Heft 38 | Dezember 2023 | 17. Jahrgang | ISSN 1864-6557

IT-GOVERNANCE

Fachzeitschrift des ISACA Germany Chapter e.V.



AUSZUG
AUS HEFT 38

Informations-, IT- und Cybersicherheit – Zusammenhänge, Entwicklungen und Auswirkungen auf Unternehmen

Ingo Struckmeyer, Marc Weber

ISACA Germany Chapter

dpunkt.verlag | it-governance.dpunkt.de | isaca.de

Heft 38 | 2023

IT-GOVERNANCE

Fachzeitschrift des ISACA Germany Chapter e.V.

Inhalt

Fachthemen

2 **Informations-, IT- und Cybersicherheit – Zusammenhänge, Entwicklungen und Auswirkungen auf Unternehmen**
Ingo Struckmeyer, Marc Weber

5 **Die Umsetzung der NIS-2-Richtlinie in Deutschland – Adressaten, Pflichten und andere wichtige Inhalte**
Carsten Beisheim, Michael Herold

11 **KI-basierte Anomaly Detection in der Revision**
Andrei Todea, Robert Birk

16 **Darstellung einer Methodik zur Quantifizierung von Informationssicherheitsrisiken am Beispiel von FAIR**
Sebastian Hoffmann

Rubriken

22 Zum Thema
Nach Microsoft-Schlüssel-Diebstahl aus Crash-Dump – neues IT-Audit-Prüfthema: IT-Diagnose-Daten
Stephen Fedtke

28 Standards
Mit DORA zu einer erhöhten Resilienz des europäischen Finanzsektors
Lucas Pausewang

31 **Veranstaltungen**

35 **Aus den ISACA-Fachgruppen**

36 **Inserenten**

36 **Vorschau**

36 **Impressum**

Informations-, IT- und Cybersicherheit – Zusammenhänge, Entwicklungen und Auswirkungen auf Unternehmen

Ingo Struckmeyer, Marc Weber

Informationen sind Vermögenswerte (Assets) von Unternehmen, Behörden und sonstigen Organisationen. Der Schutz dieser Vermögenswerte ist das Kernziel aller Bestrebungen im Kontext von Informations-, IT- und Cybersicherheit. Im aktuellen öffentlichen Diskurs sind die Begrifflichkeiten inzwischen allgegenwärtig. Dabei ist es für die Empfänger der medialen Botschaften nicht immer einfach, die überlappenden Begriffe trennscharf zu unterscheiden. Das hat unterschiedliche Ursachen. So hängt zum Beispiel die Nutzung vom konkreten Kontext ab. Häufig werden die Begrifflichkeiten auch synonym verwendet. Dieser Beitrag hat es sich zur Aufgabe gemacht, den Leserinnen und Lesern die unterschiedlichen Aspekte aufzuzeigen und die Begriffe vor allem für den Unternehmensalltag genauer herauszuarbeiten. Dabei soll neben einer Definition der Begriffe auch auf deren Unterschiede und Gemeinsamkeiten eingegangen werden.

1 Begriffsdefinitionen

Informationssicherheit betrifft den Schutz von Informationen in sämtlichen Dimensionen. Dabei ist es nicht entscheidend, wie die Informationen gespeichert sind – auf Papier, auf einem Datenträger oder in sonstiger Form. Informationen werden dabei als interpretierte Daten verstanden.

Sichergestellt wird dies durch den Schutz relevanter Informationen hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit. Dies ergibt sich für viele Unternehmen verpflichtend bereits aus unterschiedlichen rechtlichen bzw. regulatorischen Anforderungen. Dieser Schutz wird allgemein durch organisatorische, physische und technische Maßnahmen sowie entsprechende Vorgaben umgesetzt [Goeken & Roßbach 2013].

Die Kernkomponente der Informationssicherheit im Unternehmen ist das Informationssicherheits-Managementsystem (ISMS). Dieses ist für Unternehmen, die zu den kritischen Infrastrukturen zählen, verpflichtend, sollte jedoch für jedes Unternehmen mit schützenswerten Informationen selbstverständlich sein.

