## 1.7 Interview Social Engineering 05.08.2019

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

(M): herzlich willkommen zum Interview 3. Sind Sie bereit ein Interview zu geben? Die Teilnahme ist freiwillig. Ich muss Sie darauf hinweisen!

(IP): Ja, gerne!

(M): okay, super! Dann meine erste Frage ist, was sind Ihrer Meinung nach, die wichtigsten Techniken, die Social Engineers anwenden und warum?

(IP): die wichtigsten (2) also, aus meiner Sicht gibt es ganz unterschiedliche Arten mit Social Engineering umzugehen. Aus meiner Sicht das ist die Frage aus welcher Motivation die Angreifer vorgehen. Einmal kann ein Social Engineer unterwegs sein und sagen „ich mache es im Sinne einer Maßenabfrage“. Typisches Beispiel sind: Phishing E-Mails dann. Das heißt ich gestallte einen Angriff, den ich möglichst auf eine große Zielgruppe verwenden kann. Typische andere Variante ist Anruf.

(M): also, Vishing.

(IP): also, ich habe mindestens schon 3 Anrufe privat bekommen. Wo jemand gesagt hat „Hallo, hier ist Microsoft aus Kalifornien“ <lacht>. Manchmal wird Spaß daraus gemacht, aber (1) egal. Von daher, wenn es auf die Masse geht, dann eher generelle Telefonanrufe, Vishing E-Mails. Wenn es spezifisch wird, dann glaube ich ganz entscheidender Punkt ist dass (2) eine Kombinatorik angewendet wird. Das ist viel Phishing, dass man sagt, okay, ich sehe mal zu, dass ich in die interne Kommunikation einer Firma versuche (2) nachzustellen und dann so eine E-Mail versuche nachzusenden. Oder auch was auch in der Praxis ist, dass die Kombination angewendet wird. Erstmal eine E-Mail geschickt, die so aussieht, als ob, da ist auch kein böser Link ist (1) wenn ich gucken würde, ist da ein böser Link? Ne. Die sieht ganz normal aus, also ich musste mich irgendwie nicht vorfürchten. Dann bekomme ich einen Anruf aus irgendeinem Sekretariat, dann anschließend Anruf von einem Chef und von einem Dritten, der sagt mir so, Mensch, Sekretariat hat Sie doch angerufen, es wird ein Netz aufgebaut (2) und ich glaube, die zweite wichtige Technik, sehr spezifischer wird, dass ich hingehe und sage, ich spinne ein Netz aus verschiedenen Fakes, solange dass ich schaffe meinen Angegriffenen einzuwickeln und dass er dann in die Drucksituation gebracht wird und schnell reagieren muss.

(M): okay, wenn wir schon beim Thema Phishing sind, meine kurze spontane Frage

(IP): also, ich konnte natürlich weiter gehen (2) das wäre jetzt mehr Richtung Technik gewesen (2) natürlich kann ich Social Engineering sehr einfach auf dem privaten Ebene oder auf die persönliche Eben bringen zu sagen, ich lerne jemanden kennen, in einem Hotel, wie auch immer, es gibt ja typische Geschäftsreisenden –Hotels. Und dort wird das Ganze (2) man wird es in ein Gespräch verwickelt (2) also, private, persönliche Gespräche, wo man sich auch vielleicht vorstellt ich bin von dort und dort. Und dann glaube ich einer der wichtigsten Punkte beim Social Engineering, dass (2) a, versucht wird Vertrauen zu gewinnen.

(M): ja.

(IP): b (2) vielleicht über soziale Medien einige Informationen eingeholt worden sind (2) um zu wissen, wo kann ich meinen Gegenüber packen, wo seine Interessen und dann c (2) vielleicht kann ich hingehen über den Social Engineering und sagen, ich gehe ran an den, der richtig Geschäftsführung übernimmt und von daher Informationen hat, oder auch was sehr fruchtbar sein kann, ich gehe an den Techniker heran und versuche ihn im persönlichen Gespräch vielleicht sogar vor mit Internetrecherche auf das zu triggern, worauf er stolz ist (2) Häufig fängt er an darüber zu erzählen, weil er so begeistert ist davon. Also, von den Techniken her, ist dann Anruf, persönlicher Kontakt, E-Mail. Kann auch eine Kontaktaufnahme über Social Media sein. Wobei, damit habe ich nicht so viel Erfahrung mit. Aber die jüngere Generation natürlich (2)

(M): ja

(IP): vielleicht mit Facebook, oder Whatsapp (2) Und dann mit anderen. Und dann das Vorgehen dann entweder gestreut oder dann mit der Kombinatorik, wenn ich sage dann ich habe ein Ziel.

