HMD (2020) 57:597–612
https://doi.org/10.1365/s40702-020-00613-y

SCHWERPUNKT

Spear Phishing 2.0: Wie automatisierte Angriffe Organisationen vor neue Herausforderungen stellen

Anjuli Franz · Alexander Benlian

Eingegangen: 19. Januar 2020 / Angenommen: 28. März 2020 / Online publiziert: 14. April 2020

Zusammenfassung Vom ursprünglichen „Phishing = Passwort + Fishing“ wandelt sich das Angriffsmuster durch neue Technologien zum boomenden Geschäftsmodell der cyberkriminellen Szene. Schadsoftware wie „Emotet“ zeigt, dass automatisierte Spear Phishing-Angriffe Realität geworden sind und immense Schäden verursachen. Der Mitarbeiter rückt damit in den Fokus von IT-Sicherheitsmaßnahmen. Das Ziel dieses Beitrags ist es, einen Rundumblick zur aktuellen und zukünftigen Bedrohungslage durch Spear Phishing zu geben und konkrete Handlungsempfehlungen abzuleiten. Zur Messung der Security Awareness im organisatorischen Umfeld wird die Kennzahl „Employee Security Index“ vorgestellt, welche das Sicherheitsbewusstsein von Mitarbeitern gegenüber Phishing-Angriffen standardisiert messbar macht. Es wurde ein Feldexperiment in einer deutschen Organisation durchgeführt, um die Verwundbarkeit der Belegschaft gegenüber Spear Phishing und die Wirksamkeit verschiedener Trainingsmaßnahmen zu untersuchen. Die erhobenen Daten werden mithilfe des „Employee Security Index“ bewertet. Insgesamt verdeutlichen die Ergebnisse, dass neben technischen und organisatorischen Schutzmaßnahmen sowohl eine Schulung der Mitarbeiter als auch ein Umdenken nutzerverbundener Prozesse unabdingbar ist.

Schlüsselwörter Spear Phishing · Security Awareness · Social Engineering · Emotet · Faktor Mensch · Employee Security Index

A. Franz (✉) · A. Benlian
Technische Universität Darmstadt, Hochschulstraße 1, 64289 Darmstadt, Deutschland
E-Mail: franz@ise.tu-darmstadt.de

A. Franz
IT-Seal GmbH, Hilpertstraße 31, 64295 Darmstadt, Deutschland

Spear Phishing 2.0: How Automated Attacks Present Organizations With New Challenges

Abstract From the original "Phishing = Password + Fishing", new technology allows attack patterns to change and make Phishing a booming business of the cybercriminal scene. Malware, such as "Emotet", shows that automated Spear Phishing attacks have become reality and cause immense damage. This puts the employee in the focus of IT security measures. The aim of this paper is to provide an overview of the current and future threat posed by Spear Phishing and to derive guidance for IT security management. We introduce the "Employee Security Index", an index to measure security awareness against Phishing attacks in the organizational environment in a standardized way. A field experiment was conducted in a German organization in order to investigate the vulnerability of its workforce to Spear Phishing and the effectiveness of various training measures. The data collected is evaluated using the "Employee Security Index". Overall, the results of this paper make it clear that, in addition to technical and organizational protective measures, both employee training and a rethinking of user-related processes are indispensable.

Keywords Phishing · Spear phishing · Security awareness · Social engineering · Emotet · Human factor · Employee Security Index

1 Einleitung

Im Zeitalter der Digitalisierung stellen Phishing-Angriffe Unternehmen, Organisationen sowie Privatpersonen vor wachsende Herausforderungen (Benlian 2020). Phishing ist ein Teilbereich von Social Engineering. Social Engineering bezeichnet Angriffsmuster, welche auf die Schwachstelle Mensch abzielen, um IT-Systeme anzugreifen. Cyber-Kriminelle geben sich hierbei z. B. als vertrauenswürdige Quelle aus und nutzen E-Mails als Angriffsvektor, um Schadsoftware im Netzwerk zu platzieren, Zugangsdaten abzugreifen oder sich finanziell zu bereichern (Wright et al. 2014).

Da Unternehmen zunehmend mehr in technische Schutzmaßnahmen investieren, ist der Weg über den „Faktor Mensch" für Angreifer oft der einfachere. Der Nutzer wird daher häufig als das schwächste Glied der IT-Sicherheitskette bezeichnet. Sogenannte Spear Phishing-Angriffe beschreiben dabei fortgeschrittene, zielgerichtete Phishing-Angriffe, welche individuell auf Personen oder Organisationen ausgerichtet sind. Spear Phishing war im Jahr 2019 der beliebteste Angriffsvektor bei Cyber-Angriffen (Symantec 2019). Schaffen es die Angreifer, mit einer Spear Phishing-E-Mail Zugang zum Firmennetzwerk zu erhalten, geht der finanzielle Schaden schnell in die Höhe: Die durchschnittlichen Kosten eines solchen Vorfalls betragen für KMU etwa 1,4 Mio. € (Cloudmark 2016).

Neben rein finanziellen Schäden sind bei Phishing-Angriffen häufig Produktionsausfälle, Reputationsschäden und Wirtschaftsspionage die Folge. Denkt man in Richtung Internet of Things (IoT), stellen hochvernetzte IT-Infrastrukturen ein äußerst lukratives Angriffsziel für beispielsweise DDoS (Distributed Denial of Service)-

Angriffe dar (Hertel 2015). Laut einer Studie des Digitalverbands Bitkom entsteht der deutschen Wirtschaft durch digitale Spionage, Sabotage und Datendiebstahl ein Schaden von 21 Mrd. € jährlich (Bitkom 2018).

Dieser Beitrag gibt einen Einblick in die Thematik „Spear Phishing“ und beleuchtet, welche Maßnahmen Unternehmen und Organisationen ergreifen sollten, um sich gegen aktuelle Bedrohungen zu schützen. Abschn. 2 behandelt die Evolution von Phishing über die letzten Jahre und präsentiert Angriffsmuster realer Vorfälle aus 2019. Abschn. 3 widmet sich dem Thema „Security Awareness“, d. h. dem Sicherheitsbewusstsein von Mitarbeitern, und stellt verschiedene Trainingsansätze vor. In Abschn. 4 präsentieren wir die Ergebnisse eines Feldexperiments, welches die Messung und Steigerung der Security Awareness gegenüber Spear Phishing in einer Organisation untersucht. Abschließend gibt Abschn. 5 konkrete Handlungsempfehlungen für Informationssicherheitsverantwortliche.

2 Phishing: Eine kurze Evolutionsgeschichte

Von der ursprünglichen Definition „Phishing = Passwort + Fishing“ wandelt sich das Angriffsmuster durch neue Technologien zum boomenden Geschäftsmodell der cyberkriminellen Szene. Angreifer nutzen automatisiert öffentlich verfügbare Informationen und setzen immer komplexere und glaubwürdigere Angriffsmuster ein. Dies fordert einen gemeinsamen Kraftakt von technischen und organisatorischen Schutzmaßnahmen sowie aufmerksamen Mitarbeitern. Dieses Kapitel gibt einen aktuellen Rundumblick zum Thema Phishing.

