Magdeburger Journal zur Sicherheitsforschung

Gegründet 2011 | ISSN: 2192-4260
Herausgegeben von Stefan Schumacher
Erschienen im Magdeburger Institut für Sicherheitsforschung
http://www.sicherheitsforschung-magdeburg.de/publikationen/journal.html

Was ist Informationssicherheit?

Positionierung, Chancen und Risiken

Dr. Hubert Feyrer

Es werden die Besonderheiten von Informationen aufgezeigt und ihr Wert als schützenswertes Gut dargestellt. Informationssicherheit wird erklärt und in Bezug zu verwandten Begriffen gesetzt. Aspekte der Umsetzung lassen Raum für individuelle Entscheidungen um Chancen zu nutzen und Risiken zu bekämpfen. Dabei ist Risikomanagement ein zentrales Instrument.
Keywords: Sicherheit, Informationssicherheit, Information, Datenschutz, Risikomanagement

Citation: Feyrer, H. (2018). Was ist Informationssicherheit? Positionierung, Chancen und Risiken. *Magdeburger Journal zur Sicherheitsforschung*, *15*, 871–878. Zugriff 19. Februar 2018, unter http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS_058_Feyrer_Sicherheit.pdf

1 Motivation

Verfolgt man Mainstream-Medien oder gar die sogenannte Fachpresse, so zeigt sich, dass die Begrifflichkeiten von Sicherheit, IT-Sicherheit, Informationssicherheit, Datenschutz, Datensicherheit und Cybersicherheit immer wieder kunterbunt gemischt werden. Bei näherer Betrachtung sind diese Begriffe in der Tat nicht sehr trennscharf[1]. Aufgrund der rechtlichen Grundlage des Bundesdatenschutzgesetzes sind »Datenschutz« und »Datensicherheit« relativ klar umrissen[2][3][4]. Vor allem die Begriffe »Informationssicherheit« und »IT-Sicherheit« werden jedoch häufig gleichgesetzt, wobei auch hier unterschieden werden muss.

Im Folgenden werden diese beiden Begriffe in Bezug zueinander gesetzt, um sie durch diese Positionierung begrifflich zu festigen. Weiterhin wird der Bezug zum Datenschutz und der dort angesiedelten Datensicherheit dargestellt.

Der Fokus liegt hier darauf, Information als zu schützenden Wert zu betrachten, wobei auf eine Besonderheit eben dieser Informationen eigegangen wird. Im Weiteren werden die Aspekte für den Schutz sowie eine individuelle Abschätzung beim Vorgehen dazu aufgezeigt.

Dieser Überblicksartikel stellt den Gesamtzusammenhang dar, ohne sich in Details zu verlieren. Für Umsetzung und Details sei auf weiterführende Literatur verwiesen[5][6].

2 Der Wert von Informationen

Abbildung 1 zeigt die zentrale Bedeutung von Informationen in Unternehmensabläufen, die Zusammenhänge sind dabei wie folgt.

»Information« ist kein Ding das man anfassen, hören, riechen, schmecken oder sonstwie sinnlich erfassen kann. Die begriffliche Nähe zu »Daten« und »Wissen« hilft wenig beim Verständnis[7][8][9]. Um »Informationen« näher zu greifen soll deswegen die Abgrenzung in Abbildung 1 vorgenommen werden, und so der Wert von Informationen dargelegt werden.

Um das ungreifbare Ding »Information« zu speichern und zu verarbeiten werden technische Systeme benötigt – Informationstechnik oder kurz »IT« in Form von Computern, Hardware[10]. Diese Computersysteme – egal ob Smartphone, Tablet, Notebook, Desktop, Serversysteme – können wahlweise im Fachhandel, beim Elektronik-Discounter oder gar im Supermarkt erworben werden. Diese Computer sind jedoch erst durch die auf ihnen gespeicherten und verarbeiteten Informationen individuell und dadurch wertvoll[11].

Ergänzt werden diese einzelnen Computer heute durch Netzwerke zur Datenübertragung und durch Speichersysteme zur zentralen Ablage von Informationen[12]. Dies gilt vor allen in größeren Verbünden zur Informationsverarbeitung, wie sie in heutigen Wirtschaftsunternehmen gegeben sind. Genau wie Computer sind diese Netze und Speicher ebenso ohne die Informationen käuflich zu erwerben, und erhalten erst durch die auf ihnen gespeicherten Informationen an Wert.

