Information Security Awareness – eine konzeptionelle Neubetrachtung

Sebastian Richter[1], Tobias Straub[1], Carsten Lucke[2]

[1] DHBW Stuttgart, Zentrum für Wirtschaftsinformatik, Stuttgart, Germany
{sebastian.richter@dhbw-stuttgart.de, tobias.straub@dhbw-stuttgart.de }
[2] TH Mittelhessen, Kompetenzzentrum für Informationstechnologie, Friedberg, Germany
{carsten.lucke@mnd.thm.de}

Abstract. Das Konzept „Information Security Awareness" (ISA) wird zur Betrachtung und Bemessung des menschlichen Sicherheitsbewusstseins herangezogen. Der vorliegende Beitrag illustriert die gegenwärtige Heterogenität der Benutzung des ISA-Konzepts und unternimmt eine konzeptionelle Neubetrachtung. Unsere Definition basiert auf einer Analogie zum aus der Psychologie stammenden Konzept des Situationsbewusstseins (Situation Awareness) und unterscheidet die Dimensionen von ISA vergleichbar dem Informationsmanagement nach Krcmar, um so eine differenzierte Betrachtungsweise zu ermöglichen. Dies fördert den intuitiven Umgang mit dem Begriff und verringert Missverständnisse.

Keywords: Informationssicherheit, Information Security Awareness, Konzeptentwicklung, Mentales Modell

1 Einleitung

Es liegt im vitalen Interesse von Organisationen im öffentlichen und privaten Sektor, Vertraulichkeit, Integrität und Authentizität sowie Verfügbarkeit als die grundlegenden Schutzziele der Informationssicherheit (Information Security, IS) zu gewährleisten [1]. Bei der Umsetzung dieser Anforderungen hat der Faktor Mensch eine wesentliche Rolle, sind es doch häufig Mitarbeiter der eigenen Organisation, die – meist ungewollt, teilweise auch gewollt – eine Kompromittierung der Sicherheit erst ermöglichen [2,3].

Vor allem, um ungewolltes Fehlverhalten bezüglich der Informationssicherheit zu vermeiden, bilden Organisationen ihre Mitarbeiter zunehmend aus, um die Information Security Awareness (ISA) zu erhöhen (vgl. [4-6]). Gleichzeitig formulieren Organisationen Regeln (vgl. [7,8]), um ihren Mitarbeitern Sicherheit im Umgang mit schützenswerten Informationen (*Assets*, sowohl digitalisiert als auch analog) zu geben.

Bei der Analyse des in der Wissenschaft genutzten Konzepts fällt auf, dass die Definition von ISA sehr heterogen und in weiten Teilen einschränkend erfolgt. Oft wird darunter nur das Bewusstsein über Vorhandensein und Inhalt der

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

Sicherheitsregeln verstanden (vgl. [9,10]). In dieser Arbeit wird eine neue Sichtweise entwickelt, die es ermöglicht, das Mitarbeiterverhalten bezüglich der Informationssicherheit differenzierter beschreiben zu können. Dazu wird im folgenden Abschnitt zunächst die Bandbreite der Definitionen dargestellt. Der zentrale Beitrag dieser Arbeit ist die in Abschnitt 3 vorgeschlagene Neukonzeption auf Basis des Ansatzes der *Situation Awareness* unter Einbeziehung des Modells des Informationsmanagements nach Krcmar (vgl. [25]). Die Konzeptualisierung wird abgerundet durch eine Betrachtung, aus welcher Analyseperspektive (Individuum, Team, Organisation) ISA untersucht werden kann.

2 Das ISA-Konzept – State-of-the-Art-Analyse

Eine *Leitlinie zur Informationssicherheit* (Information Security Policy, ISP) wird auf strategischer Ebene einer Organisation definiert. Für Mitarbeiter werden verbindliche *Richtlinien* (Information Security Regulations) abgeleitet, die der operativen Umsetzung der Leitlinie dienen [9,11]. Dies ist ein probater und auch aus Gründen der Governance ratsamer Weg, um Mitarbeitern Handlungssicherheit im Umgang mit Assets zu ermöglichen. Zur sprachlichen Vereinfachung ist im Verlauf einheitlich von *Regeln* die Rede, wenn Vorgaben der Leitlinie und der Richtlinien gemeint sind. Bei der Analyse, wann und warum sich Mitarbeiter an die Regeln halten oder nicht, spielt das Konzept ISA eine wichtige Rolle (vgl. [5,7,9]).

2.1 Gängige Definitionen

Nachfolgend wird aufgezeigt, wie das ISA-Konzept in der Wissenschaft definiert ist. Anstelle eines ausführlichen Literature Review (wie ihn etwa [1] bzgl. der möglichen Maßnahmen zur Steigerung und Aufrechterhaltung von ISA durchführt), wird hier anhand ausgewählter Definitionen die Heterogenität bei der Benutzung des ISA-Konzepts illustriert.