2.1 Besser, leichter, öfter: Wachsende Risiken durch Phishing

Im klassischen Sinn beschreibt Phishing das Abgreifen von Zugangsdaten auf gefälschten Login-Seiten, das heißt das „Fischen“ von Passwörtern. Da die Angriffsmuster und -motive immer komplexer werden, versteht man heute den Begriff oft im breiteren Sinn und fasst darunter alle Arten von Cyber-Angriffen per E-Mail. Oft ist die Phishing-E-Mail dabei nur der erste Schritt, um Zugang zum System zu erlangen. Das Nachladen von Schadsoftware oder der Missbrauch von E-Mail-Postfächern zum Versand weiterer Angriffe folgt unter Umständen unbemerkt. Der technische Angriff kann dabei über geklonte Login-Seiten stattfinden oder Links nutzen, welche einen Drive-by-Download auslösen. Hier führt allein der Besuch einer Website zum Download einer Datei, welche im Anschluss gegebenenfalls Sicherheitslücken in veralteter Software ausnutzen kann. Cyber-Kriminelle können mit den neuesten technischen Standards durchaus mithalten: Da Dateitypen mit direktem Systemzugriff (wie beispielsweise .exe-Dateien) von E-Mail-Filtersystemen mittlerweile häufig aussortiert werden, nutzen mittlerweile 48 % aller schadhaften E-Mail-Anhänge Microsoft Office-Dateien wie .docm oder .xlsm, welche über Makros Schadsoftware nachladen können (Symantec 2019). Viele Browser sprechen außerdem eine Warnung aus, wenn sich der Nutzer auf nicht-verschlüsselten Webseiten („http“) bewegt. Die Folge: 58 % aller Phishing-Websites nutzen eine SSL-Verbindung, d. h. sind unter „https“ erreichbar (APWG 2019).

Da sich die Angriffsmuster dynamisch ändern, reichen generalistische technische Schutzmaßnahmen wie Firewalls oder E-Mail-Filter mit einfachen Heuristiken nicht mehr aus, um IT-Systeme effektiv abzuschotten. Cyberkriminellen steht eine Vielzahl an kostengünstigen Werkzeugen zur Verfügung, um mit geringem technischen Know-how komplexe Angriffe durchzuführen (Pienta et al. 2018).

Einen Schritt weiter als Phishing geht das sogenannte Spear Phishing, welches zielgerichtete Angriffe auf Personen oder Organisationen beschreibt. Die Kriminellen nutzen hier bestehende Vertrauensverhältnisse aus, indem sie sich auf Personen oder Sachverhalte beziehen, die der Empfänger bereits kennt. Beispiele sind E-Mails im Namen von Kollegen, gefälschte Rechnungen von tatsächlichen Lieferanten oder Anfragen, die mit Branchenwissen glänzen. Solche Angriffe nutzen oft Informationen aus öffentlich zugänglichen Quellen, im Fachjargon wird dies als Open Source Intelligence (OSINT) bezeichnet. Das Problem: Spear Phishing-Angriffe sind heute nicht mehr mit großem manuellen Aufwand verbunden, sondern können automatisiert durchgeführt und millionenfach eingesetzt werden. Der altbekannte Glaube, Phishing-E-Mails erkenne man an Rechtschreibefehlern und fehlendem Kontext, ist für Nutzer im Arbeitsalltag demnach nicht mehr zutreffend.

2.2 Automatisiertes Spear Phishing in freier Wildbahn: Emotet

Das Jahr 2019 bewies eindrucksvoll, dass Spear Phishing kein Einzelfall mehr ist, vor dem sich nur hochrangige Ziele zu fürchten haben. Ein Beispiel für automatisiertes Spear Phishing im großen Stil ist Emotet. Die Schadsoftware versendet E-Mails mit schädlichem Dateianhang (häufig .docm oder .xlsm) oder Links und ist dabei in der Lage, „auf bestehende E-Mail-Konversationen zu antworten und daher authentisch wirkende E-Mails zu verschicken“ (BSI 2019a). Dabei führt eine Erstinfektion dazu, dass organisationsintern weitere Phishing-E-Mails im Namen der Betroffenen versendet werden. Der eigentliche Schaden entsteht durch nachgeladene Software, beispielsweise durch Trojaner, welche den Tätern Komplettzugriff auf das Netzwerk verschaffen, bevor eine Ransomware eingesetzt wird. Diese verschlüsselt Daten oder ganze Netzwerke und fordert Lösegeld.

Die Schadsoftware hat Ende 2019 binnen weniger Tage für IT-Ausfälle bei Industrie und Bundesbehörden gesorgt (BSI 2019a), außerdem waren die Städte Frankfurt am Main und Bad Homburg, das Berliner Kammergericht, die Justus-Liebig-Universität Gießen und das Klinikum Fürth über mehrere Tage komplett offline (Heise 2019a, 2019b, 2019c). Neben rein finanziellen Schäden brachten diese Angriffe Produktionsausfälle, die Abmeldung eines Klinikums von der Notfallversorgung und geschlossene Bürgerämter mit sich, sowie 38.000 E-Mail-Nutzer der JLU Gießen, welche sich neue Passwörter für ihren Account persönlich in der Turnhalle des Campus abholen durften. In den genannten Fällen fand Emotet durch das Aktivieren eines Makros in einem Dateianhang Zugang zum Netzwerk.

2.3 Verstärkte Gefahr durch Phishing im KI-Zeitalter

Neben Emotet sorgen auch andere automatisierte Spear Phishing-Angriffsmuster für immer schwieriger zu erkennende Phishing-E-Mails. Cyberkriminelle nutzen öffent-

liche Daten von Unternehmenswebseiten oder aus sozialen Netzwerken, um gezielte Angriffe zu generieren (Maedche et al. 2011). Diese OSINT-Analyse wird oft nicht mehr manuell durchgeführt – relevante Daten werden mithilfe von Crawling-Tools von Webseiten und aus Sozialen Netzwerken gesammelt und anschließend automatisiert zur Erstellung von maßgeschneiderten Phishing-E-Mails genutzt. Informationen wie die Namen der Geschäftsführung, firmeninterne Strukturen oder Ansprechpartner sind für die Angreifer dabei genauso interessant wie persönliche Daten aus Sozialen Netzwerken, z. B. ehemalige Arbeitgeber, Kontakte, Hobbys oder der Geburtstag. Dies alles hilft, Angriffe so persönlich und glaubwürdig wie möglich zu gestalten. Neben Phishing nutzen Cyber-Kriminelle auch andere Angriffsvektoren, wie beispielsweise Telefon-Phishing. Mehrstufige Angriffe beinhalten das gezielte Sammeln von Informationen, das Aufbauen eines Kanals ins Unternehmen bis hin zum technischen Angriff. Ein Blick in Richtung Zukunft lässt ahnen, welches Ausmaß an Komplexität mit künstlicher Intelligenz (KI) gesteuerte Social Engineering-Angriffe erreichen können: Den technologischen Vorteil von Conversational Agents oder selbstlernenden Angriffsmustern werden sich auch Cyberkriminelle zu Nutze machen.

