Hochschule Düsseldorf
University of Applied Sciences

Fachbereich Medien
Faculty of Media

Berichte zu HSD-intern geförderten Forschungsprojekten
Nr. 1

ISSN 2625-3690

DOI 10.20385/2625-3690/2018.1
URN urn:nbn:de:hbz:due62-opus-11880

Studie zur Information Security Awareness in kleinen und mittleren Unternehmen (KMU)

Holger Schmidt, Jeremy Gondolf und

Peter Haufs-Brusberg

Hochschule Düsseldorf

Fachbereich Medien

Professur für Informatik, insb. IT-Sicherheit

Studie zur Information Security Awareness in kleinen und mittleren Unternehmen (KMU)

Autor:
Holger Schmidt

Weitere Autoren:
Jeremy Gondolf
Peter Haufs-Brusberg

10. Juli 2018

Der Bereich der *Informationssicherheit* stellt große und insbesondere *kleine und mittlere Unternehmen (KMU)* vor erhebliche Herausforderungen. Zunehmende Angriffe auf IT-Systeme und Infrastrukturen haben die Informationssicherheit zum kritischen Erfolgsfaktor gemacht. Neben klassischen Zielen und Bereichen der Informationssicherheit hat vor allem die *Security Awareness* - das Sicherheitsbewusstsein aller Mitarbeiter eines Unternehmens - an Bedeutung gewonnen. Security Awareness bezieht sich auf jegliches Wissen und Handeln der Mitarbeiter eines Unternehmens und ist daher ein bedeutsamer Baustein zur *ganzheitlichen Gewährleistung* von Informationssicherheit. Die Motivation zur Entwicklung und Einführung von Informationssicherheit und insbesondere Security Awareness geht in großen Unternehmen vor allem von externen Faktoren, so z. B. der Regulierung von Branchen, aus und ist mittels globaler Standards, Normen und Frameworks implementiert. KMU sind grundsätzlich keinen geringeren Risiken als große Unternehmen ausgesetzt, verfügen jedoch nur selten über vergleichbare Schutzmaßnahmen hinsichtlich Informationssicherheit. Im Rahmen des Projekts wurden externe Anforderungen für große Unternehmen analysiert und hinsichtlich der Eignung als Grundlage für KMU bewertet. Das Projekt thematisiert weiterhin die Messbarkeit von Security Awareness sowie die in großen Unternehmen eingesetzten Maßnahmen zur Gewährleistung von Security Awareness besonders hinsichtlich ihrer Eignung für KMU.

Der vorliegende Projektbericht enthält in Abschnitt 1 eine detaillierte Projektbeschreibung und die Projektziele, in Abschnitt 2 eine Beschreibung der erreichten Ergebnisse und abschließend mit Abschnitt 3 einen Ausblick.

1. Ausgangssituation

Das Projekt „Studie zur Information Security Awareness in kleinen und mittleren Unternehmen (KMU)“ wurde von Prof. Dr.-Ing. Holger Schmidt im Rahmen der Hochschulinternen Forschungsförderung der Hochschule Düsseldorf durchgeführt. Wesentliche Ziele des Projektes waren die Initiierung von Forschung im Bereich von Information Security Awareness und die Entwicklung eines entsprechenden Promotionsthemas für einen Doktoranden. Im Folgenden wird das Projekt in Abschnitt 1.1 beschrieben und die Projektziele in Abschnitt 1.2 erläutert.

1.1. Projektbeschreibung

Angriffe auf IT-Systeme stellen nicht nur für große Unternehmen und Organisationen eine Herausforderung dar. Neben technischen Maßnahmen im Bereich der Informationssicherheit – die vor allem dem Schutze vor direkten Angriffen auf IT-Systeme dienen – ist eine Vielzahl weiterer Instrumente der Informationssicherheit zum kritischen Erfolgsfaktor insbesondere für KMU geworden.

Klassische Schutzziele der Informationssicherheit umfassen die Gewährleistung von Vertraulichkeit, Verfügbarkeit und Integrität. Dadurch kann ein ausreichender Schutz vor Angriffen und damit verbundenen etwaigen wirtschaftlichen Schäden erreicht werden.

Eine entscheidende Rolle zur Sicherstellung der Informationssicherheit nimmt die Security Awareness – das Sicherheitsbewusstsein von Mitarbeitern und der Geschäftsführung hinsichtlich der Informationssicherheit – ein. Die permanente Gewährleistung von Security Awareness

ist entsprechend ein zentrales Instrument des Risikomanagements im Kontext der Informationssicherheit von Unternehmen.

Security Awareness bedeutet, dass die innere Einstellung, das Wissen und somit auch die Handlungsweise von Mitarbeitern eines Unternehmens fundamentale Faktoren der Informationssicherheit widerspiegeln und damit einhergehend zum Schutze von Informationen, physischen Wirtschaftsgütern – und letztendlich allen existenziellen Werten – maßgeblich beitragen. Der Faktor Mensch nimmt im Bereich der Informationssicherheit und speziell beim Thema Security Awareness eine Schlüsselrolle ein, d. h. die Hauptbedrohungen sind auf den Faktor Mensch gerichtet (Bundesamt für Sicherheit in der Informationstechnik, 2014). Der Mensch stellt z. B. bei Angriffen mittels Spam und Social Engineering den maßgeblichen Faktor zur Verhinderung erfolgreicher Angriffe dar.

Die Anforderungen, die z. B. durch gesetzliche oder regulatorische Vorgaben, hinsichtlich der Security Awareness existieren, sind häufig nur für große Unternehmen bzw. Organisationen verbindlich und teilweise stark von der individuellen Branche bzw. dem Wirtschaftszweig abhängig.

So tritt beispielsweise die BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht) als Regulator für Unternehmen des Finanzwesens in Deutschland auf und stellt speziell auf diese Branche zugeschnittene Anforderungen. Security Awareness findet explizite Berücksichtigung in Standards, Normen und Frameworks für Informationssicherheit und wird somit z. B. auch bei der Zertifizierung nach einem Standard berücksichtigt. Häufig kommen im Bereich der Informationssicherheit die ISO/IEC 27000-Reihe, der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder Common Criteria (ISO/IEC 15408) zum Einsatz. Diese werden im Umfeld großer Unternehmen und Organisationen als Grundlage für eine Zertifizierung genutzt und dienen neben der tatsächlichen Verbesserung der Informationssicherheit der Gewährleistung einer unternehmensübergreifenden Vergleichbarkeit.

Zum einen wird Security Awareness in großen Unternehmen mittels spezieller Schulungen und Trainings erreicht, wobei ein nicht unerheblicher Aufwand für die initiale Einführung und fortwährende Weiterentwicklung erforderlich ist. Adobe Systems Incorporated (Adobe Systems Incorporated, 2014) implementiert Security Awareness beispielsweise über interne jährliche Trainings, interne Seminare mit Experten aus der Branche und der Möglichkeit an externen Konferenzen und Workshops teilzunehmen.

Zum anderen geht Security Awareness in der Regel mit technischen und organisatorischen Regelungen und Maßnahmen zum Schutze von Informationen einher. Dies kann beispielsweise bedeuten, dass sog. Non-Disclosure-Agreements (NDAs) vertraglich vor der Weitergabe vertraulicher Informationen schützen sollen. Technisch können diese Vereinbarungen z. B. mit der Klassifizierung von Dokumenten kontrolliert bzw. implementiert werden. Ein ausgeglichenes Maß bestehend aus Security Awareness und implementierten Kontrollen hat unmittelbaren Einfluss auf das Sicherheitsniveau eines Unternehmens. Holistische Systeme für das Management von Informationssicherheit können jedoch nur bei direkter Berücksichtigung der Security Awareness betrieben werden.

Da Security Awareness nahezu durchweg als Bestandteil von Standards, Normen und Frameworks Anwendung in Unternehmen findet, ist ein Zusammenhang zwischen der Größe von Unternehmen und der Einführung bzw. der Existenz von Programmen für Security Awareness gegeben. Security Awareness wird in KMU hingegen häufig weder durch einen Regulator noch durch besondere zusätzliche Anforderungen vorausgesetzt. Eine Zertifizierung nach Standards,

Normen und Frameworks geschieht in diesem Umfeld häufig auf freiwilliger Grundlage oder zur Steigerung der Reputation. Sichere Produkte/ Unternehmen erhöhen das Vertrauen der Kunden (Banerjee, Banerjee & Murarka, 2013).

- „There should be limitations on what cloud vendors can do with our data; rights, like the requirement that they delete our data when we want them to; and liabilities when vendors mishandle our data.“ (Bruce Schneier)(Crowther et al., 2013)
- „The costs incurred from a Data Breach event far outstrip the cost of a proactive Cyber Security approach.“ (Darek Dabbs) (Crowther et al., 2013)
- „Social Engineering attacks are costly especially in large organizations“ (Dimensional Research, 2011)

Im Umfeld der KMU ist die tatsächliche Umsetzung von Security Awareness zu überprüfen und mit Anforderungen, die z. T. nur geringfügig von Anforderungen großer Unternehmen abweichen, zu vergleichen (Bundesamt für Sicherheit in der Informationstechnik & secunet Security Networks, 2011). In Deutschland, Großbritannien, den USA und Japan zeigten Mitarbeiter kleiner Unternehmen eine geringere Sensibilisierung für Sicherheitsfragen und gleichzeitig eine höhere Bereitschaft zu risikoreichen Aktivitäten (Holst, 2008).

1.2. Projektziele

Im Rahmen einer Studie sind primär nachfolgende Fragestellungen untersucht worden:

1. Welche Anforderungen an die Informationssicherheit von großen Unternehmen und Organisationen existieren und wovon gehen diese im Detail aus? (Gesetzgebung, regulatorische Anforderungen etc.)
2. Umfassen diese Anforderungen explizit den Bereich der Security Awareness?
3. Auf welche Weise wird diesen Anforderungen im genannten Umfeld nachgekommen? (Zertifizierung nach Standards, Normen Frameworks etc.)
4. Wie wird Security Awareness im genannten Umfeld gemessen?
5. Welche Motivation außerhalb gesetzlicher und regulatorischer Anforderungen dient als Antrieb zur Verbesserung der Informationssicherheit und im Speziellen der Security Awareness in KMU?
6. Können die Anforderungen, die für große Unternehmen und Organisationen verbindlich gelten, auch auf KMU übertragen werden? Welche Gemeinsamkeiten und tatsächlichen Schnittmengen gibt es sowohl bei den Anforderungen als auch bei den möglichen individuellen Implementierungen mitigierender Maßnahmen?
7. Inwieweit können Methoden zur Gewährleistung und Verbesserung von Security Awareness, die in großen Unternehmen im Einsatz sind, auf KMU adaptiert und genutzt werden? Beispiele: Kampagnen zu Verbesserung der Security Awareness (Newsletter, Poster etc.) oder Methoden zur Schulung von Mitarbeitern.

2. Projektergebnisse

Die Projektergebnisse sind vielfältig. In Abschnitt 2.1 wird dazu die Erfüllung der Projektziele besprochen. Abschnitt 2.2 erörtert Fortschritte im Bereich der Einwerbung von Drittmitteln, Abschnitt 2.3 geht auf das Thema Serious Gaming ein, Abschnitt 2.4 präsentiert aufgebaute Kontakte zu Industrie- und Hochschulpartnern und Abschnitt 2.5 enthält eine Aufstellung der ausgearbeiteten Projektartefakte, die nun in der Lehre eingesetzt werden.

2.1. Erfüllung der Projektziele

Nachfolgend wird die Bearbeitung der in Abschnitt 1.2 vorgestellten Fragestellungen stichpunktartig beschrieben. Ein detailliert kommentiertes Verzeichnis der relevanten Literatur befindet sich in Anhang A.

1. Welche Anforderungen an die Informationssicherheit von großen Unternehmen und Organisationen existieren und wovon gehen diese im Detail aus? (Gesetzgebung, regulatorische Anforderungen etc.)
   - IT-Sicherheitsgesetz (2015) ist ein Artikelgesetz zur Erhöhung der Sicherheit informationstechnischer Systeme. Ergänzungen des BSI-Gesetzes um Sicherheitsanforderungen an „Kritische Infrastrukturen“. Somit müssen solche Infrastrukturen branchenspezifische Standards erfüllen und ein „Informationssicherheitsmanagementsystem (ISMS)“ einführen (Bundesamt für Sicherheit in der Informationstechnik, 2008; Bundesgesetzblatt, 2015).
   - Weitere Gesetze erfordern die Einführung eines ISMS:
     - Bundesdatenschutzgesetz (BDSG) (Bundestag, 1997)
     - Telekommunikationsgesetz (TKG) (Bundestag, 2004)
     - Telemediengesetz (TMG) (Bundestag, 2007)
   - IS0/IEC-27000 Familie adressiert die Implementierung und den Betrieb von ISMS.
   - IT-Grundschutz (Bundesamt für Sicherheit in der Informationstechnik - BSI, 2012) umfasst nationale Vorgehensweisen und Leitlinien des BSI zur Erreichung von Informationssicherheit.
   - VdS Cyber-Security für kleine und mittlere Unternehmen (KMU) (VdS Schadenverhütung, 2015) sind Richtlinien speziell für KMU und stellen Grundlage für eine Zertifizierung durch die VdS.
2. Umfassen diese Anforderungen explizit den Bereich der Security Awareness?
   - Die einzuführenden ISMS umfassen nicht explizit den Bereich der Security Awareness. Jedoch sind die Mitarbeiter eine der zentralen Komponenten eines ISMS und müssen somit in den Sicherheitsprozess eingebunden werden. Es wird dabei soweit nur die Einarbeitung und Verpflichtung der Mitarbeiter angesprochen. Bei der Einarbeitung sollen Aspekte des jeweiligen Arbeitsplatzes berücksichtigt werden (Bundesamt für Sicherheit in der Informationstechnik, 2008).

- In den Richtlinien des VdS wird ebenfalls kurz auf das Personal eingegangen, doch werden dort nur die bereits in der ISO/IEC 27001 genannten Punkte wiederholt (VdS Schadenverhütung, 2015).
- Im IT-Grundschutz wird jedoch der Faktor Mensch und somit die Security Awareness direkt angesprochen und verlangt dort eine Sensibilisierung der Mitarbeiter (Bundesamt für Sicherheit in der Informationstechnik - BSI, 2012, p.50 ff).
- SIZ „Sicherer Betrieb“ (Sicherheitsstandart der Sparkassen-Finanzgruppe) (Kaltenböck & Schuster, 2013) fokussiert auf Security Awareness.
- Zulieferer benötigen einen gemeinsamen Standard. Information Security Forum (ISF) als Informations- und Hilfsstelle (Nowak, 2010).

