Nutzerverhalten als Teil der IT-Security – ein IS-Literaturüberblick

Christoph Buck[1], Tim Kessler[2], Torsten Eymann[1]

[1] Lehrstuhl Wirtschaftsinformatik, Universität Bayreuth, Germany
{christoph.buck,torsten.eymann}@uni-bayreuth.de
[2] Juniorprofessur Internationales Technologiemanagement, insb. industrielle Dienstleistungen, Universität Bayreuth, Germany
tim.kessler@uni-bayreuth.de

Abstract. Mit der zunehmenden Nutzung von privaten Endgeräten, der IT-Konsumerisierung und dem Verschwimmen von Arbeits- und Privatleben wird das Nutzerverhalten im Bereich der IT-Sicherheit immer wichtiger. Während Informationssysteme den Konsumenten-Massenmarkt durch portable Endgeräte und einfach zu bedienende Anwendungen erschließen, schwebt das hierdurch erreichte everyday life computing immer deutlicher wie ein Damoklesschwert über der Informationssicherheit von Organisationen und Unternehmen. Durch die steigende Zahl von beabsichtigten und unbeabsichtigten Angriffen auf die Datensicherheit durch Mitarbeiter wird der „Risikofaktor Mensch" eine wachsende Bedrohung. Aufgrund der zunehmenden Relevanz widmet sich auch die wissenschaftliche Forschung im Bereich der IT-Sicherheit den „Human Factors in IT-Security". Der vorliegende Literaturüberblick zeigt den Stand der Forschung in der Literatur der Wirtschaftsinformatik und des Information Systems Management auf und adressiert zukünftige Forschungsvorhaben.

Keywords: IT-Security, IT-Sicherheit, Nutzerverhalten, Human Factors

12th International Conference on Wirtschaftsinformatik,
March 4-6 2015, Osnabrück, Germany

Buck, C.; Kessler, T.; Eymann, T. (2015): Nutzerverhalten als Teil der IT-Security - ein IS-Literaturüberblick, in: Thomas. O.; Teuteberg, F. (Hrsg.): Proceedings der 12. Internationalen Tagung Wirtschaftsinformatik (WI 2015), Osnabrück, S. 1115-1130

1 Nutzerverhalten im Fokus der IT-Sicherheit

Digitale Informationssysteme werden zunehmend allgegenwärtig. Mit der Nutzung und vor allem Vernetzung von mobilen Endgeräten und deren Anwendungen, sowie der Anbindung von Sensoren in der Peripherie von Nutzern in Verbindung mit weitreichenden Cloud-Computing-Angeboten wird die Vision des »ubiquitous compting« von Weiser immer mehr zur Realität [1].

Während durch die Entwicklung im Informationszeitalter zunehmend der Konsumenten-Massenmarkt durch portable Endgeräte und einfach zu bedienende Anwendungen erschlossen werden kann, schwebt das durch zahlreiche Autoren beschriebene »experiential computing« immer deutlicher wie ein Damoklesschwert über der Informationssicherheit von Organisationen und Unternehmen [2-4]. Im Rahmen des »experiential computing« stehen die Konsumenten nahezu in dauerhafter Interaktion mit Informationssystemen [3]. Diese Interaktion gründet auf der zunehmenden Alltagsintegration von Rechnerelementen im Sinne des »ubiquitous computing«. Informationssysteme werden hierdurch allgegenwärtig und ihre Nutzung durch die Konsumenten im alltäglichen Leben zu einem hohen Grad selbstverständlich. Als Alltagsgegenstände oder -artefakte werden Objekte bezeichnet, die in einem vom Konsumenten als selbstverständlich erachteten Wirklichkeitsbereich eingebunden sind und zumeist erst dann bewusst wahrgenommen werden, wenn sie von ihrem gewohnten Dasein abweichen [5], [6]. Eine Abweichung vom gewohnten Dasein kann in Bezug auf die Informationssicherheit meist in den Folgen eines Angriffs gesehen werden.

In der alltäglichen und teilweise unbewussten Nutzung von (hochpersonalisierten) Informationssystemen muss eine massive Bedrohung von privater und organisationaler Informationssicherheit gesehen werden. Durch das mit dem everyday life computing einhergehende Verwischen der Grenzen von Arbeits- und Privatleben, bedrohen Sicherheitsangriffe auf private Endgeräte auch die IT-Sicherheit von Unternehmen [7-9].

Gründe hierfür können zum einen in den Unternehmen selbst und zum anderen im Nutzungsverhalten gesehen werden. Da Unternehmen den Arbeitnehmern oft keine oder kaum Vorgaben zur Vermeidung von Cyberkriminalität machen [10], muss (privaten) Nutzungsgewohnheiten von Anwendern im Rahmen der IT-Sicherheit zunehmende Beachtung geschenkt werden.

Aufgrund wachsender Wirtschaftsspionage und Cyberkriminalität rangiert IT-Sicherheit (70%) vor Netzwerk-Infrastruktur (64%) und Implementierung von Software (60%) auf Rang eins der Zukunftsinvestitionen von Unternehmen im Technologie-Bereich [11]. 74% der befragten Unternehmen betrachten „Angriffe auf ihre Computer und Datennetze durch Cyberkriminelle oder ausländische Geheimdienste als reale Gefahr“ [12] und signalisieren ein erhöhtes IT-Sicherheitsbewusstsein.

Da viele Sicherheitsvorfälle durch eigene oder externe Unternehmensmitarbeiter mit Zugang zu sensiblen Daten verursacht werden, sollte dem Risikopotential des Faktors Mensch eine zunehmende Beachtung im wissenschaftlichen Diskurs geschenkt werden [8], [13].

Der vorliegende Beitrag erfasst einen Status Quo der aktuellen wissenschaftlichen Wirtschaftsinformatik-relevanten (IS-relevanten) Literatur zum Thema „Human Fac-

tors in IT-Security“. Nachdem der Risikofaktor Mensch in die IT-Security thematisch eingeordnet wird, leistet der vorliegende Artikel mit einem Literaturüberblick einen Beitrag zum wissenschaftlichen Diskurs und zeigt aus der Perspektive der Wirtschaftsinformatik Lücken sowie zukünftige Forschungsfelder auf.

