Kommunikation & Recht

Schriftenreihe

Deusch/Eggendorfer

Beauftragte für IT-Sicherheit und Informationssicherheit

dfv Mediengruppe

R&W Fachmedien Recht und Wirtschaft

Kommunikation & Recht

Beauftragte für IT-Sicherheit und Informationssicherheit

von

Dr. Florian Deusch

und

Professor Dr. Tobias Eggendorfer

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.de abrufbar.

ISBN 978-3-8005-1873-9

dfv Mediengruppe

www.ruw.de

Druck: Beltz Grafische Betriebe GmbH, 99947 Bad Langensalza

Printed in Germany

Vorwort

„Ohne Sicherheit vermag der Mensch weder seine Kräfte auszubilden, noch die Frucht derselben zu geniessen; denn ohne Sicherheit ist keine Freiheit.“[1]

Was Wilhelm von Humboldt auf das Wesen eines Staates bezog, gilt gleichermaßen für die digitalisierte Wirtschaft und Gesellschaft. Ein IT-System, das seine Verarbeitungsprozesse nicht sicher ausführt, ist wertlos. Unsichere IT-Systeme verschaffen Unternehmen und Behörden keine Freiheit und keine Vorteile, sondern Misstrauen und Schäden. Sie hemmen die Produktivität, Innovation und Kreativität. Daher ist die Sicherheit von IT-Systemen und der damit verarbeiteten Informationen von zentraler Bedeutung für jede Organisation, sei es eine staatliche Stelle mit öffentlichem Auftrag oder ein Unternehmen.

Diese Sicherheit bedrohen Angriffe Krimineller auf IT-Systeme von Unternehmen, Politik und Behörden, Nachlässigkeiten von Nutzern oder schlicht Unsicherheiten im Umgang mit neuen Techniken. Das verursacht Personen- und Vermögensschäden und lähmt die Schaffenskraft innerhalb der betroffenen Organisation.

Verschiedene Normen und Standards beschreiben, wie Organisationen Informations- und IT-Sicherheit behandeln können. Wo solche Aufgaben bestehen, sind Personen notwendig, die sie erfüllen. Dies sind die Beauftragten für Informations- und für IT-Sicherheit einer Organisation.

Das vorliegende Werk gibt Aufschluss darüber, was Informations- und IT-Sicherheitsbeauftragte sind, welche Aufgaben sie erfüllen und wie sie ihre To-dos erledigen können. Die Autoren haben dabei die gesetzlichen Vorgaben und die Anforderungen in Management-Standards zugrunde gelegt sowie die aktuellen technischen Gegebenheiten. In die Darstellung sind auch die praktischen Erfahrungen der Autoren eingegangen, die sie im Laufe ihrer jeweiligen beruflichen Tätigkeit, in der Forschung und im Austausch mit Informationssicherheitsbeauftragten, IT-Sicherheitsbeauftragten, Datenschutzbeauftragten sowie IT-Sicherheitsbehörden gemacht haben.

Für Kritik, weitere Anregungen aus der Praxis und Feedback sind die Autoren dankbar.

Ravensburg/München, Januar 2024

Florian Deusch Tobias Eggendorfer

1 Wilhelm von Humboldt, Ideen zu einem Versuch, die Grenzen der Wirksamkeit des Staats zu bestimmen, Breslau, 1851, S. 45.

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
ACL	Access Control List
AES	Advanced Encryption Standard
AktG	Aktiengesetz
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
B3S	Branchenspezifische Sicherheitsstandards (durch das BSI genehmigt)
BNetzA	Bundesnetzagentur
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BSIG-E	Entwurf zur Änderung des BISG (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG)
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Drucksache des Deutschen Bundestags
dDOS	distributed Denial of Service
DES	Data Encryption Standard
DMARC	Domain-based Message Authentication, Reporting and Conformance
DORA	Digital Operational Resilience Act
DSGVO	Datenschutzgrundverordnung
EDV	Elektronische Datenverarbeitung
eIDAS	electronic IDentification, Authentication and trust Services
EnWG	Energiewirtschaftsgesetz
EuGH	Europäischer Gerichtshof
EU	Europäische Union
ETSI	European Telecommunication Standards Institute
GG	Grundgesetz
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
HTML	Hypertext Markup Language
HIDS	Host Intrusion Detection System
IEC	International Electrotechnical Commission

IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISB	Informationssicherheitsbeauftragter/Informationssicherheitsbeauftragte
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization/ Internationale Organisation für Normung
IT	Informationstechnologie
IT-SiBe	IT-Sicherheitsbeauftragter/IT-Sicherheitsbeauftragte
K&R	Kommunikation und Recht (Zeitschrift)
KAGB	Kapitalanlagegesetzbuch
KSchG	Kündigungsschutzgesetz
KWG	Kreditwesengesetz
KRITIS	Kritische Infrastruktur
LG	Landgericht
NIDS	Network Intrusion Detection System
NIS	Netz- und Informationssicherheit
OLG	Oberlandesgericht
PGP	Pretty Good Privacy
RAID	Redundant Array of Independent Disks
RL	Richtlinie
RSA	*Rivest–Shamir–Adleman* (asymmetrisches kryptographisches Verfahren, benannt nach seinen Erfindern)
S.	Seite, Satz
SGB	Sozialgesetzbuch
S/MIME	Secure/Multipurpose Internet Mail Extensions
SPF	Sender Permitted From
SSL	Secure Socket Layer
SQL	Structured Query Language
TI	Telematikinfrastruktur
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security
TOM	Technische und organisatorische Maßnahmen
URL	Uniform Resource Locator
USP	Unique Selling Proposition

VAG	Versicherungsaufsichtsgesetz
VO	Verordnung
VPN	Virtual Private Network
WpHG	Wertpapierhandelsgesetz
ZAG	Zahlungsdiensteaufsichtsgesetz

1. Einführung und Grundlagen

1.1. Ziele dieses Buchs

Egal ob mit oder ohne Erfahrung als Informationssicherheitsverantwortlicher ist es oft hilfreich, nachschlagen zu können, Checklisten zu finden, und kompakt das nötige Wissen in einem Buch zu finden. So ist das Buch als eine Einführung einerseits, eine Sammlung Aufbauwissens andererseits und zusätzlich als Hilfsmittel für die tägliche Arbeit mit Checklisten und weiteren Tools entstanden.

Dabei ist das Ziel, das Wissen griffbereit und praxisnah darzustellen, sofort umsetzbar, und womöglich auch so erklärt, dass einzelne Seiten für einen Entscheider leicht verständlich sein können. Denn häufig scheitert in der Praxis die Kommunikation zwischen Beratern und Verantwortlichen an der fehlenden gemeinsamen Sprache.[2]

Im Buch finden sich daher Handlungsempfehlungen in grau hinterlegten Kästen. Weiß hinterlegte Kästen enthalten Zusammenfassungen und Checklisten.

1.2. Was dieses Buch enthält

Dieser erste Abschnitt zeigt, was ein Informationssicherheitsbeauftragter (ISB) bzw. ein IT-Sicherheitsbeauftragter (IT-SiBe) ist, welche Aufgaben er hat und welche Qualifikationen er vorzuweisen hat.[3]

Der ISB/IT-SiBe bewegt sich dabei immer in einem Rahmen, der durch rechtliche Vorgaben und technische Gegebenheiten gesetzt ist. Daher ist dieses Buch in Zusammenarbeit eines Fachanwaltes für IT-Recht und eines Professors für IT-Sicherheit entstanden: Denn Recht und Technik sind gleich wichtig, um eine gute Lösung zu finden.

Daher stürzt sich Kapitel 2 auch umfangreich auf die technischen Grundlagen, ausführlich und kritisch. Nachfolgend stellt Kapitel 3 die Rechtsgrundlagen für die Arbeit des IT- und Informationssicherheitsbeauftragten dar.

---

2 Apropos Sprache: Sie werden im Buch sicher leicht erkennen, welcher der Autoren für welchen Abschnitt hauptsächlich verantwortlich war. So wie sich Juristen und Informatiker klischeehaft unterschiedlich kleiden, so drücken wir uns auch unterschiedlich aus. Etwas Kontrast darf sein, er belebt und hält die Diskussion im Gang, die nötig ist, um die inhaltlichen Vorstellungen beider Welten zusammenzuführen.

