Zur Wirksamkeit von Security-Awareness-Maßnahmen

Giulio Schembre · Andreas Heinemann

Hochschule Darmstadt
Fachbereich Informatik
schembre.hda@gmail.com
andreas.heinemann@h-da.de

Zusammenfassung

Im Rahmen einer elfwöchigen Studie bei einem mittelständigen Unternehmen wurde untersucht, ob das Investment in ein Präsenztraining zur Verbesserung der Security Awareness mit Fokus auf E-Mail-Phishing-Angriffe lohnenswert ist. Das erstellte Präsenztraining wird mit kostengünstig erwerbbaren Online-Lernspielen verglichen. Die Auswertung der Daten zeigt, dass beide Maßnahmen sich positiv auf das Verhalten der Mitarbeiter auswirken, jedoch die Verbesserungen durch das Präsenztraining überwiegen. Hierbei ist auffällig, dass bei einer freiwilligen Teilnahme die Motivation, eigenständig ein Online-Lernspiel zu absolvieren, sehr gering ist. Bemerkenswert ist ebenfalls, dass allein das Versenden von fingierten Phishing-E-Mails zu einer Sensibilisierung der Mitarbeiter führt.

1 Einführung und Motivation

Bei der Betrachtung von IT-Sicherheit im Unternehmen spielt neben technischen Maßnahmen (z.B. Firewalls, Virenschutz etc.) die Sensibilisierung des Personals eine wichtige Rolle, insbesondere da Phishing-Angriffe (z.B. in Form von E-Mails) weit verbreitet sind und eine ernst zu nehmende Bedrohung darstellen, vgl. [Cerm14], [Reut17], [Bund16], [Jesc16]. Wie präsent die Bedrohungslage ist, verdeutlicht die Cyber-Sicherheits-Umfrage des Bundesamtes für Sicherheit in der Informationstechnik. In der Umfrage geben 65,5% der Unternehmen an, bereits Ziel eines Cyber-Angriffs geworden zu sein, vgl. [BSI17]. Besonders Social-Engineering-Angriffe, welche u.a. auf die Leichtgläubigkeit des Nutzers abzielen [Kevi06], stellen Unternehmen vor die Herausforderung ihr Personal entsprechend auszubilden, damit solche Angriffe ins Leere laufen. Hier setzen sogenannte Security-Awareness-Maßnahmen an, die ein Zusammenspiel aus Wissen, Können und Wollen in Bezug auf IT-sicherheitsrelevante Aspekte schulen.

Unternehmen stehen vor der Aufgabe für ihr Personal geeignete Security-Awareness-Maßnahmen auszuwählen und umzusetzen. Das in dieser Arbeit im Fokus stehende mittelständische Unternehmen hat ein Präsenztraining zur Verbesserung der Security Awareness seiner Mitarbeiter erarbeitet. Im Rahmen einer empirischen Studie wird die Wirksamkeit dieser ressourcenintensiven Maßnahme untersucht und mit einem Online-Lernspiel als kostengünstigere Alternative verglichen. Die Studie untersucht vor allem, ob die Gefahr durch Phishing-Angriffe in Form von E-Mails gelindert werden kann.

Diese Arbeit ist im Weiteren wie folgt strukturiert: Abschnitt 2 geht knapp auf wichtige verwandte Arbeiten ein. Im Abschnitt 3 wird das Design und die Durchführung der empirischen

P. Schartner · A. Baumann (Hrsg.) · D•A•CH Security 2017 · syssec (2017) 13-23.

Studie beschrieben. Die wesentlichen Ergebnisse der Studie werden in Abschnitt 4 diskutiert. Abschnitt 5 fasst die Arbeit noch einmal zusammen.

2 Verwandte Arbeiten

Eminağaoğlu et al. [EmUE09] zeigen, dass Security-Awareness-Maßnahmen den Umgang mit Passwörtern in einem Unternehmen verbessern. Als Maßnahmen wird eine Kombination aus Schulungen, Postern und einem Informationsportal zum Selbststudium verwendet. Vor Durchführung der Maßnahmen werden 22,4 % der Passwörter mit einem Brute-Force-Angriff in weniger als einer Minute gebrochen. Sechs weitere Monate danach sind es noch 10,6 % der Passwörter und nach zwölf Monaten sind es nur noch 3,1 % der Passwörter. Unklar bleibt, welche der Maßnahmen hier den größten Einfluss haben.

Mit der Phishing-Problematik befassen sich ebenfalls die Arbeiten von Jagatic et al. [JJJM07], Caputo et al. [CPFJ14] und Stockhardt et al. [StRV15, SRVM+16]. Nach Jagatic et al. kann gezeigt werden, dass individualisierte Phishing-Mails von vermeintlichen Bekannten deutlich erfolgreicher sind als Phishing-Mails unbekannter Herkunft. Jagatic et al. haben Informationen über amerikanische Studenten im Alter von 18 bis 24 Jahren gesammelt. Angriffe von vermeintlichen Bekannten der Studenten waren in 72 % der Fälle erfolgreich. Bei Angriffen von unbekannten Personen lag die Erfolgsquote nur bei 16 %.

Eine neue Herangehensweise zeigt der Einsatz von sogenannten *Emdedded Trainings* [CPFJ14], d.h. Benutzer werden bei Fehlverhalten unmittelbar darauf aufmerksam gemacht, dass sie Opfer einer vermeintlichen Phishing-Mail sind. Diese Maßnahme erzielte jedoch nicht den gewünschten Erfolg. Den Benutzern wird nach dem Klick auf einen präparierten Link keine Phishing-Webseite angezeigt, sondern es werden Sicherheitshinweise und Verhaltensweisen vorgeschlagenen. In einer anschließend durchgeführten Umfrage zeigt sich, dass viele Benutzer die angezeigten Inhalte nicht beachtet haben.

