EasyChair Preprint

№ 11721

Ethical Analysis of so-Called Attack Studies in the Context of Raising Security Awareness in Public Spaces

Nhu Thi Thanh Vuong

January 9, 2024

Ethische Analyse von sogenannten Angriffsstudien im Kontext der Erhebung der Security Awareness im öffentlichen Raum

Seminararbeit

von

Name

Studiengang:

Matrikelnummer:

Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB)

KIT-Fakultät für Wirtschaftswissenschaften

Prüfer:

Zweiter Prüfer:

Betreuer:

Eingereicht am: 7. Januar 2024

Inhaltsverzeichnis

1 Einführung

Meist fahre ich mit der Bahn zum KIT und manchmal liegt auf den Sitzen eine Zeitung herum. Überall, sogar beim Bäcker finde ich QR-Codes[1], die meine Aufmerksamkeit suchen. Erwarte ich einen Cyberangriff, wenn ich den einen oder anderen Code scanne, um die betreffende Internetseite aufzurufen?

Die Nutzung von Mobilgeräten im öffentlichen Raum nimmt zu und die Anzahl der Aufrufe von Internetseiten durch QR-Codes hatte sich schon 2022 mehr als vervierfacht [7]. Noch stärker nimmt die Anzahl der Angriffe auf Mobilgeräte zu [28]. Besonders hervorzuheben ist die Zunahme von Phishing [24]. Damit werden persönliche Daten durch Täuschung gestohlen. Dies führt oft zu Identitätsdiebstahl, Kreditkartenbetrug und finanziellen Verlusten [14].

Viele Mobilgeräte sind nicht durch Virenscanner geschützt auch deshalb weil ein Virenscanner laut den Entwicklern von Android nicht notwendig sei [20]. Umso mehr ist der Anwender gefragt, der mit seinem gesunden Menschenverstand ein mehr oder weniger vorhandenes Sicherheitsbewusstsein hat, die so genannte „Security Awareness“. Gemeint ist hier die Fähigkeit zur Wahrnehmung von Gefahren im Internet OHNE vorhergehendes Security Awareness Training[2].

Mit Angriffsstudien wird das menschliche Verhalten erforscht, um die Maßnahmen zur Abwehr von Angriffen im Bereich der Cyber-Security zu bewerten und zu verbessern. Die Angriffe werden bei den Studien nur simuliert, der Proband wird also mehr oder weniger gar nicht oder falsch über die Studie aufgeklärt, denn würde er vorab umfassend aufgeklärt und gar eine explizite Einwilligung eingeholt, so wäre das Ergebnis falsch und unbrauchbar.

Öffentlicher Raum bedeutet nicht nur den physischen freien Zugang von jedermann, sondern auch zufällige Probanden anstelle einer festen Zielgruppe. Auch wird unterstellt, dass sich hier Probanden finden ohne Security Awareness Training. Öffentlicher Raum bedeutet aber auch, dass der Proband bei der Durchführung der Studie arglos ist und keinen Cyberangriff erwartet.

Diese Arbeit will unter ethischen Gesichtspunkten Argumente identifizieren und abwägen, ob und unter welchen Umständen solche Angriffsstudien zur Erhebung der Security Awareness im öffentlichen Raum an arglosen Probanden gerechtfertigt werden können. In diesem Kontext steht meine Forschungsfrage: „Inwieweit sind fehlende Aufklärung, fehlende Information, Irreführung oder gar Täuschung von Probanden in unserem heutigen

[1] Bei einem QR-Code („Quick-Response-Code“) handelt es sich um eine Grafik zur Darstellung von Buchstaben, Ziffern und Zeichen, die im öffentlichen Raum überwiegend Internetadressen darstellt.

[2] Security Awareness Training wird bspw. von Dienstleistern oder vom Bundesamt für Sicherheit in der Informationstechnik [1] angeboten insbesondere für Firmen zur Mitarbeiterschulung.

westlichen Wertesystem ethisch gerechtfertigt?“.

Ein bewährter Ansatz bei den bisherigen Angriffsstudien ist das Debriefing[3] . Mit dieser nachträglichen Aufklärung werden die Probanden nach der Studie über die Täuschung oder Irreführung informiert, was zu massiven Beschwerden und teilweise zu seelischen Beeinträchtigungen geführt hat [21].

Im zweiten Kapitel werden wichtige Begriffe beleuchtet, definiert und eingegrenzt. Damit wird diese Arbeit zugleich auf die ethischen Gesichtspunkte begrenzt. Verzichtet wurde bewusst auf die im Vorfeld erstellte Auflistung der Vor- und Nachteile von Angriffsstudien, da bei gründlicher Betrachtung die Argumente rein sachlicher Natur sind und es sich somit nicht um ethische Gesichtspunkte handelt. Im dritten Kapitel werden die ethischen Gesichtspunkte herausgearbeitet und in ein Kategoriensystem nach ethischer Relevanz eingeordnet. Die Forschungsfrage wird nach ethischer Relevanz abgestuft und schließlich beantwortet. Die Diskussion und das Fazit runden diese Seminararbeit ab.

[3]Debriefing ist eine Nachbesprechung anstelle vom Briefing als Vorgespräch. Bei solchen Angriffsstudien dient das Debriefing dazu, die fehlende Einwilligung nachzuholen, die Irreführung und Täuschung zum Zwecke der Studie aufzuklären und schlechte Gefühle, Groll und Ärger über die durchlebte Täuschung aufzufangen und so gut wie möglich wieder zu heilen. Als eine Art von Entschädigung wird hier sogar ein kostenloses kleines Security Awareness Training vorgeschlagen [21].