Wie sich zeigt ist »Information« ohne die sie speichernde Hardware nichts. Aber wie wird etwas bearbeitet das nicht greifbar ist? Es gibt kein Werkzeug, keinen Hammer und keinen Schraubendreher der (grob vereinfacht) 1en und 0en Manipulieren kann. Stattdessen geschieht dies heute durch Software – Anwendungen, Computerprogramme[13]. Je nach Sinn und Art der zu verarbeitenden Informationen kann diese Software in Form von Standardanwendungen oder auch von eigens entwickelten, sehr spezifischen Programmen geschehen. Ohne die verarbeiteten Informationen ist jedoch jede Software »nur« ein Teil der Maschine zur Automatisierung von Abläufen, und Wert entsteht erst durch die Anwendung der nachvollziehbaren, wiederholbaren und kostengünstigen Automatisierung dieser Abläufe[14].

Die genannten Abläufe entstehen selten zufällig, sondern stellen Firmenabläufe – Geschäftsprozesse – dar, die es verlässlich im Sinne eines gegebenen Unternehmenszieles auszuführen gilt[15]. Unabhängig davon ob in den Abläufen Dinge produziert oder Dienste geleistet werden unterstützen Sie am Ende das Ziel des Unternehmens, Geld zu verdienen. Dazu benötigt werden im Kern die Informationen die von der Software manipuliert und auf der Hardware und Infrastruktur verarbeitet, übertragen und gespeichert werden wie in Abbildung 1 dargestellt[16].

In diesem Zusammenhang zeigt sich, dass Prozesse, Hard- und Software sowie Infrastruktur nichts sind ohne die sie verbindenden Informationen. Information ist entsprechend ein zentraler Wert und gilt als schützenswert um einen Zustand von »Sicherheit« dieser Informationen herzustellen[17][18]. Im Folgenden wird gezeigt wie dies erreicht werden kann.

1 Spitta und Bick (2008) S. 45ff
2 Zeugner (2016)
3 dtv (2016)
4 Bundesministerium des Inneren (2016)
5 Wikipedia (2016a) Informationssicherheit: Mindmap
6 Klipper (2015) S. 13ff
7 Kuhlen, Semar, und Strauch (2014) S. 1f, S. 265ff
8 Gleick (2012) S. 28
9 Janich (2006) S. 42
10 Schneider (2012) S. 30ff und S. 90ff
11 Linde (2005) S. 12
12 Schneider (2012) S. 119ff und S. 302ff
13 Schneider (2012) S. 38ff, S. 45ff und S. 78ff
14 Schneider (2012) S. 27
15 Bernd Pfitzinger und Thomas Jestädt (2016) S. 44
16 Bernd Pfitzinger und Thomas Jestädt (2016) S. 421ff und S. 549ff
17 Schneider (2012) S. 488ff
18 Spitta und Bick (2008) S. 65ff