Stockhardt et al. untersuchen und vergleichen ebenfalls Security-Awareness-Maßnahmen im Hinblick auf Phishing-Angriffe. Die Autoren kommen zu dem Ergebnis, dass Präsenztrainings im Vergleich zu Lernspielen eine größere Verbesserung bieten, allerdings wird dies nur unter Laborbedingungen und ohne Kontrollgruppe untersucht.

Unsere Studie baut auf den Erkenntnissen der genannten Arbeiten auf mit dem Unterschied, dass diese Studie in einem realistischen Umfeld (KMU mit mehreren Standorten in Deutschland, insgesamt 380 Mitarbeiter) in der Praxis durchgeführt wird. Zu betonen ist, dass die Teilnehmer unserer Studie während ihrer regulären Arbeit mit Phishing-Mails angegriffen und nicht über die Studie in Kenntnis gesetzt werden. Darüber hinaus werden im Studiendesign zwei Kontrollgruppen berücksichtigt, mit deren Hilfe wir weitere begleitende Hypothesen untersuchen.

3 Studiendesign und -durchführung

Unsere Studie unterteilt sich in die folgenden Phasen (vgl. [Diek10]). In der ersten Phase „Formulierung und Präzisierung des Forschungsproblems“ wird mit Hypothesen das Untersuchungsziel konkretisiert. In der zweiten Phase „Planung und Vorbereitung der Erhebung“ legen wir fest, wie die Untersuchung gestaltet wird. Dafür werden für die folgenden Phasen organisatorische sowie technische Vorbereitungen durchgeführt und ein Erhebungsinstrument wird erstellt. In der darauf folgenden Phase „Datenerhebung“ erfassen wir die für unsere Studie benötigten Informationen mit dem zuvor konstruierten Erhebungsinstrument. In der

vierten Phase „Datenauswertung“ werden die erhobenen Informationen und Erfahrungswerte in ein analysefähiges Format gebracht und im Hinblick auf die grundlegende Fragestellung ausgewertet. In der letzten Phase „Berichtserstattung“ fassen wir die ausgewerteten Ergebnisse zusammen und belegen oder widerlegen die aufgestellten Hypothesen.

Dieser Abschnitt geht auf die ersten drei Phasen ein. Der nächste Abschnitt dann auf die Phasen vier und fünf. Die Studie dient der Überprüfung der folgenden Hypothese:

H1: Das im Unternehmen erstellte Präsenztraining erzielt bessere Erfolge bei der Sensibilisierung von IT-Anwendern in Bezug auf E-Mail-Phishing-Angriffe als das im Rahmen dieser Studie ausgewählte Lernspiel.

Dieser Hypothese liegt die Vermutung zugrunde, dass ein Präsenztraining effektiver ist, da Teilnehmer dadurch direkt angesprochen werden können und sie die Möglichkeit erhalten, individuelle Fragen zu stellen. Darüber hinaus hat die Arbeit [SRVM+16] bereits unter Laborbedingungen gezeigt, dass Präsenztrainings besser zur Sensibilisierung geeignet sind.

Unser Studiendesign erlaubt uns, zwei weitere begleitende Hypothesen aufzustellen und zu untersuchen. Erste begleitende Hypothese:

H2: Je häufiger IT-Anwender mit Angriffsszenarien konfrontiert werden, desto kritischer und sicherheitsbewusster werden sie durch diese Konfrontation.

Es wird vermutet, dass IT-Anwender bereits durch die Durchführung der Phishing-Angriffe kritischer werden und dadurch eine höhere Security Awareness erreichen.

Zweite begleitende Hypothese:

H3: Techniker besitzen eine ausgeprägtere Security Awareness als Endbenutzer und Führungskräfte.

Es wird vermutet, dass Techniker durch ihr technisches Hintergrundwissen bereits sensibilisiert sind und sicherheitsbewusst mit IT-Systemen umgehen.

Abbildung 1 zeigt den geplanten und so umgesetzten Studienverlauf. Für die Erstellung der Testgruppen werden Mitarbeiter von vier örtlich getrennten Geschäftsstellen des Unternehmens ausgewählt. Mitarbeiter der ersten Geschäftsstelle werden der Testgruppe A zugeordnet, Mitarbeiter der zweiten Geschäftsstelle werden Testgruppe B zugeordnet und Mitarbeiter der dritten sowie vierten Geschäftsstelle den Kontrollgruppen C und D. Gruppe A mit 49 Teilnehmern absolviert das Präsenztraining, Gruppe B mit 68 Teilnehmern absolviert ein Lernspiel, Gruppe C mit 111 Teilnehmern dient als erste Kontrollgruppe und Gruppe D mit 44 Teilnehmern als zweite Kontrollgruppe. Die Zuordnung der Gruppen auf die Geschäftsstellen ergibt sich zum einen aus der Notwendigkeit, das Präsenztraining glaubwürdig zu motivieren und zum anderen erschwert es den Austausch der Mitarbeiter über die Maßnahmen zwischen den Angriffsphasen. Alle ausgewählten Geschäftsstellen sind bzgl. Mitarbeiterstamm und Organisation ähnlich aufgebaut. Eine zweite Kontrollgruppe ist für die Untersuchung der ersten begleitenden Hypothese notwendig. Der Vergleich von zwei ungeschulten Gruppen wird auf diese Weise ermöglicht.