3. Auf welche Weise wird diesen Anforderungen im genannten Umfeld großer Unternehmen und Organisationen nachgekommen? (Zertifizierung nach Standards, Normen, Frameworks, etc.)
    - Gesetzlicher Zwang einer Einführung eines ISMS
    - Zertifizierungen durch das BSI, Grundschutzanalyse, IT-Grundschutz (Bundesamt für Sicherheit in der Informationstechnik, 2009; Bundesamt für Sicherheit in der Informationstechnik - BSI, 2012)
    - ISO/IEC 27001 Zertifikat (Bundesamt für Sicherheit in der Informationstechnik, 2008)
    - VdS Cyber-Security für kleine und mittlere Unternehmen (VdS Schadenverhütung, 2015)
    - ISIS12 (Netzwerk Informationssicherheit im Mittelstand (NIM) des Bayerischen IT-Sicherheitscluster e.V., 2018) für KMU (Auf KMU zugeschnittene Zertifizierung) vom Netzwerk Informationssicherheit im Mittelstand (NIM) des Bayerischen IT-Sicherheitscluster e.V.
    - European Network and Information Security Agency (ENISA) unterstützt bei der Mitarbeitersensibilisierung (ENISA, 2009)
    - Verhaltensregeln für Mitarbeiter
    - Aufklärung (Bedrohungen aufzeigen)
    - Access Control + Information Security Managers + information protection awareness course (Dabei wird überprüft, ob die Angestellten diesen online Kurs regelmäßig abschließen) (Oracle Consulting, 2015)
    - Poster, Seminare, Angriffe
    - Regelmäßige Kurse/Kampagnen erhöhen den Erfolg.
    - Beispiele für etablierte Ansätze:
        - Mitarbeiter Zertifizierung mit verschiedenen Stufen; enthält Gamification Inhalte (Adobe Systems Incorporated, 2014).
        - Microsoft jagt das Phantom: Aufzeigen von Schwachstellen durch tatsächlichen Angriff auf das Unternehmen. Das Unternehmen kämpft gegen das Phantom, Emotionen sollen dadurch erzeugt werden (Köhler, 2014).

  - Security Parcours: Event, bei dem Mitarbeiter in Gruppen Stationen mit Miniplanspielen durchlaufen (Buzgo, Schog & Pokoyski, 2013).
  - Vom Poster zur Kampagne: Pflichttrainings für Angestellte, wobei Manager ein gesondertes Training erhalten und die es besteht die Möglichkeit freiwillige Ergänzungstrainings zu machen (Schimmer, 2013).
- Wünschenswerte Ansätze:
  - Security by Design / Security as a Service (Houdeau & Rose, 2015)
  - Gesetzlicher Grundschutz (Houdeau & Rose, 2015)
- „Accepting that foundational information security measures will become less effective over time, this stage focuses on the changing environment and highlights the actions necessary to ensure that organizations can continue to adapt to keep pace and match the changing business requirements and dynamics.“ (van Kessel & Allan, 2015)
- Es wird für die Umsetzung Personal und Budget im großen Umfang benötigt;.ebenso die Kooperation der Managementebene (Schimmer, 2013).

4. Wie wird Security Awareness im genannten Umfeld großer Unternehmen und Organisationen gemessen?
   - In den Standards, da dort Security Awareness kaum explizit genannt, werden keine Methoden zur Messung von Security Awareness genannt.
   - Checkliste für ISMS, bietet aber kein Vorgehen um Security Awareness zu messen (Bundesamt für Sicherheit in der Informationstechnik - BSI, 2012).
   - Social Engineering Angriffe, Audits in denen der Sicherheitsverantworliche die Büros der Mitarbeiter auf Sicherheitsmängel überprüft oder Versenden gezielter Phishing E-Mails (Ziegler & Rocholl, 2012).
   - „In manchen Unternehmen erfolgt die Messung des Sicherheitsbewusstseins der Mitarbeiter ausschließlich über die Erfassung des tatsächlichen sicherheitsrelevanten Verhaltens durch z. B. Auswertung von Log-Files oder die statistische Erfassung von Sicherheitsvorfällen“ (Zerr, 2007).
   - Fragebögen (Zerr, 2007)
   - Keine Literatur zur Security Awareness Messung explizit in KMU vorhanden.

5. Welche Motivation außerhalb gesetzlicher und regulatorischer Anforderungen dient als Antrieb zur Verbesserung der Informationssicherheit und im Speziellen der Security Awareness in KMU?
   - 60% der erwerbstätigen Personen arbeiten in KMU (Statistisches Bundesamt, 2016).
   - Der Digitalisierungsgrad bei KMU ist erheblich angestiegen (Littger, Brandl & Böhme, 2014, S. 7).
   - „People and vendors are one of the most critical yet one of the weakest links in the cyber defence chain.“ (KPMG India, 2015)
   - Anstieg in Cyberangriffen auf kleine und mittlere Unternehmen (Matzer, 2016)

- Angriff auf den Bundestag (Boie & Strunz, 2015), als Beispiel eines Angriffs, der vor allem aufgrund mangelnder Security Awareness in dieser Weise möglich war.
- Phishing und Mangelndes Verständnis/Generelles Bewusstsein werden als größte Risiken angesehen (SANS, 2015).
- In KMU: „Die Rolle der Mitarbeiter wird unterbewertet.“ „89% aller befragten Unternehmen verzichten auf regelmäßige Zertifizierungen.“ (Stand 2014) (Littger et al., 2014, S. 13)
- Fahrlässigkeit und Böswilligkeit sind Grund für viele Datenpannen (Ponemon Institute, 2012, S. 2).
- KMU werden öfter Ziel von Spear-Phishing Angriffen als große Unternehmen und mehr als im Vorjahr (2012-2013) (Wood, Nahorney, Chandrasekar, Wallace & Haley, 2014).
- Budget für Informationssicherheit liegt bei den meisten Unternehmen bei unter 5% der IT-Ausgaben. (KPMG India, 2015, S. 15).
- Sichere Produkte bzw. Unternehmen erhöhen das Vertrauen der Kunden (Banerjee et al., 2013).
- Vorherige Sicherheitsvorfälle (Lardschneider, 2007)
- Insider-Angriffe auf das eigene Unternehmen gehören laut einer von Secure Computing in Auftrag gegebenen Umfrage zu den derzeit größten Befürchtungen von IT-Sicherheitsverantwortlichen (Holst, 2008).
- „Awareness of cyber threats propels improvement“ (Ernest & Young, 2013)
- Differenzierung im Wettbewerb (Rumpel et al., 2011)
- Interner Nutzen einer Zertifizierung:
  - Konsequente Reduzierung der Verluste durch Sicherheitsvorfälle
  - Höhere Verfügbarkeit der IT-Systeme
  - Bessere Qualität der Geschäftsprozesse
  - Kundenbindung
  - Wichtiger Beitrag zur Erfüllung von gesetzlichen Anforderungen (Datenschutzgesetze, Bilanzrechtsgesetze) (Rumpel et al., 2011)

6. Können die Anforderungen, die für große Unternehmen und Organisationen verbindlich gelten, auch auf KMU übertragen werden? Welche Gemeinsamkeiten und tatsächlichen Schnittmengen gibt es sowohl bei den Anforderungen als auch bei den möglichen individuellen Implementierungen mitigierender Maßnahmen?
   - Anforderungen, die für große Unternehmen verbindlich sind, sind auch für KMU einzuhalten. Aus der Literatur dazu wird keine Unterscheidung deutlich.
   - Produktions- und Termindruck, personell knappe Besetzung der IT-Abteilung und sich einschleichende Routine verhindern jedoch häufig eine zeitlich angemessene Auseinandersetzung mit der IT-Sicherheit und neuen Risiken (Bundesamt für Sicherheit in der Informationstechnik & secunet Security Networks, 2011).

- Geringe Angestelltenanzahl macht es einfacher, gezielter Security Awareness zu vermitteln, jedoch wird durch Personalmangel die Umsetzung eines ISMS oder einer Security Awareness Kampagne schwierig.
- Geringere finanziellen Mittel eines KMU müssen berücksichtigt werden.
- Bei großen Unternehmen muss mehr generalisiert werden (Kaltenböck & Schuster, 2013).

7. Inwieweit können Methoden zur Gewährleistung und Verbesserung von Security Awareness, die in großen Unternehmen im Einsatz sind, auf KMU adaptiert und genutzt werden? Beispiele: Kampagnen zu Verbesserung der Security Awareness (Newsletter, Poster etc.) oder Methoden zur Schulung von Mitarbeitern.
   - Planung statt reaktive Aktionen. Erstellen eines Security Plans (Speed, 2012).
   - Konzentrieren auf Schlüsselthemen (Passwörter, Internet und E-Mail Nutzung, Computersicherheit, Datensicherheit, Netzwerksicherheit) (Little, 2014).
   - Kampagnen nutzen, welche bereits auf KMU getrimmt sind und einen Organisationsvorteil bieten, z. B. IS-FOX Security Awareness Tools (CBT Training & Consulting, 2014).

Literatur, die Unterschiede zwischen KMU und großen Unternehmen in Bezug auf Security Awareness thematisiert, ist sehr begrenzt. Im Bereich der Forschung werden KMU zwar bereits speziell thematisiert, man findet jedoch keine Erfahrungsberichte von Kampagnen oder ähnlichem, die ursprünglich für ein großes Unternehmen verwendet wurden und dann auf ein KMU adaptiert wurden. In Deutschland gibt es zwar bereits Hilfestellungen extra für KMU zum Einführen eines ISMS (z. B. ISIS12 (Fraunhofer AISEC, 2014)), doch der Aspekt der Security Awareness fehlt explizit in der Definition eines ISMS und wird somit nicht ausreichend thematisiert.

Die grundsätzliche Abhängigkeit vieler Unternehmen von KMU als Zulieferer und Dienstleister kritischer Technologien bzw. kritischen Know-hows verlagert die Notwendigkeit des Managements von Informationssicherheit bis hin zu KMU.

Die zunehmende Anzahl der Angriffe auf KMU zeigen eine deutliche Verlagerung der Angriffsziele. Ursache hierfür sind die meist unzureichenden bzw. z. T. nicht-existierenden Kontrollen für Informationssicherheit (Proofpoint, 2015a, S. 70 ff., aufgerufen am 27.09.2015). Diese Lücke ist sowohl auf geringere Budgets als auch auf mangelnde Awareness für Informationssicherheit zurückzuführen – nicht selten vom Management ausgehend.

Die Gefährdung für KMU stellt gleichzeitig eine ebenso große indirekte Gefährdung der von den KMU abhängigen großen Unternehmen dar. In diesem Zusammenhang sind besonders kritische Rollen in einem Unternehmen zu untersuchen, z. B. Administratoren der IT eines Unternehmens, die meist deutlich geringeren technischen Einschränkungen als normale Angestellte unterliegen. Unterschiedliche Sicherheitsstufen werden bei Security Awareness Programmen kaum mit einbezogen. Es werden meist Informationen für die breite Masse und nicht für spezielle Positionen geliefert (Choi & Lee, 2013).

2.2. Drittmittel

Die Verbesserung der Security Awareness in KMU zur Stärkung der allgemeinen Informationssicherheit in KMU ist das übergeordnete Ziel eines auf diesem HiFF-Projekt aufbauenden umfangreicheren Projektes. Dabei finden auch neuerliche Anforderungen wie z. B. das kürzlich in Kraft getretene IT-Sicherheitsgesetz (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme) für Betreiber kritischer Infrastrukturen Beachtung. Die im Rahmen dieses HiFF-Projektes entwickelten Ergebnisse dienen primär als Vorarbeiten für die Beantragung weiterer Drittmittelprojekte, so z. B. BMBF Forschungsförderung (Bundesministerium für Bildung und Forschung).

Während der Doktorand das Projekt bearbeitet hat, ist ein Entwurf für einen Drittmittelprojektantrag entstanden. Es war geplant, diesen für das Landesforschungsprogramm Ziel2 IKT.NRW 2016 einzureichen. Mangels Praxispartner wurde der Antrag nicht eingereicht.

Mit der Idee einen neuen Doktoranden zu aquirieren wurde ein Dissertationsthema im Bereich der Information Security Awareness in Zusammenarbeit mit Prof. Dr. Maritta Heisel von der Universität Duisburg-Essen und der telexiom AG, Köln ausgearbeitet und Drittmittel für eine entsprechende Doktorandenstelle in einem vom Land NRW geförderten Graduiertenkolleg NERD beantragt. Dieser Antrag war zunächst in der ersten Runde erfolgreich, wurde jedoch in der zweiten, entscheidenden Runde abgelehnt.

2.3. Serious Gaming

Im Rahmen der Literaturrecherche und durch verschiedene Kontakte, z. B. zur Social Engineering Academy (SEA) GmbH in Frankfurt am Main, wurde verstärkt das Thema „Serious Gaming“ zur Verbesserung von Information Security Awareness bearbeitet. Spiele in diesem Bereich funktionieren nach dem Prinzip „learning by doing“ und sollen typischerweise die Motivation der Lernenden verstärken (Popescu, Romero & Usart, 2012) und Lernprozesse fördern. Wichtige Merkmale der Spiele (Le, Weber & Ebner, 2013) sind:

- aktives Lernen (durch den kontinuierlichen Spielzyklus)
- konstruktives Lernen (durch das Austesten von Handlungsalternativen nach dem trial-and-error-Prinzip und durch individuelle Interpretation der gesammelten Erfahrungen)
- selbstgesteuertes Lernen (durch individuelle Vorgehensweisen und freigewählte Spieldauer)
- soziales Lernen (in Mehrspielervarianten durch Kooperation, Wettbewerb oder durch Erfahrungsaustausch zwischen den Spielenden)
- emotionales Lernen (durch tiefgreifende Beteiligung am Handlungsgeschehen mit persönlicher Identifikation - parasozialer Interaktion - und der Selbstwirksamkeitserfahrung)
- situiertes Lernen (durch Versetzung in unterschiedliche Rollen und Spielsettings mit entsprechenden Problemen und Aufgaben)

Insbesondere digitales Game-Based Learning findet durch die Popularität von digitalen Spielen Interesse, da bisherige Ansätze nicht den erhofften Erfolg brachten (z. B. hohe Abbruchquoten aufgrund von mangelnder intrinsischer Motivation) (Le et al., 2013). Das Interesse an Game-based Learning Produkten wächst stetig (Adkins, 2016). Gründe (Adkins, 2016, S.10) hierfür sind:

- schnell schwindender Widerstand gegenüber Lernspielen in Unternehmen und dem Akademischen Bereich
- Wachsender Umfang an empirischen Beweisen für die Effektivität von Game-based Learning

Serious Games erscheinen speziell für den Bereich Information Security Awareness in KMU gut anwendbar, denn:

- Serious Games können für den gewünschten Zweck angepasst werden und sind somit sehr flexibel und weitreichend einsetzbar.
- Es ist kostengünstiger Angriffe auf das Unternehmen innerhalb eines Serious Games zu simulieren, als einen technisch realisierten Test-Angriff durchzuführen.
- Die meisten Angestellten empfinden Sicherheitstrainings als lästig; Serious Games erhöhen die Motivation zum Lernen.
- Mobile Serious Games können die Notwendigkeit von festen Terminen für Trainings obsolet machen.