Die folgende Definition aus [12] verdeutlicht das in der Literatur vorherrschende Konzeptverständnis exemplarisch.

> *"We thus view security awareness as consisting of three interrelated and inter-dependent parts that are required to be mutually understood and in balance: formal security awareness, cognitive security awareness and behavioral security awareness. […] Security awareness is thus about understanding the information security policies, as well as complying with them."*

ISA im engeren Sinne drückt somit aus, ob und inwieweit Mitarbeiter die Regeln ihrer Organisation kennen und verstehen. Ein hohes Maß an ISA führt – bei entsprechender Motivation und Nutzenerkenntnis – zur Befolgung der Regeln [9,10]. Ein weiteres Beispiel [13] betont den instrumentalen Charakter von ISA sowie die Ausrichtung auf die Einhaltung der Regeln wie folgt:

„Information security awareness is a vital communication tool used by organizations to influence end-users towards compliance with information security policies and controls in the organization.“

Ohne Anspruch auf Vollständigkeit zeigt **Tabelle 1** verschiedene Definitionen für das ISA-Konzept, auf die im Verlauf teilweise eingegangen wird.

Tabelle 1: Einige Beispiele für verschiedene Informations- bzw. informationssystem- und informationstechnologiebezogene Awareness-Begriffe.

Nr.	***Quelle*** / **Definition (D)** / **Verständnis (V)**	***Begriff***
1	*Wilson und Hash 2003 [14]* **D:** „Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly.” **V:** Initiales Wissen, dass es IT-Sicherheit gibt und welche Verhaltensmuster für jedermann adäquat sind.	*IT Security Awareness*
2	*Hellquist et al. 2013 [12]* **D:** “Security awareness is thus about understanding the information security policies, as well as complying with them.” **V:** Ziel von Awareness ist, dass sich Mitarbeiter der Verhaltensregeln bewusst sind und sich entsprechend verhalten.	*Security Awareness*
3	*Banerjee et al. 2013 [15]* *Banerjee und Pandey 2010 [16]* **D:** „Security awareness can be defined as the knowledge that members of an organization possess regarding protection of the physical and information assets of that organization.” **V:** Software Security Awareness wird als Konzept selbst nicht definiert, stützt sich jedoch auf eine Definition der Security Awareness ab. Als allgemeinerer Wissensbegriff umfasst es Wissen, wie schützenswerte Güter gesichert werden können.	*Software Security Awareness*
4	*Bulgurcu et al. 2010 [9]* **D:** “Information security awareness is defined as an employee’s general knowledge about information security and his cognizance of the information security policy (ISP) of his organization. General information security awareness and ISP awareness are the key dimensions of ISA. General information security awareness is defined as an employee’s overall knowledge and understanding of potential issues related to information security and their ramifications. Beyond general ISA, organizations have specific expectations of their employees that are reflected in the ISP. ISP awareness is defined as an employee’s knowledge and understanding of the requirements prescribed in the organization’s ISP and the aims of those requirements.” **V:** Unterscheidung zwischen generellem Wissen über IT-Sicherheit und dem Wissen um die in der Organisation geltenden Regeln.	*- Information Security Awareness* *- General Information Security Awareness* *- Information Security Policy Awareness*

Nr.	*Quelle* **Definition (D)** **Verständnis (V)**	*Begriff*
5	*Choi et al. 2008 [17]* **D:** “Managerial Information Security Awareness in the current study particularly focuses on how senior managers regard the significance of information security.” **V:** Begriff beschreibt die wahrgenommene Wichtigkeit von Information Security bei Managern der obersten Führungsebene mit Bezug zur eigenen Aufgabe.	*Managerial Information Security Awareness*
6	*Siponen 2000 [10]* **D:** "The term 'information Security awareness' is used to refer to a state where users in an organization are aware of - ideally committed to - their security mission (often expressed in end-user security guidelines)." **V:** Begriff bezieht sich auf den Idealzustand, dass sich Mitarbeiter nicht nur ihres Sicherheitsauftrags bewusst sind, sondern ihn befolgen.	*Information Security Awareness*
7	*Spears und Barki [18]* **D:** "Thus, organizational awareness refers to different target groups (e.g., end users, IS professionals, senior management, third parties, etc.) that exhibit a consciousness about organizational policies, procedures, or the need to protect sensitive information." **V:** Differenzierte Sichtweise, die verschiedene Nutzergruppen bezüglich der Sensitivität von schützenswerter Information unterscheidet und den Mitgliedern dieser Gruppen unterschiedliche Sichtweisen zuspricht.	*Organizational Awareness*

2.2 Begriffskritik

Bei Betrachtung der Konzeptdefinitionen in Tabelle 1 fällt auf, dass verschiedene Bezeichner für gleiche bzw. ähnliche Konzepte verwendet werden, ohne dass die Gründe hierfür ersichtlich wären. Die sich ergebende Frage angesichts der Begriffsheterogenität ist, ob IT Security Awareness und Information Security Awareness tatsächlich das gleiche Konzept ist.