(M): kurze Frage dann zum Thema Phishing. Also, Phishing jetzt (1) wie du schon sagtest, nicht immer so ein Link, klick dadrauf. Oder hier ist ein Anhang klick dadrauf! Was denkst du, wird Phishing sich irgendwie verändern in dem Sinne? Aus deiner Erfahrung? Oder wird es immer so, klick drauf! Öffne den Anhang.

(IP): ja [mhm]

(M): wie hast du es erlebet? Hast du irgendwelche Gedanken dazu?

(IP): [mhm]

(M): ja, weil ich schon gehört habe, dass man gar nicht auf einen Link oder einen Anhang öffnen. Du musst nur eine E-Mail öffnen.

(IP): ja, das kann vorkommen, hängt natürlich vom Browser ab, den man verwendet. Oder von der E-Mail Programm, das man verwendet. Das kann technisch noch perfider sein, da ist klar (2) man kennt doch auch diese Drive-by Viren aus dem Internet (2) was man so bei sozialen Medien sofort schon zugreifen könnte. Aber (1) ja (2) dann muss ich schon gehen und sagen, da bin ich schon viel elaborierter. Da muss ich wesentlich noch viel technisches Know-how reinstecken. Und sobald ich nur die E-Mail lesen würde und nur in der Vorschau lesen würde und dann entsprechend schon Schadscode ausgeführt werden würde, dann wäre es ganz klar eine Schwäche des Programms. Ja klar, so was benutzt man auch, aber ja [mhm] da habe ich im Endeffekt keine Chance.

(M): wie sicher ist zum Beispiel (2) weil ich habe Gmail (1) also, google E-Mail. Wie sicher ist dass dieses Programm schon vor mir die E-Mails einsortiert (2) sprich (1) Spam oder Phishing E-Mails (2) wie sicher das ist?

(IP): Also, aus meiner Sicht, kann man sich darauf einfach nicht verlassen. Fertig. Wer sich anfängt darauf zu verlassen, es wird schon gekennzeichnet, wenn es schon vorsortiert war, ne (1) vergiss es. Dafür sind die Angreifer zu flexibel unterwegs und da gibt es zu viel grau Zone. Ich kann jetzt zwei Beispiele nennen, die waren ganz niedlich. Einmal das ist schon eine ältere Geschichte. Da hieß es dann, es wäre jemand von der Behörde XY, und es sollen Informationen gegeben werden und darin hat sich auch ein Formular befunden. Das Formular war fast original (2) Fast original. Es war zwar PdF Dokumente, aber gar nichts verseucht, das war total sauber (1) allerdings hieß es dann bitte ausfüllen. Hier ist eine Kreditkarteninformation darauf bringen und dann bitte faxen.

(M): faxen?

(IP): Faxen! Ja, deswegen die Geschichte ist schon ein bisschen her.

(M): ah, okay, verstehe.

(IP): genau, damals wurde noch gefaxt. Leider das Ziel hieß dann einfach nimm die Kreditkarteninformationen und fang an damit einzukaufen. Und die andere Variante war mal Phishing E-Mails wo es darum ging, ja die interne Diskussion abgebildet, und aus diesem oder jenem Grunde brauchen wir von Ihnen lieber Herr Müller jetzt nochmal die Kopie von Ihrem Personalausweiß und Ihre Kontoverbindung. Und schicken sie es bitte per E-Mail. Da wurde es einfach auf die E-Mail antworten geklickt, eine Kopie Personalausweiß, E-Mail Konto und so weiter wurde dann drangehängt, und dann anschließend ist es dazu gekommen, dass Leute irgendwie in Banken aufgetaucht sind und wollten damit irgendwie die Konto zum Beispiel schließen und das positive Beitrag sich auszahlen.

