

Sichere Softwareentwicklung von Cloud-Anwendungen

Identifikation und Validierung von Erfolgsfaktoren
aus strategischer und operativer Perspektive unter besonderer
Berücksichtigung von Systemen, Prozessen und Werkzeugen

Marc Aurel Schubert, M. Sc.
marc.schubert@hs-mainz.de

Erstbetreuer:

Prof. Dr. Harald F. O. von Korfflesch
Universität Koblenz-Landau

Zweitbetreuer:

Prof. Dr. Sven Pagel
Hochschule Mainz

Virtuell, Freitag, 28.05.2021

Promotionsprojekt InnoProm Security



- Kooperative Promotion, gefördert durch den Europäischen Fonds für regionale Entwicklung (EFRE)
- Kofinanziert vom Ministerium für Wissenschaft, Weiterbildung und Kultur RLP (MW/WK)
- **Kooperationspartner:** sapite GmbH, Universität Koblenz-Landau
- **Erstbetreuer:** Prof. Dr. Harald von Korflesch (Universität Koblenz-Landau)
- **Zweitbetreuer:** Prof. Dr. Sven Pagel (Hochschule Mainz)
- **Laufzeit:** 4 Jahre (Juli 2018 - Juni 2022)
- **Weitere Beiträge aus dem Promotionsprojekt (Spin-Offs):**
Sichere Softwareentwicklung des Corona-Impftermin-Portals in RLP:
impftermin.rlp.de



innoprom-security.eu

Agenda

- Motivation und Relevanz
- Problemstellung und Forschungsfragen
- Ziel und Ergebnis der Promotion
- Methodisches Vorgehen
- Ergebnisse der Expertenstudie
- Implikationen für die Praxis

Cloud Computing

- **Bedarfsorientierte Ressourcennutzung**

- Ressourcen: Netze, Server, Speicher, Anwendungen und Dienste
- Bereitstellung: Hochgeschwindigkeitsnetze
- Minimaler Managementaufwand
- Betrieb von Cloud-Anwendungen

(Bedner, 2013; Chen & Zhao, 2012; Karam et al., 2012; Mell & Grance, 2011; Repschläger et al., 2010; Suryateja, 2018; Zhang, 2018).

- **Bitkom: 3 von 4 Unternehmen in Deutschland setzen auf Cloud Computing**

- 87% speichern unkritische Geschäftsdaten
- 70% befürchten unberechtigten Zugriff
- 57% befürchten Verlust von Daten

(Pols & Vogel, 2019; Pols & Heidkamp, 2020)



- **Bedenken zur Informationssicherheit beeinträchtigt die Nutzung von Cloud Computing**

(Pols & Vogel, 2019; Pols & Heidkamp, 2020)

Bedenken zur Informationssicherheit

- **Schutzziele**

- Vertraulichkeit / Confidentiality
- Integrität / Integrity
- Verfügbarkeit / Availability

(Bundesamt für Sicherheit in der Informationstechnik, 2018;
Müller, 2018)

- **Von der Bedrohung zum Schaden**



(Eigene Darstellung, 2020 erstellt in
Anlehnung an: Freiling, Grimm et al., 2014;
Müller, 2018; Suryateja, 2018)

Bedenken zur Informationssicherheit

- **Beispielszenario**

- Cloud-Anwendung kann über das Internet abgerufen werden
- Annahme einer Schwachstelle im Programmcode

- **Von der Bedrohung zum Schaden**



(Eigene Darstellung, 2020 erstellt in Anlehnung an: Freiling, Grimm et al., 2014; Müller, 2018; Suryateja, 2018)

Standards und sichere Softwareentwicklung

- **Standards**

- ISO 27001:2013 Informationssicherheitsmanagementsystem
- ISO 27001:2013, Anhang A, Kapitel 14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen

(ISO, 2013)

- **Sichere Softwareentwicklung**

- Integriert Sicherheitspraktiken in alle Projektphasen
- Training, Sicherheitsanalysen, Code Reviews, Sicherheitswerkzeuge
- Potenzial das Sicherheitsniveau von Cloud-Anwendungen zu erhöhen

(Dodson, 2019;
Müller, 2018;
Waidner, 2013)

- **Ansätze sicherer Softwareentwicklung**



- **Reduktion von Schwachstellen durch sichere Softwareentwicklung**

(Assal & Chiasson, 2018)