Beispiele für Serious Games für Information Security Awareness:

- CyberCIEGE (Cone, Thompson, Irvine & Nguyen, 2006)
  - genutzt von der U.S. Navy
  - Möglichkeit eigene Szenarios zu erstellen für spezielle Zielgruppen (zum Beispiel erweiterte Szenarien für das IT-Personal mit zusätzlichem Inhalt über Netzwerksicherheit)
  - flexibel einsetzbar
  - Spieler übernimmt die Rolle eines „security decision maker“ auf einem Schiff und muss Aufgaben bewältigen, die die Sicherheitslage des Unternehmes erhöhen.
- SIRET Security Game (D'Apice, Grieco, Liscio & Piscopo, 2015)
  - gezielt für nicht IT-Experten
  - klassischen „Adventure Games“ nachempfunden (Fortschreiten in der Rahmengeschichte durch das Lösen von Rätselaufgaben)
  - Spieler übernimmt die Rolle eines Angestellten eines berühmten Unternehmens und muss Unternehmensdaten vor Spionen und Saboteuren beschützen.

2.4. Netzwerk

Da eine Verbesserung der eingangs aufgezeigten Problematik bzw. der damit verbundenen Risiken nur in direkter Zusammenarbeit und unter Berücksichtigung etwaiger Besonderheiten von KMU erreicht werden kann, sind diesbezüglich Kooperationen mit Unternehmen angestrebt worden. Dabei erforderte der interdisziplinäre Charakter der Security Awareness (Corona, 2009) die Einbeziehung von über die Informatik hinausgehender Expertise. Der Aufbau eines möglichst lokalen Netzwerks aus Hochschul- und Industriepartnern dient somit der Realisierung des Projektziels der Initiierung von Forschung im Bereich der Information Security Awareness.

Hochschulpartner Im Rahmen des Projektes ist ein Kontakt zu Prof. Dr. Maritta Heisel, Professorin für Software Engineering der Abteilung Informatik und Angewandte Kognitionswissenschaft der Fakultät für Ingenieurwissenschaften der Universität Duisburg-Essen aufgebaut worden.

Industriepartner Schwerpunktmäßig sind Kontakte zu Industriepartnern aufgebaut worden. Besonders hervorzuheben sind dabei folgende Firmen:

- **telexiom AG**
  Spichernstraße 6B
  50672 Köln
- **Social Engineering Academy (SEA) GmbH**
  Eschersheimer Landstraße 42
  60322 Frankfurt am Main
- **MS Deutschland GmbH**
  Holzmarkt 2a
  50676 Köln
- **TÜV IT GmbH**
  Langemarckstraße 20
  45141 Essen
- **ITESYS GmbH**
  Emil-Figge-Str. 76
  44227 Dortmund
- **IT Akademie Dr. Heuer**
  Erkrather Str. 343
  40231 Düsseldorf
- **Salzerfilm Marcus Wildelau und Daniel Blazek GbR**
  Bleichstr. 77a
  33607 Bielefeld

2.5. Transfer

Basierend auf der ausführlichen Literaturrecherche im Rahmen dieses Projektes sind einerseits Lehrmaterialien entstanden und andererseits studentische Projekte und Abschlussarbeiten initiiert worden. Eine Lehreinheit zur Einführung in das Thema Information Security Awareness im Umfang von zwei 90 minütigen Vorlesungseinheiten mit zugehörigem Übungsmaterial ist nun Teil des Bachelormoduls „IT-Sicherheit“ und des Mastermoduls „Faktor Mensch in der Informationssicherheit“ in den Medieninformatik Studiengängen des Fachbereichs Medien an der Hochschule Düsseldorf. Zwei studentische Projekte haben Serious Games für Information Security Awareness entwickelt; insbesondere das von einer Gruppe von Masterstudenten der Medieninformatik entwickelte Spiel „What the Hack“[1] hat nachhaltig Einfluss auf weitere Projekte und Abschlussarbeiten, sodass aktuell bereits an Erweiterungen und Verbesserungen für das Spiel gearbeitet wird.

3. Ausblick

Die in dem vorliegenden Projektbericht beschriebenen Ergebnisse sollen zukünftig für die Beantragung eines Drittmittelprojekts, z. B. einem Antrag im Rahmen des FH Basis Programms des Landes NRW und für den bilateralen Transfer mit der Lehre an der Hochschule Düsseldorf, dabei insbesondere im Rahmen von Abschlussarbeiten und studentischen Projekten, genutzt werden. Wünschenswert ist die in Kooperation mit Industriepartnern durchgeführte Erstellung eines Framework für Security Awareness Training mit angeschlossener Prüfung auf Effektivität sowie der Entwicklung eines Serious Game – jeweils unter Berücksichtigung KMU-spezifischer Anforderungen.

[1] https://hendrik-schulte.github.io/what_the_hack/, aufgerufen am 12.04.2018

Literatur

Aaron, G. & Manning, R. (2014). Phishing Activity Trends Report: 2nd Quarter 2014. APWG, Lexington. Zugriff unter http://docs.apwg.org/reports/apwg_trends_report_q2_2014.pdf

Aaron, G. & Rasmussen, R. (2014). Global Phishing Survey: Trends and Domain Name Use in 2H2014. APWG, Lexington. Zugriff unter http://docs.apwg.org/reports/APWG_Global_Phishing_Report_2H_2014.pdf

Aaron, G., Rasmussen, R. & Routt, A. (2014). Global Phishing Survey: Trends and Domain Name Use in 1H2014. Lexington. Zugriff unter http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2014.pdf

Abdel-Aziz, A. (2010). A Bit of Psychology to Improve your Security Awareness Program. The SANS Technology Institute. Zugriff unter http://docplayer.net/12383687-A-bit-of-psychology-to-improve-your.html

Adkins, S. S. (2016). The 2016-2021 Global Game-Based Learning Market: July 26, 2016 at the Serious Play Conference. Ambient Insight. Zugriff unter https://seriousplayconf.com/wp-content/uploads/2016/07/AmbientInsight_2016_2021_Global_Game-basedLearning_Market_SeriousPlay2016_ExecutiveOverview.pdf

Adobe Systems Incorporated. (2014). Adobe Security Training.

Aircademy. (o.D.). *Der Faktor Mensch - human factors*. Advanced PPL-Guide.

Albrechtsen, E. (2008). Friend or foe? Information security management of employees: Thesis for the degree of philosophiae doctor. Norwegian University of Science and Technology, Trondheim. Zugriff unter https://pdfs.semanticscholar.org/40cf/125b1bb89e3d8f566708ebaa3f119e84beed.pdf

Amrin, N. (2014). The Impact of Cyber Security on SMEs. Faculty of Electrical Engineering, Mathematics and Computer Science. Zugriff unter http://essay.utwente.nl/65851/1/Amrin_MA_EEMCS.pdf

Awareness Program Special Interest Group PCI Security Standards Council. (2014). Information Supplement: Best Practices for Implementing a Security Awareness Program: Version 1.0. Security Standards Council. Zugriff unter https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

Bada, M., Sasse, A. & Nurse, J. (Hrsg.). (2015). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? Zugriff unter https://ora.ox.ac.uk/objects/uuid:cfed4907-d32a-4450-b075-ad37477b10d8

Banerjee, C., Banerjee, A. & Murarka, P. D. (2013). An Improvised Software Security Awareness Model. *International Journal of Information, Communication and Computing Technology*, *1*(2), 43–48.

Berkenkopf, S. & Benzmüller, R. (2011). Gefährliche E-Mails. G Data. Zugriff unter https://www.gdata.de/fileadmin/web/de/documents/whitepaper/G_DATA_Whitepaper_E-Mail_Gefahren_German.pdf

Beyer, M. & Ahmed, S. (2012). Information Security Awareness. Hewlett-Packard Development Company. Zugriff unter https://www.riscs.org.uk/wp-content/uploads/2015/12/Awareness-is-Only-the-First-Step.pdf

Binational Working Group on Cross Border Mass Marketing Fraud. (2006). Report on Phishing: A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States.

Boie, J. & Strunz, B. (2015). Experten identifizieren Angriffs-Methode. *Süddeutsche Zeitung vom 12.09.2015*. Zugriff unter http://www.sueddeutsche.de/politik/hacker-attacke-auf-den-bundestag-experten-identifizieren-angriffs-methode-1.2645171

Bundesakademie für öffentliche Verwaltung im Bundesministerium des Inneren. (2011). Die Initiative - Resümee und Ausblick. *Sicher gewinnt!*

BSI-Standard 100-1 Managementsysteme für Informationssicherheit (ISMS). (2008). Bonn. Zugriff unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1001.pdf?__blob=publicationFile

Bundesamt für Sicherheit in der Informationstechnik. (2009). Act to Strengthen the Security of Federal Information Technology. Zugriff unter https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf?__blob=publicationFile&v=2

Die Lage der IT-Sicherheit in Deutschland 2014. (2014). Berlin. Zugriff unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

Die Lage der IT-Sicherheit in Deutschland 2015. (2015). Bonn. Zugriff unter https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf%3F__blob%3DpublicationFile%26v%3D5

Leitfaden Informationssicherheit: IT-Grundschutz kompakt. (2012). Bonn. Zugriff unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile

Bundesamt für Sicherheit in der Informationstechnik & secunet Security Networks. (2011). Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen: Grad der Sensibilisierung des Mittelstandes in Deutschland. Bonn. Zugriff unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.pdf?__blob=publicationFile

Bundesgesetzblatt. (2015). Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz): Vom 17. Juli 2015. *Bundesgesetzblatt, Teil 1*(Nr. 31). Zugriff unter https://www.bmi.bund.de/SharedDocs/downloads/DE/gesetztestexte/it-sicherheitsgesetz.pdf?__blob=publicationFile&v=1

Bundestag. (1997). Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz - BDSG): Ausgegeben zu Bonn am 1. Februar 1977. *Bundesgesetzblatt*, (Nr. 7). Zugriff unter https://www.bgbl.de/xaver/bgbl/text.xav?SID=&tf=xaver.component.Text_0&tocf=&qmf=&hlf=xaver.component.Hitlist_0&bk=bgbl&start=%2F%2F*%5B%40node_id%3D%27294920%27%5D&skin=pdf&tlevel=-2&nohist=1

Bundestag. (2004). Telekommunikationsgesetz (TKG). Bundesrepublik Deutschland und Bundesrepublik Deutschland.

Bundestag. (2007). Gesetz zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer - Geschäftsverkehr - Vereinheitlichungsgesetz - EIGVG). Bundesrepublik Deutschland.

Butavicius, M., Parsons, K., Pattinson, M. & McCormac, A. (2015). Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails: Australasian Conference on Information Systems. Adelaide.

Buzgo, I., Schog, C. & Pokoyski, D. (2013). SECURITY AWARENESS @T-SYSTEMS. T-Systems. Zugriff unter https://www.eco.de/wp-content/blogs.dir/27/files/20130605_awarenessts_fuer_eco-1.pdf

CBT Training & Consulting. (2012). Datenblatt Security Awareness Kampagnen. HvS-Consulting AG - IS-FOX Security Awareness Tool, München. Zugriff unter https://www.it-secuta.de/files/Security-Awareness-ISFOX-Tools-PDFs/Security-Awareness-Infopaper.pdf

CBT Training & Consulting. (2014). Security Awareness Mittelstand. HvS-Consulting AG - IS-FOX Security Awareness Tool, München. Zugriff unter https://www.it-secuta.de/files/Security-Awareness-ISFOX-Tools-PDFs/Security-Awareness-Mittelstand.pdf

CERT Insider Threat Team. (2014). Unintentional Insider Threats: Social Engineering. Software Engineering Institute. Zugriff unter https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_77459.pdf

Choi, K.-H. & Lee, D. (2013). A study on strengthening security awareness programs based on an RFID access control system for inside information leakage prevention. *Multimedia Tools and Applications*, *74*(20), 8927–8937.

CIS - Certification & Information Security Service. (2009). IS027001 in KMU effizient umsetzen: case study. Wien. Zugriff unter http://ch.cis-cert.com/Media/490856a6-ee37-422f-bff2-0e5e02dd34f0/AT/Broschueren/ISO_27001_in_KMU.pdf

Cone, B. D., Thompson, M. F., Irvine, C. E. & Nguyen, T. D. (2006). Cyber Security Training and Awareness Through Game Play. In S. Fischer-Hübner, K. Rannenberg, L. Yngström & S. Lindskog (Hrsg.), *Security and Privacy in Dynamic Environments. SEC 2006* (S. 431–436). IFIP International Federation for Information Processing. Boston: Springer US.

Corona, C. O. (2009). Information security awareness: an innovation approach. Royal Holloway, University of London, London. Zugriff unter https://repository.royalholloway.ac.uk/file/9e7de7b8-d65c-dc5c-222c-e33946e5d74e/1/RHUL-MA-2009-03.pdf

Cramer, J. (2009). IT-Security Governance und Awareness im RWE-Konzern. RWE IT.

Crowther, J., Dabbs, D., Dakin, S., Freed, A. M., Herold, R., Kam, R., ... Westby, J. (2013). 2013 Data privacy, information security and cyber insurance trends. Cyber Data Risk Managers. Zugriff unter http://databreachinsurancequote.com/wp-content/uploads/2013/02/2013-Data-Privacy-Information-Security-and-Cyber-Insurance-Trends-Report.pdf

Cybersecurity Nexus. (2015). State of Cybersecurity: Implications for 2015. ISACA, RSA.