Um diese Frage zu beantworten, kann man sich über verschiedene Rollen und deren Tätigkeiten dem Konzeptverständnis nähern. Zunächst scheint es ratsam, Endnutzer oder Manager nicht mit detaillierten technischen Vorgaben (z.B. Firewall-Regeln) zu konfrontieren, wie der Bezeichner IT Security Awareness implizieren würde. Ein Manager muss jedoch Bewusstsein bezüglich schützenswerter Informationen, die in seiner Reichweite sind, haben. Hierzu gehören z.B. auch ausgedruckte Unterlagen, die er physisch transportiert, was intuitiv dem Bezeichner Information Security Awareness zuzuordnen wäre. Es liegt also nahe, mit Hilfe von Rollen und deren Umgang mit Technik bzw. Information das Konzept Security Awareness zu durchdenken.

Bei den obigen Definitionen fällt weiter auf, dass der Begriff Awareness – also am ehesten Bewusstheit – sich auf Wissen um Regeln (Nummern 2, 4, 6, 7) oder aber auf ganz allgemeines Wissen bezüglich Informationssicherheit (Nummern 3, 4) bezieht. Somit hat das Konzept im Gegensatz zum allgemein in der Psychologie gebräuchlichen Awarenesskonzept keinen expliziten Umweltbezug. Im Kern meint das Awarenesskonzept, abhängig von der Umweltentwicklung eigene Handlungen

anzupassen. Die mentale Bewusstheit über Vorgänge – sowohl im Inneren des Menschen aber vor allem bezüglich der Wirkung der äußeren Umgebung auf den eigenen Erfahrungskontext sind Gegenstand des Awarenesskonzepts. Der gestalttherapeutische Begriff Awareness meint *"ein 'mehr Dinge in der Umwelt oder an sich selbst Wahrnehmen' [...], in welchem weniger Bewertung und Absichtlichkeit liegt."* [19]. Insofern würde der Begriff Information Security Awareness eher auf einen Zustand hindeuten, in dem Mitarbeiter bei Ihren Handlungen die Gefährdung und den Schutz von Informationen durch ihre Handlungen ständig bewerten und entsprechend handeln. Regularien können hierbei zweifelsohne helfen.

Ein entscheidender Nachteil, wenn sich Awareness nur auf Regularien bezieht, ist, dass das Konzept zu widersprüchlichen Aussagen führen kann. Crossler et al. identifizieren in ihren Untersuchungen zur „Behavioral Information Security" den Bedarf, Innentäter, die mit vollem Bewusstsein und Willen handeln, von Personen, die aus Versehen und Unwissenheit handeln, zu unterscheiden und dazu passende Konzepte zu entwickeln [20]. Interessanterweise würde man bei beiden Verhaltensweisen eine geringe ISA im engeren Sinn konstatieren, was insofern kontraintuitiv ist, als dass ein Mitarbeiter, der Regeln bewusst bricht, diese sehr gut kennt, aber eben Schaden anrichten möchte.

Basierend auf diesen Gedanken erscheint es sinnvoll, das Konzept Information Security Awareness zu überdenken. Dabei werden folgende Anforderungen gestellt:

1. Die Konzeptverwendung sollte der allgemeinen sprachlichen Intuition entsprechen.
2. Der bewusst gewählte Begriff Awareness sollte ebenso wie in der Psychologie, aus dem er entstammt, einen Bezug zur Handlung und zur Umwelt haben.
3. Das Grundkonzept sollte Security Awareness heißen, so dass die Präfixe *IT*, *IS* und *Information* als qualifizierende Bezeichner echte Bedeutung erlangen.
4. Bei der Verwendung des Konzepts sollte Klarheit über die Analyseebene herrschen: Ist das Konzept auf der Ebene des Individuums, auf der Ebene des Teams oder auf der Ebene der Organisation angesiedelt?

3 Das Konzept Security Awareness – eine Neubetrachtung

Ganz intuitiv soll hohe Information Security Awareness eines Mitarbeiters zunächst so verstanden werden, dass er sich bei seinem Handeln darüber bewusst ist, dass – aber auch in welchem Maße – die Informationen, mit denen er umgeht, schützenswert sind und welche Bedrohungen der Informationssicherheit im Rahmen seiner Handlungen bestehen oder erst durch seine Handlungen entstehen und wie er diesen begegnen kann (vgl. hierzu auch [5]).