2 Faktor Mensch in der IT-Sicherheit

2.1 IT-Security

Der englische Begriff „security“ wird im Deutschen übersetzt als Informationssicherheit und stellt die Eigenschaft eines funktionierenden Systems dar, „nur solche Systemzustände anzunehmen, die zu keiner unautorisierten Informationsveränderung oder -gewinnung führen“ [14]. Beispiele solch einer Veränderung sind der Gebrauch, die Offenlegung, die Modifizierung oder die Zerstörung der Informationen, wobei sich die Informationssicherheit auf die Komponenten der Sicherheit der Personen, Aktivitäten, Daten, Technologien und Netzwerke richtet [15].
Der Terminus „security“ ist abzugrenzen von „safety“, das den Schutz vor unbeabsichtigten Ereignissen darstellt und sich auf die „Gewährleistung von Zuverlässigkeit (das IT-System liefert stabile Ergebnisse entsprechend den Vorgaben der Spezifikation), Fehlertoleranz (das IT-System fängt fehlerhafte Eingaben geeignet ab) und Korrektheit der IT-Systeme (das IT-System liefert überprüfbar richtige Ergebnisse)“ konzentriert [16]. Die Begriffe Datensicherheit (engl. protection) und Datenschutz (engl. privacy) werden häufig mit „security“ gleichgesetzt, beziehen sich jedoch vor allem auf den Zugriff von Daten, Maßnahmen zur Datensicherung und das Selbstbestimmungsrecht persönlicher Daten [14]. Ziele und Komponenten der Informationssicherheit sind die sogenannte CIA-Triade – Vertraulichkeit (confidentiality), Integrität (integrity) und Verfügbarkeit (availability). Informationen dürfen demnach nur durch befugte Nutzer verwendet, modifiziert und zugänglich gemacht werden [15].

2.2 Kategorien des Risikofaktors Mensch

Da rein technische Lösungen zur Sicherstellung der Informationssicherheit nicht ausreichen, richtet widmen sich unlängst Forschungsarbeiten dem Risikofaktor Mensch [17-22]. Die (organisationalen) Anwender als Risiko für die IT-Security werden in der IS-Literatur zunehmend diskutiert [8], [23], [24]. Hierbei werden Insider-Angriffe auf die Informationssicherheit durch Mitarbeiter gesehen, welche entweder privilegierte Zugangsrechte zu den Informationssystemen des Unternehmens haben oder über sensible Daten verfügen [8].
Bereits in den frühen 1990er Jahren haben Loch et al. eine Klassifizierung für Angriffe auf Informationssysteme entworfen, welche den Anwender als Sicherheitsbedrohung identifiziert [25]. Abbildung 1 veranschaulicht die Klassifizierung von Loch et al. die interne und externe Angriffe voneinander abgrenzt.

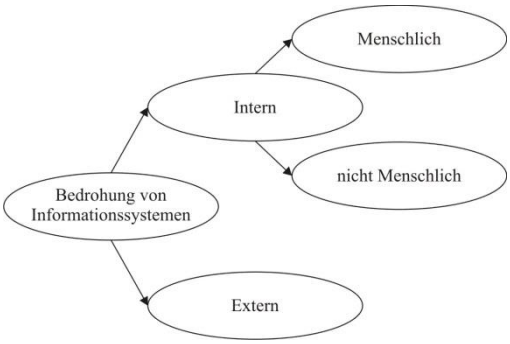

Abb. 1. Klassifikation von Bedrohungen der Informationssicherheit

Während externe menschliche Angriffe als vorsätzlich zuzuordnen sind (Hacker, Spionage) unterteilen Loch et al. die internen menschlichen Angriffe feingranularer. Bei internen Attacken – durch Mitarbeiter oder Insider – wird das Kontinuum von ungewollten, passiven und fahrlässigen bis hin zu gewollten, aktiven und vorsätzlichen Angriffen beschrieben [8]. Abbildung 2 veranschaulicht das Kontinuum interner menschlicher Angriffe.

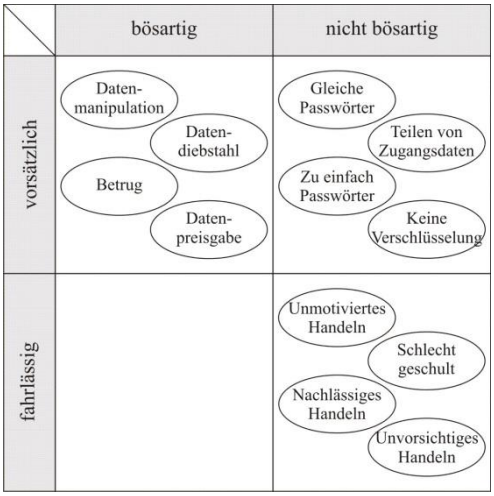

Abb. 2. Einordnung menschliche Bedrohungsarten

Eine ungewollte und passive Bedrohung wird durch nicht gewissenhafte, schlecht geschulte, nachlässige oder unmotivierte Mitarbeiter verursacht [24].
Gewollte aber nicht bösartige Bedrohungen der IT-Sicherheit entstehen meist durch die Umgehung oder Nichteinhaltung von Verhaltensregeln. Beispiele hierfür sind die Verwendung des identischen Passworts für mehrere Systeme, das Teilen von Zugangsdaten, die Nichtverschlüsselung von Daten oder das Unterlassen von Back-Ups [8].

Das andere Ende des Kontinuums wird beschrieben durch vorsätzliche Attacken auf die Informationssicherheit von Unternehmen. Vorsätzliche Angriffe auf die Informationssicherheit können durch das Manipulieren oder Entfernen von (sensiblen) Informationen, Datendiebstahl, Betrug oder Erpressung entstehen [8].