2 Begriffsdefinitionen und Eingrenzungen

2.1 Wahrheit als Grundlage der Ethik

Im heutigen westlichen Wertesystem ist die Erforschung der Wahrheit ethisch gesehen das wissenschaftliche Ziel. „Anlässlich meiner Promotion in Basel musste ich in einem vorformulierten Gelübde versprechen, die wissenschaftliche Erforschung der Wahrheit immer als eine ernste und notwendige Aufgabe zu betrachten‘ [12]“. Das schreibt die Lehrbeauftragte für Ethik an verschiedenen deutschen Universitäten und Hochschulen [10] Prof. Dr. Dagmar Fenner in Ihrem Werk „Einführung in die Angewandte Ethik“.

„Ethik ist die Lehre bzw. Theorie vom Handeln gemäß der Unterscheidung von gut und böse.“ sagt Prof. Dr. Andreas Suchanek im Gabler Wirtschaftslexikon [18] als Vorstandsvorsitzender des Wittenberg-Zentrums für Globale Ethik [23]. Und Fenner [9] führt aus: „Die Ethik versucht ganz generell die Frage zu beantworten, wie die Menschen handeln sollen. Anders als die theologische Ethik setzt die philosophische säkulare Ethik bei der Beantwortung dieser Frage keinen Glauben an eine bestimmte Religion voraus.“

2.2 Ethik – Wissenschaftliche Bereichsethik

In der Ethik wird zwischen einer Vielzahl von Bereichsethiken unterschieden wie z. B. Medizinethik, Tierethik, Wirtschaftsethik, Umweltethik u.v.a.m. In dieser Seminararbeit wird der Begriff der Ethik eingegrenzt auf die Wissenschaftsethik, denn „Wissenschaftsethik ist die Bereichsethik, die sich mit den ethischen Problemen bei der Gewinnung und Verwendung wissenschaftlicher Erkenntnisse befasst [11].“

2.3 Security Awareness im öffentlichen Raum

Bei der Security Awareness geht es – wie in der Einführung schon hinreichend definiert - um den gesunden Menschenverstand und um dessen Fähigkeit zur Wahrnehmung von Gefahren im Internet OHNE vorhergehendes Security Awareness Training. Der Proband ist also arglos und erwartet keinen Cyberangriff. In dieser Seminararbeit erfolgt eine Eingrenzung auf die Nutzung des Internets im öffentlichen Raum, zu dem jedermann einen physischen freien Zugang hat wie z. B. Öffentliche Verkehrsmittel, Bushaltestellen, Einkaufszentren, Bahnhöfe oder Flughäfen.

2.4 Angriffsstudien – Verhalten

Der Begriff der Angriffsstudie ist zu definieren und sehr deutlich einzugrenzen. Denn aus der Frage, was mit der Studie erforscht wird, ergeben sich bereits eine Vielzahl an Möglichkeiten.
- Wird der Angriff selbst erforscht?
- Wird sein Inhalt erforscht, also die Art und Weise seiner Durchführung?
- Soll erforscht werden, unter welchen Umständen ein Angriff ausgelöst wird oder nicht?
- Soll erforscht werden, welche Umstände welche Art von Angriff auslösen oder verhindern?
- Wird der Ablauf eines Angriffes erforscht und wie dieser das Opfer erreicht?

Der Begriff der Angriffsstudie ist derart vielseitig, dass die vorliegende Seminararbeit nur solche Angriffsstudien ethisch analysieren kann, mit denen das Sicherheitsbewusstsein der Probanden erforscht wird, also deren Verhalten vor, während und nach einem Cyber-Angriff bei der Internetnutzung im öffentlichen Raum. Hierzu gehört insbesondere die Frage, wie sich der Proband bei dem Angriff gefühlt hat und warum er wie genau auf den Angriff reagierte.

2.5 Phishing und Rechtliche Hintergründe in Europa und den USA

Der Begriff des Phishings wird dermaßen unterschiedlich verstanden, verwendet und definiert, dass er einer stufenweisen Definition bedarf, aus der sich das Kategoriensystem des nachfolgenden Kapitels ableitet. Das Wort Phishing ist laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ein Kunstwort, welches sich aus PASSWORT und FISHING zusammensetzt [2]. Laut den vom BSI herausgegebenen Verbraucherinformation ist unter Phishing die Preisgabe vertraulicher ZUGANGSDATEN [4] zu verstehen. Zu den Zugangsdaten gehört grundsätzlich das Passwort. Ohne das Ausspähen von Passwörtern liegt folglich KEIN Phishing vor.

Hier kollidiert das BSI bereits mit der Europäischen Datenschutzgrundverordnung (DSGVO), denn dort sind keinesfalls die Zugangsdaten bestehend aus Zugangsname mit dem dazugehörenden Passwort besonders geschützt, sondern es werden alle personenbezogenen Daten gleichgestellt [8]. Schon das Ausspähen einer E-Mail-Adresse darf demnach als Phishing gelten.

