ISIS12-Hack: Mitarbeiter sensibilisieren statt informieren

Kristin Weber[1] und Andreas Schütz[1]

[1] Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt, Fakultät Informatik und Wirtschaftsinformatik, Würzburg, Deutschland
{kristin.weber,andreas.schütz}@fhws.de

Abstract. Mit zunehmender Digitalisierung stehen auch kleine und mittlere Unternehmen (KMU) vermehrt vor der Herausforderung sich mit der Thematik Informationssicherheit auseinanderzusetzen. Wie Mitarbeiter sich im Umgang mit Informationen und Informationssystemen verhalten, spielt hierbei eine entscheidende Rolle. Das Framework ISIS12 bietet ein Verfahren zur Etablierung eines Managementsystems für Informationssicherheit speziell für KMU. Die Bedeutung der Mitarbeiter für die Informationssicherheit wird in ISIS12 allerdings nur oberflächlich berücksichtigt. Diese Arbeit stellt ein Vorgehensmodell vor, das ergänzend zu ISIS12, die Sensibilisierung der Mitarbeiter für die Informationssicherheit zum Ziel hat. Um eine tatsächliche Verhaltensänderung bei den Mitarbeitern zu bewirken, werden hierfür Erkenntnisse der Sozialpsychologie genutzt. Das Vorgehensmodell analysiert zunächst vor allem die Kognition und Handlungsabsicht der Mitarbeiter. Eine individualisierte Security Awareness Kampagne geht anschließend gezielt auf die Bedürfnisse der jeweiligen Mitarbeiter ein und berücksichtigt dabei die besonderen Ansprüche eines KMU. Durch die Anpassung an den Ablauf von ISIS12 entsteht für Unternehmen nur wenig organisatorischer Mehraufwand.

Keywords: Informationssicherheit, Security Awareness, Mitarbeitersensibilisierung, ISMS

1 Motivation

Kleine und mittlere Unternehmen (KMU) haben für Deutschland eine enorme volkswirtschaftliche Bedeutung. KMU wollen, wie auch die großen Unternehmen, vom aktuell propagierten digitalen Wandel profitieren. Insgesamt weisen mittelständische Unternehmen der Digitalisierung eine hohe bis sehr hohe Bedeutung zu [1]. Dennoch geht der digitale Wandel nur langsam vonstatten. Gemäß einem Bericht des Bundesministeriums für Wirtschaft und Energie (BMWi) haben gerade KMU einen unterdurchschnittlichen Digitalisierungsgrad [2]. Die fortschreitende Digitalisierung stellt zweifelsohne hohe Anforderungen an die Informationssicherheit [3,4]. So bezeichnen viele KMU Herausforderungen im Bereich der Informationssicherheit als Hemmnis für den digitalen Wandel [2,5,6].

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

Der „Faktor Mensch“ nimmt eine zentrale Stellung für die Gewährleistung der Informationssicherheit ein [7-9] und hat inzwischen die technischen Begebenheiten als beliebtestes Angriffsziel überholt [10]. Die eigenen Mitarbeiter sollten von Unternehmen als eine wertvolle Ressource zum Schutz sensibler Unternehmensinformationen und der IT-Infrastruktur verstanden werden. Durch Sensibilisierungsmaßnahmen kann der „Faktor Mensch“ von einer Schwachstelle zu einer Stütze des Informationssicherheitskonzeptes werden [7].

Die Sensibilisierung von Mitarbeitern ist ein komplexes, andauerndes Vorhaben, das letztendlich auf eine Verhaltensänderung der Mitarbeiter abzielt [11]. Erfolgreiche Verhaltensänderungen benötigen u. a. eine individuell auf die Überzeugungen des jeweiligen Mitarbeiters abgestimmte Vorgehensweise [12]. Umfragen zeigen jedoch, dass viele Unternehmen ein gemeinsames Maßnahmenpaket für alle Mitarbeiter schnüren und selten branchenspezifische Risiken berücksichtigen [13]. Die Individualisierung der Inhalte spielt häufig keine Rolle.

Vor dem Hintergrund, dass KMU vermehrt in den Fokus von Cyberkriminellen geraten und einen großen Nachholbedarf in der Sensibilisierung ihrer Mitarbeiter für das Thema Informationssicherheit sehen, verfolgt diese Arbeit das Ziel, das ISIS12-Vorgehensmodell zu optimieren. ISIS12 ist ein leichtgewichtiges Information Security Management Framework, das sich speziell an KMU richtet [14]. Die Arbeit schlägt ein Vorgehensmodell zur Mitarbeitersensibilisierung vor, das sich an der Abfolge von ISIS12 orientiert. Das Vorgehensmodell berücksichtigt Erkenntnisse aus der Verhaltensforschung und wird den Anforderungen von KMU nach zeit- und ressourceneffizienten Sensibilisierungsmaßnahmen gerecht. Das vorgeschlagene Modell wird derzeit im Rahmen eines Informationssicherheitsprojektes an einer Hochschule erprobt. Erste Erkenntnisse aus diesem Projekt fließen in die nachfolgende Betrachtung ein.

