Peter Mayer, Fabian Ballreich, Reyhan Düzgün, Christian Schwartz, Melanie Volkamer

Erstellung von effektiven Sensibilisierungsmaterialien zur Passwortsicherheit

Die Verwendung sicherer Passwörter ist ein wichtiges Element jedes Informationssicherheitskonzepts. Daher hat eine effektive Sensibilisierung von Mitarbeitern für mögliche Angriffe auf Passwörter und die Vermittlung des für eine geeignete Passwortwahl erforderlichen Wissens eine große Bedeutung für Unternehmen. Der vorliegende Beitrag beschreibt einen iterativen Prozess zur Erstellung von effektiven Materialien für die Sensibilisierung von Mitarbeitern für Passwortsicherheit. Dessen Effektivität wurde durch eine Evaluierung der Materialien in drei mittelständischen Unternehmen überprüft. Die Evaluation zeigte, dass die teilnehmenden Mitarbeiter ihre Fähigkeit zur Erkennung von unsicherem passwortbezogenen Verhalten sowie der zutreffenden Einschätzung der Sicherheit von Passwörtern durch den Einsatz der Materialien signifikant verbessern konnten und diese signifiankte Verbesserung auch nach mehreren Monaten noch nachweisbar war.

1 Einleitung

Die Vergabe und Verwaltung sicherer Passwörter bereitet vielen Nutzern große Probleme [16, 27, 28], wodurch ein unsicheres Passwortverhalten begünstigt wird. Vielen Nutzern ist nicht bekannt, wie mögliche Angriffe funktionieren und wie man sich effektiv gegen sie verteidigen kann [27, 31]. Gleichzeitig stellen passwortbezogene Angriffe nach [32, 33] die häufigste Ursache für Sicherheitsvorfälle in Unternehmen dar: So lassen sich für das Jahr

2016 63%, für 2017 sogar 81% der Schadensfälle auf schwache oder entwendete Passwörter bzw. nicht geänderte Standardpasswörter zurückführen. Insbesondere das hierdurch entstehende Risiko eines finanziellen Schadens ist für ein Unternehmen von hoher Relevanz. So beträgt laut einer Studie[1] des Branchenverbandes Bitkom von 2019 der finanzielle Gesamtschaden in Folge von Sicherheitsvorfällen derzeit 102,9 Mrd. € jährlich. Die gleiche Studie zeigt, dass Angriffe auf Passwörter dabei den Spitzenplatz der erfolgreichen Angriffe einnehmen, noch vor Malware und Phishing. Folglich muss die Sensibilisierung der Mitarbeiter für mögliche Angriffswege auf Passwörter sowie effektive Schutzmaßnahmen für jedes Unternehmen in besonderem Maße Beachtung finden. Der beste Weg, um dies zu erreichen, ist die Erstellung geeigneter Schulungs- und Sensibilisierungsmaterialien [14, 19, 20, 35]. Jedoch zeigt sich insbesondere im Bereich der Passwortsicherheit, dass sich die Inhalte der vorhandenen Materialien nur schwerlich mit der Anwendungsrealität der Nutzer vereinbaren lassen. So kann sich die vermeintlich sinnvolle Vorgabe „*Nutzen Sie nur komplexe Passwörter, wechseln Sie diese häufig, schreiben Sie sie niemals nieder*" für den Nutzer problematisch erweisen [16, 27, 28]. Zudem widerspricht dieses Vorgehen dem Prinzip sinnvoller Sensibilisierung, wonach Nutzer in die Lage versetzt werden müssen, die Inhalte nachzuvollziehen und ihr erlangtes Wissen auf unterschiedliche Anwendungsszenarien ihres Alltags anwenden zu können [2, 21, 37].

Der vorliegende Beitrag beschreibt einen Prozess zur Erstellung von effektiven Materialien zur Sensibilisierung der Nutzer für verschiedenen Angriffe auf Passwörter und Benutzerkonten sowie über Schutzmaßnahmen gegen diese Angriffe. Dieser Prozess beinhaltet als initialen Schritt die Aggregierung relevanter Inhalte aus den Erkenntnissen der Forschung zu Passwortsicherheit. Daraufhin werden die Inhalte von unabhängigen Sicherheitsexperten aus Forschung und Industrie bewertet und deren Verbesserungsvorschläge eingearbeitet. Danach wird das Material von Laien getestet sowie die visuelle Gestaltung der Inhalte festgelegt. Zuletzt werden die hierdurch erstellten Materialien in drei mittelständischen Unternehmen hinsichtlich ihrer Effektivität evaluiert.

