UNIVERSITÄT DUISBURG ESSEN
Offen im Denken
WIRTSCHAFTS- & ORGANISATIONS-PSYCHOLOGIE
Komplexität und Lernen
Newsletter für Organisationales Lernen, Simulation und Training
Ausgabe 30 | März 2014

Komplexität & Lernen

Ausgabe 30 | März 2014

Editorial zur 30. Ausgabe

Liebe Leserin, Lieber Leser,
wir alle haben uns in den letzten Wochen und Monaten bestimmt bei verschiedenen Meldungen zu Daten-Le(a)cks, "gehackten" Daten von Online-Spiele-Anbietern oder bei Meldungen, dass Staaten die Überwachung von Mailverkehr oder Video-Chats nutzen, um für Sicherheit zu sorgen, gefragt, welche unserer Mails, Chats, SMS da so mitgelesen wurden, wer welches Passwort von uns schon besitzt oder wer gerade mit unserer Kreditkarte bezahlt.
Wir sind beim Thema IT-Sicherheit dabei gefühlt die Opfer, aber weniger "Täter/in". Zumindest keine absichtlichen Täter/innen.
Die in diesem Newsletter vorgestellten Projekte zeigen jedoch auf, dass wir selbst auch zu "Täter/innen" werden können, ohne das wir eine "böse" Absicht haben. Häufig ist es einfach Unwissen, vielleicht aber auch eine gewisse Unbekümmertheit, weil wir nicht davon ausgehen, dass "uns" das passiert oder dass sich jemand für unsere Daten auf dem Rechner interessieren würde.
In diesem Newsletter stellen wir Ihnen mehrere Möglichkeiten vor, Mitarbeiter/innen für das Thema "Security Awareness" zu sensibilisieren: Mit einem webbasierten Trainingstools für Praktikanten/innen, einer sprachlichen Überarbeitung der Geheimhaltungsvereinbarung und Leitfäden zur Unterweisung, die Sebastian Brandhorst vorstellt, sowie einem Fragebogen, der das Sicherheitsbewußtsein von Mitarbeiter/innen erfassen und rückmelden kann, den Lena Koldner vorstellt.

Das Lesen dieses Newsletters ist dabei frei von unerwünschten IT-Nebeneffekten, aber man weiss ja nie wer mitliest....
Haben Sie einen schönen Frühling,

Annette Kluge & das ganze Wips-Team

Abbildung 1. Die Elbe bei Magdeburg (wo der Workshop Kognitive Systeme diesmal stattfand), im März 2014.

Zum Inhalt

Herausgeberin: Prof. Dr. Annette Kluge & Team, Fachbereich Wirtschafts- und Organisationspsychologie, Fakultät für Ingenieurwissenschaften, Fachbereich Informatik und Angewandte Kognitionswissenschaft & OPSY - HSG

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken
WIRTSCHAFTS- & ORGANISATIONS-psychologie
Komplexität und Lernen
Newsletter für Organisationales Lernen, Simulation und Training
Ausgabe 30 | März 2014

Aus der Lehre

Information Security Awareness: Entwicklung, Evaluation und Implementierung von Methoden und Tools

Von Sebastian Brandhorst

Worum geht es? Informationen haben im betrieblichen Kontext eine Schlüsselfunktion, da der Unternehmenserfolg letzten Endes stets auf einem Informationsvorsprung begründet ist (Picot, Reichwald & Wigand, 2001). Schützenswert sind Informationen allerdings nicht nur als Produktionsfaktor, sondern auch aufgrund gesetzlicher Vorgaben, wie dem Bundesdatenschutzgesetz (Gola, Peter, Schomerus et al., 2005). In diesem Kontext sollen hier alle Informationen, welche ein Schadenspotential bei ungewolltem Bekanntwerden außerhalb unternehmerischer Grenzen besitzen, als **sensible Daten** bezeichnet werden.
Eine Form der rechtlichen Absicherung gegen ungewollte Weitergabe sensibler Daten stellen sogenannte **Geheimhaltungsvereinbarungen (GHVs)** dar. In diesen Verträgen werden Inhalte, Geltungsbereich und –dauer sowie Konsequenzen bei Vertragsbruch festgehalten.
Die juristische Fachsprache unterscheidet sich jedoch sehr von der Alltagssprache (Busse, 1994), was dazu führt und erklärt, dass Geheimhaltungsvereinbarungen nicht zur *Vorbeugung* ungewollter Datenweitergabe geeignet sind. Einen Ansatz zur Vorbeugung liefert nun das Themengebiet der sogenannten *Information Security Awareness*. Diese damit gemeinte Achtsamkeit gegenüber der Informationssicherheit beschreibt den Umstand bzw das Ausmaß, in dem Personen die Vorgaben und Richtlinien zum Umgang mit sensiblen Daten kennen und sich auch dementsprechend verhalten (Siponen, 2000).

