LAND BRANDENBURG

5. Technologie- und Anwendungs-Dialog

Stärkefaktor Mensch:
Digitalisierung **nicht ohne Informationssicherheit.**
Informationssicherheit **nicht ohne Awareness.**

Prof. Dr. rer. nat. Margit Scholl

7. Dezember 2017

Technische Hochschule Wildau
(Wirtschafts- und Verwaltungsinformatik;
Trainingszentrum für Informationssicherheit –
„IT Security Arena“)

TH WILDAU

margit.scholl@th-wildau.de
http://www.th-wildau.de/scholl

Wildau Institut für innovative Lehre,
lebenslanges Lernen und
gestaltende Evaluation

Wille

wille@twz-ev.de
http://www.twz-ev.org/

Informationssicherheit

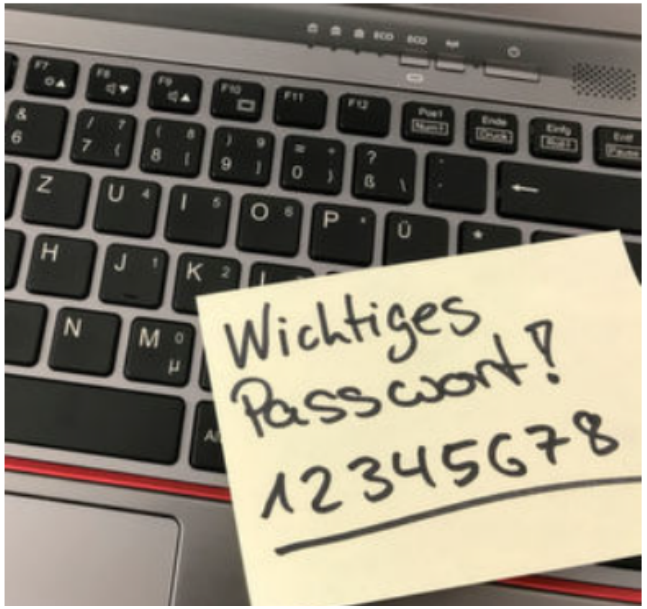
IT Security wird für Unternehmen im Windschatten der Digitalisierung immer wichtiger.

Security Insider

Datensicherheit

IT-Security funktioniert nur als Gesamtpaket

30.11.17 | Autor / Redakteur: Oliver Windhorst / Peter Schmitz



Fast kein Tag vergeht ohne Meldungen über Cyber-Attacken auf Unternehmen. Wer jetzt meint, dass dieses Firmen und ihre Mitarbeiter angesichts dieses Nachrichten-Dauerfeuers perfekte Schutzmechanismen entwickelt hätten, täuscht sich. Eine aktuelle Umfrage sieht hier noch „Luft nach oben". Auch im Fokus: Fahrlässiges Verhalten von Mitarbeitern.

Quellen: https://www.security-insider.de/index.cfm?pid=1&pk=661760&p=1&cmp=nl-36&uuid=3B10C402-D57C-4A08-8E093243626CC222 und https://www.triumph-adler.de/ta-de-de/idc-studie. Zugriff: 1.12.2017.

Fachkräfte als „Risikofaktor“ ?

Die deutschen IT-Verantwortlichen sind sich einig:

84 Prozent beklagen den laxen Umgang mit Vorschriften,

82 Prozent würden sich freuen, wenn die Regeln überhaupt bekannt wären.


Security Insider

Insider-Bedrohungen und Fachkräftemangel

Mitarbeiter als Risikofaktor und heißbegehrte Fachkraft

03.04.17 | Autor / Redakteur: Dirk Pfefferle* / Peter Schmitz

Der Mensch im U
gesucht und gefü
und heißbegehrte
„gefährlich“ ein M
Unternehmen ist,
Alter. Die Altersg
(18 bis 35) ist laut
Ponemon Institut
Gruppe. Trotz die
Millenials die wicl
Unternehmen: Nu
der Fachkräftema

„Risikogruppe Mensch“ steht auf einer Stufe mit Hacks und dem Verlust wertvoller Informationen.

Schwachstellen, Bedrohungen, Risiken

Digitalisierung und die Folgen 2017…

Spam

E-Mail Betrug + 29%

Quelle: https://www.proofpoint.com/de. Zugriff: 28.11.2017.