Agenda

- Motivation und Relevanz
- Problemstellung und Forschungsfragen
- Ziel und Ergebnis der Promotion
- Methodisches Vorgehen
- Ergebnisse der Expertenstudie
- Implikationen für die Praxis

Problemstellung

Problem

- Informationssicherheitsbedenken im Cloud Computing
- Beeinträchtiger Einsatz von Cloud Computing
- Beeinträchtigte Verarbeitung von kritischen Geschäftsdaten von Unternehmen in Deutschland

(Pols & Vogel, 2019)

Beitrag zur Problemlösung

- Sichere Softwareentwicklung
- Entwicklung von Cloud-Anwendungen mit weniger Schwachstellen
- Hervorbringen von Cloud-Anwendungen mit erhöhtem Sicherheitsniveau



- **Einflussfaktoren aus strategischer und operativer Perspektive**

Forschungsfragen

1. Welche **Merkmale** zeichnen eine Cloud-Anwendung aus?
2. Wie kann **Erfolg** von sicherer Softwareentwicklung von Cloud-Anwendungen gemessen werden?
3. Welche **Rolle spielen strategische und operative Aspekte** in sicherer Softwareentwicklung von Cloud-Anwendungen?
4. Welche **Rolle spielen Systeme, Prozesse und Werkzeuge** in sicherer Softwareentwicklung von Cloud-Anwendungen?
5. Welche **theoretischen Grundlagen** erklären Erfolg in sicherer Softwareentwicklung von Cloud-Anwendungen aus strategischer und operativer Perspektive?
6. Welche **subjektiv-validierten Erfolgsfaktoren** bestehen in sicherer Softwareentwicklung von Cloud-Anwendungen aus strategischer und operativer Perspektive?
7. Welche **objektiv-validierten Erfolgsfaktoren** bestehen in sicherer Softwareentwicklung von Cloud-Anwendungen aus operativer Perspektive und gegebenenfalls strategischer Perspektive?

Agenda

- Motivation und Relevanz
- Problemstellung und Forschungsfragen
- Ziel und Ergebnis der Promotion
- Methodisches Vorgehen
- Ergebnisse der Expertenstudie
- Implikationen für die Praxis

Ziel der Promotion

Das **Ziel** der Arbeit ist es, **Erfolgsfaktoren** in sicherer Softwareentwicklung von Cloud-Anwendungen aus strategischer und operativer Perspektive unter besonderer Berücksichtigung von Systemen, Prozessen und Werkzeugen zu identifizieren und zu validieren, um das **Sicherheitsniveau von Cloud-Anwendungen zu erhöhen.**

Ergebnis der Promotion

Das **Ergebnis** der angestrebten Arbeit ist die Erstellung eines **Erfolgsfaktorenmodell** in sicherer Softwareentwicklung von Cloud-Anwendungen aus strategischer und operativer Perspektive unter besonderer Berücksichtigung von Systemen, Prozessen und Werkzeugen.

Agenda





- Motivation und Relevanz
- Problemstellung und Forschungsfragen
- Ziel und Ergebnis der Promotion
- Methodisches Vorgehen
- Ergebnisse der Expertenstudie
- Implikationen für die Praxis

Methodisches Vorgehen

- Orientierung am Prozess zur Erfolgsfaktorenforschung nach Daschmann (1994)
- Promotionsvorhaben enthält vier Arbeitsschritte und drei Teilstudien (Studie I-III)