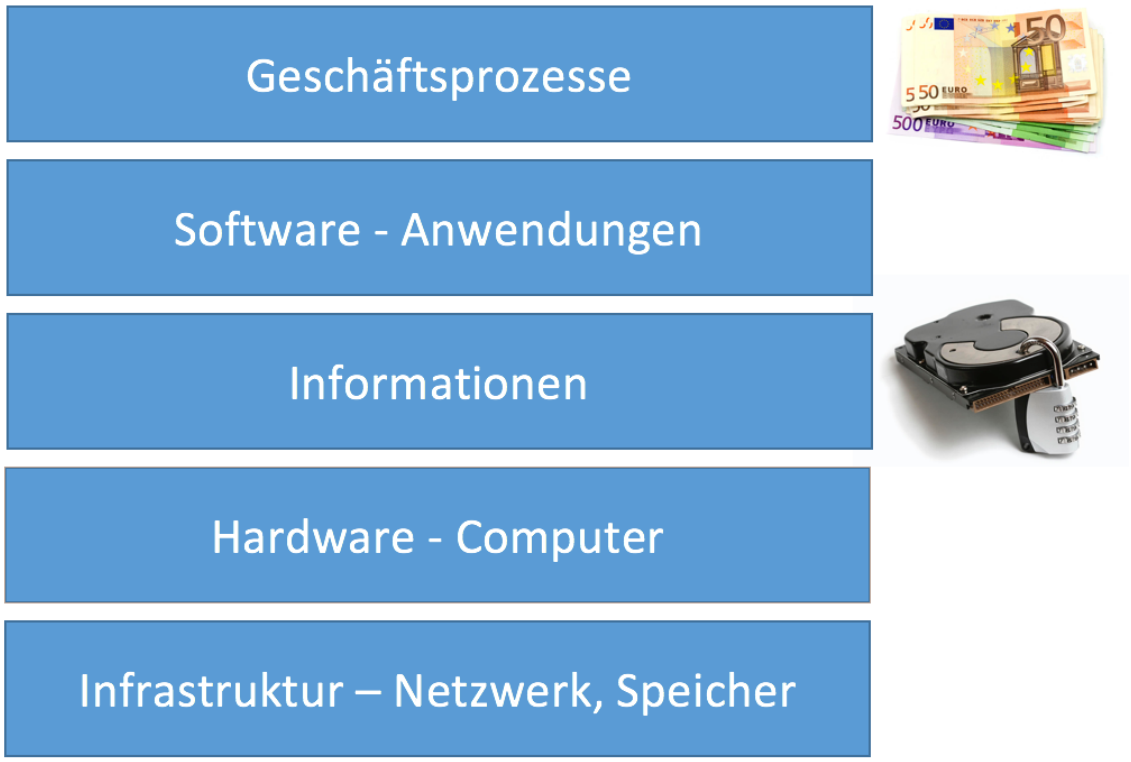

Abbildung 1: Information im Kontext

3 Schutz von Information als Wert

Beim Schutz von Informationen und der sie verarbeitenden Systeme (Hardware, Software etc.) wird schnell die Assoziation von »IT« – Informations*technik* – zu »IT-Sicherheit« hergestellt. »IT« ist hier als die informationsverarbeitende Technik zu verstehen, entsprechend ist »IT-Sicherheit« auch als Satz von Maßnahmen zu verstehen, die sich auf diese technischen Einrichtungen beziehen. Virenscanner, EMail-Verschlüsselung und Firewalls sind hier als Beispiele zu nennen[19][20]. Dies sind heute wichtige Komponenten ohne die (leider) kein Auskommen mehr ist. Aber reicht dies?

Wie sich zeigt: Nein. Werden in heutigen Unternehmen zwar viele Abläufe technisch automatisiert und können entsprechend durch technische Maßnahmen gesichert werden, so besteht dennoch – je nach Unternehmen – weiterhin ein großer Teil an Abläufen, die manuell von Menschenhand ausgeführt werden müssen. Und wo gearbeitet wird, da geschehen nun einmal Fehler. Verhindert werden kann dies durch »kluges« – sicheres – Vorgehen. Damit hier nicht jeder Mitarbeiter das Rad neu für sich und seinen Tätigkeitsbereich erfinden muss, werden bereichs- und firmenweite Regelungen erstellt. Diese Regelungen bilden die *Organisation*, und entsprechende Maßnahmen unterstützen die sichere Erstellung, Verarbeitung, Übertragung und Speicherung von Informationen über die reine Technik hinaus[21][22][23][24].

All diese organisatorischen Regelungen und ihre Einhaltung sind jedoch nichts ohne den dritten und wichtigsten Faktor der nicht vergessen werden darf: der Mensch. Die Mitarbeiter und Ihnen allen voran das Management sind für Bedrohungen zu sensibilisiert und müssen regelmäßig über die korrekten Prozessschritte und ihre Bedeutung zum Schutz von Informationen geschult werden[25][26][27][28].

Letztendlich ist für den Schutz von Informationen erst die Beachtung aller drei Faktoren – Technik, Organisation, Mensch – zusammen zielführend[29]. Dies wird unter dem Begriff »Informationssicherheit« zusammengefasst[30][31], mit den drei Aspekten IT-Sicherheit, Security Awareness und Organisationssicherheit für Maßnahmen in den Bereichen Technik, Organisation

19 Feyrer (2012a)

20 Eckert (2014) S. 643ff

21 Bundesministerium der Justiz (2016a) BGB §§823, 831, 31

22 Bundesministerium der Justiz (2016b) HGB §347

23 Stephan Grüninger, Jantz, Schweikert, und Steinmeyer (2011) S. 7f

24 Weber, Rüdiger Kabst, und Baum (2015) S. 107ff

25 Mitnick und Simon (2003) S. 245ff

26 Hadnagy (2016) S. 339ff

27 Weber u. a. (2015) S. 305ff

28 Jörg Stender (2016) S. 107ff

29 Klipper (2015) S. VIII und S. 37ff

30 ISO/IEC (2013)

31 Libmann (2016) S. 15ff

und Mensch[32]. Abbildung 2 zeigt diesen Zusammenhang[33].

Hinsichtlich der häufigen Vermischung der Begriffe ist hier also klar festzuhalten, dass »Informationssicherheit« als Oberbegriff weit mehr ist als »IT-Sicherheit«[3435].

Dieser Sachverhalt ist auch in den aktuell existierenden Berufsbezeichnungen zu beobachten. Der Fokus eines IT-Sicherheitsbeauftragten ist eher technischer Natur, während bei einem Chief Information Security Officer (CISO) der vollumfängliche Schutz aller Informationen durch Betrachtung (auch) von Prozessen und organisatorischen Regelungen sowie der Sensibilisierung aller Mitarbeiter in der Bezeichnung festgelegt ist[3637].