Die Durchführung der Studie ist aufgrund des sogenannten Hackerparagraphs §202c StGB nur auf Basis des Einverständnisses des angegriffenen Unternehmens möglich, welche im Vorfeld eingeholt wurde. Ein weiterer unternehmensrelevanter Aspekt betrifft die Benutzergruppen. Für

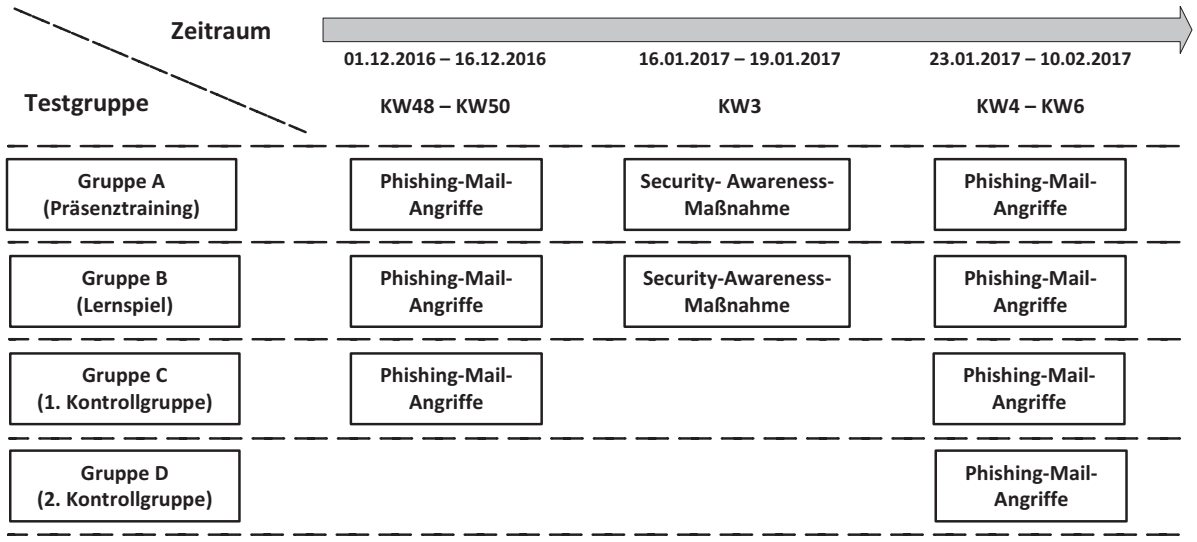


Abb. 1: Zeitlicher Verlauf der Datenerhebung

die zweite begleitende Hypothese werden die Berufsbezeichnungen der E-Mailsignaturen den Benutzergruppen „Führungskräfte“, „Techniker“ und „Endbenutzer“ zugeordnet.

Zur Teilnahme an den jeweiligen Trainings innerhalb der Gruppen A und B besteht kein Zwang seitens des Unternehmens. Beide Gruppen werden via E-Mail durch den Leiter der IT-Abteilung gebeten, das jeweilige Training zu absolvieren. Eine Ablehnung der Teilnahme wird jedoch nicht sanktioniert.

Es wird angenommen, dass viele Mitarbeiter des Unternehmens bereits durch die Konfrontation mit den Angriffsszenarien und aufgrund der Autorität des IT-Leiters freiwillig an den Security-Awareness-Maßnahmen teilnehmen. Da die geplanten Angriffe aus der Perspektive der Mitarbeiter eine reale Bedrohung darstellen, ist es notwendig und auch Unternehmenspraxis, dass die IT-Abteilung anschließend Warnungen versendet. Aus diesem Grund wird die IT-Abteilung in die Studie eingeweiht. Es wird vereinbart, dass Warnungen an die Mitarbeiter erst zwei Stunden nach der Durchführung der Angriffe per E-Mail versendet werden. In dieser Warnung werden alle Mitarbeiter dazu aufgefordert die entsprechende Phishing-Mail zu löschen und ihre Passwörter zu ändern.

Das Präsenztraining hat einen zeitlichen Umfang von 90 Minuten (inkl. Fragerunden). Als Lernspiel kommt „NoPhish“ der TU Darmstadt [SECU16] zum Einsatz. Dieses Spiel wurde anhand eines vorab definierten Kriterienkatalogs (vgl. [Sche17]) ausgewählt.

Die Studiendauer umfasst elf Wochen. In dieser Zeit werden insgesamt sechs Phishing-Mails pro Gruppe versendet (in zwei Angriffsphasen zu jeweils drei E-Mails). Diese E-Mails enthalten eingebettete Links, die einen Nutzer auf fingierte Webseiten der aufgebauten Infrastruktur leiten (siehe Abbildung 2). Auf den jeweiligen Webseiten wird der Nutzer aufgefordert, Daten seines Nutzerkontos einzugeben. Die Webseiten fragen hier private und geschäftliche Account-Daten ab. Dies ist vor dem Hintergrund der Tatsache, dass Nutzer i.d.R. wenige Passwörter verwenden [FlHe07], für Unternehmen kritisch, da mit der Kompromittierung eines privaten Accounts auch ein Unternehmensaccount in Gefahr ist.