Bezugsrahmen

Arbeitsschritt	Vorläufiges konzeptionelles Modell potenzieller Erfolgsfaktoren	Studie I: Qualitativ-explorative Vorstudie	Studie II: Quantitative Validierungsstudie	Studie III: Feldexperiment zur Validierung ausgewählter Erfolgsfaktoren
Fokus	Identifikation von potenziellen Erfolgsfaktoren aus dem Stand der Forschung	Identifikation von weiteren potenziellen Erfolgsfaktoren	Validierung der identifizierten potenziellen Erfolgsfaktoren anhand des wahrgenommenen Erfolgs	Weitere Validierung der Erfolgsfaktoren, welche durch ein Feldexperiment überprüft werden können (beispielsweise den Einfluss von Sicherheitswerkzeugen auf den Erfolg)
Funktion	Selektion von potenziellen Erfolgsfaktoren 	Selektion von potenziellen Erfolgsfaktoren 	Explication der Erfolgsfaktoren durch wahrgenommenen Erfolg (subjektive Erfolgsindikation) <input checked="" type="checkbox"/> = <input type="checkbox"/> =	Explication der Erfolgsfaktoren durch gemessenen Erfolg (objektive Erfolgsindikation)  <input checked="" type="checkbox"/> = <input type="checkbox"/> =
Forschungsansatz	Systematisches Literaturreview Breite Literatursuche in einschlägigen Datenbanken (vom Brocke et al., 2009) Gezielte Literatursuche in Konferenz-Proceedings (Cooper and Hedge, 1993) Gezielte Literatursuche nach Research Agendas (vom Brocke et al., 2009)	Empirische Forschungsmethode: Qualitative Forschung <i>Datenerhebung:</i> Leitfadengestützte Experteninterviews (Bogner et al., 2014) <i>Datenauswertung:</i> Qualitative Inhaltsanalyse (Mayring, 2014) <i>Erkenntnislogik:</i> Induktiv (Sandberg, 2016) <i>Zielgruppen:</i> Oberste Verantwortliche für Informationssicherheit (strategisch), Entwickler & Tester (operativ)	Empirische Forschungsmethode: Quantitative Forschung <i>Datenerhebung:</i> Fragebogen (Wilde & Hess, 2007) <i>Datenauswertung:</i> Strukturgleichungsmodell (Wilde & Hess, 2007) <i>Erkenntnislogik:</i> Deduktiv (Sandberg, 2016) <i>Zielgruppen:</i> Oberste Verantwortliche für Informationssicherheit (strategisch), Entwickler & Tester (operativ)	Konstruktives Paradigma Feldexperiment (Wilde & Hess, 2007) I) Bereitstellung von Arbeitsumgebungen unter Einfluss der Erfolgsfaktoren (Gruppe A-n) und ohne Einfluss der Erfolgsfaktoren (Kontrollgruppe) II) Entwickler erstellen eine Cloud-Anwendung gemäß einer Aufgabenbeschreibung III) Die erstellte Software wird zur Erfolgsmessung nach Schwachstellen untersucht und nach CVSS 3.1 bewertet
Theoretische Grundlagen	Path Goal Theory (Evans, 1970; House, 1971) Social Exchange Theory (Homans, 1958)	Voraussichtlich Path Goal Theory, Social Exchange Theory und/oder weitere/andere theoretische Grundlagen	Voraussichtlich Path Goal Theory, Social Exchange Theory und/oder weitere/andere theoretische Grundlagen	Common Vulnerability Scoring System v3.1 Application Score 
Erwartetes Ergebnis	Vorläufiges konzeptionelles Modell: Bestehend aus potenziellen Erfolgsfaktoren aus der Literatur (beispielsweise Belohnung für sicheren Softwarecode, Richtlinien für Sicherheitswerkzeuge, Commitment zur Organisation, [...])	Erweitertes konzeptionelles Modell: Bestehend aus potenziellen Erfolgsfaktoren aus der Literatur und aus der Vorstudie.	Subjektiv-validiertes konzeptionelles Modell: Bestehend aus Erfolgsfaktoren, die durch den wahrgenommenen Erfolg bestätigt wurden.	Objektiv-validiertes konzeptionelles Modell: Bestehend aus Erfolgsfaktoren, die durch den wahrgenommenen Erfolg und dem Erfolg im Feld bestätigt wurden.

Agenda

- Motivation und Relevanz
- Problemstellung und Forschungsfragen
- Ziel und Ergebnis der Promotion
- Methodisches Vorgehen
- Ergebnisse der Expertenstudie
- Implikationen für die Praxis

Experteninterviews

- **Anzahl:** 15 Experteninterviews
- **Dauer:** 12:36 Stunden Interview-Material
- **Fokus:** Organisationen mit Sitz in Deutschland
- **Perspektive:**
 - Strategische Perspektive (4)
 - Operativer Perspektive (6)
 - Sowie Mischformen (5)
- **Wirtschaftszweige:**
 - Verkehr und Lagerei (3)
 - Gesundheits- und Sozialwesen (1)
 - Finanz- und Versicherungswesen (1)
 - Information und Kommunikation (9)
 - Erbringung von freiberuflichen Dienstleistungen (1)