3 Security Awareness ist unabdingbar – nur wie erreicht man sie?

Aufgrund der steigenden Gefahr durch Social Engineering-Angriffe wie Spear Phishing beinhalten Informationssicherheitskonzepte im organisatorischen Umfeld immer öfter Maßnahmen zur Security Awareness. Der Begriff Security Awareness beschreibt das Ausmaß, in dem Mitarbeiter die Bedeutung von Informationssicherheit in ihrem Unternehmen sowie die Tragweite ihrer eigenen Sicherheitsverantwortlichkeit verstehen und dementsprechend handeln (ISF 2007). Security Awareness ist dabei als dynamischer Prozess zu verstehen: Neue Angriffsmethoden und -vektoren stellen, wie am Beispiel Emotet erläutert, Mitarbeiter und Informationssicherheitsverantwortliche vor ständig neue Herausforderungen. Ein anpassungsfähiges Awarenesskonzept sollte daher ein dauerhafter und integraler Bestandteil jeder Unternehmenskultur sein (Kruger und Kearney 2006).

Die Fachliteratur (z. B. Wright et al. 2014) nennt in Bezug auf Security Awareness häufig die von Kahneman (2011) beschriebene Unterteilung des menschlichen Denkens in schnelles („System 1“) und langsames („System 2“) Denken: Während System 1 für erfahrungsbasierte oder automatisierte Informationsverarbeitung zuständig ist und dabei intuitive, schnelle Entscheidungen erlaubt, beschreibt System 2 das abwägende, rationale und analytische Verhalten, welches zur Bewertung größerer und langsamer Entscheidungen genutzt wird.

Der Netzaktivist und Hacker Linus Neumann (2019) erläutert, wie sich im Bereich Security Awareness fast alle eingesetzten Maßnahmen auf das Training von System 2 fokussieren: Schulungsmaßnahmen sind auf das rationale Denksystem ausgerichtet und sollen durch Wissensvermittlung und Checklisten dem Nutzer eine Hilfestellung zum Erkennen riskanter Inhalte geben. Der Haken dabei ist, dass man sich im Kontext von Phishing-Angriffen nicht auf System 2 verlassen kann: Intuitive, schnelle und teils emotionale Handlungen (System 1-Denken) bestimmen häufig

das Verhalten in der konkreten Situation. Somit ist es unabdingbar, System 1 gegen Phishing-Angriffe abzusichern, d. h. intuitive Handlungen als Teil der Sicherheitsmechanismen zu antizipieren. Von organisatorischer Seite kann dies durch technische und prozessuale Maßnahmen unterstützt werden (siehe Abschn. 5). Der Nutzer selbst wird jedoch weiterhin in der Pflicht bleiben, sicherheitsbewusst zu handeln. Im Rahmen von Phishing kann dieses Verhalten neben konservativen Schulungsmaßnahmen wie beispielsweise E-Learning durch „Selbsterfahrung" trainiert werden. Die Erfahrung, als Nutzer selbst getäuscht oder „gehackt" zu werden, kann z. B. im Rahmen einer Phishing-Simulation stattfinden und dabei einen wichtigen „teachable moment" für einen Trainingseffekt in „System 1" bieten (Neumann 2019).

Verschiedene Forschungsbeiträge haben sich bisher in Form von Feldexperimenten dem Thema Phishing-Simulation gewidmet (beispielsweise (Wright und Marett 2010; Wright et al. 2014; Williams et al. 2018)), und hierbei den Einfluss von Beeinflussungsmechanismen oder Verhaltensfaktoren auf die Empfänglichkeit des Nutzers gegenüber Phishing-Angriffen untersucht. Dieser Beitrag geht einen Schritt weiter und präsentiert ein Feldexperiment, welches im organisatorischen Umfeld den Einsatz von Security Awareness-Trainingsmaßnahmen, speziell bezogen auf Spear Phishing, untersucht. Hierbei wurden Schulungsmaßnahmen zur Wissensvermittlung mit einer Phishing-Simulation zur „Selbsterfahrung" kombiniert. Weiterhin führen wir eine Kennzahl ein, welche Security Awareness in Organisationen standardisiert messbar macht.

4 Feldexperiment: Messen und Trainieren der Security Awareness im organisatorischen Umfeld

Die im Folgenden vorgestellten Daten wurden in Kooperation mit der IT-Seal GmbH, einem Anbieter für Spear Phishing-Simulationen und Security Awareness-Trainings, erhoben.

Abschn. 4.1 beschreibt das Projektziel und die Rahmenbedingungen. Die darauffolgende Präsentation von Methodik und Ergebnissen gliedert sich in zwei Teile. Teil I (Abschn. 4.2) konzentriert sich auf die Messung der Security Awareness, in Teil II (Abschn. 4.4) wird auf die eingesetzten Trainingsmaßnahmen und deren Wirkung eingegangen. Zur standardisierten Bewertung der Ergebnisse dient das Framework der Kennzahl „Employee Security Index", welches in Abschn. 4.3 eingeführt wird.

4.1 Projektziel und Rahmenbedingungen

Das Feldexperiment wurde über einen Zeitraum von sechs Monaten in einer deutschen Organisation mit ca. 500 Mitarbeitern durchgeführt (Roethke et al. 2020). Ziel des Projekts war es, die Security Awareness in der Organisation zu messen und zu steigern. Dafür wurden von IT-Seal etablierte Schulungsformate wie E-Learning und Präsenzschulungen in Kombination mit einer realitätsnahen Phishing-Simulation unter Nutzung des „teachable moments" eingesetzt: In dem Moment, in dem der

Nutzer durch Selbsterfahrung („ich werde gehackt“) auf das Risiko von sorglosem Umgang mit E-Mails aufmerksam wird, entsteht eine erhöhte Lernbereitschaft.

Die Testgruppe besteht aus 511 Mitarbeitern einer deutschen Organisation. Von den 511 Personen sind 58 % weiblich und 42 % männlich. Alle Mitarbeiter nutzen E-Mail als tägliches Kommunikationsmittel. Die Durchführung einer „Phishing Awareness-Maßnahme“ wurde innerhalb der Organisation ca. 3 Wochen vor Beginn des Projekts in Form eines Rundschreibens angekündigt. Um dem Mitarbeiter- und Datenschutz zu genügen, erfolgt die Auswertung der Messdaten auf Gruppenbasis mit einer Mindestgruppengröße von 30 Mitarbeitern.