Zwischen den zwei Angriffsphasen liegen für Gruppe A und Gruppe B die Security-Awareness-Maßnahmen (Präsenztraining bzw. Lernspiel). Eine Herausforderung besteht hier, in bei-

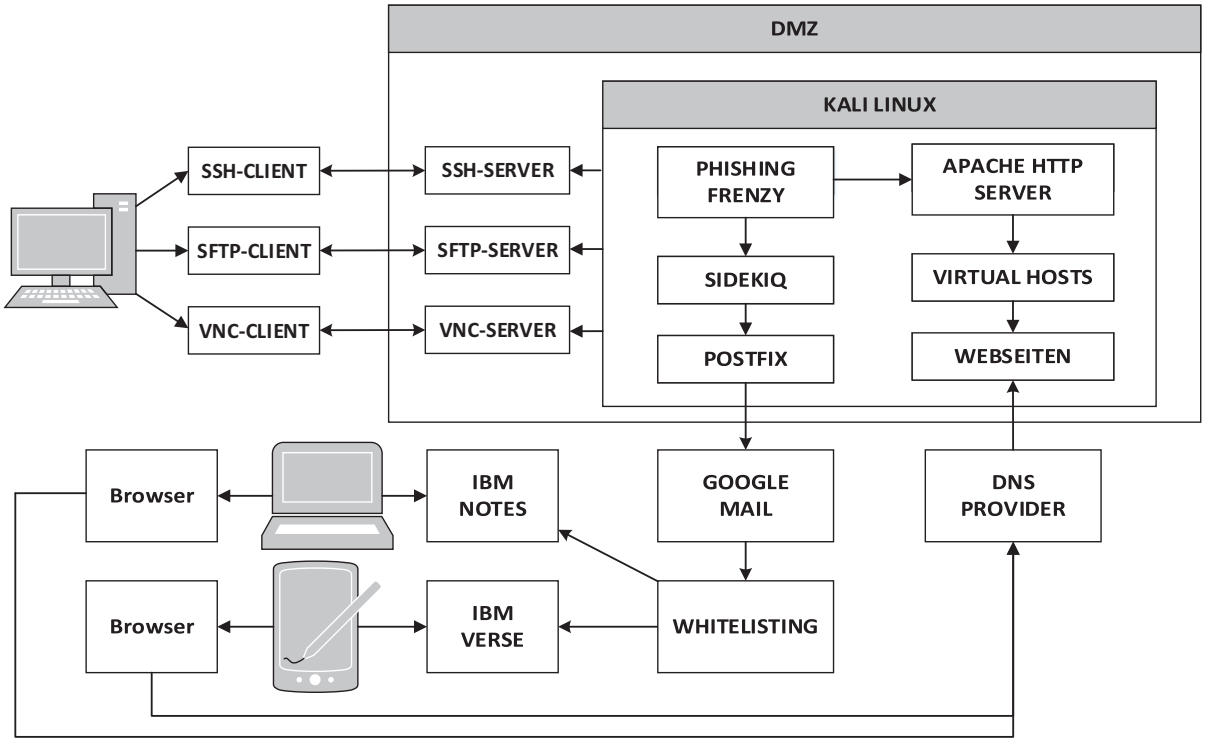


Abb. 2: Aufbau der Infrastruktur zur Datenerhebung

den Angriffsphasen ähnliche, jedoch nicht identische Phishing-E-Mails zu versenden. Hierzu werden thematische Blöcke (Kategorien) gebildet, bspw. in der ersten Angriffsphase gefälschte E-Mails des Anbieters „Amazon“ und in der zweiten Angriffsphase gefälschte E-Mails des Anbieters „PayPal“. Diese lassen sich der Kategorie eCommerce zuordnen. Die Inhalte dieser E-Mails sind in Bezug auf die Zugehörigkeit als unternehmensextern einzuordnen.

Die Angriffe wurden auf die Kategorien eCommerce, Marketing und Social Media aufgeteilt. Tabelle 1 zeigt die Zuordnung der fingierten E-Mails zu den geplanten Angriffsszenarien. Da die jeweiligen Angriffe ähnlich jedoch nicht identisch sind, wird ihre Vergleichbarkeit sichergestellt. Bei identischen Angriffen ist nicht nachvollziehbar, ob die IT-Anwender sich in Bezug auf Security Awareness verbessert haben oder nur daran erinnern, dass es sich bei der E-Mail um einen Angriffsversuch handelt.

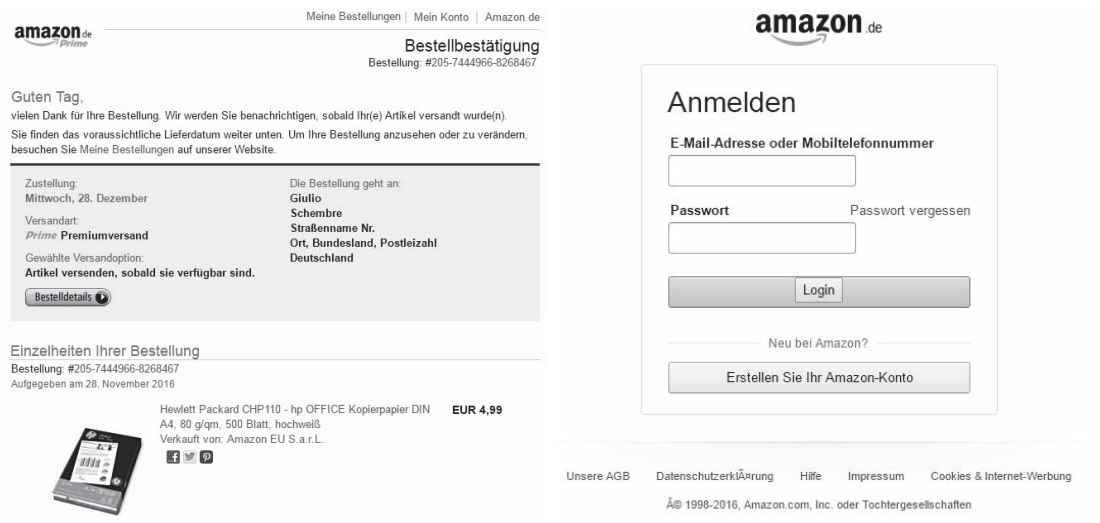
Tab. 1: Zuordnung von Kategorie zu Angriffsphasen

Kategorie	1. Angriffsphase	2. Angriffsphase	Thematik	Zugehörigkeit
eCommerce	Amazon	PayPal	Rechnung	Unternehmensextern
Marketing	Weihnachten	Karneval	Geschenk	Unternehmensintern
Social Media	Twitter	Facebook	Neuigkeit	Unternehmensextern

Für die Datenerhebung wird eine auf Open-Source-Werkzeugen basierende Infrastruktur aufgebaut. Zum einen wird auf diese Weise die Durchführung von Studien mit einer ähnlichen technischen Basis für weitere Arbeiten illustriert und zum anderen werden damit kostengünstige und effektive Vorgehensweisen für KMUs aufgezeigt.