Begrifflich ist noch darauf hinzuweisen, dass die Sicherheit der Technik mit den Schlagworten »IT-Sicherheit« bzw. Englisch »IT-Security« belegt ist, und ebenso die Sensibilisierung der Menschen als »Security Awareness« bezeichnet wird. Lediglich für den größten – und erfahrungsgemäß am ehesten unterschätzten – Bereich der organisatorischen Sicherheitsmaßnahmen existiert kein eigener, etablierter Begriff. Der Terminus »Organisationssicherheit« sollte hier verstärkt etabliert werden, auch wenn dies einerseits wenig sexy klingt und andererseits auch mit anderen Bereichen der Unternehmensorganisation verschwimmen[3839]. Findigen Geistern bietet sich hier ein Feld für eine kreative Wortschöpfung!

4 Datenschutz?

Es bleibt festzuhalten, dass Informationen von Wert sind. Dies betrifft sowohl Informationen mit als auch ohne Personenbezug. Erstere werden in Deutschland durch das Bundesdatenschutzgesetz (BDSG) vor dem Hintergrund der informationellen Selbstbestimmung geschützt[404142].

»Datenschutz« ist also der Schutz personenbezogener Daten und Informationen, »Informationssicherheit« wiederum mehr als »nur« Datenschutz, da dort alle Informationen im Fokus stehen, nicht nur die mit Personenbezug.

Die im Datenschutz verankerten technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten werden oft als »Datensicherheit« bezeichnet[4344]. Die Fokuspunkte Technik, Organisation und Mensch zur Etablierung der Informationssicherheit decken also auch die Datensicherheit ab. Das Schaffen von Informationssicherheit deckt also auch Datensicherheit als Schutz und die Sicherheit von personenbezogenen Daten ab[4546].

5 Risiken und Chancen

Werte sind zu schützen um sie zu erhalten. Zu Schützen ist vor Bedrohungen von außen und innen sowie durch inhärente Schwachstellen. Schutzmaßnahmen können gegen diese helfen. Bedrohungen und Schwachstellen können mit einer bestimmten Wahrscheinlichkeit bzw. Häufigkeit zu negativen Beeinträchtigungen führen, deren Schadenshöhe angegeben werden kann. Man spricht bei dieser Kombination aus Schadenshöhe und Wahrscheinlichkeit von »Risiken«[4748].

Diese Risiken mit ihren Faktoren zu kennen bildet die Grundlage für den Schutz von Werten. Dies stellt kein leichtes Unterfangen dar: Schwachstellen können versteckt und verdeckt in Produkten (Hardware, Software) enthalten sein, Bedrohungen werden ständig neu in einem Rat Race zwischen Angreifer und Verteidiger entdeckt. Und selbst wenn all dies bekannt ist, so sind Gegenmaßnahmen oft nicht kostenlos. Schutzmaßnahmen wird man wohl kaum nach dem Gießkannenprinzip verteilen. Letztendlich muss abgeschätzt werden was teurer ist – einen Schaden hinzunehmen, oder Geld für eine Schutzmaßnahme auszugeben. Spätestens jenseits des Schadenswertes wird eine Schutzmaßnahme unrentabel - die sprichwörtliche Kanone mit der auf Spatzen geschossen wird[49].

In der Praxis ist diese Grenze jedoch wesentlich weniger klar, und die Erfahrung zeigt, dass die Bereitschaft, ein Risiko einzugehen, durchaus gegeben ist. Das heißt es geschieht (leider) öfters als gedacht, dass Risiken bzw. die damit verbundene Schwachstellen und Bedrohungen ohne Gegenmaßnahmen akzeptiert werden. Der mögliche Schaden wird dann entsprechend nach dem Sankt-Florians-Prinzip billigend in Kauf genommen werden, in der Hoffnung, dass der Ernstfall schon nicht eintreten werden[50]. Dem

32 Aufmerksamen Leser die an dieser Stelle die Erfüllung rechtlicher und regulatorischer Auflagen vermissen werden diese bei den technischen und organisatorischen Maßnahmen sowie bei der Sensibilisierung wiederfinden. Die detaillierte Ableitung ist zentrale Aufgabe des IT Compliance Managements, das im Rahmen der Informationssicherheit zu etablieren ist, um entsprechende Bedrohungen durch die Nicht-Erfüllung dieser Auflagen zu vermeiden