2.3 Nutzungsverhalten von Endkonsumenten als Risikofaktor

Wie die voranstehenden Kapitel zeigen, sind die individuellen Nutzer eines Informationssystems im Rahmen der IT-Security bereits Teil des wissenschaftlichen Diskurses. Überwiegend wird der menschliche Risikofaktor für die Informationssicherheit jedoch aus der organisationalen Perspektive betrachtet.
Im Informationszeitalter und einer zunehmenden Durchsetzung des Alltags von Endkonsumenten muss auch deren (private) Nutzungsgewohnheiten Aufmerksamkeit geschenkt werden. Im Rahmen der IT-Konsumerisierung verschwimmt die Grenze zwischen Berufs- und Privatleben zunehmend [7], [17], [26]. Durch „innovation first on consumer market“ wird die Nutzung von Informationssystemen im Rahmen der betrieblichen Tätigkeit maßgeblich von der privaten Nutzung und in letzter Konsequenz von privaten Nutzungsgewohnheiten beeinflusst [7], [27].
Durch die tiefgreifende Alltagsverankerung ändert sich der Umgang mit und die Nutzung von Informationssystemen von Privatanwendern und es steigen in der Konsequenz die Risiken für die organisationale Informationssicherheit. Durch bspw. Malware auf privaten Endgeräten wie Smartphones und Tablets, web- und netzwerkbasierten Attacken und vor allem Social-Engineering-Attacken geraten die privaten Anwender (unwissentlich) zunehmend in den Fokus von IT-Bedrohungen. In einer Studie von Buck et al. konnte bspw. bei Downloadentscheidungen von Smartphone-Apps aufgezeigt werden, dass lediglich ca. 19% der Anwender aktiv Privacy- und Security-relevante Entscheidungskriterien in ihre Downloadentscheidung von mobilen Applikationen mit einbeziehen [28].

3 Literaturüberblick: Vorgehen und Methode

Eine steigende Anzahl an Bücherveröffentlichungen und Journalartikeln, der zunehmende Umfang von Journalen sowie die zunehmende Komplexität in der wissenschaftlichen Forschung führen zu einer zunehmend unübersichtlichen Literaturlandschaft [29-31]. Im wissenschaftlichen Diskurs hat sich aufgrund der stark wachsenden Literatur schon früh die Forschungsdomäne des Literaturüberlicks (literature review) entwickelt, da die fundierte Literaturarbeit einen wesentlichen Schritt bei der Durchführung eines Forschungsvorhabens darstellt [29], [32], [33]. In der wissenschaftlichen Literatur ist die Methodik des Literaturüberblicks zentraler Bestandteil der wissenschaftlichen Forschung und im Speziellen in der Wirtschaftsinformatik als solcher anerkannt [29], [31], [34-36].
Ein Literaturüberblick versucht die relevante Literatur einer Forschungsdomäne zu identifizieren und die bisher gewonnenen Erkenntnisse zu kondensieren. Hierdurch werden zum einen redundante Forschungstätigkeiten vermieden und zum anderen

können weiterführende Forschungsvorhaben durch die effektive Zusammenführung der bestehenden Erkenntnisse an Stringenz gewinnen [33], [35].
Da der Begriff „Überblick“ (review) in Forschung und Wissenschaft mehrdeutig Verwendung findet, wird hinsichtlich der Struktur und Form des Literaturüberblicks dem strukturierten Ansatz von Webster und Watson gefolgt [34]. Das zentrale Element des strukturierten Literaturüberblicks stellt der Prozess der Suche und Identifikation relevanter Literatur dar [37]. Webster und Watson identifizieren den Kern eines wissenschaftlichen Literaturüberblicks in anerkannten wissenschaftlichen Literaturdatenbanken durch vorher festgelegte Suchbegriffe und die Vorwärts- und Rückwärtsrecherche von, für das adressierte Themengebiet, relevanten Publikationen [34]. Der von Webster und Watson proklamierte Ansatz basiert demnach auf zwei grundlegenden Prinzipien [34]. Einerseits sollen die Ergebnisse umfassend sein, d.h. die Suche soll einen möglichst großen Teil der relevanten Literatur abdecken und verschiedene Forschungsansätze, Journale und Regionen einschließen. Anderseits ist mit einem systematischen Ansatz die Replizierbarkeit sicherzustellen, damit der Wahrheitsgehalt des Reviews für Dritte nachweisbar und somit glaubwürdig ist. Des Weiteren ist die qualitative Eignung der Beiträge möglichst objektiv zu bewerten.
Prozessual wird eine weitreichende Literaturrecherche durch eine rückwärtsgerichtete und eine vorwärtsgerichtete Suche abgebildet [34], [35]. Bei der rückwärtsgerichteten Suche werden die durch die Datenbankrecherche (anhand vordefinierter Suchworte) gewonnenen Beiträge aufgearbeitet. Im Rahmen der vorwärtsgerichteten Recherche wird themenrelevante Literatur überprüft, welche in den durch die Datenbankrecherche gewonnenen Ergebnissen verwendet werden. Hierdurch können u.a. Anpassungen bei den verwendeten Suchbegriffen vorgenommen werden. Die rückwärtsgerichtete und die vorwärtsgerichtete Literaturrecherche können somit nicht unabhängig voneinander betrachtet werden sondern stellen eine dynamische Interaktion im Rahmen eines (ganzheitlichen) Literaturüberblicks dar [34], [36].
Vor dem Hintergrund der steigenden Anzahl wissenschaftlicher Publikationen und dem zunehmenden Schnittstellenbedeutung der Wirtschaftsinformatik mit angrenzenden Wissenschaftsdomänen ist die Transparenz der Suche von themenrelevanter Literatur, und gleichbedeutend der Ausschluss von (irrelevanter) Literatur, in höchstem Maße transparent zu gestalten, um eine möglichst hohe Reliabilität und Validität der Ergebnisse sicherstellen zu können [36].
Der vorliegende Literaturüberblick konzentriert sich auf WI- bzw. IS-relevante Literatur. Es wird ausschließlich Literatur verwendet, die in dem adressierten Wissenschaftsbereich hohe Qualität und Reputation aufweist. Die Untersuchungsgruppe umfasst die führenden internationalen Zeitschriften im Bereich der Informationssysteme – den „Basket of 8“. Zusätzlich wurden die Zeitschriften Business and Information Systems Engineering (BISE) und Electronic Markets (EM) sowie die Proceedings der European Conference on Information Systems (ECIS) und die Proceedings der International Conference on Information Systems (ICIS) aufgenommen.
Aufgrund unterschiedlicher Gründungsjahre der jeweiligen Zeitschriften und Konferenzen, erstreckt sich der gesamte Umfang der Suche auf den Zeitraum von 1977 bis 2014. Im Rahmen der Untersuchung wurde eine „all field“-Datenbankabfrage mit