Was kann man machen? Das Forschungsprojekt des Fachgebiets Wirtschaftspsychologie (Wintersemester 2013/14) hat sich unter der Leitung von Prof. Dr. Annette Kluge und Dr. Vera Hagemann mit der Thematik der *Information Security Awareness* befasst. Studierende haben unter dem Titel „Entwicklung von Maßnahmen zur Sensibilisierung von MitarbeiterInnen im Rahmen Know-How kritischer Projekte“ ein halbes Jahr gemeinsam für und mit einem Unternehmen in der IT Branche gearbeitet, mit dem Ziel PraktikantInnen und MitarbeiterInnen auf die Bedeutsamkeit sensibler Daten zielgruppengerecht aufmerksam zu machen, Kenntnisse zu vermitteln und den Umgang mit sensiblen Daten zu üben.

Abbildung 2. Auch im Büro lauern "Gefahren".
http://tk.eversjung.de/www/downloads/Presse_ Situation_Buero_2.JPG

Wie macht man das? Zu Beginn analysierten die Studierenden das Unternehmen hinsichtlich des tatsächlichen Bedarfs und des aktuellen Stands. Leitfragen wie *„Wie ist der momentane Umgang mit sensiblen Daten?“, „Wie ist der Kenntnisstand bezüglich der GHV?“, „Was gehört zu den sensiblen Daten dieses Unternehmens?“* wurde in Interviews mit den MitarbeiterInnen und durch Fragebogenunterstützung nachgegangen. Ausgehend von dem so ermittelten Ist-Zustand formulierten die Studierenden gewünschte Soll-Zustände.
Die Analyse ergab, dass zwar eine sehr positive Einstellung gegenüber dem Wahren von Geheimnissen, also dem Umgang mit sensiblen Daten besteht, jedoch kein einheitliches Verständnis darüber herrscht, was eigentlich genau sensible Daten im eigenen Unternehmen sind. Unter anderem ist dies auf die GHVs zurückzuführen, von denen nicht nur eine Vielzahl unterschiedlicher Versionen existiert, sondern diese auch keine inhaltliche Auskunft darüber geben, was als vertraulich einzustufen ist, und was nicht.
Auch berichteten die BetreuerInnen von PraktikantInnen von individuell unterschiedliche Vorgehensweisen bei der Unterweisung in die GHV. Besonders deutlich stellte sich heraus, dass das Thema der Verschwiegenheit als sehr bedeutsam angesehen wurde, jedoch nur in geringer Weise im Arbeitsalltag kontinuierlich kommuniziert wurde. Der Bedarf und Wunsch nach mehr Klarheit, Verständlichkeit und Struktur in Hinblick auf den Umgang mit sensiblen Daten wurde somit sehr stark geäussert.

Aufbauend auf den Ergebnissen der Analyse wurde eine Vielzahl an Maßnahmen entwickelt, um die erkannten

Defizite zu reduzieren und vorhandene Stärken zu unterstützen.

Kategorisierung sensibler Daten: Zur Vereinheitlichung des Verständnisses von sensiblen Daten wurden diese von den Studierenden identifiziert und in einer grafisch aufgearbeiteten Kategorisierung auf einem Poster sowie für weitere Unterlagen visualisiert (Abbildung 3).

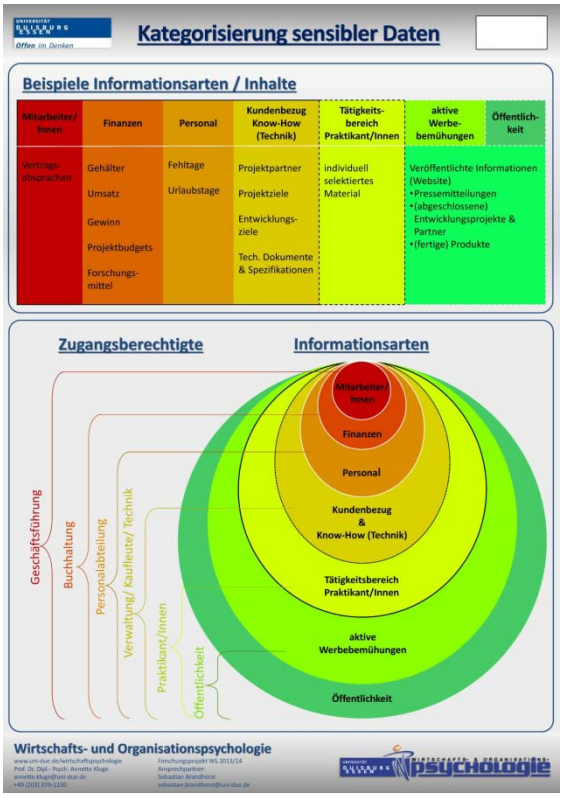


Abbildung 3. Poster zur Kategorisierung sensibler Daten.

Vereinheitlichung der GHV: Da es für unterschiedliche Zwecke unterschiedliche GHVs gab, wurden diese vereinheitlicht und (in den Grenzen der juristischen Sprache) vereinfacht.

Handbuch zur GHV: Es wurde ein umfangreiches Handbuch mit Erklärungen, Frequently Asked Questions (FAQs) und Handlungsempfehlungen zu allen Paragraphen der GHV erstellt.

MitarbeiterInnen-Training: Für eine jährliche Auffrischung des Wissens und einer konstanten Sensibilisierung steht nun ein online-basierter Selbstcheck zur Verfügung.