64% Ransomware

Malware

24% Bank-Trojaner

Viren

Würmer

Hoax

Spyware

Adware

Scareware

Fake

Backdoor

CEO Fraud

Rootkit

SQL-Injection

+ 85%

Botnet-Armee

oder Local File Inclusion

Keylogger

DDoS + 8 %

schädliche URLs + 600%

APT

Web-Attacken + 30%

Phishing Links + 10%

Identitätsdiebstahl

Zero-Day-Exploit

Doppelgänger-

Identitätsmissbrauch

Drive-by-Exploit

Domänen 20:1

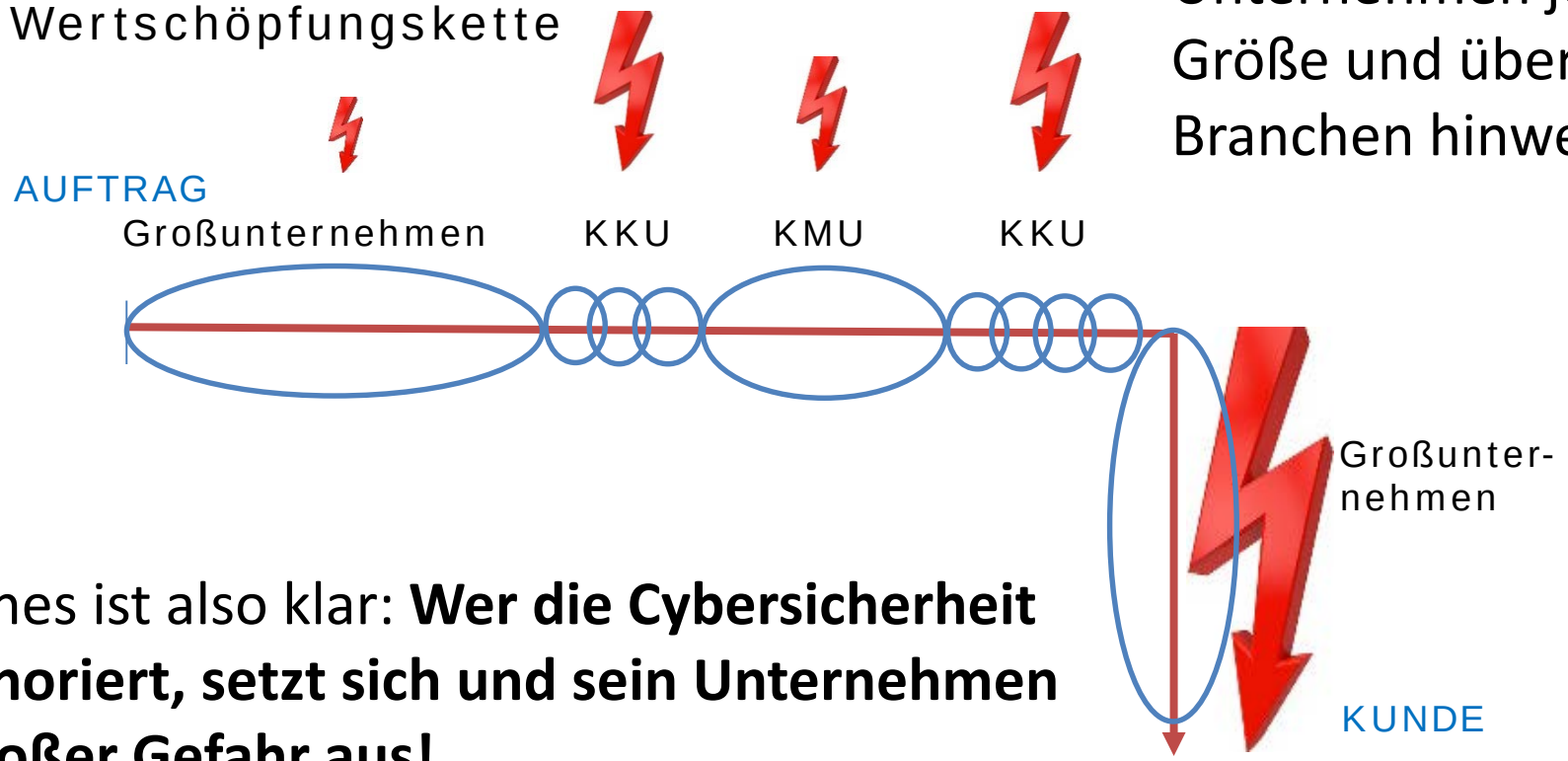
SE

gefälschte Kundendienst-Konten + 5%

Bildquelle: A Tale, https://de.toonpool.com/cartoons/Wahl%20in%20Frankreich_291937. Zugriff: 28.11.2017.

IS-Risiken Wertschöpfungskette

Die Häufigkeit solcher Angriffe und der Umfang nimmt ständig zu – bei Unternehmen jeder Größe und über alle Branchen hinweg.

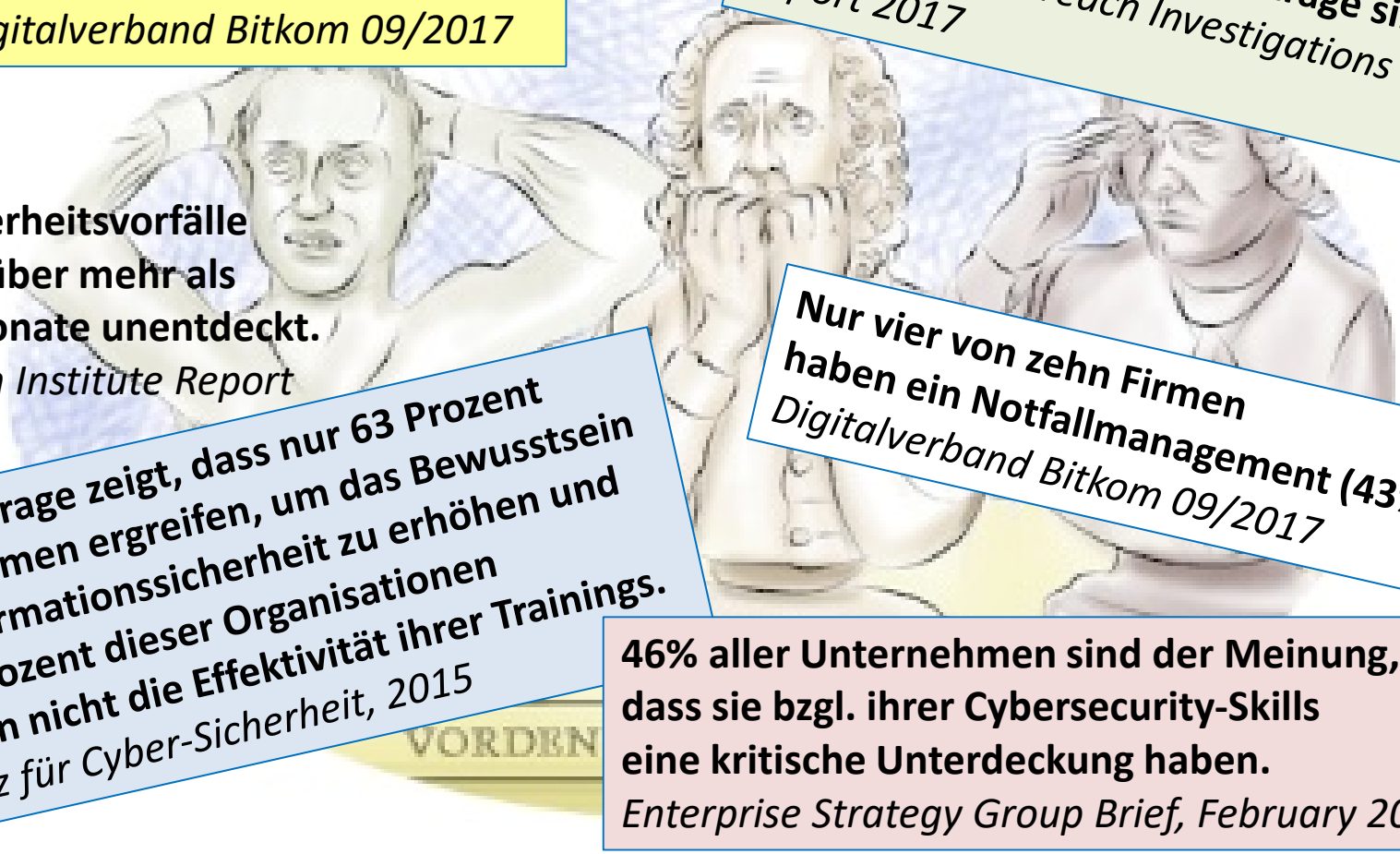


Eines ist also klar: **Wer die Cybersicherheit ignoriert, setzt sich und sein Unternehmen großer Gefahr aus!**

Strategische Defizite…

Nicht einmal die Hälfte der (befragten) Unternehmen in Deutschland ist ausreichend auf einen Cyberangriff vorbereitet. *Digitalverband Bitkom 09/2017*

Manager zahlen eher Lösegeld, als in neue Schutzfunktionen zu investieren – großes Risiko, da Lösegeldzahlungen in der Regel sechsstellige Beträge sind. *Verizon's Data Breach Investigations Report 2017*



74%
der Sicherheitsvorfälle bleiben über mehr als sechs Monate unentdeckt.
Ponemon Institute Report

Nur vier von zehn Firmen haben ein Notfallmanagement (43%). *Digitalverband Bitkom 09/2017*

Eine Umfrage zeigt, dass nur 63 Prozent Maßnahmen ergreifen, um das Bewusstsein für Informationssicherheit zu erhöhen und 40,5 Prozent dieser Organisationen messen nicht die Effektivität ihrer Trainings. *Allianz für Cyber-Sicherheit, 2015*

46% aller Unternehmen sind der Meinung, dass sie bzgl. ihrer Cybersecurity-Skills eine kritische Unterdeckung haben. *Enterprise Strategy Group Brief, February 2016*

Bildquelle: A Tale, https://de.toonpool.com/cartoons/Wahl%20in%20Frankreich_291937. Zugriff: 28.11.2017.