Hervorzuheben sei das Werkzeug „Phishing Frenzy“ [McCa13], welches es erlaubt, auf einfache Weise E-Mail- sowie Webseiten-Templates zu erzeugen und zu verwalten. Ein weiterer Vorteil ist die Möglichkeit beliebig viele Angriffsziele zu adressieren. Vergleichbare Werkzeuge wie z.B. „Lucy“ [AOPL17] sind in der kostenlosen Version in dieser Hinsicht eingeschränkt. Der mit „Phishing Frenzy“ verbundene Hintergrundprozess „Sidekiq“ [PADC17] hat bei der Durchführung der Studie jedoch zu Problemen geführt. Beim Versenden der Phishing-Mails hat „Sidekiq“ alle E-Mails zum gleichen Zeitpunkt an den E-Mailprovider „Google Mail“ weitergeleitet. Dieser Umstand hat dazu geführt, dass die Sendebeschränkungen des E-Mailproviders überschritten wurden und die E-Mails blockiert wurden. Zur Lösung dieser technischen Herausforderung wurde Postfix installiert, welcher die Phishing-Mails im Zehn-Sekunden-Takt weitergeleitet hat.

Das Erstellen von individuellen Templates erlaubt es uns insbesondere, die Teilnehmer persönlich mit Vor- und Nachname anzusprechen. Die dafür notwendigen Informationen wurden aus dem Unternehmensverzeichnis entnommen. Die persönliche Anrede lässt die Phishing-Mails noch authentischer erscheinen. Es ist davon auszugehen, dass sich dieser Sachverhalt positiv auf die Erfolgsquote der Angriffe auswirkt. In Abbildung 3 wird ein Angriff am Beispiel von „Amazon“ dargestellt.



a) Phishing-E-Mail

b) Zugehörige Phishing-Webseite

Abb. 3: Beispiel eines Phishing-Angriffs

Die Phishing-Mails selbst werden von mehreren für diese Studie erstellten Google Mail Konten versendet (diese wurden vorab von der internen IT-Abteilung auf eine Spamfilter-Whitelist gesetzt). Bei einem DNS-Provider werden fingierte Linkadressen registriert, welche möglichst ähnlich zu den originalen Linkadressen sind. Am Beispiel von „Amazon“ wird „http://www.amazon.secure.simple-url.de“ als eine solche authentisch wirkende Linkadresse gewählt.

4 Ergebnisse der Studie

Zunächst kann festgehalten werden, dass die Motivation innerhalb der Gruppen, sich an einem Training zu beteiligen, sehr unterschiedlich ausfällt: Die Teilnehmerquote in Gruppe A

(Präsenztraining) liegt bei 59,16 %, während die Teilnehmerquote in Gruppe B (Lernspiel) mindestens 8,82 %[1] beträgt. Die Freiwilligkeit an der Teilnahme von Security-Awareness-Maßnahmen wirkt sich hier deutlich aus.

Für die „Marketing"-Phishing-Mails sind in Tabelle 2 die Ergebnisse pro Angriffsphase aufgeführt. Dieser Phishing-Angriff war erfolgreicher als die beiden übrigen Angriffe und wird in dieser Arbeit detailliert beschrieben[2]. Es wird vermutet, dass dieser Sachverhalt der internen Zugehörigkeit der Phishing-E-Mails zugrunde liegt. Der vermeintliche Absender war in diesem Fall eine bekannte Person aus dem angegriffenen Unternehmen.

In der Auswertung ist zu erkennen, dass sich das Verhalten aller Gruppen bzgl. Phishing-E-Mails verbessert. Die Teilnehmer klicken nach den Trainingsmaßnahmen seltener auf die in den E-Mails eingebetteten Links und geben auch seltener ihr Passwort preis. In der Gruppe A kann nach der Trainingsmaßnahme überhaupt kein Passwort mehr abgegriffen werden.

Auffällig ist, dass vor den Schulungsmaßnahmen in allen drei Gruppen die Bereitschaft, auf unbekannte Links zu klicken, im Mittel bei fast ein Drittel der Teilnehmer vorhanden ist. Dies stellt vor dem Hintergrund von *Drive-by-download*-Angriffen [CoKV10, Sche16] bereits eine Gefährdung der Unternehmens-IT dar.