D'Apice, C., Grieco, C., Liscio, L. & Piscopo, R. (2015). Design of an Educational Adventure Game to teach computer security in the working environment. In KSI Research Inc. and Knowledge Systems Institute Graduate School (Hrsg.), *DMS* (S. 179–185). Journal of Visual Languages and Sentient Systems. Vancouver. Zugriff unter http://ksiresearchorg.ipage.com/seke/Proceedings/dms/DMS2015_Proceedings.pdf

Deloitte. (2014). Phishing as a Service: Cyber Risk Managed Services. Zugriff unter https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-cyber-risk-managed-service-phishing-noexp.pdf

Dimensional Research. (2011). The risk of social engineering on information security: a survey of IT professionals. Zugriff unter https://www.stamx.net/files/The-Risk-of-Social-Engineering-on-Information-Security.pdf

Dimler, S., Federrath, H. & Nowey, T. (2006). Awareness für IT-Sicherheit und Datenschutz in der Hochschulausbildung–Eine empirische Untersuchung. In J. Dittmann (Hrsg.), *Sicherheit 2006* (S. 18–21). GI-Edition Proceedings. Bonn.

Dodge, R. C. & Ferguson, A. J. (2006). Using Phishing for User Email Security Awareness: Security and Privacy in Dynamic Environments: Proceedings of the IFIP TC-11 21st International Information Security Conference (SEC 2006), 22–24 May 2006, Karlstad, Sweden. In S. Fischer-Hübner, K. Rannenberg, L. Yngström & S. Lindskog (Hrsg.), *Security and Privacy in Dynamic Environments. SEC 2006* (S. 454–459). IFIP International Federation for Information Processing. Boston: Springer US.

ENISA. (2008). Sicherer Umgang mit USB-Speichersticks. Heraklion.

ENISA. (2009). Die ENISA-Plattform für die Zusammenarbeit bei der Sensibilisierung. Heraklion. Zugriff unter https://publications.europa.eu/en/publication-detail/-/publication/01454107-a868-46e5-8211-6ec2ec73cfdd/language-de

Ernest & Young. (2013). Under cyber attack: EY's Global Information Security Survey 2013. Zugriff unter http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf

Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen: (Bekannt gegeben unter Aktenzeichen K(2003) 1422). (2003).

Exter, A. & Drodt, M. (2013). CSI:DB - Die IT Security-Awareness-Kampagne der Deutschen Bahn. *Datenschutz und Datensicherheit - DuD*, *37*(5), 279–282.

Fletscher, T. (2011). FAA Secure Application Development and SDLC. Federal Aviation Administration. Zugriff unter https://pdfs.semanticscholar.org/presentation/099f/deedd9dd6ac51280264dd438ffddec70152d.pdf

Fox, D. (2013). Awareness 3.0. *Datenschutz und Datensicherheit - DuD*, *37*(5), 269.

Fraunhofer AISEC. (2014). Gutachten zur Anwendbarkeit von ISIS12 in der öffentlichen Verwaltung. Zugriff unter https://www.stmi.bayern.de/assets/stmi/sus/datensicherheit/aisec_%E2%80%93_gutachten_isis12.pdf

Gardner, B. & Thomas, V. (2014). *Building an Information Security Awareness Program : Defending Against Social Engineering and Technical Threats*. Elsevier Science.

Gillis, J. & Millar, D. (2014). Redesigning Boston Colleges information security awareness program based on curren research. Boston University Security Camp, Boston. Zugriff unter Redesigning%20Boston%20Colleges%20information%20security%20awareness%20pprogram%20based%20on%20curren%20research

Gragg, D. (2003). A multi-level defense against social engineering. SANS Institute. Zugriff unter https://www.sans.org/reading-room/whitepapers/engineering/multi-level-defense-social-engineering-920

Hadnagy, C. (2010). *Social Engineering : The Art of Human Hacking*. Indianapolis: Wiley.

Haeussinger, F. & Kranz, J. J. (2013). Information security Awareness: Its antecedents and mediating effects on security compliant behavior: Completed Research Paper: Thirty Fourth International Conference on Information Systems, Milan 2013. Georg-August-Universität,

Götttingen. Zugriff unter http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.669.8230&rep=rep1&type=pdf

Haumann, U. (2011). Bedrohungen / Sensibilisierungsmaßnahmen und deren Erfolgskontrolle: BSI IT - Grundschutztag. HypoVereinsbank.

Helisch, M. & Pokoyski, D. (Hrsg.). (2009). *Security Awareness – Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung*. Wiesbaden: Vieweg+Teubner.

Herold, R. (2010a). *Managing an Information Security and Privacy Awareness and Training Program* (2 Aufl.). Boca Raton: CRC Press.

Herold, R. (2010b). Why Information Security Training and Awareness Are important. *Information System Security*. Zugriff unter http://www.infosectoday.com/Articles/Security_Awareness_Training.htm

Hinson, G. (2013). Raising security awareness through marketing: Seven steps to promote your information security brand. Hastings. Zugriff unter http://www.noticebored.com/Raising_security_awareness_through_marketing.pdf

Holst, H. (2007). Mission Security. *Datenschutz und Datensicherheit - DuD*, *31*(7), 515–518.

Holst, H. (2008). Mission Security. *Datenschutz und Datensicherheit - DuD*, *32*(9), 579–582.

Houdeau, D. & Rose, O. (2015). Industrie 4.0 - Wie sichert man Produktionsketten gegen Wirtschaftsspionage ab? Forschungszentrum Cyber Defence - Universität der Bundeswehr München, München.

Hülsbömer, S. (2013). Der Cyber-Krieg hat gerade erst begonnen. *Computerwoche vom 05.03.2013*. Zugriff unter https://www.computerwoche.de/a/der-cyber-krieg-hat-gerade-erst-begonnen,2500941

HvS-Consulting AG. (2014). SaarLB IS-FOX Security Awareness Tools.

Information Security Forum. (2005). Systems Development.

Internet Identity. (2010). Phishing Trends Report. Internet Identity.

Islanders Bank. (2015). Cybersecurity Awareness. Zugriff unter http://www.islandersbank.com/wp-content/uploads/2015/10/IB-Cyber-Security-Awareness-Presentation.pdf

Jerakano. (2013). Getting the best from the ISF Standard of good practice. London. Zugriff unter http://www.jerakano.com/docs/247%20ISF%20SOGP%20Brochure%20for%20web.pdf

Kaltenböck, R. & Schuster, S. (2013). Awareness für Informationssicherheit und Datenschutz in der Sparkassen-Finanzgruppe. *Datenschutz und Datensicherheit - DuD*, *37*(5), 283–286.

Kaschow, R. (2014). Der Faktor Mensch im Mittelpunkt - Cyber Security Training. Cyber Akademie. Zugriff unter http://docplayer.org/637124-Der-faktor-mensch-im-mittelpunkt-cyber-security-training.html

Kaspersky. (2015). Kaspersky Security Intelligence Services. Cybersecurity training. Zugriff unter https://media.kaspersky.com/en/business-security/enterprise/Kaspersky_Security_Intelligence_Services_Cybersecurity_training.pdf

Kearney, P. (2010). *Security: The Human Factor*. IT Governance Publishing.

Khan, B., Alghathbar, K. S. & Khan, M. K. (2011). Information Security Awareness Campaign: An Alternate Approach. In T.-h. Kim, H. Adeli, R. J. Robles & M. Balitanas (Hrsg.), *Information Security and Assurance* (S. 1–10). Communications in Computer and Information Science. Berlin: Springer.

Khan, B., Alghathbar, K. S., Nabi, S. I. & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, *5*(26), 10862–10868.

Köhler, T. (2014). SECURITY AWARENESS: MICROSOFT JAGT DAS PHANTOM. Zugriff unter http://docplayer.org/6427169-Security-awareness-microsoft-jagt-das-phantom.html

KPMG India. (2014). Cybercrime survey report 2014. KPMG India. Zugriff unter https://assets.kpmg.com/content/dam/kpmg/pdf/2014/07/KPMG_Cyber_Crime_survey_report_2014.pdf

KPMG India. (2015). Cybercrime survey report 2015. KPMG India. Zugriff unter https://assets.kpmg.com/content/dam/kpmg/pdf/2016/03/Cyber-Crime-Survey-2015.pdf

Kraiger, K., Ford, J. K. & Salas, E. (1993). Application of Cognitive, Skill-Based, and Affective Theories of Learning Outcomes to New Methods of Training Evaluation. *Journal of Applied Psychology*, *78*(2), 311–328.

Lardschneider, M. (2007). Security Awareness — Grundlage aller Sicherheitsinvestitionen. *Datenschutz und Datensicherheit - DuD*, *31*(7), 492–497.

Lardschneider, M. (2008). Social Engineering. *Datenschutz und Datensicherheit - DuD*, *32*(9), 574–578.

Le, S., Weber, P. & Ebner, M. (2013). Game - Based Learning: Spielend Lernen? In M. Ebner & S. Schön (Hrsg.), *Lehrbuch für Lernen und Lehren mit Technologie* (S. 267–276). Berlin: epubli.

Littger, M., Brandl, S. & Böhme, K. (2014). DsiN Sicherheitsmonitor 2014 / Mittelstand – IT-Sicherheitslage 2014 in Deutschland. DsiN Sicherheitsmonitor Mittelstand.

Little, B. (2014). Small Business Security. Lewis University, Romeoville. Zugriff unter http://www.cs.lewisu.edu/mathcs/msisprojects/papers/SMBSecurity_BrianLittle.pdf

Long, J. & Mitnick, K. D. (2011). *No Tech Hacking : A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing: A guide to social engineering, dumpster diving, and shoulder surfing*. Oxford: Elsevier Science.

Maddock, V. (2010). *IT Induction and Information Security Awareness*. IT Governance Ltd.

Mahabi, V. (2010). *Information security awareness: system administrators and end-users perspectives at florida state university: Dissertation*. Zugriff unter http://diginole.lib.fsu.edu/islandora/object/fsu:181044/datastream/PDF/view

Mancuso, V. F., Strang, A. J., Funke, G. J. & Finomore, V. S. (2014). Human factors of cyber attacks a framework for human-centered research. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Bd. 58, S. 437–441).

Matzer, M. (2016). Drastischer Anstieg von Cyberangriffen auf kleine und mittlere Unternehmen. *VDI Nachrichten*.

McLaughlin, B. (2003). Creighton University: Information Security Philosophy. Creighton University. Zugriff unter https://www.creighton.edu/fileadmin/user/doit/docs/security/SEC_PHILv7.pdf

Milletary, J. (2005). Technical trends in phishing attacks. CERT and CERT Coordination Center und Carnegie Mellon University. Zugriff unter https://resources.sei.cmu.edu/asset_files/WhitePaper/2005_019_001_50315.pdf

Näckros, K. (2007). Learning Security through Computer Games: Studying user behavior in a real-world situation. In L. Futcher & R. Dodge (Hrsg.), *Fifth World Conference on Infor-*

mation Security Education (S. 95–103). IFIP — International Federation for Information Processing. doi:10.1007/978-0-387-73269-5{\textunderscore}13

Netzwerk Informationssicherheit im Mittelstand (NIM) des Bayerischen IT-Sicherheitscluster e.V. (2018). ISIS12 - InformationsSicherheitsmanagementSystem in 12 Schritten. Zugriff unter https://isis12.it-sicherheitscluster.de/

Nowak, G. (2010). The Information Security Forum (ISF) and Information secruity for external suppliers: a common baseline. Information Security Forum. Zugriff unter https://pdfs.semanticscholar.org/presentation/4bc2/aca315fc36b6b6bd10720c5f6be1e4aa5d08.pdf

Oracle Consulting. (2015). Oracle Consulting & advanced costumer support security practices.

Paget, F. (2007). Identity theft. *McAfee Avert Labs technical white paper No*, *1*.

Parsons, K., McCormac, A., Butavicius, M. & Ferguson, L. (2010). Human Factors and Information Security: Individual, Culture and Security Environment. Australian Government Department of Defence.

Pokoyski, D. (2008). Wer nicht „lehren" will, muss „fühlen" lassen. *Datenschutz und Datensicherheit - DuD*, *32*(9), 588–592.

Ponemon Institute. (2012). The Human Factor in Data Protection: Research Report. Zugriff unter https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/reports/rpt_trend-micro_ponemon-survey-2012.pdf

Popescu, M., Romero, M. & Usart, M. (2012). Using serious games in adult education serious business for serious people-the MetaVals game case study. In *The 7th International Conference on Virtual Learning* (S. 125–134). Bucureşti: Bucharest University Press. Zugriff unter https://www.researchgate.net/publication/272818460_Using_Serious_Games_in_adult_education_Serious_Business_for_Serious_People-the_MetaVals_game_case_study

Proofpoint. (2014). The Human Factor: How attacks exploit people as the weakest link in secruity: A Proofpoint White Paper. Proofpoint. Zugriff unter http://go.proofpoint.com/rs/proofpoint/images/Proofpoint-The-Human-Factor-v8.pdf

Proofpoint. (2015a). Proofpoint Threat Report. Sunnyvale. Zugriff unter https://www.proofpoint.com/sites/default/files/Proofpoint-Threat-Report-May2015.pdf

Proofpoint. (2015b). The Human Factor 2015: A Proofpoint Research Report. Zugriff unter https://www.proofpoint.com/sites/default/files/documents/bnt_download/pp-human-factor-2015_0.pdf

PWC. (2014). Defending yesterday Key findings from The Global State of Information Security Survey 2014. Zugriff unter https://www.pwc.com/gx/en/consulting-services/information-security-survey/pwc-gsiss-2014-key-findings-report.pdf

PWC. (2016). Turnaround and transformation in cybersecurity Key findings from The Global State of Information Security Survey 2016. Zugriff unter https://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf

Rogge, S. (2004). Der (Un)Sicherheit Faktor Mensch. Netzwerk Elektronischer Geschäftverkehr, Bamberg. Zugriff unter https://www.bayreuth.ihk.de/upload/3036906798_1708.pdf

RSA. (2011). Anatomy of an attack. Zugriff unter https://www.rsa.com/en-us/blog/2017-12/anatomy-of-an-attack-carbanak

Rumpel, R., Chrostowski, A., Greifzu, U., Hebestreit, F., Pakosch, P. & Rieger, H. (2011). Zertifizierung von Informationssicherheit in Unternehmen - ein Überblick. BITKOM, Berlin. Zugriff unter https://www.security-finder.ch/fileadmin/dateien/pdf/buecher/Zertifizierung_von_Informationssicherheit_in_Unternehmen.pdf

SANS. (2015). SANS Securing the Human - 2015 Security Awareness Report. SANS.

