Phishing still works: Erfahrungen und Lehren aus der Durchführung von Phishing-Experimenten

Nadina Hintz
Friedrich-Alexander-Universität
91058 Erlangen
nadina.hintz@cs.fau.de

Markus Engelberth
Pi-One GbR
64625 Bensheim
markus@pi-one.net

Zinaida Benenson
Friedrich-Alexander-Universität
91058 Erlangen
zinaida.benenson@cs.fau.de

Felix C. Freiling
Friedrich-Alexander-Universität
91058 Erlangen
felix.freiling@cs.fau.deF

Abstract: Wir beschreiben die Durchführung und die Ergebnisse zweier Experimente, bei denen der Einfluss verschiedener Gestaltungsparameter von E-Mails und Webseiten auf den Erfolg von Phishing-Angriffen untersucht wurde. Wir berichten außerdem über unsere Erfahrungen, welche technischen, ethischen und rechtlichen Aspekte beim Design und der Durchführung solcher Experimente beachtet werden müssen.

1 Einführung

Motivation. Das Kunstwort "Phishing" bezeichnet Angriffe, die mittels betrügerischer E-Mails und manipulierter Webseiten durchgeführt werden, indem die Opfer unter einem Vorwand zur Eingabe von Passwörtern, Konto- und Kreditkarteninformationen oder anderen sensiblen Daten aufgefordert werden. Das kriminelle Ziel dieser Angriffe ist, mit den so erlangten Daten Identitätsdiebstahl zu betreiben. Angriffe auf Unternehmen haben häufig unternehmensinterne Daten oder Kundendaten zum Ziel. Phishing kann somit einen erheblichen finanziellen Schaden verursachen oder den Ruf einer Person oder eines Unternehmens nachhaltig schädigen. Laut einer Statistik des Bundeskriminalamts [Bun12] lagen die Schäden, die in Deutschland durch Phishing im Bereich Online-Banking entstanden sind, von 2010 bis 2012 zwischen 13,8 und 25,7 Mio. Euro pro Jahr. In den USA bewegt sich der jährliche Schaden nach unterschiedlichen Einschätzungen zwischen 61 Millionen und 3 Milliarden US-Dollar [Hon12].

Phishing ist ein Kriminalitätsfeld, das auf vielen Ebenen angegangen wird. So arbeiten etwa die Strafverfolgungsbehörden an der Zerschlagung der Phishing-Infrastrukturen wie z.B. Botnetzen. Andere Organisationen, wie etwa die Anti Phishing Working Group (APWG) [APWG13] in den USA haben das Ziel, die Aktivitäten von Behörden und privaten Akteuren besser zu koordinieren. Bekannt sind auch Freiwilligenorganisationen wie PhishTank [Phi13], die Blacklisten mit Webadressen pflegen, an denen sich Phishing-Seiten befinden. In Deutschland befasst sich die Arbeitsgruppe „Identitätsschutz im In-

ternet“ [ai3] mit technischen und rechtlichen Fragen zu Phishing und Identitätsdiebstahl. Es gibt auch eine Vielzahl von technischen Werkzeugen zur Erkennung von Phishing-Angriffen, und auch Internet- und E-Mail-Provider bieten mittlerweile Anti-Phishing-Dienste an. Diese Tools können jedoch bei weitem nicht alle Angriffe erkennen. So untersuchten Zhang et al. [ZECH07] 10 Anti-Phishing-Tools, wovon nur ein Tool 90 % der Phishing-Webseiten korrekt identifizierte und die meisten Tools weniger als 50% der Phishing-Webseiten erkannt haben.

Das mutmaßlich relevanteste Problem im Kontext von Phishing ist jedoch der „Faktor Mensch“. Einerseits sind Anti-Phishing-Tools oft nicht nutzerfreundlich gestaltet, so dass die Personen nicht verstehen, um welches Problem es sich handelt, wo die Gefahr liegt und warum sie z.B. nicht auf einen Link klicken sollten [Hon12]. Deswegen reagieren Opfer in vielen Fällen nicht angemessen auf Warnungen, bemerken sie nicht oder halten diese für ungültig [WMG06]. Andererseits nutzen auch die raffiniertesten technischen Gegenmaßnahmen nichts, wenn Menschen von der Authentizität einer Phishing-Mail überzeugt sind. Hong [Hon12] schreibt hierzu:

> „*It does not matter how many firewalls, encryption software, certificates or two-factor authentication mechanisms an organization has, if the person behind the keyboard falls for a phish.*“

Die Qualität der Manipulation eines Opfers ist somit ein wesentlicher Einflussfaktor auf den Erfolg der Phishing-Angriffe. Da das menschliche Verhalten von verschiedenen Faktoren, wie z.B. der aktuellen Lebenssituation, den gemachten Erfahrungen und der natürlichen Neugier abhängt, ist es besonders schwer, geeignete Schutzmechanismen zu entwickeln.

Forschungsbeitrag. Studien, die den Einflussfaktor bestimmter Aspekte auf den Erfolg von Phishing-Angriffen untersuchten, wurden bisher größtenteils in den USA im universitären Umfeld durchgeführt, die meisten Teilnehmer waren Studierende oder Universitätsmitarbeiter (die verwandten Arbeiten werden in Abschnitt 2 genauer beschrieben). In dieser Arbeit werden zwei Phishing-Experimente vorgestellt, die in Deutschland durchgeführt wurden und sich auch auf das Unternehmensumfeld erstreckten. Aus den Erfahrungen dieser beiden Studien beschreiben wir weiterhin, welche technischen, ethischen und rechtlichen Aspekte beim Design und der Durchführung solcher Experimente eine Rolle spielen, und wie diese Experimente korrekt umgesetzt werden können. Wir möchten damit auch eine Diskussion im deutschsprachigem Raum über die sinnvolle und korrekte Durchführung von Phishing-Experimenten anstoßen.