IBM als börsennotiertes US-amerikanisches IT- und Beratungsunternehmen definiert Phishing für seine mehr als eine Viertelmillion Mitarbeiter [22] so: „Bei Phishing-Angriffen handelt es sich um betrügerische E-Mails, Textnachrichten, Telefonanrufe oder Websites, die darauf abzielen, Menschen dazu zu verleiten, Malware herunterzuladen, vertrauliche Informationen weiterzugeben (z. B. Sozialversicherungs- und Kreditkartennummern,

Bankkontonummern, Anmeldedaten) oder andere Handlungen vorzunehmen, die sie selbst oder ihr Unternehmen der Cyberkriminalität aussetzen. [14]“

In den USA definiert das National Institute of Standards and Technology (NIST) das Phishing unter Verzicht auf das Ausspähen des Passworts deutlich breiter als eine Technik, mit der versucht wird, durch eine betrügerische Aufforderung an sensible Daten wie bspw. Kontonummern zu gelangen [25].

Auf der rechtlichen Ebene bestätigt das US-amerikanische Legal Information Institute (LII) den Ansatz der DSGVO und geht noch darüber hinaus, indem es schon das Verleiten zur Preisgabe von personenbezogenen Daten ausdrücklich als Phishing definiert [16]. Nicht ohne auf die Schadenersatzpflicht hinzuweisen, die in Höhe von mindestens 500.000 US-Dollar für Phishing-Opfer nach Kalifornischem Recht gegeben ist [16]. In diesem fast 19 Jahre alten Gesetz wird schon in der Einleitung definiert, dass Phishing ALLE Persönlichen Daten umfasst (also auch den Namen oder die E-Mail-Adresse), die „fraudulently“ erlangt werden, also nicht nur betrügerisch, sondern auch wissentlich falsch, unter Vorspiegelung falscher Tatsachen oder arglistig [13].

2.6 Aufkommende Gefahren

Durch einen „erfolgreichen“ Phishing-Angriff wird gerade mal nur ein einzelnes Paar an Zugangsdaten gestohlen, nämlich ein bestimmter Zugangsname mit dem dazugehörenden Passwort. Deutlich mehr Zugangsdaten sind bei vielen Nutzern im Browser gespeichert oder in einem eventuell vorhandenen Passwort-Manager. Eine brandneue Meldung vom 14.11.2023 in „cybersecurity news“ teilt mit, dass die neue Schadsoftware „Stealc“ nicht nur Passwörter aus den üblichen Browsern stiehlt, sondern ganze Passwortdateien [17]. Auch Online-Anbieter sind betroffen. Bei diesen wurden im Jahr 2020 bei 117 Vorfällen jeweils durchschnittlich 17 Millionen Datensätze gestohlen [15].

Eine Schadsoftware kann durch den Klick auf einen Link ebenso installiert werden wie durch den Seitenaufruf einer infizierten Seite, durch das sogenannte „Drive-by“. Die Schadsoftware installiert sich dabei unbemerkt im Hintergrund und kann nur noch durch einen guten Virenscanner entdeckt werden. Doch viele Mobilgeräte haben keinen Virenscanner [20]. Dabei sind Drive-by Angriffe auf Mobilgeräte seit mehr als 10 Jahren bekannt [19] und auch heute aktuell [6].

Aufkommende Gefahren sind folglich Phishing-Angriffe auf Mobilgeräte bis hin zum Diebstahl von Passwortdateien. Dies hat das BSI bisher noch nicht erkannt, denn die Verwendung von Passwortmanagern wird ausdrücklich empfohlen [3], obwohl Experten in der Fachpresse vor deren Verwendung schon seit mehr als sieben Jahren warnten [5][26].

3 Ethische Analyse - Gesichtspunkte und Rechtfertigung

Gegenstand dieser Seminararbeit ist die ethische Analyse von sogenannten Angriffsstudien im Kontext mit der Erhebung von Security Awareness im öffentlichen Raum. Es werden ethische Gesichtspunkte identifiziert und abgewogen. Die Forschungsfrage hierzu lautet: „Inwieweit sind fehlende Aufklärung, fehlende Information, Irreführung oder gar Täuschung von Probanden in unserem heutigen westlichen Wertesystem ethisch gerechtfertigt?“

3.1 Kategoriensystem nach ethischer Relevanz

Im ersten Schritt der ethischen Betrachtung und Analyse steht die Angriffsstudie an sich, also die Frage nach dem genauen Gegenstand der Angriffsstudie. Die große Vielfalt von möglichen Angriffen zum Ersten, die rechtliche Gleichstellung per Definition zum Zweiten sowie die großen Gegensätze beim Verständnis von Phishing (siehe Kapitel 2.5) zum Dritten erfordern diese Einteilung in Kategorien.

3.1.1 Kategorie 1

In dieser ersten Kategorie erfolgt ohne Simulation lediglich eine nachträgliche wissenschaftliche Untersuchung von tatsächlichen Ereignissen. So werden auch bspw. Morde, Körperverletzungen, Vergewaltigungen oder Silvesterausschreitungen ausschließlich im Nachhinein untersucht und keinesfalls vorsätzlich für wissenschaftliche Studienzwecke begangen. Gleiches gilt in dieser Kategorie 1 auch für mögliche seelische Verletzungen der Probanden durch die Angriffsstudien selbst oder durch ein nach der Studie versäumtes, abgebrochenes, enttäuschendes oder gar missglücktes Debriefing. Nachträglich durchgeführte Studien zu tatsächlichen Angriffen sind daher ethisch stets gerechtfertigt. Die Studie selbst und ihre Ergebnisse können ethisch nicht in Frage gestellt werden und entsprechen aus ethischer Sicht einer lupenreinen wissenschaftlichen Arbeit.

