Security Awareness: Nicht nur schulen – überzeugen Sie!

Andreas Schütz · Kristin Weber

Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt
{andreas.schuetz | kristin.weber}@fhws.de

Zusammenfassung

Im Zeitalter der Digitalisierung steigt die Bedeutung von Informationen und Informationstechnik und damit auch die der Informationssicherheit. Der Mensch rückt stärker in den Fokus der Angreifer und muss daher umfassend über seine Rolle für die Informationssicherheit aufgeklärt werden. Maßnahmen zur Sensibilisierung von Mitarbeitern (auch „Security Awareness“) beschränken sich häufig auf die Vermittlung von Wissen über informationssicherheitskonformes Verhalten. Mitarbeiter müssen aber auch dazu motiviert werden, dieses Wissen situationsbedingt anzuwenden und sie müssen die passenden Rahmenbedingungen im Unternehmen vorfinden. Das *Integrierte Verhaltensmodell* (IBM – Integrated Behavior Model) aus der Disziplin Sozialpsychologie erklärt, welche Faktoren einen Menschen dazu bringen, ein bestimmtes Verhalten zu zeigen. Neben dem Wissen gehören zu diesen Faktoren z.B. die Verhaltensabsicht, die Gewohnheit oder Einschränkungen aus dem Umfeld. Diese Arbeit wendet das IBM auf den Kontext Informationssicherheit an. Sie zeigt, welches komplexe Zusammenspiel mehrerer Faktoren das informationssicherheitskonforme Verhalten eines Mitarbeiters bestimmt und mit welchen Werkzeugen Unternehmen gezielt auf einzelne Faktoren eingehen können. Das Ziel ist es, Unternehmen zu befähigen, ihre Mitarbeiter tatsächlich für Informationssicherheit zu sensibilisieren und nicht nur Wissen zu vermitteln.

1 Motivation

Digitalisierte Prozesse und digitale Geschäftsmodelle werden für Unternehmen zunehmend wichtiger, um Wettbewerbsvorteile zu erhalten und auszubauen. Digitalisierung bietet Chancen, birgt aber auch neue Risiken. Mit der zunehmenden Nutzung von Informationstechnik in Unternehmen steigen die Ansprüche an die Informationssicherheit. Technische Sicherheitsmaßnahmen helfen nur begrenzt die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten. Der „Faktor Mensch“ wird inzwischen als größtes Angriffsrisiko gesehen, und als „Schwachstelle“ gezielt durch Phishing, Malware oder Social Engineering ausgenutzt [ISAC16].

Bei der Eröffnung der Messe für Informationstechnik CeBIT im März 2017 forderte die deutsche Bundeskanzlerin Angela Merkel dazu auf, die Menschen in das neue Zeitalter der Digitalisierung mitzunehmen [Zeit17]. Mitarbeiter können durch gezielte Sensibilisierung im Unternehmen von einer Schwachstelle zu einer Stütze des Informationssicherheitskonzeptes werden [ScPi15] und so die digitale Strategie des Unternehmens mittragen. Sensibilisierungsmaßnahmen sollen bei den Mitarbeitern, die mit schützenwerten Informationen konfrontiert sind, Achtsamkeit schaffen und sie zu einem sicherheitskonformen Verhalten am Arbeitsplatz motivieren. Für diese Achtsamkeit hat sich der Begriff „Security Awareness“ etabliert.

P. Schartner · A. Baumann (Hrsg.) · D•A•CH Security 2017 · syssec (2017) 1-12.

Aktuell zielen Sensibilisierungsmaßnahmen häufig auf die Vermittlung von Wissen zur Informationssicherheit ab [Alli16]. Erkenntnisse aus der Sozial- und Gesundheitspsychologie zeigen jedoch, dass das Verhalten eines Menschen neben seinem Wissen aus einem komplexen Geflecht verschiedener Faktoren bestimmt wird. Ein Mitarbeiter weiß beispielsweise, dass das Verwenden von fremden USB-Sticks zur Installation von Malware auf dem Firmencomputer führen kann. Dies bedeutet aber im Umkehrschluss nicht, dass er dieses Verhalten unterlässt. Gründe hierfür gibt es viele: Der Mitarbeiter schätzt das Risiko geringer ein als es tatsächlich ist, er hat ansonsten keine Möglichkeit Daten auszutauschen oder er beobachtet, dass andere Mitarbeiter ebenfalls USB-Sticks verwenden.

Diese Arbeit untersucht, wie Unternehmen ihre Mitarbeiter wirklich für ein informationssicherheitskonformes Verhalten sensibilisieren können. Mit einer explorativen Vorgehensweise werden hierfür Erkenntnisse der Sozial- und Gesundheitspsychologie untersucht. Das *Integrierte Verhaltensmodell* (IBM) [MoKa08] gibt Aufschluss über die Faktoren, die das sicherheitskonforme Verhalten einer Person beeinflussen. Es werden Vorschläge für Werkzeuge erarbeitet, mit welchen ein Unternehmen diese Faktoren gezielt beeinflussen kann.

Der Rest der Arbeit ist wie folgt strukturiert. Das nächste Kapitel führt in die Themenbereiche Security Awareness und Sozialpsychologie ein. Kapitel 3 stellt das IBM und die Faktoren vor, die menschliches Verhalten beeinflussen. Anschließend beschreibt die Arbeit, wie die Kenntnis dieser Faktoren hilft, gezielte Sensibilisierungsmaßnahmen zu erstellen. Werkzeuge, die auf das Verhalten der Mitarbeiter einwirken können, werden dargestellt und wie diese am effektivsten verwendet werden können. Das abschließende Kapitel diskutiert die Ergebnisse und gibt einen Ausblick auf zukünftige Arbeiten.