Tab. 2: Auswertung der „Marketing"-Phishing-Mails vor und nach dem jeweiligen Training

	Link angeklickt			Passwort erhalten		
Testgruppen	1. Angriffs-phase	2. Angriffs-phase	Differenz	1. Angriffs-phase	2. Angriffs-phase	Differenz
Gruppe A	36,73 %	2,04 %	34,69 %	16,33 %	0,00 %	16,33 %
Gruppe B	25,00 %	5,88 %	19,12 %	16,18 %	1,47 %	14,71 %
Gruppe C	29,73 %	10,0 %	19,73 %	18,02 %	2,70 %	15,32 %
Gruppe D	N/A	22,73%	N/A	N/A	6,82%	N/A

In der ersten Angriffsphase zeigt Gruppe B in Hinblick auf die Security Awareness die beste Verhaltensweise. Beispielsweise klicken dort bei der „Weihnachten"-Phishing-Mail 25,00 % der Mitarbeiter auf den Link. Bei Gruppe A sind es 36,73 % der Mitarbeiter. Nach den Sensibilisierungsmaßnahmen ändert sich dies und Gruppe A überholt Gruppe B. In der „Karneval"-Phishing-Mail klicken 5,88 % der Gruppe B auf den Link. Bei Gruppe A sind es nur noch 2,04 % der Mitarbeiter.

Das beobachtete Verhalten der geschulten Gruppen bei der Aktion „Angeklickt" spiegelt sich ebenfalls bei der „Passworteingabe" wider. In beiden Gruppen geben bei der ersten Angriffsphase etwa 16 % der Mitarbeiter Passwörter auf der fingierten Phishing-Webseite ein. In der zweiten Angriffsphase geben keine Mitarbeiter der Gruppe A mehr Passwörter ein. Bei Gruppe B sind es hingegen noch 1,47 %.

Insgesamt kann festgehalten werden, dass im Rahmen dieser Studie die Hypothese belegt wird:

H1: Das im Unternehmen erstellte Präsenztraining erzielt bessere Erfolge bei der Sensibilisierung von IT-Anwendern in Bezug auf E-Mail-Phishing-Angriffe als das im Rahmen dieser Studie ausgewählte Lernspiel.

[1] Dieser Wert wurde durch eine anschließende Umfrage ermittelt und könnte höher liegen.

[2] Die weiteren Phishing-Angriffe und deren Auswertung sind in [Sche17] ausführlich beschrieben.

Gruppe A zeigt die größte Verbesserung und erzielt nach der Durchführung der Sensibilisierungsmaßnahme bessere Ergebnisse als Gruppe B.

Mit Blick auf die erste Kontrollgruppe (Gruppe C) ist zu beobachten, dass sich auch in dieser Gruppe der Umgang mit Phishing-E-Mails deutlich verbessert hat. Die Verbesserungen liegen sehr nah an den beobachteten Verbesserungen in Gruppe B. Wie in Tabelle 2 dargestellt, klicken in Gruppe C nur noch 10,00 % der Mitarbeiter auf den Link der „Karneval“-Phishing-Mail. Davor waren es bei der „Weihnachten“-Phishing-Mail noch 29,73 % der Mitarbeiter. Mithilfe dieses Sachverhaltes ist es bereits möglich, die erste begleitende Hypothese (siehe Seite 3) zu belegen. Darüber hinaus wird die erste begleitende Hypothese ebenfalls durch den Vergleich zwischen den beiden Kontrollgruppen bei der zweiten Angriffsphase gestützt. Wie in Tabelle 3 beispielhaft an der „Karneval“-Phishing-Mail dargestellt, erzielt Gruppe C bessere Ergebnisse als Gruppe D.

Tab. 3: Vergleich der beiden Kontrollgruppen bei der „Karneval“-Phishing-Mail

Phishing-Aktion	Gruppe C	Gruppe D	Differenz
Link angeklickt	10,00 %	22,73 %	-12,73 %
Passwort erhalten	2,70 %	6,82 %	-4,12 %

Wir sehen somit, dass allein durch das Versenden von fingierten Phishing-E-Mails ein Sensibilisierungsprozess bei den betroffenen Mitarbeitern stattfindet. So wurde nach der 1. Angriffsphase auch die IT-Abteilung häufiger und direkter auf Phishing-Angriffe angesprochen.

Bei der zweiten begleitenden Hypothese geht es um die Security Awareness bei unterschiedlichen Benutzergruppen und ob Techniker ein höheres Sicherheitsbewusstsein als andere Benutzergruppen besitzen. Zur Untersuchung der Hypothese wird zunächst die erste Angriffsphase betrachtet. In Bezug auf die angeklickten Links erzielen Mitarbeiter der Benutzergruppe Techniker bei der „Amazon“-Phishing-Mail das beste Ergebnis. Bei der „Weihnachten“- und „Twitter“-Phishing-Mail erzielen hingegen die Endbenutzer das beste Ergebnis. Bei der zweiten Angriffsphase erzielt die Benutzergruppe Techniker in Bezug auf die angeklickten Links das beste Ergebnis bei der „Karneval“-Phishing-Mail. Bei der „Facebook“- und „PayPal“-Phishing-Mail erzielt diese Benutzergruppe jedoch das schlechteste Ergebnis.

Insgesamt betrachtet ist kein eindeutiges Verhaltensmuster bei der Auswertung erkennbar. Weder im Vergleich mit den jeweiligen Angriffsphasen noch mit den thematisch zusammenpassenden Phishing-Mails ist ein Verhaltensmuster erkennbar. Somit ist nicht eindeutig feststellbar, welche Benutzergruppe die beste Security Awareness besitzt. Die ausgewerteten Ergebnisse stützen die zweite begleitende Hypothese nicht. Auf diesem Sachverhalt basierend kann die zweite begleitende Hypothese widerlegt werden. Die aus dieser Untersuchung resultierende Erkenntnis ist somit, dass Techniker gleichermaßen für Phishing-Angriffe anfällig sind wie Endbenutzer und Führungskräfte.