dem Suchbegriff „Human Factors in IT-Security“ in den genannten Untersuchungsobjekten durchgeführt.
Ziel der Literaturrecherche ist es, die Forschungsarbeiten zu finden, welche menschliche Risikofaktoren als Teil der IT-Security sehen. Dementsprechend zentral bei der „all-field“-Datenbankabfrage ist der Begriff IT-Security, durch welchen der Untersuchungsrahmen festgelegt wurde. Mit Human Factors wurde ein breiter Such-begriff verwendet, um ein möglichst umfassendes Suchergebnis erzeugen zu können.
Ausgehend von allen Treffern der „all field“-Datenbankabfrage wurden die Ergebnisse nach Relevanz gefiltert. Die Auswahl der Beiträge, die eine hohe Themenrelevanz aufwiesen, wurden in der Ergebnisdarstellung detailliert analysiert.
Die Datenbankabfrage nach der „all field“-Sucheingabe „Human Factors in IT-Security“ in den genannten Zeitschriften und Konferenzen führt zu einer kumulierten Trefferanzahl von 1292 Artikeln. Tabelle 1 fasst die Ergebnisse der Datenbankabfrage aus dem Zeitraum 07.03.2014 - 23.03.2014 zusammen. Mit 191 Treffern mussten 14,78% der gefundenen Artikel aus der Analyse ausgeschlossen werden, da sie im Hinblick auf die dargestellten Kernthemen als nicht relevant eingestuft wurden (bspw. Autoreninformationen oder Kommentarbeiträge). Anhand einer Inhaltsanalyse von Titel und Zusammenfassung wurden die verbleibenden 1101 Artikel nach Themenrelevanz überprüft. Zum einen richtet sich die Überprüfung auf die expliziten Schlagwörter „Human Factors“ und „IT-Security“, zum anderen wird beachtet, ob Synonyme verwendet werden. Im Bereich der „Human Factors“ sind dies z.B. „Human Behavior“, „Attitude“ und „Interaction“. In Bezug auf „IT-Security“ sind dies z.B. „IS-Security“ oder „Cyberattack“.
Als Ergebnis der auf Titel und Zusammenfassung gestützten Inhaltsanalyse konnten mit 24 Beiträgen nur knapp zwei Prozent aus der Datenbankabfrage gewonnenen Artikel als themenrelevant für das Thema „Human Factors in IT-Security“ identifiziert werden.

Tab. 1. Ergebnis der Datenbankabfrage

Zeitschriften/Konferenzen	Datenbank	Überblick über Ausgabe/Jahr	Anzahl Treffer	Anzahl n.a.	Neue Anzahl Treffer	relevante Artikel
European Journal of Information Systems (EJIS)	Palgrave Macmillan Journals	1/1991 - 23/2013	45	9	36	0
Information Systems Journal (ISJ)	Wiley Online Library	1/1991 - 24/2014	4	0	4	1
Information Systems Research (ISR)	Informs Pubs.OnLine	1/1990 - 25/2014	96	9	87	0
Journal of the Association for Information Systems (JAIS)	Association for Information Systems (AIS)	1/2000 - 15/2014	63	2	61	2
Journal of Information Technology (JIT)	Palgrave Macmillan Journals	1/1986 - 29/2014	20	7	13	0
Journal of Management Information Systems (JMIS)	Metapress	17/2000 - 30/2013	3	0	3	0
Journal of Strategic Information Systems (JSIS)	ScienceDirect	1/1991 - 23/2014	147	14	133	1
Management Information Systems Quarterly (MIS Quarterly)	AIS	1/1977 - 37/2013	87	17	70	4
Business & Information Systems Engineering (BISE)	AIS	1999-2013	12	2	10	0
Electronic Markets (EM)	Taylor & Francis Online	1/1991 - 18/2008	47	12	35	0
International Conference on Information Systems (ICIS)	AIS	1994-2013	381	30	351	14
European Conference on Information Systems (ECIS)	AIS	2000-2013	387	89	298	2
Gesamtergebnis			**1292**	**191**	**1101**	**24**

4 Ergebnisse des Literaturüberblicks

Das Ergebnis einer umfassenden Datenbankabfrage zeigt, dass 24 Veröffentlichungen aus relevanten Zeitschriften und Konferenzbeiträgen der Wirtschaftsinformatik Relevanz zum Thema „Human Factors in IT-Security“ aufweisen. Diese erstrecken sich im Zeitraum von 2005 bis 2014 und wurden vorwiegend in den Proceeding der ICIS und der ECIS veröffentlicht (16 der 24 Artikel). Der Anstieg der Publikationen in den vergangenen Jahren und insbesondere die steigenden Journalveröffentlichungen im aktuellen Jahrzehnt spiegeln eine wachsende Relevanz des Themas im Rahmen der IT-Security wieder.