3.1.2 Kategorie 2

In der zweiten Kategorie geht es um Angriffe zur Erlangung von einfachen persönlichen Daten wie Name oder Anschrift. Im einfachsten Fall wird nur die E-Mail-Adresse ausgeforscht bspw. dadurch, dass der Proband getäuscht wird und denkt, er melde sich für einen Newsletter an. Damit entspricht eine derartige Angriffsstudie zwar der gesetzlichen Definition einer Phishing-Studie, doch es darf unterstellt werden, dass ein argloser Proband

ohne vorhergehendes Security-Awareness-Training unter Phishing die Preisgabe der ganz persönlichen Kombination seines Zugangsnamens und des dazu gehörenden Passworts versteht. Damit ist eine solche Studie gesetzlich gerechtfertigt, denn das Ausforschen der E-Mail-Adresse ist in Europa wie in den USA dem Ausspionieren der Zugangsdaten per rechtlicher Definition gleichgestellt. Doch das wissenschaftliche Ergebnis ist unbrauchbar, weil der Proband – hier der arglose Proband im öffentlichen Raum – eine ganz andere Vorstellung von Phishing hat als der Gesetzgeber und der die Studie durchführende Wissenschaftler. Damit ist eine solche Studie schon im Vorfeld (also ohne Analyse der Täuschung) bereits auf Grund ihrer Unbrauchbarkeit ethisch nicht gerechtfertigt. Einen ethischen Wert bekäme eine derartige Angriffsstudie der Kategorie 2 zumindest dadurch, dass der Proband im Rahmen des Debriefings auch dazu befragt wird, ob er das Eintragen seiner E-Mail-Adresse in einen Newsletter schon vor seiner Teilnahme an der Studie als Phishing verstanden hat oder nicht.

3.1.3 Kategorie 3

In der dritten Kategorie sollen sensible persönliche Daten ausgeforscht werden, wie die Kreditkartennummer, die Kontonummer oder das Einkommen des Probanden. In der Kategorie 3 ist wie folgt abzustufen und zu unterteilen:

a) Die Preisgabe der Kreditkartennummer oder gar des Sicherheitscodes auf der Rückseite bei alltäglichen Online-Bezahlvorgängen lässt ein äußerst geringes Sicherheitsbewusstsein erwarten.

b) Ein höheres Sicherheitsbewusstsein hat, wer beim Bezahlvorgang stets seine Kontonummer zwecks Lastschrift hinterlegt und auf das achtwöchige Widerspruchsrecht vertraut.

c) Eine noch höhere Security Awareness hat derjenige, der seine Kreditkartendaten oder seine Bankdaten nur bei seinem Zahlungsdienstleister wie bspw. PayPal hinterlegt und stets – so auch im öffentlichen Raum – nur über seinen Dienstleister bezahlt. Zu diesem Zweck werden häufig QR-Codes angeboten, die direkt zum Dienstleister führen.

d) Ein sehr hohes Sicherheitsbewusstsein ohne Security Awareness-Training hat derjenige, der zum Ersten die Adresse seines Bezahldienstes sehr genau prüft insbesondere nach dem Scan eines Q-Codes gerade im öffentlichen Raum und der zum Zweiten innerhalb fremder WLANs einen Bezahlvorgang spätestens vor der Eingabe seines Passworts abbricht in dem Bewusstsein, dass andere diese Daten mitlesen (sniffen) könnten.

e) Die höchste Sicherheit hat, wer im öffentlichen Raum beim Bezahlen auf QR-Codes verzichtet und stattdessen die kontaktlose, sogenannte NFC-Bezahlfunktion seiner Karte oder seines Mobilgerätes nutzt.

Wie in Kategorie 2 wird auch in Kategorie 3 die Preisgabe der Daten von einem arglo-

sen Probanden im öffentlichen Raum noch NICHT als Phishing erlebt. Die Erforschung der Security Awareness gerade im öffentlichen Raum und insbesondere bei der Verwendung von QR-Codes macht zwar Sinn, auch ethisch gesehen, doch sind Angriffsstudien mit simulierten Angriffen hier ein ungeeignetes Mittel. Denn zum einen würden sie das Vertrauen der Kunden in ihren bargeldlosen Bezahlvorgang massiv untergraben und zum anderen hätte die hierdurch erforschte Security Awareness wie schon in der Kategorie 2 keinen brauchbaren Wert, denn die arglosen Probanden sehen in der gewollten Preisgabe dieser Daten noch kein Phishing. Richtiges Phishing beginnt in dieser Kategorie allerdings mit dem Ausspähen der Karten-PIN oder des Passworts für den Bezahldienst.

Es darf abschließend unterstellt werden, dass die weiteren sensiblen Daten wie Einkommen oder Sozialversicherungsnummer ohnehin nur in Ausnahmefällen wie bspw. bei einer Kontoeröffnung oder bei einer Kreditbeantragung weitergegeben werden.

3.1.4 Kategorie 4

In der Kategorie 4 erhält der Proband unter einem Vorwand einen Link zum Download von Schadsoftware und wird aufgefordert, diese herunterzuladen und zu installieren. Vorstellbar wäre bspw. eine kostenlose Fußball-App, die an den Bushaltestellen und Bahnhöfen nach einem Fußballspiel auf Plakaten zum Download per QR-Code angeboten wird.