2 Related Work

2.1 Security Awareness

In der Informationssicherheit hat sich Security Awareness als eigener Forschungsbereich etabliert. Dieser beschäftigt sich mit dem „Faktor Mensch“ und wie IT-Anwender zu einem informationssicherheitskonformen Verhalten bewegt werden können. Die IT-Anwender sollen dazu gebracht werden, ihr theoretisches Wissen über Informationssicherheit praktisch anzuwenden [BaSN14, S. 121] und davon überzeugt werden, wie wichtig ihr Handeln ist [Hari15, S. 193]. In der Praxis wird bei Security-Awareness-Kampagnen vor allem Eines getan [Alli16, S. 23]: In Schulungen bekommt der Mitarbeiter theoretisches Wissen zum Thema Informationssicherheit vermittelt. Das tatsächliche Verhalten eines Mitarbeiters ist allerdings mit klassischen Schulungen nur bedingt zu beeinflussen [Wolf12].

Der Begriff Security Awareness kann aus der kognitiven Verhaltens- oder Prozessperspektive betrachtet werden [Häuß15, S. 35]. Diese Arbeit orientiert sich an der Definition von [HePo09], die Security Awareness als ein Zusammenspiel von Kognition, Handlungsabsicht und Organisation sehen und wählt somit die kognitive Prozessperspektive. Greifbar wird dies anhand des Beispiels der sicheren Passwortwahl. Die Kognition umfasst das Wissen und das Verständnis des Mitarbeiters wie ein sicheres Passwort aussieht. Die Organisation liegt in der Verantwortung des Unternehmens und stellt sicher, dass der Mitarbeiter sich sicherheitskonform verhalten kann, indem er zum Beispiel die Möglichkeit hat, sein Passwort regelmäßig zu ändern. Die

Handlungsabsicht oder Intention beschreibt den Willen des Mitarbeiters sich gemäß den Richtlinien der Informationssicherheit zu verhalten. Der Mitarbeiter muss also davon überzeugt sein, auch wirklich ein sicheres Passwort zu wählen.

Die Veröffentlichung von [Sipo01] unterscheidet verschiedene Dimensionen von Security Awareness und schließt dabei auch Awareness im öffentlichen Umfeld und der Politik mit ein. Diese befinden sich allerdings außerhalb des direkten Einflussbereiches von Unternehmen, so dass die vorliegende Arbeit diese Dimensionen außer Acht lässt. Da Mitarbeiter ihre Erfahrungen aber auch in ihr privates Umfeld übernehmen können, beeinflussen unternehmerische Maßnahmen indirekt auch die anderen Dimensionen.

Verschiedene Ansätze untersuchen, wie Security Awareness operationalisiert werden kann, um den Erfolg von Maßnahmen zur Mitarbeitersensibilisierung zu überprüfen. Im Ansatz von [KrKe05] wird eine Scorecard erstellt, welche Ergebnisse eines Fragebogens darstellt, der von den Mitarbeitern eines Unternehmens ausgefüllt wurde. [KrKe05] untersuchen wie die Faktoren Wissen, Einstellung und Verhalten gemessen werden können. In der Arbeit von [KANK11] wird Security Awareness im Unternehmen anhand von Kennzahlen gemessen, wie beispielsweise die Anzahl der Helpdesk-Anrufe, der Anzahl der geöffneten Phishing-Mails oder die Anzahl der gemeldeten Sicherheitsvorfälle. Die Zahlen werden anschließend anhand von Erkenntnissen aus der Gesundheitspsychologie bewertet. Während die Kennzahlen problematische Unternehmensbereiche gut visualisieren, lassen sie keine Rückschlüsse zu, warum die Security Awareness unter Umständen schlecht ausgeprägt ist. So könnten sowohl organisatorische Barrieren als auch ein Mangel an Fähigkeiten oder fehlender Verhaltensabsicht die Kennzahlen stark beeinflussen.

2.2 Sozialpsychologie

Informationssicherheitsforschung betrachtet häufig technische Aspekte, wie Backups, Intrusion-Detection-Systeme, Firewalls und sichere Softwareentwicklung. Der Fokus auf den Menschen erfordert einen anderen Blickwinkel. Das Gebiet der Sozialpsychologie kann helfen, das menschliche Verhalten in Bezug auf Informationssicherheit zu verstehen [Kaba02]. Insbesondere bei der Handlungsabsicht („Ich möchte sicherheitskonform handeln.“) spielen psychologische Vorgänge in den Köpfen der Mitarbeiter eine große Rolle. [Kaba02] gibt eine Übersicht über verschiedene sozialpsychologische Themen, wie Überzeugungen, Einstellungen oder soziale Normen, die auch im Bereich der Informationssicherheit in Unternehmen verwendet werden können.

Die Gesundheitspsychologie als Teilgebiet der Sozialpsychologie versucht bereits seit vielen Jahren das Verhalten von Menschen zu erklären und untersucht, wie sich unerwünschtes Verhalten ändern lässt. Die Forscher haben beispielsweise Raucher oder Menschen, die sich ungesund ernähren, im Visier. Im Laufe der Zeit sind dazu mehrere Theorien und Modellen entstanden. Eine Reihe von Arbeiten nutzen diese Verhaltensmodelle der Gesundheitspsychologie im Kontext Security Awareness [Boss07, GaGu09, Häuß15]. Die Arbeiten ziehen einzelne Erkenntnisse aus den Modellen heraus, um Hypothesen im eigenen Modell zu begründen. Am häufigsten wird die Theorie des überlegten Handelns (TRA – Theory of Reasoned Action) von [FiAj75] bzw. die Theorie des geplanten Verhaltens (TPB – Theory of Planned Behavior) von [Ajze91] verwendet [LUN+13]. Der große Vorteil der Theorie ist ihre Allgemeingültigkeit [StSN98]. Das von [MoKa08] beschriebene IBM erweitert TRA/TPB um einige wichtige Faktoren, wie dem Wissen oder der Gewohnheit von Personen. Das Modell interpretiert hierfür Erkenntnisse aus verschiedenen Verhaltensmodellen und Theorien. Das IBM wurde bereits

mehrfach erfolgreich im Kontext der HIV-Prävention verwendet [HaKe01, KaMo07, KAH+01] und wird in dieser Arbeit zur Erklärung eines informationssicherheitskonformen Verhaltens genutzt.