Schimmer, K. (2013). Ein Poster ist zu wenig! *Datenschutz und Datensicherheit - DuD*, *37*(5), 275–278.

Schlienger, T. & Teufel, S. (2005). Tool Supported Management of Information Security Culture. In Sasaki R., Qing S., Okamoto E., Yoshiura H. (Hrsg.), *Security and Privacy in the Age of Ubiquitous Computing. SEC 2005* (S. 65–77). IFIP Advances in Information and Communication Technology. Boston: Springer US.

Schneier, B. (2013). *Carry on: Sound advice from Schneier on security*. Heraklion: Wiley.

Sedova, M. (2013). Hot to Eat An Elephant: Transforming Security Awareness One Bite at a Time. Zugriff unter https://c.ymcdn.com/sites/www.issa.org/resource/resmgr/security_awarness_group/eatelephants_sedova.pdf

Shaw, E., Ruby, K. & Post, J. (1998). The insider threat to information systems: The psychology of the dangerous insider. *Security Awareness Bulletin*, (2-98), 1–10.

Soens, T. (2012). Mit Dr. Jekyll und Mr. Hyde zu mehr Sicherheit im Unternehmen: Erster deutscher Preis für IT-Sicherheit in KMU. CASED, Ismaning. Zugriff unter http://www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Redaktion/PDF/20121129-msg-services-ag,property=pdf,bereich=itsicherheit,sprache=de,rwb=true.pdf

Speed, T. J. (2012). *Asset protection through security awareness*. CRC Press.

Destatis: Mehr als 60 % der tätigen Personen arbeiten in kleinen und mittleren Unternehmen. (2016). Wiesbaden.

Symantec. (2013). Internet Security Threat Report 2013. Mountain View. Zugriff unter http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

Symantec. (2015a). Internet Security Threat Report. Mountain View.

Symantec. (2015b). Symantec Security Awareness Program.

Takemura, T. (2011). Statistical Analysis on Relation between Workers management Information Security Awareness and the Behaviors in Japan. *Journal of Management Policy and Practice*, *12*(3), 27–36.

Tan, T. C. C., Ruighaver, A. B. & Ahmad, A. (2010). Information Security Governance: When Compliance Becomes More Important than Security. In K. Rannenberg, V. Varadharajan & C. Weber (Hrsg.), *Security and Privacy – Silver Linings in the Cloud. SEC 2010* (S. 55–67). IFIP Advances in Information and Communication Technology. Berlin: Springer.

Tawileh, A., Hilton, J. & McIntosh, S. (2007). ISSE/SECURE 2007 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe/SECURE 2007 Conference. (Kap. Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach, S. 331–339). doi:10.1007/978-3-8348-9418-2_35

Toth, P. & Klein, P. (2014). A Role-Bases Model for Federal Information Technology / Cybersecurity Training. National Institut of Standards and Technology, Gaithersburg. Zugriff unter https://csrc.nist.gov/CSRC/media/Publications/sp/800-16/rev-1/draft/documents/sp800_16_rev1_3rd-draft.pdf

TrendLabs Research Team. (2012). Spear-Phishing Email: Most Favored APT Attack Bait. Cupertino. Zugriff unter https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf

Uffen, J. (2007). Wie begeistert man Mitarbeiter für IT-Sicherheit? Seminarunterlagen Sommersemester 2007. Hannover. Zugriff unter http://textarchive.ru/c-2885227-pall.html

Uffen, J., Kaemmerer, N. & Breitner, M. H. (2013). Personality Traits and Cognitive Determinants - an Empirical Investigation of the Use of Smartphone Security Measures. *Journal of Information Security*, *4*(4), 203–212.

Valli, C., Martinus, I. C. & Johnstone, M. N. (2014). Small to Medium Enterprise Cyber Security Awareness: an initial survey of Western Australian Business. In *Proceedings of the International Conference on Security and Management (SAM)* (S. 71–75). Las Vegas.

van Kessel, P. & Allan, K. (2015). Creating trust in the digital world: EY's Global Information Security Survey 2015. Ernest and Young. Zugriff unter http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf

van Niekerk, J. & von Solms, R. (2004). Corporate Information Security Education: Is Outcomes Based Education the Solution? In Y. Deswarte, F. Cuppens, S. Jajodia & L. Wang (Hrsg.), *Information Security Management, Education and Privacy: IFIP 18th World Computer Congress TC11 19th International Information Security Workshops 22–27 August 2004 Toulouse France* (S. 3–18). doi:10.1007/1-4020-8145-6{\textunderscore}1

Cyber-Security für kleine und mittlere Unternehmen (KMU): Anforderungen. (2015). Köln. Zugriff unter https://shop.vds.de/de/download/67b944842126c7b00c5031b16c44ae87/

Wagner, V. (2012). Risiko-Management in Großunternehmen: Die Herausforderung global vernetzter Infrastrukturen. Deutsche Telekom. Zugriff unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Fachkonferenz_Cyber-Sicherheit/2012_05_30_Fachkonferenz_BSI_Wagner.pdf%3F__blob%3DpublicationFile

Waidner, M. (2014). IT Security in "Industrie 4.0". TU Darmstadt & Fraunhofer Institute for Secure Information Technology, Darmstadt. Zugriff unter https://www.sit.informatik.tu-darmstadt.de/fileadmin/user_upload/Group_SIT/Presentations/140617c_Berlin_BMWi_Autonomik_IT_Security_cl.pdf

Wilson, M. & Hash, J. (2003). Building an Information Technology Security Awareness and Training Program. Gaithersburg.

Wipawayangkool, K. (2009). Exploring the Nature of Security Awareness: A Philosophical Perspective. *Issues in Information Systems*, *10*(2), 407–414.

Wolkerstorfer, P. (2014). IT-Security Awareness - Grundlagen und Lösungsansätze aus der Sicht der HCI-Forschung: PITS Public IT-Security, dbb forum berlin, 23.09.2014 - 24.09.2014. Austrain Institute of Technology.

Wood, P., Egan, G., Haley, K., Nisbet, M. & et al. (2012). Internet Security Threat Report 2011 Trends. Symantec, Mountain View. Zugriff unter http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf

Wood, P., Nahorney, B., Chandrasekar, K., Wallace, S. & Haley, K. (2014). Internet Security Threat Report 2014. Symantec, Mountain View. Zugriff unter http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

Zec, M. (2015). Cyber security Measures in SME's: a study of IT professionals' organizational cyber security awareness. Linnaeus University, Kalmar. Zugriff unter http://www.diva-portal.org/smash/get/diva2:849211/ATTACHMENT01.pdf

Zerr, K. (2007). Security-Awareness-Monitoring. *Datenschutz und Datensicherheit - DuD*, *31*(7), 519–523.

Ziegler, S. & Rocholl, P. (2012). Erfolge der IT-Security Awareness im Unternehmen messen? Pressemitteilung Profundis Labs GmbH und Co KG und Ziegler Marketing, München den 10.09.2012. München. Zugriff unter https://www.it-sa.de/Filestore.aspx/2012-09-10-PM_Messbarkeit_Awareness.pdf?fair=itsa&type=file&key=ef0b1b84-bd34-47c2-a8e0-72e438211cb6&language=de&filegroup=&filetype=file&indexfile=true

A. Kommentiertes Literaturverzeichnis

- Die Literaturrecherche wurde mit einer Suche nach Veröffentlichungen zum Thema Security Awareness mittels der Plattformen Springer.link und ProQuest Ebook Central begonnen.
- Anschließend wurde gezielt nach Jahresstatistiken über Cyber-Security und Informationssicherheit gesucht (KPMG, pwc, etc.)
- Dazu wurde eine allgemeine Google-Suche getätigt, um nach verschiedenen Bereichen zu suchen. Dabei wurde stets nur nach .pdf- Dateien gesucht, die offen zu Verfügung standen.
- Suchbegriffe waren dabei z. B.: „Cyber Security Awareness“, „Security Awareness“, „Security Awareness Kampagne“, „Cyber Security KMU“
- Bei der Recherche mit Google wurde zunächst versucht Informationen über den aktuellen Stand der Security Awareness in Unternehmen zu ermitteln, wobei sich hauptsächlich Beiträge von großen Unternehmen finden ließen.
- Es sollte bei der Recherche darauf geachtet werden, dass möglichst aktuelle Quellen (ab 2010) gefunden werden. Jedoch konnten für den eingeschränkten Zeitraum nicht genügen Quellen gefunden werden, sodass auch Quellen mit einem Erscheinungsjahr von 2005 und später einbezogen wurden.
- Kampagnen verschiedener Unternehmen um Security Awareness zu stärken wurden dabei ebenfalls gesucht.
- Dabei wurde auch nach Standards und Richtlinien für den Bereich Security Awareness gesucht, auch speziell für KMU.
- Als letztes wurden noch Theorien zur Steigerung der Security Awareness recherchiert.
- Abschließend wurd die gefundene Literatur kategorisiert und kommentiert.

A.1. State of the Art – Große Unternehmen

1. **Security Awareness – Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung; Michael Helisch; 2009**

   Buch welches ein breites Spektrum über den Begriff Security Awareness und Methoden für Programme, welche Sec. Aw. stärken sollen, umfasst.

   Helisch und Pokoyski, 2009, S. 65

2. **Oracle Consulting & advanced costumer support security practices; Oracle; 2015**

   Oracle Sicherheitspraktiken, Abschnitt Employee Training

   Oracle Consulting, 2015

3. **Adobe Security Training; Adobe Systems Incorporated; 2014**

   Adobe Systems – Security Training. WhitePaper zu Adobes Security Training Je nach Arbeitsbereich soll eine andere Stufe erreicht werden. Angestellte können ihren Fortschritt über ein Webinterface mitverfolgen. Mitarbeiter müssen ein jährliches Security Awareness Training absolvieren. Ebenso finden regelmäßige Seminare mit Experten statt. Dazu werden Mitarbeiter ermutigt auch an Security Meet-ups und Konferenzen teilzu nehmen, wobei sie von Adobe finanziell gefördert werden. Des weiteren finden „Hackfests“ statt, in denen Mitarbeiter in die Rolle des Angreifers schlüpfen und versuchen einen hack auszuführen.

   Adobe Systems Incorporated, 2014

4. **Awareness für Informationssicherheit und Datenschutz in der Sparkassen-Finanzgruppe; Robert Kaltenboeck und Sabine Schuster; 2013**

   In der Sparkassenfinanzgruppe wird eher generalisiert vorgegangen, somit wird ein Programm für alle Sparkassenfilialen erstellt. Die Idee basiert auf der Sensibilisierung durch Bilder, wie z. B. Poster.

   Kaltenböck und Schuster, 2013

5. **Information Security Awareness; Marcus Beyer und Sarah Ahmed; 2012**

   Hewlett-Packard(Schweiz): Präsentation zur Herangehensweise an das Security Awareness bei HP. Inkl. Bildbeispiele.

   Beyer und Ahmed, 2012

6. **Kaspersky Security Intelligence Services. Cybersecurity training; Kaspersky; 2015**

   Cybersecurity Trainingskampagne 2015 von Kaspersky.

   Kaspersky, 2015

7. **Security Awareness: Microsoft jagt das Phantom; Tom Köhler; 2014**

   Security Awareness Kampagne bei Microsoft mit Schwerpunkt Social Engineering (Phantom Jagd)

   Köhler, 2014

8. **SaarLB IS-FOX Security Awareness Tools; HvS-Consulting AG; 2014**

   Erfahrungsbericht von SaarLB über die IS-FOX Tools

   HvS-Consulting AG, 2014

9. **Security Awareness @ T-Systems; Dr.Christoph Schog Ivett Buzgo und Dietmar Pokoyski; 2013**

   Programm bei T-Systems – Security Parcours, umfassende Präsentation zur Entstehung des Programms. Gruppenweise werden hier an Stationen Miniplanspiele durchlaufen.

   Buzgo et al., 2013

10. **Ein Poster ist zu wenig!; Klaus Schimmer; 2013**

    Entwicklung eines Security Awareness Programms bei SAP. (Vom Poster zur Kampagne)

    Schimmer, 2013

11. **Risiko-Management in Großunternehmen; Volker Wagner; 2012**

    Risiko-Management in Großunternehmen

    Wagner, 2012

12. **Security Awareness – Grundlage aller Sicherheitsinvestitionen; Michael Lardschneider; 2007**

    Erfahrungsbericht der Security Awareness Kampagne der Münchener Rück. Vielfältige Vermarktung von Security Awareness, angepasst an die jeweilige Zielgruppe. Programm auch mit Leuten aus dem Bereich Marketing erstellt.

    Lardschneider, 2007

13. **CSI:DB – Die IT Security-Awareness-Kampagne der Deutschen Bahn; Andreas Exter und Matthias Drodt; 2013**

    Bericht über die Security Awareness Kampagne der Deutschen Bahn, CSI:DB. „Nebenbei sollte das Thema ‚IT-Sicherheit' entstaubt werden." Lernen durch positive/negative Beispiele. Kampagne enthielt Tipps und Hinweise, welche auch für den privaten Umgang mit IT interessant waren. „Web 2.0", Mitarbeiter sollten nicht nur konsumieren, sondern auch selber Beiträge schreiben, welche von anderen Teilnehmern gelesen werden konnten, um aus weiteren Erfahrungen zu lernen.

    Exter und Drodt, 2013

14. **Mission Security; Heinrich Holst; 2007**

    T-Systems Awareness Kampagne. Fiktiver Kollege „James Bit" als Vorbild. Image von Informationssicherheit sollte umgekrempelt werden. Mit der Kampagne sollte auch dem Kunden vermittelt werden, dass Informationsschutz bei T-Systems einen hohen Stellenwert hat. Kampagne richtete sich an Mitarbeiter auf der ganzen Welt, worauf bei der Planung geachtet werden musste. Mitarbeiter wurden aufgerufen Verbesserungsvorschläge zu machen, von denen die besten mit einem Preis gekrönt wurden.

    Holst, 2007

15. **Mission Security; Heinrich Holst; 2008**

    Weiterführung der Mission Security, mit „James Bit". Privater Nutzen sollte für Mitarbeiter herausgestellt werden. Kampagne gut auf KMU übertragbar, da geringe Kosten anfallen, durch die Nutzung von kostengünstigen Kommunikationsmedien, wie z. B. Intranet und E-Mail.