Der Rest der Arbeit ist wie folgt strukturiert: In Kapitel 2 werden die Besonderheiten von KMU in Bezug auf Informationssicherheit herausgearbeitet, Grundlagen von Security Awareness und der Beitrag der Sozialpsychologie diskutiert und ISIS12 hinsichtlich der Umsetzung der Mitarbeitersensibilisierung betrachtet. In Kapitel 3 wird die verwendete Forschungsmethodik vorgestellt. Kapitel 4 stellt schließlich das entwickelte Vorgehensmodell vor. In Kapitel 5 ziehen die Autoren ein Fazit und geben einen Ausblick auf weitere Forschungsarbeiten.

2 Related Work

2.1 Informationssicherheit in KMU

Ein System gilt als informationssicher, wenn es keine Zustände annimmt, die zu unautorisierter Informationsveränderung oder -gewinnung führen [15]. Im Unternehmen können hierfür verschiedene Schutzziele identifiziert werden. Vor allem die Ziele Vertraulichkeit, Integrität und Verfügbarkeit werden in diesem Zusammenhang häufig genannt [z. B. 15-17]. Um die Vertraulichkeit einer Information zu schützen, ist es notwendig, unautorisierten Zugriff auf sie zu

unterbinden. Mit der Integrität wird sichergestellt, dass die Informationen unverändert sind. Um dieses Schutzziel zu erreichen, müssen sie vor nicht autorisierten Änderungen geschützt werden. Mit der Verfügbarkeit soll sichergestellt werden, dass die gewünschte Information den autorisierten Nutzern zugänglich ist.

Informationssicherheit ist für KMU und Großunternehmen gleichermaßen wichtig. Bei KMU sind allerdings einige spezifische Besonderheiten zu beachten. Zum einen sind Bilanzsumme und Umsatz geringer. Aufgrund der hohen Kosten können sich KMU meist keine eigene IT-Abteilung leisten und müssen die IT-Nutzung mit weniger Ressourcen realisieren [1]. Maßnahmen zur Mitarbeitersensibilisierung müssen entsprechend kostensparend sein.

KMU haben gegenüber großen Unternehmen einen geringeren Formalisierungsgrad der zu einer niedrigen Standardisierung führt. 2016 hatten beispielsweise nur 32 Prozent der mittelständischen Unternehmen dokumentierte Sicherheitsrichtlinien [18]. Durch flache Hierarchien [19] und das stärkere Engagement der Eigentümer [20] haben die Führungskräfte in KMU einen stärkeren Einfluss auf das Verhalten der Mitarbeiter und können im Bereich der Informationssicherheit mit gutem Beispiel vorangehen. Charakteristisch ist außerdem der große Anteil der im eigenen Unternehmen ausgebildeten Facharbeiter [21]. Dies liefert Potential für Sensibilisierungsmaßnahmen, da man die Mitarbeiter bereits während der Ausbildung für die Thematik sensibilisieren kann. Dennoch bieten nur 27 Prozent regelmäßige Schulungen oder Informationen hinsichtlich der Informationssicherheit für Mitarbeiter an [18]. Zudem unterscheiden sich die KMU durch eine geringere Arbeitsteilung [19]. Ein breites Aufgabengebiet der Mitarbeiter erhöht die Ansprüche an die Informationssicherheit, da der einzelne Mitarbeiter auf mehr Informationen aus verschiedenen Bereichen zugreift. Gegenüber Großunternehmen haben KMU einiges aufzuholen: In den letzten Jahren konnten keine bedeutenden Verbesserungen der organisatorischen Maßnahmen zu Datenschutz und Sicherheit bei den Unternehmen festgestellt werden [19].

2.2 Security Awareness

Mit „Security Awareness“ wird grundsätzlich die Sensibilisierung von Mitarbeitern für Informationssicherheit umschrieben. Hänsch & Benenson [22] beschreiben drei mögliche Blickwinkel auf den Begriff Security Awareness. Die einfachste Sichtweise versteht unter Awareness, dass Mitarbeiter wissen, welche Bedrohungen es gibt und diese erkennen („Perception“). Eine weitere Sichtweise ergänzt, dass Mitarbeiter auch wissen, wie Sie sich vor Bedrohungen schützen können („Protection“). Und die dritte Sichtweise beschreibt, dass Mitarbeiter wissen, was eine Bedrohung ist und was sie dagegen tun können, und dass sie sich auch entsprechend verhalten („Behavior“). Nur der letzte Ansatz verspricht eine tatsächliche Erhöhung der Informationssicherheit im Unternehmen. Sensibilisierung heißt also, dass die Mitarbeiter wissen, wie sie sich informationssicherheitskonform verhalten (z. B. ein sicheres Passwort wählen), welche Konsequenzen ihnen und dem Unternehmen bei nichtkonformem Verhalten drohen (z. B. Imageverlust und finanzielle Schäden durch Verlust von Kundendaten) und dass sie dieses Wissen in kritischen Situationen tatsächlich anwenden.

Helisch & Pokoyski [23] nennen mit der Organisation noch einen weiteren Aspekt von Security Awareness. Die Organisation stellt sicher, dass Mitarbeiter sich im Unternehmen überhaupt informationssicherheitskonform verhalten können, dass also keine Barrieren einem entsprechenden Verhalten entgegenstehen. Gleichzeitig können organisatorische Maßnahmen, wie etwa die Erhöhung der Usability, die Informationssicherheit unterstützen. Security Awareness ist somit ein Zusammenspiel von Kognition (Verständnis des Problems und das Wissen zu dessen Lösung), Handlungsabsicht (Willen des Mitarbeiters sich informationssicherheitskonform zu verhalten) und der Organisation [23].