3 Schulen Sie noch oder überzeugen Sie schon?

3.1 Die Faktoren des Verhaltens

Um die Security Awareness zu steigern und das Mitarbeiterverhalten langfristig zu ändern, werden zielführende Kampagnen benötigt, die individuell auf die Überzeugungen der Mitarbeiter und die Rahmenbedingungen im Unternehmen eingehen. Gemäß IBM wird das menschliche Verhalten von fünf Faktoren direkt beeinflusst (vgl. Abbildung 1): Wissen und Fähigkeiten, Salienz des Verhaltens, Gewohnheit, Verhaltensabsicht sowie Einschränkungen aus dem Umfeld. Somit deckt das Modell alle Elemente der Definition von Security Awareness ab: Die Kognition wird durch Wissen und Fähigkeiten, die Salienz und die Gewohnheit repräsentiert; die Handlungsabsicht entspricht der Verhaltensabsicht und die Einschränkungen fallen in den Verantwortungsbereich der Organisation.

Der Faktor *Wissen und Fähigkeiten* ist wichtig für die Ausführung eines Verhaltens: Ein starker Wille einer Person alleine reicht nicht aus, wenn das notwendige Wissen zur Umsetzung fehlt [MoKa08]. Ein Nutzer, der die Regeln für ein sicheres Passwort nicht kennt, kann sich nicht informationssicherheitskonform verhalten, obwohl er dies vielleicht möchte.

Salienz liegt vor, wenn etwas aus dem direkten Umfeld hervorsticht und auffällt [BaVo07]. Ein salientes Verhalten muss für eine Person also prominent sein, so dass sie ihre Verhaltensabsicht auch umsetzt. Bekommt ein Mitarbeiter von einem Lieferanten einen USB-Stick geschenkt, muss sich der Mitarbeiter in diesem Moment noch an das korrekte Verhalten zum Umgang mit fremden Geräten erinnern.

Eine *Gewohnheit* verstärkt sich durch die wiederholte Ausführung eines Verhaltens [Tria77]. Das Sperren des Computers beim Verlassen des Arbeitsplatzes ist ein Beispiel für eine häufig ausgeführte Tätigkeit, die schnell zu einer Gewohnheit werden kann. Während in klassischen Schulungsmaßnahmen häufig nur Wissen und Fähigkeiten geschult werden, zeigt das integrierte Verhaltensmodell dass auch die beiden anderen kognitiven Faktoren Salienz und Gewohnheit auf das Verhalten des Mitarbeiters einwirken. Auf diese drei Faktoren können Unternehmen mit Sensibilisierungsmaßnahmen direkt Einfluss nehmen.

Die *Verhaltensabsicht* ist weitaus komplexer und wird selbst wiederum von mehreren Faktoren beeinflusst. Sie ist auch der Faktor, der das Verhalten eines Menschen am stärksten beeinflusst [FiAj75]. Ob ein Mitarbeiter eine Verhaltensabsicht bildet, ist von seiner Einstellung zum Verhalten, seiner Wahrnehmung hinsichtlich der Normen in seinem sozialen Arbeitsumfeld und seiner Einschätzung über seine persönliche Handlungsfähigkeit abhängig. Die Einstellung ergibt sich aus der Erfahrungseinstellung („Welche Erfahrungen habe ich mit dem Verhalten gemacht?“), die durch Emotionen beeinflusst ist und der instrumentellen Einstellung („Welche Folgen hat die Ausführung des Verhaltens?“), die durch Überzeugungen hinsichtlich der Auswirkungen des Verhaltens beeinflusst ist. Die wahrgenommene Norm unterteilt sich ebenfalls in zwei Bereiche: Die injunktive Norm spiegelt die Überzeugungen der Person wider, welches Verhalten ihr Umfeld von ihr erwartet, während die deskriptive Norm die Überzeugungen beschreibt, wie sich das Umfeld selbst verhalten würde. Erwartet ein Chef von seinen Mitarbeitern das Sperren des Bildschirms beim Verlassen des Arbeitsplatzes, hält sich aber selbst nicht an

die Regel, werden die wahrgenommene injunktive und deskriptive Norm des Mitarbeiters voneinander abweichen. Die persönliche Handlungsfähigkeit wird aus der wahrgenommenen Verhaltenskontrolle („Wird die Ausführung des Verhaltens in Anbetracht der Umstände einfach oder schwierig?“) und der Selbstwirksamkeitserwartung („Traue ich mir die Ausführung des Verhaltens in Anbetracht meiner Fähigkeiten zu?“) gebildet. Auch diese entstehen durch Überzeugungen einer Person. Um indirekt die Verhaltensabsicht zu beeinflussen, sollten Security-Awareness-Kampagnen auf die Emotionen und Überzeugungen des Mitarbeiters eingehen [MoKa08].

