Zinaida Benenson

Menschengerechte IT-Sicherheit

Vortrag auf der FIfF-Konferenz am 14. November 2020

Transkription und Überarbeitung: Sylvia Johnigk und Eberhard Zehendner.

Gestaltungseffektive IT-Sicherheit erfordert die Berücksichtigung der Fähigkeiten der nicht fachkundigen Nutzenden. Leider sind dabei die Anforderungen an die Nutzenden oft unrealistisch. Ihnen wird unsicheres Verhalten vorgeworfen, ohne zu fragen: Sind sie überhaupt in der Lage, sich „sicher" zu benehmen? Statt der zum Scheitern verurteilten Versuche, die Nutzenden durch Sensibilisierung und Schuldzuweisung an die IT-Systeme anzupassen, sollten die IT-Systeme an sie angepasst werden. Wie das gelingen könnte, wird in diesem Beitrag dargestellt.

Und insbesondere auch: Was passiert, wenn die Menschen angegriffen werden? Denn das kam bisher, denke ich, nicht so genau oder nicht so oft zur Sprache. Ich werde zwei Studien vorstellen, die wir in meiner Forschungsgruppe durchgeführt haben. In einer geht es um Phishing und in der anderen um Antivirus-Meldungen. Es hat sich herausgestellt, dass das nicht so ganz menschengerecht ist. Und dann werde ich versuchen, ein bisschen zu erklären oder vorzustellen, was denn menschengerechte Sicherheit sein könnte.

Die Phishing-Studie

Sie haben bestimmt schon von *Spear Phishing* gehört. Das ist gezieltes personenbezogenes Phishing, kann manchmal auch Namen oder Adressen der Empfänger:innen enthalten, und manchmal ist es auch abgestimmt auf die Umstände, in denen sie leben, und hat dann einen interessanten oder plausiblen Inhalt. Das Problem ist, dass die Nachricht versucht, per Anhang oder Link eine Malware auszuführen. Viele Angriffe, wie zum Beispiel *Advanced Persistent Threats* (APT) oder *Ransomware,* beginnen mit Spear Phishing. Das wird in den Firmen gefürchtet, insbesondere auch im Online-Banking-Bereich.

Wir haben uns in unserer Studie gefragt, welche Gründe es fürs Anklicken gibt, wenn Leute so etwas bekommen. Denn man hört oft gerade von Sicherheitsexpert:innen: „Oh, mein Gott, wie kann man auf so etwas klicken?" Und genau das wollten wir herausfinden. Wir haben dazu zwei Experimente durchgeführt. Ich werde jetzt einfach kumulativ Ergebnisse vorstellen. 2016 habe ich auf der *Black Hat USA* einen Vortrag[1,2] dazu gehalten, darin wird es ein bisschen mehr erklärt.

Die Phishing-Nachricht

Abbildung 1 zeigt den Text einer E-Mail, die wir sieben Tage nach Silvester an rekrutierte Teilnehmer:innen unter den Studierenden unserer Universität verschickt haben. *Hey wie gehts? Silvester war ja echt der hammer!* Und da gab es einen Link, der eigentlich ziemlich verdächtig ist: da war einfach eine IP-Adresse, die zur Uni gehört, zu unserem Lehrstuhl, und eine personalisierte ID für die User. Wenn sie darauf geklickt haben, erschien eine Webseite mit der Meldung „access denied". Diese Nachrichten wurden mit unterschiedlichen Namen unterschrieben, in diesem Fall sehen wir „Sabrina".

Warum war das Spear Phishing? Naja, das wurde eben kurz nach Silvester verschickt, und man weiß, dass da viele Leute feiern. Daher haben wir gehofft, dass insbesondere auch Studierende Silvester zusammen mit anderen Menschen feiern und dort eventuell auch Fotos machen. Das war jetzt nicht so super gezielt, aber schon ein bisschen an die Empfänger:innen angepasst.

Wir haben uns auch bemüht, ein bisschen „Jugendsprache" zu sprechen. Das klingt jetzt ein wenig blöd, aber die ganzen Fehler, die Kleinschreibung in der E-Mail usw., das war einfach ein Versuch, sich anzupassen. Und wir hatten diese Nachrichten von Facebook-Accounts und von E-Mail-Accounts geschickt, die alle zu nichtexistierenden Personen gehören. Wir haben bei den Facebook-Accounts sogar variiert, wie viel Inhalte ein Account hat. Da gab es zum Beispiel den Account von einem „Tobias", der irgendwie gar nichts auf seinem Profil hatte, und den Account von einem „Daniel", der ein bisschen mehr hatte, ein paar Infos, und mehr nach einer realen Person aussah.

Ergebnisse

Wir hatten eine ganz gute Klickrate, insbesondere mehr als 40 % bei Facebook und 20 % bei E-Mail. Und da sagen vielleicht einige Leute, das waren dann blöde Studenten, was soll man denn noch von ihnen erwarten. Ich hoffe, dass ich diese Einstellung ein bisschen abmildern kann, wenn ich erzähle, was wir herausgefunden haben. Wie erklären denn die Nutzenden, warum sie geklickt haben? Ich habe dazu ein paar wörtliche Zitate gesammelt (siehe Kasten Seite 34). Was ich fett gekennzeichnet habe, sind Gründe, die man hier bei der Textanalyse herauslesen könnte.