Gerade im öffentlichen Raum und insbesondere über QR-Codes ist eine derartige Angriffsstudie sehr hilfreich zur Erforschung der Security Awareness im öffentlichen Raum. Ethisch gerechtfertigt ist eine derartige Angriffsstudie der Kategorie 4 jedoch nur, wenn die vermeintliche Installation der Schadsoftware keine Installation auslöst, sondern eine Befragung und das Debriefing. Im Rahmen des Debriefings könnte der Proband in Abstimmung mit einem Anbieter von Antivirenprogrammen ein kostenloses Jahresabonnement der Schutzsoftware für sein Mobilgerät erhalten. Ethisch sehr fair wäre es, wenn der Proband bei der Installation dieser Zugabe wählen könnte zwischen automatischer Verlängerung nach einem Jahr oder automatischem Ende des Abonnements.

(Tipp zur praktischen Ausführung: der Proband sollte nach dem Scannen des Codes oder schon auf dem Plakat aufgefordert werden, den Link nur abzuspeichern und die App später in Ruhe zu installieren.)

3.1.5 Kategorie 5

In der Kategorie 5 besucht der Proband eine Internetseite und allein schon durch diesen Besuch wird eine Schadsoftware installiert. Für diese sogenannten Drive-by-Downloads sind Mobilgeräte besonders geeignet, da sie oft keinen Virenscanner haben [20]. Der öffentliche Raum bietet sich durch seine QR-Codes nahezu an. Im schlimmsten Fall werden

Passwortdateien und Zugangsdaten aus dem Browser gestohlen. Derartige Angriffsstudien sind unter keinen Umständen ethisch gerechtfertigt. Dabei wären sie – sachlich wie objektiv gesehen – besonders wichtig. Es wird sogar vermutet, dass selbst solche Nutzer, die um die Risiken einer Ausforschung von Passwörtern aus den Browsern wissen und die deshalb nie am PC ihre Passwörter im Browser speichern, dies im Mobilgerät aus Bequemlichkeit dennoch tun. Hier hilft nur eine umfangreiche Aufklärung und ein guter Virenscanner auch auf dem Mobilgerät am besten in Verbindung mit einem Security-Awareness-Training.

3.1.6 Kategorie 6

Diebstahl und Ausforschen von echten Zugangsdaten (Name und Passwort als Paar), also echtes Phishing so wie es von arglosen Probanden im öffentlichen Raum ohne Security Awareness Training verstanden wird. Es bedarf keiner näheren Erläuterung, dass eine derartige Angriffsstudie aus ethischen Gründen überhaupt nicht zulässig ist. Der wissenschaftlicher Wert einer solchen Studie wäre zudem ethisch gesehen höchst zweifelhaft. Zu Studienzwecken wird auf den Vorschlag in Kategorie 4 verwiesen. Ergänzend könnten die Erfahrungen aus der Kategorie 6 einfach nur abgefragt werden. Hierbei sollte zu jeder Fragestellung die aktuelle Tagesform des Probanden erhoben werden, denn diese spielt eine erhebliche Rolle, wie eine persönliche Autorenerfahrung zeigt:
„Zum Jahreswechsel sollte noch schnell der Stand des Gaszählers an den Anbieter übermittelt werden. Die Seite Oktopus.de wurde aufgerufen und die Zugangsdaten wurden eingegeben. Offenbar enthielt die Eingabe einen Fehler, denn es erfolgte kein Login. Also wurde erneut sehr langsam eingegeben. Wieder erfolgte kein Login und erst jetzt wurde bemerkt, dass die Seite Oktopus.de anstelle von Octopus.de aufgerufen worden war. Da der falsche Seitenaufruf ersichtlich nicht zu einer Phishing-Seite führte, sondern eine Seite vom deutschen Akademischen Austauschdienst e.V. aufgerufen hat, wurde auf die ansonsten gebotene Änderung der Zugangsdaten ausnahmsweise verzichtet im Vertrauen darauf, dass Passwörter zu Fehleingaben in den üblichen Zugriffsprotokollen nicht aufgezeichnet werden. Doch was war die Ursache für einen derartigen Kardinalfehler? Subjektiv gesehen war das zum einen der massive Zeitdruck wegen der unfertigen Seminararbeit und zum anderen ein Augenblicksversagen so wie es jedermann beim Autofahren schon mal passieren kann.“

3.2 Abstufung der Forschungsfrage nach ethischer Relevanz

Aus der Forschungsfrage „Inwieweit sind fehlende Aufklärung, fehlende Information, Irreführung oder gar Täuschung von Probanden in unserem heutigen westlichen Wertesystem ethisch gerechtfertigt?“ ergibt sich die folgende Abstufung nach ethischer Relevanz:

a) Aufklärung der Probanden bedeutet hier, dass der Proband umfassend und mindestens nach allen gesetzlichen Vorgaben VORAB sehr genau über die Studie aufgeklärt und informiert wurde und dass er somit schon vor Beginn der Exploration umfassend vorbereitet wurde und die Details auch verstanden hat. Zudem wurde seine Zustimmung zu der Studie aktiv und explizit eingeholt. So soll es ethisch sein. Mit diesem Ansatz ist jede Angriffsstudie unter ethischen Gesichtspunkten gerechtfertigt, auch wenn sie gemäß dem zuvor vorgestellten Kategoriensystem für sich gesehen zunächst nicht zulässig wäre.

b) Information der Probanden bedeutet hier, dass der Proband wahrheitsgemäß, umfassend und vollständig informiert wurde und somit insbesondere keine Irreführung oder Täuschung vorliegt. Jedoch bleibt es dem Probanden überlassen, ob er alle Hinweise liest oder nicht. Wahrscheinlich wird er die Hinweise nicht lesen. Anstelle einer aktiven Zustimmung gilt bereits die Teilnahme als Zustimmung.