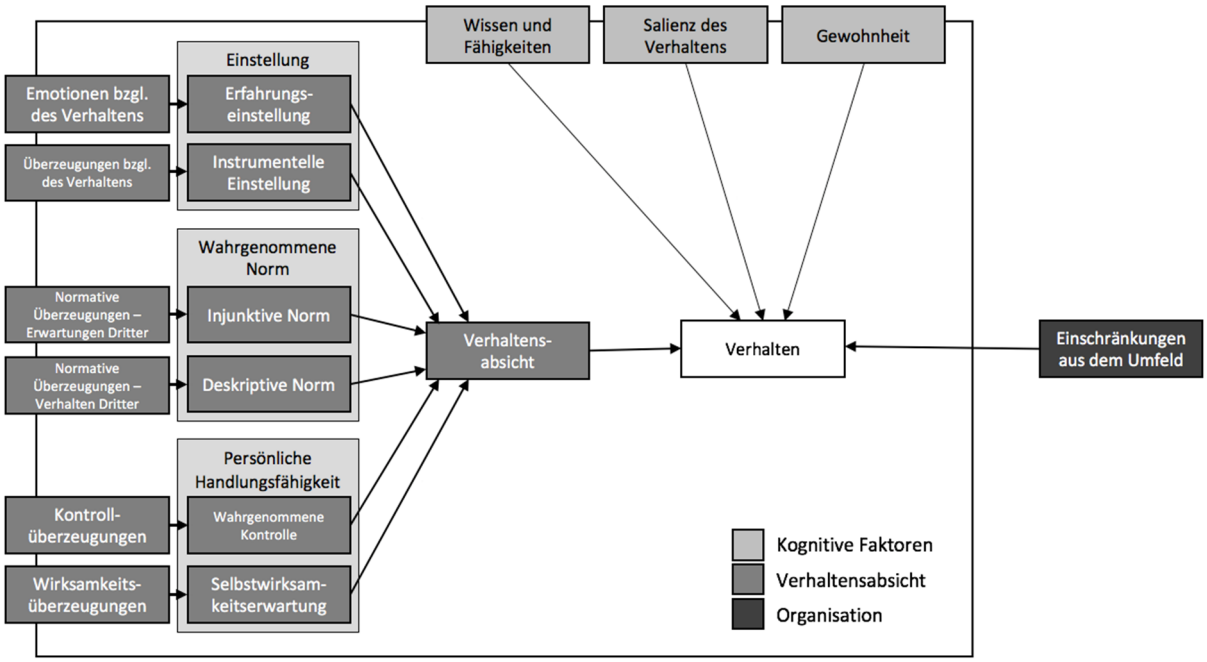

Abb. 1: Die Faktoren des integrierten Verhaltensmodells (in Anlehnung an [MoKa08, S. 77])

Die im IBM ebenfalls dargestellten *Einschränkungen aus dem Umfeld* wirken direkt auf das Verhalten einer Person ein. Einschränkungen aus dem Umfeld liegen vor, wenn beispielsweise ein Anwendungssystem die Ausführung eines informationssicherheitskonformen Verhaltens verhindert, indem die Wahl eines sicheren Passworts nicht zulässig ist. Auch mögliche Einschränkungen sollten daher generell im Sicherheitskonzept berücksichtigt werden.

Bei der Anwendung des Modells muss darauf geachtet werden, an Stelle des Verhaltens ein konkretes „informationssicherheitskonformes Verhalten“, wie etwa „Einhalten der Passwortregeln“, zu setzen. Die Faktoren, die auf das Verhalten einwirken, müssen dann auf dem gleichen Allgemeinheitsniveau sein. So bezieht sich beispielsweise der Einflussfaktor „Wissen“ auf das spezifische Wissen zu den Passwortregeln. Faktoren wie Einstellung oder Verhaltensabsicht korrelieren höher mit dem tatsächlichen Verhalten, wenn sie sich auf dem gleichen Allgemeinheitsniveau befinden [Schw04, S. 45, StSN98, S. 30]. Zudem gilt: Je spezifischer die Faktoren gefasst sind, umso besser korrelieren sie [Schw04, S. 45]. Eine global gefasste Einstellung oder Verhaltensabsicht, wie „Ich werde mich informationssicher verhalten“, umfasst viele verschiedene Verhaltensweisen [AjTi86], die sehr unterschiedlich sein können. Sensibilisierungsmaßnahmen sollten daher gezielt die spezifischen Einstellungen und Überzeugungen der Mitarbeiter beeinflussen, anstatt ein allgemeines Ziel, wie die Steigerung der Informationssicherheit, zu propagieren [StSN98, S. 31].

3.2 Wie überzeugt sind die Mitarbeiter?

Bevor ein Unternehmen beginnen kann die Faktoren zum Mitarbeiterverhalten gezielt im Rahmen einer Kampagne zu beeinflussen, muss eine Ist-Analyse durchgeführt werden. Ziel dieser Analyse ist es herauszufinden, wie die einzelnen Faktoren ausgeprägt sind und welche Emotionen oder Überzeugungen im Unternehmen vorherrschen. [MoKa08] empfehlen hierfür zuerst eine qualitative Studie in Form von Interviews durchzuführen. Durch die Interviews werden die hervorstechendsten Probleme identifiziert. 15-20 Mitarbeiter jeder Zielgruppe, wie zum Beispiel Verwaltungsangstellte oder Vertriebsmitarbeiter, sollten interviewt werden, um folgende Informationen zu gewinnen [MoKa08]:

- Erfahrungseinstellung: Welche positiven oder negativen Emotionen bestehen hinsichtlich der Ausführung des Verhaltens?
- Instrumentelle Einstellung: Welche positiven oder negativen Attribute bzw. Ergebnisse resultieren aus der Ausführung des Verhaltens?
- Normative Beeinflusser: Welche einflussnehmenden Individuen oder Gruppen befürworten das Verhalten oder sind dagegen?
- Kontrollüberzeugungen und Selbstwirksamkeitserwartungen: Welche situationsbedingten Barrieren oder unterstützenden Faktoren behindern oder unterstützen die Ausführung des Verhaltens?