(M): ja. also, das ist nicht immer mit klicken oder so, das sind immer elaborierte Methoden. Da gehe ich schon spezifischer auf die Zielgruppe ein. Und versuche Sie gut zu personalisieren und im guten Deutsch oder im guten Englisch zu schreiben. (1) was denken Sie, wie sieht Social Engineering in fünf Jahren aus? Wie wird sich das ganze weiter entwickeln? Das Spiel ist nicht neu, aber wie wird sich das ganze weiter entwickeln?

(IP): Es zielt ja ab a Kultur und b und auf Möglichkeiten. Ich glaube die Möglichkeiten werden sich in fünf Jahren um einiges verbessert haben, also, wir werden anderes Umfeld haben und technische Möglichkeiten. Ich bin mir gar nicht so sicher in welcher Form es sich entwickeln wird (1) kann mir aber gut vorstellen, dass im Sinne vernetzter Dinge, also, Internet of Things, es soll Geräte geben, die kommunizieren. Wenn es mehr Geräte gibt, die kommunizieren. Also, man hat schon die Apple-Watch und es wird noch mehr Geräte geben, kleine Sachen, die ich noch in der Wohnung habe oder was auch immer (1) die angreifbar sind und über die ich entsprechend eventuell gefischt werde, die Micros haben, was auch immer. Ich glaube in die Richtung wird sich einiges weiter entwickeln (2) und ich persönlich habe das dann eine (2) das es dann einen stärkeren Fokus auf das Thema Identitätsklau geben wird. Das heißt also ich spiele vor, eine andere Identität (1) die Identität eines anderen zu haben und je weniger ich bei einer elektronischen Kommunikation nicht erkennen kann, dass mein Gegenüber gar nicht der ist, von dem ich glaube, dass das er ist, je eher kann es dazu kommen, dass ich Informationen Preis gebe im Vertrauen, obwohl mein Gegenüber gar nicht der oder die einige (1) heutzutage

verlasse ich mich wenn ich sehe, okay, die E-Mail Adresse so und so ist der und der (1) vielleicht sogar noch etwas stärker hiterlegt, dass ich weiß, dass okay, das ist ein bestimmter, ich habe mit ihm per SMS Kontakt oder per WhatsApp, jetzt per E-Mail (1) ich glaube da ist noch eine gewisse (1) Veränderung liegt, und was wir schon jetzt sehen können, was sich schon bewegt ist natürlich Social Engineering vielleicht etwas anders angesetzt, nämlich zu sagen, ich benutze die verschiedenen Medien auch zu Manipulation. Was wir schon jetzt mitbekommen in die Richtung Wahl und so weiter. Ich glaube da wird sich noch weiter bewegen (2) Also, ich habe erstmal gesagt, wo es sich hinbewegen wird (1) ich habe noch gar nicht gesagt, wie es mein Verhalten beeinflussen wird.

(M): genau, deswegen meine spontane Frage wäre, komplett darauf zu verzichten (1) auf das Handy oder Laptop.

(IP): nein, ganz im Gegenteil, das wird mehr. Wir sind mittlerweile (1) auf der sozialen Ebene ist es schon schwierig sage ich jetzt mal die Kontakte zu halten ohne gleichzeitig auf die Medien zu verzichten. Ich glaube auch in fünf Jahren sind wir noch eine ganze Ecke weiter was die ökonomischen Auswirkungen anbelangt (2) wenn ich mich nicht beteilige an der elektronischen Transparenz, dann glaube ich, wird es stärker hingehen mit der ökonomischen Nachteil. Wenn ich zum Beispiel meinen Fahrverhalten nicht transparent mache gegenüber der Versicherung, dann zahle ich höhere Versicherungsbeiträge. Wenn ich meinen Bewegungsverhalten nicht transparent mache gegenüber der Krankenkasse, dann zahle ich höhere Krankenversicherungsbeiträge. Oder wenn ich zum Beispiel mit jemandem was persönlich besprechen möchte, dann muss ich hinfahren. Also, wir haben die Tendenz und die Trends schon, und das wird sich stärker (1) das wird sich ausweiten. Und weil ich das ganz elektronisch kommuniziere, aus meiner Sicht das Ganze sich klar stärker ausweiten wird, das es sich mehr zum Alltag gehört. Elektronisches Bezahlen (1) alles. Wird es dann um so interessanter, wenn ich sage, mit Social Engineering kriege ich mehr zum Fassen und über ein Vorspielen falscher Tatsachen oder Identitäten beispielsweise kriege ich von jemandem auch dann (unv)