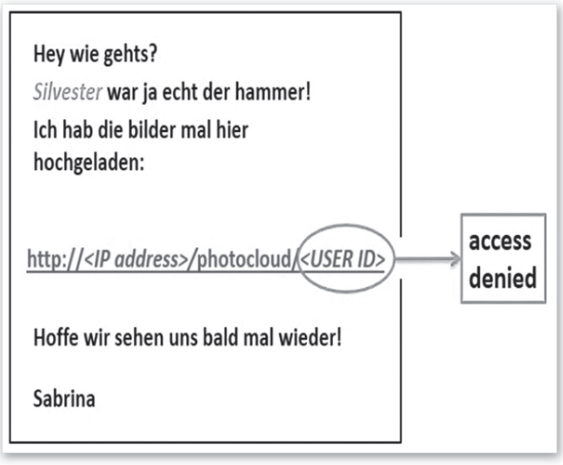


Abbildung 1: Text einer Phishing-Nachricht

Da hat jemand aus Neugier geklickt. Neugier ist eine sehr gute Eigenschaft. Sie führt zum Beispiel dazu, dass man Forschung betreibt oder sich informiert. *Wollte sehen, was passiert.* Das ist auch Neugier, nur anders ausgedrückt. *Ich dachte das ist eine Mail von einem Freund.* Warum dachte die Person das? Naja, wir haben die Top Ten der Vornamen der Studierendengeneration – man weiß ja ungefähr, wie alt sie sind – benutzt, und da gab es wohl ein paar Tobiasse, Daniels und Sabrinas, von denen man etwas erwartet hat oder die man kannte. Dann war jemand an Fotos interessiert, die von Leuten stammen hätten können, mit denen die Person Silvester verbracht hatte. Wir haben dann alles kategorisiert (siehe Tabelle 1).

– 34 %	Neugier/Interesse
– 27 %	Inhalt plausibel, wie erwartet (passt zur eigenen Silvesterfeier)
– 17 %	Nachforschungen (Was ist passiert? Kann ich helfen?)
– 16 %	dachten, dass sie den Absender kennen
– 11 %	Vertrauen in Technologie/Organisation
– 7 %	Angst
– 2 %	automatisch

Tabelle 1: Gründe für das Anklicken der Phishing-Nachricht (Mehrfachnennung möglich)

Am häufigsten haben Leute aus Neugier und Interesse geklickt. Dann haben sie geklickt, weil der Inhalt plausibel schien und in diesem Fall zur eigenen Silvesterfeier passte. Einige Leute haben Nachforschungen angestellt. Sie wussten, es kann nicht für sie sein, aber sie wollten herausfinden, was passiert ist. Vielleicht könnten sie die Nachricht weiterleiten, vielleicht Leute auf den Fotos erkennen. Und relativ viele dachten auch, dass sie den Sender kennen. Da hat es sich gelohnt, diese Top Ten der deutschen Vor- und Nachnamen zu verwenden.

Ein weiterer wichtiger Grund – das ist vielleicht auch für Leute interessant, die in Firmen für IT-Sicherheit verantwortlich sind – ist Vertrauen in Technologie und Organisation. Da haben Leute gesagt, mein Computer oder mein Antivirus-Programm wird mich schützen. Oder, ich habe einen sicheren Browser benutzt, in einem sicheren Betriebssystem wie macOS. Oder, ich bin über Tor gegangen – was natürlich gegen Spear Phishing nicht wirklich hilft. Manche Leute haben gegoogelt, nach dem Link oder nach der E-Mail-Adresse, von der die Nachricht kam. Und es gab auch welche, die gesagt haben, die IP kam aus der Uni Erlangen, also schon technisch versiert. Oder, die Webmail der Uni Erlangen war bisher sicher und ich glaube, da kommt auch kein Spam und nichts Gefährliches rein.

Ein sehr interessanter Grund ist Angst. Die Angst, ob ein Fremder Fotos von mir haben könnte. Es ist durchaus möglich heutzutage, dass mich jemand fotografiert hat und ich das überhaupt nicht bemerkt habe. Und jetzt wer weiß was auf diesen Fotos ist. Das heißt, auch Klicken ist nicht immer ein Zeichen von fehlendem Sicherheitsbewusstsein. Es kann das Ergebnis einer Abwägung sein, zwischen der Angst, eventuell den Rechner zu infizieren, und der Angst, dass die eigenen Fotos in fremden Händen sind.

Wörtliche Zitate von Phishing-Opfern

„Ich wollte mir die Fotos ansehen, aus reiner **Neugier**. Obwohl ich mir dachte, es könnte ein Virus sein – ich habe das Konto daraufhin blockiert."

„Wollte sehen, was passiert …"

„Ich dachte das ist eine **Mail von einem Freund** und war **gespannt** auf die Bilder."

„Weil ich an den Fotos **interessiert** war, und die Nachricht durchaus **von Leuten stammen hätte können,** mit denen ich Silvester verbracht habe."

„Weil ich anhand möglicher Bilder erkennen wollte, **ob ich die Person eventuell kenne.** Da ich **privat gefeiert** habe und nur wenige mir unbekannte Freunde meiner Freunde da waren, habe ich die Gefahr nicht hoch eingestuft. Ebenso wenig Gefahr empfand ich, da ich die **Webmail der Uni bisher für sicher empfand.** Zudem **Interesse** für eventuell lustige Silvesterbilder mir fremder Personen."

„Weil der Link unbedenklich aussah und **mein Computer** bei einem Virusproblem sofort den Zugang verhindert."

„Ich wusste, falls es was gefährliches ist, das **mein Kaspersky** Sicherheitsprogramm mich vor Gefahren schützen wird."

„Da ich mit Firefox einen meiner Meinung nach **sicheren Browser** verwende und zudem **Mac OS** verwende."

„Ich habe den Link in einem anderen **sicheren Browser** geöffnet. (Vorkonfigurierter Firefox aus dem Tor Bundle)"

„Nachdem ich **gegoogelt** habe, schien Photocloud eine sauber Seite zu sein."

„Habe davor die E-Mail Adresse **gegoogelt,** um sicherzugehen, ob etwas über die Adresse im Internet steht"

„**ip kam aus uni erlangen** deshalb dachte ich es kann nix böses sein"

„Ebenso wenig Gefahr empfand ich, da ich die **Webmail der Uni bisher für sicher empfand.**"

„Weil er auf mein Uni-email-konto kam. Hier gab es **noch nie Werbung, Spam, etc**"

„Trotz Unsicherheit war die **Angst** zu groß tatsächlich Bilder von mir in fremden Händen zu wissen, bei heutigem Ausmaß an Möglichkeiten Fotos zu erstellen weiß man schließlich nie wer wo wie unter Umständen doch welche gemacht hat."