Zur näheren Analyse der 24 relevanten Artikel wurden sie anhand der von Cooper empfohlenen Charakterisierung von Literaturbeiträgen in die Kategorien Typ, Fokus, Ziel (Formulierung und Inhalt) sowie Zielgruppe eingeordnet [29]. Die in Tabelle 2 dargelegte Kategorisierung der Artikel nach Cooper zeigt, dass der Bereich „Human Factors in IT-Security“, durch die mehrheitlich mathematisch-statistischen Studien (Typ), einen aktiven Forschungszweig mit ersten Forschungsrichtungen aufweist [31]. Obwohl die bisherige Forschung bspw. mit dem Elaboration Likelihood Model [38], [39], dem Technology Acceptance Model [40], [41] oder der Theory of Planned Behavior [38], [42-44] auf bereits bestätigten theoretischen Fundamenten basiert (Fokus), sind die vorhandenen Erkenntnisse zur Erklärung der Realität noch nicht zufriedenstellend. Im Hinblick auf die Zielsetzung (Ziel) zeigt sich im Rahmen der explizierten Forschung ein heterogenes Bild. Während nur ein Artikel mit Kritik explizit zu neuen Forschungsansätzen aufruft, konzentrieren sich die übrigen Beiträge vorwiegend auf zentrale Aspekte der Themenstellung. Das heterogene Bild zeigt, dass die wissenschaftliche Community eine Forschungslücke identifiziert hat und unterschiedlichste Aspekte untersucht werden, welche sich jedoch in unterschiedliche Richtungen und mit diversen Zielsetzungen entwickeln. Obwohl in der bisherigen Forschung vorwiegend Wissenschaftler angesprochen werden (Zielgruppe), richten sich bereits zahlreiche Autoren in ihren Beiträgen mit Implikationen an die Praxis. Auf der einen Seite zeigt diese Zielgruppenansprache, dass weitere Forschungsfragen auftreten und theoretische Modelle überprüft werden müssen. Auf der anderen Seite verdeutlichen die Implikationen für Manager und IT-Sicherheitsbeauftragte die Relevanz und Aktualität der Thematik in der Wirtschaft auf.

Tab. 2. Kategorisierung der relevanten Literatur nach Cooper [29]

Charakteristik	**Kategorie**			
Typ	Natürlich-sprachlich (7; 29%)		Mathematisch-statistisch **(17; 71%)**	
Fokus	Forschungs-ergebnis **(17; 71%)**	Forschungs-methode (0; 0%)	Theorie (11; 46%)	Erfahrung (0; 0%)

Ziel	Formulierung	Nicht expliziert (0, 0%)		Expliziert **(24; 100%)**	
	Inhalt	Integration (4; 17%)	Kritik (1; 4%)	Zentrale Themen **(19; 79%)**	
Zielgruppe		Allgemeine Öffentlichkeit (0; 0%)	Praktiker (19, 79%)	Forscher im Allgemeinen **(23; 96%)**	Spezialisierte Forscher (0, 0%)

Nach der Kategorisierung von Cooper werden im Folgenden die zu Grunde liegenden Thematiken und Schlüsselkonzepte in den als relevant eingestuften Artikeln vorgestellt [29].

Grundsätzlich zeigt sich in der Auswertung der relevanten Artikel ein stark organisationaler Bezug der untersuchten Literatur. Bei genauerer Betrachtung der Fragestellungen der 24 relevanten Artikel wird erkennbar, dass sich die Forscher überwiegend mit vier Themen auseinandersetzen: dem allgemeinen Verhalten, aktivierenden Einstellungsprozessen, kognitiven Wahrnehmungsprozessen und dem expliziten Entscheidungsverhalten (Handeln) [45]. Ein weiterer Aspekt ist die Untersuchung von Ursachen und Gründen von Gefahren sowie die Rolle der Sicherheitspolitik, die in einem Bericht von Yayla erfolgt [46]. Die zusammengefassten Gruppierungen werden im weiteren Verlauf näher vorgestellt, wobei auch auf die Einflussfaktoren, die diese Zusammenhänge begünstigen, detailliert eingegangen wird.

Verhalten. Unter dem Begriff „Verhalten“ wird in der Literatur die Nutzung von Sicherheitstechnologien, die Intention sicheres Verhalten anzunehmen, die Einhaltung von Sicherheitsrichtlinien und das Gefahrvermeidungsverhalten, verstanden. Die Forscher konzentrieren sich auf die Einflussfaktoren, die zur Adaption von Sicherheitsprogrammen wie bspw. E-Mail-Authentifizierungsprogrammen [41] oder Sicherheitstechnologien bei Spyware [40] führen. Herath et al. bestätigen einen positiven Zusammenhang der Risikowahrnehmung und der Einstellung zum Sicherheitsservice auf die Nutzung von Sicherheitstechnologien. Als weitere Faktoren werden das Bewusstsein von Gefahren [40], die subjektive und die deskriptive Norm [47] identifiziert, welche ebenfalls einen positiven Zusammenhang auf die Nutzung von Sicherheitstechnologien aufweisen. In Bezug auf das Verhalten der Mitarbeiter wird auch die Absicht, ein sicherheitskonformes Verhalten anzunehmen, untersucht.

Burns et al. entwickeln ein dreistufiges Modell, das die Einflussfaktoren auf ein sicherheitskonformes Verhalten erklären soll [48]. Dabei wird das Bestreben, solch ein Verhalten einzunehmen, durch die Faktoren der Selbstwirksamkeit, der Erwartung hinsichtlich des Ergebnisses, der Risikowahrnehmung und der auf individuellen sowie auf Erfahrung basierenden Faktoren begünstigt. In einem weiteren Modell vermuten Jenkins et al., dass einerseits die Einstellung zur Sicherheit einen positiven und andererseits die kognitive Überladung einen negativen Effekt auf das Verhalten aufweisen. Jedoch sind nicht alle genannten Faktoren bisher empirisch belegt. Bereits bestätigte Erkenntnisse über Einflussfaktoren liefern Jenkins et al. sowie Wynn et al. [43], [44]. So wirken Empfänglichkeit, Vermeidbarkeit, Antwortwirksamkeit, subjektive Nor-

men und Vergleichbarkeit [44], [49] positiv auf die Verhaltensintention und Faktoren wie die Einstellung, die wahrgenommene Verhaltenskontrolle und Just-in-time Erinnerungen [50] bewirken ebenfalls eine positive Verhaltensweise.

Die Einstellung zur Einhaltung der Sicherheitspolitik zeigt neben der normativen Ansicht und der Selbstwirksamkeit [42] einen positiven Einfluss auf das Compliance-Verhalten, genauso wie deskriptive und gerichtliche Normen, die durch Bewusstseinstrainings gestärkt werden können [51]. In einem Experiment finden Jenkins et al. heraus, dass Schulungen zum sicherheitskonformen Verhalten einen größeren Einfluss auf das tatsächliche Verhalten haben, wobei die Einhaltung der Richtlinien in deutlich geringerem Ausmaß von Vorgaben zur Nutzername- und Passwort-Authentifizierung beeinflusst wird.