    Holst, 2008

16. **IT-Security Governance und Awareness im RWE-Konzern; Dr. Joachim Cramer; 2009**

RWE über IT-Sicherheits-Führung und Awareness. Irrtum und Nachlässigkeit der Mitarbeiter bilden einen der wichtigsten Gefahrenbereiche, in dem auch am meisten Schaden aufkommt. Mangelndes Bewusstsein ist ein großes Hindernis für die Informationssicherheit. Eine Security-Awareness-Kampagne richtet sich an den Umgang mit Information im dienstlichen und privaten Umfeld. Es werden viele unterschiedliche Medien genutzt, um eine große Bandbreite von Themen zu vermitteln. Diese sind mit unterschiedlich hohem Awareness-Effekt und Kosten verbunden.

Cramer, 2009, S. 16

17. **Die Initiative – Resümee und Ausblick; Bundesakademie für öffentliche Verwaltung im Bundesministerium des Inneren; 2011**

    Security-Programm bzw. Hilfestellung zur Umsetzung eines Security-Programms der Bundesverwaltung. Allgemeine Definition des Programms mit individueller Umsetzung je nach Verwaltungsstelle. Enthält Erfahrungsberichte aus den Veranstaltungen. „Bereits bei der Definition der Ziele einer Sensibilisierungskampagne muss deren Evaluation vorbereitet werden.“ [Kapitel 10 Seite 20] Verschiedene Arten der Evaluation, teils auch in Kombination.

    Bundesakademie für öffentliche Verwaltung im Bundesministerium des Inneren, 2011

A.2. State of the Art – KMU

1. **Cyber security Measures in SMEs: a study of IT professionals' organizational cyber security awareness; Milos Zec; 2015**

    Masterarbeit zu Cyber-Sicherheitsmaßnahmen in KMU. Im Speziellen geht es um Cyber-Security-Awareness. Die Analyse basiert auf Interviews mit IT-Fachleuten aus Unternehmen in der Slowakei.

    Zec, 2015

2. **Cybersecurity Awareness; Islanders Bank; 2015**

    Präsentation der Islanders Bank über Cyber-Security-Awareness. Auflistung von Trends im Bereich Cyber-Crime und Beispiele für Gegenmaßnahmen.

    Islanders Bank, 2015

3. **Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen; Erkki Liikanen; 2003**

    Definition von KMU.

    Europäische Union, 2003

4. **The Impact of Cyber Security on SMEs; Nabila Amrin; 2014**

    Masterarbeit über die Wirkung von Cyber-Security auf KMU. Cyber-Crime wird mit der steigenden Abhängigkeit von Informationstechnologien und dem Internet zu einer zunehmenden Bedrohung für KMU. Präventive Maßnahmen werden in KMU vernachlässigt.

Mittels einer Studie wurden unterschiedliche europäische Unternehmen (KMU) hinsichtlich präventiver Maßnahmen, Trends etc. befragt. Der Einsatz von Policies bzw. Richtlinien für Informationssicherheit ist in KMU nicht besonders verbreitet.

Im Allgemeinen sind sich KMU nicht aller möglichen Risiken im Bereich des Cyber-Crime bewusst. Etwaige Zwischenfälle werden nicht transparent unter KMU kommuniziert, da beispielsweise ein Reputationsschaden entstehen könnte.

Detaillierte Beschreibung möglicher Bedrohungen. Auch am Beispiel der Studie bzw. am Thema „Bring Your Own Device“ (BYOD).

Amrin, 2014, Kapitel 2.5

5. **DsiN Sicherheitsmonitor 2014 / Mittelstand – IT-Sicherheitslage 2014 in Deutschland; Dr. Michael Littger, Stefan Brandl und Katrin Böhme; 2014**

   Studie zur Sicherheitslage in kleinen und mittleren Unternehmen. Grundlage hierfür ist der „DsiN-Sicherheitscheck“.

   Grundsätzlich nimmt die Verbreitung der Informationstechnologie weiter zu. Notwendige Sicherheitsmaßnahmen können hierbei jedoch nicht immer Schritt halten.

   Sicherheitsmaßnahmen werden grundsätzlich als wichtig empfunden – werden jedoch nicht konsequent genug umgesetzt. Es ergibt sich ein großer Handlungsbedarf, der sowohl technische als auch nicht-technische Maßnahmen umfasst.

   Die Veröffentlichung zeigt Handlungsfelder auf und nennt Beispiele zur Steigerung des IT-Sicherheitsbewusstseins.

   Littger et al., 2014

6. **Industrie 4.0 – Wie sichert man Produktionsketten gegen Wirtschaftsspionage ab?; Dr. Detlef Houdeau und Prof. Dr. Oliver Rose; 2015**

   Prognosen für großes Wachstum von bzw. durch Industrie 4.0. Für bevorstehende Entwicklungen mangelt es bisher an Standards. Die Realisierbarkeit ist vor allem für große Unternehmen gegeben. Für KMU ist die Realisierbarkeit bisher unklar.

   Aufgrund der zunehmenden Vernetzung, die gleichzeitig Grundlage für die Konzepte der Industrie 4.0 ist, weisen Firmen und deren IT-Systeme eine erhöhte Verwundbarkeit auf.

   Schäden, die sich aus Angriffen, so z. B. Industriespionage über das Internet, ergeben, werden auf jährlich 50–100 Mrd. EUR (in Deutschland) geschätzt. KMU benötigen sehr lange, um einen erfolgreichen Angriff vollständig als solchen zu erkennen und ggf. zu reagieren. Grund hierfür könnte u. a. der verhältnismäßig geringe Anteil an Stammpersonal in diesen Unternehmen sein.

   Houdeau und Rose, 2015

7. **IS027001 in KMU effizient umsetzen; CIS Certification and Information Security Services GmbH; 2009**

   Nachweise für Informationssicherheit werden häufiger von Kunden gefordert und können beispielsweise über eine Zertifizierung nach ISO/IEC 27001 erbracht werden. Die ISO/IEC

27001 kann sowohl für große Unternehmen als auch KMU angewandt werden. Der Handlungsbedarf wird über eine Risikoanalyse ermittelt. Drei Fallbeispiele beschreiben die Zertifizierung und daran geknüpfte Erfahrungen in KMU.

CIS - Certification & Information Security Service, 2009

8. **Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach; Anas Tawileh, Jeremy Hilton and Stephen McIntosh; 2007**

   KMU machen einen großen Teil der globalen Wirtschaftsaktivität aus. Aufgrund der Eigenschaften und Besonderheiten von KMU können Ansätze für das Management von Informationssicherheit, die ursprünglich für große Unternehmen entwickelt wurden, nicht einfach auf KMU angewandt werden. Die Autoren beschreiben Herausforderungen, die sich bei der Umsetzung von Ansätzen für das Management von Informationssicherheit in KMU ergeben. Mittels eines holistischen Ansatzes, der auf der Soft Systems Methodology basiert, soll die Entwicklung eines Systems zum Management der Informationssicherheit (Informationssicherheitsmanagementsystems (ISMS)) erleichtert werden.

   Beispiele für Herausforderungen für KMU: knappes Budget, begrenzte Anzahl an Arbeitskräften und eine ständig wechselnde Geschäftsumgebung [S. 9]. Rahmenbedingungen und Ziele müssen für die Implementierung eines Informationssicherheitsmanagementsystems definiert werden.

   Tawileh, Hilton und McIntosh, 2007, S. 5

9. **Small Business Security; Brian Little; 2014**

   Einfach umzusetzende bzw. anzuwendende Einführung zur Gewährleistung von Informationssicherheit in KMU. Die Tipps benötigen kein großes technisches Vorwissen. Die Themen sind aufgeteilt in: Passwörter, Benutzung von Internet und E-Mails, Computer-, Daten- und Netzwerksicherheit.

   Little, 2014

10. **Small to Medium Enterprise Cyber Security Awareness: an initial survey of Western Australian Business; Craig Valli, Ian Martinus und Mike Johnstone; 2014**

    Auch in Australien machen KMUs einen großen Teil der gesamten Wirtschaftsaktivität aus. Berichte und Studien zu Sicherheits-Bedrohungen gegen Unternehmen, die z. B. in erfolgreichen Hacker-Angriffen resultieren, fokussieren in der Regel nicht auf KMU. Die Veröffentlichung beschreibt eine initiale Umfrage in KMU und die Ergebnisse, die sich aus Maßnahmen zur Steigerung der Informationssicherheit in KMU ergeben haben. Den meisten KMUs fehlt alleine schon das nötige Wissen zur Umsetzung von Informationssicherheit. Dies umfasst auch die Basics: Einrichtung einer Firewall, Anti-Virus-Software etc.

    Der Großteil der KMUs glaubt beispielsweise, dass sie kein Ziel für Cyberangriffe wären bzw. dass keine Daten, welche für Angreifer interessant wären, existieren.

    Valli, Martinus und Johnstone, 2014

11. **Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen; Bundesamt für Sicherheit in der Informationstechnik; 2011**

    Sehr große Abhängigkeit des Erfolgs der deutschen Wirtschaft von KMUs. Aufgrund der großen Abhängigkeit, auch beispielsweise des öffentlichen Sektors, ist es besonders wichtig, dass die Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität in KMU gewährleistet werden. Die Studie dient der Ermittlung des Ist-Zustands der IT-Sicherheit- und des Krisenmanagements in KMU. Handlungsempfehlungen und aufgezeigtes Verbesserungspotenzial dienen den teilnehmenden Unternehmen als zukünftige Unterstützung.

    „Das Bewusstsein für Themen der IT-Sicherheit ist in deutschen KMU vorhanden." [S. 9] Deutsche KMU sind größtenteils gut im Bereich der IT-Sicherheit ausgestattet, doch fehlt oft ein durch das Unternehmen aufeinander abgestimmtes Sicherheitsmanagement. Ebenso werden Anpassungen eher durch „trial and error" durchgeführt und weniger durch ein festgelegtes Konzept.

    Bundesamt für Sicherheit in der Informationstechnik und secunet Security Networks, 2011

A.3. State of the Art – Wissenschaft / Forschung

1. **An Improvised Software Security Awareness Model; C. Banerjee, Arpita Banerjee und P.D. Murarka; 2013**

   Improvisiertes Software Awareness Modell, psychologische Behandlung involvierter Personen vor Insider-Angriffen. Software Security Awareness Modell eingebunden in den Software Development Life Cycle

   Banerjee et al., 2013

2. **Carry On : Sound Advice from Schneier on Security; Bruce Schneier; 2013**

   Bruce Schneier, Kapitel 3: „Human Aspekts of Security".

   Schneier, 2013, Kapitel 3

3. **2013 Data Privacy, Information Security and Cyber Insurance Trends; James Crowther und weitere; 2013**

   Kommentare von Personen aus der IT-Sicherheits-Branche (Schneier, Herold)

   Crowther et al., 2013

4. **IT Induction and Information Security Awareness; Valerie Maddock; 2010**

   IT-Einweisung im Verbund mit Security Awareness + Feldstudie

   Maddock, 2010

5. **A Role-Bases Model for Federal Information Technology / Cybersecurity Training; Patricia Toth und Penny Klein; 2014**

   NIST Entwurf für ein Trainingsprogramm zur Verbesserung der Security Awareness, für Bundesbehörden und Organisationen (Rolenbasiertes Training).

   Toth und Klein, 2014

6. **Managing an Information Security and Privacy Awareness and Training Programm; Rebecca Herold; 2010**

   Buch von Rebecca Herold, welches, alle Bereiche abdeckend, Informationen zum erstellen eines Security Awareness Training Programms beinhaltet.

   Herold, 2010a

7. **Asset protection through security awareness; Tyler Justin Speed; 2012**

   Bietet Informationen über Security Awareness ohne nötiges Vorwissen im Bereich IT. Betrachtet werden verschiedene Themen mit je einen kurzen Überblick, wie man in diesem Bereich Sicherheit gewährleisten kann.

   Speed, 2012

8. **Security: The Human Factor; Paul Kearney; 2010**

   Menschen machen Fehler, doch selten absichtlich. Der Faktor Mensch soll mit in die Planung der Sicherheit mit ein berechnet werden.

   Kearney, 2010

9. **Human Factors and Information Security: Individual, Culture and Security Environment; Kathryn Parsons, Agata McCormac, Marcus Butavicius und Lael Ferguson; 2010**

   Befasst Faktoren, die das Handeln eines Menschen im Umgang mit Informationssicherheit beeinflussen und gibt Beispiele diese zu mindern.

   Parsons, McCormac, Butavicius und Ferguson, 2010

10. **Die Lage der IT-Sicherheit in Deutschland 2015; Bundesamt für Sicherheit in der Informationstechnik; 2015**

    Stand der Informationssicherheit in Deutschland. Beschrieben wird die Gefährdungslage durch Ursachen, Rahmenbedingungen und Angriffsmethoden, mit Erklärungen, Bewertungen und Fallbeispielen.

    Bundesamt für Sicherheit in der Informationstechnik, 2015

11. **How to eat an elephant; Masha Sedova; 2013**

    Präsentation von Salesforce.com über die Umsetzung von „Gamification“ im Bereich Security (Vollständige Präsentation auch als Video auf YouTube zu finden www.youtube.com/watch?v=avNXQ2TiH0I)

    Sedova, 2013

12. **Getting the best from the ISF Standard of good practice; Jeranko; 2013**

    Broschüre von Jerakano zur Umsetzung des ISF Standards

    Jerakano, 2013

13. **A Bit of Psychology to Improve your Security Awareness Program; Ahmed Abdel-Aziz; 2010**

    Verbesserung von Security Awareness Programmen durch Anwendung psychologischer Ansätze. Verstehen, warum ein Mensch in einer bestimmten Situation Handelt und wie man ihn dazu bringen kann optimal zu agieren.

    Abdel-Aziz, 2010

14. **Mit Dr.Jekyll und Mr.Hyde zu mehr Sicherheit im Unternehmen; Cased; 2012**

    Erster deutscher Preis für IT-Sicherheit in KMU. Spielerisch das Thema IT-Sicherheit vermitteln. Sehr regelmäßige Schulungen, Newsletter etc.

    Soens, 2012

15. **Corporate information security education; Johan van Niekerk und Rossouw von Solms; 2006**

    Erläuterung von „Outcome Based Education“ und ob es für Informationssicherheit geeignet ist.

    van Niekerk und von Solms, 2004

16. **Cyber Security Awareness Campaigns: Why do they fail to change behaviour?; Jason Nurse; 2015**

    Essentielle Bestandteile von Awareness Campagnen und welche Bestandteile sie zum Erfolg oder Scheitern bringen.