Durchgeführte Interviews

Nr.	Rolle	Perspektive	Wirtschaftszweig	Cloud-Erfahrung	Rolle-Erfahrung	SE für	Tätig in
1	CISO	Strategisch	Gesundheit- und Sozialwesen	10 Jahre	30 Jahre	Eigene Organisation & Kunden	Deutschland (überwiegend)
2	CISO	Strategisch	Finanz- und Versicherungsdienstleistungen	7 Jahre	> 5 Jahre	Eigene Organisation & Kunden	Deutschland (überwiegend)
3	CISO	Strategisch	Verkehr und Lagerei	10 Jahre	5 Jahre	Eigene Organisation & Kunden	Deutschland (überwiegend)
4	CEO	Strategisch	Information und Kommunikation	10 Jahre	> 5 Jahre	Eigene Organisation & Kunden	Deutschland (überwiegend)
5	Cloud Administrator	Operativ	Information und Kommunikation	7 Jahre	> 7 Jahre	Eigene Organisation & Kunden	Deutschland (überwiegend)
6	Senior Cloud Engineer	Operativ	Information und Kommunikation	> 10 Jahre	> 20 Jahre	Eigene Organisation & Kunden	International gleichgew.
7	Senior Software Engineer	Operativ	Verkehr und Lagerei	9 Jahre	16 Jahre	Eigene Organisation & Kunden	Deutschland (überwiegend)
8	Microsoft 365 Architect	Operativ	Information und Kommunikation	8 Jahre	5 Jahre	Eigene Organisation & Kunden (als Beratungsleistung)	International gleichgew.
9	Senior Software Engineer	Operativ	Verkehr und Lagerei	5 Jahre	> 12 Jahre	Eigene Organisation & Kunden	Deutschland (überwiegend)
10	Senior Software Engineer	Operativ	Information und Kommunikation	5 Jahre (aber kein Kundeneinsatz)	15 Jahre	Kunden	Deutschland (überwiegend)
11	Leiter Softwareentwickler	Mischform	Information und Kommunikation	3 Jahre (wenig Kundeneinsatz)	14 Jahre	Kunden	Deutschland (überwiegend)
12	Cloud Sales Engineer und Security Architekt	Mischform	Information und Kommunikation	10 Jahre	8 Jahre	Kunden	International gleichgew.
13	Managing Consultant	Mischform	Information und Kommunikation	7-8 Jahre	5 Jahre	Eigene Organisation & Kunden (als Beratungsleistung)	Deutschland (überwiegend)
14	Lead Auditor Informationssicherheit (BSI IT-Grundschutz / ISO 27001)	Mischform	Information und Kommunikation	13 Jahre	15 Jahre	Kunden (als Prüf- und Beratungsleistung)	Deutschland (überwiegend)
15	Leiter Solution Architect	Mischform	Erbringung von freiberuflichen [...] Dienstleistungen	7 Jahre	> 10 Jahre	Eigene Organisation & Kunden	Deutschland (überwiegend)

Expertenverständnis über den Begriff „Cloud-Anwendung“



Betrieb als **Software-as-a-Service** (SaaS) (bspw. Microsoft Office 365)



Betrieb von **VMs in der Public Cloud** als Infrastructure-as-a-Service (IaaS)



Betrieb von **Containern** (Docker und/oder Kubernetes)



Entwicklung und Betrieb einer **Web-Anwendung**



Entwicklung und Betrieb einer **selbstheilenden Anwendung**



Entwicklung und Betrieb einer **skalierbaren Anwendung**



Entwicklung auf **Basis von Cloud Services** bzw. Platform-as-a-Service (PaaS) und/oder Mischformen

Strategische Perspektive (potenzielle Erfolgsfaktoren)



Cloud- und Plattform-Strategie: Aufbau eines Ökosystems: „Cloud sicher konsumierbar machen“



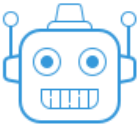
State und Compliance: Abhängigkeiten zu US-amerikanischen Cloud Providern managen



Security Trainings und Sicherheitskultur: ... etablieren und zwar bereits vor dem Projektgeschäft!



Sicherer Baukasten: Geprüfte Bausteine für Entwickler bereitstellen.