3 Zur erleichterten Lesbarkeit nutzt die vorliegende Darstellung das generische Maskulin für die Berufsbezeichnung „Informationssicherheitsbeauftragter/IT-Sicherheitsbeauftragter“, die alle Personen jeglichen Geschlechts (m/w/d) einschließt, die diese Aufgabe wahrnehmen.

Das vierte Kapitel hilft als eine Art Nachschlagewerk für die verschiedenen Arbeitsgebiete, die nötigen Ansprechpartner und Behörden zu identifizieren.

Weil gerade im IT-Bereich die One-Man-Show beliebt ist und auch in den Köpfen steckt, dass selbstverständlich ein Informatikprofessor jederzeit Bildbearbeitung in allen Finessen beherrscht, jedes defekte Windowsgerät in Gang bringt und nebenbei auch WLANs installieren kann, grenzt Kapitel fünf ab: Wer ist wofür verantwortlich, wie sind die Claims abgesteckt.

Das sechste und letzte Kapitel entwickelt aus den vorhergehenden Kapiteln To-do-Listen, wie sich die Arbeit organisieren lässt.

Der Anhang enthält Musterverträge, mit denen ein ISB/IT-SiBe beauftragt werden kann. Die Regelungen für interne und externe ISB/IT-SiBe sind einander gegenübergestellt.

1.3. Was sind ISB/IT-SiBe?

Der Einsatz von IT ist nur sinnvoll, wenn die IT und die damit verarbeiteten Informationen verfügbar, integer und vertraulich sind. Mit anderen Worten: sicher. Grund genug, für die Leitung einer Organisation, bestimmte Personen mit der Aufgabe der IT- bzw. Informationssicherheit zu beauftragen – die IT-Sicherheitsbeauftragten bzw. Informationssicherheitsbeauftragten.

Der ISB bzw. IT-SiBe erfüllt seine Aufgaben immer innerhalb einer bestimmten Organisation, dies kann ein privates oder staatlich getragenes Unternehmen sein oder eine öffentlich-rechtliche Einheit wie eine Behörde, Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts.

Obwohl es rechtliche Pflichten gibt, IT- und Informationssicherheitsbeauftragte zu bestellen (unten Ziffer 3.1), sind die Bezeichnungen gesetzlich nicht definiert und werden auch außerhalb gesetzlicher Normen nicht einheitlich verwendet.

Ein sehr wichtiges untergesetzliches Konvolut an Management-Normen zur IT-Sicherheit sind die BSI-Standards zum IT-Grundschutz. Der BSI-Standard 200-2 trifft Aussagen über ISB und IT-SiBe.

Hinweis: Das BSI ist eine Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Inneren und für Heimat (BMI) (www.bmi.bund.de). Es ist die zentrale Stelle für Informationssicherheit auf nationaler Ebene in Deutschland (§ 1 BSIG). Das BSI hat verschiedene Empfehlungen und Standards zur IT- und Informationssicherheit auf seiner Webseite veröffentlicht (www.bsi.de). Mit den BSI-Standards zum

IT-Grundschutz hat das BSI eine Methodik beschrieben, mit der eine Organisation ihre Ziele und Schutzmaßnahmen zur Informationssicherheit festlegen kann. Die BSI-Standards sind Teil des IT-Grundschutzes (näher dazu unten Ziffer 3.3.2). Im Gegensatz zu vielen anderen Standards sind die Empfehlungen des IT-Grundschutzes kostenfrei verfügbar. Der IT-Grundschutz ist mit der verbreiteten Norm ISO/IEC 27001 kompatibel und deckt deshalb das Vorgehen gemäß ISO/IEC 27001 mit ab.