    Bada, Sasse und Nurse, 2015

17. **Awareness für IT-Sicherheit und Datenschutz in der Hochschulausbildung– Eine empirische Untersuchung; Simone Dimler, Hannes Federrath, Thomas Nowey und Klaus Plößl; 2006**

    Grundbildung im Bereich IT-Sicherheit und Datenschutz kommt in bereits in der Hochschulausbildung zu kurz. Security Awareness bereits in der Hochschule vermitteln Dimler, Federrath und Nowey, 2006

18. **FAA Secure Application Development and SDLC; Terry Fletscher; 2011**

    Mehr Schwachstellen in Applikationen als im Betriebssystem. Schritte zur Ausbesserung dieser Schwachstellen im Life-cycle einer Applikation

    Fletscher, 2011

19. **Friend or foe? Information security management of employees; Eirik Albrechtsen; 2008**

    Trainiert und Gelernt wird am besten in einem Diskurs. Meiste Programme beinhalten meist weniger Interaktion zwischen Angestelltem und Lehrendem. Beteiligung der Angestellten soll verstärkt werden.

    Albrechtsen, 2008

20. **Information Security Awareness Campaign: An Alternate Approach; Bilal Khan, Khaled S. Alghathbar und Muhammad Khurram Kahn; 2011**

    Gesundheits- und Umweltbewusstseins Strategien für Security Awareness Programme nutzen

    B. Khan, Alghathbar und Khan, 2011

21. **Information security awareness: system administrators and end-users perspectives at florida state university; Victoria Mahabi; 2010**

    Nutzer brauchen „Awareness Education“ um fähig zu sein sich gegen Sicherheitsangriffe schützen zu können

    Mahabi, 2010, S. 9

22. **Awareness 3.0; Dirk Fox; 2013**

    DuD – Früher Web Based Trainings, bei denen die Wirkung kaum messbar waren. Erste Security Awareness Kampagnen legten Schwächen des Sicherheitsmanagement bloß. Begeisterung ist eine zentrale Voraussetzung für menschliches Lernen.

    Fox, 2013

23. **Der Faktor Mensch im Mittelpunkt – Cyber Security Training; Ralf Kaschow; 2014**

    Alle möglichen Bereiche stehen unter der Gefahr von Cyber-Angriffen. Technik ist ein wichtiger Faktor in der Cyber Security, hat aber seine Grenzen. „Der Faktor Mensch: potenzielle Sicherheitslücke und „-Enabler“ (das schwächste und das stärkste Glied der Kette)“ [S. 11]. Anforderungen der für Führungskräfte/Manager, Experten und Mitarbeiter getrennt aufgelistet, unterschiedliche Anforderungen. „Ein Mindest-Wissen und Sensibilität bei allen Beteiligten ist der erste Schritt für mehr Sicherheit “ [S. 18]

    Kaschow, 2014

24. **Information Security Governance: When Compliance Becomes More Important than Security; Terence C. C. Tan, Anthonie B. Ruighaver und Atif Ahmad; 2010**

    Sicherheitsstrategie nicht immer auf allen Ebenen klar und einheitlich. Unternehmensweite sicherheits Führung notwendig.

    Tan, Ruighaver und Ahmad, 2010

25. **Information security Awareness: Its antecedents and mediating effects on security compliant behavior; Felix Häussinger und Johann Kranz; 2013**

    Wissen/Erfahrung über Informationssicherheit beeinflusst das Bewusstsein direkt. Information Security Awareness kann gut auf negative Erfahrungen aufbauen. Enthält Grafik über die verschiedenen Einflüsse auf ISA und was es bewirkt

    Haeussinger und Kranz, 2013, S. 6

26. **Personality Traits and Cognitive Determinants-an Empirical Investigation of the Use of Smartphone Security Measures; Jörg Uffen, Nico Kämmerer und Michael H. Breitner; 2013**

    Einflüsse von Persönlichkeitsmerkmalen und Vorwissen auf Informationssicherheit.

    Uffen, Kaemmerer und Breitner, 2013

27. **Learning Security through Computer Games: Studying user behavior in a real-world situation; Kjell Näckros; 2007**

    Studie über das erlernen von besserem Sicherheitsverhalten durch Computerspiele. Computerspiele hatten positiven Einfluss, jedoch 12 Personen getestet und mit einer bereits vorherigen Studie ebenfalls mit 12 Personen verglichen

    Näckros, 2007

28. **Exploring the Nature of Security Awareness: A Philosophical Perspective; Kamphol Wipawayangkool; 2009**

    Philosophischer Ansatz an Security Awareness durch Herausstellung der Grundeigenschaften von S.A und einer eigenen Konzeption von S.A.

    Wipawayangkool, 2009

29. **Der Faktor Mensch – human factors; Aircademy; 2015**

    Die meisten Flugunfälle ruhen auf menschlichem Versagen. Faktoren für Fehlverhalten: Selbstüberschätzung und mangelnde Selbstkritik

    Aircademy, o.D.

30. **Human factors of cyber attacks a framework for human-centered research; Vincent F. Mancuso, Adam J. Strang, Gregory J. Funke und Victor S. Finomore; 2014**

    Faktor Mensch meist außer acht gelassen in Frameworks zu Cyber Attacks. Vorgestellt wird ein Ansatz mit dem Menschen im Mittelpunkt.

    Mancuso, Strang, Funke und Finomore, 2014

31. **Systems Development; Information Security Forum; 2005**

    Faktor Mensch in der Informationssicherheit muss aus verschiedenen Sichten Betrachtet werden, Psychologe, Philosophen, Soziologen, Cyber-Security Forscher, etc.

    Corona, 2009

32. Sicherheit bereits in der Entwicklung ins Produkt ein bauen. S.A Richtlinien/Regeln für Mitarbeiter in der Entwicklung

    Information Security Forum, 2005, section SD2.2 S.8

33. **Information Security Philosophy; Bryan McLaughlin; 2002**

    Informationssicherheits Philosophie der Creighton University

    McLaughlin, 2003

34. **Wie begeistert man Mitarbeiter für IT-Sicherheit?; Jörg Uffen; 2007**

    Größte Gefahr geht vom Nutzer aus. Analyse der Motivation eines Mitarbeiters zu fahrlässigem Verhalten (Anreizsystem)[S. 15]. Mitarbeiter sollen in verschiedene Menschenbilder unterteilt werden und den Bildern entsprechende Anreize zugeordnet werden.

    Uffen, 2007

35. **Resdesigning Boston Colleges information security awareness program based on current research; Julie Gillis und David Millar; 2014**

    Kritik an SETA. Zu theoretisch, zu allgemein und weckt kein Interesse beim Nutzer. Lösungsvorschlag, den Nutzer bei der Entwicklung von SETA für das Unternehmen(Hier College) mit ein zu beziehen, mit anschließender Umfrage zu dem Programm.

    Gillis und Millar, 2014

36. **IT-Security Awareness - Grundlagen und Lösungsansätze aus der Sicht der HCI-Forschung; Peter Wolkerstorfer; 2014** Endbenutzer in Entwicklung inkludieren, Eigenschaften des Menschen nutzen, Mentale Modelle „human centric design“

    Wolkerstorfer, 2014

37. **Why Information Security Trainingand Awareness Are Important; Rebecca Herold; 2010** Es gibt immer mehr Gesetzte und Regulationen, die eine Form von Awareness Training voraussetzen (in den USA). Zusätzlich steigen die Fälle, in denen gegen diese Regulationen verstoßen wird oder nicht ausreichend nachgegangen wird, wofür Geld- und andere Strafen dafür verhängt werden. Es werden Punkte genannt, die ein der Regulationen genügendes Programm beinhalten sollte. Ebenso Punkte, welche die Kunden und Konsumenten des Unternehmens adressieren, wobei auf Transparenz geachtet werden sollte, in der Hinsicht, dass der Kunde weiß, und teilweise auch wie, mit ihren vertraulichen Daten umgegangen wird und wie ihr Schutz gewährt wird.

    Herold, 2010b

A.4. Methoden zum erstellen von Security Awareness Programmen

1. **Building an Information Security Awareness Program : Defending Against Social Engineering and Technical Threats; Bill Gardner und Valerie Thomas; 2014**

    Buch, welches als Anleitung genommen werden kann, um ein Security Awareness Programm von Grund auf aufbauen zu können.

    Gardner und Thomas, 2014

2. **Building an Information Technology Security Awareness and Training Program; Mark Wilson und Joan Hash; 2003**

    NIST Publikation, stellt einen Leitfaden für ein effektives Informationssicherheitsprogramm dar.

    Wilson und Hash, 2003

3. **Wer nicht „lehren“ will, muss „fühlen“ lassen; Dietmar Pokoyski; 2008**

   Kampagnen müssen Interesse für das Thema wecken.„Mehr von Sicherheit verstehen und diese „anders“ sehen.“ [S. 589] „Awareness 2.0 führt und bewegt die Menschen und könnte die Chance ergreifen, Enabler einer neuen Unternehmenskultur zu werden“ [S. 592]

   Pokoyski, 2008

A.5. Security Awareness Programme

1. **Datenblatt Security Awareness Kampagnen; CBT Training & Consulting GmbH; 2012**

   CBT Training und Consulting GmbH, Anbieter des IS-FOX, einer Security Awareness Kampagne mit einem modularen Angebot. Es können nur einzelne Bausteine erworben werden oder eine ganze Kampagne. Auflistung verschiedener Methoden zum Sensibilisieren der Mitarbeiter.

   CBT Training & Consulting, 2012

2. **Best Practices for Implementing a Security Awareness Program; Security Awareness Program Special Interest Group PCI Security Standards Council; 2014**

   Sammlung an Trainingsmethoden und Leitfaden für ein Security Awareness Programm.

   Awareness Program Special Interest Group PCI Security Standards Council, 2014

3. **A study on strengthening security awareness programs based on an RFID access control system for inside information leakage prevention; Kyong-Ho Choi und DongHwi Lee; 2013**

   Hier erläutertes Security Awareness Program, besteht aus 3 Phasen (On/Off line Security Training, Zugangskontrolle, Intensives Training bei Sicherheitsverstoß) in Phase 2 wird mit Radio Frequenz Identifikation die Zugangsberechtigung überprüft und anhand dessen Personen für Phase 3 ausgesucht.

   Choi und Lee, 2013

4. **Raising security awareness through marketing; Dr Gary Hinson PhD MBA CISSP; 2013**

   Marketing-Strategien benutzen um Security Awareness zu verstärken, dem Angestellten Security Awareness verkaufen.„Security awareness, like information security as a whole, is a team sport.“ [S. 6] Manage, measure and improve [Step 7.]

   Hinson, 2013

5. **Symantec Security Awareness Program; Symantec; 2015**

   Symantec Security Awareness Programm, fahrlässige Mitarbeiter sind die häufigste Ursache für Datenpannen

   Symantec, 2015b

6. **Security Awareness Mittelstand; CBT Training & Consulting GmbH; 2014**

   IS-Fox Security Awareness Mittelstandspaket 2014

   CBT Training & Consulting, 2014

7. **Cyber Security Training and Awareness Through Game Play; Benjamin D. Cone, Michael F. Thompson, Cynthia E. Irvine und Thuy D. Nguyen; 2006**

   Vorstellung von des Videospiels „CyberCIEGE“ als Methode Security Awareness zu stärken, für ein weites Zielgruppenspektrum.

   Cone et al., 2006

8. **Bedrohungen / Sensibilisierungsmaßnahmen und deren Erfolgskontrolle**

   Sensibilisierung der Mitarbeiter muss regelmäßig stattfinden In KMU, setzen uninformierte/Naive Angestellte ihre Firma einem Risiko aus (vgl. S. 69). Awareness Programm soll Angestellte zu einem positiven sicherem Handeln erziehen.

   Haumann, 2011

9. **Social Engineering; Michael Lardschneider; 2008**

   Ein geplanter, von der Führung des Unternehmens eingeleiteter, Social Engineering Angriff zur Sensibilisierung der Mitarbeiter gegen über Social Engineering.

   Lardschneider, 2008

10. **Using Phishing for User Email Security Awareness; Ronald C. Dodge und Aaron J. Ferguson; 2006**

    Phishing-Angriff zur Analyse der Bereitschaft Phishing-E-Mails zu öffnen und zur Steigerung der Aufmerksamkeit für Angriffe auf sensible Informationen.

    Dodge und Ferguson, 2006

A.6. Angriffs-Methoden,Schwachstellen und Gefahren

1. **Stop phishing attacks; Deloitte; 2014**

   Deloitte – Artikel speziell zum Thema Phishing

   Deloitte, 2014

2. **Experten identifizieren Angriffs-Methode; Johannes Boie und Benedikt Strunz; 2015**

   Angriff auf den Bundestag durch Spearphishing.

   Boie und Strunz, 2015

3. **No Tech Hacking : A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing; Johnny Long und Kevin D. Mitnick; 2011**

   No-Tech-Hacking. Mögliche Arten von Angriffen auf Unternehmen, die keinen hohen technischen Aufwand haben, z.B Sozialengineering, Dumpster diving und Shoulder surfing.

   Long und Mitnick, 2011

4. **Social Engineering : The Art of Human Hacking; Christopher Hadnagy; 2010**

   Socialengineering, beschreibt die Methoden und Vorgänge beim Socialengineering und bietet Tipps um Socialengineering vorzubeugen.

   Hadnagy, 2010

5. **Anatomy of an attack; RSA; 2011**

   Zusammenfassung eines APTs auf RSA mit detaillierter Beschreibung der Umsetzung von APTs.

   RSA, 2011

6. **Unintentional Insider Threats: Social Engineering; CERT Insider Threat Team; 2014**

   Einflüsse von Social Engineering, welcher Insider zum unabsichtlichen in Gefahr bringen von Sensiblen Daten führt

   CERT Insider Threat Team, 2014

7. **Der (Un)Sicherheit Faktor Mensch; Stephan Rogge; 2004**

   Mehr professionalisierte Cyber-Angriffe auf Unternehmen. Komplexere Angriffe Hülsbömer, 2013

8. Gefahrenquelle Mensch

   Rogge, 2004

9. **Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing E-Mails; Marcus Butavicius, Kathryn Parsons, Malcom Pattinson und Agata McCormac; 2015**

   Studie über verschiedene Arten von Phishing und wie man die Ergebnisse für Trainings oder Lehrprogramme nutzen kann.

   Butavicius, Parsons, Pattinson und McCormac, 2015

10. **Gefährliche E-Mails; Sabrina Berkenkopf und Ralf Benzmüller; 2011**

    Bericht über Spam, mit verschiedenen Maschen der Angreifer. Am Ende werden noch Tipps für den Umgang mit Spam gegeben.