Das erste Experiment wurde in Zusammenarbeit mit vier deutschen Unternehmen durchgeführt und untersuchte den Einfluss des Absenders (extern oder unternehmensintern), des Inhalts und der Formulierung einer Phishing-Mail und des Designs der entsprechenden Webseite auf den Erfolg der Phishing-Angriffe. Nicht überraschend (aber trotzdem beunruhigend) war das Ergebnis, dass auch eine unpersönlich formulierte E-Mail, die einen Link zu einem (nicht existierenden) reißerischen Artikel enthält, eine Klickrate von mehr als 10% verursacht hat. Durch eine persönliche Ansprache und eine Aufforderung zur Änderung der unternehmensinternen Zugangsdaten wurde die Anfälligkeit für den Angriff fast verdoppelt.

Das zweite Experiment fand an einer deutschen Universität statt und untersuchte die Reaktion der Studierenden auf einen Phishing-Angriff, der absichtlich möglichst „einfach“ gestaltet wurde: keine persönliche Anrede, kein besonders ausgeklügelter Vorwand, und eine leere Webseite, die nur Eingabefelder für Login und Passwort enthält. Überraschenderweise haben auch hier mehr als 10 % der Teilnehmer versucht, ihre Daten einzugeben.

Ausblick. Dieser Artikel ist folgendermaßen organisiert. Im Abschnitt 2 werden verwandte Arbeiten aufgeführt. Im Abschnitt 3 werden die durchgeführten Studien und deren Ergebnisse vorgestellt. Im Abschnitt 4 diskutieren wir wichtige Aspekte bei der Durchführung von Phishing-Studien. Anschließend werden im Abschnitt 5 unsere Ergebnisse zusammengefasst.

2 Verwandte Arbeiten

Einflussfaktoren auf die Anfälligkeit für Phishing-Angriffe. Erste Arbeiten zu psychologischen Einflussfaktoren untersuchten, nach welchen Kriterien die Nutzer Phishing-Angriffe erkennen. Downs et al. [DHC06] analysierten mit Hilfe von Interviews und Rollenspielen, nach welchen Entscheidungskriterien Personen E-Mails als gefährlich einstufen. Dhamija et al. [DTH06] erforschten, welche Strategien die Benutzer einsetzen um zu entscheiden, ob eine Webseite echt oder gefälscht ist. Jakobsson und Ratkiewicz haben sogenannte „context-aware“ Experimente durchgeführt, indem sie öffentlich verfügbare Daten von eBay-Nutzern und die typischen Kommunikationsmuster bei eBay verwendet haben, um die Glaubwürdigkeit der Phishing-Mails zu erhöhen. Jagatic et al. [JJJM07] entnahmen Informationen über soziale Kontakte aus sozialen Netzwerken und haben anschließend eine simulierte Phishing-Mail so dargestellt, als komme sie von einem Bekannten, was den Erfolg der Phishing-Angriffe drastisch verbesserte im Vergleich zu unpersönlich formulierten E-Mails.

Ergebnisse dieser Arbeiten haben gezeigt, dass es den Nutzern schwer fällt, Phishing zu erkennen und dass ihre Entscheidungskriterien nicht angemessen sind. Als Blythe et al. [BPC11] fünf Jahre später ähnliche Untersuchungen durchführten, haben sie herausgefunden, dass sich nicht viel geändert hat. Nach wie vor achten die Benutzer bei E-Mails auf den Absender („wenn ich bei dieser Firma Kunde bin, oder wenn ich den Absender persönlich kenne, dann ist die E-Mail echt“), auf das Design und die Sprache der E-Mails und Webseiten („wenn keine offensichtlichen Sprachfehler auffallen, vertraute Markenzeichen präsent sind und alle Links funktionieren, dann ist die E-Mail oder die Webseite echt“) und haben Schwierigkeiten, technische Details zu interpretieren, wie z.B. den Aufbau der Links oder die Präsenz von „padlock icons“.

Der Einfluss der demographischen Unterschiede (Alter und Geschlecht) auf den Umgang mit Phishing wurde in mehreren Arbeiten gemessen, meistens ebenfalls im universitären Umfeld. Während einige Untersuchungen keine Korrelation zwischen demographischen Faktoren und der Anfälligkeit für Phishing finden konnten [DTH06, SMK+07], haben andere Experimente signifikante Unterschiede festgestellt [JJJM07, SHK+10, BPC11]. So

waren jüngere Personen (18-25 Jahre) anfälliger für Phishing-Attacken, und Frauen waren anfälliger als Männer. Der Einfluss des demographischen Merkmals „Bildung“ wurde dagegen noch nicht ausreichend untersucht.

Die Wirksamkeit von Anti-Phishing Tools und Warnungen wurde in einer Reihe von Arbeiten untersucht. Dhamija et al.[DTH06] fanden heraus, dass die meisten Benutzer die passiven Browser-Hinweise auf die Vertrauenswürdigkeit einer Webseite („security indicators“) nicht beachten und daher viele Phishing-Webseiten als echt einstufen. Egelman et al. [ECH08] haben untersucht, ob aktive und passive Warnungen beim Öffnen einer Phishing-Webseite das Verhalten der Nutzer beeinflusst. 79% der Nutzer haben aktive Warnungen und 13% der Nutzer haben passive Warnungen beachtet. Lin et al. [LGT+11], Kirlappos et al. [KS12] und Li et al. [LHB12] haben die Benutzbarkeit von weiteren Anti-Phishing Maßnahmen getestet. Die Ergebnisse dieser Studien haben gezeigt, dass nur aktive Warnungen zu einer signifikanten Reduktion der Anzahl der Phishing-Opfer führen, wobei die Verständlichkeit der Warnungen und der Indikatoren nicht ausreicht, um die Nutzer bei ihren Entscheidungen ausreichend zu unterstützen.

Benutzerschulungen sind eine weitere Maßnahme zum Schutz gegen Phishing. Die an der CyLab der CMU entwickelten „Anti-Phishing Phil“ [SMK+07] und „PhishGuru“ [KCA+09] sind die am meisten bekannten Systeme zur Unterstützung von Nutzer-Schulungen. In einer vergleichender Untersuchung der beiden Systeme [KSA+10] fanden die Entwickler heraus, dass die beiden Schulungsmaßnahmen die Anzahl der Phishing-Opfer reduziert haben. Allerdings zeigten die Nutzer keine intrinsische Motivation auf, etwas über den sicheren Umgang mit Phishing-Angriffen zu lernen. Wahrscheinlich hängt die Wirksamkeit der Schulungen hochgradig vom Umfeld ab, in dem diese durchgeführt werden.