Leitfaden zur GHV-Unterweisung: Alle neuen MitarbeiterInnen und PraktikantInnen können mit Hilfe von neu entwickelten Leitfäden nun zukünftig von den jeweils Verantwortlichen im Unternehmen standardisiert und umfassend in das Thema eingeführt werden.

PraktikantInnen-Training (Trainingstool): Alle neuen PraktikantInnen erhalten vor Beginn ihres Praktikums eine webbasierte zielgruppenorientierte Einführung bezüglich sensibler Informationen und der dazugehörigen Kategorisierung.

Wurden die Ziele erreicht? Im Anschluss an die Erarbeitung der Materialien wurden diese in mehreren Evaluationsstudien auf ihre Wirksamkeit hin geprüft.

Die Wirksamkeitsprüfung (Evaluation)

Die Evaluation des Trainingstools für PraktikantInnen wurde mit 65 Personen durchgeführt. Dabei zeigte sich eine deutliche Zunahme der Kenntnisse über Inhalte der GHV. Sogar vorherige Unterschiede in den Vorbildungsniveaus konnten ausgeglichen werden.
Das Handbuch zur GHV wurde im Test mit 14 Personen als besonders verständlich und nützlich für die Bewältigung unsicherer Situationen bewertet und stieß auf eine hohe Akzeptanz für den Einsatz im Arbeitsalltag.
Zudem wurden 60 Personen in drei unterschiedlichen Bedingungen (alte GHV, neue GHV und neue GHV mit Handbuch) die alte oder neue GHV vorgelegt. Personen, denen die überarbeitete GHV gemeinsam mit dem Handbuch ausgegeben wurde, erreichten einen höheren Wissenstand als Personen mit der alten GHV.
Somit konnte vor Einführung der erarbeiteten Materialien deren Nützlichkeit, Wirksamkeit und Akzeptanz seitens der Anwendenden methodisch/systematisch untersucht und gezeigt werden.

Und dann? Im Anschluss an die Abschlusspräsentation vor Ort im Unternehmen, im Februar diesen Jahres, wurden alle Materialien der Geschäftsführung übergeben. Die Ergebnisse wurden mit großer Wertschätzung aufgenommen und werden nun in den betrieblichen Alltag einfließen. Somit kann durch die Arbeit der Studierenden im Zuge des Projekts dazu beigetragen werden, dass die Information Security Awareness im Unternehmen unterstützt und gefördert wird.
Doch nicht nur das Unternehmen hat von diesem Projekt profitieren können. Den Studierenden bot sich die Gelegenheit während des Studiums in einen „lebenden" Betrieb nicht nur reinzuschauen, sondern gestaltend einzuwirken. Gelernte Konzepte und Theorien mussten in die Praxis umgesetzt werden. Dabei stand weniger im

Vordergrund „Was“ gemacht werden muss, sondern die Herausforderung lag in dem „Wie“.

zitierte Literatur

Busse, D. (1994). Verständlichkeit von Gesetzestexten: Ein Problem der Formulierungstechnik. In *Gesetzgebung heute*, *2*, 29-48.

Gola, P., Schomerus, R., & Klug, C. (2005). *BDSG: Bundesdatenschutzgesetz : Kommentar*. München: Beck.

Picot, A., Reichwald, R., & Wigand, R. T. (2007). Die grenzenlose Unternehmung. Information, Organisation und Management. In *Das Summa Summarum des Management* (pp. 35-47). Gabler.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31-41.

Aus der Forschung für die Praxis

Der Faktor Mensch in der Datensicherheit – Kann man Sicherheitsbewusstsein messen?

von Lena Koldner

Im Zeitalter der Digitalisierung gelten Wissen, Know-how und Informationen als wichtigste strategische Schlüsselressourcen für unternehmerischen Erfolg und Wettbewerbsfähigkeit. Folglich sollte ein Unternehmen hohen Wert auf den Schutz dieser Ressourcen legen und potenziellen Gefahren entgegenwirken. Die Enthüllungen der NSA-Affäre im Jahr 2013, sowie die jüngste Warnung des Bundesamtes für Sicherheit in der Informationstechnik (BSI), dass rund 16 Millionen Zugangsdaten in Form von E-Mail Adressen und Passwörtern in die Hände von Kriminellen geraten sind, verdeutlichen die Sicherheitsrisiken, die die Fortschritte in der Informations- und Kommunikationstechnologie mit sich bringen. Die Erkenntnis, dass in vielen Fällen die eigenen MitarbeiterInnen für Sicherheitsverletzungen im Unternehmen verantwortlich sind, führt zu einem erhöhten Bedarf an Sicherheitslösungen nicht nur auf technischer, sondern vor allem auf personeller Ebene.

Zu diesen Lösungen zählt unter anderem die **Erhöhung des Sicherheitsbewusstseins der MitarbeiterInnen durch Security Awareness Kampagnen**. Solche Maßnahmen werden mittlerweile in den meisten größeren Unternehmen umgesetzt. In Deutschland mangelt es bisher jedoch an geeigneten Instrumenten mit denen das Sicherheitsbewusstsein von MitarbeiterInnen erfasst werden kann, um gezielte Maßnahmen ergreifen zu können und Erfolge von Awareness Kampagnen messbar zu machen.