Die Ergebnisse der abschließenden Evaluation zeigen, dass die Materialien nicht nur als weitestgehend positiv und hilfreich empfunden wurden, sondern auch die Sicherheit der Unternehmen auf zwei Wegen verbessern konnten. Zum einen waren die Mitarbeiter in der Lage, ihre Fähigkeiten zur Erkennung von unsicherem, passwortbezogenem Verhalten deutlich zu verbessern. Zum anderen konnten sie nach dem Durcharbeiten der Materialien die Sicherheit von Passwörtern wesentlich zuverlässiger bewerten als zuvor. Eine wiederholte Untersuchung nach sechs Monaten zeigte zudem, dass diese Verbesserungen auch über diesen Zeitraum von mehreren Monaten erhalten bleiben.

Die verwendeten Materialien sind über das Internet frei abrufbar und können von Nutzern, Organisationen und Unternehmen jeglicher Art verwendet werden.[2]

2 Erstellung von Materialien zur Sensibilisierung

Materialien zur Sensibilisierung von Mitarbeitern für Gefahren und Risiken existieren in verschiedensten Formen (computerbasiert, textbasiert, unterrichtsbasiert etc.) mit unterschiedlichen Vor- und Nachteilen. Dieser Beitrag beschränkt sich auf die Erstellung von textbasierten Materialien, welche sich besonders gut für das zeitlich und räumlich flexible Selbststudium eignen. Im Folgenden werden die ersten drei Schritte des zuvor vorgestellten Prozesses beschrieben: das Aggregieren der Inhalte, das Einholen von Experten-Feedback sowie das Einholen von Laien-Feedback. Der letzte Schritt – die Evaluation der Effektivität der Materialien – wird danach in Abschnitt 3 beschrieben.

2.1 Aggregierung der Inhalte

Die Materialien wurden in drei Abschnitte unterteilt. Die ersten beiden Abschnitte geben einen Überblick darüber, (1) wer mögliche Angreifer sind und an welchen Stellen diese ansetzen können, sowie (2) welche Konsequenzen derartige Angriffe nach sich ziehen können. Im darauffolgenden Abschnitt (3) werden elf mögliche Angriffe im Detail beschrieben, wobei deren Auswahl auf Grundlage der Arbeit von Bonneau et al. [5] erfolgte. Bonneau et al. präsentieren in ihrer Arbeit eine Analyse unterschiedlicher Authentifikationsverfahren und vergleichen diese unter anderem anhand möglicher Angriffe. Zu jedem der elf Angriffe im Material werden passende Schutzmaßnahmen – wie beispielsweise der Einsatz von Passwortmanagern oder der Zwei-Faktor-Authentifizierung – vorgestellt. Hieran anschließend finden sich weiterführende Hinweise und speziellere Informationen zum jeweiligen Angriff, die interessierten Nutzern eine weitere Vertiefung erlauben oder nur bestimmte Nutzergruppen betreffen.

Bei der Erstellung der Materialien wurde auf eine möglichst positive Formulierung sowie die Vermeidung technischer Fachbegriffe geachtet. Insbesondere wurde das Prinzip des „intellectual need" eingehalten, welches besagt, dass Lernen deutlich einfacher fällt und nachhaltiger ist, wenn die Lernenden zuerst das Problem verstanden haben und dadurch intrinsisch motiviert sind, die Lösung zu diesem Problem zu erfahren und nachzuvollziehen. Im Fall der Sensibilisierungsmaterialien wird also erst erläutert, welcher Schaden wie entstehen kann (das Problem), und dann die Schutzmaßnahme (die Lösung) vorgestellt. Die Reihenfolge der elf in den Materialien beschriebenen Angriffe orientieren sich an der Entfernung zum Nutzer, d. h. sie beginnt bei Angriffen auf den Nutzer selbst bzw. des Nutzergeräts und endet bei Angriffen auf Webdienste.