Um ein Verständnis für das menschliche Verhalten in Bezug auf Informationssicherheit zu entwickeln, kann die Sozialpsychologie wichtige Einsichten liefern [24]. Vor allem im Bereich der Gesundheitspsychologie hat sich in den letzten Jahrzehnten eine große Anzahl an Modellen etabliert, mit denen menschliches Verhalten erklärt werden kann. Das von Montaño & Kasprzyk [12] beschriebene Integrierte Verhaltensmodell (IBM) adaptiert die wichtigsten Konstrukte von gängigen Theorien und vereint diese in einem Modell (vgl. Abbildung 1).

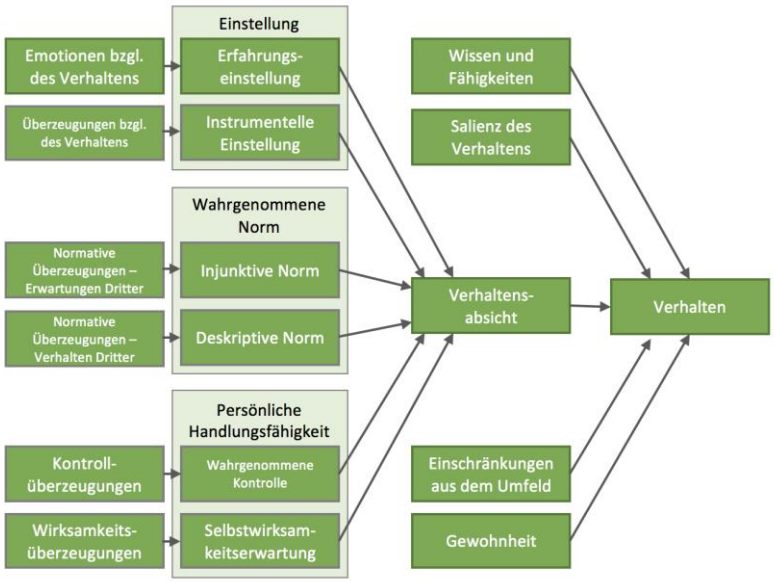

Abbildung 1. Das Integrierte Verhaltensmodell [12, S. 77].

Das Modell unterscheidet zwischen fünf verschiedenen Einflussfaktoren, die das Verhalten eines Menschen bestimmen. Dies sind zum einen das *Wissen und die Fähigkeiten* einer Person. Die *Salienz* des Verhaltens beschreibt wie prominent eine bestimmte Verhaltensweise für eine Person ist. Die von einem Mitarbeiter getroffene *Verhaltensabsicht* ist der stärkste Einflussfaktor [25] und auch der komplexeste. Sie wird wiederum durch die Einstellung, die wahrgenommene Norm und die persönliche Handlungsfähigkeit des Mitarbeiters bestimmt. Zudem können *Einschränkungen* aus

dem Umfeld die Ausführung des Verhaltens verstärken und die *Gewohnheit* eines Menschen die Wahrscheinlichkeit für die Ausführung erhöhen. Während Wissen und Fähigkeiten, Salienz, Einschränkungen und die Gewohnheit direkt vom Umfeld beeinflusst werden können, muss die Verhaltensabsicht über die Änderung von Überzeugungen und Emotionen indirekt beeinflusst werden.

Obwohl z. B. die Arbeiten [24,26,27] Ansätze aus der Sozialpsychologie nutzen, um konkrete Handlungsempfehlungen für die Steigerung der Security Awareness zu geben, ist in der Praxis der „One Size Fits All"-Ansatz bei der Mitarbeitersensibilisierung vorherrschend. Einer Umfrage der Allianz für Cybersicherheit zufolge berücksichtigen 54 Prozent der Unternehmen keine branchenspezifischen Risiken oder Gefährdungen bei der Auswahl von Security Awareness Maßnahmen [13]. 39 Prozent aller Unternehmen nutzen das gleiche Maßnahmenpaket für alle Mitarbeiter und 15 Prozent schulen nur IT-Mitarbeiter.

Bada et al. [13] zeigen, warum viele Maßnahmen zur Mitarbeitersensibilisierung versagen und identifizieren fünf Faktoren, welche die Effektivität von Security Awareness Kampagnen verbessern:

- Professionelle Vorbereitung und Organisation
- Keine Ängste bei Mitarbeitern schüren
- Zielgerichte und umsetzbare Schulungsinhalte
- Neue Verhaltensweisen kontinuierlich trainieren und Feedback geben
- Kulturelle Besonderheiten berücksichtigen

Auch das Integrierte Verhaltensmodell zeigt: Um einen Mitarbeiter zu informationssicherheitskonformen Verhalten zu bewegen, ist es notwendig zielgerichtet verschiedene Faktoren zu beeinflussen, die in einem komplexen Zusammenspiel stehen [12]. So müssen Sensibilisierungsmaßnahmen neben Wissen auch die Gewohnheit, die Salienz des Verhaltens, die Verhaltensabsicht und Einschränkungen aus dem Umfeld berücksichtigen.