4.2 Teil I: Messung der Verwundbarkeit gegenüber Spear Phishing-Angriffen

4.2.1 Methodisches Vorgehen: Spear Phishing-Simulation

Im Rahmen des Projekts standen je Mitarbeiter der Vor- und Nachname, die E-Mail-Adresse sowie Abteilung und Position in der Organisation zur Verfügung. Zusätzlich wurden von IT-Seal auf beruflich genutzten sozialen Netzwerken (Xing, LinkedIn)

Tab. 1 Beschreibung der Parameter, welche im Rahmen der Spear Phishing-Simulation genutzt oder angepasst wurden, um die Glaubwürdigkeit der simulierten E-Mails zu steigern

Parameter	Beschreibung	Beispiel
Anrede	Nutzung des Namens des Empfängers in der Anrede	Sehr geehrter Herr Mustermann/Hallo Max
Absender	Der Absender ist eine reale Person	Name eines Kollegen oder der Geschäftsführung
Domain	Die Domain eines enthaltenen Links oder der Absender-E-Mail-Adresse ist an den Empfänger angepasst, z. B. ist die Domain der Organisation mittels Nutzung eines Buchstabendrehers oder einer Subdomain nachgeahmt („spoofing“)	Cornelius.chef@musterfrima.de https://intern.musterfirma.de-index.info/
E-Mail-Signatur	Die E-Mail-Signatur des Absenders ist nachgeahmt	Die organisationsinterne E-Mail-Signatur wurde aus vorigem E-Mail-Verkehr oder von der Webseite übernommen
Geklontes Design	Die E-Mail enthält bekannte Logos oder Designs	E-Mail im nachgeahmten Design von Dropbox oder Amazon
Branchenkontext	Der Inhalt bezieht sich auf branchentypische Inhalte	Rückfrage einer Krankenkasse an einen Mitarbeiter eines Krankenhauses
Zeitlicher Kontext	Der Inhalt passt im zeitlichen Kontext	Weihnachtliche E-Grußkarte im Dezember
Bezug auf Fachbereich	Der Inhalt bezieht sich auf den Fachbereich des Empfängers	Bewerbungsschreiben an einen Mitarbeiter aus HR
Bezug auf Information aus Sozialen Medien	Der Inhalt bezieht sich auf eine vom Empfänger veröffentlichte Information	Anfrage mit Bezug auf ein Hobby, welches auf sozialen Netzwerken angegeben wurde, oder mit Bezug auf einen ehemaligen Arbeitgeber

sowie auf der Webseite der Organisation öffentlich verfügbare Informationen über Organisation und Mitarbeiter gesammelt (OSINT-Analyse).

Die Menge dieser Informationen wurde genutzt, um zielgerichtete Phishing-Angriffe zu simulieren. Über den Projektzeitraum von sechs Monaten erhielt dabei jeder Mitarbeiter 2–3 E-Mails pro Monat, wobei Inhalt und Zeitpunkt individuell waren. Die technische Zustellbarkeit der E-Mails wurde im Rahmen des Experiments durch ein Whitelisting des Absenderservers gewährleistet, sodass im Penetrationstest der Faktor Mensch isoliert betrachtet werden konnte.

Die Auswahl der simulierten Phishing-Szenarien reichte dabei von generischen Angriffsversuchen (z. B. „Ihr Postfach ist voll“) bis hin zu zielgerichteten Spear Phishing-Angriffen, welche einen oder mehrere der in Tab. 1 beschriebenen Parameter nutzten, um die Glaubwürdigkeit des E-Mail-Szenarios zu steigern. Insgesamt standen für die Simulation ca. 80 Szenarien-Templates zur Verfügung, welche automatisiert individuell an den Empfänger angepasst wurden.

Jede simulierte E-Mail enthielt einen Link oder Dateianhang, deren Öffnen über das Nachladen eines Tokens gemessen wurde. Parallel zur Phishing-Simulation wurden Schulungsangebote zum Thema Security Awareness ausgerollt (siehe Abschn. 4.4).

4.2.2 Ergebnisse: Beispiele simulierter Angriffe und deren Erfolgsraten

Im Folgenden sind beispielhaft drei der simulierten Phishing-Szenarien dargestellt. Abb. 1 zeigt eine generische Phishing-E-Mail, welche in dieser Form millionenfach versendet werden kann. Um der E-Mail Legitimität zu verleihen, wird in der Absender-Domain die Domain der Organisation nachgeahmt (hier beispielhaft verdeutlicht durch „@musterfrima.de“). Der Aufwand zur Vorbereitung einer solchen E-Mail beschränkt sich demnach im Wesentlichen auf das Registrieren einer entsprechenden Domain. Im Feldexperiment öffneten 26 % der Empfänger (14/53) den enthaltenen Link.

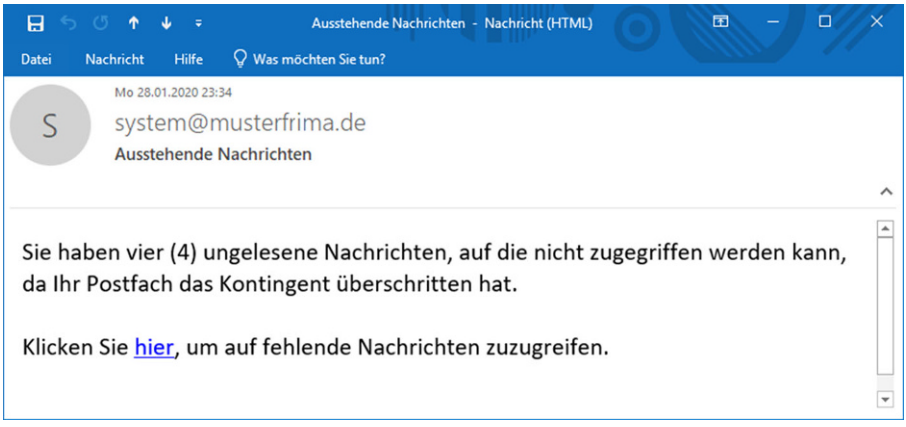

Abb. 1 Simulierte Phishing-E-Mail „Ausstehende Nachrichten“ (Quelle: IT-Seal GmbH)