Abbildung 4. Auch mal die Bürotür zumachen.
http://tk.eversjung.de/www/downloads/Presse _Situation_Buero_1.JPG

Was ist Sicherheitsbewusstsein?

Der Schutz sensibler Daten und Informationen, der im deutschsprachigen Raum als Informationssicherheit bezeichnet wird, entspricht im Englischen dem Ausdruck „information security“. In der englischen Literatur ist daher auch häufig die Bezeichnung „Information Security Awareness“ zu finden. In deutschen Unternehmen und in der Forschung haben sich die Begriffe Security Awareness bzw. Sicherheitsbewusstsein durchgesetzt. Darunter wird das **Wissen und die Einstellung in Bezug auf den Schutz sensibler Daten** verstanden (Rantos, Fysarakis & Manifavas, 2012). Zerr (2007) beschreibt Security Awareness als die gedankliche Auseinandersetzung der MitarbeiterInnen mit den Risiken, die sich im Umgang mit eingesetzten Arbeitsmitteln und Technologien ergeben können.

Wie kann Sicherheitsbewusstsein gemessen werden?

Neben der reinen Beobachtung und Erfassung von sicherheitsrelevantem Verhalten, wie z.B. die Wahl geeigneter Passwörter oder das Absolvieren von Sicherheitstrainings, wurden in den letzten Jahren vor allem **sozialpsychologische Theorien zur Erklärung und Erfassung des Sicherheitsbewusstseins** herangezogen. Für die Entwicklung eines geeigneten Instruments wurden in der hier präsentierten Arbeit daher Fragen englischsprachiger Instrumente analysiert, übersetzt und auf Grundlage der Arbeit von Yoon und Kim (2013) in vorhandene Theorien eingebettet. Der daraus entwickelte Fragebogen wurde im Rahmen einer

empirischen Studie eingesetzt, um die angenommenen Zusammenhänge der in Abbildung 5 aufgeführten Variablen zu untersuchen.

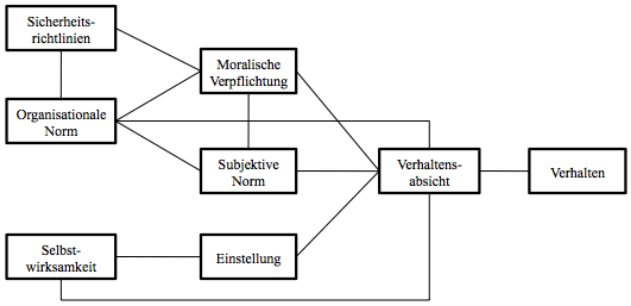


Abbildung 5. Modell zur Erklärung und Erfassung von Sicherheitsverhalten (Koldner, 2014).

Die Entwicklung des Fragebogens

Auf Grundlage der Auseinandersetzung mit verschiedenen Ansätzen zur Messung des Sicherheitsbewusstseins und bereits bestehender Instrumente (Koldner, 2014) wurden acht Unterskalen zu Aspekten des Sicherheitsbewusstseins und eine zusätzliche Skala mit Wissensfragen zum Thema Computersicherheit abgeleitet.
Insgesamt umfasst der Fragebogen 21 Items die in 15-20 Minuten zu bearbeiten sind.

Die Items basieren auf den Arbeiten von Yoon und Kim (2013), PentaSafe (2002) und Egeler et al. (2006). Die Items wurden aus dem Englischen übersetzt, auf Basis von Regeln zur Itemkonstruktion zum Teil umformuliert und anschließend den folgenden Dimensionen zugeordnet:

- *Sicherheitsrichtlinien*,
- *Organisationale Norm,*
- *Moralische Verpflichtung,*
- *Subjektive Norm,*
- *Selbstwirksamkeit,*
- *Einstellung,*
- *Verhaltensabsicht,*
- *Verhalten* und
- *Wissen*

Bis auf ein Item der Skala Selbstwirksamkeit und drei Items der Skala Wissen werden alle Items über eine 5-Stufige Likert-Skala von „stimme gar nicht zu“ bis „stimme voll zu“ "gerated".

Abbildung 6. USB-Sticks als Sicherheitsrisiko.

Die Subskala **Sicherheitsrichtlinien** beschäftigt sich mit den organisationalen Rahmenbedingungen, die durch Sicherheitsrichtlinien geschaffen werden. Dabei wird die Einstellung der MitarbeiterInnen zu den Sicherheits-richtlinien und deren Umsetzung erfragt. Beispielitem: "Ich kenne die Konsequenzen einer Nichteinhaltung der Sicherheitsrichtlinien meines Unternehmens".

Mit der Subskala **Organisationale Norm** soll die von einem Individuum wahrgenommene Einstellung anderer Personen im Unternehmen bezüglich der Sicherheits-technologien und -richtlinien erhoben werden. So soll beispielsweise eingeschätzt werden, ob die KollegInnen denken, dass man Sicherheitstechnologien nutzen sollte. Beispielitem: "Die meisten Personen in meinem Unternehmen denken, dass man die Sicherheits-vorschriften befolgen sollte".