Automation von Entwicklung, Deployment und Test: Tools und CI/CD-Pipeline voll ausschöpfen



Standards, Prozesse und Richtlinien: Rahmenwerk zur Gewährleistung sicherer Softwareprodukte



Softwareentwickler/innen: Selbstverantwortung, Freiräume, Events, Weiterbildungsmöglichkeiten, Wertschätzung, Belohnung, Maßregelungsprozess

Operative Perspektive (potenzielle Erfolgsfaktoren)



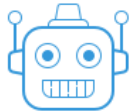
Security Trainings und Sicherheitskultur: „Aber nur wenn das Projektgeschäft es zulässt ...“



Sicherer Baukasten: „Security ... darum haben sich schon andere gekümmert ...“



Security Audits: Trügerisches Sicherheitsgefühl - „Am Ende schaut eh noch jemand einmal drauf ...“



Tools: „Frühzeitig Tools und Automatisierung verwenden ...“



Security als Pflicht: „Deal with it – da muss jeder Entwickler durch ...“



Verwendung von Standard-Implementierungen: „Sicherheitsfunktionen nicht neu implementieren.“

Agenda

- Motivation und Relevanz
- Problemstellung und Forschungsfragen
- Ziel und Ergebnis der Promotion
- Methodisches Vorgehen
- Ergebnisse der Expertenstudie
- Implikationen für die Praxis

Implikationen für die Praxis

Hinweis: Die Ergebnisse der Expertenstudie sind nicht repräsentativ für Organisationen mit Sitz in Deutschland. Es handelt sich um eine erste vorsichtige Annäherung - qualitativ-explorative Studie (!):

Mögliche Handlungsempfehlungen für die Praxis (strategisch und operativ):

1. Cloud Services als Plattform/Ökosystem/Baukasten sicher (!) konsumierbar machen
2. Freiräume für Softwareentwickler/innen zur Weiterbildung schaffen und nutzen (!)
3. Potentiale der Cloud ausschöpfen – nicht nur auf Lift-and-shift reduzieren
4. Automation und Tools frühzeitig nutzen – es lohnt sich!
5. Verwendung von Standard-Sicherheit-Implementierungen

Vielen Dank!

Marc Aurel Schubert, M.Sc.

Doktorand InnoProm IT Security und Datenschutz in der Cloud

E marc.schubert@hs-mainz.de | T 0049 172 933 78 79 | wimm.hs-mainz.de

ISO 27001 Lead Auditor (IRCA)

BSI IT-Grundschutz Praktiker

Spezielle Prüfverfahrenskompetenz für § 8a BSIg

ITSM Projekt Award 2017 e. V. Winner (Project Lead)

Forschungsgruppe Wirtschaftsinformatik und Medienmanagement

Prof. Dr. Sven Pagel - Fachbereich Wirtschaft

Hochschule Mainz - University of Applied Sciences

Lucy-Hillebrand-Straße 2 | 55128 Mainz | Raum A0.22

Lizenzhinweis: Diese Präsentation enthält Symbole von Icons8.



innoprom-security.eu

Literatur (1/4)

A Fuqun Huang, B Bin Liu, & C Bing Huang. (2012). A Taxonomy System to Identify Human Error Causes for Software Defects. <https://doi.org/10.13140/2.1.4528.5445>

Acar, Y., Fahl, S., & Mazurek, M. L. (2016). You are Not Your Developer, Either: A Research Agenda for Usable Security and Privacy Research Beyond End Users. 2016 IEEE Cybersecurity Development (SecDev), 3–8. <https://doi.org/10.1109/SecDev.2016.013>

Aljawarneh, S. A., Alawneh, A., & Jaradat, R. (2017). Cloud security engineering: Early stages of SDLC. *Future Generation Computer Systems*, 74, 385–392. <https://doi.org/10.1016/j.future.2016.10.005>

Assal, H., & Chiasson, S. (2018). Security in the software development lifecycle. *Fourteenth Symposium on Usable Privacy and Security*, 281–296.

Baumgarth, C., Eisend, M., & Evanschitzky, H. (2009). Empirische Mastertechniken. In C. Baumgarth, M. Eisend, & H. Evanschitzky (Hrsg.), *Empirische Mastertechniken* (S. 3–26). Gabler Verlag. https://doi.org/10.1007/978-3-8349-8278-0_1

Bedner, M. (2013). *Cloud Computing: Technik, Sicherheit und rechtliche Gestaltung*. Kassel University Press.

Benbasat, I., & Zmud, R. W. (1999). Empirical Research in Information Systems: The Practice of Relevance. *MIS Quarterly*, 23(1), 3–16. JSTOR. <https://doi.org/10.2307/249403>

Bertalanffy, L. (1949). Zueiner allgemeinen Systemlehre. *Biologia Generalis*, 19, 114–129.