Laut BSI-Standard 200-2 des IT-Grundschutzes ist der **ISB von der Organisationsleitung eingesetzt** und **zentraler Ansprechpartner** für die **Koordination, Verwaltung** und **Kommunikation** des Prozesses „**Informationssicherheit**". Dabei erfasst die Informationssicherheit alle Arten von Informationen, unabhängig davon, ob sie mithilfe von IT verarbeitet werden oder nicht. Der **IT-SiBe** ist für die **Sicherheit der IT (IT-Infrastruktur und IT-Betrieb)** zuständig. Dazu kann es auch gehören, für die **technische Umsetzung von Maßnahmen** zu sorgen, die der ISB zur Informationssicherheit definiert hat.[4]

> *Beispiel: Der ISB hat sich auch um die Sicherheit von Informationen zu kümmern, die in gedruckter Form körperlich wahrnehmbar sind, zum Beispiel vertrauliche Vertragsunterlagen in Papierform.*
>
> *Der IT-SiBe ist nach diesem Verständnis nicht für die Sicherheit von Papierunterlagen zuständig. Wenn die Vertragsdokumente aber eingescannt werden, muss der IT-SiBe für die Verfügbarkeit, Vertraulichkeit und Integrität der Scan-Dateien sorgen.*

Außerhalb des IT-Grundschutzes des BSI werden die Aufgaben der Informations- und IT-Sicherheit nicht immer den Titeln ISB und IT-SiBe zugeschrieben. Bisweilen werden die Begriffe ISB und IT-SiBe synonym verwendet oder der ISB ist auch für die infrastrukturelle IT-Sicherheit verantwortlich. Es gibt auch Organisationen, die ihrem IT-SiBe die Verantwortung für die Informationssicherheit insgesamt zuweisen. Wieder andere Organisationen bezeichnen ihre Verantwortliche für die Informationssicherheit als (Chief) Information Security Officer – (C)ISO – oder Informationssicherheitsmanager (ISM).

Der Informationssicherheitsstandard ITIL (Information Technology Infrastructure Library, ursprünglich von der britischen Regierung stammend)

4 Die Vorgängerversion BSI-Standard 100-1 bezog sich ausschließlich auf den IT-SiBe; die Funktion des ISB und seine Abgrenzung zum IT-SiBe nimmt der IT-Grundschutz erstmals im BSI-Standard 200-2 (Ziffer 4) vor.

weist die Informationssicherheit der Verantwortung des Information Security Managers zu.[5]

Hinweis: Einige Unternehmen haben ihre Führungsebene nach sogenannten „C-Levels" strukturiert. „C" steht dabei für „Chief" und kennzeichnet eine Führungsposition. Chief Executive Officer (CEO) bezeichnet die Gesamtleitung (Geschäftsführer bzw. Vorstandsvorsitzender). Daneben gibt es bereichs- und aufgabenspezifische Führungspositionen, z. B. Chief Operating Officer (zweiter Geschäftsführer/ Vorstand, meist für das Tagesgeschäft zuständig) und Chief Financial Officer (Leitung des Rechnungswesens). Auch Spezialaufgaben werden je nach Bedeutung im Unternehmen dem C-Level zugeordnet bzw. dort geschaffen, z. B. der Chief Digital Officer für die Digitalisierung im Unternehmen, Chief Information Officer (CIO) oder Chief Technology Officer (CTO) für die IT.[6]

Ein „Chief Information Security Officer" sollte daher klären, welcher Führungsebene er zugeordnet ist. Je nach Weisungskompetenzen im Unternehmen kann ein CISO auch dem Vorstand bzw. der Geschäftsführung zugeordnet sein. In einer solchen Position arbeitet ein CISO nicht nur Empfehlungen aus, sondern trägt die Entscheidungs- und Haftungsverantwortung (siehe unten Ziffer 1.6).

Stets ist die Funktion des ISB/IT-SiBe an eine bestimmte Person gebunden, und zwar an eine natürliche Person iSd § 1 BGB. Denn die Benennung als ISB oder IT-SiBe dient laut BSI-Standard 200-2 dazu, Ansprechpartner und Zuständigkeiten für die Aufgaben der Informations- und IT-Sicherheit der Organisation zu bestimmen. Juristische Personen, z. B. GmbHs, können dagegen keine ISB oder IT-SiBe sein. Sie können der Organisation allenfalls ihre Dienstleistungen anbieten, indem sie der Organisation einen Mitarbeiter bereitstellen, der dort als externer ISB/IT-SiBe tätig wird (siehe dazu unten Ziffer 3.2.3).