(M): also, das heißt das Ziel von Social Engineering in fünf Jahren (1) wird meine Identität sein.

(IP): ja (2) auch. Es ist immer mehrstufig, wenn meine Identität beispielsweise geklaut ist, dann wird meine Identität benutzt um von jemandem anderen wiederum etwas anders Geld zu bekommen.

(M): ja.

(IP): oder es wird meine Identität genommen (1) darüber versucht jemand weitere zehn Identitäten zu bekommen und über die zehn vielleicht hundertweitere Identitäten zu bekommen und mit diesen hunderten von Identitäten startet er einen anderen Angriff.

(M): ja (2) welche Techniken werden dann wichtiger? Wir haben schon über Phishing und Vishing gesprochen (2) und auch über so Social Engineering über den persönlichen Kontakt gesprochen. Aber welche Techniken werden wichtiger? Oder es werden neue Techniken entwickelt? Was denkst du?

(IP): [mhm] ja. Ist natürlich ins Glaskugel gucken.

(M): ja.

(IP): weil wenn ich jetzt annehmen würde, in drei Jahren gibt es wie auch immer einen Durchbruch oder setzt sich einen neue Art von elektronischer Kommunikation oder elektronischer Möglichkeiten durch, wird das dann dafür anschließend genutzt werden.

(M): ja.

(IP): von daher denke ich, dass Social Engineering, was die Medien anbelangt (2) neben den klassischen, die es bereits gibt, weitere neue Möglichkeiten weiter nutzen. Fertig. [mhm] Und das natürlich überall da, wo es Interaktion eine Rolle spielt. Heutzutage in online-Spielen gibt es eine entsprechende Interaktion (2) da gibt es ja auch Social Engineering (2) das eher einen erschreckenden Hintergrund hat, man (2) ist ja auch eine alte Geschichte, dass es versucht wird, Kinder zu interessieren um dann persönlichen Kontakt aufzubauen für was auch immer an Straftaten (2) von daher was ist weiter an den Möglichkeiten gibt, wird stattfinden. Ich habe keine Ahnung. Könnte mir so eine Phantasie vorstellen. Ob ich (2) ob es in Richtung virtuelle Identitäten oder virtuelle Reality also virtual reality da viellleicht noch was passiert. Aber also, da ich (2) ich weiß es nicht. Was ich sicher weiß, dass wenn neue Techniken kommen, wird es garantiert neue verschiedene Kombinationen daraus (2) Also, alte Techniken oder die bestehenden werden dann mit den neuen kombiniert, das glaube ich.

(M): Ja. Also, wir gucken stückweit in Glaskugel. Ich kann jetzt von keinem eine Antwort bekommen: „Hey, in 5 Jahren sieht es so und so aus. Das Thema 1, 2 und 3 ist wichtig“. Das ist nicht möglich (2) Okay. Gut. Social Engineering jetzt in Bezug auf das Unternehmen. Kannst du was dazu sagen? Inwiefern das Ganze für Social Engineers attraktiv ist vielleicht?

(IP): also, durch die Presse ging es schon, die so genannte [mhm] wie heiß es [mhm] ne, ich komme nicht darauf, egal, den Spezialbegriff lasse ich erstmal weg. Das sie (1) das Personen, die in der Lage sind, Geldflüsse auszulösen (1) im Unternehmen (2) diese Fälle dann wenn sie geschehen, dann in der Öffentlichkeit erscheinen. Großer bekannter Fall war bei Leoni.