„**Aus Reflex,** habe das Fenster aber gleich bevor es geladen hatte wieder geschlossen."

„Ich habe **erst auf den Link geklickt und dann kapiert,** dass eine Person mit diesem Namen eigentlich gar nicht da war"

Am meisten mag ich die Antworten, wo Leute gesagt haben, dass sie aus Reflex geklickt haben. Man klickt einfach zuerst und merkt dann: Moment, was habe ich denn jetzt gemacht? Und natürlich ist die Frage: Könnte es Ihnen passieren? Könnte es mir passieren? Ich weiß nicht, ob es Ihnen passieren kann. Mir kann es passieren, und es ist mir auch passiert. Deswegen bin ich immer sehr vorsichtig, wenn Leute sagen, man muss Awareness schaffen, und Leuten erklären, was passieren kann. Denn ich würde annehmen, dass ich eigentlich Security-aware bin.

Dazu ein erstes persönliches Beispiel. Ich habe erwähnt, dass ich diese Studie auf der Black Hat USA vorgetragen habe, das ist ein ziemlich großes Event – so ein Hackerevent. Und ich habe – das ist so durch die Presse gegangen – sogar von CNN eine E-Mail bekommen. Das ist mir vorher noch nie passiert und danach auch nicht mehr. Und Sie können in Abbildung 2 sehen, das ist ein CNN Request, „Your topic looks fantastic!" und „Here's a link to my work". Und das erste, was ich gemacht habe: Ich habe darauf geklickt. Und als ich dann gesehen habe, wie sich mein Browser öffnet, habe ich mir gedacht: Moment, was habe ich gerade gemacht? Denn alle Informationen, die hier in dieser E-Mail stehen, waren öffentlich zugänglich. Das hätte mir jeder Angreifer problemlos schicken können. Zum Glück war diese E-Mail tatsächlich echt. Aber das zeigt, wie schnell es passiert, dass man sich in einem emotionalen Moment, hier wegen einer E-Mail von CNN, eben verklickt.

From: john.smith@turner.com
To: zinaida.benenson@fau.de
Subject: CNN request -- about your upcoming Black Hat talk
Zinaida,
John at CNN here. I'm the news network's cybersecurity reporter. Here's a link to my work, in case you're not familiar with it.
I saw the description of your upcoming Black Hat talk. Your topic looks fantastic!
Can we get an exclusive look at your research and write the first news story about it?
Cheers,
John Smith
john.smith@CNN.com

Abbildung 2: Echte Anfrage von CNN

Ein anderes Beispiel ist mir vor ungefähr einem Jahr passiert. Wir hatten Kontakt zu einer Firma, die von uns ein Security-Audit haben wollte. Wir haben uns über ein Produkt unterhalten, noch ein Kollege war daran beteiligt, und dann ist das Ganze irgendwie eingeschlafen. Und ein Jahr später, nachdem wir das alles mit der Firma auszuhandeln versucht haben, kam eine E-Mail (Abbildung 3).

From: senior-manager@important-company.com
To: zinaida.benenson@fau.de
Subject: Re: Re: <*Product X*> Security Audit – call follow up

Morning,

Please see attached and confirm.
Any questions please do not hesitate to contact us.

Thanks,
<normal email signature>

Attachment:
Product X_Inquiry.doc

Abbildung 3: Phishing-E-Mail

Das war tatsächlich eine passende Antwort auf eine E-Mail, die ich vorher geschickt hatte. Da steht „Product X" (also das, worüber wir vorher gesprochen hatten) „Security Audit – call follow up", „Please see attached and confirm". Und es war auch ein Dokument beigefügt. Ich war schon dabei, darauf zu klicken, dann ist mir eingefallen: Moment, solche Beispiele erzähle ich doch die ganze Zeit in der Vorlesung, also vielleicht doch lieber nicht klicken. Dann bin ich aus dem Büro gestürmt, ins Büro von meinem Kollegen, der auch an dem Projekt beteiligt war, mit einem Schrei: „Bitte nicht klicken!" Er hat mich so angeschaut von seinem Rechner und meinte: „Ich habe schon geklickt." Ich meinte dann: „Und?" „Ja nichts. Mein Antivirus ist hochgegangen." Das heißt, er hatte Glück, und ich hatte auch Glück, denn es war irgendwas drin, es war tatsächlich ein Angriff, aber zum Glück konnte es durch den Antivirus abgefangen werden. Und das war eine Person, die sich seit fünf Jahren sehr erfolgreich mit IT-Sicherheit professionell beschäftigt hatte.

Was folgt daraus? Ein Kollege und ich, wir wurden beide in einem Moment gefangen, wo wir keinen Verdacht geschöpft haben. Das heißt, eigentlich müssten die Nutzer:innen, wenn sie diese Angriffe abwehren sollen, immer misstrauisch sein; egal, was kommt, egal, ob die Nachricht plausibel ist, egal, ob sie deren Erwartungen entspricht, egal, ob man den Absender kennt. Also muss man sich immer in einem Zustand des permanenten Misstrauens befinden, wenn man tatsächlich 100 % dieser Angriffe abwehren möchte. Und das ist etwas, was man gerne *Sicherheitsmentalität* nennt.