In der Skala **Moralische Verpflichtung** soll erfasst werden, inwieweit eine moralische Verpflichtung der MitarbeiterInnen gegenüber den Sicherheitsrichtlinien besteht, indem z.B. gefragt wird, inwiefern eine Verletzung der Sicherheitsrichtlinien gegen die eigenen Prinzipien verstößt. Beispielitem: "Die Sicherheitsrichtlinien zu verletzen, verstößt gegen meine Prinzipien".

Der Einfluss von wichtigen Bezugspersonen auf das Sicherheitsbewusstsein wird in der Subskala **Subjektive Norm** operationalisiert. Es wird z.B. gefragt, inwiefern die Bezugspersonen die aktive Nutzung von Sicherheits-technologien befürworten würden. Beispielitem: "Die meisten Menschen die mir wichtig sind, würden es befürworten, wenn ich aktiv Sicherheitstechnologien benutzen würde".

Die Subskala **Selbstwirksamkeit** soll die wahrgenommene Fähigkeit der MitarbeiterInnen, mit den Herausforderungen der Computersicherheit umzugehen, erfassen. Die TeilnehmerInnen werden unter anderem gebeten einzuschätzen, inwieweit sie in der Lage sind, die Informationen auf ihrem Computer vor anderen Personen zu schützen. Beispielitem: "Ich bin davon überzeugt, dass ich eine Verletzung der Sicherheitsrichtlinien erkennen würde, wenn ich sie sehen würde".

Die Subskala **Einstellung** fragt verschiedene Meinungen zu Sicherheitsgefährdungen und –maßnahmen ab, wie z.B. die Frage danach, inwiefern der Verlust persönlicher Informationen ein ernstzunehmendes Problem darstellt oder inwiefern Präventivmaßnahmen ein effektives Mittel zum Schutz sensibler Daten sind. Beispielitem: "Dass jemand ohne meine Zustimmung an die Daten in meinem Computer gelangt, wäre ein ernstzunehmendes Problem für mich".

In der Subskala **Verhaltensabsicht** soll erfasst werden, inwieweit Verhaltensabsichten in Bezug auf die Computersicherheit vorhanden sind. Beispielitem Verhaltensabsicht: "Ich werde (auch) in Zukunft Maßnahmen ergreifen, um Informationen und Computerdaten vor Sicherheitsverletzungen zu schützen".

In der Subskala **Verhalten** wird erfasst, inwiefern die MitarbeiterInnen in der letzten Zeit tatsächlich Sicherheitsbewusst gehandelt haben. Beispielitem Verhalten: "Ich verlasse meinen Arbeitsplatz auch bei kurzer Abwesenheit immer so, dass keine sensiblen Daten abrufbar sind (passwortgeschützter Screensaver, Schränke abgesperrt, Büro abgesperrt)".

Die Skala **Wissen** besteht schließlich aus Wissensfragen zu verschiedenen Aspekten wie E-Mails, Passwörtern und Angriffsarten. Das Wissen konnte im Rahmen dieser Studie nicht umfassend abgefragt werden, da je nach Unternehmensbranche, Position und Aufgabenbereich der TeilnehmerInnen ein anderer Wissensstand als angemessen betrachtet und mit Security Awareness in Zusammenhang gebracht werden kann.
Die Wissens-Skala diente daher nicht der direkten Erfassung des Sicherheitsbewusstseins, sondern wurde in dieser Studie für die Prüfung der Kriteriumsvalidität verwendet.

Abbildung 7. Verlässt man den Arbeitsplatz auch bei kurzer Abwesenheit immer so, dass keine sensiblen Daten abrufbar sind (passwortgeschützter Screensaver, Schränke abgesperrt, Büro abgesperrt)?

Beispieitem: "Angenommen, Sie erhalten eine E-Mail von einer Ihnen bekannten Person, mit der Sie jedoch nicht über diese E-mail gesprochen haben. Diese E-Mail enthält einen Dateianhang mit einer der folgenden Dateiendungen. Welche Datei ist ihrer Meinung nach sicher genug, um sie per Doppelklick zu öffnen?

- .exe
- .doc
- .xls oder .xlsx
- .pdf
- .vbs
- .bmp
- Ich würde keine der Dateien öffnen.

Beispielitem 2 "Welche der folgenden Passwörter sind ihrer Meinung nach zulässige und sichere Netzwerk-Passwörter?

- banane
- frosch1
- Yamaha99
- aCtoHM23
- fido23
- 6814745
- be!St&8
- jT35lo!ki$iD@23aq
- Keines der aufgeführten Passwörter ist sicher und zulässig.

Beispielitem 3: "Ich kenne den Unterschied zwischen Hacking und Social Engineering".

Die Untersuchungsdurchführung

Insgesamt nahmen 135 Personen an der Studie teil. Davon mussten 41 TeilnehmerInnen aus der Datenanalyse ausgeschlossen werden, da sie angaben weniger als 50% ihrer Arbeitszeit am Computer zu verbringen, oder es in ihrem Unternehmen/ ihrer Organisation keine Sicherheitsrichtlinien gibt, bzw. die TeilnehmerInnen nicht wussten ob es Sicherheitsrichtlinien gibt.
Die verbliebene Stichprobe mit *N*= 94 setzt sich aus 45 weiblichen und 49 männlichen TeilnehmerInnen zusammen.
Das Alter der TeilnehmerInnen liegt zwischen 20 und 55 Jahren bei einem Durchschnittsalter von *M*= 37.04 (*SD*= 10.03).
Die UntersuchungsteilnehmerInnen arbeiten in den Branchen Bauwesen und Handwerk, Einzel-/Großhandel, Finanz-/Versicherungsleistungen, öffentliche Verwaltung, in technischen Berufen, in der Werbung, Unternehmensberatung, Telekommunikation, Verteidigung und Forschung, Entwicklung und Lehre. Die meisten TeilnehmerInnen waren Angestellte/r, Teamleiter/in, Abteilungsleiter/in, Geschäftsführer/in oder Werkstudent/in.