Ethische Aspekte. Neben allgemeinen Diskussionen zur ethischen Orientierung im Bereich der IT-Sicherheitsforschung [DBD11] gibt es auch Literatur, die sich spezifisch mit der Durchführung von Phishing-Experimenten beschäftigt hat. So beschreiben Jakobsson et al. [JJF08] drei Möglichkeiten, um Phishing-Experimente durchzuführen: (1) mit Hilfe von Umfragen, (2) durch Labor-Experimente oder (3) durch lebensnahe Experimente. Gleichzeitig führen die Autoren auch die Vor- und Nachteile dieser Möglichkeiten auf. Die Autoren argumentieren, dass lebensnahe Experimente trotz der ethischen Nachteile die beste Möglichkeit bieten, das reale Verhalten von Personen zu messen. Nur so könnten neue Erkenntnissen erzielt werden, welche Entwicklern helfen, die Maßnahmen gegen Phishing zu verbessern. Als Beispiel für ethisch korrekt durchgeführte Experimente nennen sie ihre eigenen Arbeiten [JR06, JJJM07].

Schrittweiser et al. [SMW13] stellen diese Art von Studiendesign in Frage und kritisieren das ethische Vorgehen einiger Forscher, u.a. Jagatic et al. [JJJM07], bei der Durchführung von Phishing-Studien. Die Autoren führen auf, dass die Forscher gewährleisten müssen, dass die Probanden durch die Studiendurchführung keinen Schaden nehmen und dass die Forscher sich bewusst sein sollten, dass ihre Forschungsergebnisse von Kriminellen missbraucht werden könnten. Sie diskutieren grundlegende ethische Prinzipien der Forschung und schlagen vor, dass die wissenschaftliche Gemeinschaft der IT-Sicherheitsforscher ethisch verpflichtende Standards entwickelt, vergleichbar mit denen in der Medizin.

3 Durchgeführte Studien

Wir stellen zwei Phishing-Studien vor. Die erste Studie wurde in vier deutschen Unternehmen durchgeführt mit dem Ziel, den Grad der Sensibilisierung der Mitarbeiter zu messen. Die zweite Studie fand an einer deutschen Universität statt. In beiden Studien wurden einige Faktoren gemessen, die die Anfälligkeit für Phishing beeinflussen. Nachdem der Aufbau und die Ergebnisse der Studien in diesem Abschnitt vorgestellt werden, diskutieren wir im Abschnitt 4 wichtige Aspekte der Durchführung der Phishing-Studien anhand unserer Erfahrungen.

3.1 Studie 1: Phishing-Experimente im Unternehmensumfeld

3.1.1 Aufbau der Studie 1

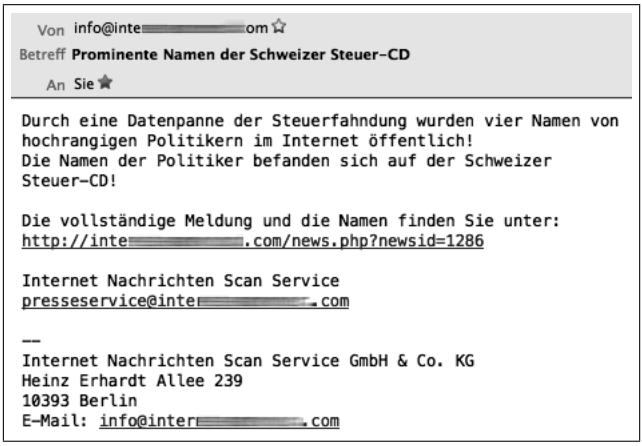
In Zusammenarbeit mit einem Unternehmen aus der IT-Sicherheitsbranche haben wir über einen Zeitraum von einem Jahr eine experimentelle Studie durchgeführt mit dem Ziel, die Reaktionen der Mitarbeiter deutscher Unternehmen auf den Erhalt von Spam- und Phishing-Mails zu messen. Nach umfangreicher Teilnehmerakquise haben sich vier Unternehmen, die zum Zeitpunkt der Studie zwischen 103 und 425 Mitarbeiter beschäftigten, dazu bereit erklärt, an dieser Studie teilzunehmen.

Die Motivation der teilnehmenden Unternehmen bestand darin, quantitative Informationen über das Sicherheitsbewusstsein ihrer Mitarbeiter zu erhalten. Nach Abschluss der Studie haben wir den teilnehmenden Unternehmen jeweils einen Abschlussbericht vorgelegt. Alle Unternehmen haben die Abschlussberichte genutzt, um ihren Mitarbeitern in Form von Vorträgen die Ergebnisse zu präsentieren. Vor Durchführung der Studie haben wir mit allen beteiligten Unternehmen die geplanten Spam- und Phishing-Mails abgesprochen und die jeweiligen Systemadministratoren über die Durchführung der Studie informiert.

Im Rahmen der Experimente wurden zwei Arten von E-Mails versandt. Die erste E-Mail war eine klassische Spam-Mail mit einem Verweis auf eine externe Internetseite. Anhand der Spam-Mail lässt sich die Rate der Empfänger ermitteln, die bereits dem Verweis einer unpersönlichen, reinen Spam-Mail folgen. Dies ist deshalb ein hochinteressanter Wert, da das Anklicken eines Links das initiale und notwendige Ereignis eines erfolgreichen Phishing-Betrugs darstellt. Die zweite E-Mail war personalisiert, d. h. die Empfänger wurden namentlich angesprochen. Zudem war sie stark auf das jeweilige Unternehmen zugeschnitten, so dass sie das andere Ende des Spektrums möglicher Phishing-Angriffe darstellt: so genanntes *Spear-Phishing*. Nachfolgend werden die beiden verwendeten E-Mail-Arten detailliert beschrieben.