3.1 Situation Awareness

Um dieses intuitive Verständnis genauer zu modellieren, wird in Analogie das Konzept *Situation Awareness* (Situationsbewusstsein), das mit Hilfe von [21] erklärt wird, genutzt. Einzelpersonen oder Gruppen von Personen erzeugen mentale Repräsentationen ihrer Umgebung, um eigene Handlungen an dieser Repräsentation,

aber vor allem an der Antizipation der kurzfristigen Weiterentwicklung der Umgebung auszurichten [21]. Der Prozess des Aufbaus des mentalen Modells verläuft in den Phasen *Perzeption*, *Verarbeitung* und *Projektion*, bezogen auf die Umwelt und deren jeweilige Veränderung (vgl. [22,23]). Die Phase *Handlung* wird zur Situation Awareness nicht hinzugezählt. Das Modell stellt dar, dass Individuen zyklisch durch sensorische Wahrnehmungen und deren mentaler Verarbeitung das für das eigene Handeln relevante Umweltbild aktualisieren. Bereits in der Ursprungstheorie hat Endsley dieses Modell auf Teams übertragen [21].

Warum eignet sich die Übertragung dieses Modells auf das ISA-Konzept? Bei der Betrachtung von Gefährdungen der Informationssicherheit geht man typischerweise von einer dynamischen Umwelt aus, in der a priori unbekannte Akteure versuchen, auf (Informations-)Ressourcen der Organisation in von ihr nicht intendierter Weise zuzugreifen. Die Dynamik ergibt sich insbesondere dadurch, dass zeitgleich viele legitime Zugriffe geschehen und so eine hohe Änderungsrate im Informationsbestand herrscht. Eingebettet in diese dynamische Umwelt, sollten Mitarbeiter zunächst „aware“ bei eigenen Handlungen sein. Sie sollten Umweltveränderungen, aber auch die durch eigene Handlungen entstehende Veränderung zunächst wahrnehmen, auf dieser Basis verarbeiten, und darauf aufbauend ein Bewusstsein entwickeln, wie die Veränderungen in naher Zukunft wirken (bspw., welche Sicherheitsgefahren aus den Handlungen entstehen, aber auch, ob eigene Handlungen Regularien widersprechen).

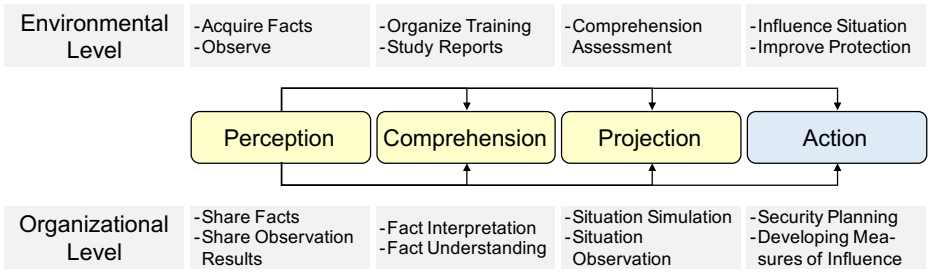

Abbildung 1: ISA basierend auf der Entwicklung von Situation Awareness

Die Abbildung visualisiert die Modellübertragung aus Sicht der Gesamtorganisation (die hier Awareness erlangt):

- *Perzeption* von Veränderung bedeutet, die Umwelt zu beobachten und so relevante Fakten zu sammeln. Dies können neue Angriffsvektoren oder Sicherheitswerkzeuge sein, auf die die Organisation aufmerksam wird. Beobachten bedeutet, dass die Organisation Angriffsversuche detektieren kann, etwa weil einzelne Mitarbeiter Bewusstsein für entsprechende Vektoren haben. Auf Organisationsebene gilt es, gesichtete Fakten und Beobachtungen zu teilen, um die Awareness zu steigern.
- Bei weitergehender Verarbeitung dieser „Reize“ (*Comprehension*) gilt es, bereits verarbeitete und zur Organisation passende organisationsexterne Information bzw. Wissen zu sichern. Dies kann in Form „eingekaufter“ Trainings, aber auch in der gezielten Auswertung von Studien und Erkenntnissen, geschehen. Diese

Verarbeitung ist im Innern zu interpretieren, zu verdichten und ins mentale Bewusstsein aufzunehmen, um künftige Gefährdungen erkennen und adäquat handeln zu können.
- Zum Schutz vor Bedrohungen wird bei der *Projektion* die nahe Zukunft vorhergesagt, insbesondere unter Berücksichtigung aktueller Eintrittswahrscheinlichkeiten. Auf organisationaler Ebene können hierbei „Simulationen" von Bedrohungsszenarien helfen, aber auch die gezielte Überwachung von Situationen, z.B. durch Honeypots. Diese Projektion ermöglicht Handlungen, die letztlich in ein integriertes Sicherheitsmanagement führen.

Bei diesem Modellansatz wird dem Mitarbeiter nicht nur eine passive Rolle der Regeleinhaltung zugewiesen. Vielmehr soll ein tiefergehendes Verständnis der Regeln bezüglich der jeweiligen Rollen der Mitarbeiter entwickelt werden. Handlungssicherheit ist das Ziel.