Aus den in den Interviews gesammelten Erkenntnissen wird dann ein Fragebogen erstellt, der quantitativ ausgewertet wird [KaMo07]. Dieser soll möglichst von allen Mitarbeitern des Unternehmens beantwortet werden. Zur Erstellung des Fragebogens werden die im ersten Schritt gesammelten Überzeugungen generalisiert, in Fragen umgewandelt und den vier Faktoren Wissen und Fertigkeiten, Salienz, Gewohnheit sowie Verhaltensabsicht zugeordnet [KaMo07, S. 150–151]. Die Messung erfolgt durch mit den Fragen verknüpften Skalen, die von den Mitarbeitern ausgefüllt werden sollen. Eine Frage zu den normativen Überzeugungen könnte lauten: „Mein Chef beeinflusst mich in meinem Umgang mit USB-Sticks“. Eine Verhaltensüberzeugung könnte so aussehen: „Bei Passwortdiebstahl kann nur auf meinem eigenen PC Schaden angerichtet werden“. Die Antworten der Mitarbeiter erfolgen auf einer Fünf-Punkt-Skala mit dem Wertebereich von „Ich stimme nicht zu“ bis „Ich stimme zu“ [MoKa15, S. 113]. Die Skalen können dabei je nach Konstrukt variieren. Im Rahmen der Fragebögen ist es auch möglich, die Faktoren Wissen und Fertigkeiten sowie die Gewohnheit (z.B. durch den „Self-Report Habit Index“ [VeAa99]) abzufragen. Um die Erhebung so einfach wie möglich zu gestalten, sollte die Befragung computergestützt stattfinden und in angemessener Zeit (z.B. einer halben Stunde) von dem Mitarbeiter zu bewältigen sein. Die ebenfalls computergestützte Auswertung der Fragebögen gibt schließlich Auskunft über die Ausprägung der Faktoren im Unternehmen. Das Ergebnis dient nun als Grundlage zur Planung einer Security-Awareness-Kampagne mit individuellen Inhalten.

3.3 Überzeugende Kampagnen gestalten

Um Mitarbeiter nachhaltig zu informationssicherheitskonformen Verhaltensweisen zu bewegen, sollte eine Security-Awareness-Kampagne gezielt auf die einzelnen Faktoren unter Berücksichtigung der Messergebnisse einwirken. Dieses Kapitel untersucht, auf welche Faktoren „klassische“ Security-Awareness-Werkzeuge einwirken können und wie dies am effektivsten getan werden kann.

Das BSI empfiehlt in seinen Grundschutzkatalogen Werkzeuge aus den Bereichen Sensibilisierung, Schulung, Verstärkung und Öffentlichkeitsarbeit [Bund16, S. 1898] für die Mitarbeiter einzusetzen. Diese Werkzeuge werden in dieser Arbeit in die Kategorien intensive *Präsenzveranstaltungen* (z.B. Präsenzschulungen, Vorträge) und *Soziales Marketing* (z.B. Flyer, Poster, bedruckte Tassen) eingeteilt. Im Informationssicherheitsmanagementsystem (ISMS) „Informations-Sicherheitsmanagement System in 12 Schritten“ (ISIS12) [Baye17] finden sich Werkzeuge, welche die organisatorischen Aspekte der Security Awareness adressieren. Diese sind die Informationssicherheitsleitlinie und das Informationssicherheitsteam. Neben diesen wird in dieser Arbeit auch der Einfluss von unterstützenden Faktoren, die die Ausführung des Verhaltens erleichtern, wie beispielsweise eine optimierte Usability, betrachtet. Einen Überblick über die verschiedenen Werkzeuge sowie die von ihnen jeweils beeinflussbaren Faktoren gibt Tabelle 1.

Tab. 1: Darstellung der Werkzeuge und der von ihnen beeinflussten Faktoren.

Werkzeug	Beeinflusste Faktoren
Präsenzveranstaltungen	Wissen und Fertigkeiten, Gewohnheit, Emotionen, Verhaltensüberzeugungen, Wirksamkeitsüberzeugungen, Kontrollüberzeugungen, normative Überzeugungen (Erwartungen)
Soziales Marketing	Wissen, Salienz, Verhaltensüberzeugungen, Emotionen, normative Überzeugungen (Erwartungen)
Informationssicherheitsleitlinie	Wissen, Verhaltensüberzeugungen, normative Überzeugungen (Erwartungen)
Informationssicherheitsteam	Wirksamkeitsüberzeugungen
Unterstützende Faktoren	Kontrollüberzeugungen, Wirksamkeitsüberzeugungen

Präsenzveranstaltungen haben aufgrund ihrer Flexibilität das Potential, auf fast alle verhaltensbildenden Faktoren einzuwirken. Klassischerweise werden in diesen Veranstaltungen Wissen und Fertigkeiten erhöht. Durch Übungen und Training kann auch die Gewohnheit beeinflusst werden. Je öfter ein Mitarbeiter ein Verhalten wiederholt, umso eher kann sich eine Gewohnheit etablieren [Tria77]. So kann zum Beispiel gefördert werden, dass ein Mitarbeiter beim Verlassen seines Arbeitsplatzes aus Gewohnheit den Bildschirm sperrt. Hierfür sollte das Verhalten möglichst situationsnah, beispielsweise durch Plan- und Rollenspiele trainiert werden [RHL+17]. Durch Einübung des Verhaltens können auch die Emotionen, wie zum Beispiel Angst vor einer bestimmten Verhaltensweise gemindert und die Überzeugungen diesbezüglich gefördert werden. Um Überzeugungen in den Präsenzveranstaltungen zu beeinflussen ist es wichtig, den Teilnehmern die richtigen, individualisierten Inhalte zu präsentieren. Diese müssen die Überzeugungen je nach erwünschtem Verhalten stärken, schwächen oder aber ändern [Ajze06, S. 4]. Eine Überzeugung kann sich beispielsweise ändern, wenn der Person, die die Überzeugung hält, widersprüchliche Informationen präsentiert werden [Kaba02]. Einem Mitarbeiter, der glaubt, dass das Nutzen von fremden USB-Sticks harmlos ist, könnten Gegenbeispiele präsentiert und die Folgen dieses Handelns aufgezeigt werden. Der Trainer kann durch die Präsentation von neuen Informationen die Bildung von neuen Überzeugungen anstoßen [Ajze06, S. 5]. Wenn man einem Mitarbeiter erklärt, dass ihm für die Folgen der fahrlässigen Nutzung eines USB-Sticks Sanktionen erwarten, wird er dies als Verhaltensüberzeugung verinnerlichen. Verhaltensüberzeugungen können so durch das Darstellen der positiven Effekte eines informationssicherheitskonformen Verhaltens und dem Aufzeigen der Sanktionen geändert oder neu gebildet werden. Dies kann noch unterstrichen werden, indem die Teilnehmer der Maßnahme für das korrekte Ausführen eine kleine Belohnung erhalten [ThSo98, S. 172]. Das