Während die meisten Forscher vornehmlich auf Individualfaktoren eingehen, stellen Yoo und Sanders eine Theorie der Einflussfaktoren auf Gruppenebene auf [52]. Sie stellen die Vermutung auf, dass die zentrale Ausrichtung der Sicherheitswirksamkeit, der Sanktionen und der Belohnungen positive Beziehungen zu der Einhaltung der Sicherheitspolitik aufzeigen. Für den Beleg dieser Annahmen ist eine empirische Überprüfung unabdingbar. Liang und Xue untersuchen das Verhalten, Gefahren zu vermeiden [7]. Die Wahrnehmung der Gefahr, die Kosten und Effektivität des Schutzes sowie die Eigenwirksamkeit zeigen eine positive Beziehung zur Motivation, eine Gefahr zu umgehen, auf, was wiederum zu tatsächlichem Verhalten führen kann.

Einstellung. Die Haltung zur Informationssicherheit wird als weiterer Aspekt der menschlichen Faktoren in der Informationssicherheit betrachtet. Eine positive Beziehung dazu ist abhängig von Argumenten und dem Erkennen von Sicherheitshinweisen [43]. In detaillierterer Betrachtung ist dieser positive Zusammenhang abhängig von der Qualität und Quantität der Argumente, die für die Informationssicherheit genannt werden, sowie der Ausprägung der Variablen des Elaboration Likelihood Models, zu dem Motivation, Fähigkeit und Gelegenheit zur Argumentaufnahme gehören [39]. Uffen et al. zeigen empirische Belege für die Persönlichkeitsmerkmale Gewissenhaftigkeit, Offenheit, Extrovertiertheit, Verträglichkeit und emotionale Stabilität sowie mögliche Auswirkungen auf unterschiedliche Dimensionen des Informationssicherheitsmanagements auf [61]. Bei der Betrachtung der Intentionen für sicherheitskonformes Verhalten stellen Anderson und Agarwal positive Zusammenhänge von den Faktoren der Bedenken zu Sicherheitsgefahren, der wahrgenommenen Wirksamkeit und der Eigenwirksamkeit von Sicherheitsverhalten auf die Einstellung zu Sicherheitsverhalten fest [18]. Dinev und Hu sowie Bulgurcu et al. belegen zudem, dass das Bewusstsein und der gefühlte Nutzen der Einhaltung der Richtlinien sowie die möglichen Kosten der Nicht-Einhaltung in positiver Beziehung zur Einstellung der Menschen zur IT-Sicherheit stehen [40], [42].

Wahrnehmung. Anhand einer Case Study identifiziert Taylor Faktoren der Risikowahrnehmung von Managern in Unternehmen [53]. Die Hypothesen, dass Manager das Sicherheitslevel in ihrem Unternehmen als hoch ansehen und davon ausgehen, dass die Mitarbeiter sich an die Sicherheitsrichtlinien halten, werden bestätigt. Jedoch nehmen sie nicht wahr, dass ein Sicherheitsrisiko von unabsichtlichen Handlungen der Mitarbeiter ausgeht. Ähnlich stellt Vaast fest, dass sich die Sicherheitswahrnehmung unterscheidet [54]. So fokussieren sich IT-Fachleute auf die technischen Si-

cherheitsaspekte, während Mitarbeiter sich auf die Sicherheit von vertraulichen Daten konzentrieren. Zusätzlich kommt es bei der Wahrnehmung häufig zu Verzerrungen. So stellen Rhee et al. fest, dass Menschen oftmals der Meinung sind, nicht von Gefahren betroffen zu sein. Eine weitere Verzerrung, die auftreten kann ist, dass Menschen sich selbst falsch einschätzen und daraus resultierend im Glauben sind Gefahren selbst erkennen zu können [55].

Handeln. Einige der relevanten Artikel konzentrieren sich auf aktive Handlungen der Mitarbeiter im Kontext der IT-Sicherheit. Goode und Lacey ermitteln Faktoren, die Einfluss auf die Weitergabe von vertraulichen Informationen haben [56]. Zu diesen gehören Vertrauen, Risiko- und Unsicherheitsfaktoren sowie Faktoren des Wissensmanagements und der Beziehungen untereinander. Diese Einflüsse wurden bis-lang jedoch nicht empirisch belegt. In einem weiteren Modell wird untersucht wie die Einhaltung der Internetnutzungsbestimmungen positiv beeinflusst werden kann um Missbrauch entgegenzuwirken [57]. Hierbei werden die Wahrnehmung von Sanktionen, persönliche Moralvorstellungen sowie verfahrensorientierte und distributive Gerechtigkeit angeführt. Willison und Warkentin fordern die Wissenschaftler der IT-Sicherheit auf, weitere Fragestellungen des absichtlichen Computermissbrauchs zu beantworten [8]. In ihrem Forschungskommentar erläutern sie, dass nicht nur die Gründe für Missbrauch näher erforscht werden müssen, sondern, in Bezug dazu auch, den Fragen nach der Rolle von Emotionen, Persönlichkeitsmerkmalen und dem Ungerechtigkeitsempfinden der Arbeitnehmer nachgegangen werden muss.

5 Limitation und Ausblick

Vier übergeordnete (und nicht trennscharf voneinander abgrenzbare) Themengebiete konnten im Rahmen des Literaturüberblicks in der IS-relevanten Literatur identifiziert werden: Verhalten, Einstellung, Wahrnehmung und Handeln. Der Literatur-überblick zeigt, trotz seiner Limitationen, Forschungslücken der IS-Community im Bereich der menschlichen Risikofaktoren hinsichtlich der Informationssicherheit auf. Um das Thema „Human Factors in IT-Security“ von einem klar definierten Ausgangspunkt betrachten und vor allem eine hohe Transparenz gewährleisten zu können, beschränkt sich der dargestellte Literaturüberblick auf IS-relevante Literatur. Hinsichtlich der Publikations-Outlets haben sich die Autoren bewusst auf qualitativ hochwertige Publikationsorgane konzentriert, wodurch eine ganzheitliche Betrachtung nicht sichergestellt werden kann. Des Weiteren beschränkt sich der Literatur-überblick auf eine reine einperiodige Rückwärtssuche.