Je nach Aufgabe und Größe der Organisation werden auch gesonderte ISB bzw. IT-SiBe für spezifische Bereiche betraut. Unternehmen, die industrielle Steuerungen (Industrial Control Systems – ISC) einsetzen, bestellen z. B. ISC-ISB (dazu unten Ziffer 3.3.2).

5 Ebel, Basiswissen ITIL 4 (2021), S. 295 ff.

6 Zur Verortung des „Chief Digital Officers" auf die Vorstands- bzw. Geschäftsführungsebene: Dahm/Winter, Die Rolle des CDO in der digitalen Transformation (2023), S. 15 ff.

Zusammenfassung: Ein ISB ist eine natürliche Person, welche die Leitung einer Organisation als zentraler Ansprechpartner zur Informationssicherheit beauftragt hat. Der IT-SiBe verantwortet die Sicherheit der IT-Infrastruktur und des IT-Betriebs einer Organisation.

Die Titel sind gesetzlich nicht definiert; in der Praxis ist entscheidend, welche Aufgaben dem bzw. der Beauftragten zugewiesen sind.

1.4. Überblick über die Aufgaben

Das Wichtigste an den Aufgaben von IT-SiBe und ISB ist:

Die Leitung der Organisation muss die Aufgaben des ISB/IT-SiBe definieren. Denn es gibt keinen gesetzlichen oder sonst allgemeingültigen Aufgabenkatalog. Das passende Mittel zur Definition dieser Aufgaben ist der Vertrag oder die Bestellungsurkunde des ISB/IT-SiBe (siehe dazu unten Ziffer 3.2).

Üblicherweise ist der ISB in einer Organisation verantwortlich für ein systematisches Vorgehen zur Informationssicherheit. Einschlägige Management-Normen (IT-Grundschutz des BSI sowie ISO 27001) verlangen die Einrichtung, den Betrieb und die Weiterentwicklung eines **Informations-Sicherheits-Management-Systems (ISMS)**. Der BSI-Standard 200-2 verlangt vom ISB sogar, dass er die Informationssicherheit in der Organisation vorantreibt.

Für den IT-SiBe gilt Entsprechendes in Bezug auf die IT-Infrastruktur und den IT-Betrieb, sofern sein Aufgabenbereich dahingehend begrenzt ist (zur „Blaupause“ des IT-SiBe gemäß § 166 TKG siehe unten Ziffer 3.1.2).

Hinweis: Wie ein ISB/IT-SiBe diese Aufgaben strukturiert angehen kann, ist in Ziffer 6 unten dargestellt.

ISB und IT-SiBe sind indes keine Entscheidungsträger in der Organisation. Die generelle Aufgabe und Letztverantwortung, Informations- und IT-Sicherheit zu betreiben, trägt stets die Leitung der Organisation. Der ISB/IT-SiBe kann und muss dabei Ziele und Maßnahmen vorschlagen, die Entscheidung über die Verbindlichkeit der Ziele und Umsetzung der Maßnahmen hat aber die Organisationsleitung zu treffen.

> *Ein Beispiel: Der Außendienstmitarbeiter eines Unternehmens stimmt mit seinem Vorgesetzten die Reiseroute für die kommende Woche per E-Mail ab. Bei unverschlüsselter E-Mail-Kommunikation besteht das*

> *Risiko, dass unbefugte Dritte die E-Mails lesen und manipulieren. Das geeignete Mittel zur Herabsetzung dieses Risikos ist eine Ende-zu-Ende-Verschlüsselung der E-Mails. Der ISB/IT-SiBe kann und muss der Organisationsleitung die Risiken und Optionen zur Risikovermeidung aufzeigen; ob die Ende-zu-Ende-Verschlüsselung aber umgesetzt wird, hat die Leitung selbst zu entscheiden. Maßgeblich dafür ist, welchen Wert die Leitung der Reiserouten-Kommunikation beimisst, wie hoch sie das Risiko des unbefugten Zugriffs einstuft und wie sie die Folgen einer Realisierung des Risikos einstuft.*[7]

Um der Aufgabe der Informations- und IT-Sicherheit Herr zu werden, bietet sich für ISB/IT-SiBe folgende **Unterscheidung** an:[8]