Bogner, A., Littig, B., & Menz, W. (2014). *Interviews mit Experten: Eine praxisorientierte Einführung*. Springer-Verlag.

Bundesamt für Sicherheit in der Informationstechnik. (2018, November 8). IT-Grundschutz—Glossar und Begriffsdefinitionen [Informationswebsite]. BSI - Glossar - IT-Grundschutzkataloge. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html

Buxmann, P., Hess, T., & Lehmann, S. (2008). Software as a Service. *WIRTSCHAFTSINFORMATIK*, 50(6), 500–503. <https://doi.org/10.1007/s11576-008-0095-0>

Carvalho, C. A. B. de, Andrade, R. M. de C., Castro, M. F. de, Coutinho, E. F., & Agoulmine, N. (2017). State of the art and challenges of security SLA for cloud computing. *Computers & Electrical Engineering*, 59, 141–152. <https://doi.org/10.1016/j.compeleceng.2016.12.030>

Chen, D., & Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. 2012 International Conference on Computer Science and Electronics Engineering, 1, 647–651. <https://doi.org/10.1109/ICCSEE.2012.193>

CVSS Special Interest Group (SIG). (2019). Common Vulnerability Scoring System v3.1: Specification Document. https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf

Daschmann, H.-A. (1994). *Erfolgsfaktoren/Erfolgsfaktoren mittelständischer Unternehmen: Ein Beitrag zur Erfolgsfaktorenforschung*. Stuttgart.

Davenport, T., & Markus, M. (1999). Rigor vs Relevance Revisited: Response to Benbasat and Zmud. *Management Information Systems Quarterly - MISQ*, 23. <https://doi.org/10.2307/249405>

Dekker, M. A. C., Liveri, D., European Union, & European Network and Information Security Agency. (2015). *Cloud security guide for SMEs: Cloud computing security risks and opportunities for SMEs*. ENISA. <http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115227:EN:HTML>

Derbyshire, R., Green, B., Prince, D., Mauthe, A., & Hutchison, D. (2018). An Analysis of Cyber Security Attack Taxonomies. 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 153–161. <https://doi.org/10.1109/EuroSPW.2018.00028>

Literatur (2/4)

- Dodson, D. (2019). Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF). 23.
- Eckert, C. (2013). IT-Sicherheit: Konzepte—Verfahren—Protokolle. De Gruyter. <https://books.google.de/books?id=ysvpBQAAQBAJ>
- Ermakova, T. (2015). Security and Acceptance of Cloud Computing in Healthcare. 138.
- European Network and Information Security Agency. (2014). Security Framework for Governmental Clouds. ENISA.
- Eurostat. (2018). Cloud computing services used by more than one out of four enterprises in the EU. <https://ec.europa.eu/eurostat/documents/2995521/9447642/9-13122018-BP-EN.pdf/731844ac-86ad-4095-b188-e03f9f713235>
- Evans, M. G. (1970). The effects of supervisory behavior on the path-goal relationship. *Organizational Behavior and Human Performance*, 5(3), 277–298. [https://doi.org/10.1016/0030-5073\(70\)90021-8](https://doi.org/10.1016/0030-5073(70)90021-8)
- Fehling, C., Leymann, F., Retter, R., Schupeck, W., & Arbitter, P. (2014). *Cloud Computing Patterns*. Springer Vienna. <https://doi.org/10.1007/978-3-7091-1568-8>
- Fehling, C., Leymann, F., Rütshlin, J., & Schumm, D. (2012). Pattern-Based Development and Management of Cloud Applications. *Future Internet*, 4(1), 110–141. <https://doi.org/10.3390/fi4010110>
- Freiling, F., Grimm, R., Großpietsch, K.-E., Keller, H. B., Mottok, J., Münch, I., Rannenber, K., & Saglietti, F. (2014). Technische Sicherheit und Informationssicherheit: Unterschiede und Gemeinsamkeiten. *Informatik-Spektrum*, 37(1), 14–24. <https://doi.org/10.1007/s00287-013-0748-2>
- Fuchs, H. (1972). Systemtheorie. In K. Bleicher (Hrsg.), *Organisation als System* (S. 47–57). Gabler Verlag. https://doi.org/10.1007/978-3-322-86022-4_3
- Gentile, M., Collette, R., & August, T. D. (o. J.). *The CISO Handbook*. 103.
- Gondrom, T. (2014). CISO Survey and Report 2013. 29.
- Grobauer, B., Kossakowski, K.-P., & Schreck, T. (2016). Klassifikation von IT-Sicherheitsvorfällen. *Datenschutz und Datensicherheit - DuD*, 40(1), 17–21. <https://doi.org/10.1007/s11623-016-0536-7>
- Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding Cloud Computing Vulnerabilities. *IEEE Security & Privacy Magazine*, 9(2), 50–57. <https://doi.org/10.1109/MSP.2010.115>
- Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(1), 5. <https://doi.org/10.1186/1869-0238-4-5>
- Homans, G. C. (1958). Social Behavior as Exchange. *American Journal of Sociology*, 63(6.), 597–606.
- House, R. J. (1971). A path goal theory of leader effectiveness. *Administrative science quarterly*, 321–339.
- House, R. J., & Mitchell, T. R. (1975). Path-goal theory of leadership. WASHINGTON UNIV SEATTLE DEPT OF PSYCHOLOGY.