EU-DSGVO gilt ab 25. Mai 2018 direkt…

- **(Interne) Kosten** eines Datenschutzvorfalls pro Datensatz **178 Euro**:

500 Kunden:	89.000 Euro
2.500 Kunden:	445.000 Euro
12.500 Kunden:	2.225.000 Euro

- **(Externe) Kosten**: u.a. …

	Negative Innen- und Außenwirkung
	Beeinträchtigung der Aufgabenerfüllung
Verstoß gegen Gesetze	Informationelles Selbstbestimmungsrecht
Bußgelder	bis zu 4 Prozent des weltweiten Umsatzes

Quelle interne Kosten: Michael Schröder, Schutzziele der DSGVO, Vortrag am 23.11.2017, Business Development Manager New Technologies, ESET Deutschland GmbH

Erfolgreiche Digitalisierung…

…benötigt

eine **Strategie**,

…gewährleistet

ein **angemessenes** IT-Sicherheitsniveau, Sicherheitsstandards und Datenschutz,

…braucht

ausreichend **qualifiziertes** Personal,

…erfordert

einen **Kulturwandel** in der Organisation,

…bedarf

einer kontinuierlichen, zielgruppen-orientierten **Fort- und Weiterbildung** für **alle** Beschäftigten

Maßnahmen für angemessene Sicherheit …

- … bedeuten Aufwand
- … benötigen Zeit
- … kosten Geld

Bedeutet

- nicht nur technische,
- sondern auch organisatorische
- und Sensibilisierungs- und wissensvermittelnde Maßnahmen.

Bedrohungen 3/2017

?

WARUM?

Zusammenfassung:

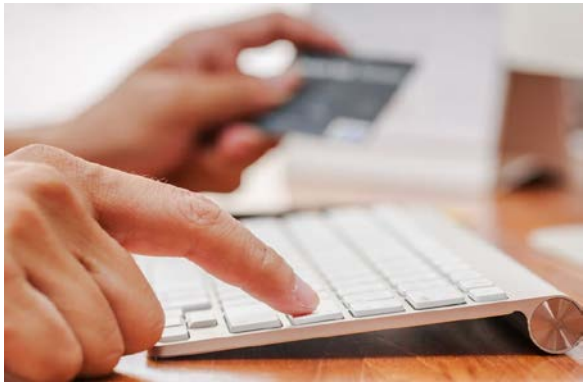
Cyber-Angriffe zielen auf Menschen, nicht auf Technologien ab!

Quelle:
https://www.proofpoint.com/de.
Zugriff: 28.11.2017.

Forschungserkenntnisse I

- Institutionen führten immer mehr Systeme ein, die auf dem Internet und seinen Diensten basieren, was es Millionen von Kunden ermöglichte, solche Systeme **ohne angemessene Informationssicherheit** (IS) extern zu nutzen.

- Ein direktes Ergebnis war, dass Kriminelle ihre Aufmerksamkeit unter ihrem neuen Motto auf den Endbenutzer verlagerten:
  "Versuchen Sie nicht, sich in die IT-Systeme des Unternehmens zu hacken;
  es kann sehr schwierig sein
  - gehen Sie über den naiven Endbenutzer!“



Quelle: von Solms, S.H., “The 5 Waves of Information Security – From Kristian Beckman to the Present”, in: K. Rannenberg, V. Varadharajan, and C. Weber (eds.), SEC 2010, IFIP International Federation for Information Processing AICT 330, 2010, pp. 1-8.
Bildquelle: https://static.giga.de/wp-content/uploads/2016/07/Windows-10-Kosten-rcm992x0.jpg. Zugriff: 28.11.2017.

„Risikofaktor“ Mensch

Die **51- bis 69-Jährigen** sind laut der Studie dabei besonders leicht auszutricksen.

Die Gruppe der **35- bis 50-Jährigen** setzt sich am ehesten über bekannte Regeln hinweg.

Die risikoreichste Gruppe sind jedoch die jungen Mitarbeiter und Mitarbeiterinnen, die Gruppe der Millenials (**18 bis 35**), da sie alle Arten von *unautorisierter* Technologie benutzen.

Forschungserkenntnisse II

- Wenn eine **einzelne Benutzeraktion** ein gesamtes Sicherheitsprogramm gefährden kann, **dann ist das Problem das Sicherheitsprogramm selbst**.

Winkler, I., "The Human Exploitation Kill Chain" (Video), RSA Conference, https://www.rsaconference.com/events/us17/agenda/sessions/6682-The-Human-Exploitation-Kill-Chain%20RSA, 2017, accessed May 30, 2017.

Das menschliche Element spielt eine bedeutende Rolle bei der erfolgreichen Bereitstellung von IS in heutigen Organisationen:

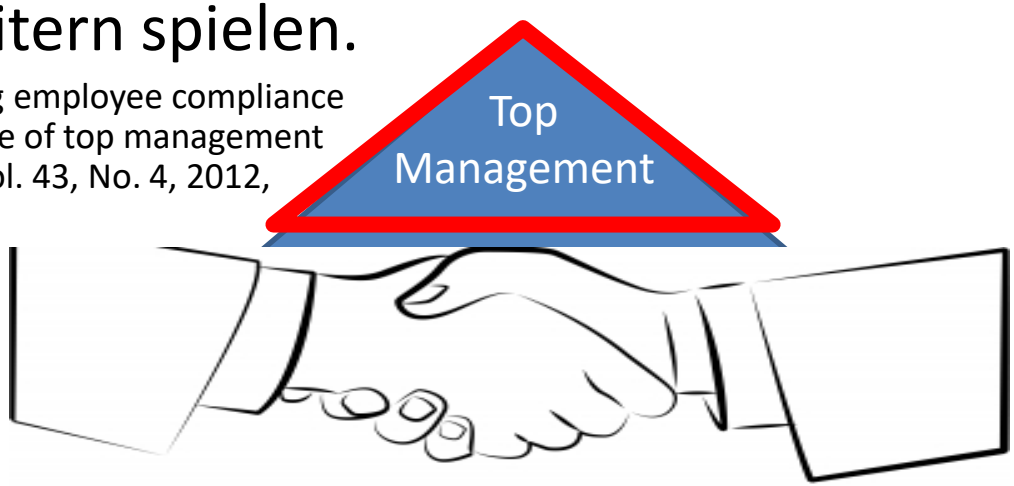
- Das Sicherheitsverhalten wird stark von der persönlichen **Risikowahrnehmung der Mitarbeiter und Mitarbeiterinnen** beeinflusst und **diese Wahrnehmungen können [durch Sensibilisierung und Schulung] positiv verändert** werden.