Psychologie der Sicherheitsmentalität

Sehen wir uns doch diese Sicherheitsmentalität mit Hilfe von Psychologie etwas näher an. Ich weiß nicht, ob viele von Ihnen das Buch *Schnelles Denken, langsames Denken* von Daniel Kahneman gelesen haben. Kahneman ist Nobelpreisträger in der Ökonomie, aber eigentlich Psychologe. Er unterscheidet zwischen zwei Systemen des Denkens. System 1 ist die Intuition, aus dem Bauchgefühl handeln. Und System 2 ist logisches Denken. Ich zitiere einfach aus dem Buch, damit Sie vielleicht besser nachvollziehen und mir vielleicht auch glauben können, was ich meine. Es gibt eine „wachsende Zahl von empirischen Befunden, die darauf hindeuten, dass eine positive Stimmungslage, Intuition, Kreativität, Leichtgläubigkeit und zunehmende Beanspruchung von System 1 ein Cluster bilden". Was bedeutet das? Wenn man in System 1 ist, im Flow, in Intuition, in Kreativität, hat man eine positive Stimmungslage, ist aber auch leichtgläubig, und das ist ein Cluster.

Welches Cluster gibt es denn für System 2? „Andererseits sind auch Niedergeschlagenheit, Vigilanz, Argwohn, eine analytische Herangehensweise und vermehrte Anstrengung eng miteinander verbunden." Man kann nicht gleichzeitig leichtgläubig und argwöhnisch sein. Man kann nicht gleichzeitig positive Stimmungslage und Niedergeschlagenheit verspüren. Das heißt, wir können normalerweise nur in einem der beiden Systeme sein. Und weil System 2 mit vermehrter Anstrengung verbunden ist, sind wir normalerweise im System-1-Zustand. Und das ist etwas, was wirklich jeder von uns macht, praktisch fast jede Minute unseres Lebens. Und nur sehr selten schalten wir unser logisches Denken ein, dafür brauchen wir spezielle Trigger, sonst

wäre es eine zu hohe Anstrengung, das würden wir einfach nicht durchhalten.

Wenn wir jetzt sagen, die Mitarbeiter:innen, die Nutzer:innen sollen gezielte Angriffe stets erfolgreich abwehren, dann wollen wir eigentlich, dass sie sich ständig in System 2 befinden – überall – in der Beratung, im Verkauf, in der Presseabteilung, in der Kundenbetreuung, in der Personalabteilung und auch zu Hause. Manche Unternehmen meinen vielleicht, im Beruf sollte es doch möglich sein, unter bestimmten Voraussetzungen in all diesen Abteilungen Leute mit sehr hohem Sicherheitsbewusstsein zu haben. Nur sollte man dann wohl Stellenanzeigen und Gehälter ein bisschen anpassen – und geeignetes Training wäre natürlich auch nötig. Im Privatleben dagegen sieht man sofort, dass das zu kompliziert würde und deswegen auch nicht realistisch ist.

Und dann gibt es noch dieses schöne Problem der False Negatives und False Positives. *False Negatives* heißt hier, dass gefährliche Nachrichten nicht entdeckt werden. Sicherheitsexpert:innen bemühen sich natürlich vorwiegend um diese, denn sie wollen ja die Gefahren abwehren. *False Positives* sind gutartige Nachrichten, die irrtümlich als gefährlich eingestuft werden. Und für die normalen Nutzer:innen ist das total wichtig, denn wenn diese Nachrichten ausgefiltert oder gelöscht oder nicht ernst genommen werden, dann gibt es vielleicht verpasste Chancen oder geschäftliche und persönliche Konflikte.

Und hierzu wieder ein persönliches Beispiel aus meinem Forschungsleben. Ich habe einmal von einer Firma, mit der ich ein Projekt hatte, die Nachricht aus Abbildung 4 bekommen. Aha, „we need your bank account details". Und ich dachte mir: „Hahaha. Ja, das mache ich natürlich. Klar!" Und dann habe ich gemerkt, das scheint ja an mich adressiert zu sein, wenn auch nicht direkt, aber jedenfalls steht mein Name drin. Also habe ich die Firma auf einem separaten Kanal angeschrieben und gefragt:

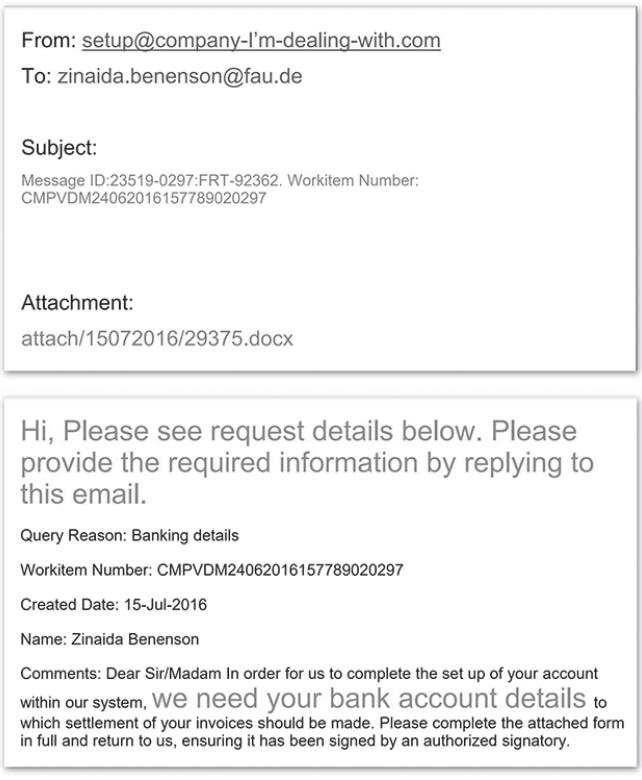


Abbildung 4: Phishing oder echt?

„Habt ihr das geschickt?" Und sie haben geantwortet: „Ja, haben wir. Ist ja nichts Besonderes."

Solche Dinge passieren im Geschäftsleben, denke ich, nicht sehr selten. Und deswegen ist es sehr schwer, da auf der Hut zu sein. Auch private Nutzer:innen bekommen widersprüchliche Awareness-Hinweise. Ich bin PayPal-Kundin und bekomme ab und zu eine PayPal-Kontoübersicht. In dieser legitimen E-Mail gibt es eine Schaltfläche „Weiter zu PayPal", hinter der sich ein Link verbirgt. Dieser Link beginnt aber nicht mit www.paypal.com, wie in den Awareness-Hinweisen von PayPal behauptet. Die Ungenauigkeit der Hinweise führt also zu False Positives.