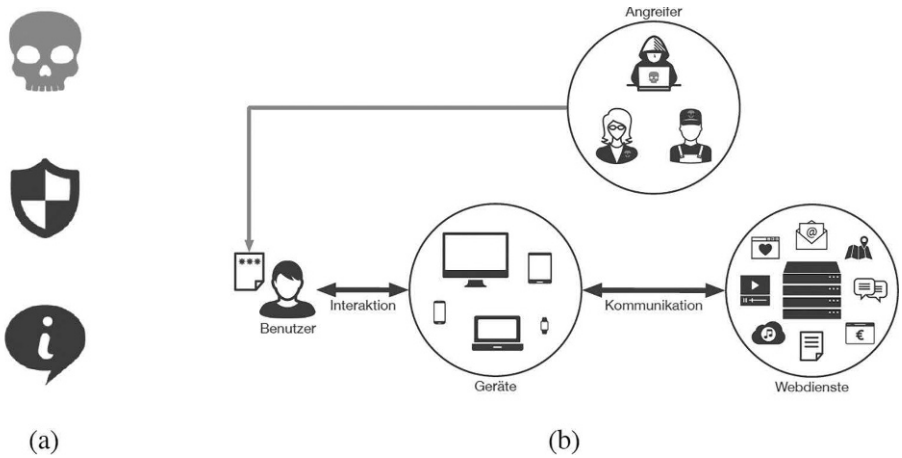
2.2 Feedback von Experten

Um die Korrektheit und Vollständigkeit der erstellten Materialien sicherzustellen, wurde diesbezügliches Feedback von 13 Sicherheitsexperten eingeholt. Hierbei handelt es sich um einschlägige Experten aus dem Bereich der Forschung (3x), der Beratung (4x) sowie von Wirtschaftsunternehmen (6x). Neben verschiedenen inhaltlichen Änderungen wurden durch die Experten ebenfalls detailliertere Beschreibungen der konkreten Konsequenzen möglicher Angriffe angeregt.

1 https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019_0.pdf

2 https://secuso.org/passwortsicherheit

Abb. 1 | Visuelle Gestaltungselemente: (a) Icons zur Gliederung des Inhalts (Totenkopf: Angriffsbeschreibung, Schutzschild: Schutzmaßnahmen, Sprechblase: Weitere Informationen) (b) Grafische Darstellung eines Angriffes (hier: Diebstahl eines niedergeschriebenen Passworts)



2.3 Feedback von Laien

Im dritten Schritt wurden die Beschreibungen mit visuellen Elementen ergänzt. Anschließend wurden die Materialien mit Laien aus dem universitären Umfeld getestet. Zur Verbesserung der Materialien wurden geringfügige Änderungen, wie z. B. die Darstellung von Icons (Abb. 1) zur besseren inhaltlichen Orientierung, vorgenommen.

3 Evaluation der Materialien

Im vierten und letzten Schritt des Prozesses – der Evaluierung der Effektivität der Materialien – wurde eine Nutzerstudie durchgeführt. Dabei wurde insbesondere die Effektivität der Materialien im Hinblick auf die Vermittlung von Angriffen und Schutzmaßnahmen bewertet.

3.1 Studiendesign

Die Studie umfasste insgesamt 90 Teilnehmer aus drei deutschen kleinen und mittleren Unternehmen (sog. KMU). Die Auswahl der Teilnehmer sowie die Abwicklung der Studie wurde durch eine Kontaktperson intern in den jeweiligen Unternehmen durchgeführt, wodurch die Anonymität der Teilnehmenden gewahrt werden konnte. Bei der Auswahl geeigneter Teilnehmer sollten ausschließlich Laien berücksichtigt werden, die nicht über einschlägiges Wissen oder ausgeprägte Erfahrung im untersuchten Bereich verfügen.