2.3 ISMS: ISIS12

Um die zunehmende Komplexität der Informationssicherheit in Unternehmen zu beherrschen, empfiehlt sich eine organisierte, kontinuierliche und strukturierte Vorgehensweise durch die Etablierung eines Managementsystems für Informationssicherheit (ISMS). Mit ISIS12 wurde ein Framework zur Entwicklung und Umsetzung eines ISMS geschaffen, dass speziell für die Ansprüche mittelständischer Unternehmen ausgelegt ist [14]. ISIS12 orientiert sich an den Vorgaben der ISO/IEC 27000 Serie und den BSI IT-Grundschutz-Maßnahmen. Das ISIS12-Vorgehensmodell folgt dem aus dem Qualitätsmanagement bekannten PDCA-Zyklus (Plan, Do, Check, Act) (vgl. Abbildung 2). Dies bedeutet, dass die Phasen Planen, Tun, Überprüfen und Handeln wiederholt durchlaufen werden, um das ISMS kontinuierlich zu verbessern, auf aktuelle Bedrohungen zu reagieren und neue Anforderungen umzusetzen.

Der zweite Schritt des Vorgehensmodells heißt „Mitarbeiter sensibilisieren". Die Aktivitäten in diesem Schritt befassen sich mit dem Informieren der Mitarbeiter über

die Informationssicherheit im Unternehmen [14]: Vortrag über ISIS12, die Informationssicherheitsleitlinie des Unternehmens sowie spezifische Bedrohungen und Regelungen; Aushändigen und Unterschreiben der Unternehmensleitlinie für Informationssicherheit; Regelmäßige Information über Richtlinien, Fortgang von Projekten, Ansprechpartnern und anderen Informationssicherheitsthemen; sowie Informationen über Konsequenzen bei Verstößen.

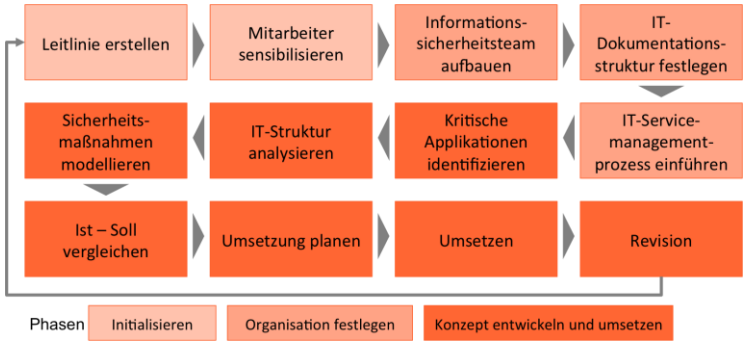

Abbildung 2. Das ISIS12-Vorgehensmodell (in Anlehnung an [14], S. 10).

Diese Art der Mitarbeitersensibilisierung beschränkt sich auf die Sichtweisen Perception und Protection von Security Awareness. Die individuelle Verhaltensabsicht (das Wollen) der Mitarbeiter wird vernachlässigt. Auch werden die meisten der o. g. Erfolgsfaktoren von Security Awareness Kampagnen in die Aktivitäten nicht berücksichtigt. Der Aspekt der Organisation gemäß [23] und der Faktor Einschränkungen aus dem Umfeld (vgl. IBM) werden hingegen in anderen Schritten des ISIS12-Vorgehensmodells adressiert. Organisatorische Maßnahmen, wie die Erstellung einer Leitlinie für Informationssicherheit (Schritt 1), der Aufbau eines Informationssicherheitsteams (Schritt 2) oder die Modellierung von Sicherheitsmaßnahmen (Schritt 8) können die Security Awareness erhöhen, indem die Organisation optimiert und Einschränkungen beseitigt werden.

3 Methodik

Die grundsätzliche Vorgehensweise dieser Arbeit orientiert sich am Design Science-Framework nach Hevner et al. [28] und ordnet sich der gestaltungsorientierten Wirtschaftsinformatik gemäß Österle et al. [29] zu. Demnach verläuft der Forschungsprozess in den vier Phasen Analyse, Entwurf, Evaluation und Diffusion, die iterativ wiederholt werden [29]. Nach Gesprächen mit Vertretern von KMU, Organisationen wie der IHK und Security Awareness Experten sowie einer Literaturrecherche wurde die Forschungslücke identifiziert (Analysephase). In der interdisziplinären Literaturrecherche wurden ISMS-Frameworks sowie wissenschaftliche Veröffentlichungen zu Security Awareness und der Sozialpsychologie einbezogen. Die dabei gewonnenen Erkenntnisse flossen in die

Entwicklung des Vorgehensmodells (Artefakt) ein (Entwurfsphase). Die Forschung befindet sich derzeit am Beginn der ersten Evaluationsphase.

Ein Vorgehensmodell beschreibt eine zeitlich logische Abfolge von Schritten eines Problemlösungsprozesses [30]. Es unterteilt den Prozess in einzelne Phasen und Aktivitäten mit klar definierten Ergebnissen. Der vorgeschlagene Prozess zur Sensibilisierung von Mitarbeitern in KMU stellt ein solches Vorgehensmodell dar.