Der Vorteil des beschriebenen Konzepts liegt darin, Mitarbeiter zu eigenständigem Handeln und zur Eigenverantwortung zu ermutigen. Wie Balozian und Leidner zeigen, empfinden Mitarbeiter negativen Stress, wenn sie Regeln nicht verstehen und diese ihre Arbeit beeinflussen, was oftmals zum Umgehen der Regeln führt [11]. Awareness würde aber bedeuten, dass Mitarbeitern der Nutzen der Regeleinhaltung klar ist und ihre Motivation hierfür steigert. Ein anderes Problem entsteht, wenn die Regeln nicht mehr geeignet sind, neuesten Bedrohungen zu begegnen. Im Rahmen der Systemadministration etwa bedeutet Security Awareness mehr als Regelkenntnis und -einhaltung, weil Administratoren eben selbst die Regeln entwickeln müssen und zwar gemäß ihrer Awareness bezüglich der Bedrohungen der Umwelt. In diesem Kontext werden Mitarbeiter beim Testen der Sicherheit bewusst Regeln brechen, gerade weil ihre Security Awareness so hoch ist. Das vorgeschlagene Konzept bringt den Begriff der Security Awareness in Einklang mit diesen Beispielen und macht ihn intuitiv nutzbar.

3.2 Bildung von Subkategorien

Tabelle 1 macht deutlich, dass bezüglich des Konzepts Security Awareness die Bezeichner IT, IS und Information überraschenderweise weitestgehend synonym verwendet werden. Erachtet man den qualifizierenden Bezeichner als reine Geschmackssache, so wird das Konstrukt unspezifischer und den unterschiedlichen Gefährdungen der Informationen nicht gerecht. Diese können stark variieren, je nachdem, welches Medium zum Transport bzw. zum Speichern der Information betrachtet wird. Die Gefährdung, die z.B. durch einen im PKW verbliebenen Papierausdruck von Geschäftsunterlagen (Information) entsteht, ist eine andere, als wenn durch Vergabe leicht zu erratender Passwörter tausende Datensätze eines Datenbanksystems kopiert werden können (IS) oder aber, wenn durch unerlaubtes Öffnen eines Ports Schadsoftware den Weg ins organisationseigene Netz finden kann (IT). Da zumindest in größeren Organisationen Mitarbeiter bezüglich des Zugriffs und der Konfiguration der IT-Infrastruktur aber auch der Informationen an sich sehr

unterschiedliche Kenntnisse und auch Rechte haben, ist es durchaus sinnvoll, das Konzept Security Awareness klarer zu differenzieren.

Krcmar schlägt für das Informationsmanagement ein Modell gemäß Abb. 2 vor, das verschiedene Managementebenen unterscheidet, bei denen jeweils die gleichen Führungsaufgaben, wozu auch IT-Sicherheit gehört, umzusetzen sind [25]. Die vorgeschlagenen Ebenen sind Informations- und Kommunikationstechnik (IKT), Informationssysteme (IS) und Information.

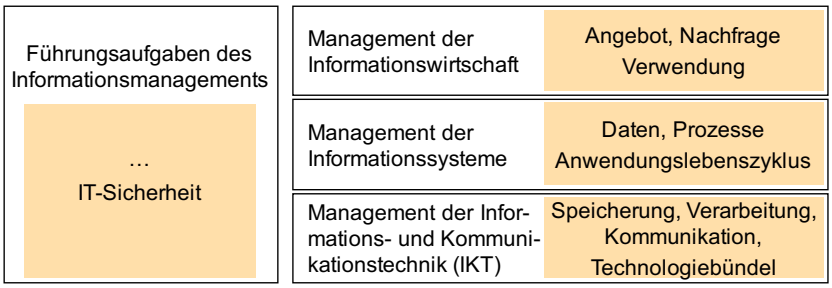

Abbildung 2: Modell des Informationsmanagements nach Krcmar [25]

Es scheint sinnvoll und fruchtbar, diese Unterscheidung für eine Neukonzeption der Security Awareness in folgender Weise zu übernehmen.[1]

- *IT Security Awareness* wird definiert als der (bezüglich der Sicherheitsgefahren) bewusste Umgang mit IT. Hier sind z.B. Konfiguration und Betrieb von Firewalls oder die Nutzung von Antiviren-Software gemeint. Eine ausgeprägte IT Security Awareness ist etwa für Mitarbeiter erforderlich, die IT bereitstellen. Diese Art Awareness ist dagegen weniger für Mitarbeiter nötig, die als Anwender IT nutzen, wenngleich die Übergänge nicht trennscharf sind.
- *IS Security Awareness* wird definiert als der bewusste Umgang mit Informations- und Kommunikationssystemen. Darunter fällt der Umgang mit Passwörtern, die Auswirkungen von Phishing-Mails und anderen Gefahren, die der Organisation durch Anwendung komplexer IS drohen. Diese Art Awareness benötigen zwar alle Mitarbeiter einer Organisation, aber wiederum sehr unterschiedlich. Während auf technischer Ebene Fragen des Identity and Access Managements relevant sind, müssen Benutzer eher den Zugangsschutz oder das Verteilen der Informationen aus sicherheitsrelevanter Sicht durchdringen.
- *Information Security Awareness* schließlich wird definiert als der bewusste Umgang mit Informationen, unabhängig vom Medium.