Literatur (3/4)

- Houy, C., Frank, J., Niesen, T., Fettke, P., & Loos, P. (2014). Zur Verwendung von Theorien in der Wirtschaftsinformatik – Eine quantitative Literaturanalyse. 88.
- ISO. (2013). ISO/IEC 27001 Information Security Management. <https://www.iso.org/isoiec-27001-information-security.html>
- ISO/IEC/IEEE. (2017). ISO/IEC/IEEE Systems and software engineering Vocabulary. ISO/IEC/IEEE 24765:2017(E), 1–541. <https://doi.org/10.1109/IEEESTD.2017.8016712>
- Ivkic, I., Pichler, H., Zsilak, M., Mauthe, A., & Tauber, M. (2019). A Framework for Measuring the Costs of Security at Runtime: Proceedings of the 9th International Conference on Cloud Computing and Services Science, 488–494. <https://doi.org/10.5220/0007761604880494>
- Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing (NIST SP 800-144). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-144>
- Kao, T.-C., Mao, C.-H., Chang, C.-Y., & Chang, K.-C. (2012). Cloud SSDLC: Cloud Security Governance Deployment Framework in Secure System Development Life Cycle. 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 1143–1148. <https://doi.org/10.1109/TrustCom.2012.106>
- Karam, Y., Baker, T., & Taleb-Bendiab, A. (2012). Security Support for Intention Driven Elastic Cloud Computing. Proceedings of the 2012 Sixth UKSim/AMSS European Symposium on Computer Modeling and Simulation, 67–73. <https://doi.org/10.1109/EMS.2012.17>
- Kissel, R. (2019). NIST Special Publication 800-64 Revision 2, Security Considerations in the System Development Life Cycle. 68.
- Kuntze, N., Rudolph, C., Brisbois, B., Boggess, M., Endicott-Popovsky, B., & Leivesley, S. (2015). Safety vs. Security: Why do people die despite good safety? 2015 Integrated Communication, Navigation and Surveillance Conference (ICNS), 1–13. <https://doi.org/10.1109/ICNSURV.2015.7121276>
- Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST Cloud Computing Reference Architecture (Special Publication 500-292).
- Martens, B., & Teuteberg, F. (2011). Risk and Compliance Management for Cloud Computing Services: Designing a Reference Model. 17th Americas Conference on Information Systems 2011, AMCIS 2011, 3.
- Mayring, P. (2014). Qualitative content analysis: Theoretical foundation, basic procedures and software solution.
- McKay, M. (2016). The Virtual Desktop Infrastructure Handbook—Everything You Need To Know About Virtual Desktop Infrastructure. Emereo Publishing.
- Mell, P., & Grance, T. (2011). NIST Definition of Cloud Computing.
- Microsoft. (2018). About Microsoft SDL. <https://www.microsoft.com/en-us/securityengineering/sdl/about>
- Moody, G. D., Siponen, M., University of Jyväskylä, Pahlila, S., & University of Oulu. (2018). Toward a Unified Model of Information Security Policy Compliance. MIS Quarterly, 42(1), 285–311. <https://doi.org/10.25300/MISQ/2018/13853>
- Müller, K.-R. (2018). IT-Sicherheit mit System: Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement – Sichere Anwendungen – Standards und Practices. Springer Fachmedien Wiesbaden. <https://doi.org/10.1007/978-3-658-22065-5>
- Papazoglou, M. P., & Heuvel, W.-J. van den. (2011). Blueprinting the Cloud. IEEE Internet Computing, 15(6), 74–79. <https://doi.org/10.1109/MIC.2011.147>

Literatur (4/4)

Pols, A., & Vogel, M. (2019). Bitkom Cloud Monitor 2019.