- **Initiale Aufgaben**, die zu Beginn der Tätigkeit als ISB/IT-SiBe zu erledigen sind, insbesondere die Erhebung des IST-Stands mit Erhebung und Analyse der Risiken, Erstellung eines hierauf beruhenden IT-Sicherheitskonzepts und einer grundlegenden Leitlinie zur Informationssicherheit für die Organisation (welche von der Leitung zu verabschieden ist) sowie die Erstellung eines Notfallkonzepts.
- **Permanente Aufgaben**, die regelmäßig anfallen, zum Beispiel Überprüfung der ergriffenen Sicherheitsmaßnahmen, deren Fortentwicklung, die Vermittlung der Informationssicherheit bei den Nutzern (einschließlich Sensibilisierungen etwa durch Schulungen), turnusmäßiger Bericht an die Leitung.
- **Anlassbezogene Aufgaben** wie zum Beispiel der Umgang mit Störungen („Incidents“) einschließlich Pflichtmeldungen an Aufsichtsbehörden oder projektbezogene Unterstützungen.

Inhaltlich hängen die Aufgaben von den Eigenschaften der Organisation selbst ab. Ziffer 4.3 des BSI-Standards 200-2 nennt folgende Aufgaben für einen ISB:

- Informationssicherheitsprozess steuern und bei allen damit zusammenhängenden Aufgaben mitwirken,
- Leitungsebene bei der Erstellung der Leitlinie zur Informationssicherheit unterstützen,
- Erstellung eines Sicherheitskonzepts, eines Notfallvorsorgekonzepts und anderer Teil-Konzepte und System-Sicherheitsrichtlinien koordinieren

---

7 Hinweis: Laut BSI-Standard 200-2 kann ein IT-SiBe auch in die IT-Abteilung eingegliedert sein. In diesem Fall muss er nicht von der Leitung der Organisation beauftragt sein, sondern kann auch der Leitung der IT-Abteilung in der Organisation unterstehen. Nach der hier vertretenen Auffassung ist es aber effektiver, wenn der IT-SiBe seinen Auftrag unmittelbar von der Organisationsleitung erhalten hat. Denn es können Interessenkonflikte zwischen dem operativen IT-Betrieb und der IT-Sicherheit auftreten (siehe unten Ziffer 1.5).

8 So Schmidl/Thannen in: Kipker, Cybersecurity, 2. Aufl., Kap. 8 Rn. 45.

sowie weitere Richtlinien zur Realisierung der Informationssicherheit erlassen,
- Realisierung von Sicherheitsmaßnahmen initiieren und überprüfen,
- Leitungsebene und dem IS-Management-Team über den status quo der Informationssicherheit berichten,
- sicherheitsrelevante Projekte koordinieren,
- Sicherheitsvorfälle untersuchen,
- Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit initiieren und koordinieren.

Außerdem ist eine enge Zusammenarbeit mit anderen betrieblichen Beauftragten sinnvoll, zum Beispiel dem Datenschutzbeauftragten (DSB).

Zusammenfassung:
- Die Aufgaben eines ISB/IT-SiBe sind gesetzlich nicht definiert.
- Deshalb muss die Leitung der Organisation die Aufgaben des ISB bzw. des IT-SiBe im Rahmen des Auftrags definieren.
- ISB und IT-SiBe betreiben in ihren Organisationen systematische Informations- bzw. IT-Sicherheit.
- Die Aufgaben lassen sich einteilen in initiale, permanente und anlassbezogene Tätigkeiten.
- Wichtig ist: ISB und IT-SiBe informieren die Organisationsleitung und schlagen Maßnahmen vor. Die Entscheidung darüber, welches Sicherheitsniveau angestrebt wird und welche Maßnahmen umzusetzen sind, trifft die Organisationsleitung und nicht der ISB/IT-SiBe.

1.5. Wie wird man ISB/IT-SiBe?

Die Bezeichnungen ISB und IT-SiBe beinhalten das Wort „Beauftragung“. Ein ISB/IT-SiBe kann also nur aufgrund eines **ausdrücklichen Auftrags** tätig werden.