E-Mail 1: Spam mit einem Verweis auf eine Internetseite. Die E-Mails enthielten einen Verweis, der auf eine von uns erstellte Webseite führte. Die E-Mails waren nicht personalisiert, d. h. die Empfänger wurden nicht namentlich angesprochen. Der Inhalt der E-Mails war jeweils an ein aktuelles Ereignis angelehnt, das zum Zeitpunkt des E-Mail-

Versands in den Medien diskutiert wurde. Somit sollte ein möglichst großer Empfängerkreis angesprochen werden. Ein Beispiel einer solchen E-Mail befindet sich in Abbildung 1. In unserer Studie führte der Verweis zu einer harmlosen Webseite, die den HTTP-Fehler 504 (Gateway Timeout) nachahmte. Die Verweise in den E-Mails enthielten alle eine anonyme Benutzer-ID (in dem Beispiel der Abbildung als News-ID getarnt), so dass wir die Klicks einzelner Empfänger unterscheiden konnten. Als Absender haben wir eine erfundene Internet-Nachrichtenagentur verwendet.


Von info@inte[redacted]om
Betreff **Prominente Namen der Schweizer Steuer-CD**
An Sie

Durch eine Datenpanne der Steuerfahndung wurden vier Namen von hochrangigen Politikern im Internet öffentlich!
Die Namen der Politiker befanden sich auf der Schweizer Steuer-CD!

Die vollständige Meldung und die Namen finden Sie unter:
http://inte[redacted].com/news.php?newsid=1286

Internet Nachrichten Scan Service
presseservice@inte[redacted].com

--
Internet Nachrichten Scan Service GmbH & Co. KG
Heinz Erhardt Allee 239
10393 Berlin
E-Mail: info@inter[redacted].com

Abbildung 1: Beispiel einer klassischen Spam-Mail, die im Rahmen der Studie 1 verschickt wurde.

Mail 2: Phishing-Mail zur Änderung eines internen Passworts. In den von uns versandten Phishing-Mails wurden die Empfänger dazu aufgefordert, aus Sicherheitsgründen ihre firmeninternen Zugangsdaten zu ändern. Um die Glaubwürdigkeit dieser Aufforderungen zu erhöhen, wurde als Absenderadresse die E-Mail-Adresse des Mitarbeiters des Unternehmens verwendet, der für solche administrativen Aufgaben zuständig ist. Die Empfänger der Nachrichten wurden mit Nachnamen angesprochen. In den Phishing-Mails war ein Verweis enthalten, der zu einer von uns erstellten Webseite führte, auf der die Mitarbeiter ihr altes und ein neues Passwort eingeben konnten. Solch eine Seite ist exemplarisch in Abbildung 2 dargestellt. Dabei wurde eine unternehmensfremde Domain verwendet. Um die Glaubwürdigkeit der Verweise zu erhöhen, haben wir der Domain Subdomains vorangestellt, die an den Namen des entsprechenden Kunden angelehnt waren – um dadurch wiederum die Glaubwürdigkeit der gesamten E-Mail zu erhöhen.

Die von uns erstellten Internetseiten wurden allesamt auf Servern des IT-Sicherheits-Unternehmens gehostet, mit dem wir in Kooperation die Studie durchgeführt haben. Von den Eingaben auf den „Phishing“-Seiten haben wir neben den Benutzernamen, Zeitstempeln und Benutzer-IDs auch gesalzene Hashwerte der eingegebenen Passwörter gespeichert. Auf diese Weise konnten wir Kennwörter voneinander unterscheiden ohne diese im Klartext zu kennen. Durch das Salz wird zudem verhindert, dass man durch einen Brute-Force-Angriff an zu kurze Passwörter im Klartext kommt. Auch die Kommunikation zwischen

Abbildung 2: Beispiel einer von uns erstellten Phishing-Seite, die im Rahmen der Studie 1 für einen der vier Kunden verwendet wurde.

Phishing-Seite und Webbrowser war durch die Verwendung eines Server-Zertifikats verschlüsselt, so dass auch hier die Passwörter nicht im Klartext übertragen wurden.

Alle von uns aufgezeichneten Daten haben wir nach der Übergabe der anonymisierten Auswertung der Ergebnisse wieder gelöscht. Die teilnehmenden Unternehmen hatten keinen Zugriff auf Rohdaten.

3.1.2 Ergebnisse der Studie 1

Die von uns durchgeführten Experimente haben gezeigt, dass wir „bessere“ Ergebnisse erzielen konnten, je glaubwürdiger wir die Phishing- und Spam-Mails gestaltet haben. Das Spoofen der Absenderadresse und das Erstellen einer „Phishing“-Seite, die optisch fast identisch zur Originalseite ist, haben einen erheblichen Einfluss auf die erzielten Ergebnisse. Während bei der ersten E-Mail nur ca. 12 % der Empfänger dem Verweis innerhalb der Spam-Mail gefolgt sind, hätten wir bei der zweiten E-Mailart von fast 20 % der Empfänger eingegebene Passwörter aufzeichnen können. Jeweils innerhalb der ersten 2 Stunden nach Mail-Versand konnten die meisten Klicks registriert werden, und nach durchschnittlich 5,83 Tagen wurden 90 % aller Reaktionen aufgezeichnet. Tabelle 1 fasst die Ergebnisse der Studie zusammen.

3.2 Studie 2: Phishing unter Universitätsstudenten

Eine zweite Studie wurde an einer deutschen Universität durchgeführt mit dem Ziel herauszufinden, ob die Teilnehmer einem Link folgen, der auf eine offensichtlich gefälschte Webseite führt und dort ihre Zugangsdaten eingeben. Bei Studie 2 war die „Phishing“-Webseite nicht aufwendig gestaltet. Es war lediglich eine leere Webseite mit zwei Eingabefeldern für den Nutzernamen und das Passwort. Die Empfänger wurden bei dieser E-Mail nicht mit Namen angesprochen.