In den Awareness-Hinweisen von PayPal steht auch, dass eine gefälschte E-Mail meist mit einer unpersönlichen Anrede beginnt. Diese Fehleinschätzung von PayPal kann zu False Negatives führen. Denn in den letzten Jahren haben viele Phishing-E-Mails eine korrekte Anrede benutzt.[3] Der Grund ist, dass persönliche Daten massenweise geleakt wurden. Und natürlich werden von Kriminellen im Darknet oder auf anderen Schwarzmärkten im Internet E-Mail-Adressen, Anreden usw. gehandelt.

Es gab sogar eine Ransomware, die tatsächlich Stellenanzeigen analysiert und gezielte Angriffe an Personalabteilungen verschickt hat, mit Erwähnung von aktuellen Stellenanzeigen.[4] Da fragt man sich, wie man sich denn dagegen schützen soll.

Phishing-as-a-Service?

Aber es gibt Leute, die sagen, wenn wir unsere Nutzer:innen daran gewöhnen, indem wir simulierte Phishing-Angriffe durchführen, dann werden sie vielleicht aware und sich dann doch irgendwie besser verhalten. Und hier habe ich auch ein Beispiel, zum Glück nicht aus meinem persönlichen Leben, aber das ging mal durch die Zeitungen. Das war im Dezember 2015, ich weiß nicht, ob Sie es bemerkt haben. Da wurde an zwei Dienststellen der Berliner Polizei eine E-Mail gesandt, die sie darum gebeten hat, ihre dienstlichen und privaten Passwörter im „sicheren Passwortspeicher der Polizei Berlin (SPS)" zu deponieren. Und dazu gab es einen Link, die E-Mail war im Corporate Design, unterschrieben mit *Zentrale Service Einheit* (ZSE), mit Adressen mit leichten Fehlern, von nichtexistierenden Personen.

Das hat in einer Panik resultiert in den Dienststellen, und deshalb ist das alles in die Presse geraten. Aber eigentlich war es eine simulierte Phishing-Attacke. Das war kein richtiger Angriff. Die Nachricht wurde von einer beauftragten Pentesting-Firma verschickt, von außerhalb der Organisation, und ging an mehr als 400 Leute.

Pentesting the Humans

Mehr als die Hälfte haben geklickt und über 30 Personen haben Nutzerdaten eingegeben, aber wir wissen nicht, was sie da angegeben haben. Ich nenne das – nicht sehr politisch korrekt vielleicht – „Pentesting the Humans". *Pentesting* oder *Penetration Test* ist eine Sicherheitsmaßnahme, die zum Beispiel Firmen verwenden. Wenn sie Software auf Sicherheitslücken überprüfen wollen, lassen sie ihre eigene Software oder ihre eigenen

Netze von sogenannten *Pentestern* hacken. Und hier werden eben Menschen irgendwie gehackt.

Die Polizei musste sich zu dem Ganzen natürlich äußern, weil das in der Presse war. Ein Vorstandsmitglied der Gewerkschaft der Polizei meinte, es würde keine Konsequenzen geben für Leute, die darauf reingefallen sind; die Beamten bekämen „eine Flut von dienstlichen Mails – da schaut man nicht mehr so genau hin". Und resümierte: „Die Polizei ist nur ein Spiegelbild unserer Gesellschaft." Ich finde, das ist sehr weise und sehr richtig gesagt.

Was können wir daraus lernen? Was kann die Polizei daraus lernen? Wir können lernen, dass Polizisten Menschen sind, so wie wir auch. Sie haben auch System 1 und System 2. Und da frage ich mich auch, was denn das richtige Verhalten wäre? Sollen die jede interne E-Mail überprüfen, vielleicht die Person anrufen? Oder schauen, ob die Person existiert, jedes Mal, wenn sie etwas bekommen? Jeder E-Mail misstrauen, die ganze Zeit im System-2-Zustand sein?

Das Netz war da irgendwie voll mit Foren, zum Beispiel bei Heise, voll mit abfälligen Kommentaren über die Polizei, die ich völlig unangebracht finde. Hier ist es wirklich ganz offensichtlich für mich: es waren nicht die Polizisten, die etwas falsch gemacht haben, als sie drauf geklickt haben.

Warum ist Security Awareness schwierig?

Also fragen wir uns, warum ist Security Awareness schwierig? Oder warum behaupte ich, dass Security Awareness schwierig ist? Erstens, Security Awareness heißt, dass man nicht nur aware ist, man muss auch sein Verhalten ändern. Und Verhaltensänderungen sind immer schwierig, das wissen wir alle. Alle, die versucht haben, mehr Sport zu treiben, mehr Gemüse zu essen, rechtzeitig schlafen zu gehen, rechtzeitig ihre Vorträge vorzubereiten usw. und so fort. Ich habe meinen Vortrag diese Nacht vorbereitet, obwohl ich mir schon mehrmals geschworen habe, dass ich es nicht mehr tun werde.

Und Aufrechterhalten des Sicherheitsverhaltens ist schwer. Ständige Wachsamkeit ermüdet, denn es ist ein System-2-Zustand. Man wechselt zwangsläufig in den System-1-Zustand, und dann springen Emotionen und Automatismen an.