Zur Vorbereitung der eigentlichen Evaluation in KMU wird das Vorgehensmodell derzeit in einem Projekt an einer bayerischen Hochschule erprobt. Das Bayerische E-Government-Gesetz verpflichtet in Artikel 8 alle bayerischen Hochschulen zur Erstellung und Umsetzung eines Informationssicherheitskonzeptes bis zum 01.01.2018. Um diese Anforderungen erfüllen zu können, werden in einem Teilprojekt die ersten Schritte des ISIS12-Vorgehensmodells durchgeführt. Das zweite Teilprojekt bereitet auf Grundlage des entwickelten Vorgehensmodells eine Kampagne zur Sensibilisierung von Hochschulangehörigen (Mitarbeiter und Studierende) für die Informationssicherheit vor. Hierfür wird bis zum Ende des Jahres 2017 die Ist-Situation analysiert und die Kampagne geplant. Diese soll im Jahr 2018 schließlich durchgeführt werden.

4 Erweiterung von ISIS12

4.1 ISIS12 und Mitarbeitersensibilisierung

Die Sensibilisierung der Mitarbeiter für Informationssicherheit wird im Framework ISIS12 nur unzureichend berücksichtigt. Insbesondere die Aspekte Behavior bzw. Handlungsabsicht von Security Awareness werden kaum beeinflusst. Daher wird im Folgenden eine Erweiterung von ISIS12 vorgeschlagen. Der zweite Schritt „Mitarbeiter sensibilisieren“ im ISIS12-Vorgehensmodell wird herausgenommen. Stattdessen wird ein Vorgehensmodell zur Sensibilisierung ergänzt, welches parallel zu den Aktivitäten von ISIS12 positioniert wird (vgl. **Tabelle 1**). Das Vorgehensmodell zur Mitarbeitersensibilisierung besteht aus den zwei Phasen Analyse (Aktivitäten A bis E) und Kampagne (Aktivitäten F bis H).

Die Parallelität beider Vorgehensmodelle hat folgende Vorteile:

- für beide Prozesse relevante Aktivitäten können gleichzeitig ablaufen,
- die Sensibilisierung kann einfach in das bestehende Framework integriert werden,
- die Sensibilisierung kann auch unabhängig von ISIS12 erfolgen.

Beispielsweise werden im Schritt 6 von ISIS12 kritische Applikationen identifiziert, indem u. a. Gespräche mit Mitarbeitern geführt werden [14]. Im Rahmen dieser Aktivität können die Mitarbeiter auch hinsichtlich ihrer Überzeugungen interviewt werden. Durch die Nutzung von Synergien können im Hinblick auf das Budget der KMU Zeit und Ressourcen gespart werden. Für die Gestaltung der ergänzenden Aktivitäten werden im Folgenden konkrete Handlungsempfehlungen auf Grundlage der Erkenntnisse der Verhaltensforschung gegeben.

Tabelle 1: Gegenüberstellung Vorgehensmodelle ISIS12 und Mitarbeitersensibilisierung

Schritt ISIS12	*Aktivität Mitarbeiter-sensibilisierung*	*Ergebnis*
1) Leitlinie erstellen	-	-
3) Informationssicher-heitsteam aufbauen	-	-
4) IT-Dokumentations-struktur festlegen	A) Verhalten identifizieren	Katalog mit relevanten Verhaltensweisen
5) IT-Servicemanage-mentprozess einführen	-	-
6) Kritische Applikationen identifizieren	B) Interviews führen	Transkribierte Interviews
7) IT-Struktur analysieren	C) Interviews analysieren	Katalog mit Wissensstand, Überzeugungen und Emotionen
8) Sicherheitsmaßnahmen modellieren	D) Fragebögen modellieren	Individuelle Online-Fragebögen
9) Ist – Soll vergleichen	E) Persönliche Faktoren messen	Übersicht Security Awareness Ist-Situation
10) Umsetzung planen	F) Kampagne planen	Ablaufplan der Sensibilisierungskampagne
11) Umsetzen	G) Kampagne durchführen	Zielgerichtet sensibilisierte Mitarbeiter
12) Revision	H) Erneut messen	Erfolgsmessung der Kampagne

4.2 Mitarbeitersensibilisierung – Analyse der Ist-Situation

Basis einer effektiven und zielgerichteten Sensibilisierung ist die Analyse der Ist-Situation im Unternehmen [11] (Aktivität A). Die Identifizierung der relevanten Verhaltensweisen, wie etwa „Ich wähle ein sicheres Passwort“, legt einen Grundstein für alle weiteren Schritte im Prozess. Im Hochschulprojekt wurden hierfür Maßnahmen des ISIS12-Kataloges ausgewählt, bei denen der Mitarbeiter beteiligt ist. Eine Auswahl könnte auch aufgrund von konkreten Sicherheitsvorfällen im Unternehmen erfolgen. Die ausgewählten Verhaltensweisen werden im weiteren Verlauf analysiert und in der späteren Sensibilisierung berücksichtigt.