Der Studienablauf lässt sich in vier Abschnitte gliedern: Zur Einschätzung des Ist-Zustands füllen alle Teilnehmer zu Beginn der Studie einen Vor-Fragebogen (Pre) aus. Im Anschluss erhalten Sie die erstellten Materialien, die sie – zeitlich und räumlich flexibel – selbstständig durcharbeiten können. Anschließend wird die erzielte Wirkung mittels eines weiteren Nach-Fragebogens (Post) untersucht. Nach einem Zeitraum von sechs Monaten wird mittels eines weiteren Überprüfungs-Fragebogens (Retention) die langfristige Wirkung der Materialien geprüft. Die Retention-Untersuchung nach sechs Monaten war lediglich in einem der drei Unternehmen möglich.

3.2 Fragebogen

Die Gestaltung und Inhalte der drei verwendeten Fragebögen (Pre, Post und Retention) sind identisch, variieren jedoch hinsichtlich des Umfangs der Fragen.

Im ersten Teil der Befragung werden den Teilnehmern unterschiedliche Anwendungsszenarien beschrieben, wobei für jeden der elf Angriffe jeweils zwei Szenarien erstellt wurden. Das Verhalten in jedem Szenario muss durch die Teilnehmer als *sicher* oder *unsicher* klassifiziert werden, wobei die Entscheidung

Abb. 2 | Ergebnisse der ersten beiden Fragebögen (Pre, Post). (a) Verteilung korrekter Bewertungen der Szenarien (b) Beurteilung der Passwortsicherheit

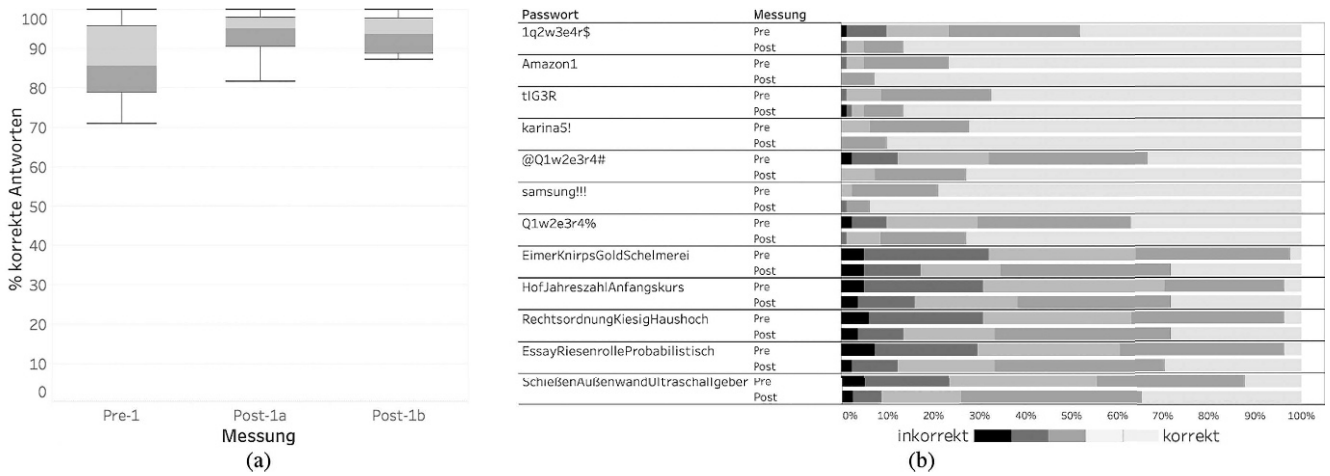
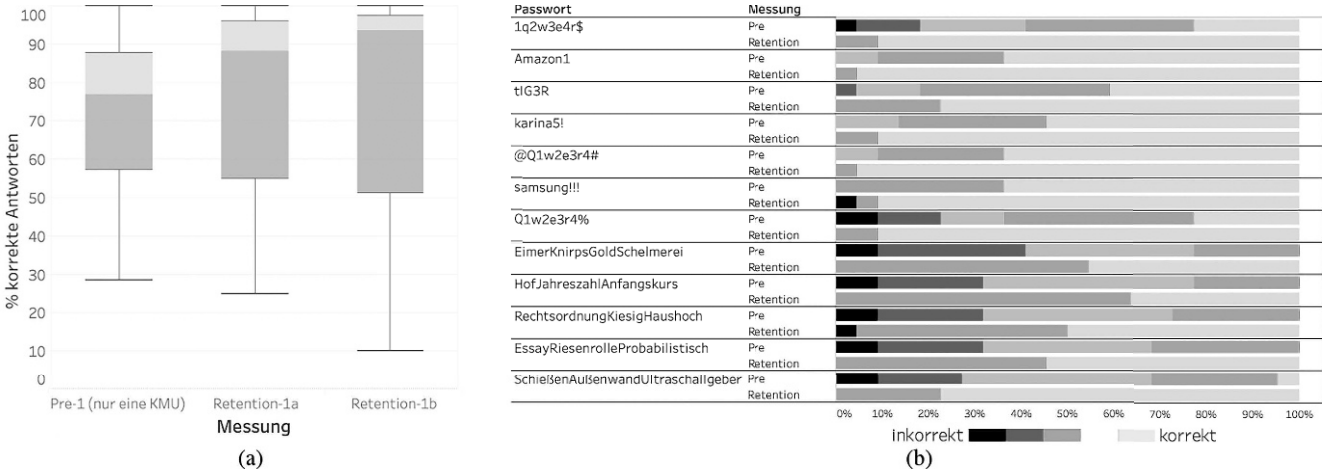