Und auch Geschäftsvorfälle und Arbeitspraktiken kollidieren mit Sicherheitsverhalten. Man kann eben nicht bei jeder E-Mail mit Anhängen und Links fragen: Hast du das geschickt? Und bist du sicher, dass es sicher ist? Das wäre schon vom Zeitaufwand schwierig. Und dann stehen natürlich auch unsere sozialen Verhaltensnormen dagegen. Vertrauen und sozialverträgliches Verhalten ist anders. Da fragt man nicht ständig nach. Was also, wenn man sagt: Dein Sicherheitsverhalten muss so und so sein. Dann denken sich normale Nutzer:innen: Was würde passieren, wenn ich zum Beispiel Kolleg:innen oder Vorgesetzte frage, ob sie wirklich diese E-Mail verschickt haben? Sie könnten das für Zeitverschwendung halten. Sie könnten mich für inkompetent halten oder denken, dass ich sie für inkompetent halte oder ihnen nicht vertraue. Das sind alles Dinge, die so ein Verhalten letztendlich nicht erlauben oder nicht wirklich gutheißen.

Der RSA-Breach

Ein anderes Beispiel, das, finde ich, auch gegen Security Awareness spricht, vielleicht haben einige von Ihnen das auch mitbekommen. RSA, das ist eine Sicherheitsfirma, die unter anderem SecurID-Tokens produziert. Ein solches Token kann z. B. für Zwei-Faktor-Authentisierung benutzt werden.

RSA wurde einmal gehackt, mit sehr weitreichenden Folgen.[5] Der Angriff begann mit einer Phishing-E-Mail. Diese E-Mail ging nur an zwei ganz kleine Gruppen von Mitarbeiter:innen. Denn die Kriminellen befürchteten, die Leute in einer Security-Firma würden es sonst merken. Die E-Mail kam von einem *Webmaster* einer Jobbörse und hatte einen Anhang: *Recruitment plan. Please open.* Das haben wir auch in dem Angriff, den ich miterlebt habe, gesehen. Und eine einzige Person in der Personalabteilung hat drauf geklickt. Eine einzige Person.

Was dann passiert ist, möchte ich jetzt nicht genau erklären. Auf jeden Fall sind die Kriminellen von diesem Rechner auf einen anderen Rechner gelangt, und dann weiter ins Netz. Dort haben sie angefangen, Daten zu exfiltrieren. Irgendwann haben Intrusion-Detection-Systeme das gemerkt, Alarm geschlagen und das Ganze wurde dann beendet. Das Problem war allerdings, dass niemand bis heute weiß, was die Kriminellen bis dahin eigentlich gesehen hatten und wo im Netz sie waren. Die Vermutung ist, dass dieses SecurID-Token gehackt wurde, in dem Sinne, dass sie eben mit Hilfe gestohlener Informationen voraussagen konnten, welche Codes so ein Token generieren würde. Und konnten sich damit einloggen.

40 Mio. Tokens ausgetauscht

Es gab natürlich einen großen öffentlichen Aufschrei. Trotzdem war RSA noch glimpflich davongekommen: Der finanzielle Schaden von 70 Mio. US-Dollar war für diese Firma nicht besonders hoch. Auch wurde der Angriff ziemlich schnell bemerkt und RSA konnte sich auch ziemlich gut herausreden. Aber als Folge dieses Hacks wurde wohl der amerikanische Rüstungskonzern Lockheed Martin angegriffen. Die haben aber immer bestritten, dass da irgendwas gestohlen wurde. Wir wissen also eigentlich nicht viel. Trotzdem ist das ein Angriff, über den wir zumindest ein bisschen was wissen. Normalerweise gelangen diese Informationen überhaupt nicht an die Öffentlichkeit. Der Angriff auf RSA erfolgte bereits 2011, wird aber trotzdem häufig als Beispiel benutzt, weil man selten überhaupt etwas Konkretes über einen Angriff auf eine Firma erfährt.[6]

RSA hat Details des Falls veröffentlicht, um transparent zu erscheinen, weil sie natürlich Angst hatten, dass ihnen die Kunden massiv abspringen. Sie mussten vierzig Millionen Tokens austauschen, quasi nur auf Verdacht, dass sie vielleicht gehackt wurden.

Was lernen wir daraus? Gut, RSA ist da irgendwie durchgekommen. Aber natürlich gibt es auch (insbesondere kleine und mittlere) Unternehmen, die diese Mittel nicht haben. Das kann gerade für kleinere Firmen, beispielsweise auch Anwaltskanzleien oder Arztpraxen, tödlich sein. Das sollte man nicht auf die leichte Schulter nehmen.

Und trotzdem ist Awareness eigentlich nicht so wichtig. Es ist schön, wenn Awareness da ist. Aber man kann nicht darauf zählen, dass sie immer ausreicht. Bei RSA hat letztendlich Intrusion Detection und auch schnelles Handeln des Sicherheitspersonals mehr oder weniger zur Begrenzung des Schadens geführt. Was man sich also merken sollte: Awareness-Maßnahmen usw. sind vielleicht gut, um die gröbsten Dinge abzufangen. Aber Angreifer, die es wirklich darauf abgesehen haben, werden reinkommen. Letztendlich müsste man schon darauf vorbereitet sein, die Angriffe zu erkennen und auch zu kommunizieren an alle möglichen Seiten, die involviert sind.

Nutzerzentrierter Schutz

Ich habe ja menschengerechte IT-Sicherheit versprochen. Was könnte man hier tun? Klar ist: unter nutzerzentriert zu verstehen, alle müssen die ganze Zeit aware sein, geht nicht.

Also, was könnte man machen? Angriffe melden. Das soll möglichst schnell geschehen, auch Antworten müssen schnell kommen. Es soll möglich sein, z. B. in einer Firma oder in einer Bank, Paypal von mir aus, Angriffe einfach zu melden. Aber man muss darauf vorbereitet sein, dass viele harmlose Vorkommnisse gemeldet werden. Und dann ist es wieder ein Trade-off. Will ich das überhaupt, als Firma zum Beispiel? Oder nehme ich in Kauf, dass einige Angriffe einfach passieren werden? Ja, das ist auch möglich, das wäre Risikoakzeptanz.