Wie der Literaturüberblick verdeutlicht, findet die übergeordnete Fragestellung des Risikofaktors Mensch Beachtung im wissenschaftlichen Diskurs, doch ist diese überwiegend einer organisationalen Perspektive zuzuordnen. Eine tiefergreifende Betrachtung der privaten individuellen Nutzung von Informationssystemen findet nur untergeordnet statt. Zwar stellen bspw. Liang und Xue mit der Technology Threat Avoidance Theory (TTAT) einen wertvollen Beitrag zu Verfügung [7], doch wird auch hier die tiefgreifende Alltagsintegration von Informationssystemen von Konsumenten nicht ausreichend betrachtet.

Durch die Allgegenwärtigkeit und die teilweise Unsichtbarkeit von Informationssystemen sollte die kontextuale Betrachtung der privaten Nutzung Aufmerksamkeit im wissenschaftlichen Diskurs zur Informationssicherheit finden. Stoßrichtungen für zukünftige Forschungsarbeiten können bspw. die Wahrnehmung von Informationssystemen, die Beziehung zu personalisierten Endgeräten, die Einstellung zum Umgang mit sensiblen Daten und die Sensibilisierung für Sicherheitsbedrohungen im privaten Kontext sein [58], [59].
Der vorliegende Literaturüberblick stellt einen ersten Einblick in das Themenfeld „Human Factors in IT-Security“ dar und kann Ausgangspunkt für weitere Forschungsvorhaben sein. Eine tiefergreifendere Analyse kann durch eine detaillierte Vorwärts- und Rückwärtssuche und feiner granulare Suchbegriffe aus dem adressierten Themenfeld erreicht werden. Ebenfalls sollten zukünftige Literaturrecherchen auf verwandte Themenbereiche wie bspw. die Informatik, das Konsumentenverhalten, Behavioral Economics, das Entscheidungsverhalten und Bereiche der Psychologie ausgeweitet werden.

Literatur

1. Weiser, M.: The Computer for the 21st Century. Scientific American 265(3), S. 94–104 (1991)
2. Jain, R.: Experiential computing. Communications of the ACM - a game experience in every application 46(7), S. 48–55 (2003)
3. Yoo, Y.: Computing in Everyday Life: A Call for Research on Experiential Computing. Management Information Systems Quarterly 34(2), S. 213–231 (2010)
4. Bødker, M., Gimpel, G., Hedman, J.: Time out/time in: the dynamics of everyday experiential computing devices. Information Systems Journal 24(2), S. 143–166 (2014)
5. Heidegger, M.: Sein und Zeit (11). Max Niemeyer, Tübingen (1967)
6. Schütz, A., Luckmann, T.: Strukturen der Lebenswelt (1). Suhrkamp, Frankfurt (1979)
7. Liang, H., Xue, Y.: Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. Journal of the Association for Information Systems 11(7), S. 394–186 (2010)
8. Willison, R., Warkentin, M.: Beyond Deterrence: An Expanded View of Employee Computer Abuse. Management Information Systems Quarterly 37(1), S. 1–20 (2013)
9. BSI: Die Lage der IT-Sicherheit in Deutschland (2007)
10. BITKOM, http://www.bitkom.org/de/presse/74532_73721.aspx (Zugriff am 08.12.2014)
11. BITKOM, http://www.bitkom.org/de/presse/78284_78077.aspx (Zugriff am 08.12.2014)
12. BITKOM, http://www.bitkom.org/de/presse/8477_78903.aspx (Zugriff am 08.12.2014)
13. Kerkmann, C., http://www.handelsblatt.com/unternehmen/it-medien/it-sicherheit-schwachstelle-mensch/8996598.html, 2013-10-29 (Zugriff am 07.12.2014)
14. Eckert, C.: IT-Sicherheit Konzepte - Verfahren - Protokolle. Oldenbourg, München (2009)
15. Raggad, B.G.: Information security management: concepts and practice. CRC Press/Taylor & Francis Boca Raton (2010)
16. Witt, B.C.: IT-Sicherheit kompakt und verständlich: Eine praxisorientierte Einführung. Vieweg, Wiesbaden (2006)
17. Buck, C., Eymann, T.: Risikofaktor Mensch in mobilen Ökosystemen. HMD Praxis der Wirtschaftsinformatik 51(1), S. 75–83 (2014)