Quelle: Beyer, M., S. Ahmed, K. Doerlemann, S. Arnell, S. Parkin, A. Sasse, and N. Passingham, Awareness is only the first step. A framework for progressive engagement of staff in cyber security, Hewlett Packard, Business white paper, 2016.

Forschungserkenntnisse III

- Zusammenfassend kann das **Top-Management** eine **proaktive Rolle** bei der Gestaltung des Compliance-Verhaltens von Mitarbeitern spielen.

Hu, Q., T. Dinev, P. Hart, and D. Cooke, "Managing employee compliance with information security policies: The critical role of top management and organizational culture", Decision Sciences, Vol. 43, No. 4, 2012, pp. 615-660.



- **Formale oder informelle Mechanismen** können bereitgestellt werden, um die **Interaktion** zwischen den Mitarbeitenden zu verbessern.
  Häufige Interaktion ist die Grundlage für die Bildung **zwischenmenschlicher Beziehung** und **psychologischer Bindung**.

Hsu, J.S.-C., S.-P. Shih, Y.W. Hung, and P.B. Lowry, "The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness", Information Systems Research, Vol. 26, No. 2, 2015, pp. 282-300.

Sicherheitsgerechtes Verhalten

Technische Sicherheit

Angesichts der gewachsenen Gefährdungslage wird zwar verstärkt in **technische Informationssicherheit** investiert und über die Risiken informiert, **doch reicht das nicht aus**.

Mangelnde Sensibilität

Befragungen zu den Belangen der Informationssicherheit in Organisationen belegen nach wie vor eine **mangelhafte Sensibilisierung**.

Sicherheitsgerechtes Verhalten

ist bei **allen** Beschäftigten notwendig und erfordert das Wissen um und ein Gefühl für die Risiken, ebenso wie die Fähigkeit und das Wollen, sach- und sicherheitsgerecht mit Daten, Informationen und Informationstechnik (IT) umzugehen.

Vorgegebene Regelungen

sind eine Voraussetzung dafür, sich adäquat zu verhalten, und sollten eindeutig formuliert, allgemein bekannt und auf Einhaltung hin kontrolliert werden.
Regelungen allein langen jedoch nicht – sie müssen auch gelebt werden.

Vorschriften

können leichter eingehalten werden, je informierter die Beschäftigten über die Sachverhalte sind und je besser sie die Motive dafür verstehen.

Sicherheit bringt Einschränkungen…

Bildquelle: Paolo Calleri, https://de.toonpool.com/cartoons/Weihnachten%202016_283863. Zugriff: 28.11.2017.

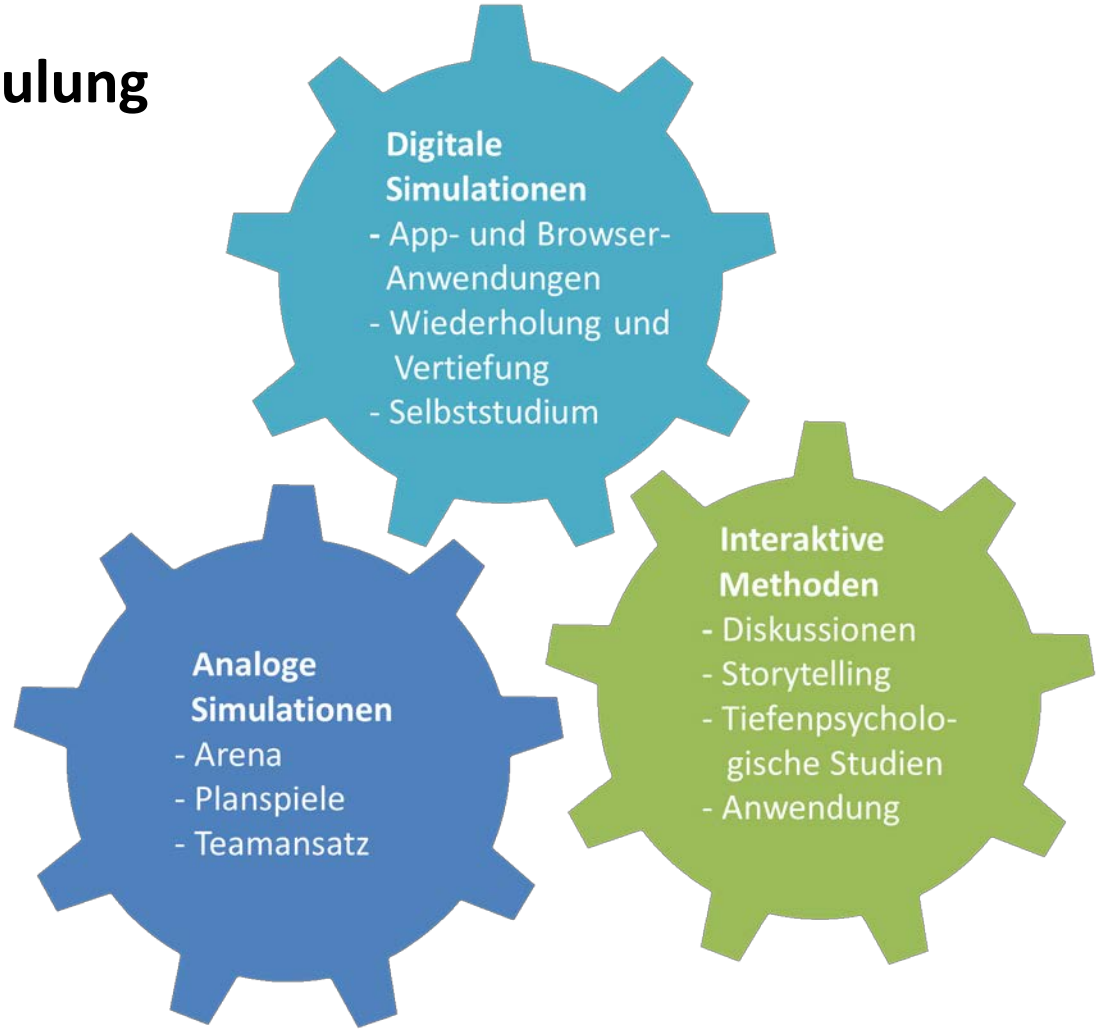
Unser Leben ist analog…
auch in Zeiten der Digitalisierung…

Bildquelle: Jan Tomaschoff, https://de.toonpool.com/cartoons/Technik_303843. Zugriff: 28.11.2017.

Erlebnisorientierte Sensibilisierung

Sensibilisierung und Schulung

– aber WIE?