schafft zudem eine positive Emotion hinsichtlich des Verhaltens. Das Entstehen von negativen Emotionen durch Scheitern wird verhindert, indem beim Einüben des Verhaltens Unterstützung gewährt wird. Die Kontrollüberzeugungen können im Dialog verändert oder neu gebildet werden, indem erwartete Barrieren entschärft oder unterstützende Faktoren präsentiert werden, die der Mitarbeiter vorher nicht kannte. Die Wirksamkeitsüberzeugungen können durch Ermutigung und Unterstützung des Mitarbeiters beeinflusst werden. Durch die Vermittlung der Richtlinien werden auch normative Überzeugungen gebildet.

Im Gegensatz zum klassischen Marketing profitiert beim sozialen Marketing nicht die Organisation die das Marketing betreibt, sondern die Zielgruppe selbst [StSR08, S. 438]. Soziales Marketing kann eingesetzt werden, um für die Änderung von Verhaltensweisen zu werben [BCN+03, S. 33]. Die Salienz des Verhaltens wird beeinflusst, indem das Verhalten dauerhaft prominent gemacht und hervorgehoben wird, z.B. durch die Erregung von Aufmerksamkeit oder durch visuelle Akzente [BaVo07, S. 776]. Wird ein Mitarbeiter beim Betreten der Kaffeeküche durch ein Plakat auf das Sperren des Bildschirmes hingewiesen, wird das Verhalten salient und der Mitarbeiter geht zurück an den Arbeitsplatz, um den Bildschirm zu sperren. Soziales Marketing schafft als Nebeneffekt auch Wissen [StSR08, S. 437], wenn auch nicht in solchem Maße wie Präsenzveranstaltungen. Durch das Aufzeigen der Vorteile und des tatsächlichen Aufwandes für eine Verhaltensänderung können auch Überzeugungen über die tatsächlichen Konsequenzen des Verhaltens geändert werden. Je nachdem welche Verhaltensweise beeinflusst werden soll, kann die Nachricht des sozialen Marketings gestaltet werden. Sollen normative Überzeugungen beeinflusst werden, könnte zum Beispiel eine Rundmail vom Vorgesetzten oder ein Plakat mit einem Mitarbeiter genutzt werden, um die Botschaft zu überbringen.

Generell ist es für Unternehmen empfehlenswert die Sensibilisierung ihrer Mitarbeiter in ein ganzheitliches Sicherheitskonzept einzupassen. Hierfür eignet sich die Einführung eines ISMS. Ein solches System bringt eine große Anzahl von organisatorischen Maßnahmen mit sich, die sich auch auf die Security Awareness der Mitarbeiter auswirken. Die Einführung von standardisierten Prozessen kann Einschränkungen („Ich kann meinen Bildschirm nicht sperren“) und Barrieren („Ich kann meinen Bildschirm nur umständlich sperren“) für die Ausführung von informationssicherheitskonformen Verhaltensweisen beseitigen. Im Rahmen eines ISMS werden außerdem ein Informationssicherheitsteam gebildet und eine Informationssicherheitsleitlinie erstellt. Ein Informationssicherheitsteam kann als permanenter Ansprechpartner für Informationssicherheit die Wirksamkeitsüberzeugungen und somit die Selbstwirksamkeitserwartung der Mitarbeiter positiv beeinflussen [GaGu09, S. 8]. Die Erstellung einer Informationssicherheitsleitlinie wird häufig als Grundlage für die Erhöhung der Informationssicherheit in Unternehmen empfohlen [Baye17, S. 12; Kaba02, S. 11]. Sie beeinflusst auch die Security Awareness des Mitarbeiters, indem sie durch ihren informativen Charakter Wissen erhöht und als Regelwerk die Grundlage für normative Überzeugungen hinsichtlich der Erwartungen des Unternehmens liefert. Auch die Konsequenzen, also Belohnungen oder Sanktionen bei Einhalten/Nichteinhalten der Sicherheitsrichtlinien, sollten in dem Dokument festgelegt sein [Baye17, S. 18]. Belohnungen für normatives und Bestrafungen für nicht normatives Verhalten spielen als extrinsische Motivation eine große Rolle für die Beeinflussung der Überzeugungen hinsichtlich der wahrgenommenen, injunktiven Normen [ArWA10]. Die Sanktionen wirken aber auch auf die Verhaltensüberzeugungen ein, indem dem Mitarbeiter aufgezeigt wird welche Folgen sein Verhalten haben kann.