»Die *IT-Sicherheit* (IT-Security) bezieht sich auf die Gewährleistung von Sicherheit aller eingesetzten Informationstechniken bzw. -technologien (IT), d.h. aller Hardware- und Softwaresysteme bzw. aller Rechner- und Netzsysteme. Ziel ist die Sicherheit der Informationsverarbeitung und der Kommunikation, die korrekte Abläufe der Hardwareoperationen und der Software- bzw. Programmsysteme voraussetzt. Somit soll auch die Daten- bzw. die Informationssicherheit durch die IT-Sicherheit gegeben sein. Die IT-Sicherheit soll schließlich die Sicherheit bzw. Korrektheit aller Anwendungen gewährleisten, die durch IT unterstützt bzw. ausgeführt werden« [Gabriel 2023]. Somit bezieht sie sich auf einzelne Dateien, Computer, Netzwerke, Cloud-Dienste bis hin zu ganzen Rechenzentren. Die drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sind durch Maßnahmen in technischen und nicht technischen Systemen umzusetzen. Cybersicherheit (auch Cyber Security) gehört zur IT-Sicherheit. Die IT-Sicherheit ist eigentlich nur ein Teil der Informationssicherheit und bezieht sich auf elektronisch gespeicherte Informationen und IT-Systeme [BSI 2017, Kap. 2.3, S. 12].

Die *Cybersicherheit* umfasst große Teile der IT-Sicherheit. Sie bezieht den Begriff IT-Sicherheit nicht nur auf den internen Unternehmenskontext, sondern auch auf den gesamten Cyberraum. Im NIST-Framework [NIST 2023] ist Cyber Security beschrieben als: »Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.« Cybersicherheit (Cyber Security) spielt sich somit im Wesentlichen im Internet und/oder in Einflusssphären von Kollaborationspartnern, Lieferanten etc. ab. Die Gesamtheit dieser Sphären stellt abstrakt den Cyberraum (Cyberspace) dar.

Weitere Begriffe, die im Zusammenhang mit Informationssicherheit, IT-Sicherheit und Cyber Security immer eine Rolle spielen bzw. einen engen Zusammenhang hiermit bilden, sind der Datenschutz sowie das Risikomanagement bzw. insbesondere das IT-Risikomanagement.

Unter *Datenschutz* verstehen wir heute die Themengebiete, die mit der Europäischen Datenschutz-Grundverordnung (DSGVO) und dem nationalen Datenschutzrecht einen konkreten rechtlichen Rahmen besitzen. Gemeint ist damit eben nicht Datensicherheit, sondern im Kern das Recht auf informationelle Selbstbestimmung, der Schutz des Persönlichkeitsrechts bei der Datenverarbeitung und insbesondere der Schutz der Privatsphäre (Privacy). Es ist ein individueller Schutz vor staatlichen »Übergriffen« und der datenhungrigen Internetindustrie. In der DSGVO wird direkt auf den Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union verwiesen. Datenschutz ist somit nicht automatisch dinghaft oder gar ein digitales Asset [COC AG 2023].

Das *Risikomanagement* und somit auch das *IT-Risikomanagement* als Teil von diesem ist eine reaktive und proaktive Managementaufgabe. Hierzu wird ein Prozess implementiert, um Risiken in einem bestimmten Bereich des Unternehmens zu identifizieren, zu analysieren, zu bewerten, zu behandeln und zu überwachen. Das Risikomanagement dient der Vermeidung oder Verringerung aktueller und künftiger Geschäftsrisiken, der Vermeidung von Betrug und menschlichen Fehlern sowie der Sicherstellung der Einhaltung von gesetzlichen sowie aufsichtsrechtlichen Verpflichtungen [Knoll 2014]. Das IT-Risikomanagement soll dabei helfen, IT-Risiken frühzeitig zu erkennen und angemessen darauf zu reagieren, um damit zum Schutz des Unternehmens beizutragen.

Um auf Basis der Begriffsdefinitionen eine Abgrenzung der Begrifflichkeiten untereinander bzw. Überschneidungen derselben darzustellen, haben die Autoren eine schematische Übersicht der Zusammenhänge für die folgende Diskussion der Begrifflichkeiten erstellt (vgl. Abb. 1). Sie ist zur verständlicheren Einordnung der Begrifflichkeiten mit einem erweiterten Kontext dargestellt. Anhand der Schnittmengen zeigen die Autoren nachfolgend markante Unterschiede, Gemeinsamkeiten und Probleme auf. Hierbei liegt der Fokus auf den Begriffen Informationssicherheit, IT-Sicherheit und Cybersicherheit.

2 Begriffsabgrenzungen

Ein signifikanter Unterschied besteht im erweiterten Betrachtungsraum von Cybersicherheit. Es werden die gleichen Aspekte wie in der IT-Sicherheit betrachtet, jedoch erstreckt sich der Betrachtungsraum auch auf den gesamten Bereich des Internets und sämtlicher relevanter Netzwerke.