Reinheimer, S., & Springer Fachmedien Wiesbaden GmbH (Hrsg.). (2018). Cloud Computing: Die Infrastruktur der Digitalisierung. Springer Vieweg.

Repschläger, J., Pannicke, D., & Zarnekow, R. (2010). Cloud Computing: Definitionen, Geschäftsmodelle und Entwicklungspotenziale. HMD Praxis der Wirtschaftsinformatik, 47(5), 6–15. <https://doi.org/10.1007/BF03340507>

Sandberg, B. (2016). Wissenschaftliches Arbeiten von Abbildung bis Zitat: Lehr- und Übungsbuch für Bachelor, Master und Promotion. De Gruyter.

Schreiner, M., Hess, T., & Benlian, A. (2015). Gestaltungsorientierter Kern oder Tendenz zur Empirie? Zur neueren methodischen Entwicklung der Wirtschaftsinformatik (Arbeitsbericht, Institut für Wirtschaftsinformatik und Neue Medien, Fakultät für Betriebswirtschaft, Ludwig-Maximilians-Universität 1/2015). Ludwig-Maximilians-Univ., Inst. f. Wirtschaftsinformatik u. Neue Medien. <http://hdl.handle.net/10419/109029>

Sens, B., Fischer, B., Bastek, A., Eckardt, J., Kaczmarek, D., Pietsch, B., Rath, S., Ruprecht, T., Thomeczek, C., Veit, C., & Wenzlaff, P. (2007). Begriffe und Konzepte des Qualitätsmanagements—3. Auflage. 76.

Smith, P. C. (1974). The development of a method of measuring job satisfaction: The Cornell studies. Studies in personnel and industrial psychology (3rd ed.). Homewood, IL: Dorsey.

Suryateja, P. S. (2018). Threats and Vulnerabilities of Cloud Computing A Review. International Journal of Computer Sciences and Engineering, 6(3), 297–302. <https://doi.org/10.26438/ijcse/v6i3.297302>

Teh, P.-L., Ahmed, P. K., & D'Arcy, J. (2015). What Drives Information Security Policy Violations among Banking Employees?: Insights from Neutralization and Social Exchange Theory. Journal of Global Information Management, 23(1), 44–64. <https://doi.org/10.4018/jgim.2015010103>

Tung, Y., Tseng, S., & Kuo, Y. (2015). A testing-based approach to SLA evaluation on cloud environment. 2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS), 495–498. <https://doi.org/10.1109/APNOMS.2015.7275375>

Uygur, S. U. (2014). Penetration Testing with BackBox. Packt Publishing. <https://books.google.de/books?id=1M7kAgAAQBAJ>

Waidner, M. (2013). Entwicklung sicherer Software durch Security by Design. 76.

Watson, M. R., Shirazi, N., Marnarides, A. K., Mauthe, A., & Hutchison, D. (2016). Malware Detection in Cloud Computing Infrastructures. IEEE Transactions on Dependable and Secure Computing, 13(2), 192–205. <https://doi.org/10.1109/TDSC.2015.2457918>

Wilde, T., & Hess, T. (2007). Forschungsmethoden der Wirtschaftsinformatik. 8.

Witschey, J., Zielinska, O., Welk, A., Murphy-Hill, E., Mayhorn, C., & Zimmermann, T. (2015). Quantifying developers' adoption of security tools. Proceedings of the 2015 10th Joint Meeting on Foundations of Software Engineering - ESEC/FSE 2015, 260–271. <https://doi.org/10.1145/2786805.2786816>

Wurster, G., & van Oorschot, P. C. (2008). The developer is the enemy. Proceedings of the 2008 Workshop on New Security Paradigms - NSPW '08, 89. <https://doi.org/10.1145/1595676.1595691>

Xiao, S., Witschey, J., & Murphy-Hill, E. (2014). Social influences on secure development tool adoption: Why security tools spread. Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing - CSCW '14, 1095–1106. <https://doi.org/10.1145/2531602.2531722>

Zhang, T. (2018). Detection and Mitigation of Security Threats in Cloud Computing. 273.