(M): ja, 40 Millionen hat es gekostet.

(IP): ja, 50 Millionen, die dann tatsächlich gezahlt wurden, und die (1) so stark relevant war es (unv). Und die Sekretärin konnte das tun, also an die falsche Person die ganz Summe überweisen. Und dann wurde es ausgenutzt. Das heißt so was ist natürlich lukrativ (1) braucht natürlich mehr wissen, und mehr Konzentration auf die einzelne Person. Was im Unternehmen geschieht ist logischerweise ist die üblichen Cryptolocker oder wie auch immer (unv). Durch die Gegend geschickt wird, heißt es ja hallo ich habe deine Dateien gesperrt, überweise mir so und so viel. Bitcoins und was auch immer dies und jenes.

(M): aber jetzt in Bezug auf das Unternehmen?

(IP): also, in Bezug jetzt auf das Unternehmen. Tendenziell bei einem Unternehmen kann ein Social Enigineer mehr zu holen, dadurch, dass ich Daten beispielsweise blockiere durch den Cryptolocker oder wie auch immer. Das im Unternehmen ein Schaden höher sein kann als privat. Das macht ein Unternehmen interessanter als ein anders Ziel. Ein Unternehmen kann interessant auch machen, dass ich natürlich mich in ein Universum herein bewege und mich dann eine größere Menge an Menschen schnappen kann. Ja, dann Social Engineering (2) gut, der Klassiker ist dann (1) über Social Engineering irgendwelche Innovationen von deutschen Ingenieurbetrieben oder so was (1) wo es um deutsche Maschinenfabriken und solche Anlagen geht, da warnen auch davor, dass entsprechende Geheimnisse oder Patente darüber flotten gehen. Und ich kann mir gut vorstellen, dass durchaus auch (unv) nein eigentlich nicht (1) also,

entweder gezielter Angriff, weil ich heraus will aus einem Unternehmen, wo social Engineering das Ganze unterstützen kann (1) gezielter Angriff um Geld zu bekommen, ja (2) weil wie gesagt, verschlüsselte Dateien tun einem Unternehmen mehr weh, als meine private verschlüsselte Dateien, wobei die immer gilt. „Kein Backup – kein Mitleid“ <lacht> das darf man nicht vergessen. Und in einem Unternehmen [mhm] wie gesagt, ich kann mich wenn ich mich in einem Universum eines Unternehmens befinde, dann ich sehe, okay, da ist eine Schwachstelle, die ich nutzen kann, dann erreiche ich eine ganze Menge an Menschen.

(M): ja.

(IP): reicht aber dann mit ganz üblichen Angriffsarten.

(M): wie kann ein durchschnittlicher User kein Opfer von Social Engineering werden? Privat und auch im Arbeitsleben? Wobei ich glaube, die Sachen überschneiden sich.

(IP): ja. Klar. Also, ich kann mich aber dann im Arbeitsleben in einer vermeidlichen Sicherheit wiegen, indem ich feststelle, dass es in meinem Unternehmen mehr getan wird, wegen technischer Angriffe, oder dass ich stückweit geschult werde (1) das ich in noch irgendeiner Form Sensoren habe, die dann einspringen bei so was. Und grundsätzlich neben dem, was ich technisch flankieren kann, was aber ja gar nicht unbedingt in die Richtung Social Engineering gehen muss, sondern eher Richtung Schad-Software, glaube ich was das Thema Social Engineering anbelangt, ist der allerwichtigste Punkt – Bewusstsein und Aufmerksamkeit. Wenn ich weiß, so was gibt es (1) und wenn es mir bewusst wird, an welchen Stellen es zuschlagen kann (1) und aufmerksam bin, wo es vielleicht der Fall ist. Typischerweise.

(M): okay (1) Ja. Hast du jemals ein Social Engineer Angriff erlebt? Bzw. gemacht? Kannst du vielleicht was dazu sagen?