Beispiel: Ein großes Plakat im öffentlichen Raum fordert zur Teilnahme an einer wissenschaftlichen Studie auf. Als Belohnung wird bspw. eine Lotterie mit kleinen Preisen oder ein kostenloses Security Awareness Training angeboten. Auf dem großen Plakat findet sich unten das Kleingedruckte. Hier findet sich bspw. der Hinweis, dass der Proband die Studie jederzeit abbrechen kann. Über dem QR-Code steht gut lesbar, dass mit der Teilnahme die Bedingungen akzeptiert werden und dass die Studie jederzeit unterbrochen werden kann, um sie zu Hause fortzusetzen. Der Proband sieht hier wahrscheinlich nur den großgedruckten Hinweis, dass er die Studie später fortsetzen kann und erkennt nicht die Möglichkeit zum Abbrechen im Kleingedruckten.

Mag eine derartige Angriffsstudie nicht alle ethischen Wünsche erfüllen, so ist sie dennoch aus ethischer Sicht absolut in Ordnung. Ein kurzer Blick auf die alltägliche Trickserei und Irreführung in der tagtäglichen Werbung belegt diese ethische Bewertung.

c) Irreführung der Probanden bedeutet hier, dass keine Täuschung erfolgt, dass aber die Aufklärung vor dem Beginn der Angriffsstudie nicht oder nur sehr unvollständig erfolgt. Die Einwilligung des Probanden wird zunächst global (sehr grob) eingeholt und erst nachträglich noch einmal im Detail bestätigt.

Beispiel: „Nehmen Sie Teil an einer wissenschaftlichen Studie des KIT über die Nutzung Ihres Mobilgeräts in der Öffentlichkeit. Sie benötigen etwa 30 Minuten und können die Studie auch zu Hause fortführen. Wenn Sie alle Fragen beantworten, dann erhalten Sie einen Einkaufsgutschein über 10 Euro für den Supermarkt hier neben Ihnen.“ (Wird vom Einkaufszentrum gesponsert ab einem Einkauf von bspw. 30 Euro oder die Studie wird mit der Geschäftsleitung geteilt und enthält zusätzlich einige für das Unternehmen wichtige Fragen). Die eigentliche Angriffsstudie beginnt mit der Frage: „Haben Sie beim Scannen des QR-Codes für diese Befragung einen Phishing-Versuch erwartet? gar nicht__, vielleicht__, wahrscheinlich__, sicher__.“ Der Proband wurde in diesem Beispiel über den

wahren Charakter der Studie so irregeführt, dass die Beantwortung der Fragen einer echten Angriffsstudie angenähert ist. Zudem impliziert die Fragestellung bereits ein Security Awareness Training. Die zweite Zustimmung kommt dann zum Schluss: „Mit Ihrem Klick erteilen Sie Ihre Zustimmung zur Verwertung Ihrer Angaben in anonymisierter Form. Ihren Einkaufsgutschein erhalten Sie getrennt von dieser Studie direkt vom Einkaufszentrum. Bitte geben Sie hierzu noch Ihren Namen, Ihr Alter und Ihre E-Mail-Adresse an und kreuzen Sie bitte an, ob Sie regelmäßig Sonderangebote vom Einkaufszentrum erhalten möchten oder nicht."

d) Täuschung der Probanden bedeutet hier keinesfalls einen aktiven Betrug, der sich ethisch von vorneherein verbietet. Dies gilt insbesondere für das echte Phishing mit gefälschten Zugangsseiten.

Vielmehr wird unter Täuschung der Probanden hier ein sozial anerkannter Betrug verstanden im Sinne von „Verstehen Sie Spaß". Bei dieser Unterhaltungssendung werden Streiche gespielt und mit versteckter Kamera gefilmt. Ein Debriefing klärt dann alles auf und reduziert den anfänglichen Betrug zu einem lustigen Streich, an dem sich das Opfer zusammen mit Millionen Fernsehzuschauern erfreut.

Soweit es gelingt, eine ernsthafte Angriffsstudie durch ein wirkungsvolles und menschlich gutes Debriefing zu einem Streich herunterzuspielen, ist auch die damit verbundene Täuschung des Probanden ethisch gerechtfertigt.

Aus Autorensicht ist allerdings kein passendes Beispiel ersichtlich. Überträgt man diesen Ansatz (Täuschung als Streich) auf das im Kapitel 3.1 aufgestellte Kategoriensystem, so ist außerdem keine Notwendigkeit zur Täuschung bei Angriffsstudien ersichtlich.

3.3 Beantwortung der Forschungsfrage

Inwieweit sind fehlende Aufklärung, fehlende Information, Irreführung oder gar Täuschung von Probanden in unserem heutigen westlichen Wertesystem ethisch gerechtfertigt? Fehlende Aufklärung ist normalerweise immer ethisch gerechtfertigt. Täuschung ist normalerweise niemals ethisch gerechtfertigt. Täuschung als Streich mit ethisch einwandfreiem Debriefing bleibt aber zulässig. Bei allen Angriffsstudien im öffentlichen Raum hat aus ethischen Gründen immer der Proband als Mensch mit Mittelpunkt des Interesses zu stehen. „Ist der Proband zufrieden, freut sich die Studie."