Effektivität und Nutzerfreundlichkeit unbekannt

Verlässliche Indikatoren für das Umschalten in den System-2-Modus müssen da sein. Ein Beispiel für Phishing wäre, externe E-Mails als „extern" zu kennzeichnen. Es gab bis heute keine Studie, die zeigen konnte, ob Effektivität und Nutzerfreundlichkeit dieser Maßnahme irgendwie zufriedenstellend sind. Wir wissen es nicht. Deswegen bin ich da auch vorsichtig. Und letztendlich das Wichtigste ist, Fehler zu erwarten. Also Nutzerfehler werden passieren. Ja, das ist quasi dasselbe wie bei sicherheitskritischen Systemen, die mit Safety zu tun haben. Man muss darauf vorbereitet sein.

Antivirus-Studie

Jetzt stelle ich noch eine zweite Studie vor, über die Nutzbarkeit von Antivirus-Meldungen, die wir auch in meiner Gruppe gemacht haben. Es gab vor einiger Zeit eine Umfrage[7] unter Nutzer:innen und Expert:innen. Auf die Frage „Was sind die drei wichtigsten Dinge, die Sie tun, um sich im Internet zu schützen?" haben etwa 42 % der Nutzer:innen, also der Nicht-Expert:innen, Antivirus genannt. Antivirus scheint also das populärste Tool für diese Gruppe zu sein. Aber was macht Antivirus so toll, haben wir uns gefragt. Denn nur wenige Sicherheitsexpert:innen der Studie, etwa 8 %, nutzen Antivirus. Und man muss sagen, dass Antivirus von Sicherheitsexpert:innen als wirklich total schlecht bewertet wird. „Antivirus is dead", sagt John McAfee[8], „Antivirus is dead and doomed to failure", verschärft Antivirus-Pionier Symantec[9]. „Disable your antivirus software, except Microsoft's", meint ein früherer Mozilla-Ingenieur[10] – da freut sich Microsoft natürlich und titelt: „Antivirus is dead, but Windows Defender is not."[11] Und in welche Richtung die Entwicklung geht, zeigt folgender Rat: „It might be time to stop using antivirus, update your software and OS regularly instead, and practise sceptical computing."[12]

Sceptical computing ist dasselbe wie *constant vigilance.* Aber wir haben bereits gelernt, dass *constant vigilance* nicht das ist, was wir normalen Menschen können. Und das wissen sowohl Expert:innen als auch Nicht-Expert:innen. Dieses *be suspicious of everything* ist in beiden Gruppen eine äußerst unpopuläre Sicherheitsmaßnahme.

Also, was heißt das? Wir gehen zurück zu der Frage: Ist Antivirus dann doch die perfekte Sicherheitsmaßnahme?

Wir haben uns gefragt: Was passiert denn, wenn Antivirus tatsächlich einen Virus entdeckt? Wie reagieren denn Leute darauf? Denn Antivirus ist ja normalerweise irgendwie im Hintergrund, und wenn man da Usability untersuchen möchte, müsste man den irgendwie in den Vordergrund bringen mit irgendeiner Malware. Und wir haben uns gefragt: Verstehen denn die Nutzenden überhaupt Malware-Detection-Nachrichten? Und verstehen sie, dass z. B. eine Datei vom Rechner verschwunden ist, und warum?

Also haben wir uns ein Experiment überlegt. Das haben wir in einem Usability-Labor durchgeführt, wo Leute mit ihrem eigenen Laptop erschienen sind. Wir hatten als Coverstory, dass wir Usability von Word und OpenOffice und so weiter untersuchen. Und wir haben den Teilnehmenden zwei USB-Sticks gegeben mit einer harmlosen Datei, die aber so designed war, dass sie Antivirus aktiviert. Also ein harmloser Virus, könnte man sagen. Beim ersten USB-Stick haben sie die Aufgabe noch ganz normal erledigen können. Aber wenn Sie den zweiten USB-Stick in ihren eigenen Laptop reingesteckt haben, dann gab es zwei Fälle. Entweder wurde eine Datei entfernt, die sie für die Ausführung der Aufgaben nicht brauchen; es handelte sich also um ein *irrelevant infected file.* Oder es wurde eine Datei entfernt, die sie für die Aufgaben brauchen, also ein *relevant infected file.*

So, ich erkläre Ihnen mal ein Beispiel. Wird ein Windows-Rechner durch Windows Defender geschützt, erscheint eine Nachricht vom Windows Defender, verschwindet aber nach drei Sekunden wieder. Der hier betroffene Nutzer hat es nie gemerkt. Was den Nutzer aber genervt hat, war folgende Nachricht vom Windows-Betriebssystem: „An unexpected error is keeping you from copying this file. If you continue to receive this error you can use the error code to search for help." Und dann gibt es den schönen Button „Try again". Den haben die meisten Leute benutzt, ohne dabei überhaupt zu verstehen, was da eigentlich passiert ist. Sie haben ein paar Mal „Try again" geklickt, dann „Skip", und dann war die Datei weg. Und sie haben überhaupt nicht verstanden, warum.

Auf einem anderen Rechner war Avira installiert. Da kommt zuerst eine ähnliche Meldung, die besagt, man braucht Admin-Rechte, um auf die Datei zuzugreifen. Und da kann man fortfahren oder überspringen. Und irgendwann kommt auch die Avira-Meldung. Dieser konkrete Proband hat die Meldung nie bemerkt, weil er so beschäftigt damit war, auf „Vorgang wiederholen" zu klicken.

Was war nun unser Ergebnis mit 40 Leuten, die wir getestet haben? Nur 30 haben überhaupt ihre Augen auf die Antivirus-Nachricht fokussiert, das haben wir mit einem Eye-Tracker festgestellt. 19 haben gemerkt, dass es die Nachricht gab. Ja, das ist ein Unterschied. Manchmal kann man etwas sehen, aber eben nicht im Gehirn verarbeiten. Und 14 haben verstanden, was passiert ist.