Abb. 3 | Ergebnisse des dritten (Retention) im Vergleich zum ersten Fragebogen (Pre). (a) Verteilung korrekter Bewertungen der Szenarien (b) Beurteilung der Passwortsicherheit



in einem Freitextfeld begründbar ist. Abweichend von Post- und Retention-Test, in denen jeweils alle 22 Szenarien gezeigt wurden, enthielt der initiale Fragebogen (Pre) nur elf zufällig ausgewählte Szenarien.

Im zweiten Teil werden die Teilnehmer aufgefordert, die Sicherheit von zwölf Passwörtern anhand einer Fünf-Punkte-Likert Skala (*sehr sicher* bis *sehr unsicher*) zu bewerten. Von den vorgestellten Passwörtern sind sieben mittels entsprechender Standardsoft ware in wenigen Sekunden (unsichere Passwörter) bzw. fünf nicht in verhältnismäßiger Zeit (sichere Passwörter) erratbar.

Im dritten Teil werden die Teilnehmer gebeten, demografi sche Angaben (Alter, Geschlecht) zu machen sowie Feedback zum Studiendesign und den Materialien zu geben, wobei diese Angaben optional sind. Dieser Teil ist lediglich im zweiten Fragebogen (Post) enthalten.

3.3 Ergebnisse

Von der Auswertung der Szenarien mussten sechs Teilnehmer ausgeschlossen werden, da aus ihren Freitextantworten in den Fragebögen auf ein umfangreiches Wissen im untersuchten Bereich geschlossen werden konnte. Die Zahl der gültigen Teilnehmer belief sich daher auf 84, bestehend aus 56 Männern, 27 Frauen und *keine Angabe* in einem Fall. Die Altersverteilung erstreckte sich von 19 bis 43 Jahre, wobei das durchschnittliche Alter bei 30 Jahren mit einer Standardabweichung von 5,4 Jahren lag. Bei der Bewertung der Passwortsicherheit mussten aufgrund unvollständiger Angaben weitere drei Teilnehmer von der Auswertung ausgeschlossen werden.

Unterschiede von Pre zu Post

Die Teilnehmer zeigten bereits vor dem Studium der Materialien bei der Bewertung der Szenarien mit 88,2% eine hohe Häufi gkeit korrekter Antworten. Für die elf Szenarien, die in beiden Fragebögen (Pre, Post) enthalten waren, konnte die Erfolgsquote auf 93,3% gesteigert werden. Das Durcharbeiten der Materialien führt folglich zu einer signifik anten Verbesserung der Fähigkeiten, sicheres und unsicheres passwortbezogenes Verhalten zu unterscheiden. Für die elf Szenarien, die nur im zweiten Fragebogen (Post) enthalten waren, lag die gemessene Verbesserung unterhalb des statistischen Signifikanzniveaus. Folglich konnte die Annahme einer signifikanten Verbesserung der Fähigkeiten in Bezug auf unbekannte Szenarien (Wissenstransfer) nicht gestützt werden.