Kritische Applikationen werden in ISIS12 vor allem mit Hilfe von Mitarbeiter-Interviews identifiziert. Die Interviews können genutzt werden, um Erkenntnisse für die späteren Sensibilisierungsmaßnahmen zu gewinnen. Diese qualitative Untersuchung (Aktivität B) fokussiert neben technischen Hürden gezielt auch kognitive Barrieren der Mitarbeiter. So kann beispielsweise festgestellt werden, welche Überzeugungen der Mitarbeiter das Fassen einer Handlungsabsicht blockieren und welche im Rahmen einer Kampagne besonders gefördert werden müssen. So konnte im Hochschulprojekt festgestellt werden, dass die Mitarbeiter wussten, dass ein Passwort regelmäßig geändert werden sollte, jedoch keine Verhaltensabsicht bestand, dies auch zu tun. Es zeigte sich, dass die Richtlinien der Hochschule hierzu

nicht kommuniziert wurden. So herrschte die normative Überzeugung, dass die Passwortänderung von den Mitarbeitern nicht erwartet wurde. Zusätzlich war die Funktion zum Ändern des Passwortes nicht leicht zugänglich. Diese Barriere wirkte sich negativ auf die Einschätzung der persönlichen Handlungsfähigkeit aus. Durch die Befragung von zirka zehn Prozent der Mitarbeiter aus unterschiedlichen Abteilungen sollen die größten Defizite in deren Verhalten identifiziert werden. KMU erhalten eine erste Übersicht über die im Betrieb vorherrschenden Überzeugungen und Emotionen hinsichtlich des Themas Informationssicherheit. Im Hochschulprojekt wurden Mitarbeiter aus verschiedenen Fakultäten und Serviceeinheiten der Hochschule befragt. Außerdem wurden Studentengruppen aus unterschiedlichen Studiengängen interviewt. Zum Zeitpunkt der Einreichung dieser Arbeit wurde gerade die qualitative Untersuchung abgeschlossen.

Die Analyse der Security Awareness der restlichen Belegschaft erfolgt in der anschließenden quantitativen Untersuchung in Form eines auf den Ergebnissen aus den Interviews basierenden Fragebogens (Aktivität C). Die Modellierung der Fragebögen erfolgt parallel zur Modellierung der Sicherheitsmaßnahmen in ISIS12. Die anschließende Befragung (Aktivität D) parallel zum Vergleich von Ist- und Soll-Situation. Der Fragebogen zur Ermittlung der Security Awareness nutzt unterschiedliche Methoden, um die Faktoren zu messen, die das Mitarbeiterverhalten beeinflussen. Das Wissen der Mitarbeiter kann über klassische Wissensfragen abgefragt werden. Um die Auswertung möglichst einfach zu gestalten, bieten sich hier vor allem Multiple Choice Fragen an. Um die Stärke der in Aktivität B ermittelten Überzeugungen zu messen und so auf die Verhaltensabsicht zu schließen, werden mit den Fragen verknüpfte Skalen verwendet, die je nach Konstrukt variieren können. Der Mitarbeiter drückt damit aus, wie stark seine Zustimmung oder Ablehnung hinsichtlich der Überzeugung ist. Es gibt ähnliche Ansätze, um die Gewohnheit zu messen (vgl. [31]). Lediglich für die Salienz des Verhaltens konnte keine hinreichend bestätigte Testmethode gefunden werden. Dieser Teil der Analysephase sollte möglichst automatisiert ablaufen, um dem geringen Budget von KMU Rechnung zu tragen und eine schnelle und zuverlässige Auswertung der im Betrieb vorherrschenden Security Awareness ermöglichen. Im Hochschulprojekt wird für diesen Zweck die Open-Source-Software LimeSurvey verwendet.

4.3 Mitarbeitersensibilisierung – Planung und Durchführung der Kampagne

Die Ergebnisse der Analysephase fließen in die Gestaltung der Kampagne zur Erhöhung der Security Awareness ein. Die Kampagne berücksichtigt somit die individuelle Ist-Situation im Unternehmen und geht gezielt auf die sensibilisierungsbedürftigen Verhaltensfaktoren und die Unternehmensspezifika ein. Eine Sensibilisierungskampagne kombiniert zielgruppenspezifisch verschiedene Maßnahmen über einen definierten Zeitraum und ähnelt somit einer Marketingkampagne [23]. Auswahl und Inhalte der Maßnahmen (Aktivität F) finden parallel zur Planung der Umsetzung der Sicherheitsmaßnahmen in ISIS12 statt. Die Maßnahmen müssen die Eignung besitzen auf die in der Analyse festgestellten Schwachstellen einzugehen. Fehlendes Wissen soll erhöht, mangelnde Gewohnheit

gefördert, falsche Überzeugungen korrigiert und negative Emotionen ins Positive gewandelt werden. Auch gängige Maßnahmen, wie Präsenzveranstaltung und soziales Marketing haben das Potential eine große Anzahl von Faktoren anzusprechen [32]. Konkrete Maßnahmen sind die Kommunikation der Leitlinie, Newsletter, Beiträge in der Mitarbeiterzeitung, Rollenspiele oder Computer-basierte Trainings. Allerdings sollten die Inhalte der Kampagnen gezielt auf die jeweiligen Faktoren einwirken [32]. Die Gestaltung der einzelnen Maßnahmen und wie diese anhand der Analyse ausgewählt werden, ist Teil von aktuellen Forschungsarbeiten.