33 Feyrer (2012b) S. 326

34 Czernik (2016)

35 Kosutic (2016)

36 ISACA (2016) S. 7f

37 Hohl (2016)

38 Obrst, Chase, und Markeloff (2012)

39 Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2016) Technische und organisatorische Maßnahmen: Abgrenzung technisch und organisatorisch

40 Bundesministerium des Inneren (2016)

41 Bundesministerium der Justiz (2009)

42 Witt (2010) S. 47ff

43 Witt (2010) S. 102

44 Wikipedia (2016b) Informationssicherheit: Teilaspekte, Verwandte Begriffe

45 Wikipedia (2016b) Man beachte die Weiterleitung von »Datensicherheit« zu »Informationssicherheit«

46 Libmann (2016) S. 33ff

47 Klipper (2015) S. 1

48 Freiling u. a. (2016) S. 16f

49 Klipper (2015) S. 155ff

50 Klipper (2015) S. 87ff und S. 136f

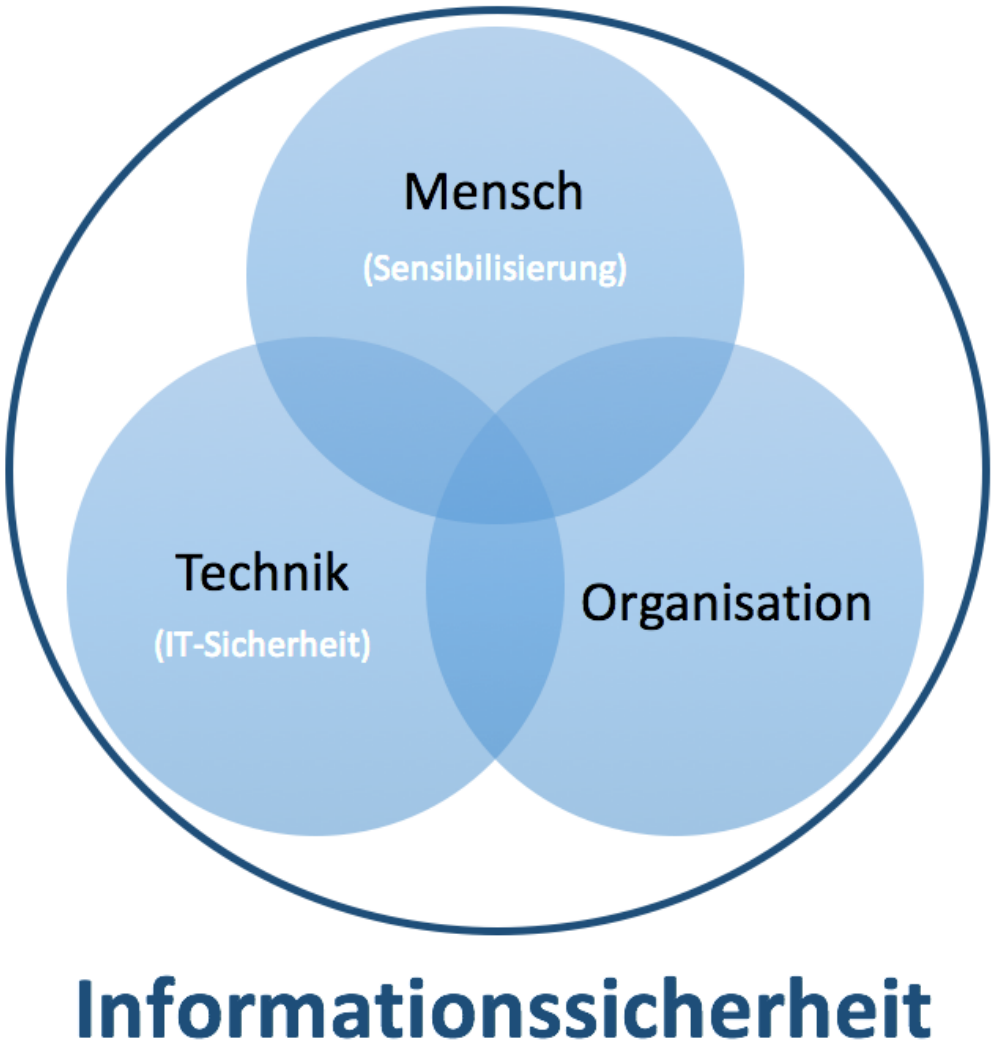

Abbildung 2: Schutz von Informationen

ist durch geeignete Sensibilisierung von Mitarbeitern und Management entgegenzuwirken.