Besonders beim Erstellen von Schulungen oder -Kampagnen sollte – im Rahmen der Personalisierung der Ausbildung – die Zuordnung der jeweiligen Ebene durchdacht sein und Bewusstsein herrschen, welches Konstrukt wirklich angesprochen wird.

[1] Aufgrund der naheliegenden Bezeichnungen für die drei Ebenen werden diese Präfixe weiter verwendet und die "Überladung" bestehender Begriffe in Kauf genommen. Im Rest des Beitrags werden die nachfolgenden Definitionen verwendet.

IT Security Awareness fokussiert nicht unmittelbar die Gefährdung der Information, sondern die technische Komponente der IT und somit nur indirekt die mittels IT „verwaltete“ Information. IS Security Awareness hat technische und informationale Anteile. Information Security Awareness behält ebenfalls eine technische Komponente, weil die meisten Informationen mittels technischer Medien gespeichert und verbreitet werden.

Es ist möglich, die drei Konzepte definitorisch scharf voneinander abzugrenzen. Es ist aber anzunehmen, dass diese Trennschärfe empirisch nicht gegeben ist, da das Konzept ein mentales ist, das primär anhand der Handlungen eines Individuums beobachtbar wird. Der Mitarbeiter wird dabei in unterschiedlichem Maße alle drei Konzepte benötigen, um das angestrebte Schutzniveau zu erreichen. Jedoch wird die Gewichtung der drei Konzepte je nach Position und Rolle eines Mitarbeiters variieren. So muss ein Administrator über viel IT Security Awareness und u.U. weniger über Information Security Awareness verfügen. Bei einem Manager strategischer Ebene wird es im Allgemeinen umgekehrt sein. Sachbearbeiter werden eher IS Security Awareness benötigen.

3.3 Die Analyseebene des Konstrukts

Bei einem sozialen bzw. organisationalen Konstrukt wie ISA sollte beschrieben werden, auf welcher Ebene der Analyse (Individuum, Team, Organisation) es betrachtet wird [26]. Zunächst ist Awareness ein kognitives, auf der **Ebene des Individuums** angesiedeltes Konstrukt [21]. Wie oben beschrieben, nimmt das Individuum Umweltreize auf und verarbeitet diese, um eigene Reaktionen anzupassen. Bezogen auf Security Awareness ist es das Individuum, das sich der Gefahren bewusst wird und entsprechend handelt. Hierbei ist das Wissen um Bedrohungen und Schutzmaßnahmen zentral. Zusätzlich benötigt das Individuum die Fähigkeit, dieses Wissen in den Anwendungskontext spezifischer Handlungssituationen zu setzen (vgl. Modell der Wissenstreppe [27]), um Wissen über z.B. IT-Sicherheit oder aber Regularien der Organisation anzuwenden. Dazu muss es die Reize der Umwelt (z.B. den Kontext von Gesprächen oder die Konfiguration von IT-Systemen) zyklisch auswerten und so die Umwelt bewerten.

IT, IS und Information Security Awareness können ebenso auf **Teamebene** betrachtet werden. Unter einem Team wird eine Gruppe von Menschen verstanden, die hohe Zielkonvergenz haben und gleichzeitig in einem Setting hoher Interdependenz arbeiten, um bspw. ein Projektziel zu verwirklichen [28]. Es stellt sich z.B. die Frage, ob ein Softwareentwicklungsteam über hohe Security Awareness verfügt. Das Konstrukt bezieht sich dann auf eine Gruppe von Menschen, die einerseits miteinander interagiert und sich beeinflusst und andererseits Sichten, Fähigkeiten und Wissen, bezogen auf das zu lösende Problem, spezialisiert (vgl. [29,30]). Mentale Modelle, die solch ein Team entwickelt, sind Team-Level-Konstrukte (vgl. [22,31]). Das bedeutet, dass dieses Konstrukt auf Teamebene nicht anhand der Individuen betrachtet werden kann (z.B. durch „Summation“ oder „Durchschnittsbildung“ der individuellen Awareness), sondern nur durch Beobachtung und Bewertung des kompletten Teams. Wenn Rollen im Team