Begriffsvermischungen entstehen üblicherweise, weil ein sehr großer Teil aller genutzten, übertragbaren und verfügbaren Informationen elektronisch im Cyberraum existent ist. Das ist einer der Gründe, warum die Bereiche sich nicht separat voneinander betrachten lassen. Deshalb müssen sämtliche zur Informationsverarbeitung erforderlichen Komponenten mit in die Betrachtung einbezogen werden. Dabei handelt es sich zum Beispiel um Informationen, Anwendungen, Speichermedien, Netzwerke, Prozesse, Stromversorgung und Kommunikationsnetzwerke.

Der hier angeführte erweiterte Betrachtungshorizont der Cybersicherheit erfordert einen viel weiter gefassten Scope an effektiven Maßnahmen und dafür erforderlichen Skills. Dies inkludiert die Fähigkeiten eines Unternehmens oder einer Organisation, Bedrohungslagen zu erkennen, abzuwehren oder gegebenenfalls die Ausgangssituation wiederherzustellen. Die Bedrohungslagen im Kontext von Cybersicherheit verhalten sich zudem dynamisch. Im Vergleich dazu wirken IT-Sicherheitssituationen wegen des abgegrenzten Raumes eher »statisch«.

Darüber hinaus müssen Unternehmen und Organisationen ebenso in der Lage sein, ihre Fähigkeiten in Bezug auf Cybersicherheit ständig zu erweitern und zu verbessern und dies auch zu budgetieren. Die Aufrechterhaltung von Compliance und Cybersicherheit hat eine direkte Abhängigkeit zwischen Investitionsgeschehen und der unternehmerischen Leistungsfähigkeit.

Die regulatorischen Vorgaben stellen sich teilweise sehr unterschiedlich dar. Während zum Beispiel die Informationssicherheitsmaßnahmen zur Gewährleistung des Datenschutzes sehr eng reguliert sind, ist dies bei der IT-Sicherheit weiter

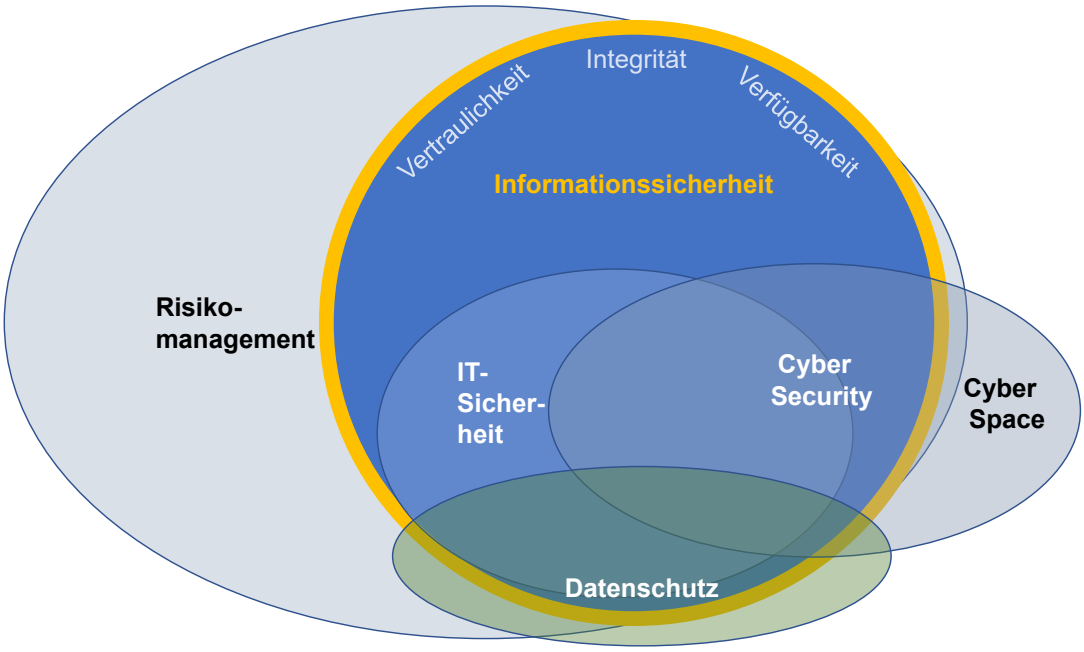


Abb. 1: Einordnung der Begrifflichkeiten Informations-, IT- und Cybersicherheit

gefasst, sodass die IT-Sicherheit größere Freiheitsgrade bei der Umsetzung durch unternehmenseigene Regeln und Richtlinien besitzt.

Die größten Gemeinsamkeiten zwischen den Ansätzen bestehen in der Zielstellung, Schäden zu vermeiden, die Systeme zu dokumentieren und sie kontinuierlich zu verbessern. Sämtliche Systematiken streben zudem einen definierten Sollzustand an. Dieser Sollzustand wird über permanente Verbesserung aktuell gehalten und erweitert.