An dieser Stelle tritt die subjektive Komponente des Risikomanagements, der sogenannte »Risikoappetit« zum Vorschein. Je nach handelnden Akteuren kann dieser eher konservativ und vorsichtig oder mutig sein[51]. Erstere sind mehr auf Sicherheit bedacht und eher bereit, Geld für Schutz auszugeben und kein Risiko einzugehen. Letztere sparen Geld für teure Schutzmaßnahmen aber riskieren entsprechende Ausfälle. In Unternehmen ist dieser Risikoappetit Teil der Unternehmensstrategie, und oft auch durch Gesetze und regulatorische Auflagen vorgegeben – eine Bank kann es sich z.B. nicht leisten, allzu leichtfertig mit dem Geld ihrer Kunden umzugehen.

Für weiterführende Ausführungen sei hier auf diverse Standardvorgehen zum Risikomanagement wie den ISO Normen 31000[52] und 27005[53], dem Standard BSI 200-3 des Bundesamts für Sicherheit in der Informationstechnik (BSI)[54] sowie dem Vorgehen des Committee of Sponsoring Organizations of the Treadway Commission (COSO)[55] verwiesen. Regulatorische Auflagen sind zum Beispiel für den Bankensektor in Basel III[56] und in den Mindestanforderungen an das Risikomanagement MaRisk[57] zu finden.

Risikomanagement als solches bietet ein gutes Werkszeug, um Werte zu schützen, auch über Informationswerte hinausgehend. Es ist aber nicht kostenlos! Es bedeutet Aufwand und benötigt den Willen zur Transparenz[58]. Oft wird gefragt »wieviel Stück verkaufen wir mehr mit Risikomanagement«. Diese Frage ist falsch formuliert, Risikomanagement kann beantworten wieviel Stück im Notfall *weniger* verkauft werden. Ein vorausschauender Unternehmer sollte sich dafür interessieren – letztendlich ist eine Aussagefähigkeit »(Im Fall X) produzieren wir Y Stück weniger« die Entscheidungsgrundlage, um Risiken einzugehen oder eher Chancen für Innovation und Entwicklung zu nutzen[59].

6 Ausblick

Dieser Artikel hat in bewusst groben Zügen die Themen um Informationen als Wert, Informationssicherheit und die Steuerung von Risiken und ihre Zusammenhänge aufgezeigt. Die individuelle Bewertung muss je nach Situation geschehen.

Dazu existiert eine Vielzahl an Artikeln, Vorgehensmodellen, Gesetzen und Standards. In diesem Dschungel fehlt jedoch oft der Überblick. Dieser ist hoffentlich mit diesem Artikel geschaffen.

Für die Umsetzung ist ein Überblick über alle vorhandenen Informationen und die Ziele der Organisation zu gewinnen. Um die Kronjuwelen von der Streu zu trennen können Informationen klassifiziert werden, um nicht alles nach dem Gießkannenprinzip zu schützen.

Eine Bedrohungs- und Schwachstellenanalyse (z.B. VDA Information Security Assessment (ISA)[60], FMEA[61], Checklisten von Herstellern wie Kaspersky[62] und viele weitere[63]) sollte dann Aufschluß über bestehende Risiken geben, die dann mit gezielten, wirtschaftlich vertretbaren Maßnahmen abgestellt werden.

Dies alles ist kein statisches, einmaliges Vorgehen und muss – basierend auf der Geschwindigkeit in der sich die Bedrohungslage ändert – ständig aktualisiert werden. In manchen Bereichen mit langfristigem Fokus, in anderen jedoch auch mit schneller Reaktion auf auftretende Situationen[64].

7 Über den Autor

Dr. Feyrer hat technische Informatik studiert und in Informationswissenschaft promoviert. Er arbeitet als Chief Information Security Officer (CISO) und Risk Manager bei einem europaweit tätigen Prozess- und Personaldienstleister der die Automotive-Branche bedient.

51 Klipper (2015) S. 75ff

52 ISO/IEC (2009)

53 ISO/IEC (2011)

54 Bundesamt für Sicherheit in der Informationstechnik (2016)

55 Committee of Sponsoring Organizations of the Threadway Commission (2016)

56 Bank for International Settlements (2016)

57 Bundesanstalt für Finanzdienstleistungsaufsicht (2012)

58 Klipper (2015) S. 155ff

59 Klipper (2015) S. 160ff

60 Verband der Automobilindustrie (2016)

61 Werdich (2012) S. 21

62 Kaspersky UK (2016)

63 Klipper (2015) S. 107

64 Deming (1986) S. 86ff

Literaturverzeichnis

Bundesanstalt für Finanzdienstleistungsaufsicht (Herausgeber). (2012). Rundschreiben 10/2012 (BA) – Mindestanforderungen an das Risikomanagement – MaRisk. Zugriff 31. Juli 2016, unter https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/rs_1210_marisk_ba.html

Bank for International Settlements (Herausgeber). (2016). Organisation and governance: Risk Management. Zugriff 31. Juli 2016, unter http://www.bis.org/about/risk_management.htm

Bernd Pfitzinger & Thomas Jestädt. (2016). *IT-Betrieb: Management und Betrieb der IT im Unternehmen*. Wiesbaden: Sprinter Vieweg Verlag.