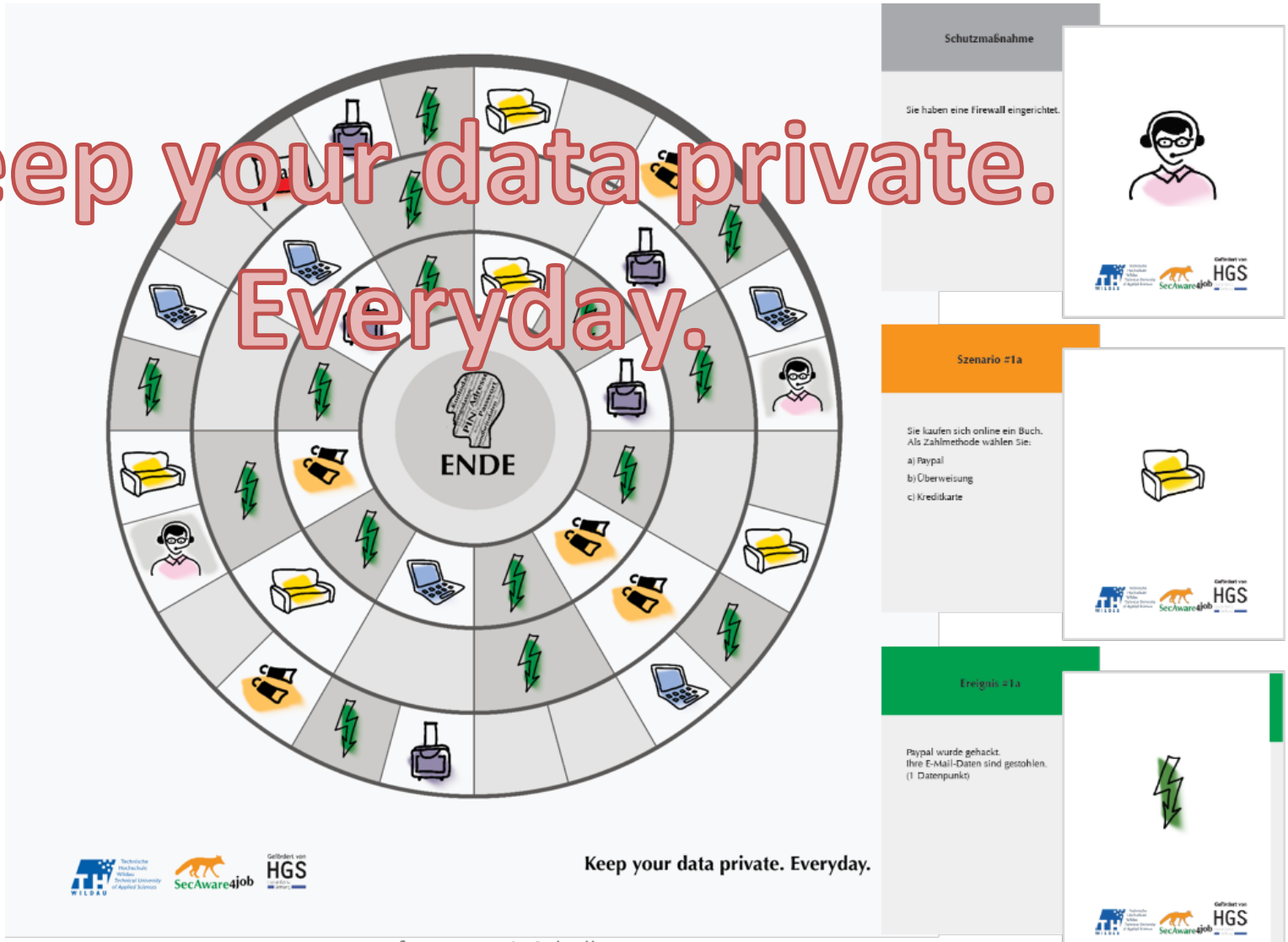
Sponsored by HGS Horst Görtz Stiftung
SecAware4job

Forschungsprojekt SecAware4job: Informationssicherheitsbewusstsein für den Berufseinstieg, 2015-2017.

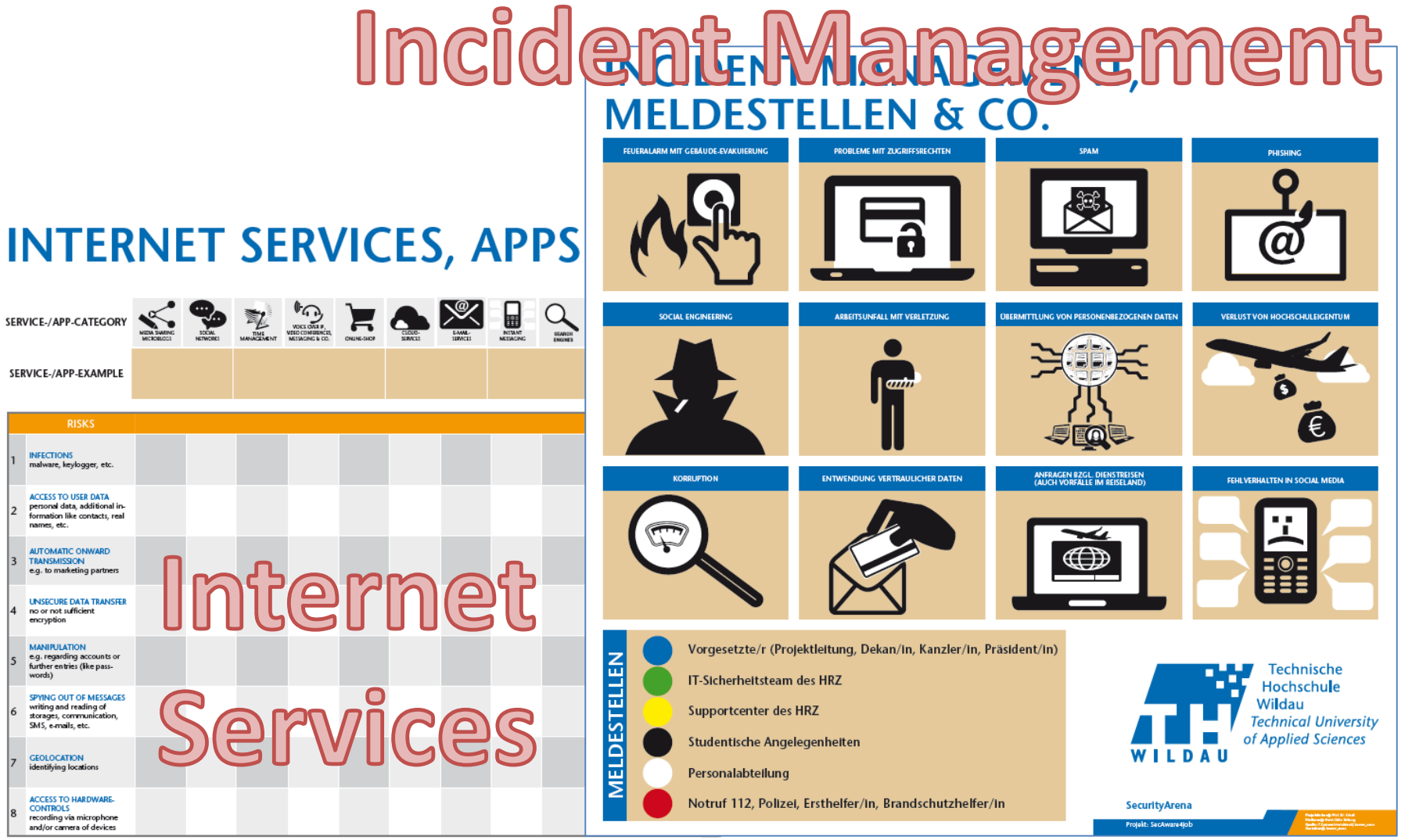
Quelle: Scholl (Hrsg.), Abschlussbericht SecAware4job, 2017. Fuhrmann, Koppatz, Edich & Scholl, 2017.