Unterstützende Faktoren, wie beispielsweise die Erhöhung der Usability von Anwendungssystemen, vereinfachen die Ausführung des jeweiligen Verhaltens und können auf die Kontrollüberzeugungen und die Wirksamkeitsüberzeugungen einer Person einwirken. Dabei spielt es

für den Mitarbeiter auch eine Rolle wie wahrscheinlich das Auftreten von unterstützenden Faktoren ist und wie stark diese sein werden [MoKa08, S. 80]. Unterstützende Faktoren, die bereits bestehen, können durch die Auswertung der Fragebögen identifiziert und wenn möglich, weiter ausgebaut werden. Für die Schaffung von neuen unterstützenden Faktoren hilft eine kritische Untersuchung der Anwendungen und Systeme, die für ein informationssicheres Verhalten benötigt werden.

4 Fazit und Ausblick

Diese Arbeit bietet einen neuen Ansatz zum Thema Security Awareness, der wissenschaftlich fundierte Erkenntnisse aus dem Forschungsfeld Sozialpsychologie ganzheitlich in den Kontext Informationssicherheit überträgt. Die komplexen Zusammenhänge der sozialpsychologischen Einsichten in das menschliche Verhalten werden konsequent auf das informationssicherheitskonforme Verhalten von Mitarbeitern angewendet. Das in der Gesundheitspsychologie bewährte *Integrierte Verhaltensmodell* bietet einen neuen Erklärungsansatz, warum neben dem Wissen um informationssicherheitskonformes Verhalten noch weitere Faktoren wie Gewohnheit, Salienz und Verhaltensabsicht bei der Sensibilisierung von Mitarbeitern berücksichtigt werden müssen. Die Kenntnis der bei den Mitarbeitern vorherrschenden Faktoren ermöglicht eine individuelle und gezielte Planung von Security-Awareness-Kampagnen, um die Mitarbeiter nicht nur zu schulen, sondern sie von einer Verhaltensänderung zu überzeugen. Die Arbeit schlägt Werkzeuge für den Einsatz in Security-Awareness-Kampagnen vor, und zeigt auf, auf welche Faktoren diese Werkzeuge einwirken können. Das Verständnis des *Integrierten Verhaltensmodells* kann auch genutzt werden, um weitere Werkzeuge gezielt zur Erhöhung der Security Awareness auszuwählen.

Um die Werkzeuge erfolgreich zu verwenden, muss die aktuelle Ausprägung aller Faktoren bei den Mitarbeitern im Unternehmen sorgfältig analysiert werden. Die Ist-Analyse mittels Interviews und Fragebögen ist anfangs aufwendig. Aufgrund der Komplexität des Faktors Verhaltensabsicht, haben auch die Autoren [MoKa08] viel Arbeit in die Untersuchung der Überzeugungen und Emotionen der Menschen gesteckt. Diese Komplexität gilt es auch im Umfeld der Informationssicherheit zu beachten. Es bleibt zu erforschen, ob sich nach der Untersuchung mehrerer Unternehmen ein allgemeingültiger Überzeugungs- und Emotionskatalog erarbeiten lässt. Dieser würde zu einem ebenso allgemeingültigen Fragebogen führen, der die Analysephase auf die quantitative Studie verkürzen würde.

Um die Thesen in dieser Arbeit zu verifizieren, findet aktuell ein Projekt statt. Die Autoren erproben im Rahmen der Einführung eines ISMS die Sensibilisierung der Hochschulangehörigen unter Anwendung der Erkenntnisse dieser Arbeit. Ein weiterer Schritt ist die Herausarbeitung von konkreten praktischen Empfehlungen für die Planung von Security-Awareness-Kampagnen für bestimmte informationssicherheitskonforme Verhaltensweisen, wie beispielsweise die Wahl eines sicheren Passworts.

Literatur

[Ajze91] I. Ajzen: The theory of planned behavior. In: Organizational Behavior and Human Decision Processes (50), Academic Press (1991), 179–211.

[Ajze06] I. Ajzen: Behavioral Interventions Based on the Theory of Planned Behavior. Brief Description of the Theory of Planned Behavior (2006). Zugriff am 20.01.2017. Verfügbar unter https://people.umass.edu/aizen/pdf/tpb.intervention.pdf

[AjTi86] I. Ajzen, C. A. Timko: Correspondence between health attitudes and behavior. In: Journal of Basic and Applied Psychology (42), Taylor & Francis (1986), 249–276.

[Alli16] Allianz für Cyber-Sicherheit: Awareness-Umfrage 2015. Bundesamt für Sicherheit in der Informationstechnik (2016).

[ArWA10] E. Aronson, T. D. Wilson, R. M. Akert: Sozialpsychologie. In: Pearson Studium - Psychologie, 6., aktualisierte Aufl., [Nachdr.]. Pearson Studium (2010).

[BaSN14] M. Bada, A. M. Sasse, J. R. Nurse: Cyber Security Awareness Campaigns: Why do they fail to change behaviour? In: Global Cyber Security Capacity Centre: Draft Working Paper, Global Cyber Security Capacity Centre (2014), 118-131.

[BaVo07] R. F. F. Baumeister, K. D. D. Vohs: Encyclopedia of Social Psychology, SAGE Publications (2007), 775.

[Baye17] Bayerisches IT-Sicherheitscluster: Handbuch zur effizienten Gestaltung von Informationssicherheit im Mittelstand, Version 1.7., Bayrischer IT-Sicherheitscluster e.V. (2017).

[BCN+03] T. Baranowski, K. W. Cullen, T. Nicklas, D. Thompson, J. Baranowski: Are Current Health Behavioral Change Models Helpful in Guiding Prevention of Weight Gain Efforts? In: Obesity, 11 (10), The Obesity Society (2003), 23–43.

[Boss07] S. R. Boss: Control, Perceived Risk and Information Security Precautions. External and Internal Motivations for Security Behavior, University of Pittsburgh (2007).

[Bund16] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge. 15. Ergänzungslieferung, BSI (2016), 1897.

[FiAj75] M. Fishbein, I. Ajzen: Belief, attitude, intention, and behavior. An introduction to theory and research (Addison-Wesley series in social psychology), Addison-Wesley Pub. Co. (1975).