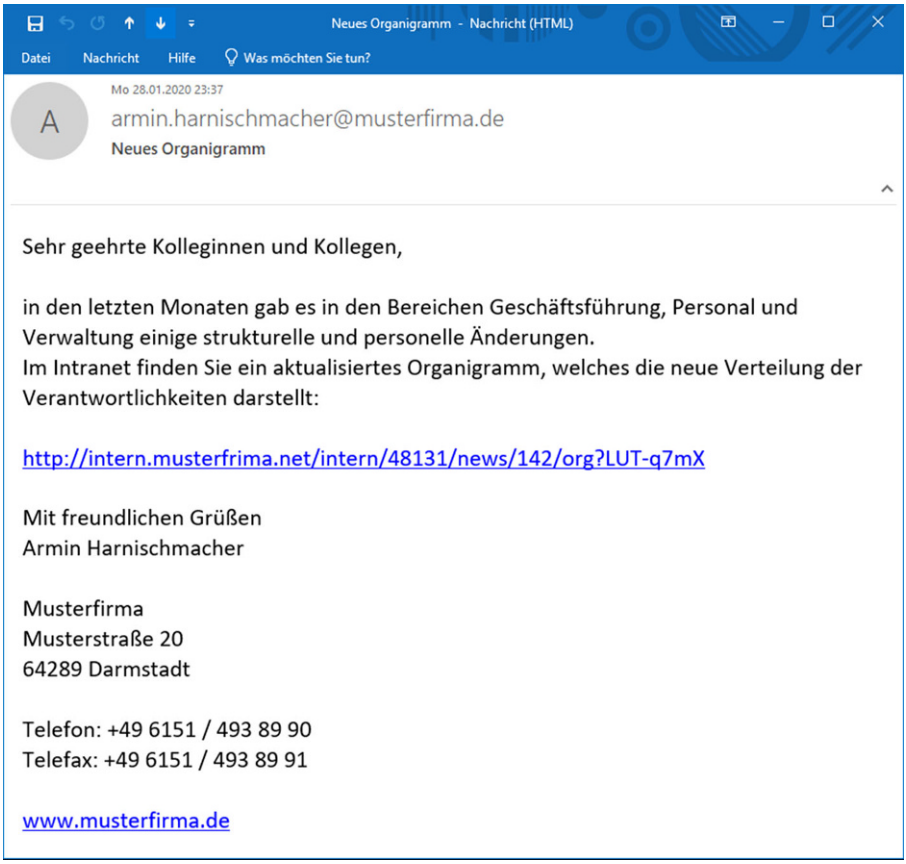

Abb. 2 Simulierte Phishing-E-Mail „Neues Organigramm“ (Quelle: IT-Seal GmbH)

In Abb. 2 ist ein Spear Phishing-Angriff dargestellt. Als Absendername wird der Name der Geschäftsführung genutzt, dieser lässt sich, wie auch die E-Mail-Signatur, ohne großen Aufwand auf der Webseite der angegriffenen Organisation finden und automatisiert verwenden. Der Link zeigt auf eine Domain, welche der Domain der angegriffenen Organisation täuschend echt nachgeahmt ist. Die E-Mail wurde 74 Mal versendet, der enthaltene Link wurde 33 Mal geöffnet (44 %).

Im dritten Beispiel (siehe Abb. 3) werden gezielt interne Strukturen ausgespäht und genutzt, um E-Mail-Verkehr zwischen Abteilungsleiter und Mitarbeiter zu fälschen. Der E-Mail hängt eine .docm-Datei an – hier ist bei realen Angriffen insbesondere das Öffnen das Makros mit einem sehr hohen Risiko verbunden. Im Experiment öffneten 23 % der Empfänger (23/98) den Dateianhang, 2 Empfänger aktivierten im Anschluss das Makro.

Die drei dargestellten Beispiele gehörten im durchgeführten Experiment zu den „erfolgreichsten“ Phishing-Szenarien.

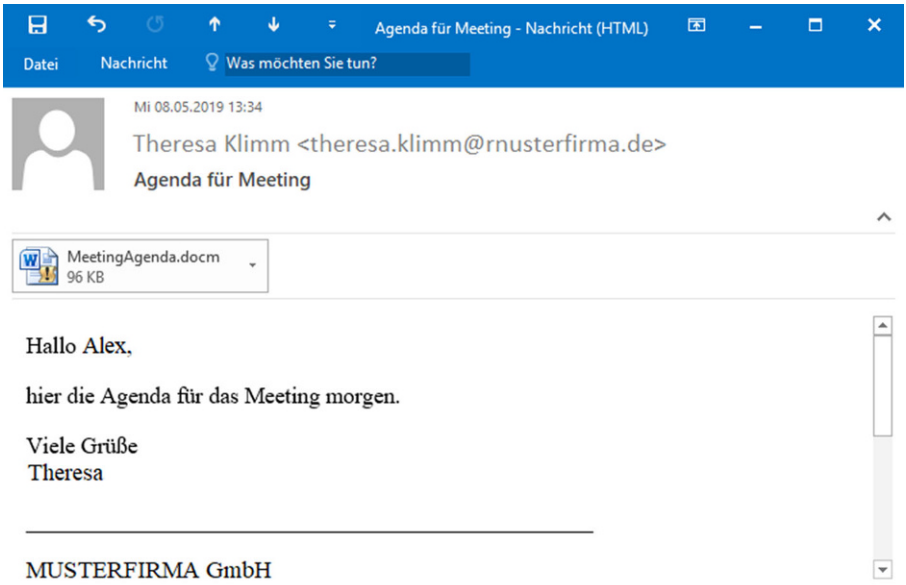

Abb. 3 Simulierte Phishing-E-Mail „Agenda für Meeting“ (Quelle: IT-Seal GmbH)

4.3 Einführung der Kennzahl „Employee Security Index“

Um die Ergebnisse einer solchen Phishing-Simulation vergleichbar zu machen, betrachten wir die gemessenen Klickraten im Framework des „Employee Security Index“ (ESI), welcher ein standardisiertes und reproduzierbares Verfahren zur Messung der Security Awareness darstellt (BSI 2019b). Wie in Abschn. 4.2.2 beispielhaft dargestellt, können sich Phishing-Angriffe bezüglich ihrer Qualität und ihres Vorbereitungsaufwands stark unterscheiden. Wir teilen daher Phishing-Angriffe in drei verschiedene Level ein (siehe Tab. 2), welche sich am Vorbereitungsaufwand orientieren. Neben der technischen Vorbereitung, dem Klonen bestehender Designs, dem Erstellen von Malware oder dem Registrieren nachgeahmter Domains wird hier insbesondere die Zeit zur Informationsbeschaffung berücksichtigt. Der Angreifende wird hierbei als professionalisierter Cyberkrimineller eingeordnet, um die tatsächliche Gefahrenlage für Unternehmen und Organisationen möglichst realitätsnah abzubilden.