Erlebnisorientierte Sensibilisierung analog/haptisch: Clear Desk

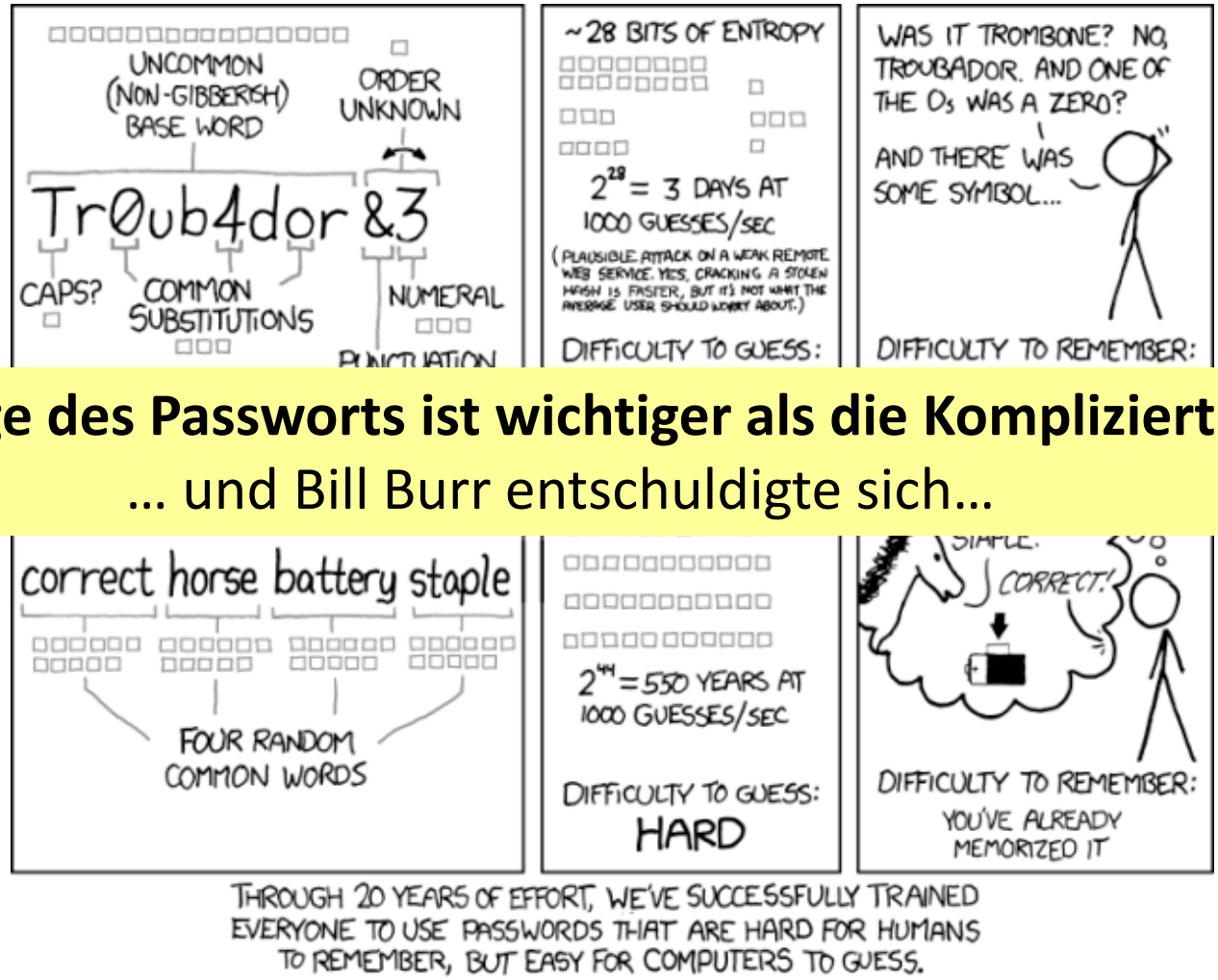
Erlebnisorientierte Sensibilisierung analog/haptisch: Brettspiel Datenschutz



Erlebnisorientierte Sensibilisierung analog/haptisch



Passwörter – ein Versagen der Menschen?



Die Länge des Passworts ist wichtiger als die Kompliziertheit!

… und Bill Burr entschuldigte sich…

Quelle: XKCD (published under a Creative Commons 2.5 license).
https://gizmodo.com/the-guy-who-invented-those-annoying-password-rules-now-1797643987. Zugriff: 1.12.2017.

Erlebnisorientierte Sensibilisierung digital/haptisch: Passwort Hacking

Erlebnisorientierte Sensibilisierung analog/haptisch *und* digital: Phishing

Phishing Übung

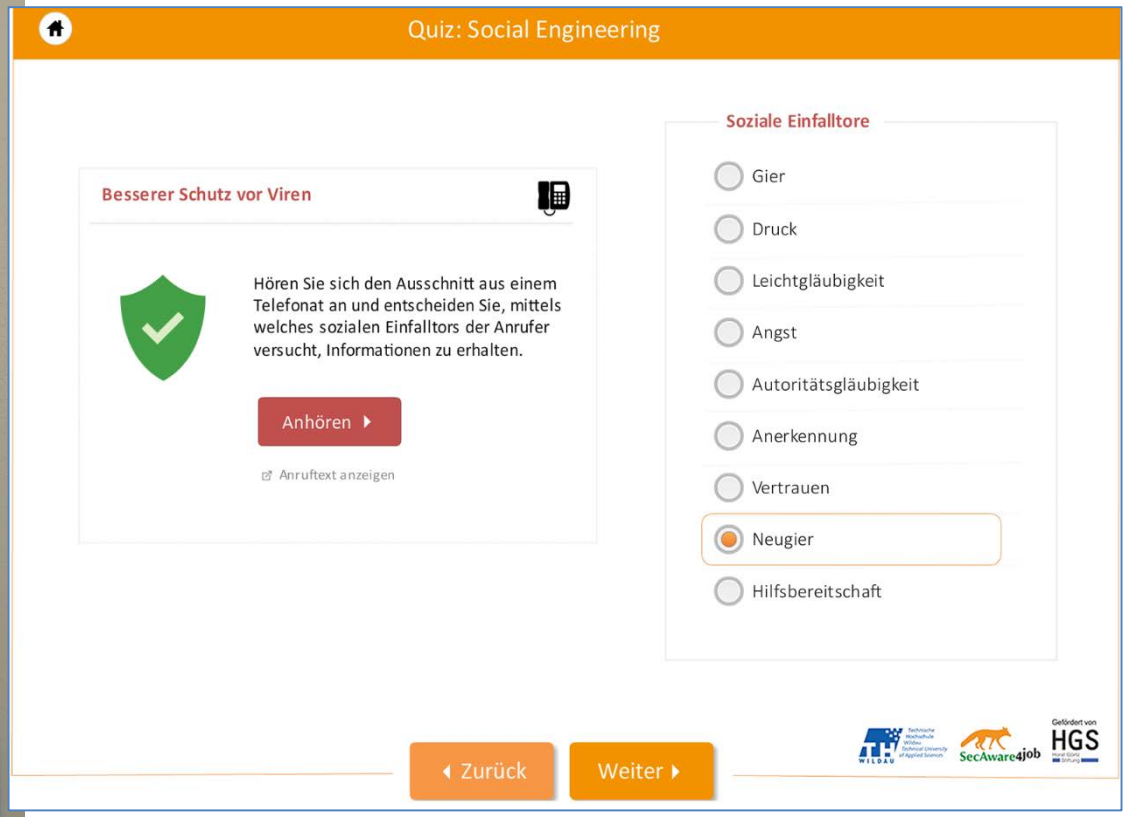
Was ist Phishing?
Kurze Einführung mit Beispielen