Die Teilnehmer klassifizierten bereits im ersten Fragebogen (Pre) einen hohen Anteil der unsicheren Passwörter korrekt. Gleichzeitig wurde die Sicherheit der sicheren Passwörter in vielen Fällen inkorrekt bewertet. Die Auswertung des zweiten Fragebogens (Post) zeigte, dass sich durch die Materialien die Fähigkeiten zur Unterscheidung von sicheren und unsicheren Passwörtern signifikant verbesserten (Abb. 2).

Das freiwillige Feedback aus dem zweiten Fragebogen (Post) fiel allgemein sehr positiv aus. 90,6% der Befragten empfanden die Materialien als relevant und hilfreich, wobei sie in sechs Fällen als zu lang bewertet wurden. Besonders häufig wurden die Inhalte zu den Themen Passwortmanager und Passworterstellung positiv hervorgehoben, wobei jedoch auch rund 20% der Befragten erhofften, hierzu noch konkretere Informationen zu erhalten. In etwa 20% der Fälle gaben die Teilnehmer an, in Zukunft einen Passwortmanager nutzen zu wollen. Lediglich 9% erkannten keine Auswirkung auf ihr zukünftiges passwortbezogenes Verhalten.

Unterschiede Pre zu Retention

In einem Unternehmen war zudem die erneute Befragung der Teilnehmer mittels des dritten Fragebogens (Retention) nach sechs Monaten möglich. Die Zahl der gültigen Teilnehmer belief sich hierbei auf 26, bestehend aus 16 Männern, 9 Frauen und *keine Angabe* in einem Fall. Die Altersverteilung erstreckte sich von 19 bis 43 Jahre, wobei das durchschnittliche Alter mit 32,2 Jahren bei einer Standardabweichung von 5,5 Jahren lag. Bei der Bewertung der Passwortsicherheit mussten aufgrund unvollständiger Angaben wieder drei Teilnehmer ausgeschlossen werden.

Hinsichtlich der Beurteilung der Szenarien während der ersten beiden Fragebögen (Pre, Post) unterscheiden sich die Ergebnisse der Teilnehmer dieses einen Unternehmens nicht signifikant von denen der anderen beiden Unternehmen. Die Ergebnisse des Retention-Fragebogens zeigen, dass die Teilnehmer die Verbesserung der Fähigkeiten, sicheres und unsicheres passwortbezogenes Verhalten zu unterscheiden, auch nach sechs Monaten aufrecht erhielten. Die Verbesserung ist hierbei sowohl für die elf Szena-

rien aus dem ersten Fragebogen (Pre) als auch für die restlichen elf Szenarien signifikant.

Bei der Bewertung der Passwortsicherheit im ersten Fragebogen (Pre) schnitten die Mitarbeiter des Unternehmens, welches an der Retention teilnahm, im Vergleich zu den Teilnehmern der anderen beiden Unternehmen signifikant schlechter ab. Die Auswertung des dritten Fragebogens (Retention) hat hingegen eine signifikante Verbesserung gezeigt (Abb. 3).

3.4 Beschränkungen

Die Ergebnisse dieser Studie unterliegen externen sowie konzeptbedingten Beschränkungen. So wurden die Teilnehmer während der Studie nicht unmittelbar überwacht, wodurch beispielsweise die Nutzung anderer Informationsquellen und Hilfsmittel nicht ausgeschlossen ist. Da die Auswahl der Teilnehmer durch eine unternehmensinterne Kontaktperson durchgeführt wurde, war die tatsächliche Eignung als Laie nur bedingt kontrollierbar. Außerdem beschränkte sich die durchgeführte Studie auf deutschsprachige Teilnehmer aus kleinen und mittleren Unternehmen in Deutschland. Darüber hinaus konnte der dritte Fragebogen (Retention) nur in einem der drei Unternehmen eingesetzt werden.