Tab. 2 Klassifizierung von Phishing-Angriffen

Level	Zeitaufwand	Beispiel
1	Ca. 1 h	Wenig vorbereitete E-Mail in Unternehmenssprache (Beispiel siehe Abb. 1)
2	Ca. 3 h	Mäßig vorbereitete E-Mail, ggf. mit persönlicher Ansprache und Verwendung öffentlicher Informationen (Beispiel siehe Abb. 2)
3	Ca. 10 h	Angreifer übernimmt in der E-Mail die Rolle eines Kollegen oder Vertrauten des Empfängers (Beispiel siehe Abb. 3)

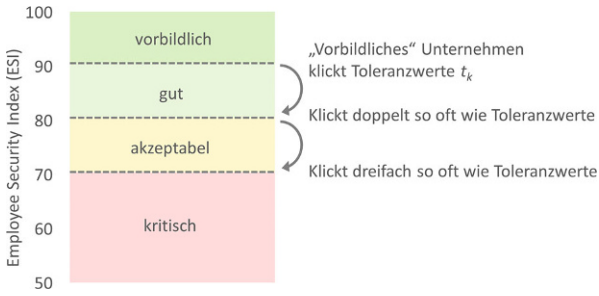

Abb. 4 Bewertungsskala des Employee Security Index (Quelle: IT-Seal GmbH)

Die Kennzahl „Employee Security Index" nutzt die Daten einer Phishing-Simulation, um das Sicherheitsverhalten von Mitarbeitern bewertbar und vergleichbar zu machen. Auf einer Skala von 0 bis 100 definiert sich eine fiktive „vorbildliche" Nutzergruppe durch das Erreichen einer 90. Unter der Annahme, dass bei Phishing-Angriffen auf Unternehmen oder Organisationen eine Klickrate von 0 % praktisch nicht erreichbar ist, definiert sich die „vorbildliche" Gruppe durch Toleranzwerte. Diese legen fest, welche Klickraten pro Level, d. h. pro für den Angriff aufgewendete Vorbereitungszeit, als ausreichend sicher bewertbar und dabei realistisch erreichbar sind. Der ESI berechnet sich für eine Testgruppe, z. B. Mitarbeiter einer Organisation, wie folgt:

$$ESI = \left(9 - \left(\frac{\sum_{k=1}^{3} A_L}{\sum_{k=1}^{3} n_L \cdot t_L} - 1\right)\right) \cdot 10$$

Hierbei ist n_L die Anzahl der simulierten Angriffe pro Level L, A_L die Anzahl der für dieses Level gemessenen Klicks und t_L der jeweils festgelegte Toleranzwert.

Der ESI macht eine Testgruppe mit der als „vorbildlich" definierten fiktiven Gruppe vergleichbar (siehe Abb. 4). Klickt die Testgruppe in einer vergleichbaren Simulation doppelt (dreifach) so oft wie die „vorbildliche" Gruppe, erreicht sie einen ESI von 80 (70). Die Skala ist unterteilt in die Bereiche „vorbildlich" (ESI ≥90), „gut" (ESI <90), „akzeptabel" (ESI <80) und „kritisch" (ESI <70). Der ESI findet seit 2018 Anwendung in Security Awareness-Projekten von IT-Seal. Basierend auf der Erfahrung mit kontinuierlichen Phishing-Trainings und dabei erreichtem Verhalten wurden die Toleranzwerte für einen ESI von 90 auf $t_1 = 1{,}7\,\%$, $t_2 = 4{,}1\,\%$ und $t_3 = 6{,}1\,\%$ Klickrate festgelegt.

Das Thema „Security Awareness" ist selbstverständlich sehr viel breiter und kann nicht alleine durch das Thema Phishing Awareness beschrieben werden. Letztere eignet sich durch die konkrete Messmöglichkeit im Rahmen einer Phishing-Simulation jedoch stark zur Ermittlung eines Vergleichswerts, und wurde daher als Grundlage eines solchen Index herangezogen. Die Ausweitung der Messung auf weitere Security Awareness-Bereiche bietet eine umfassendere Bewertung und sollte Teil weiterer Forschungsmaßnahmen sein.

4.4 Teil II: Messung der Wirksamkeit des Security Awareness-Trainings

4.4.1 Aufbau des Security Awareness-Trainings

Die in Abschn. 4.2 beschriebene Phishing-Simulation wurde als Teil eines Security Awareness-Trainings durchgeführt, welches aus drei Komponenten besteht.

a) Präsenzschulung

Vor Start der Phishing-Simulation absolvierte eine Auswahl von 100 der 511 Mitarbeiter eine ca. 90-minütige Präsenzschulung zum Thema „Phishing, Vishing, Human Hacking“. Hier wurden die Themen Social Engineering, (Spear) Phishing, E-Mail-Sicherheit, Soziale Medien und Passwortsicherheit behandelt, aus den Medien bekannte Vorfälle besprochen und anhand eines Live-Hackings gezeigt, wie ein Phishing-Angriff ablaufen kann. Die Zuordnung, welche Mitarbeiter die Präsenzschulung absolvierten, stand für die weitere Datenauswertung im Verlauf des Projekts nicht zur Verfügung.

b) E-Learning

Als zweite Komponente wurde mit Start der Phishing-Simulation organisationsweit ein E-Learning ausgerollt, welches die unter a) genannten Inhalte in einem 30-minütigen Web-Based Training behandelt. Das E-Learning zeigt unter anderem auf, welches Risiko Spear Phishing birgt, und was bei in E-Mails enthaltenen Links und Dateianhängen beachtet werden sollte. Die Bearbeitung des E-Learnings war freiwillig, es wurden nach dem initialen Roll-out über sechs Monate vier Erinnerungs-E-Mails versendet. Insgesamt haben 377 der 511 teilnehmenden Mitarbeiter (74 %) das E-Learning abgeschlossen. Sowohl E-Learning als auch die Präsenzschulung zielten auf das Training des System 2-Denkens ab.

c) Lernmoment im Rahmen der Phishing-Simulation

Als dritte Trainingskomponente diente die in Abschn. 4.2 beschriebene Spear Phishing-Simulation selbst. Diese bietet einerseits die Möglichkeit zur „Selbsterfahrung“ (das Gefühl, selbst „gehackt“ zu werden) und damit eine Schulung des System 1-Denkens. Andererseits kann der Moment, in dem ein Fehler passiert (z. B. ein Klick auf einen gefälschten Link, oder das Öffnen einer risikobehafteten Datei) als „teachable moment“ dienen, in dem eine besonders hohe Lernbereitschaft herrscht. Klickt ein Mitarbeiter auf einen in einer simulierten Phishing-E-Mail enthaltenen Link oder Dateianhang, so wird er zu einer interaktiven Lernseite weitergeleitet. Diese bietet am Beispiel der eben geöffneten E-Mail eine ca. einminütige Erklärung, wie die E-Mail als Phishing hätte enttarnt werden können. Besonderes Augenmerk liegt dabei auf dem Prüfen des Absenders der E-Mail sowie der Domain enthaltener Links, und der Vorsicht im Umgang mit Dateianhängen. Für alle Teilnehmer beginnt die Phishing-Simulation mit E-Mails des Schwierigkeitslevels 1 (siehe Tab. 2). Über den Projektzeitraum von sechs Monaten wird das Schwierigkeitslevel der E-Mails abhängig vom Klickverhalten des jeweiligen Mitarbeiters erhöht.