Und dann hatten wir 20 Leute, bei denen eine relevante Datei entfernt wurde, und 20, bei denen eine irrelevante Datei entfernt wurde, die sie also nicht brauchten. Aber selbst bei der relevanten Datei haben nicht alle gemerkt, dass sie entfernt wurde. Wie konnte das denn passieren? Nun, sie waren so mit Windows-Fehlermeldungen beschäftigt, dass sie überhaupt nichts mehr gemerkt haben. Und von den Leuten, die diese Datei in dem Moment nicht gebraucht haben, haben es nur neun, also knapp die Hälfte, gemerkt. Und verstanden hat es eigentlich nur ein ganz kleiner Teil der Nutzenden. Von 40 haben nur acht verstanden, was mit der Datei denn eigentlich passiert ist.

Wir haben gelernt, dass die Antivirus-Nachrichten selbst für Windows Defender von Windows-Nachrichten völlig verdeckt werden. Wir haben erkannt, dass die Nachrichten, die rechts unten erscheinen, überhaupt nicht bemerkt werden. Nachrichten in der Mitte des Bildschirms werden bemerkt, aber nicht gelesen und nicht verstanden. Und manche Antivirus-Software fragte die Nutzenden: Was sollen sie denn mit der Datei tun? Das führte zu sehr großer Verunsicherung.

Aber wir haben auch gelernt, dass Antivirus trotzdem, trotz all dieser Probleme, ein ideales Sicherheitsschutztool ist. Warum? Nun, die Nutzenden haben ihrem Antivirus das alles verziehen; haben gesagt, dass sie eigentlich sehr zufrieden sind, insbesondere wenn es nicht kostenlos war, haben gesagt, jetzt sind sie wenigstens sicher, dass es auch funktioniert.

Und die Wahrnehmung ist, ein Antivirus-Tool ist so eine Art Experte und Schutzengel zusammen. Und das macht etwas für mich. Etwas, was ich selber nicht machen kann. Ich kann nicht selber Dateien auf Virus überprüfen. Das kann nur der Antivirus tun. Und das ist sozusagen, trotz diesen Usability-Problemen, etwas, was man anstreben sollte. Dass die Sicherheitsmaßnahmen tatsächlich die Nutzenden schützen und ihnen auch dieses Schutzgefühl vermitteln.

Fazit

Noch einmal zusammengefasst: Was ist nutzerzentrierter Schutz? Erst einmal nutzerzentriertes Denken. Man sollte sich überlegen, welche Auswirkungen der Schutzmaßnahmen es geben könnte: auf Geschäftsvorfälle, Produktivität, normales Leben im Vertrauen, soziale Normen im Arbeitsleben, aber auch im Privatleben. Und das gilt für alles, sowohl für Richtlinien als auch für technische Maßnahmen und Schulungen. Und wenn man Prozesse für die Nutzenden gestalten möchte, z. B. in einer Firma, dann sollte man sich überlegen: Wie sollen Angriffe von ihnen gemeldet werden? Wie werden sie über Angriffe informiert? Was sollen sie im Angriffsfall tun? Und vor allem: Können sie das alles? Das ist das Wichtigste. Und man sollte auch Fehler erwarten und darauf vorbereitet sein.

Anmerkungen und Referenzen

1 *Benenson Z (2016) Exploiting Curiosity and Context; How to Make People Click on a Dangerous Link Despite Their Security Awareness. Vortragsvideo, Black Hat USA, Las Vegas, NV, 3. August 2016. https://www.youtube.com/watch?v=ThOQ63CyQR4*

2 *Benenson Z, Gassmann F, Landwirth R (2017) Unpacking Spear Phishing Susceptibility. In: Targeted Attacks Workshop at Financial Cryptography and Data Security, Springer 2017. https://www.cl.cam.ac.uk/~rja14/shb17/benenson.pdf*

3 *https://www.zdnet.de/88256621/neue-phishing-mails-sprechen-paypal-nutzer-mit-korrekter-anrede-an/*

4 *https://www.heise.de/security/meldung/Goldeneye-Ransomware-greift-gezielt-Personalabteilungen-an-3562281.html*

5 *Greenberg A (2021) The Full Story of the Stunning RSA Hack Can Finally Be Told. Wired, Backchannel, 20. Mai 2021. https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told*

6 *Im Falle des beschriebenen RSA Breach kamen erst jetzt – 10 Jahre nach dem Angriff – durch einen Wired-Artikel (vgl. Referenz 4) weitere Details an die Öffentlichkeit, da viele RSA-Beschäftigte durch NDAs (Non-Disclosure-Agreements) bisher zum Schweigen verpflichtet waren.*

7 *Ion I, Reeder R, Consolvo S (2015) „… No one can hack my mind": comparing expert and non-expert security practices. In Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security (SOUPS ,15). USENIX Association, USA, S 327–346*

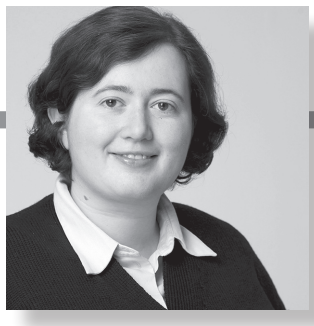
8 *https://thenextweb.com/news/john-mcafee-antivirus-is-dead*

9 *https://www.zdnet.com/article/symantec-calls-antivirus-doomed-as-security-giants-fight-for-survival/*

10 *https://www.bleepingcomputer.com/news/security/former-mozilla-engineer-disable-your-antivirus-software-except-microsofts/*

11 *https://laptrinhx.com/antivirus-is-dead-but-windows-defender-is-not-says-microsoft-3863457969/amp/*

12 *https://arstechnica.com/information-technology/2017/01/antivirus-is-bad/*



Zinaida Benenson

Dr. **Zinaida Benenson** leitet die Forschungsgruppe *Human Factors in Security and Privacy* an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Ihre Forschungsschwerpunkte sind benutzbare IT-Sicherheit, Social-Engineering-Angriffe sowie Sicherheit im Internet der Dinge.