spezialisiert sind, wird auch die individuelle Security Awareness spezialisiert sein. Wenn z.B. in einem Softwareentwicklungsteam ein Teammitglied für Datenbankprogrammierung verantwortlich ist, muss dieses Teammitglied vor allem Angriffsvektoren und Gegenmaßnahmen kennen, die sich auf Datenbanken beziehen. Das sind andere Bedrohungen als bei der Entwicklung von User Interfaces. Wichtig ist allerdings die Verbindung und Interdependenz dieser Bedrohungen. Es sollte im Team also gemeinsames Wissen darüber herrschen, dass die Umwelt in spezifischen situativen Entwicklungen unterschiedlichen Einfluss auf die Informationssicherheit bezüglich der Arbeit oder Handlungen von Mitgliedern des Teams nimmt. Weniger wichtig ist, dass jeder im Team weiß, welchen spezifischen Einfluss die Entwicklung bzgl. der Informationssicherheit bei den Partnern im Team hat. Hierfür ist das spezialisierte Wissen im Team nötig. Dennoch sollte das Wissen um die Bedrohung kommuniziert werden, sollte ein Teammitglied bspw. die Auswirkung einer spezifischen Konfiguration nicht bemerkt haben. Da Security Awareness den vorstehenden Ausführungen zufolge also nicht auf der individuellen Ebene erfasst werden kann, ist das generelle Messen des Teamkonstrukts im Grunde nur indirekt (anhand der Beobachtung der Handlungen im Team) und nicht mehr (gut) introspektiv möglich. Fragebogenmethoden sind hier beispielsweise relativ schwer anwendbar.

Awareness kann ebenso auf **Organisationsebene** angesiedelt sein. Hier gelten die Aussagen zur Teamebene weitestgehend analog. Bereits Siponen betrachtet die Organisation als Dimension für Information Security Awareness [32]. Es wird durch dieses Konstrukt das Bewusstsein der gesamten Organisation (manifestiert durch gemeinschaftliche Handlungen) hinsichtlich der Bedrohungen der Umwelt in Bezug auf Informationssicherheit adressiert. Auch hier ist die Frage nach dem Messen des Konstrukts wichtig und nicht einfach zu beantworten.

4 Synthese und Ausblick

Basierend auf der Betrachtung der vorhandenen teils heterogenen und teils ungenauen Definitionen des Konstrukts Information Security Awareness liefert dieser Beitrag eine andere – eher auf das gestalttherapeutische Konstrukt Awareness bezogene – Betrachtung und fügt weitere Dimensionen hinzu.

Das Konstrukt kann auf der Ebene des Individuums, des Teams oder der Organisation analysiert werden, wodurch sich in Relation die Umwelt ergibt, auf die sich Awareness bezieht. Security Awareness selbst beschreibt einen Verarbeitungs- und letztlich Prognoseprozess, der sich aufgrund des vorhandenen Wissens und der Perzeptionen der Umweltveränderungen ergibt. Es hilft, vor allem für Schulungen, Security Awareness in den Unterkategorien IT, IS und Information zu betrachten.

Die Vorteile des Modells liegen in der differenzierten Betrachtungsweise und vor allem darin, dass der neue Konzeptbegriff anschlussfähig zu dem Wissenschaftsgebiet – der Psychologie – wird, dem das Konzept Awareness entstammt.

Ein Nachteil des so definierten Konzepts ist, dass es, wie alle mentalen Modelle, schwer messbar ist [31,33]. Verbreitete, auf Introspektion basierende Fragebogen-

konzepte scheinen hier schwer umsetzbar. Vielmehr kann man Spuren mentaler Modelle am ehesten durch Beobachtung von Handlungen zeigen [22]. Aus diesem Nachteil ergibt sich direkt die Forderung, dass sich das vorgestellte Konzept empirisch bewährt, beides zusammen ist Gegenstand zukünftiger Forschung.

Das Security Awareness-Konzept ist hilfreich für Praktiker, weil es stark an der Handlung der Mitarbeiter orientiert ist und diese erklären hilft. Darüber hinaus können Schulungsmaßnahmen mit Hilfe des Modells besser beschrieben und somit koordiniert werden. Aus wissenschaftlicher Sicht hilft es, einige, mit der bisherigen Konzeptualisierung verbundenen Widersprüche, wie bspw. die vermeintlich niedrige Awareness von Innentätern zu überwinden. Zudem ist das Konzept differenzierter, so dass ebenfalls genauer adressiert werden kann, was Kern der Analyse ist.