Aus unserer Studie können noch weitere Erkenntnisse gewonnen werden. Die Warnungen der IT-Abteilung, welche in der Regel zwei Stunden nach den Angriffen versendet wurden, haben dazu geführt, dass weniger Mitarbeiter auf den präparierten Link klicken und Passwörter preisgeben. Jedoch hat sich herausgestellt, dass die Mitarbeiter auch nach dieser Warnung für die Angriffe anfällig bleiben. Einige Mitarbeiter, welche sich an die IT-Abteilung gewendet haben, gaben dabei an, dass Sie ihre E-Mails chronologisch bearbeiten und die Warnung zu spät gelesen haben.

Ebenso haben einige Mitarbeiter angemerkt, dass Sie mehrere Passwörter ausprobiert haben. Die anschließende Analyse der Log-Dateien bestätigt diesen Sachverhalt. Bei einer der Phishing-Mails wurden von einer ID bis zu sieben Passworteingabeversuche protokolliert. Dieses Verhalten spiegelt die Erkenntnisse der von Jagatic et al. durchgeführten Studie [JJJM07] wider. Dort haben Anwender bis zu zehn Passworteingabeversuche getätigt.

Die Geheimhaltung der Studie ist mit Vor- und Nachteilen verbunden. Der ausschlaggebendste Vorteil ist, dass sich die Mitarbeiter durch die Geheimhaltung der Studie ernsthaft mit der potenziellen Bedrohungslage beschäftigen. In der Realität werden Phishing-Mails ebenfalls nicht bekannt gegeben, daher hätte eine Bekanntgabe der Angriffe oder der Studie aus Sicht des Unternehmens nicht zu einer aussagekräftigen Einschätzung der Security Awareness geführt.

Nachteilig bei einer solchen Geheimhaltung sind hingegen die Unruhen, welche dadurch in einem Unternehmen entstehen können. Die IT-Abteilung ist durch die Geheimhaltung wiederholt in prekäre Situationen geraten. In einigen Ausnahmefällen haben Mitarbeiter des Unternehmens die Arbeitsweise der IT-Abteilung kritisch hinterfragt, da sie Warnungen unmittelbar nach dem Auftreten eines Phishing-Angriffs erwarten. Die IT-Abteilung war jedoch aufgrund der Studie an eine zweistündige Wartezeit gebunden.

Eine Möglichkeit diesen Unruhen entgegen zu wirken, wäre ein größerer zeitlicher Abstand zwischen den jeweiligen Angriffen. Eine solche Veränderung für das Studiendesign ist jedoch nur bei Langzeitstudien möglich.

5 Fazit und Ausblick

Ein Fazit dieser Studie ist, dass in diesem konkreten Fallbeispiel ein Präsenztraining besser zur Sensibilisierung geeignet ist als kostengünstige Lernspiele. Nichtsdestotrotz führen beide Maßnahmen zu einer Verbesserung der Security Awareness. Zudem stellt bereits das Versenden von fingierten Phishing-Mails eine effektive Maßnahme zur Verbesserung der IT-Sicherheit dar. Die versendeten Phishing-Mails sind bei Technikern im gleichen Maße erfolgreich wie bei Endbenutzern und Führungskräften.

Ebenso hat sich gezeigt, dass die Phishing-Angriffe erfolgreicher sind, wenn die vermeintlichen Absender und die Inhalte der Phishing-Mails das angegriffene Unternehmen betreffen. Im Optimalfall wirkt eine Phishing-Mail so authentisch, dass die Mitarbeiter eines Unternehmens sie für eine interne und offizielle E-Mail halten.

Aus den Erkenntnissen unserer Studie ergibt sich außerdem eine neue Herangehensweise für die in [CPFJ14] untersuchten *Embedded Trainings*. Die dafür notwendige Ausgangssituation wäre wie in unserer Studie die Geheimhaltung der fingierten Phishing-Angriffe. Nach der Durchführung eines solchen Angriffs wirkt die ansonsten nur in gängigen Medien aufgezeigte Bedrohungslage nicht mehr abstrakt, sondern erscheint für die angegriffenen IT-Anwender real. Ihre Aufmerksamkeit und ihr Interesse sind somit geweckt. Bei den in dieser Studie durchgeführten Angriffen hat sich bereits gezeigt, dass die Anfälligkeit der Mitarbeiter nach dem Versenden einer Warnung zwar nicht komplett erlischt, jedoch deutlich abnimmt. Versendet die IT-Abteilung zu diesem Zeitpunkt Warnungen an die Mitarbeiter, ist davon auszugehen, dass diese von den Mitarbeitern mehr Beachtung finden als zuvor. Es kann angenommen werden, dass die Inhalte eines *Embedded Trainings* sowie weitere Security-Awareness-Maßnahmen auf diese Art und Weise effektiver und nachhaltig vermittelt werden. Ein wichtiger Erfolgsfaktor ist dabei die Art und Weise der Vermittlung. Wir schlagen vor, dass diese Inhalte explizit in der

Warnung nach einem Angriff von offizieller Stelle vermittelt werden. Eine beiläufige Vermittlung, wie bei [CPFJ14], welche innerhalb von fingierten Phishing-E-Mails stattfindet, ist aus unserer Sicht nicht zu empfehlen.

Es ist geplant, die Studie zu wiederholen, hier jedoch die Teilnahme an dem Präsenztraining und die Absolvierung des Lernspiels verpflichtend für alle Mitarbeiter vorzuschreiben. Zur Erreichung von allgemeingültigen Aussagen und Ergebnissen müsste diese Studie in einem größeren Umfang und in mehreren Unternehmen wiederholt werden.

Darüber hinaus wollen wir weitere Angriffsvektoren (an unternehmens-öffentlichen Plätzen platzierte USB-Sticks mit Schadsoftware, offene WiFi-Access-Points in Unternehmensreichweite, Aufrufe von bedrohlichen Webseiten über im Unternehmen platzierte QR-Code Sticker etc.) und deren Gefahren für das Unternehmen in ähnlichen Studien untersuchen.