Ergebnisse

Die Ergebnisse der Arbeit zeigen, dass auf der Grundlage sozialpsychologischer Theorien wie der Theory of Reasoned Action und der Protection Motivation Theory eine Operationalisierung des Sicherheitsbewusstseins und die Vorhersage von sicherheitsrelevantem Verhalten möglich sein kann. Für sämtliche in Abbildung 5 dargestellten Annahmen konnten mittlere bis starke Zusammenhänge gefunden werden.
Besonders hervorzuheben ist hier der Zusammenhang zwischen der empfundenen Selbstwirksamkeit und der Verhaltensabsicht bzw. dem Verhalten. Fühlt eine Person sich in der Lage, Sicherheitsrisiken zu erkennen, geeignete Maßnahmen zum Schutz sensibler Daten zu ergreifen und fundierte Entscheidungen über den sicheren Umgang mit Informationen und Technologien zu treffen, wirkt sich diese empfundene Selbstwirksamkeit auf die Einstellungs- und Verhaltensaspekte des Sicherheitsbewusstseins aus.

Abbildung 8. http://www.handy-katalog.com/wp-content/uploads/ 2012/08/spyware-300x272.jpg

Interessanterweise zeigte sich aber auch, dass der Zusammenhang zwischen dem Gesamtscore der Security Awareness und dem tatsächlichen Wissen eher gering ist. *D.h. das tatsächliche objektive Wissen über die Gefahren hinkt dem Sicherheitsbewusstsein noch hinterher.*

Gleichzeitig wurde deutlich, dass bereits die Messung der Security Awareness das Sicherheitsbewusstsein steigern kann und dass die Häufigkeit des Umgangs mit personenbezogenen oder vertraulichen Daten mit der Höhe des Sicherheitsbewusstseins zusammenhängt.

Fazit

Die gefundenen Ergebnisse sprechen zum einen für die inhaltliche Übereinstimmung der Struktur des Fragebogens und dem zu messenden Konstrukt und zum anderen für den Einsatz sozialpsychologischer Theorien wie der Theory of Reasoned Action und der Protection Motivation Theory zur Erklärung von sicherheitsbewusstem Verhalten.

Für die Praxis stellt der entwickelte Fragebogen in der Endfassung hinsichtlich seiner Aufwandsökonomie ein praktikables Werkzeug dar, um einen ersten Eindruck des Sicherheitsbewusstseins von MitarbeiterInnen zu erlangen.

Für die Erstellung und Vermittlung von Sicherheitsrichtlinien wurde deutlich, dass besondere Sorgfalt auf die Vermittlung der Risiken und Konsequenzen bei einer Nichteinhaltung dieser Richtlinien gelegt werden sollte. Die Zusammenhänge

zwischen Selbstwirksamkeit und Einstellungs- bzw. Verhaltensaspekten verdeutlichen die **Notwendigkeit von Trainingsprogrammen und Schulungen**, die die MitarbeiterInnen befähigen, selbstständig Präventivmaßnahmen zu ergreifen und angemessen auf Sicherheitsprobleme zu reagieren.

Die letzten Enthüllungen über die NSA-Affäre und Berichte über den Diebstahl persönlicher Daten verdeutlichen, wie wichtig der sichere Umgang mit neuen Technologien und sensiblen Daten ist. Durch die vorgestellte Arbeit wurde die Wichtigkeit des Faktors „Mensch" für die Datensicherheit betont und ein Instrument entwickelt, mit dem dieser Faktor etwas greifbarer und kontrollierbarer gemacht werden kann.

zitierte Literatur

Koldner, L. (2014). Entwicklung und Validierung eines Fragebogens zur Erfassung von Security Awareness. Universität Duisburg-Essen: Fachgebiet Wirtschafts- und Organisationspsychologie.

Rantos, K., Fysarakis, K., & Manifavas, C. (2012). How Effective Is Your Security Awareness Program? An Evaluation Methodology. *Information Security Journal: A Global Perspective*, *21*(6), 328–345.

Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms. *Information Technology & People*, *26*(4), 401–419. doi:10.1108/ITP-12-2012-0147

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

Abbildung 9. Besser keinen dieser Wege einschlagen.
Photograph: www.alamy.com

Bewilligung eines Forschungsprojekts durch die DFG

"Die Wirkung von Refresher-Interventionen auf den Fertigkeitserhalt von komplexen, dynamischen Arbeitstätigkeiten der Prozesskontrolle über längere Zeitintervalle unter Berücksichtigung von Mental Workload und Situation Awareness" (KL2207/3-3)

Hauptantragstellerin: Annette Kluge
Mitantragsteller: Dr. Benjamin Weyers, RWTH Aachen

Wir freuen uns über die Bewilligung eines Forschungsprojektes durch die Deutsche Forschungsgemeinschaft (DFG). Das Projekt wird uns über die kommenden 30 Monate begleiten.