Bundesamt für Sicherheit in der Informationstechnik. (2016). BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz. Zugriff 3. Januar 2017, unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/IT-Grundschutz-Modernisierung/GS_Standards/gs_standards_node.html

Bundesministerium der Justiz. (2009). Bundesdatenschutzgesetzt (BDSG). Zugriff 29. Mai 2011, unter http://www.gesetze-im-internet.de/bdsg_1990/

Bundesministerium der Justiz. (2016a). Bürgerliches Gesetzbuch (BGB). Zugriff 31. Juli 2016, unter http://www.gesetze-im-internet.de/bgb/

Bundesministerium der Justiz. (2016b). Handelsgesetzbuch (HGB). Zugriff 31. Juli 2016, unter http://www.gesetze-im-internet.de/hgb/

Bundesministerium des Inneren. (2016). Der Schutz des Rechts auf informationelle Selbstbestimmung. Zugriff 30. Juli 2016, unter http://www.bmi.bund.de/DE/Themen/Gesellschaft-Verfassung/Datenschutz/Informationelle-Selbstbestimmung/informationelle-selbstbestimmung_node.html

Committee of Sponsoring Organizations of the Threadway Commission (Herausgeber). (2016). Guidance on Enterprise Risk Management (Website). Zugriff 31. Juli 2016, unter http://www.coso.org/-erm.htm

Czernik, A. (2016). Unterschied zw. IT-Sicherheit, Datensicherheit, Datenschutz & Informationssicherheit. Zugriff 31. Juli 2016, unter https://www.datenschutzbeauftragter-info.de/unterschiede-zwischen-datenschutz-datensicherheit-informationssicherheit-oder-it-sicherheit/

Deming, W. E. (1986). *Out of the Crisis*. New York, USA: McGraw-Hill Inc.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (Herausgeber). (2016). Datenschutz-Wiki: Technische und organisatorische Maßnahmen. Zugriff 31. Juli 2016, unter https://www.bfdi.bund.de/bfdi_wiki/index.php/Technische_und_organisatorische_Ma%C3%9Fnahmen

dtv (Herausgeber). (2016). *DatSchR - Datenschutzrecht: 8. Auflage*. München: dtv Verlag.

Eckert, C. (2014). *IT-Sicherheit: Konzepte – Verfahren – Protokolle*. Oldenburg: De Gruyter Verlag.

Feyrer, H. (2012a). IT-Security mit Open Source. *FreeX*.

Feyrer, H. (2012b). Über den Umgang mit Unsicherheit. *Magdeburger Journal zur Sicherheitsforschung*, *4*(2), 323–342. Zugriff 31. Juli 2016, unter http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS-020.pdf

Feyrer, H. (2018). Was ist Informationssicherheit? Positionierung, Chancen und Risiken. *Magdeburger Journal zur Sicherheitsforschung*, *15*, 871–878. Zugriff 19. Februar 2018, unter http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS_058_Feyrer_Sicherheit.pdf

Freiling, F., Rüdiger Grimm, Großpietsch, K.-E., Keller, H. B., Jürgen Mottock, Isabel Münch, ... Saglietti, F. (2016). Technische Sicherheit und Informationssicherheit: Unterschiede und Gemeinsamkeiten. *Informatik-Spektrum*, *37*(1). Zugriff 31. Juli 2016, unter https://fb-sicherheit.gi.de/fileadmin/gliederungen/fb-sec/AKBegriffsbildungIS-1-2014.pdf

Gleick, J. (2012). *The Information: A History, a Theory, a Flood*. New York City, USA: Harpercollins Publishers.

Hadnagy, C. (2016). *Social Engineering: The Art of Human Hacking* (1. Auflage). Weinheim: Wiley Verlag.

Hohl, P. (Herausgeber). (2016). SecuPedia: Sicherheitsberufe. Zugriff 31. Juli 2016, unter http://www.secupedia.info/wiki/Sicherheitsberufe

ISACA (Herausgeber). (2016). Information Security Career Progression: Survey Results 2008. Zugriff 31. Juli 2016, unter http://www.isaca.org/Knowledge-Center/Research/Documents/InfoSec-Career-Survey-Results_res_Eng_0508.pdf

ISO/IEC. (2009). *ISO 31000: Risk management - Prinziples and guidelines*. Geneva, Schweiz: International Organization for Standardization.