Die signifikanteste Kongruenz liegt in der Bestrebung, die Vertraulichkeit, die Integrität und die Verfügbarkeit von Informationen sicherzustellen. Das hört sich zunächst nach einer plakativen Darstellung an. Erfahrungsgemäß hilft diese Sichtweise aber, um aus Entscheiderperspektive die Dimension und Tragweite der parallelen Managementsysteme zu durchdringen und zu strukturieren.

Aktivitäten lassen sich beispielsweise besser bündeln und aufeinander ausrichten, wenn sie ganzheitlich in einem Konzept zusammenfließen. Wertvolle personelle Ressourcen können so zielgenauer und effektiver eingesetzt werden. Mit dem Stichwort »Aktivitäten bündeln« möchten die Autoren auf eine weitere Gemeinsamkeit verweisen. Hierbei handelt es sich um den allgegenwärtigen Fach- und Führungskräftemangel. Dieser Mangel schlägt in den Bereichen Datenschutz, IT-Sicherheit und Cybersicherheit besonders zu Buche. Qualifizierte, erfahrene und verfügbare personelle Ressourcen sind Mangelware. Ein in dieser Situation oft kritischer Aspekt ist deshalb die strategische Planung der personellen Ausgestaltung für die organisatorische Implementierung. Das erforderliche Skill-Set für Informationssicherheits-/Security-Experten und Entscheider ist in großen Teilen nahezu identisch. Integrierte, aufeinander abgestimmte und automatisierte Kontrollsysteme erfordern anderes und weniger Personal als co-existente Kontrollsysteme mit weniger automatischer Unterstützung und einem hohen Anteil manueller Kontrolltätigkeiten.

Literatur

[BSI 2017] *Bundesamt für Sicherheit in der Informationstechnik (BSI):* BSI-Standard 200-2: IT-Grundschutz-Methodik, Version 1.0, 2017.

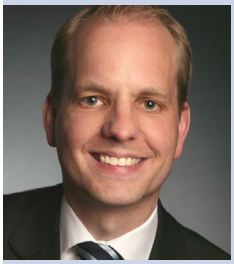
[COC AG 2023] *COC AG:* Datenschutz und Informationssicherheit, 2023; *https://www.coc-ag.de/managed-it-service-stories/datenschutz-und-informationssicherheit*; Zugriff am 21.10.2023.

[Gabriel 2023] *Gabriel, P. D.:* Definition IT-Sicherheit. Gabler Banklexikon. *https://www.gabler-banklexikon.de/definition/it-sicherheit-70719*; Zugriff am 20.10.2023.

[Goeken & Roßbach 2013] *Goeken, M.; Roßbach, P.:* Informationssicherheit und Informationssicherheitsmanagement – Grundlagen, Herausforderungen und methodische Unterstützung. IT-Governance 7 (2013), 14, S. 3-7.

[Knoll 2014] *Knoll, M.:* Praxisorientiertes IT-Risikomanagement – Konzeption, Implementierung und Überprüfung. dpunkt.verlag, Heidelberg, 2014.

[NIST 2023] *NIST Computer Security Resource Center:* Glossary – cybersecurity; *https://csrc.nist.gov/glossary/term/cybersecurity#:~:text=the%20prevention%20of%20damage%20to,and%20availability%20of%20these%20systems*; Zugriff am 21.10.2023.



Ingo Struckmeyer

ist selbstständiger Unternehmensberater und unterstützt Finanzdienstleistungsunternehmen insbesondere in den Bereichen Informationssicherheit und IT-Compliance sowie in regulatorischen Projekten. Er ist Diplom-Wirtschaftsinformatiker und verfügt über die Zusatzqualifikationen CISM, CGEIT, CISA und CIA sowie »ISO 27001 Practitioner – Information Security Officer«.

Dipl.-Wirtsch.-Inf. Ingo Struckmeyer
Rotbuchenstieg 39a
22297 Hamburg
is@ingostruckmeyer.com
www.ingostruckmeyer.com



Marc Weber

ist selbstständiger Unternehmensberater und begleitet Unternehmen bei der Umsetzung digitaler Strategien. In den Bereichen IT-Management, Financial Operations, Processes und Projektmanagement hat er Führungsaufgaben und Beratungsmandate für international tätige Unternehmen wahrgenommen. Er ist Diplom-Kaufmann und verfügt über die Zusatzqualifikationen CISA, CGEIT und CRISC.

Dipl.-Kfm. Marc Weber
TheDigitalization.com
Postfach 67 02 46
22342 Hamburg
marc.weber@thedigitalization.com
http://thedigitalization.com