[GaGu09] S. M. Galvez, I. R. Guzman: Identifying Factors that Influence Corporate Information Security Behavior, AMCIS (2009).

[HaKe01] I. von Haeften, K. Kenski: Multi-partnered heterosexuals' condom use for vaginal sex with their main partner as a function of attitude, subjective norm, partner norm, perceived behavioural control and weighted control beliefs. In: Psychology, Health & Medicine, 6 (2), Taylor & Francis (Routledge) (2001), 165-177.

[Hari15] T. W. Harich: IT-sicherheit im Unternehmen (1. Auflage), mitp-Verlag (2015).

[Häuß15] F. Häußinger: Studies on Employees' Information Security Awareness, Universität Göttingen (2015).

[HePo09] M. Helisch, D. Pokoyski: Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung. Vieweg+Teubner Verlag / GWV Fachverlage GmbH Wiesbaden (2009).

[ISAC16] ISACA: State of Cybersecurity. Implications für 2016. An ISACA and RSA Conference Survey, ISACA (2016).

[Kaba02] M. E. Kabay: Using Social Psychology to Implement Security Policies. In: S. Bosworth & M. E. Kabay: Computer Security Handbook, Wiley (2002), 1-22.

[KAH+01] K. Kenski, J. Appleyard, I. von Haeften, D. Kasprzyk, M. Fishbein: Theoretical determinants of condom use intentions for vaginal sex with a regular partner among male and female injecting drug users. In: Psychology, Health & Medicine, 6 (2), Taylor & Francis (Routledge) (2001), 179-190.

[KANK11] B. Khan, K. S. Alghatbar, S. I. Nabi, M. Khan: Effectiveness of information security awareness methods based on psychological theories. In: African Journal of Business Management, 26 (5), AJBUMA (2011), 10862–10868.

[KaMo07] D. Kasprzyk, D. E. Montaño: Application of an integrated behavioral model to understand HIV prevention behavior of high-risk men in rural Zimbabwe. In: I. Ajzen, D. Albarracin, Prediction and Change of Health Behavior: Applying the Reasoned Action Approach, Psychology Press (2007), 145–168.

[KrKe05] H. A. Kruger, W. D. Kearney: Measuring Information Security Awareness: A West Africa Gold Mining Environment Case Study. In: Proceedings of the Information Security South Africa (ISSA) Conference (2005).

[LUN+13] B. Lebek, J. Uffen, M. Neumann, B. Hohler, M. Breitner: Employees' Information Security Awareness and Behavior: A Literature Review. In: Hawaii International Conference on System Sciences, HICSS (2013), 2978-2987.

[MoKa08] D. E. Montaño, D. Kasprzyk: Theory of Reasoned Action, Theory of Planned Behavior, and the Integrated Behavioral Model. In: K. Glanz, B. Rimer, K. & K. Viswanath, Health Behavior and Health Education. Theory, Research, and Practice, 4th Edition, John Wiley & Sons (2008), 67-96.

[MoKa15] D. E. Montaño, D. Kasprzyk: Theory of Reasoned Action, Theory of Planned Behavior, and the Integrated Behavioral Model. In: K. Glanz, Rimer, Barbara, K. & K. Viswanath, Health Behavior. Theory, Research, and Practice, 5th Edition John Wiley & Sons (2008), 95–124.

[RHL+17] A. Rieb, M. Hofmann, A. Laux, S. Rudel, U. Lechner: Wie IT-Security Matchplays als Awarenessmaßnahme die IT-Sicherheit verbessern können. In Leimeister, J.M.; Brenner, W. (Hrsg.): Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017) (2017), 867-881.

[ScPi15] S. Schäfer, C. Pinnow: Industrie 4.0 – Grundlagen und Anwendungen. Branchentreff der Berliner Wissenschaft und Industrie (1.Aufl.), DIN e.V. (2015), 129.

[Schw04] R. Schwarzer: Psychologie des Gesundheitsverhaltens. Einführung in die Gesundheitspsychologie (3., überarb. Aufl.), Hogrefe (2004).

[Sipo01] M. T. Siponen: Five dimensions of information security awareness. In: ACM SIGCAS Computers and Society, 31 (2), ACM SIGCAS (2001), 24–29.

[StSN98] W. Stroebe, M. Stroebe, S. Niedernhuber: Lehrbuch der Gesundheitspsychologie. Ein sozialpsychologischer Ansatz (1. Aufl.), Klotz (1998).

[StSR08] J. D. Storey, G. B. Saffitz, J. G. Rimón (2008): Social Marketing. In: K. Glanz, Rimer, Barbara, K. & K. Viswanath (Hrsg.), Health Behavior and Health Education. Theory, Research and Practice. 4th Edition, John Wiley & Sons (2008), 435–461.

[ThSo98] M. Thomson, R. von Solms (1998): Information security awareness: educating your users effectively. In: Information Management & Computer Security, 4 (6), Emerald (1998), 167–173.

[Tria77] H. C. Triandis: Interpersonal behavior, Brooks/Cole (1977).

[VeAa99] B. Verplanken, H. Aarts: Habit, Attitude, and Planned Behaviour. Is Habit an Empty Construct or an Interesting Case of Goal-directed Automaticity? In: European Review of Social Psychology, 10 (1), European Association of Social Psychology (1999), 101–134.

[Wolf12] M. Wolf: Von Security Awareness zum Secure Behaviour. In: Hakin9 Extra – IT-Forensik, 5, Software Wydawnictwo (2012), 18 – 19.

[Zeit17] Zeit Online: Merkel und Abe wollen Freihandel stärken, http://www.zeit.de/wirtschaft/2017-03/cebit-merkel-freihandelsabkommen-japan-deutschland-digitalisierung (2017), aufgerufen am 22.03.2017.