Nach der Planung der Kampagne folgt deren Durchführung (Aktivität G). In Präsenzveranstaltungen kann ein Trainer beispielsweise Wissen vermitteln, falsche Überzeugungen durch die Präsentation von Gegeninformationen ändern oder durch Einübung positive Emotionen und Gewohnheit fördern. Soziales Marketing hat das Potential Verhalten zusätzlich salient zu machen, indem beispielsweise bei aktueller Bedrohungslage Newsletter versendet werden. Auf Basis der Analyseergebnisse können auch Erkenntnisse für organisatorische Maßnahmen gewonnen werden, deren Umsetzung die Mitarbeiter bei der Ausübung der Verhaltensweisen unterstützen. Wurde festgestellt, dass die Passwortregeln nicht klar sind, könnten diese bei der Wahl eines neuen Passworts direkt angezeigt werden. Dies wirkt sich positiv auf die Kontroll- und Wirksamkeitsüberzeugungen eines Mitarbeiters aus. In der Analysephase identifizierte unterstützende Faktoren können noch verstärkt werden. Auch Aktivität G könnte aus Budgetgründen zukünftig, in Kombination mit den automatisierten Fragebögen, z. B. durch ein digitales Lernprogramm mit individualisierten Lerninhalten unterstützt werden.

Ähnlich wie die Revision in ISIS12, sollte nach einer definierten Zeitspanne, z. B. nach einem Jahr, der Erfolg der Kampagne gemessen werden (Aktivität H). Dazu können die Fragebögen der Analysephase verwendet werden und die Ergebnisse verglichen werden. Idealerweise zeigt sich eine erhöhte Sensibilisierung der Mitarbeiter. Anschließend kann entschieden werden, ob das Vorgehen bei Aktivität A neu gestartet wird (beispielsweise, da sich die Rahmenbedingungen entscheidend verändert haben) oder ob die Erkenntnisse der Erfolgsmessung in die weitere Planung von Sensibilisierungsmaßnahmen einfließen (Aktivität F).

5 Zusammenfassung und Ausblick

Das Vorgehensmodell hilft KMU dabei einen wichtigen Faktor im Sicherheitskonzept zu analysieren und zu aktivieren: Die eigenen Mitarbeiter. Durch die Analyse der Situation im Unternehmen können zielführende, effektive Kampagnen geplant und durchgeführt werden. Statt die Mitarbeiter mit bereits bekannten Inhalten zu langweilen, werden ihre falschen Überzeugungen korrigiert. Sie werden überzeugt sich informationssicherheitskonform zu verhalten. Zum jetzigen Zeitpunkt ist die Analysephase noch sehr arbeitsintensiv. Durch weitere Forschung soll der Aufwand mit Rücksicht auf die Ressourcen der KMU auf ein Minimum reduziert werden. Die einfache Selektion der Verhaltensweisen, ein allgemeingültiger Überzeugungskatalog und ein standardisierter Wissenstest sollen einen bereits vorab entwickelten, digitalen

Fragebogen möglich machen, der in dem jeweiligen Unternehmen nur noch durchgeführt werden muss. Nach der automatisierten Auswertung der Ergebnisse soll eine Software zudem konkrete Maßnahmen und Inhalte empfehlen, die in einer Kampagne genutzt werden können.

Das Vorgehensmodell beachtet die von [11] identifizierten Erfolgsfaktoren weitgehend. Die Analyse stellt eine professionelle Vorbereitung dar und durch die Kombination mit einem ISMS wird die Organisation gewahrt. Es werden keine Ängste bei den Mitarbeitern geschürt, sondern es wird gezielt versucht negative Emotionen aufzuheben. Die Inhalte sind aufgrund der vorhergehenden Analyse zielgerichtet und können durch bekannte, umsetzbare Maßnahmen vermittelt werden. Auch das Trainieren der Verhaltensweisen wird durch den Faktor Gewohnheit berücksichtigt. Der PDCA-Zyklus sorgt für eine wiederholte Berücksichtigung von noch nicht etablierten Verhaltensweisen und lässt Feedback über den Erfolg der Kampagne zu. Kulturelle Unterschiede werden vor allem in der qualitativen Analyse sichtbar. Dies wird auch im allgemeingültigen Überzeugungskatalog berücksichtigt.

References

1. Schröder, C., Schlepphorst, S., Kay, R.: Bedeutung der Digitalisierung im Mittelstand. Institut für Mittelstandsforschung Bonn, Bonn (2015)
2. BMWi: Monitoring-Report Wirtschaft DIGITAL 2016. BMWi, Berlin (2016)
3. Hlavica, C., Hülsberg, F., Klapproth, U.: Tax Fraud & Forensic Accounting: Umgang mit Wirtschaftskriminalität. Springer Fachmedien, Heidelberg (2016)
4. Scholl, M., Fuhrmann, F.: Analog – digital? Wie sich mithilfe analoger Methoden Bewusstsein für Informationssicherheit in der digitalen Welt fördern lässt. In: Rätz, D. et al. (Hrsg.): Digitale Transformation: Methoden, Kompetenzen und Technologien für die Verwaltung. S. 101-112. Gesellschaft für Informatik, Bonn (2016)
5. Leyh, C., Bley, K.: Digitalisierung: Chance oder Risiko für den deutschen Mittelstand? – Eine Studie ausgewählter Unternehmen. In: HMD Praxis der Wirtschaftsinformatik, 53 (1), S. 29-41. Springer, Heidelberg (2016)
6. Saam, M., Viete, S., Schiel, S.: Digitalisierung im Mittelstand: Status Quo, aktuelle Entwicklungen und Herausforderungen, ZEW GmBH, Mannheim (2016)
7. Schäfer, S., Pinnow, C.: Industrie 4.0 – Grundlagen und Anwendungen. Branchentreff der Berliner Wissenschaft und Industrie. DIN e.V., Berlin (2015)
8. Semba, B., Eymann, T.: Developing a Model to Analyze the Influence of Personal Values on IT Security Behavior. In: Nissen, V. et al. (Hrsg.): Multikonferenz Wirtschaftsinformatik (MKWI) 2016, S. 1083-1091. TU Ilmenau, Ilmenau (2016)
9. Hirshfield, L. et al.: The Role of Human Operators' Suspicion in the Detection of Cyber Attacks. In: International Journal of Cyber Warfare and Terrorism, 5(3), S. 28-44. IGI Global, Hershey (2015)
10. ISACA: State of Cybersecurity. Implications for 2016. An ISACA and RSA Conference Survey. ISACA, Rolling Meadows (2016)
11. Bada, M., Sasse, A., Nurse, J.: Cyber Security Awareness Campaigns: Why do they fail to change behaviour?. In: 1st International Conference on Cyber Security for Sustainable Society, S. 118-131. Coventry University, Coventry (2015)