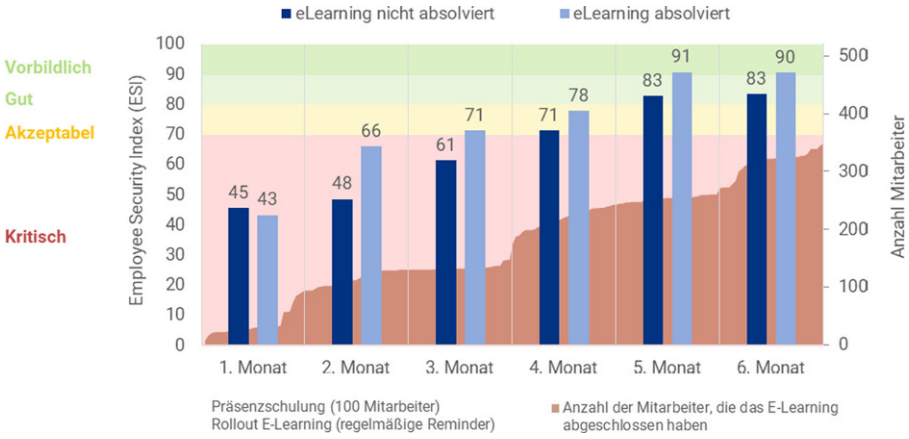

Abb. 5 Trainingsverlauf des sechsmonatigen Security Awareness-Trainings (Quelle: IT-Seal GmbH)

4.4.2 Entwicklung der Security Awareness im Trainingsverlauf

Abb. 5 zeigt das Verhalten der Mitarbeiter gegenüber simulierten Spear Phishing-Angriffen in Form der Kennzahl „Employee Security Index“ (siehe Abschn. 4.3). Der ESI wurde organisationsweit von einem Startwert von 44 über sechs Monate hinweg auf 89 gesteigert. Dabei schnitten Mitarbeiter, die das E-Learning absolviert haben, im Durchschnitt besser ab als ihre ungeschulten Kollegen. Der Anteil der Mitarbeiter, die das E-Learning-Angebot nutzten und das 30-minütige Training komplett absolvierten, lag am Ende des Trainingszeitraums bei 67 %. Auch bei den Mitarbeitern, die das E-Learning nicht absolviert haben, ist eine signifikante Steigerung des ESI messbar. Dies zeigt den Trainingseffekt der interaktiven Phishing-Simulation.

In diesem konkreten Fall wurde von Seiten der Organisation entschieden, nach einer 6 bis 12-monatigen Pause die Maßnahme zu wiederholen – um den Effekt der Selbsterfahrung im Rahmen der Phishing-Simulation präsent zu halten, und um auch neue Mitarbeiter thematisch abzuholen. Da diejenigen Teilnehmer, welche auch das E-Learning absolvierten, deutlich bessere Ergebnisse erzielten, bietet es sich an, das E-Learning in einem weiteren Durchgang als verpflichtend zu gestalten.

5 Implikationen für Forschung und Praxis

Aktuelle Cyber-Angriffe auf Unternehmen und Organisationen zeigen, dass insbesondere Spear Phishing eine ernstzunehmende Gefahr ist. Aufgrund steigender Automatisierung wird die Menge solcher Angriffe in den kommenden Jahren stark zunehmen, und dabei für Nutzer schwieriger zu erkennen sein. Die Schadsoftware Emotet ist dabei ein prominentes Beispiel, welches Ausmaß an Komplexität und Schaden diese Angriffsmuster mit sich bringen. Aus dem in Abschn. 4 beschriebe-

nen Feldexperiment lassen sich folgende Implikationen ableiten, wie die Sicherheit gegenüber Cyber-Angriffen auf den „Faktor Mensch“ gesteigert werden kann.

Multidimensionales Security Awareness-Training Während die Vermittlung eines gewissen Grund-Know-hows (im vorgestellten Projekt umgesetzt durch ein E-Learning und Präsenzschulungen) für Nutzer nach wie vor als sinnvoll angesehen wird, reicht dies allein nicht aus, um eine nachhaltige Verhaltensänderung im Umgang mit Phishing-Angriffen zu bewirken. Das in dieser Arbeit beschriebene Feldexperiment zeigt, dass in Kombination mit wiederholter Selbsterfahrung in Form einer Phishing-Simulation unter Nutzung des „teachable moments“ eine signifikante Verbesserung im Umgang mit Phishing-E-Mails erreicht werden kann. Um diese Art des Trainings durch Selbsterfahrung auch in anderen Bereichen der Security Awareness zu ermöglichen, sollten künftige Forschungsbemühen genau hier ansetzen und beispielsweise die Bereiche Passwortkultur oder Vishing (Telefon-Phishing) in den Fokus nehmen. Für ein anhaltend hohes Sicherheitsbewusstsein sollten solche Trainingsmaßnahmen regelmäßig durchgeführt werden.

Nutzung von Kennzahlen Zur Messung der Security Awareness in Organisationen kann eine Kennzahl wie der Employee Security Index (siehe Abschn. 4) dienen. Idealerweise wird eine solche Kennzahl zum kontinuierlichen Monitoring der Security Awareness im strategischen (Informationssicherheits-) Management etabliert. Sie macht dabei Handlungsbedarf bestenfalls in Echtzeit erkennbar und bietet gleichzeitig die Möglichkeit der einfachen Kommunikation sowie Rückschlüsse auf den Return on Investment von Security Awareness-Maßnahmen. Von Management-Seite wird diese Kennzahl erfahrungsgemäß gut angenommen: IT-Seal setzt bereits mit mehreren Organisationen ein kontinuierliches Awareness-Programm um, wobei für einzelne Nutzergruppen abhängig von deren Rolle im Unternehmen ein „Ziel-Employee Security Index“ festgelegt wird. Neben der Angriffssimulation werden dann weitere Schulungsmaßnahmen gezielt eingesetzt, um die Security Awareness auf den gewünschten Stand zu bringen und dort zu halten.

Aus wissenschaftlicher Sicht ist die Erweiterung des hier vorgestellten ESI-Frameworks auf weitere Aspekte der Security Awareness von Interesse, um neben Phishing auch andere Bereiche standardisiert bewerten zu können.

Neben den Implikationen, welche sich direkt aus dem vorgestellten Feldexperiment ableiten lassen, sind aus Sicht der Autoren folgende Handlungsempfehlungen unabdingbar für eine Absicherung von Organisationen gegenüber aktuellen Cyber-Angriffen.

Ausbau technischer und organisatorischer Schutzmaßnahmen Firewalls oder E-Mail-Filter sind mittlerweile gängige Maßnahmen im Kampf gegen Phishing, Malware und Co. Zusätzlich ist der Ausbau technologisch fortgeschrittener Schutzmaßnahmen, wie beispielsweise Advanced Threat Protection, stark zu empfehlen. Die bei Emotet-Angriffen häufig genutzten Makros stellen ein besonders hohes, und dabei schwierig zu bändigendes Sicherheitsrisiko dar. Makros können entweder organisationsweit deaktiviert oder nur mit digitaler Signatur erlaubt werden, um das Risiko einer Infektion mit Schadsoftware zu senken. Aus organisatorischer Sicht

bilden etablierte Schutzmaßnahmen wie ein defensives Berechtigungsmanagement sowie regelmäßige Backups und Updates aller verwendeter Software eine unverzichtbare Sicherheitsgrundlage.