		Mail 1	**Mail 2**
Unternehmen	Anzahl der Mitarbeiter	Dem Verweis der Spam-Mail gefolgt	Eingaben auf „Phishing"-Webseite gemacht
1	186	15 *(8,06 %)*	24 *(12,90 %)*
2	425	65 *(15,29 %)*	84 *(19,76 %)*
3	112	7 *(6,25 %)*	28 *(25,00 %)*
4	103	11 *(10,68 %)*	25 *(24,27 %)*
Gesamt	826	98 *(11,86 %)*	161 *(19,49 %)*

Tabelle 1: Übersicht über die Ergebnisse der Experimente in Unternehmen. Hinter den absoluten Zahlen ist jeweils der Prozentanteil der Mitarbeiter des jeweiligen Unternehmens angegeben, von dem wir eine Reaktion aufzeichnen konnten.

Als Absender der E-Mail fungierte der Paketlieferservice Hermes mit der Domain *no-reply@hermes-support.de* (die eigentliche Domain von Hermes heißt *myhermes.de*). Den Empfängern wurde mitgeteilt, dass ein Paket nicht zugestellt werden konnte und dass sie sich für eine erneute Zulieferung unter dem beigefügten Link auf der Webseite anmelden müssen. Jedem Link wurde wie bei Studie 1 ein individualisierter Hashwert beigefügt, so dass wir Klicks unterschiedlicher Empfänger unterscheiden konnten. Wir haben gespeichert, wie oft die Probanden auf den Link geklickt haben und, falls sie ihre Zugangsdaten eingegeben haben, wie oft sie dies wiederholt getan haben. Falls die Probanden versucht haben, ihre Daten einzugeben, haben sie eine Fehlermeldung angezeigt bekommen.

Für die Studie wurden 919 Studenten über einen E-Mail-Verteiler rekrutiert. Um die Studenten in ihrem Verhalten nicht zu beeinflussen, haben wir ihnen zunächst mitgeteilt, die Studie behandle das Thema „Nutzerverhalten im Internet". Insgesamt sind 50 % aller Studienteilnehmer dem Link in der Hermes E-Mail gefolgt und 11 % haben ihre Nutzerinformationen eingegeben. 29 % aller Empfänger haben mehrfach auf den Link geklickt und einige haben ihre Nutzerdaten erneut angegeben, obwohl die erste Eingabe nicht funktionierte. Genau wie bei Studie 1 konnten die meisten Klicks innerhalb der ersten 2 Stunden gemessen werden. Tabelle 2 fasst die Ergebnisse der Studie zusammen.

Teilnehmer	Anzahl der Teilnehmer	Dem Verweis auf Hermes gefolgt	Nutzerdaten eingegeben	Mehrfach auf Link geklickt
Frauen	596	375 *(62,92 %)*	69 *(11,58 %)*	223 *(37,42 %)*
Männer	323	85 *(26,32 %)*	34 *(10,53 %)*	46 *(14,24 %)*
Gesamt	919	460 *(50,05 %)*	103 *(11,21 %)*	269 *(29,27 %)*

Tabelle 2: Übersicht über die Ergebnisse des Experiments an der Universität. Hinter den absoluten Zahlen ist jeweils der Prozentanteil der Teilnehmer angegeben, von dem wir eine Reaktion aufzeichnen konnten.

3.3 Zusammenfassung der Ergebnisse

Die Ergebnisse beider Studien belegen erneut: *Phishing still works.* Insgesamt haben die Angestellten von Unternehmen und die Studierenden ähnliche Anfälligkeitsrate und Reaktionszeit aufgewiesen. Auf „einfachere“ Phishing-Versuche haben ca. 10 % der Empfänger reagiert, und der Großteil der Reaktionen konnte innerhalb der ersten beiden Stunden gemessen werden. Die meisten im Abschnitt 2 angeführten Arbeiten kamen zu ähnlichen Ergebnissen.

Dies bedeutet für den Angreifer, falls seine Webseite nach einiger Zeit geblacklistet wird, dass er in den ersten zwei Stunden bereits eine große Erfolgschance hat, denn laut den Angaben des Phishing-Blacklistenbetreibers PhishTank [Phi13] brauchte dieser im Jahr 2012 im Mittel 2 Stunden und 54 Minuten, um eine Webseite als bösartig zu identifizieren.

4 Lehren aus der Durchführung unserer Experimente

Wir sind bei der Durchführung unserer Experimente auf vielfältige Probleme gestoßen. Einige davon waren erwartet worden, andere waren unerwartet. In diesem Abschnitt beschreiben wir einige Lehren, die wir dokumentieren und weitergeben wollen.

4.1 Nutzen der Phishing-Experimente

Insbesondere ökonomische Anreize können hier eine Rolle spielen: Die Aufwendungen (sowohl monetärer als auch zeitlicher und organisatorischer Art), die aufgrund der Durchführung der Experimente entstehen, fallen in der Regel wesentlich geringer aus als Folgeschäden, die ein Phishing-Betrug innerhalb der Belegschaft nach sich ziehen würde.

Spätestens wenn in einer Organisation nach einem solchen Experiment das Fehlen eines klar definierten Vorgehens bei Phishing-Angriffen bewusst wird (wie kann man diese Angriffe erkennen, was tun beim Verdacht auf einen Angriff, wer und wie warnt die Mitarbeiter), wird der Nutzen dieser Experimente klar erkennbar.

4.2 Kommunikation mit beteiligten Institutionen

Es gibt viele verschiedene Institutionen, die von der Durchführung einer Phishing-Studie betroffen sind. Zuvorderst ist natürlich die Organisation zu nennen, deren Mitglieder die Zielgruppe des Experiments sind. Meist ist dies der Auftraggeber der Studie, aber auch unabhängig davon ist es notwendig, dass diese Organisation mit der Durchführung einverstanden ist. Eine andere betroffene Institution ist diejenige, in deren Namen die Phishing-Mails versendet werden. Dies kann der Auftraggeber sein oder nicht. Schließlich ist diejenige Institution noch betroffen, über die die Phishing-Mails verschickt werden bzw. die die

Phishing-Seite auf ihren Servern vorhält. Dies kann ebenfalls der Auftraggeber sein aber auch eine davon unabhängige Organisation (z.B. ein anderer E-Mail-Provider). Inwiefern diese Institutionen in die Kommunikation eingebunden werden können oder sollten, wird weiter unten diskutiert.