Die unerwartete Verbesserung von Gruppe C (erste Kontrollgruppe), welche keine Security-Awareness-Maßnahme erhalten hat, liefert zudem die Basis für weitere Fragestellungen. Von Interesse wäre, ob aggressive Methoden (Phishing-Angriffe etc.) oder wohlwollende Methoden (Präsenztraining, Lernspiel etc.) besser dazu geeignet sind ein IT-Sicherheitsbewusstsein bei IT-Anwendern zu schaffen. Hier müsste ebenfalls untersucht werden, inwieweit die jeweiligen Methoden gewinnbringend kombiniert werden können.

Literatur

[AOPL17] Anton, Oliver, Palo, Lucy Phishing GmbH: Lucy – Simuliertes Phishing, SMiShing, Malware, Ransomware und Mehr. https://www.lucysecurity.com/de/, Stand: 22.05.2017 (2017).

[BSI17] BSI: Ergebnisse der Cyber-Sicherheits-Umfrage 2016. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/cybersicherheitslage/umfrage2016_ergebnisse.pdf, Stand: 03.05.2017 (2017).

[Bund16] Bundeskriminalamt: Cybercrime – Bundeslagebild 2015. https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html, Stand: 31.03.2017 (2016).

[Cerm14] F. Cerminara: Hackerangriffe – Tendenz steigend. https://security.infoguard.ch/hubfs/InfoGuard/Publikationen/infoguard_hackerangriff_kmurundschau_1403.pdf, Stand: 31.03.2017 (2014).

[CoKV10] M. Cova, C. Kruegel, G. Vigna: Detection and Analysis of Drive-by-download Attacks and Malicious JavaScript Code. *In: Proceedings of the 19th International Conference on World Wide Web*, WWW '10, ACM, New York, NY, USA (2010), 281–290.

[CPFJ14] D. D. Caputo, S. L. Pfleeger, J. D. Freeman, M. E. Johnson: Going Spear Phishing: Exploring Embedded Training and Awareness. In: *IEEE Security Privacy*, 12, 1 (2014), 28–38.

[Diek10] A. Diekmann: Empirische Sozialforschung: Grundlagen, Methoden, Anwendungen. Rowohlt, 4 Aufl. (2010).

[EmUE09] M. Eminağaoğlu, E. Uçar, Şaban Eren: The Positive Outcomes of Information Security Awareness Training in Companies – A Case Study. In: *Information Security Technical Report*, 14, 4 (2009).

[FlHe07] D. Florencio, C. Herley: A Large-scale Study of Web Password Habits. *In: Proceedings of the 16th International Conference on World Wide Web*, WWW '07, ACM, New York, USA (2007).

[Jesc16] M. Jeschke: IBM-IT-Sicherheitsreport – Die grössten Cybergefahren. http://www.searchsecurity.de/news/450286708/IBM-IT-Sicherheitsreport-die-groessten-Cybergefahren, Stand: 31.03.2017 (2016).

[JJJM07] T. N. Jagatic, N. A. Johnson, M. Jakobsson, F. Menczer: Social Phishing. In: *Commun. ACM*, 50, 10 (2007), 94–100.

[Kevi06] W. S. Kevin Mitnick: Die Kunst der Täuschung. mitp-Verlag (2006).

[McCa13] B. McCann: Phishing Frenzy – Manage Email Phishing Campaigns – Penetration Testing. https://www.phishingfrenzy.com, Stand 28.03.2017 (2013).

[PADC17] M. Perham, T. Arcieri, R. Dardour, J. Cooke: Sidekiq – Simple, efficient background processing for Ruby. http://sidekiq.org/, Stand: 22.05.2017 (2017).

[Reut17] Reuters/dpa: Hackerangriffe auf Nato nehmen dramatisch zu. http://www.faz.net/aktuell/politik/ausland/nato-ist-beliebtes-opfer-von-hackern-bei-cyberangriffen-14695571.html, Stand: 31.03.2017 (2017).

[Sche16] F. A. Scherschel: Dogspectus: Erste Android-Geräte im Vorbeisurfen mit Exploit-Kit verseucht. https://www.heise.de/security/meldung/Dogspectus-Erste-Android-Geraete-im-Vorbeisurfen-mit-Exploit-Kit-verseucht-3190235.html, Stand 28.03.2017 (2016).

[Sche17] G. Schembre: Eine empirische Studie über die Wirksamkeit von Security Awareness Maßnahmen: Der Vergleich von Präsenztrainings zu Lernspielen in Bezug auf Security Awareness am Beispiel eines mittelständischen Unternehmens. Masterarbeit, Hochschule Darmstadt, University of Applied Sciences, Haardtring 100, 64295 Darmstadt (2017).

[SECU16] SECUSO: NoPhish – the Anti-Phishing Training. https://www.secuso.informatik.tu-darmstadt.de/en/secuso/research/results/nophish/, Stand: 31.03.2017 (2016).

[SRVM+16] S. Stockhardt, B. Reinheimer, M. Volkamer, P. Mayer, A. Kunz, P. Rack, D. Lehmann: Teaching Phishing-Security: Which Way is Best? *In: 31st International Conference on ICT Systems Security and Privacy Protection - IFIP SEC 2016*, Springer (2016), 135–149.

[StRV15] S. Stockhardt, B. Reinheimer, M. Volkamer: Über die Wirksamkeit von Anti-Phishing-Training. *In: Usable Security and Privacy Workshop in conjunction with Mensch und Computer 2015*, A. Weisbecker, M. Burmester & A. Schmidt (2015), 647–655.