    Berkenkopf und Benzmüller, 2011

11. **Technical trends in phishing attacks; Jason Milletary und CERT Coordination Center; 2005**

    Phishing - Vielfalt und Technik in Phishing Angriffen, dazu sind die Mittel fürs Phishing relativ einfach zu beschaffen.

    Milletary, 2005

12. **Identity theft; Francois Paget; 2007**

    Identity Theft, Tipps für Individuen und Unternehmen.

    Paget, 2007, S. 13

13. **Report on Phishing; Binational Working Group on Cross Border Mass Marketing Fraud; 2006**

    Phishing – Tipps für den Umgang mit Phishing und wie man möglichst verhindern kann davon Betroffen zu werden.

    Binational Working Group on Cross Border Mass Marketing Fraud, 2006

14. **A multi-level defense against social engineering; David Gragg; 2003**

    Multi-level defense against social engineering. „Employees must be willing to question the caller and withhold information when it looks like things don't add up" [S. 11] Angestellten muss klar werden, was einen Wert für das Unternehmen hat und lernen, wie man Social Engineering angriffe erkennt, z.B. an der Art der Fragen. „key points" die jeder Nutzer sich merken sollte: „Know what has value", „Friends are not always friends", „Passwords are personal" and „Uniforms are cheap" [S. 12]

    Gragg, 2003

15. **The insider threat to information systems: The psychology of the dangerous insider; Eric Shaw, Keven Ruby und Jerrold Post; 1998**

    Insider stellen große Gefahr fürs Unternehmen dar, besonders diejenigen, welche das nötige IT-Können haben. Viele Beispiele zu dem Thema Insiderthreats

    Shaw, Ruby und Post, 1998

16. **Sicherer Umgang mit USB-Speichersticks; ENISA - Agentur der Europäischen Union für Netz- und Informationssicherheit; 2008**

    USB-Sticks als mögliche Gefahr. Stellt potenzielle Risiken mit dem unbedachten Gebrauch von USB-Stick dar.

    ENISA, 2008

17. **Spear-Phishing E-Mail: Most Favored APT Attack Bait; Trend Micro; 2012**

    spear-phishing weiterhin eine große Bedrohung und beliebtes mittel um sich Zugang für einen APT zu beschaffen.

    TrendLabs Research Team, 2012

A.7. Umfragen und Statistiken

1. **Cybercrime survey report 2015; KPMG India; 2015**

   KPMG India, Cybercrime Survey Report 2015.

   KPMG India, 2015

2. **Cybercrime survey report 2014; KPMG India; 2014**

   KPMG India, Cybercrime Survey Report 2014.

   KPMG India, 2014

3. **Defending yesterday Key findings from The Global State of Information Security® Survey 2014; PWC; 2014**

   pwc,Global State of Information Security Survey 2014.

   PWC, 2014

4. **Turnaround and transformation in cybersecurity Key findings from The Global State of Information Security® Survey 2016; PWC; 2016**

   pwc,Global State of Information Security Survey 2015.

   PWC, 2016

5. **Under cyber attack EY's Global Information Security Survey 2013; Ernest and Young; 2013**

   Ernest and Young Global Information Security Survey 2013. Statistik zum Stand der Cyber Security in Unternehmen, mit Theorien zur Verbesserung

   Ernest und Young, 2013

6. **Creating trust in the digital world EY's Global Information Security Survey 2015; Paul van Kessel und Ken Allan; 2015**

   Ernest and Young G.I.S.S 2015. Wie sich die Welt für Unternehmen ändert und wie sie sich anpassen können. Größte Bedrohungen: Phishing und Malware.

   van Kessel und Allan, 2015

7. **State of Cybersecurity: Implications for 2015; Cybersecurity Nexus; 2015**

   ISACA, Statistik. Listet Gefahren und Bedrohungen auf und beinhaltet Statistiken über das Thema IT-Security im Unternehmen

   Cybersecurity Nexus, 2015

8. **Drastischer Anstieg von Cyberangriffen auf kleine und mittlere Unternehmen; Michael Matzer; 2016**

   Starke Zunahme von Angriffen auf das produzierende Gewerbe und KMU.

   Matzer, 2016

9. **Research Report : The Human Factor; Proofpoint; 2015**

   proofpoint Statistik über den Faktor Mensch in der Informationssicherheit („Who is clicking? Where are people clicking on?... ").

   Proofpoint, 2015b

10. **Mehr als 60 % der tätigen Personen arbeiten in kleinen und mittleren Unternehmen; Statistisches Bundesamt; 2016**

    60% der tätigen Personen arbeiten in KMU.

    Statistisches Bundesamt, 2016

11. **Internet Security Threat Report; Symantec; 2015**

Symantec Internet Security Theat Report

Symantec, 2015a

12. **The Human Factor in Data Protection; Ponemon Institute; 2012**

Studie über das Verhalten von Angestellten, welche Gefahren für die Informationssicherheit darstellen und was Unternehmen dagegen unternehmen.

Ponemon Institute, 2012

13. **SANS Securing the Human – 2015 Security Awareness Report; SANS; 2015**

Weitere Statistik über Security Awareness, hier wird nach Unternehmensbereichen unterschieden und auch nach Mitarbeiteranzahlen, jedoch ist die kleinste Gruppe mit 1000 und weniger Mitarbeitern betitelt.

SANS, 2015

14. **Global Phishing Survey: Trends and Domain Name USe in 1H2014; Greg Aaron, Rod Rasmussen und Aaron Rout; 2014**

APWG Global Phishing Report 1H2014, Trends in Domainnamen für Phishing.

Aaron, Rasmussen und Routt, 2014

15. **Global Phishing Survey 2H2014 Trends and Domain Name Use; Greg Aaron und Rod Rasmussen; 2014**

APWG Global Phishing Report 2H2014

Aaron und Rasmussen, 2014

16. **Phishing Activity Trends Report 2nd Quarter 2014; Greg Aaron und Ronnie Manning; 2014**

APWG Phishing Activity Trends Report 2q2014, USA weiterhin Top-Hoster für Phishingseiten, neue Online-Bezahl-Services werden regelmäßiger als Ziel genommen.

Aaron und Manning, 2014

17. **Internet Security Threat Report 2011 Trends; Paul Wood, Gerry Egan, Kevin Haley, Mathew Nisbet und weitere; 2012**

Symantec, Internet Security Threat Report 2011 Trends. Nette Grafik über Ereignisse in 2011 je Monat, ebenso als Fazit eine Liste von Richtlinien für Unternehmen und Nutzer.

Wood, Egan, Haley, Nisbet und et al, 2012

18. **Internet Security Threat Report 2013; Symantec; 2013**

Symantec, Internet Security Threat Report 2013. „Small Businesses Are the Path of Least Resistance for Attackers“ [S. 4], „Think Before You Click“ [S. 52]

Symantec, 2013

19. **Internet Security Threat Report 2014; Paul Wood, Ben Nahorney, Kavitha Chandrasekar, Scott Wallace und Kevin Haley; 2014**

    Symantec, Internet Security Threat Report 2014. „Small businesses and consumers are most at risk from losing data“ [S. 6] , gezielte Angriffe gegen kleine Unternehmen machten den Großteil gezielten Spear-Phishing Angriffe aus.[S. 18],„In 2012, Symantec's Norton Report showed that 44 percent of adults were unaware that security solutions existed for mobile devices, highlighting the lack of awareness of the mobile danger.“ [S. 69]

    Wood et al., 2014

20. **Phishing Trends Report; Internet Identity; 2010**

    Phishing – KMU erleiden kaum erholbaren Schaden durch Angriffe während laufender Online-Banking Sitzung

    Internet Identity, 2010

21. **The Human Factor How attacks exploit people as the weakest link in secruity; Proofpoint; 2014**

    proofpoint Statistiken und Zusammenfassung zum Faktor Mensch in Informationssicherheit 2014.

    Proofpoint, 2014

22. **Proofpoint Threat Report; Proofpoint; 2015**

    Verweis auf andere proofpoint papers, Zusammenfassung von Cyber-Threat-News und kleine Information über Spam.

    Proofpoint, 2015a

23. **Statistical Analysis on Relation between Workers management Information Security Awareness and the Behaviors in Japan; Toshihiko Takemura; 2011**

    Ergebnisse einer Web-Based-Survey über den Zusammenhang von Informationssicherheitsbewusstsein von Mitarbeitern und ihrem Verhalten.

    Takemura, 2011

24. **The risk of social engineering on information security: a survey of IT professionals; Dimensional Research; 2011**

    Die Gefahr ausgehend von Social Engineering - eine Studie. Neue Mitarbeiter stellen größtes Risiko gegenüber Social Engineering dar.

    Dimensional Research, 2011

A.8. Methoden zum Evaluieren von Trainings-Methoden

1. **Application of Cognitive, Skill-Based, and Affective Theories of Learning Outcomes to New Methods of Training Evaluation; Kurt Kraiger, Kevin J. Ford und Eduardo Salas; 1993**

    Konzepte zum Evaluieren von Trainings-Methoden (Psychology)

Kraiger, Ford und Salas, 1993

2. **Effectiveness of information security awareness methods based on psychological theories; Bilal Khan, Khaled S. Alghathbar, Syed Irfan Nabi und Muhammad Khurram Khan; 2011**

   Analysiert verschiedene Security Awareness Tool auf ihre Effektivität aus psychologischer Sicht, dazu wird beschrieben, wie man Security Awareness misst.

   B. Khan, Alghathbar, Nabi und Khan, 2011

3. **Security-Awareness-Monitoring; Konrad Zerr; 2007**

   Wiederholungsmessungen um Veränderungen des Sicherheitsbewusstseins zu identifizieren. Mögliche Optimierungsmaßnahmen können aus den Messungen herausgestellt werden.

   Zerr, 2007

4. **Tool Supported Management of Information Security Culture; Thomas Schlienger und Stephanie Teufel; 2005**

   Informationssicherheit soll ein natürlicher Aspekt täglicher Aktivitäten werden. [S. 65] „Decision Support System“ zum Analysieren und entwickeln von Vorschlägen zur Verbesserung der Sicherheitskultur. Mit Anwendungsbeispiel in einer Schweizer Privat Bank.

   Schlienger und Teufel, 2005

A.9. Gesetzesgrundlagen und Standards

1. **Act to Strengthen the Security of Federal Information Technology; Bundesamt für Sicherheit in der Informationstechnik; 2009**

   Definitionen und Aufgaben des BSI

   Bundesamt für Sicherheit in der Informationstechnik, 2009

2. **The Information Security Forum (ISF) and Information security for external suppliers: a common baseline; Gregory Nowak, 2010**

   Zulieferer benötigen einen gemeinsamen Standard. ISF als Informations- und Hilfsstelle.

   Nowak, 2010

3. **Leitfaden Informationssicherheit — IT-Gundschutz kompakt; Bundesamt für Sicherheit in der Informationstechnik; 2012**

   Leitfaden Informationssicherheit, BSI. Fallbeispiel, wo es zu Schaden durch einen „Innentäter“ kam, wo ein Mitarbeiter, der von dem Unternehmen weg wechselte, Industriespionage betrieb und geheime Informationen an sein neues Unternehmen weitergab [S. 23]. Faktor Mensch — Kapitel, in dem Punkte aufgelistet wurden, welche von Unternehmen beachtet werden sollten, um das Risiko von den eigenen Mitarbeitern ausgehend zu senken. Dabei wird Wert darauf gelegt, dass die Mitarbeiter ein ausreichendes Grundverständnis über die Sicherheitsrichtlinien besitzen und regelmäßige Schulungen für diese erhalten.

Ebenso sollten Sanktionen ausgearbeitet werden, die bei einem Verstoß der Richtlinien eintreten, welche angemessen des Verstoßes sein sollten. Dazu sollte Rat von Experten eingezogen werden, wenn das Problem dem eigenen Maß überschreiten [ch. 7.4]. Zertifizierungsmöglichkeiten werden ebenfalls genannt, wobei dabei eher eine allgemeine Sicherheit mit angesprochen wird und eine Zertifizierung in Richtung Security Awareness speziell nicht direkt erwähnt wird [ch. 9].

Bundesamt für Sicherheit in der Informationstechnik - BSI, 2012

4. **IT Security in „Industrie 4.0“; Prof. Dr. Michael Waidner; 2014**

   keine einheitlichen Standards, fehlende Kooperation zwischen Instituten.

   Waidner, 2014

5. **Zertifizierung von Informationssicherheit in Unternehmen - ein Überblick; Prof. Dr. Rainer Rumpel, Arnd Chrostowski, Ulf Greifzu, Frank Hebestreit, Peter Pakosch und Holger Rieger; 2011**

   Möglichkeit des Nachweises von Informationssicherheit durch Zertifizierung. Wachsende Abhängigkeit von Informations- und Kommunikationstechnologie. Auflistung wichtiger Standards, Gründe für eine Zertifizierung, Tipps, Aufwand und Fallstudien.

   Rumpel et al., 2011

A.10. Institutionen zur Förderung der Sensibilisierung

1. **Die ENISA-Plattform für die Zusammenarbeit bei der Sensibilisierung; ENISA; 2009**

   ENISA-Plattform für die Zusammenarbeit bei der Sensibilisierung

   ENISA, 2009

IMPRESSUM

Informationen zur Publikationsreihe:
Berichte zu HSD-intern geförderten Forschungsprojekten
https://www.hs-duesseldorf.de/forschung/Seiten/publikationen.aspx

Herausgeber
Hochschule Düsseldorf
Der Vizepräsident für Forschung und Transfer
Münsterstr. 156
40476 Düsseldorf

Redaktion und Ansprechpartnerinnen
Dr. Rebekka Loschen, Stabstelle Forschung und Transfer
Stefanie Söhnitz, Hochschulbibliothek

Titelblattgestaltung: Katharina Regulski, Hochschulbibliothek

Zitationsvorschlag:
Schmidt, Holger; Gondolf, Jeremy, Haufs-Brusberg, Peter (2018): Studie zur Information Security Awareness in kleinen und mittleren Unternehmen (KMU). Düsseldorf: Hochschule Düsseldorf (Berichte zu HSD-intern geförderten Forschungsprojekten, Nr. 1).
Verfügbar unter: https://nbn-resolving.org/urn:nbn:de:hbz:due62-opus-11880
DOI: 10.20385/2625-3690/2018.1

ISSN: 2625-3690