Mit den entsprechenden Institutionen sollten die notwendigen Fragen zum Schutz personenbezogener Daten geklärt werden, also welche Daten für welchen Zeitraum erhoben und gespeichert werden. Dies sollte Teil einer ausführlichen Studiendokumentation sein, die mit der betroffenen Institution abgestimmt werden muss. Aus der Beschreibung der Studie sollte hervorgehen, welche Daten gespeichert werden, ob personenbezogene Daten gespeichert werden, wo diese Daten gespeichert und wann sie wieder gelöscht werden, von welchem Netzwerk aus und unter welchem Absender E-Mails versandt werden und was der Inhalt der Nachrichten sein wird.

Unserer Erfahrung nach kommt es im Rahmen von Phishing-Experimenten fast immer zu Situationen, in denen Mitarbeiter vermehrt eine zuständige Person oder Abteilung auf die Geschehnisse aufmerksam machen. Deshalb sollten also insbesondere alle Institutionen darüber informiert werden, wann die Nachrichten versandt werden, damit ggf. eine erhöhte Anzahl an Beschwerden oder Warnhinweisen der Studienteilnehmer entgegengenommen werden kann. Ebenfalls haben wir erlebt, dass ein aufmerksamer Abteilungsleiter etliche Mitglieder seiner Abteilung vor dem Öffnen unserer E-Mail gewarnt hat.

Bei Studien an Universitäten sollten das Rechenzentrum, der/die Datenschutzbeauftragte, die Ethikkommission (falls vorhanden) und das HelpDesk über die Durchführung informiert sein und dieser zustimmen. Bei Studien an Unternehmen sollten der Geschäftsführer, der Betriebsrat, die IT-Revision und/oder die zuständigen Systemadministratoren über die Durchführung informiert sein und dieser zustimmen.

Schließlich sind noch die eigentlichen Teilnehmer der Studie in die Betrachtungen mit einzubeziehen. Eine explizite Information dieser Personen über den Sinn und Zweck der durchgeführten Experimente ist natürlich nicht sinnvoll, da sie dem Zweck der Studie widerspricht. Trotzdem sollte in irgend einer Form eine Art Einverständnis dieser Personengruppe herbeigeführt werden, präferiert entweder indirekt über den Vorgesetzten (die beauftragende Organisation) oder durch eine allgemeine Zustimmung zu einem “Experiment zur Internetnutzung”. Wir sind uns bewusst, das letzteres ethische Schwierigkeiten mit sich bringt. Dies sind jedoch dieselben Schwierigkeiten, mit denen auch viele Experimente im Bereich der Psychologie behaftet sind.

Alle Studienteilnehmer sollten jedoch *nach* Durchführung der Studie über diese vollständig aufgeklärt werden. Allen betroffenen Institutionen sollte ein Abschlussbericht mit den Ergebnissen vorgelegt werden. Der Zeitpunkt der Aufklärung sollte bereits vor Durchführung der Studie feststehen. In welcher Form die Studienteilnehmer über die Durchführung der Studie informiert werden, sollte in jeder Institution individuell festgelegt werden (z.B. per E-Mail oder in einem Vortrag). Aus der Aufklärung sollten das Ziel und der Zweck sowie ein eindeutiger Ansprechpartner hervorgehen, damit Studienteilnehmer die Möglichkeit haben, weitere Fragen zu klären oder Feedback zu geben.

4.3 Technische Aspekte

Phishing-Studien sind nicht nur organisatorisch, sondern auch technisch eine Herausforderung. Viele Institutionen wie Universitäten und Unternehmen haben technische Maßnahmen (Spamfilter, automatische Entfernung von Anhängen), um den Eingang von Phishing-Mails zu verhindern. Diese technischen Maßnahmen sollten im Zuge dieser Studie nicht abgeschaltet werden. Es muss jedoch auch gewährleistet sein, dass die Phishing-Mails, die Teil der Studie sind, auch zuverlässig ihre Adressaten erreichen. Vor der Umsetzung einer Studie sollten die Phishing-Mails also an unabhängigen Personen getestet werden, damit eventuell auftretende Probleme frühzeitig erkannt werden.

Eine besondere technische Herausforderung stellt der Umgang mit Passwörtern dar, die von den Teilnehmern eventuell eingegeben werden. Entweder sollen diese überhaupt weder übertragen noch gespeichert werden oder, falls der Studienzweck dies erfordert, unbedingt verschlüsselt übertragen, als gesalzener Hashwert gespeichert und so schnell wie möglich gelöscht werden. Der Zeitpunkt der Löschung soll schon vor Beginn der Studie feststehen.

Eine andere Möglichkeit zum Umgang mit Passwörtern besteht, wenn die Experiment-Teilnehmer, die auf den Link in der simulierten Phishing-Mail klicken, zur echten Webseite umgeleitet werden und dort ihre Daten eingeben [JR06, JJJM07]. Das ist allerdings nur dann möglich, wenn die Eingabe der Login-Daten auf der echten Webseite registriert und von „normalen“ Login-Vorgängen unterschieden werden kann.

4.4 Rechtliche Aspekte

Die rechtliche Würdigung von Phishing-Experimenten kann in einem Beitrag wie diesem nicht abschließend behandelt werden. Wir können hier nur mögliche Problemfelder anreißen und Argumente sammeln, die in zukünftigen Diskussionen noch vertieft werden müssen.

Aus strafrechtlicher Sicht kann man beim Versand von Phishing-Mails die Täuschung durch den gefälschten Absender unter § 269 Abs. 1 StGB (Fälschung beweiserheblicher Daten) fassen. Weidemann schreibt dazu:

> Beim Versenden von “Phishing-E-Mails” ist dies ebenfalls der Fall, weil die E-Mail nach dem Absenden jedenfalls beim Empfänger nach dem Aufrufen gespeichert und dem Empfänger vorgetäuscht wird, es handele sich bspw. um eine E-Mail eines Vertragspartners. [Wei10b, Rdn. 9 m.w.N.]