12. Montaño, D., Kasprzyk, D.: Theory of Reasoned Action, Theory of Planned Behavior, and the Integrated Behavior Model. In: Glanz, K. et al (Hrsg.): Health Behavior and Health Education. Theory, Research and Practice. S. 67–96. John Wiley & Sons, Hoboken (2008)
13. Allianz für Cybersicherheit: Awareness-Umfrage 2015. Bundesamt für Sicherheit in der Informationstechnik, Bonn (2016)
14. Bayerischer IT-Sicherheitscluster (Hrsg.): Handbuch zur effizienten Gestaltung von Informationssicherheit im Mittelstand. Version 1.7. Bayerischer IT-Sicherheitscluster e.V., Regensburg (2014)
15. Eckert, C.: IT-Sicherheit. Konzepte, Verfahren, Protokolle. 4., überarbeitete Aufl. De Gruyter, Oldenburg (2006)
16. Freiling, F. et al.: Technische Sicherheit und Informationssicherheit. In: Informatik Spektrum, 37 (1), S. 14-24. Springer, Berlin, Heidelberg (2014)
17. Kardel, D.: IT-Sicherheitsmanagement in KMU. In: HMD Praxis der Wirtschaftsinformatik, 48 (5), S. 44–51. Springer Vieweg, Wiesbaden (2011)
18. Brandl, S. et al.: DsiN-Sicherheitsmonitor Mittelstand 2016. Deutschland sicher im Netz e.V., Berlin (2016)
19. Pfohl, H.: Abgrenzung der Klein- und Mittelbetriebe von Großbetrieben. In: Pfohl, H. (Hrsg.): Betriebswirtschaftslehre der Mittel- und Kleinbetriebe. S. 1–24. Erich Schmidt Verlag, Berlin (2006)
20. Institut für Mittelstandforschung Bonn: Definitionen. http://www.ifm-bonn.org/definitionen/ (Aufgerufen: 25.10.2016)
21. Bussiek, J.: Anwendungsorientierte Betriebswirtschaftslehre für Klein- und Mittelunternehmen. Oldenbourg Wissenschaftsverlag, München (1996)
22. Hänsch, N., Benenson, Z.: Specifying IT security awareness. In: Morvan, F., Wagner, R., Tjoa, A. (Hrsg.): 25th International Workshop on Database and Expert Systems Applications 2014, S. 326-330. IEEE Computer Society, Los Alamitos, CA (2014)
23. Helisch, M., Pokoyski, D.: Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung, Vieweg+Teubner Verlag /GWV Fachverlage GmbH, Wiesbaden (2009)
24. Kabay, M.: Using Social Psychology to Implement Security Policies. In: Bosworth S., Kabay M. (Hrsg.): Computer Security Handbook. S. 1–22. Wiley, Hoboken (2002)
25. Fishbein, M., Ajzen, I.: Belief, attitude, intention, and behavior. An introduction to theory and research. Addison-Wesley Pub. Co., Reading (1975)
26. Siponen, M.: Five dimensions of information security awareness. In: ACM SIGCAS Computers and Society, 31 (2), S. 24–29. ACM, New York (2001)
27. Thomson, M., Solms, R.: Information security awareness: educating your users effectively. In: Information Management & Computer Security, 4 (6), S. 167–173. Emerald Group Publishing Limited, Bingley (1998)
28. Hevner A. et al.: Design Science in Information Systems Research. In: MIS Q 28, S. 75–105. University of Minnesota, Mineapolis (2004)
29. Österle, H. et al.: Memorandum zur gestaltungsorientierten Wirtschaftsinformatik. In: Zeitschrift für betriebswirtschaftliche Forschung, 6, Nr. 62, S. 664-672 (2010)
30. Winter, R.: Business Engineering Navigator. Springer-Verlag. Berlin, Heidelberg (2011)
31. Verplanken, B., Orbell, S.: Reflections on Past Behavior: A Self-Report Index of Habit Strength. In: Journal of Applied Social Psychology (33), S. 1313–1330 (2003)
32. Schütz, A., Weber K.: Security Awareness: Nicht nur schulen – überzeugen Sie! In: Schartner, P., Baumann, A. (Hrsg): D•A•CH Security 2017, S. 1-12. Syssec, Frechen (2017)