4 Diskussion

Neben dem im vorhergehenden Kapitel vorgestellten eigenen ethischen Ansatz gibt es weitere ethische Ansätze in der Literatur. So enthält bspw. das Werk „Empirisches wissenschaftliches Arbeiten“ [27] eine umfangreiche und sehr detaillierte Anleitung mit ethischen Richtlinien zum wissenschaftlichen Arbeiten. Wahrhaftigkeit, Offenheit, Selbstdisziplin, Selbstkritik und Fairness sind die Leitlinien, welche von den Schweizer Akademien der Wissenschaften übernommen wurden. Bis zur Gestaltung der Datenerhebung und dem Umgang mit Daten finden sich hier sehr gründliche, in die Tiefe gehende und ausführliche Leitlinien. Diese eignen sich zur Vertiefung der ethischen Fragen, passen aber nicht als Ansatz für das hier behandelte Thema. Hervorzuheben sind allerdings die Schlussbemerkungen, wonach jede wissenschaftliche Arbeit in ihrer Art einmalig ist und ihre eigenen ethisch relevanten Bereiche ausweist. Neben dem Befolgen der Richtlinien und Empfehlungen ist außerdem die ethische Sensibilität des Forschenden notwendig.

Eine weitere ethische Herangehensweise findet sich in der Finn-Studie [21]. Diese unterscheidet zwischen der Befragung von Einzelpersonen zu ihren Erfahrungen mit Phishing-Angriffen, zwischen dem Test von Probanden unter Laborbedingungen zu ihrer Fähigkeit zum Erkennen von Phishing-Mails und der Zusammenarbeit mit Organisationen (bspw. Bildungseinrichtungen und Arbeitgebern) zur Nachahmung von Phishing-Angriffen. Auch dieser Ansatz passt hier nicht zum Thema.

Zu diskutieren und zu hinterfragen ist auch die Rolle von Ethikkommissionen, auch Institutional Review Board oder IRB genannt, da diese anders als der Name vermuten lässt neben der Ethik sehr stark auf die rechtlichen, sozialen und moralischen Gesichtspunkte eines Forschungsvorhabens achten. Anders als in den USA könnte sich ein europäisches, insbesondere ein deutsches Forschungsvorhaben gegenüber seiner Kommission auf Artikel 33 der DSGVO berufen. Dort sind die Ausnahmen für wissenschaftliche Zwecke geregelt. Fehlende Aufklärung, fehlende Information und Irreführung durch unterlassene Information wie im Kapitel 3 definiert sind demnach für wissenschaftliche Zwecke ausdrücklich erlaubt und dürfen „oft“ genutzt werden.

5 Fazit

Die ethische Analyse von sogenannten Angriffsstudien im Kontext der Erhebung von Security Awareness im öffentlichen Raum führt über die Forschungsfrage „Inwieweit sind fehlende Aufklärung, fehlende Information, Irreführung oder gar Täuschung von Probanden in unserem heutigen westlichen Wertesystem ethisch gerechtfertigt?“ zu dem Fazit: Fehlende Aufklärung ist normalerweise immer ethisch gerechtfertigt. Täuschung ist normalerweise niemals ethisch gerechtfertigt. Täuschung als Streich mit ethisch einwandfreiem Debriefing bleibt aber zulässig. Bei allen Angriffsstudien im öffentlichen Raum hat aus ethischen Gründen immer der Proband als Mensch mit Mittelpunkt des Interesses zu stehen. „Ist der Proband zufrieden, freut sich die Studie.“

Literatur

[1] BSI. 2024. awareness - problembewusstsein und sicheres verhalten. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Faktor-Mensch/Awareness/awareness_node.html, letzter Zugriff: 07.01.2024.

[2] Bundesamt für Sicherheit in der Informationstechnik. 2022. Passwortdiebstahl durch Phishing E-Mails. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/passwortdiebstahl-durch-phishing_node.html#:~:text=Spam%20verstopft%20nicht%20nur%20E,aus%20Passwort%20und%20Fishing%20zusammensetzt., letzter Zugriff: 07.01.2024.

[3] Bundesamt für Sicherheit in der Informationstechnik. 2023. Bundesamt für Sicherheit in der Informationstechnik - Online-Accounts mit dem Passwortmanager schützen. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Projekt-Accountschutz/browser-passwortmanager.html, letzter Zugriff: 07.01.2024.

[4] Bundesamt für Sicherheit in der Informationstechnik. 2023. Wie schützt man sich gegen Phishing? https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Schutz-gegen-Phishing/schutz-gegen-phishing_node.html, letzter Zugriff: 07.01.2024.

[5] Redaktion CHIP/DPA. Vorsicht vor Passwortmanagern: Experten warnen vor Sicherheitsrisiko - CHIP. https://www.chip.de/news/Vorsicht-vor-Passwortmanagern-Experten-warnen-vor-Sicherheitsrisiko_103205665.html, letzter Zugriff: 07.01.2024.

[6] Ritesh Chugh. 2023. Can your mobile phone get a virus? Yes – and you'll have to look carefully to see the signs. https://theconversation.com/can-your-mobile-phone-get-a-virus-yes-and-youll-have-to-look-careful\ly-to-see-the-signs-181720, letzter Zugriff: 07.01.2024.

[7] Benjamin Claeys. 2024. QR-Code-Nutzungsstatistik 2022: 433 % Scan-Anstieg und 438 % Generierungsschub. https://www.qrcode-tiger.com/de/qr-code-statistics-2022-q1, letzter Zugriff: 07.01.2024.