Allerdings schränkt die Norm den Tatbestand derart ein, dass er „zur Täuschung im Rechtsverkehr“ ausgeübt werden muss. Rechtlich bedeutet das, dass er „auf die Herbeiführung eines Irrtums bei dem Getäuschten sowie die Veranlassung des Getäuschten zu einem rechtserheblichen Handeln“ [Wei10a, Rdn. 29] gerichtet sein muss. [Erb03, Rdn. 205] führt dazu aus:

> Nicht rechtserheblich ist ein Sachverhalt dann, wenn im Einzelfall (selbst bei Aufdeckung der Täuschung) sicher auszuschließen ist, dass der Getäuschte ein Verhalten an den Tag legen wird, das über eine Reaktion im zwischenmenschlichen Bereich hinaus die Erfüllung einer (vermeintlichen) Rechtspflicht oder die Einforderung eines (vermeintlichen) Rechts beinhaltet.

Da es nicht unsere Absicht ist, dass die Probanden rechtserheblich handeln (und wir dies auch durch geeignete technische Maßnahmen ausschließen), erscheint § 269 StGB nicht einschlägig. Andere strafrechtliche Vorschriften der Computerkriminalität, etwa §§ 202a–202c oder 303a–303b, sind auf diesen Sachverhalt ebenfalls nicht anwendbar, es sei denn, Passwörter werden tatsächlich im Klartext ausgespäht und abgespeichert. Dies muss durch technische Vorkehrungen wie eine verschlüsselte Verbindung für die Kommunikation sowie Speicherung gesalzener Passwort-Hashes soweit wie irgend möglich ausgeschlossen werden.

Der Bereich des Zivilrechts erscheint hier ergiebiger. Beispielsweise könnte die Organisation, in dessen Namen E-Mails verschickt werden, die Verletzung des Namensrechts (§ 12 BGB) geltend machen. Auch müssen die AGBs oder Benutzerrichtlinien der Organisation, über die die E-Mails versendet werden und bei der die Phishing-Seite vorgehalten wird, beachtet werden. Auf die Datenschutzrisiken sind wir weiter oben bereits eingegangen. Ohne die Zustimmung der Betroffenen könnte der Versand von Phishing-Mails in all diesen Fällen zu Abmahnungen und/oder Unterlassungserklärungen führen. Da man in der Praxis von Firmen wie Facebook oder Hermes wohl kaum eine offizielle Zustimmung erhalten wird, muss dieses Risiko in Betracht gezogen und durch einen begrenzten Adressatenkreis, dem Hinweis auf die Umstände der Forschung usw. minimiert werden.

Trotz all dieser Vorkehrungen kann es passieren, dass die Studienteilnehmer durch die Studie zu Schaden kommen. Einem Studienteilnehmer waren beispielsweise durch eine Phishing-Mail dadurch Kosten entstanden, dass er einen Computerspezialisten aufgesucht hatte aus Angst, sein Computer sei mit Schadsoftware infiziert. Dem kann beispielsweise durch unmittelbare Aufklärung im Anschluss an das Experiment vorgebeugt werden.

4.5 Ethische Aspekte

Die Durchführung solcher Experimente trifft insbesondere im Unternehmensumfeld auf starke ethische Vorbehalte, wobei diese Vorbehalte auch für die Durchführung der Phishing-Experimente in anderen Umgebungen gelten. Bedenken bestehen beispielsweise dagegen, dass einzelne Mitarbeiter durch die Experimente bloßgestellt werden könnten.

Bedenklich könnte auch die Tatsache sein, dass sich Mitarbeiter einer Firma überwacht fühlen könnten, wenn die Firmenleitung entsprechenden Experimenten zustimmt. Diese Bedenken können wir natürlich nicht komplett ausräumen, denn es ist schwer vorauszusagen, was die Mitarbeiter fühlen, wenn sie über die Studie aufgeklärt werden. Durch die anonymen Benutzer-IDs war jedoch bereits sichergestellt, dass kein einzelner Mitarbeiter denunziert werden kann. Zudem haben wir mit den Unternehmen abgesprochen, dass sie ihre Mitarbeiter nach der Studie über diese selbst aufklären, um Transparenz zu schaffen.

Einerseits kann man zwar leider nicht ausschließen, dass sich die Mitarbeiter trotzdem „ertappt“ gefühlt haben. Andererseits haben die Unternehmen mit der Durchführung der Studie eine gute Möglichkeit, die Mitarbeiter zu sensibilisieren, denn der Schulungseffekt einer solchen Maßnahme kann als besser eingestuft werden als der Effekt einer theoretischen Belehrung. Außerdem könnte man argumentieren, dass auch für einen Mitarbeiter die Folgen eines Fehlers bei einem simulierten Angriff viel harmloser sind, und die Mitarbeiter durch die nach dem Experiment folgende Aufklärung vor Anfälligkeit für echte Angriffe geschützt werden.

Wichtig ist auf jeden Fall, dass durch die Phishing-Experimente und andere Betrugsexperimente keine Atmosphäre des allgemeinen Misstrauens in der Organisation entsteht. Dieser Punkt, genauso wie die Auswirkungen der Aufklärung über die Experimente auf einzelne Teilnehmer, wurde bisher nicht untersucht und bedarf nach unserer Meinung einer erhöhten Aufmerksamkeit.

5 Fazit und Ausblick

Unsere Ergebnisse haben gezeigt, dass nach wie vor eine viel zu hohe Anzahl an Personen Opfer von Phishing-Angriffen werden. Über die Hintergründe dieses Phänomens, d.h. welche Einflussfaktoren dazu führen, dass Personen einer Phishing-Mail oder einer Phishing-Webseite vertrauen schenken, sind sich die Forscher derzeit noch uneinig, wie in dem Kapitel 2 „Verwandte Arbeiten“ dargestellt. Aus diesem Grund ist es wichtig, auf diesem Gebiet weiter zu forschen um Wege zu finden, die Anzahl der Opfer und der Angriffe nachhaltig zu reduzieren.

