Meinung nach, man muss schon ziemlich vieles kritisch betrachten und wirklich keine dubiösen Links anklicken <lacht>

(M): <lacht> okay, ja, da hast du schon Recht. Wenn du nichts zu dem Thema mehr hast, dann gehen wir eben weiter. Meine nächste Frage wäre (1) hast du jemals einen Social Engineering-Angriff erlebt bzw. gemacht? Kannst du von der Erfahrung berichten?

(E): ob ich einen Social Engineering-Angriff erlebt bzw. gemacht habe [mhm] ja, erlebt auf jeden Fall. Zählt eine Phishing E-Mail als Social Engineering-Angriff?

(M): ja, ich denke schon.

(E): dann erlebe ich die social Engineering Angriffe jeden Tag <lacht> aber generell außer Phishing, weiß ich nicht [mhm] ja gut doch, manchmal testen wir unsere IT-Systeme selber anhand von Pentest. Aber das ist ja kein social Engineering in dem klassischen Sinne [mhm] ne, ich habe nur Phishing erlebt.

(M): Hast du jemals einen Social Engineering-Angriff dann selber gemacht?

(E): selber gemacht auch nicht <lacht> warum nimmst du das alles auf noch mal? <lacht>

(M): ja, ich möchte halt wissen, wie die Hacker ticken <lacht>

(E): nein ich verstehe. Ne, selber habe ich aber keinen Social Engineering-Angriff gestaltet (2) nur erlebt <lacht>

(M): okay, dann gehen wir zu dem anderen Thema und zwar (1) das ist übrigens meine letzte Frage an dich heute. Welche Maßnahmen sollten ergriffen werden, um das Awareness für Social Engineering zu fördern?

(E): also ja (2) schulen und sensibilisieren, so viel wie es nur möglich ist.

(M): ja, okay.

(E):Also, ich sage jetzt nicht nur einfach irgendeinen 90-minutigen Vortrag über DSGVO bei dem alle einschlafen, sondern verschiedenes Angebot mit möglichst vielen Formaten (1) digital und offline (2) in einer Gruppe oder separat (1) so was (1) zu ganz verschiedenen Themen, wie Phishing, Passwortmanagement etc. Also schulen, schulen und nochmal schulen.

(M): okay, alles klar. Hast du zu der Frage oder generell zu dem Thema irgendwas was du gerne hinzufügen würdest?

(E): ich überlege grad (2) nein, denke ich nicht, ich habe alles gesagt.

(M): okay, dann vielen lieben Dank für deine Antworten und für das Interview. Hat mir Spaß gemacht und ich werde dann von den Ergebnissen meiner Dissertation mal berichten!

(E): danke dir und ja, hat Spaß gemacht dir ein Interview zu geben.