Mit den nun geförderten Experimenten wird das übergeordnete Ziel verfolgt, neue Erkenntnisse zur Förderung des Erhalts von komplexen, dynamischen, prozeduralen Fertigkeiten durch Refresher-Interventionen (RIs) zu gewinnen.
Im Bereich der Prozesskontrolle gibt es bisher nur wenige Studien zum Fertigkeitsverlust und -erhalt, obwohl gerade dieser im Zusammenhang mit den Nebenwirkungen von Automation an sich als bedeutsam thematisiert wird. **Durch eine RI soll ein am Ende eines Ersttrainings erreichtes Leistungsniveau wiederhergestellt werden**, nachdem ein Zeitintervall des Nichtabrufens seit dem Ersttraining vergangen ist. Aufbauend auf den Erkenntnissen unserer bisherigen Experimente soll die Wirkung von den RIs wie Practice (weiteres Üben), Symbolic Rehearsal (nicht-offenes gedankliches Ausführen), das Abrufen der Fertigkeit unter Prüfungsbedingungen (Testen)

a) in Ergänzung zu den bisher verwendeten sog. Fixed Sequences auch an **Parallel und Contingent Sequences** untersucht werden, sowie
b) deren Wirkung unter Berücksichtigung psychophysiologischer Masse hinsichtlich des **Mental Workloads** und der **Situation Awareness** untersucht werden, sowie
c) um ein innovatives Konzept einer **Gaze-Guiding** Benutzerschnittstelle erweitert werden, bei dem das Refreshen zur Zeit des Abrufen stattfinden soll.

Fixed, Parallel und Contingent Sequences bilden dabei einen Großteil der Aufgaben ab, die in der Mensch-Maschine Interaktion in unterschiedlichen Bereichen der Prozesskontrolle zu erfüllen sind.

Die Berücksichtigung von Mental Workload und Situation Awareness zielt darauf ab Erkenntnisse zu gewinnen, wie RIs gestaltet sein müssen, um in den meist stressinduzierenden abnormalen Situationen des Abrufs eine Fertigkeit möglichst ressourcenschonend abzurufen.

Obwohl vereinzelte Hinweise zur Wirkung der von uns eingesetzten RIs bereits vorliegen, so ist die Erprobung der Wirkung dieser RIs für komplexe, dynamische Fertigkeiten innovativ und sinnvoll. Denn in unseren bisherigen Untersuchungen hat sich gezeigt, dass sich Ergebnisse, die z.B. hinsichtlich des Test-Effekts und des Symbolic Rehearsals an einfachen, nicht dynamischen Aufgaben gewonnen wurden, bei komplexen, dynamische Aufgaben nicht 1:1 replizieren lassen, oder nicht gewünschte Nebenwirkungen aufweisen, wie z.B. einen höheren Mental Workload erzeugen als solche RIs, die eine weitere Schemaautomatisierung fördern, wie z.B.eine Practice-RI.

Auf Basis der Ergebnisse können Gestaltungs-empfehlungen für Maßnahmen zum Fertigkeitserhalt, wie z.B. Refresher-Interventionen oder zur Gestaltung von abruffreundlichen Benutzerschnittstellen abgeleitet werden.
Die Erkenntnisse sind für die Gestaltung von Trainings im Sinne des Qualifikationserhalts für Industrien mit hoher Prozessautomation bedeutsam, sowie prinzipiell auch für weitere Branchen, in denen es auf den Fertigkeitserhalt ankommt, wie z.B. in der Medizin oder der Aviatik.

News

Aktuelle Projekte zum Thema Crew/Team Resource Management

Forschungserkenntnisse in der Praxis anzuwenden hat für uns einen hohen Stellenwert. Somit freuen wir uns über Anfragen unterschiedlicher Personen und Institutionen z.B. im Bereich Luft- und Raumfahrt oder auch Medizin, welche sich beruflich mit den Themen CRM, TRM und High Responsibility Teams befassen, sie in ihrer Arbeit zu unterstützen. Gerne stellen wir Ihnen eine Auswahl unserer aktuellen Kooperationen kurz vor.

In der zentralen interdisziplinären Notaufnahme des **Florence-Nightingale Krankenhauses der Kaiserswerther Diakonie** werden unter der Leitung von **Dr. Martin Pin** Team Resource Management Trainings mit theoretischen Inputs und praktischen Simulationen durchgführt. Wir unterstützen diese Maßnahmen sehr gerne in Bezug auf eine fundierte Evaluation.

Auch im **Universitätsklinikum Essen** findet in der Klinik für **Anästhesiologie und Intensivmedizin (Prof. Dr. Jürgen Peters)** unter der Leitung von **Dr. Frank Herbstreit** und **Dr. Clemens Kehren** ein CRM-Seminar im Rahmen der Notarztausbildung statt. Hier unterstützen wir die Wirksamkeitsprüfung der Maßnahme ebenfalls mit Hilfe einer fundierten Evaluation.