Umdenken nutzerverbundener Prozesse Neben etablierten technischen und organisatorischen Schutzmaßnahmen sollten Prozesse so umgestaltet werden, dass intuitive Handlungen von Nutzern als Teil der Sicherheitsmechanismen antizipiert werden (siehe Abschn. 3, „schnelles und langsames Denken"). Dies bedeutet, dass Sicherheitsmaßnahmen bezüglich des „Faktor Mensch" nicht lediglich in der Wissensvermittlung bzw. regelbasiert stattfinden sollten, sondern prozessual so ausgelegt sein müssen, dass auch intuitive Handlungen sicher stattfinden können. Ideen zur Umsetzung solcher Prozesse sind beispielsweise das Umdenken von der Kultur selbst wählbarer Passwörter hin zu unterstützenden Sicherheitsmechanismen wie Zwei-Faktor-Authentisierung oder neuen Standards wie dem passwortfreien Login FIDO2, sowie der Einsatz unterstützender Tools, welche Links im E-Mail-Programm oder Browser für den Nutzer transparent machen. Ein gut gemachter Phishing-Angriff kann für den Empfänger eine Stresssituation darstellen. Das Einschränken herunterladbarer Software auf vertrauenswürdige Quellen führt dazu, dass der Nutzer trotz intuitiver Aktionen nicht direkt risikobehaftete Dateiformate wie z. B. .exe-Dateien ausführen kann.

Sicherheitskultur etablieren Zur wirklichen Umsetzung und Akzeptanz von Sicherheitsmaßnahmen gegenüber Spear Phishing in einer Organisation ist der Aufbau einer Sicherheitskultur unabdingbar. Dabei besteht die Herausforderung darin, ein potentiell negativ konnotiertes Thema (Informationssicherheit wird oft mit Angst, Frust oder Langeweile in Verbindung gebracht) für alle Mitarbeiter als relevant darzustellen und die Verantwortung des Einzelnen in der Unternehmenskultur zu verankern. Eine transparente und offene Kultur zum Umgang mit Fehlern ist dabei ebenso wichtig wie eine ausgeprägte Reporting-Kultur: Dringen neue Angriffe auf die Organisation schnell zur IT vor, kann hiervor gezielt gewarnt bzw. das Netzwerk technisch abgesichert werden. Gleichzeitig wird der Mitarbeiter aktiv in seiner Rolle als Mitverantwortlicher für Informationssicherheit eingebunden. Die dem Mitarbeiter zur Verfügung gestellte Meldekette sollte dabei möglichst schlank und aufwandsarm sein, am Beispiel von Phishing ist ein Melde-Button im E-Mail-Client denkbar. Weiterhin sind Ansätze in Richtung Gamification oder Belohnungssysteme vielversprechend, um diese sogenannten „extra-role behaviours" (Handlungen, die nicht in den eigentlichen Tätigkeitsbereich des Nutzers fallen), zu motivieren.

Zusammenfassend lässt sich festhalten, dass der Faktor Mensch in der Informationssicherheit auch in Zukunft eine entscheidende Rolle spielen wird. Informationssicherheitsverantwortliche stehen vor der Aufgabe, in der Belegschaft ein nachhaltiges Sicherheitsbewusstsein aufzubauen und gleichzeitig nutzerverbundene Prozesse so umzudenken, dass schwerwiegende Fehler seltener möglich sind. Nur so können sich Organisationen auch gegen die künftig steigende Anzahl automatisierter Cyberangriffe wappnen.

Funding Open Access funding enabled and organized by Projekt DEAL.

Literatur

APWG (2019) "Phishing Activity Trends Report". 3rd Quarter 2019. https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf. Zugegriffen: 13. Jan. 2020

Benlian (2020) A daily field investigation of technology-driven stress spillovers from work to home. MISQ (forthcoming)

Bitkom (2018) Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie. Studienbericht 2018, Bitkom e. V. https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf. Zugegriffen: 13. Jan. 2020

BSI (2019a) https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/Spam-Bundesbehoerden_181219.html. Zugegriffen: 13. Jan. 2020

BSI (2019b) Franz, A. "Security Awareness messbar machen – der Employee Security Index". Tagungsband des 16. Deutscher IT-Sicherheitskongress, 2019

Cloudmark (2016) Spear phishing: the secret weapon behind the worst cyber attacks

Heise (2019a) https://www.heise.de/newsticker/meldung/Computervirus-Klinikum-Fuerth-offline-und-mit-eingeschraenktem-Betrieb-4615427.html. Zugegriffen: 13. Jan. 2020

Heise (2019b) https://www.heise.de/newsticker/meldung/IT-Systeme-der-Stadt-Frankfurt-am-Main-wegen-Malware-Befall-offline-4619634.html. Zugegriffen: 13. Jan. 2020

Heise (2019c) https://www.heise.de/newsticker/meldung/Uni-Giessen-naehert-sich-nach-Hacker-Attacke-wieder-dem-Normalbetrieb-4628715.html. Zugegriffen: 13. Jan. 2020

Hertel (2015) Risiken der Industrie 4.0 – Eine Strukturierung von Bedrohungsszenarien der Smart Factory. HMD 52:724–738

ISF (2007) Information Security Forum. „ISF Standard of Good Practice 2007", CB3.4.

Kahneman (2011) Thinking, fast and slow. Farrar Straus, and Giroux, New York

Kruger, Kearney (2006) A prototype for assessing information security awareness. Comput Secur 25:289–296

Maedche et al (2011) AI-based digital assistants. Bus Inf Syst Eng 61(4):535–544

Neumann (2019) Hirne hacken – Menschliche Faktoren der IT Sicherheit. Vortrag auf dem 36. Chaos Communication Congress (36C3). (https://media.ccc.de/v/36c3-11175-hirne_hacken)

Pienta D, Thatcher JB, Johnston AC (2018) A taxonomy of Phishing: attack types spanning economic, temporal, breadth, and target boundaries. In: Proceedings of the 13th pre-ICIS workshop on information security and privacy, Bd. 1

Roethke K et al (2020) Social influence tactics in e-commerce onboarding: The role of social proof and reciprocity in affecting user registrations. Decis Support Syst 131:113268. https://doi.org/10.1016/j.dss.2020.113268

Symantec (2019) Internet security threat report Bd. 24

Williams EJ, Hinds J, Joinson AN (2018) Exploring susceptibility to phishing in the workplace. Int J Hum Comput Stud 120:1–13. https://doi.org/10.1016/j.ijhcs.2018.06.004

Wright RT, Marett K (2010) The influence of experiential and dispositional factors in phishing: an empirical investigation of the deceived. J Manag Inf Syst 27(1):273–303. https://doi.org/10.2753/MIS0742-1222270111

Wright RT, Jensen ML, Thatcher JB, Dinger M, Marett K (2014) Influence techniques in phishing attacks: an examination of vulnerability and resistance. Inf Syst Res 25(2):385–400