(IP): ja, also, erlebt wie ich schon gesagt habe mittlerweile drei Anrufe. Immer von verschiedenen Social Engineers, die sich als verschiedene Firmen ausgegeben haben. Einmal war es eine russische Nummer, also 007, einmal eine der bekannten Handynummer über die (1) die für entsprechende Angriffe verwendet werden. Und dann gab es einen dritten Anruf (1) Natürlich habe ich auch diverse E-Mails schon gekriegt (1) klar. L mal 3 . Lesen, lachen, löschen. Oder manche habe ich dann an CERT weitergeleitet. Klar. Wenn sie mir schon gesagt haben, okay, die E-Mail sieht jetzt schon ein bisschen anders als sonst. Ich überlege mir (2) social Engineering (1) per Telefon [mhm] persönlich (2) habe ich nur das privat erlebt, aber dann im beruflichen Kontext nicht (2) ich weiß, dass es entsprechende Anrufe auch im beruflichen Kontext gibt (2) dass zum Beispiel Kontakte ausgefragt werden (1) regelmäßig immer wieder. Was weiß ich über Social Engineering noch? Selber angegriffen habe ich (1) also, einmal dachte ich auch es ist Social Engineering. Da habe ich von einer italienischen Behörde was gekriegt. War auch in Italien. Und in dem Fall habe ich auch dann im Internet geguckt, habe gesehen dann ah, okay, das kann durchaus Phishing sein. Habe sein lassen. Habe dann es von einer italienischen Autovermittlung es bekommen. Dann habe ich nicht darauf geklickt, habe zurück geschickt und gefragt, okay können Sie mir näheres dazu nennen? Ich habe den Kontakt aufgenommen um zu sehen, wer ist dahinter, war es jetzt was vernünftiges? Und selber Social Engineering Angriffe vorgenommen, so zu sagen, ob es Social Engineering kann man geteilter Meinung sein (2) wenn wir auf Assessments sind, versuchen wir mal hier und da aus den Büros was rauszuholen [mhm] ist dann ein [mhm] klassischer Angriff ist zum Beispiel ein Rechner rauszuholen, Unterlagen zu sehen (1) da war ich schon mehrere Male erfolgreich.

(M): also, das heißt, ihr guckt dann nach, ob sage ich jetzt mal, der Laptop gesperrt ist.

(IP): ja, genau, oder ob die Unterlagen einfach da liegen (1) ob ich jetzt einfach als nicht zum Unternehmen erkennbar angehörige Person einfach durchmarschieren kann.

(M): Wenn du in ein Büro reinkommst, weißt du schon, wo du hinguckst, sage ich jetzt mal. Gibt es da bestimmte Bereiche oder Orte?

(IP): also, erstmal, was ich wichtig finde, ist dass ich freundlich grüße um durchzukommen, dann häufig werde ich dann nicht mehr weiter gefragt, dann manchmal warte ich vor der Tür, wenn ich zum Mittagessen oder wie auch immer Leute da zur Arbeit kommen, schließe ich mich einfach an, und dann wenn ich mich einfach irgendwo in Büro Räumen bewege, weiß ich das Wichtigste ist, dass ich nicht hilflos gucke, sondern dass ich zielgerichtet einfach irgendwohin hingehe. Nochmal in den Raum reingucke, einfach freundlich grüße (1) wenn ich sehe, da ist ein leerer Raum, dann ich weiß, aha da kann ich reingehen, jetzt kann ich ein Paar Fotos machen. Ich gucke dann in einen Raum wo niemand ist (1) logisch. Das muss dann ein Raum sein, der durch andere nicht ansehbar ist, weil sie dann auch sofort fragen würden, was machst du am Rechner vom XY?

(M): Verstehe.

(IP): wir sind dann in anderen Situationen auch in Aktenraum reingegangen und haben einfach uns 2 Ordner rausgeholt (1) war kein Problem. Bin nochmal reingegangen, habe einen dritten rausgeholt (1) Da kam da jemand hat gesagt, hallo, ich sollte hier ein Paar Aktenordner rausholen. Ich habe dann gesagt, hallo, ich muss hier ein Paar Ordner rausholen (1) dann habe ich den dritten rausgeholt. Wurde auch so freundlich begrüßt und dann ja, dann war alles gut.