Da es wahrscheinlich auch zukünftig Untersuchungen auf diesem Gebiet geben wird, ist es umso wichtiger, von den Erfahrungen der vergangenen Studien profitieren zu können. Aus diesem Grund haben wir in dieser Arbeit von unseren Erfahrungen berichtet und verschiedene Aspekte erläutert, die bei der Umsetzung solcher Studien berücksichtigt werden sollten. Wir hoffen, dass wir mit dieser Arbeit einen ersten Schritt zur Erstellung eines Grundgerüstes solcher Studien gemacht haben und unsere Forschungsergebnisse und Erfahrungen durch zukünftige Forscher ergänzt werden.

Danksagungen

Wir danken Dominik Brodowski für hilfreiche Diskussion zu den rechtlichen Aspekten von Phishing-Experimenten.

Diese Arbeit wurde unterstützt durch das Bundesministerium für Bildung und Forschung im Rahmen des Forschungsverbunds open C3S (www.open-c3s.de) und durch das Bayerische Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst im Rahmen des Forschungsverbunds ForSEC (www.bayforsec.de).

Literatur

[ai3] Arbeitsgruppe Identitsschutz im Internet e.V. (a-i3). Available online at https://www.a-i3.org/; visited on November 25th 2013.

[APWG13] Inc. Anti-Phishing Working Group. Anti Phishing Working Group (APWG). Website, 2013. Available online at http://www.antiphishing.org; visited on November 25th 2013.

[BPC11] Mark Blythe, Helen Petrie und John A. Clark. F for Fake: Four Studies on How We Fall for Phish. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, Seiten 3469–3478, 2011.

[Bun12] Bundeskriminalamt. Bundeslagebild Cybercrime 2012. *Lagebilder Cybercrime*, Seite 7, 2012.

[DBD11] David Dittrich, Michael Bailey und Sven Dietrich. Building an Active Computer Security Ethics Community. *IEEE Security & Privacy*, 9(4):32–40, 2011.

[DHC06] Julie S. Downs, Mandy B. Holbrook und Lorrie Faith Cranor. Decision Strategies and Susceptibility to Phishing. In *Proceedings of the Second Symposium on Usable Privacy and Security*, SOUPS '06, Seiten 79–90, New York, NY, USA, 2006. ACM.

[DTH06] Rachna Dhamija, J. D. Tygar und Marti Hearst. Why Phishing Works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06, Seiten 581–590, New York, NY, USA, 2006. ACM.

[ECH08] Serge Egelman, Lorrie Faith Cranor und Jason Hong. You'Ve Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '08, Seiten 1065–1074, 2008.

[Erb03] Volker Erb. *Münchener Kommentar zum StGB*, Kapitel §269. Beck, 2003.

[Hon12] Jason Hong. The State of Phishing Attacks. *Commun. ACM*, 55(1):74–81, Januar 2012.

[JJF08] Markus Jakobsson, Nathaniel Johnson und Peter Finn. Why and How to Perform Fraud Experiments. *IEEE Security and Privacy*, 6(2):66–68, Marz 2008.

[JJJM07] Tom N. Jagatic, Nathaniel A. Johnson, Markus Jakobsson und Filippo Menczer. Social Phishing. *Commun. ACM*, 50(10):94–100, Oktober 2007.

[JR06] Markus Jakobsson und Jacob Ratkiewicz. Designing Ethical Phishing Experiments: A Study of (ROT13) rOnl Query Features. In *Proceedings of the 15th International Conference on World Wide Web*, WWW '06, Seiten 513–522, New York, NY, USA, 2006. ACM.

[KCA+09] Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair und Theodore Pham. School of Phish: A Real-world Evaluation of Anti-phishing Training. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, SOUPS '09, Seiten 3:1–3:12, New York, NY, USA, 2009. ACM.

[KS12] Iacovos Kirlappos und Martina Angela Sasse. Security Education against Phishing: A Modest Proposal for a Major Rethink. *Security & Privacy, IEEE*, 10(2):24–32, 2012.

[KSA+10] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor und Jason Hong. Teaching Johnny Not to Fall for Phish. *ACM Trans. Internet Technol.*, 10(2):7:1–7:31, Juni 2010.

[LGT+11] Eric Lin, Saul Greenberg, Eileah Trotter, David Ma und John Aycock. Does Domain Highlighting Help People Identify Phishing Sites? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, Seiten 2075–2084, 2011.

[LHB12] Linfeng Li, Marko Helenius und Eleni Berki. A Usability Test of Whitelist and Blacklist-based Anti-phishing Application. In *Proceeding of the 16th International Academic MindTrek Conference*, MindTrek '12, Seiten 195–202, 2012.

[Phi13] PhisTank. PhishTank: Out of the Net, into the Tank! Website, 2013. Available online at https://www.phishtank.com; visited on November 25th 2013.

[SHK+10] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor und Julie Downs. Who Falls for Phish?: A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, Seiten 373–382, New York, NY, USA, 2010. ACM.

[SMK+07] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong und Elizabeth Nunge. Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, SOUPS '07, Seiten 88–99, New York, NY, USA, 2007. ACM.

[SMW13] Sebastian Schrittweiser, Martin Mulanzzani und Edgar Weippl. Ethics in Security Research Which Lines Should Not Be Crossed? Cyber-security Ethics Dialog & Strategy Workshop (CREDS 2013), 2013.

[Wei10a] Weidemann. §267. Beck'scher Online Kommentar zum StGB, 2010.

[Wei10b] Weidemann. §269. Beck'scher Online Kommentar zum StGB, 2010.

[WMG06] Min Wu, Robert C. Miller und Simson L. Garfinkel. Do Security Toolbars Actually Prevent Phishing Attacks? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06, Seiten 601–610, New York, NY, USA, 2006. ACM.

[ZECH07] Yue Zhang, Serge Egelman, Lorrie Cranor und Jason Hong. Phinding phish: Evaluating anti-phishing tools. In *In Proceedings of the 14th Annual Network and Distributed System Security Symposium (NDSS 2007*, 2007.