[8] Datenschutz-Grundverordnung. 2016. Art. 1 DSGVO – Gegenstand und Ziele - Datenschutz-Grundverordnung (DSGVO). https://dsgvo-gesetz.de/art-1-dsgvo/.

[9] Dagmar Fenner. 2022. Einführung in die Angewandte Ethik (Seite 12). https://elibrary-utb-de.ezproxy.blb-karlsruhe.de/doi/10.36198/9783838559025.

[10] Dagmar Fenner. 2022. Einführung in die Angewandte Ethik (Seite 2). https://elibrary-utb-de.ezproxy.blb-karlsruhe.de/doi/10.36198/9783838559025.

[11] Dagmar Fenner. 2022. Einführung in die Angewandte Ethik (Seite 208). https://elibrary-utb-de.ezproxy.blb-karlsruhe.de/doi/10.36198/9783838559025.

[12] Dagmar Fenner. 2022. Einführung in die Angewandte Ethik (Seite 212). https://elibrary-utb-de.ezproxy.blb-karlsruhe.de/doi/10.36198/9783838559025.

[13] Rep. Hooley. 2005. Text - H.R.1099 - 109th Congress (2005-2006): Anti-phishing Act of 2005. https://www.congress.gov/bill/109th-congress/house-bill/1099/text?s=1&r=186, letzter Zugriff: 07.01.2024.

[14] IMB. 2024. was ist phishing? https://www.ibm.com/de-de/topics/phishing, letzter Zugriff: 07.01.2024.

[15] Davor Kolaric. 2021. Credential Stuffing Report: Immer mehr Diebstahl von Anmeldedaten. https://www.all-about-security.de/credential-stuffing-report-immer-mehr-diebstahl-von-anmeldedaten/, letzter Zugriff: 07.01.2024.

[16] LII / Legal Information Institute. 2023. phishing. https://www.law.cornell.edu/wex/phishing#:~:text=Phishing%20is%20a%20type%20of,via%20email%20or%20URL%20to, letzter Zugriff: 07.01.2024.

[17] Cybersecurity News Redaktion. 2023. Neue Schadsoftware "Stealc" stiehlt Passwörter und Kreditkarteninformationen aus Chrome und. https://www.cybersecurity-news.de/neue-schadsoftware-stealc-stiehlt-passwoerter-und-kreditkarteninforma\tionen-aus-chrome-und-firefox/, letzter Zugriff: 07.01.2024.

[18] Prof. Dr. Andreas Suchanek. 2021. Gabler Wissenschaftslexikon - Definition: Ethik. https://wirtschaftslexikon.gabler.de/definition/ethik-34332.

[19] Daniel Bachfeld Uli Ries. 2012. Android-Smartphones per Drive-by infiziert. https://www.heise.de/news/Android-Smartphones-per-Drive-by-infiziert-1446758.html, letzter Zugriff: 07.01.2024.

[20] Annika Frings und Ayessa Fischer. 2023. android: Ist ein Virenscanner notwendig? https://www.computerbild.de/artikel/cb-Tipps-Handy-Ist-ein-Virenscanner-fuer-Android-notwendig\-31555631.html, letzter Zugriff: 07.01.2024.

[21] David B. Resnik und Peter R. Finn. 2017. Ethics and Phishing Experiments. https://finn.lab.indiana.edu/PDFs/Resnik%20Finn%202017.pdf, letzter Zugriff: 07.01.2024.

[22] Wikipedia. 2023. IBM. https://de.wikipedia.org/w/index.php?title=IBM&oldid=238824210, letzter Zugriff: 07.01.2024.

[23] Gabler Wirtschaftslexikon. 2021. Prof. Dr. Andreas Suchanek • Autor und Experte. https://wirtschaftslexikon.gabler.de/autoren/prof-dr-andreas-suchanek-186.

[24] www.apwg.org. 2023. phishing activity trends report. https://docs.apwg.org/reports/apwg_trends_report_q4_2022.pdf, letzter Zugriff: 07.01.2024.

[25] www.csrc.nist.gov. phishing - Glossary | CSRC. https://csrc.nist.gov/glossary/term/phishing#:~:text=Definitions%3A,legitimate%20business%20or%20reputable%20person., letzter Zugriff: 07.01.2024.

[26] www.impulse.de. 2023. Passwortmanager: Hilfsmittel oder Sicherheitsrisiko? Das können Passwortmanager | impulse. https://www.impulse.de/organisation/passwortmanager/3542110.html, letzter Zugriff: 07.01.2024.

[27] www.impulse.de. Verlag Julius Klinkhardt: Jürg Aeppli / Luciano Gasser / Eveline Gutzwiller / Annette Tettenborn: Empirisches wissenschaftliches Arbeite. https://www.klinkhardt.de/verlagsprogramm/6168.html, letzter Zugriff: 07.01.2024.

[28] Zimperium. 2023. 2023 global mobile threat report - zimperium. `https://www.zimperium.com/global-mobile-threat-report/`, letzter Zugriff: 07.01.2024.

Erklärung

Ich versichere wahrheitsgemäß, die Arbeit selbstständig verfasst, alle benutzten Hilfsmittel vollständig und genau angegeben und alles kenntlich gemacht zu haben, was aus Arbeiten anderer unverändert oder mit Abänderungen entnommen wurde sowie die Satzung des KIT zur Sicherung guter wissenschaftlicher Praxis in der jeweils gültigen Fassung beachtet zu haben.

Karlsruhe, 7. Januar 2024 VORNAME NACHNAME