ISO/IEC. (2011). *ISO/IEC 27005: Information security risk management*. Geneva, Schweiz: International Organization for Standardization.

ISO/IEC. (2013). *ISO/IEC 27001: Information security management systems – Requirements*. Geneva, Schweiz: International Organization for Standardization.

Janich, P. (2006). *Was ist Information?* Berlin: Suhrkamp Verlag.

Jörg Stender. (2016). *Betriebliches Weiterbildungsmanagement: Ein Lehrbuch*. Stuttgart: S. Hirzel Verlag.

Kaspersky UK (Herausgeber). (2016). IT-Gesundheitscheck. Zugriff 31. Juli 2016, unter http://www.kaspersky.co.uk/ithealthcheck

Klipper, S. (2015). *Information Security Risk Management: Risikomanagement mit ISO/IEC 27001, 27005 und 31010* (2. Auflage). Wiesbaden: Springer Verlag.

Kosutic, D. (2016). Information Security or IT Security? Zugriff 31. Juli 2016, unter http://www.infosecisland.com/blogview/5482-Information-Security-or-IT-Security.html

Kuhlen, R., Semar, W., & Strauch, D. (2014). *Grundlagen der praktischen Information und Dokumentation: Handbuch zur Einführung in die Informationswissenschaft und praxis*. Oldenburg: De Gruyter Verlag.

Libmann, J. (2016). *Informationssicherheit: kompakt, effizient und unter Kontrolle* (3. Auflage). Berlin: Neopubli Verlag.

Linde, F. (2005). *Ökonomie der Information*. Göttingen: Universitätsdrucke Göttingen.

Mitnick, K. D. & Simon, W. L. (2003). *The Art of Deception: Controlling the Human Element of Security*. Weinheim: Wiley Verlag.

Obrst, L., Chase, P., & Markeloff, R. (2012). Developing an Ontology of the Cyber Security Domain. Zugriff 31. Juli 2016, unter http://ceur-ws.org/Vol-966/STIDS2012_T06_ObrstEtAl_CyberOntology.pdf

Schneider, U. (Herausgeber). (2012). *Taschenbuch der Informatik* (7. Auflage). München: Hanser Verlag.

Spitta, T. & Bick, M. (2008). *Informationswirtschaft: Eine Einführung*. Heidelberg: Springer Verlag.

Stephan Grüninger, Jantz, M., Schweikert, C., & Steinmeyer, R. (2011). Organisationspflichten: eine Synopse zum Begriffsverständnis und den daraus abzuleitenden Anforderungen an Aufsichts- und Sorgfaltspflichten aus juristischer und betriebswirtschaftlicher Perspektive. Zugriff 31. Juli 2016, unter https://opus.htwg-konstanz.de/files/180/KICG_Forschungspapier_4_Organisationspflichten.pdf

Verband der Automobilindustrie. (2016). Informationssicherheit: Informationsschutz und Risk Management: Informationsschutz-Sicherheitsanforderungen in der Automobilindustrie / ISO 2700x. Zugriff 31. Juli 2016, unter https://www.vda.de/de/themen/sicherheit-und-standards/informationssicherheit/informationssicherheit-sicherheitsanforderungen.html

Weber, W., Rüdiger Kabst, & Baum, M. (2015). *Einf+hrung in die Betriebswirtschaftslehre* (9. Auflage). Heidelberg: Springer Verlag.

Werdich, M. (2012). *FMEA – Einführung und Moderation: Durch systematische Entwicklung zur übersichtlichen Risikominimierung (inkl. Methoden im Umfeld)*. Heidelberg: Springer Verlag.

Wikipedia. (2016a). Informationssicherheit: Mind Map. Zugriff 30. Juli 2016, unter https://de.wikipedia.org/wiki/Informationssicherheit#/media/File:Mind_map_of_information_security.svg

Wikipedia. (2016b). Informationssicherheit. Zugriff 30. Juli 2016, unter https://de.wikipedia.org/wiki/Informationssicherheit

Witt, B. C. (2010). *Datenschutz kompakt und verständlich: Eine Praxisorientierte Einführung* (2. Auflage). Wiesbaden: Vieweg+Teubner Verlag.

Zeugner, V. (2016). Ein Modell für Datenschutz durch Datensicherheit. *Datenschutz und Datensicherheit - DuD*, *40*(7). Zugriff 30. Juli 2016, unter http://link.springer.com/article/10.1007/s11623-016-0635-5