4 Fazit

In diesem Beitrag wurde ein neuer, systematischer Ansatz zur Erstellung von Materialien zur effektiven Sensibilisierung von Laien für Angriffe auf Passwörter und Nutzerkonten sowie entsprechende Schutzmaßnahmen vorgestellt. Der zugrundeliegende Prozess setzt hierzu auf die Aggregierung von Forschungsergebnissen der Passwortsicherheit sowie die Bewertung der Materialien durch unabhängige Experten aus Wirtschaft und Wissenschaft sowie Laien. Mit Hilfe der durchgeführten Evaluation ließ sich zeigen, dass das Durcharbeiten der Materialien zu einer signifikanten Verbesserung der Fähigkeiten zur Einschätzung passwortbezogenen Verhaltens sowie der Sicherheitsbeurteilung von Passwörtern führt und somit wohlinvestierte Zeit durch Mitarbeiter darstellt. Die Materialien wurden zudem durch die Teilnehmer weitestgehend positiv aufgenommen. Darüber hinaus hat das Feedback der Teilnehmer weitere Forschungsansätze angeregt, beispielsweise einen stärkeren Fokus auf Passwortmanager und Passworterstellung zu legen. Des Weiteren lassen sich der in diesem Beitrag beschriebene Prozess und die gewonnen Erkenntnisse mit geringem Aufwand auf andere Kontexte der IT-Sicherheit übertragen und dort anwenden.

Danksagung

Wir danken allen Teilnehmern und Experten für ihre Beteiligung. Diese Arbeit ist an der Technischen Universität Darmstadt im Rahmen des Projekts KMU AWARE entstanden. KMU AWARE wird im Rahmen der Initiative *IT-Sicherheit in der Wirtschaft* vom Bundesministerium für Wirtschaft und Energie gefördert. Diese Arbeit wurde darüber hinaus durch das Kompetenzzentrum für angewandte Sicherheitstechnologie (KASTEL) vom Bundesministerium für Bildung und Forschung unterstützt.

Literatur

[1] Apple Inc. *Face ID Security*. Tech. rep., 2017.

[2] Bada, M., and Sasse, A. *Cyber Security Awareness Campaigns – Why do they fail to change behaviour?* Tech. rep., July 2014.

[3] Bock, C. *Fujitsu and Microsoft focused on advancing security in the modern workplace*, 2018.

[4] Bonneau, J., Bursztein, E., Caron, I., Jackson, R., and Williamson, M. *Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google*. In International Conference on World Wide Web (2015), pp. 141–150.

[5] Bonneau, J., Herley, C., van Oorschot, P. C., and Stajano, F. *The quest to replace passwords: A framework for comparative evaluation of web authentication schemes*. In IEEE Symposium on Security and Privacy (2012), pp. 553–567.

[6] Bonneau, J., Just, M., and Matthews, G. *What's in a Name?* In International Conference on Financial Cryptography and Data Security (2010), pp. 98–113.

[7] Bulgurcu, B., Cavusoglu, H., and Benbasat, I. *Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness*. MIS quarterly (2010).

[8] Burnett, M. *Today I Am Releasing Ten Million Passwords*, Feb. 2015.

[9] Cohen, J. *Statistical power analysis for the behavioral sciences* (2nd ed.). Academic Press (1988).

[10] Eminagaoglu, M., Uçar, E., and Eren, S. *The positive outcomes of information security awareness training in companies – A case study*. Information Security Technical Report 14, 4 (Nov. 2009), 223–229.

[11] Florêncio, D., Herley, C., and van Oorschot, P. C. *An Administrator's Guide to Internet Password Research*. In Large Installation System Administration Conference (2014), pp. 35–52.

[12] Fuller, E., Rabin, J. M., and Harel, G. *Intellectual Need and Problem-Free Activity in the Mathematics Classroom*. International Journal for Studies in Mathematics Education 4, 1 (2011), 80–114.

[13] Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richter, J. P., Lefkovitz, N. B., Danker, J. M., Choong, Y.-Y., Greene, K. K., and Theofanos, M. F. *Digital Identity Guidelines: Authentication and Lifecycle Management*. Tech. rep., June 2017.

[14] Haeussinger, F., and Kranz, J. *Antecedents of Employees' Information Security Awareness – Review, Synthesis, and Directions for Future Research*. In European Conference on Information Systems (July 2017), pp. 1–20.

[15] Hänsch, N., and Benenson, Z. *Specifying IT Security Awareness*. Database and Expert Systems Applications (DEXA), 2014 25th International Workshop on (2014), 326–330.