18. Anderson, C.L., Agarwal, R.: Practical Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. Management Information Systems Quarterly 34(3), S. 613–643 (2010)
19. Aytes, K, Terry, C.: Computer Security and Risky Computing Practices: A Rational Choice Perspective. Journal of Organizational and End User Computing 16(3), S. 22–40 (2004)
20. Ng, B.-Y., Kankanhalli, A, Xu, Y. C.: Studying Users' Computer Security Behavior: A Health Belief Perspective. Decision Support Systems 46(4), S. 815–825 (2009)
21. Woon, I., G. W. Tan, and R. Low: A Protection Motivation Theory Approach to Home Wireless Security. ICIS 2005 Proceedings S. 367–380 (2005)
22. Workman, M., Bommer W. H., Straub D.: Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test. Computers in Human Behavior 24(6), S. 2799–2816 (2008)
23. Hu Q, Xu Z, Dinev T, Ling H.: Does Deterrence Really Work in Reducing Information Security Policy Violations by Employees? Communications of the ACM 54(6), S. 54–60 (2011)
24. Stanton, J. M., Stam, K. R., Mastrangelo, P., Jolton, J.: Analysis of End User Security Behaviors. Computers & Security 24(2), S. 124–133 (2005)
25. Loch, K., Carr, H., Warkentin, M.: Threats to Information Systems: Today's Reality, Yesterday's Understanding. Management Information Systems Quarterly 16(2), S. 173–186 (1992)
26. Weiß, F., Leimeister, J. M.: Consumerization. Wirtschaftsinformatik 54(6), S. 1–4 (2012)
27. Terryn, W.C.: Consumerization. Information technology, Neologism, Consumer electronics Fer, Mauritius (2011)
28. Buck, C., Horbel, C., Germelmann, C.C., Eymann, T.: The Unconscious App Consumer: Discovering and Comparing the Information Seeking Patterns among Mobile Application Consumers. ECIS 2014 Proceedings (2014)
29. Cooper, H.: Literature Searching Strategies of Integrative Research Reviews. Knowledge: Creation, Diffusion, Utilization 8(2), S. 372–383 (1986)
30. Peffers, K. and Ya, T. (2003). Identifying and Evaluating the Universe of Outlets for Information Systems Research: Ranking the Journals. Journal of Information Technology Theory and Application 5(1), S. 63–84.
31. Fettke, P.: State-of-the-Art des State-of-the-Art: Eine Untersuchung der Forschungsmethode "Review" innerhalb der Wirtschaftsinformatik. Wirtschaftsinformatik 48(4), S. 257–266 (2006)
32. Garvey, W., Griffith, B.: Scientific Communication: Its Role in the Conduct of Research and Creation of Knowledge. American Psychologist 26(2), S. 349–361 (1971)
33. Baker, M.J.: Writing a Literature Review. The Marketing Review 1(2), S. 219–247 (2000)
34. Webster, J., Watson, R.T.: Analyizing the Past to Prepare for the Future: Writing a Literature Review. Management Information Systems Quarterly 26(2), S. 12–23 (2002)
35. Levy, Y., Ellis, T.J.:A Systems Approach to Conduct an Effective Literature Review. Support of Information Systems Research. Informing Science 9, S. 181–212 (2006)
36. Vom Brocke, J., Simons, A., Niehaves, B., Niehaves, B., Reimer, K., Plattfaut, R., Cleven, A.: Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process. ECIS 2009 Proceedings (2009).
37. Zorn, T., Campbell, N.: Improving the Writing of Literature Reviews Through a Literature Integration Exercise. Business Communication Quarterly, 69(2), S. 172–183 (2006)

38. Jenkins, J.L., Durcikova, A., Ross, G., Nunamaker, J.F.J.: Encouraging Users to Behave Securely: Examining the Influence of Technical, Managerial, and Educational Controls on Users' Secure Behavior. ICIS 2010 Proceedings (2010)
39. Ng, B.Y., Kankanhalli, A.: Processing Information Security Messages: An Elaboration Likelihood Perspective. ECIS 2008 Proceedings (2008)
40. Dinev, T., Hu, Q.: The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. Journal of the Association for Information Systems 8(7), S. 386–408 (2007)
41. Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., Rao, R.: Security Services as Coping Mechanisms: An Investigation into User Intention to Adopt an Email Authentication Service. Information Systems Journal 24, S. 61–84 (2014)
42. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information Security Policy Compliance: An Empircal Study of Rationality-Based Beliefs and Information Security Awareness. Management Information Systems Quarterly 34(3), S. 523–548 (2010)
43. Jenkins, J.L., Durcikova, A., Burns, M.B.: Get a Cue on IS Security Training: Explaining the Difference Between How Security Cues and Security Agruments Improve Secure Behavior. ICIS 2011 Proceedings (2011)
44. Wynn, D.J., Williams, C.K., Karahanna, E., Madupalli, R.: Preventive Adoption of Information Security Behaviors. ICIS 2012 Proceedings (2012)
45. Kroeber-Riel, W., Gröppel-Klein, A.: Konsumentenverhalten. 10. Auflage, Vahlen (2013)
46. Yayla, A.: Controlling Insider Threats With Information Security Policies. ECIS 2011 Proceedings (2011)
47. Harrington, S., Anderson, C., Agarwal, R.: Practicing Safe Computing: Message Framing, Self-View, and Home Computer User Security Behavior Intentions. ICIS 2006 Proceedings (2006)
48. Burns, M.B., Durcikova, A., Jenkins, J.L.: On Not Falling For Phish: Examing Multiple Stages of Protective Behavior of Information Systems End-Users. ICIS 2012 Proceedings (2012)
49. Johnston, A.C., Warkentin, M.: Fear Appeals and Information Security Behaviors: An Empirical Study. Management Information Systems Quarterly 34(3), S. 549–566 (2010)
50. Jenkins, J.L., Durcikova, A.: What, I Shouldn't Have Done That?: The Influence of Training and Just-In-Time Reminders on Secure Behavior. ICIS 2013 Proceedings (2013)
51. Merhi, M.I., Midha, V.: The Impact of Training and Social Norms on Information Security Compliance: A Pilot Study. ICIS 2012 Proceedings (2012)
52. Yoo, C.W., Sanders, G.L.: An Exploration of Group Information Security Compliance: A Social Network Analysis Perspective. ICIS 2013 Proceedings (2013)
53. Taylor, R.: Management Perception of Unintentional Information Security Risks. ICIS 2006 Proceedings (2006)
54. Vaast, E.: Danger is In The Eye of The Beholders: Social Representations of Information Systems Security in Healthcare. Strategic Information Systems 16, S. 130–152 (2007)
55. Moody, G., Galletta, D., Walker, J., Dunn, B.: Which Phish Get Caught? An Exploratory Study of Individual Susceptibility to Phishing. ICIS 2011 Proceedings (2011)
56. Goode, S., Lacey, D.: Exploring Interpersonal Relationships in Security Information Sharing. ICIS 2011 Proceedings (2011)
57. Li, H., Sarathy, R., Zhang, J.: Understanding Compliance with Internet Use Policy: An Integrative Model Based on Command-and- Control and Self-Regulatory Approaches. ICIS 2010 Proceedings (2010)
58. Schneier, B.: Psychology of Security. https://www.schneier.com/essays/archives /2008/01/the_psychology_of_se.html (Zugriff am 08.12.2014)

59. Bosworth, S., Kabay, M.E.: Toward a New Framework for Information Security. The Computer Security Handbook 4, New York, (2002)
60. Kraemer, S., Carayon, P., Clem, J.: Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities. Computer & Security 28(2), S. 509–520 (2009)
61. Uffen, J., Guhr, N., Breitner, M. H.: Personality Traits and Information Security Management: An Empirical Study of Information Security Executives. ICIS 2012 Proceedings (2012)
62. Vacca, J.R.: Computer and Information Security Handbook (2009)