Test: Phishing erkennen
Entscheiden Sie, ob es sich bei der entsprechenden E-Mail um Phishing handelt oder nicht.

Test: Phishingmerkmale erkennen
Alle weiteren E-Mails sind Phishing-Mails. Finden Sie die Merkmale und Hinweise, die die E-Mail als Phishing-Versuch erkennen lassen.

Phishing = Passwort + Fishing

Erlebnisorientierte Sensibilisierung analog/haptisch *und* digital: SE



Social Engineering

Mensch = „Kritischer Faktor?“

… wegen Mangel an Verständnis für Sicherheitsfragen in Verbindung mit dem allgegenwärtigen Gebrauch von Computern …

Technologielösungen reichen **allein** nicht aus,

um Gegenmaßnahmen zu gewährleisten!

Aufmerksame und sachkundige Menschen sind durchaus besser in der Lage, moderne Verletzungen der Informations-Sicherheit zu verhindern…

Menschen können auf Zwischenfälle effizient und effektiv reagieren, indem sie sie umgehend melden, Probleme unter Quarantäne stellen und diese Probleme richtig diagnostizieren und behandeln.

Dark, M.J., “Security Education, Training and Awareness from a Human Performance Technology Point of View”, in M.E. Whitman, and H.J. Mattord (eds.), *Readings and Cases in Management of Information Security,* Course Technology, Mason, 2006, pp. 86–104.
Singh, A.N., A. Picot, J. Kranz, M.P. Cupta, and A. Ojha, “Information security management (ism) practices: Lessons from select cases from India and Germany”, *Global Journal of Flexible Systems Management*, Vol. 14, No. 4, 2013, pp. 225–239.

BAköV-Handbuch: Schulungsinhalte

1. Grundlagen der Informationssicherheit
2. Informationssicherheit am Arbeitsplatz
3. Gesetze und Regularien
4. Sicherheitskonzept der Organisation
5. Risikomanagement
6. Informationssicherheitsmanagement
7. IT-Systeme
8. Operativer Bereich
9. Technische Realisierung von Sicherheitsmaßnahmen
10. Notfallvorsorge/Notfallplanung
11. Neue Entwicklungen im IT-Bereich
12. Betriebswirtschaftliche Seite der Informationssicherheit
13. Infrastruktur-Sicherheit

p. 121f

BAköV-Handbuch

- Seite 123: **Table 4**: Zielgruppen und Schulungsmodule

Zielgruppe	Schulungsmodul Nr.												
	1	2	3	4	5	6	7	8	9	10	11	12	13
Vorgesetzte	X	X	X	X							O	X	
Sicherheitsmanagement	X	X	X	X	X	X	X	X	X	X	X	X	X
Datenschutzbeauftragte	X	X	X	X							X	O	
Infrastrukturbeauftragte	X	X	X	X	X	O				X			X
Benutzer	X	X											
Administratoren	X	X		X	X		X	X	X	X	X		O

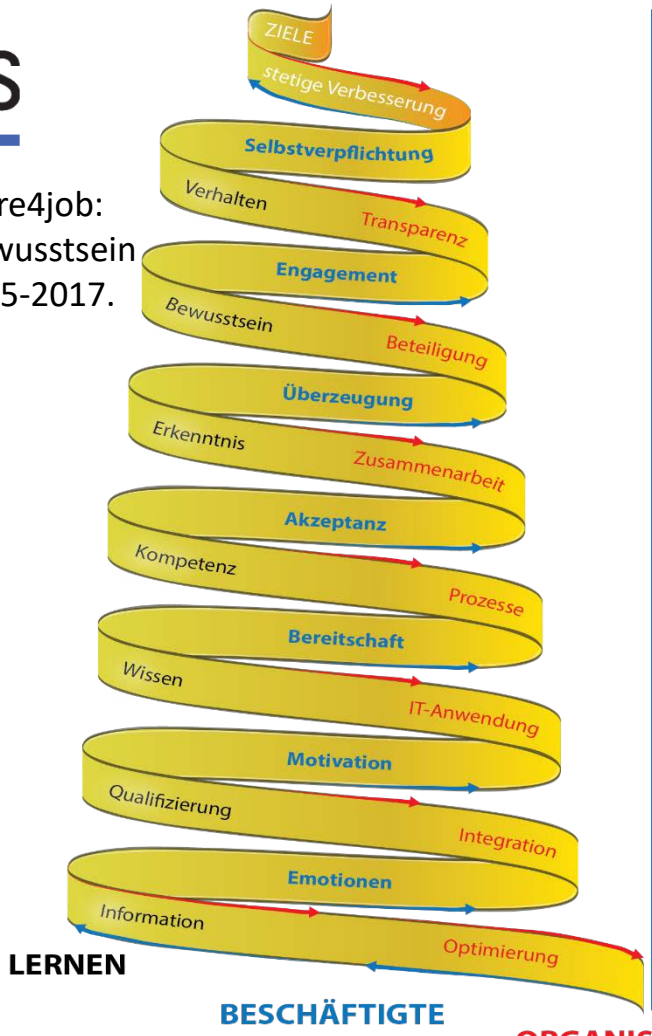
Legende: X: Modul wird empfohlen, O: Modul ist optional

Und mit welchen Methoden?

Spirale der transformativen Wechselwirkung

Sponsored by HGS Horst Görtz Stiftung
SecAware4job

Forschungsprojekt SecAware4job: Informationssicherheitsbewusstsein für den Berufseinstieg, 2015-2017.



Quelle: Scholl (Hrsg.), Abschlussbericht SecAware4job, 2017.

„Risikofaktor“ Mensch

Ponemon INSTITUTE

The Need for a New IT Security Architecture: Global Study

Sponsored by Citrix

Independently conducted by Ponemon Institute LLC

Publication Date: January 2017

Wer Fachkräfte nicht werben oder halten kann, der wird auf Lange Sicht die bestehenden Risiken noch erhöhen.

Daher ist ein **starkes Team** den Befragten wichtiger als alles andere.