Abbildung 10. Einsatzkräfte der Feuerwehr.
http://media0.faz.net/ppmedia/aktuell /wissen/528682568/1.629736/article_aufmacher_klein/einsatzkraefte-der-feuerwehr-dresden-proben-was-im-fall-eines-feuers-im-residenzschloss-zu-unternehmen-ist.jpg

Zusammen mit **Achim Hackstein** (Kooperative Regionalleitstelle Nord), **Florentin von Kaufmann** (Branddirektion München) und **Helge Regener** (SIRMED AG, Schweizer Institut für Rettungsmedizin) gibt **Vera Hagemann** in der Stumpf + Kossendey Verlagsgesellschaft mbH ein *Handbuch Simulation für den präklinischen Bereich* heraus. Ziele des Buches sind Hintergründe und Verfahren der Simulation zu beschreiben und Lehrenden Handwerkszeug zur praktischen Abwicklung von Simulationen für unterschiedliche Anwendungsfelder zur Verfügung zu stellen. Grundlagen zu Teamarbeit in Hochrisiko Bereichen, Crew Resource Management und Lernen werden mit dem Thema Simulation praktisch verknüpft. Darüber hinaus gibt es Checklisten zur Vorbereitung, Debriefings zur Nachbereitung und Hilfen zum Umgang mit den häufigsten Problemen bei Simulationen. Erscheinen soll das Buch in der ersten Hälfte 2015.

Aktuelle Veröffentlichungen

Kluge, A. & Frank, B. (2014). Counteracting skill decay: Four refresher interventions and their effect on skill retention in a simulated process control task. *Ergonomics.* DOI:10.1080/00140139.2013.869357

Frank, B. & Kluge, A. (2014). Development and first validation of the PLBMR for lab-based mircorworld research. In A. Felnhofer & O.D. Kothgassner (Eds.), *Challenging Presence*. Proceedings of the International Society for Presence Research. 15th International Conference on Presence (pp. 31-42). Facultas.wuv

Kluge, A., Frank, B. & Miebach, J. (2014). Measuring skill decay in process control - results from four experiments with a simulated process control task. In De Waard, D., Brookhuis, K., Wiczorek, R., Di Nocera, F., Barham, P., Weikert, C., Kluge, A., Gerbino, W., and Toffetti, A., (Eds.) (2014), *Proceedings of the Human Factors and Ergonomics Society Europe Chapter 2013 Annual Conference*. Available as open source download from http://conference.hfes-europe.org/

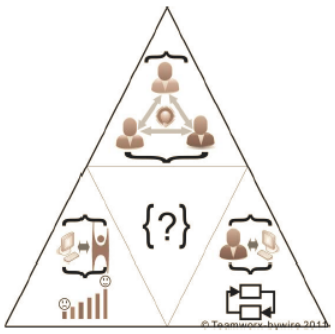
Nazir, S., Kluge, A. & Manca, D. (2014) Automation in process industry: cure or curse? How can training improve operator's performance? Jiří Jaromír Klemeš, Petar Sabev Varbanov and Peng Yen Liew (Editors) *Proceedings of the 24th European Symposium on Computer Aided Process Engineering* – ESCAPE 24, June 15-18, 2014, Budapest, Hungary.

Nazir, S., Kluge, A. & Manca, D. (2014). Can immersive virtual environments make the difference in training industrial operators? I In De Waard, D., Brookhuis, K., Wiczorek, R., Di Nocera, F., Barham, P., Weikert, C., Kluge, A., Gerbino, W., and Toffetti, A., (Eds.) (2014), *Proceedings of the Human Factors and Ergonomics Society Europe Chapter 2013 Annual Conference*. Available as open source download from http://conference.hfes-europe.org/

Abbildung 11. Die Elbe bei Magdeburg (Austragungsort des Workshop Kognitive Systeme 2014) in den Morgenstunden.

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
sfb transregio 62 Companion Technology
DLR
UNIVERSITÄT DUISBURG ESSEN Offen im Denken

3. Interdisziplinärer Workshop Kognitive Systeme: Mensch, Teams, Systeme und Automaten



Verstehen, Beschreiben und Gestalten Kognitiver (Technischer) Systeme

25 - 27. März 2014 in Magdeburg

Universität Duisburg-Essen
Offen im Denken
Wirtschafts- & Organisationspsychologie
Komplexität und Lernen
Newsletter für Organisationales Lernen, Simulation und Training
Ausgabe 30 | März 2014

Impressum

"Komplexität und Lernen"
ISSN 1661-8629
erscheint vierteljährlich

Herausgeberin:

Prof. Dr. Annette Kluge

Universität Duisburg-Essen
Fachbereich Wirtschafts- & Organisationspsychologie
Fakultät für Ingenieurwissenschaften
Abteilung für Informatik und Angewandte Kognitionswissenschaften
Lotharstr. 65
47048 Duisburg
annette.kluge@uni-due.de
Gastprofessorin am Lehrstuhl für Organisationspsychologie
Universität St. Gallen

Wenn Sie Interesse an dem Newsletter haben, dann mailen Sie bitte an annette.kluge@uni-due.de dann nehmen wir Sie gerne in unseren Verteiler auf.