Literatur

1. Puhakainen, M.: A design theory for information security awareness. Faculty of Science, University of Oulu, Oulu (2006)
2. Chen, Y., Ramamurthy, K., Wen, K.-W.: Organizations' Information Security Policy Compliance. Stick or Carrot Approach? Journal of Management Information Systems 29, 157–188 (2012)
3. PwC: Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security® Survey 2015, www.pwc.com/gsiss2015
4. Puhakainen, M., Siponen, M.T.: Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. MIS Quarterly 34, 757–778 (2010)
5. Häussinger, F., Kranz, J.: Antecedents of Employees' Information Security Awareness - Review, Synthesis, and Directions for Future Research. In: Proceedings of the Twenty-Fifth European Conference on Information Systems (ECIS) (2017)
6. Karjalainen, M., Siponen, M.: Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches. Journal of the Association for Information Systems (JAIS) 12, 518–555 (2011)
7. D'Arcy, J., Hovav, A., Galletta, D.: User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse. A Deterrence Approach. Information Systems Research 20, 79–98 (2009)
8. Whitman, M.E., Townsend, A.M., Aalberts, R.J.: Information Systems Security and the Need for Policy. In: Dhillon, G. (ed.) Information Security management: Global Challenges in the New Millennium, pp. 10–20. IGI Global, Hershey (2001)
9. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS. MIS Quarterly 34, 523–548 (2010)
10. Siponen, M.T.: A conceptual foundation for organizational information security awareness. Information Management & Computer Security 8, 31–41 (2000)
11. Balozian, P., Leidner, D.: IS Security Menace: When Security Creates Insecurity. In: Proceedings of the 37th International Conference on Information Systems (ICIS) (2016)
12. Hellquist, F., Ibrahim, S., Jatko, R., Andersson, A., Hedström, K.: Getting their Hands Stuck in the Cookie Jar - Students' Security Awareness in 1:1 Laptop Schools. International Journal of Public Information Systems 9, 1–19 (2013)

13. Rastogi, R., von Solms, R.: Information Security Service Branding – beyond information security awareness. SYSTEMICS, CYBERNETICS AND INFORMATICS 10, 54–59 (2012)
14. Wilson, M., Hash, J.: Building an Information Technology Security Awareness and Training Program. NIST - National Institute of Standards and Technology, Gaithersburg (2003)
15. Banerjee, C., Banerjee, A., Murarka, P.D.: An Improvised Software Security Awareness Model. International Journal of Information, Communication and Computing Technology 1, 43–48 (2013)
16. Banerjee, C., Pandey, S.K.: Research on software security awareness: Problems and Prospects. SIGSOFT Software Engineering Notes 35, 1–5 (2010)
17. Choi, N., Kim, D., Goo, J., Whitmore, A.: Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. Information Management & Computer Security 16, 484–501 (2008)
18. Spears, J.L., Barki, H.: User Participation in Information Systems Security Risk Management. MIS Quarterly 34, 503–522 (2010)
19. Blankert, S., Doubrawa, E.: Lexikon der Gestalttherapie. Peter Hammer Verlag, Wuppertal (2005)
20. Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R.: Future directions for behavioral information security research. Computers & Security 32, 90–101 (2013)
21. Endsley, M.R.: Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors 37, 32–64 (1995)
22. Richter, S.: Kommunikation und Performanz in Command & Control Teams. Eine Analyse von World of Warcraft(TM)- und Battlefield 2(TM)-Teams. WiKu, Duisburg, Köln (2014)
23. Richter, S., Lechner, U.: Transactive Memory Systems and Shared Situation Awareness: A World of Warcraft Experiment. In: Proceedings of the International Conference on Organizational Learning, Knowledge and Capabilities (OLKC) (2009)
24. Hänsch, N., Benenson, Z.: Specifying IT Security Awareness. In: 25th International Workshop on Database and Expert Systems Applications (DEXA), pp. 326–330 (2014)
25. Krcmar, H.: Informationsmanagement. Springer Gabler, Berlin, Heidelberg (2015)
26. Suddaby, R.: Editor's Comment: Construct Clarity in Theories of Management and Organization. Academy of Management Review 201035, 346–357 (2010)
27. North, K.: Wissensorientierte Unternehmensführung. Wertschöpfung durch Wissen. Gabler, Wiesbaden (2011)
28. Mathieu, J., Maynard, M.T., Rapp, T., Gilson, L.: Team Effectiveness 1997-2007: A Review of Recent Advancements and a Glimpse Into the Future. Journal of Management 34, 410–476 (2008)
29. Wegner, D.M.: A Computer Network Model of Human Transactive Memory. Social Cognition 13, 319–339 (1995)
30. Wegner, D.M., Erber, R., Raymond, P.: Transactive memory in close relationships. Journal of Personality and Social Psychology 61, 923–929 (1991)
31. Klimoski, R., Mohammed, S.: Team Mental Model. Construct or Metaphor? Journal of Management 20, 403–437 (1994)
32. Siponen, M.T.: Five dimensions of information security awareness. Computers and Society 31, 24–29 (2001)
33. Mohammed, S., Klimoski, R., Rentsch, J.R.: The Measurement of Team Mental Models: We Have No Shared Schema. Organizational Research Methods 3, 123–165 (2000)