[16] Inglesant, P. G., and Sasse, M. A. *The true cost of unusable password policies*. In Conference on Human Factors in Computing Systems (2010), pp. 383–392.

[17] Ion, I., Reeder, R., and Consolvo, S. *"...no one can hack my mind": Comparing Expert and Non-Expert Security Practices*. In Symposium on Usable Privacy and Security (2015), pp. 327–346.

[18] Kajtazi, M., and Bulgurcu, B. *Information Security Policy Compliance: An Empirical Study on Escalation of Commitment*. In Americas Conference on Information Systems (2013).

[19] Lebek, B., Uffen, J., Neumann, M., Hohler, B., and Breitner, M. H. *Information security awareness and behavior: a theory-based literature review*. Management Research Review 37, 12 (2014), 1049–1092.

[20] Lin, C., and Kunnathur, A. S. *Toward Developing a Theory of End User Information Security Competence*. In Americas Conference on Information Systems (2013), pp. 1–10.

[21] Murray, H., and Malone, D. *Evaluating password advice*. In Irish Signals and Systems Conference (2017).

[22] Neumann, S., Reinheimer, B., and Volkamer, M. *Don't Be Deceived: The Message Might Be Fake*. In International Conference on Trust and Privacy in Digital Business (2017), pp. 199–214.

[23] Ögütçü, G., Testik, Ö. M., and Chouseinoglou, O. *Analysis of personal information security behavior and awareness*. Computers & Security 56 (Feb. 2016), 83–93.

[24] PCI Security Standards Council LLC. *Payment Card Industry (PCI) Data Security Standard* (Version 3.2), Apr. 2016.

[26] Safa, N. S., Sookhak, M., von Solms, R., Furnell, S., Ghani, N. A., and Herawan, T. *Information security conscious care behaviour formation in organizations*. Computers & Security 53 (2015), 65–78.

[27] Stobert, E., and Biddle, R. *The Password Life Cycle: User Behaviour in Managing Passwords*. In Symposium on Usable Privacy and Security (2014), pp. 243–255.

[28] Stobert, E., and Biddle, R. *Expert Password Management*. In International Conference on Passwords (2015), pp. 3–20.

[29] Stockhardt, S., Reinheimer, B., Volkamer, M., Mayer, P., Kunz, A., Rack, P., and Lehmann, D. *Teaching Phishing-Security: Which Way is Best?* In ICT Systems Security and Privacy Protection. 2016, pp. 135–149.

[30] Tsohou, A., Karyda, M., and Kokolakis, S. *Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs*. Computers & Security 52 (July 2015), 128–141.

[31] Ur, B., Noma, F., Bees, J., Segreti, S. M., Shay, R., Bauer, L., Christin, N., and Cranor, L. F. *"Added 'I' at the End to Make It Secure": Observing Password Creation in the Lab*. In Symposium on Usable Privacy and Security (2015), pp. 123–140.

[32] Verizon. *2016 Data Breach Investigations Report*. Tech. rep., 2016.

[33] Verizon. *2017 Data Breach Investigations Report*. Tech. rep., 2017.

[34] Volkamer, M., Renaud, K., Reinheimer, B. M., Rack, P., Ghiglieri, M., Mayer, P., Kunz, A., and Gerber, N. *Phishing detection: Developing and evaluating a five minutes security awareness video* [in press]. In Proceedings of the 15th International Conference on Trust, Privacy and Security in Digital Business – TrustBus 2018, Regensburg, 5.-6. September 2018 (2018).

[35] Wilson, M., and Hash, J. *Building an Information Technology Security Awareness and Training Program*. Tech. Rep. 800-50, National Institute of Standards and Technology, Oct. 2003.

[36] Zhang-Kennedy, L., Chiasson, S., and Biddle, R. *Password advice shouldn't be boring: Visualizing password guessing attacks*. In eCrime Researchers Summit (2013).

[37] Zhang-Kennedy, L., Chiasson, S., and van Oorschot, P. *Revisiting Password Rules: Facilitating Human Management of Passwords*. In APWG Symposium on Electronic Crime Research (2016).