Die meisten Unternehmen versagen hier jedoch:

Nur **44 Prozent** schaffen es, gut ausgebildete Mitarbeiter einzustellen und sie im Unternehmen zu halten.

Erlebnisorientierte Sensibilisierung

Sponsored by HGS Horst Görtz Stiftung
SecAware4job

Forschungsprojekt SecAware4job: Informationssicherheitsbewusstsein für den Berufseinstieg, 2015-2017.

Quelle: Scholl (Hrsg.), Abschlussbericht SecAware4job, 2017. Scholl, Fuhrmann & Pokoyski, 2016.

The Six Blind Men and Digital Media…

Quelle: https://www.google.de/search?q=mollers.dk. Zugriff: 28.11.2017.

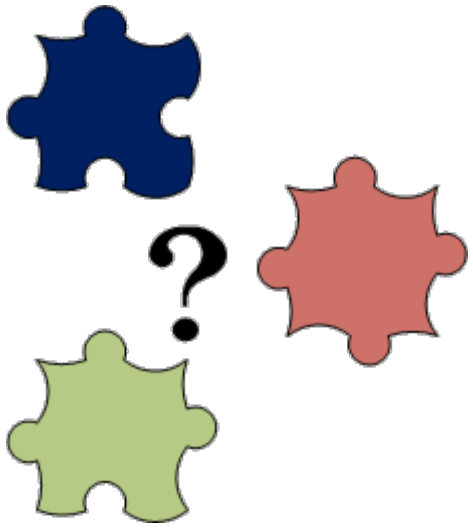
Zusammenfassung

- **Digitalisierung** **nicht ohne Informationssicherheit**
- **Informationssicherheit** **nicht ohne Awareness**
- **Awareness** (Informationssicherheitsbewusstsein) **durch *nutzerzentrierte* Sensibilisierung und Schulungen**, die

  zielgruppenorientiert im konkreten Arbeitskontext sind, definiert anhand **spezifischer** Bedrohungsanalysen der Geschäftsprozesse und Aufgabenstellungen, und **kreative** und **interaktive** Techniken mit rollenbasiertem sowie situationsbezogenem Lernen nutzen, um **individuelle Emotionalität** und **Motivation** im **teambasierten Austausch** zu erzielen.

Austausch / Diskussion

- Fragen?



Prof. Dr. Margit Scholl (TH Wildau)

Wirtschafs- und Verwaltungsinformatik

- **Projektmanagement** inklusive E-Government und Internationalisierung.
- **Prozessmanagement** inklusive Akzeptanz- und Qualitätsmanagement sowie Risiko und Change.
- **(Mobile) Betriebliche Anwendungen** wie z. B. SAP ERP oder Dokumentenmanagement- und Vorgangsbearbeitungssysteme (DMS/VBS) und eAkte.
- **Multimedia** inklusive Lerntechnologien & Lernformen und Interkultur.

Seit September 2014: 5 Jahre **Forschungsprofessur** mit halbem Lehrdeputat (9 SWS).
Fokus „Ganzheitlicher Aufbau und partizipatives Management von Smart-Technologien des 21. Jahrhunderts“.
Professorin Scholl ist mit „Verwaltungsinformatik und digitale Medien“ sowohl dem Forschungsfeld 2 (Informatik/Telematik) als auch dem Forschungsfeld 6 (Management und Recht) zugeordnet.

Offizielle Qualifizierungsstelle

- Zertifizierter Fortbildungslehrgang zur/zum **IT-Sicherheitsbeauftragten (IT-SiBe)** der öffentlichen Verwaltung über WILLE/TWZ e.V., adaptiert von der Bundesakademie für öffentliche Verwaltung (BAköV) für Kommunen und KMU
- Zertifizierter Fortbildungslehrgang zur/zum **Datenschutzbeauftragten (DSB)** nach EU-DSGVO über WILLE/TWZ e.V., adaptiert von der BAköV für Kommunen und KMU
- DLGI-Prüfungsstelle für den **Datenschutzführerschein** und den **ECDL** (European Computer Driving Licence)

Veröffentlichungen: https://publister.bib.th-wildau.de/publister/public/publist/filter/author/62

Prof. Dr. Margit Scholl & Team

Ausgewählte Projekte:

- Gendersensible Studien- und Berufsorientierung für den Beruf Security Spezialistin (Security) (2017-2019) http://security.wildau.biz/
- Skill Up: Matching graduates´skills and labour world demands through authentic learning scenarios (2016-2019) http://skill-up-project.eu/
- SecAware4job: Informationssicherheitsbewusstsein für den Berufseinstieg (2015-2017) secaware4job.th-wildau.de
- TechPedia: European Virtual Learning Platform for Electrical and Information Engineering (2014-2017) http://techpedia.fel.cvut.cz/de/home/blocks
- iBaMs: Barrierereduzierte Maschinen in innovativer Interaktion (2014) ibams.th-wildau.de
- IT- Sicherheit@KMU: Technische Investition einer mobilen Sensibilisierungsinitiative für KMU (2013-2014)
- Interkulturelle Weiterbildung für, mit und in KMU: kmu-interkomp20.th-wildau.de
- TEDS-Evaluationstool für Informationssysteme (Systemintegration in die E-Learning-Plattform Moodle der TH Wildau) (2012-2013)
- Labor - Infrastrukturveränderungen zur technischen Modernisierung als Basis von project- and problem-based Blended Learning (PPBBL) (2012-2013)
- Virtu: Modernisierungspilot innovations- und technologieorientierter Infrastruktur zur Hochschuldidaktik für interaktive Lehre (2011-2012)

Weitere, genutzte Literatur

- BSI-Standards **200-1, 200-2, 200-3, 100-4**.
- BAköv-Handbuch, IT-Sicherheitsbeauftragter in der öffentlichen Verwaltung, Version 5.0, 2016.
- Scholl, M., Fuhrmann, F., & Pokoyski, D. (2016). Information Security Awareness 3.0 for Job Beginners In J. E. Quintela Varajão, M. M. Cruz-Cunha, R. Martinho, R. Rijo, N. Bjørn-Andersen, R. Turner, & D. Alves (Eds.), *Conference on ENTERprise Information Systems (CENTERIS)*, Porto, Portugal, 433-436.
- Scholl, M. (Hrg.). Fuhrmann, F., Scholl, M., Edich, D., Koppatz, P., Scholl, L., Leiner, K., et al. (2017). *Informationssicherheitsbewusstsein für den Berufseinstieg: Abschlussbericht Projekt SecAware4job*. Aachen: Shaker.
- VM Verwaltung & Management, Zeitschrift für moderne Verwaltung, 5/2017
  - Lück-Schneider, Dagmar & Schuppan, Tino: Gestaltungskompetenzen für die Öffentliche Verwaltung im digitalen Zeitalter, S. 236-244.
  - Fuhrmann, Frauke/ Koppatz, Peter/ Edich, Denis/ Scholl, Margit: Sicher unterwegs in der digitalen Welt – spielend begreifend, S. 263-266.
  - Hill, Hermann: Wie geht Innovation? Ein Beitrag zur verhaltensorientierten Innovationsförderung, S. 270-279.