(M): das wäre schon so ein Finding in einem Assessment, oder?

(IP): ja, klar, dann hinterher dementsprechend transparent gemacht, zurück gebracht (1) vorher abgestimmt die Aktion, aber (2) ja, wir haben es gemacht um festzustellen, wie gut sind wir aufgestellt. Also, das ist, ich behaupte, wenn eine Einzelperson sich die Mühe gibt, eine Truppe von drei zwei Leuten sich Mühe gibt, kann sie viel erreichen (1) ja. Unterlagen einsammeln, technische Equipment einsammeln.

(M): welche Maßnahmen sollen ergriffen werden, um Das Awareness-Level zu steigern zu fördern? Jetzt im Unternehmen aber auch so privat?

(IP): also, einmal ist es gut, wenn ich da so Standart-Awareness Maßnahmen habe, im Sinne von ich weiß noch (unv) es gibt noch was weiß ich (unv) im Rahmen von jährlichen Arbeitssicherheitsunterweisungen. Da auch mal Hinweis zu (1) wobei, das sich ausläuft und ich glaube (unv) kann in die Vergessenheit geraten. Ich persönlich glaube, dass zwei weitere Sachen, also mit zwei Dingen kann ich rangehen, was wir auch hier machen. Das eine ist, dass ich es in irgendeiner Form mit Spaß verbinde, sagen wir okay, gehen wir auf die Entdeckungsreise, wo könnte man vielleicht (1) oder spiele mal Spiel mit uns. Das ist das eine (2) Die positiven Emotionen damit verbunden werden, und das andere, was glaube ich schon, wenn negative Emotionen damit verbunden werden. Wobei man gut gucken musst, dass man keinen falschen Touch kriegt (1) sage ich jetzt mal, Personen nicht beschädigt, ja (1) aber dann so ein Schreck-Erlebnis dann glaube ich sehr heilsam, um zu sagen, okay, Mensch, dann muss ich tatsächlich stückweit aufmerksamer sein. Eine Phishing Kampagne ist ein Beispiel. Und das andere wäre tatsächlich, wenn ich auf einen Telefonanruf eingefallen wäre, was auch

immer. Okay, das ich echt selber erlebt habe, vielleicht wenn man so weit kommen kann, wenn man Menschen hat, die so, die negative Erfahrung gemacht haben, die sich bereit erklärt haben, für ein weiteres Publikum darüber zu berichten. Weil, ja, aus meiner Sicht ganz klar, der Lerneffekt, ja, der Lerneffekt ist nachhaltiger größer, wenn stärkere Emotionen damit verbunden sind. Und dann reicht es vielleicht schon, wenn ich jemanden kenne, der so was erlebt hat und davon berichtet, und es kann bei mir eine Menge ankommen, wenn emotionaler ein Stück verbunden bin, das ist so eine (1) das ist so von der akademischen Ebene (1) reine Wissensvermittlung oder wie auch immer (1) von diesem nüchternen und trocknen ein bisschen weg geht. Ich glaube, wir müssen (1) oder es ist gut, wenn wir eine Chance haben das stärker zu kombinieren. Und jetzt aber ein bisschen bösartig gesagt, ich weiß auch natürlich, dass wir uns damit leicht überfordern können (1) aber bösartig gesagt, als eine Anregung, ich darf ja mal durchaus fragen, wenn ich jetzt irgendein spielerisches Herangehen nehme, an das Thema (1) dann darf es ruhig mal auf der Höhe der Zeit sein. Solls heißen, wenn ich schon mal ein physisches Spiel mache, dann es ist dann eins, was echt lustig ist, und wenn ich es mit einem echten Spiel mache, dann muss ich sagen, es hat richtig gute Qualität. Das macht auch Leuten Spaß zu spielen (1) das ist mit einer guten Grafik, oder von der Inhalt her, so ne <lacht>, was soll das wieder. Lustig verpackt, aber der gleiche Mist. Ja, deswegen wirklich Emotionen dabei.

(M): ich versuche es zu machen <lacht>. Ja, das war meine letzte Frage, vielen Dank nochmal für dein Interview.

(IP): Gerne.