Informations- und IT-Sicherheit sind kein Selbstzweck. Wird die IT einer Organisation angegriffen, kann dies zum Betriebsstillstand, drastischen Schäden oder sogar zur Existenzvernichtung führen. Gleiches gilt, wenn Informationen nicht verfügbar sind oder in falsche Hände geraten. Die Existenzsicherung und das Fernhalten von Schäden gehört zu den Kernaufgaben der Organisationsleitung. IT- und Informationssicherheit sind deshalb Chefsache. ISB und IT-SiBe können Sicherheitsmaßnahmen ausarbeiten, vorschlagen und umsetzen; die Entscheidung und Verantwortung dazu liegt aber bei der Organisationsleitung. Wichtig ist deshalb, dass der ISB/IT-SiBe seinen **Auftrag unmittelbar von der obersten Leitungsebe-**

ne der Organisation erhält (zur Ausnahme beim IT-SiBe siehe unten Ziffer 3.2.1).

Aus rechtlicher Sicht besteht der Auftrag aus einem **Vertrag zwischen der Organisation und dem ISB/IT-SiBe**. Ein solcher Vertrag ist nur dann eine taugliche Basis, wenn er den Leistungsumfang und die Leistungspflichten des ISB/IT-SiBe ausreichend definiert. Wichtig ist, dass die Organisationsleitung dem ISB/IT-SiBe **ausreichende Ressourcen** für die Aufgabenerfüllung zusagt (gegebenenfalls vertraglich). Hierzu gehört auch eine angemessene Vergütung (näher dazu unten Ziffer 3.2). Ein Mustertext für einen solchen Vertrag ist im Anhang enthalten.

Zusätzlich zum Vertrag kann eine **gesonderte Bestellungsurkunde** sinnvoll sein (siehe unten Ziffer 3.2.1). Darin bestätigt die Organisation ihren Auftrag an den ISB/IT-SiBe und gegebenenfalls seine Kompetenzen. Die Bestellungsurkunde ist damit eine Art Legitimation, die der ISB/IT-SiBe innerhalb oder außerhalb der Organisation zum Nachweis seines Auftrags verwenden kann. Dies kann es erleichtern, Auskünfte zu erhalten oder Anweisungen im Namen der Unternehmensleitung durchzusetzen, sei es an interne oder externe Beteiligte.

Für die **Qualifikation eines ISB/IT-SiBe** gibt es keine gesetzlichen Vorgaben. Allerdings ergeben sich die Anforderungen an die Eignung eines ISB/IT-SiBe aus dessen Aufgaben und dem Inhalt seines Auftrags: Je umfangreicher die Aufgaben und der Auftrag sind, desto breiter und detaillierter müssen die Qualifikationen des ISB/IT-SiBe sein. Geht man von den Aufgaben des BSI-Standards 200-2 aus (siehe oben 1.4), so sind vom ISB **technische Kenntnisse** sowie **Kommunikations- und Organisationsfähigkeiten** zu verlangen. Wichtig ist auch das **Wissen um die Arbeitsabläufe bzw. Geschäftsprozesse der Organisation**. Außerdem gehört die **persönliche Zuverlässigkeit** und **Konfliktfähigkeit** zu den Eigenschaften eines ISB und eines IT-SiBe. Wer ISB/IT-SiBe einer lebens- oder verteidigungswichtigen Einrichtung werden will, muss zur Feststellung seiner Zuverlässigkeit mit einer Sicherheitsprüfung nach dem **Sicherheitsüberprüfungsgesetz (SÜG)** rechnen (näher siehe unten Ziffer 3.2). Bisweilen tritt die Informations- und IT-Sicherheit, die zusätzlichen Aufwand erfordern kann, in Konflikt mit Interessen von IT-Nutzern, die diesen zusätzlichen Aufwand vermeiden möchten. Ein IT-SiBe und ein ISB können ihre Aufgabe nur dann sinnvoll lösen, wenn sie keine widerstreitenden Interessen in einer Person wahrnehmen müssen. Deshalb kann das Amt des ISB mit der Aufgabe der IT-Leitung unvereinbar sein. Das bayerische Landesamt für Sicherheit in der Informationstechnik z. B. empfiehlt für behördliche ISB folgende Qualifikationen:[9]

9 https://lsi.bayern.de/mam/aktuelles/lsi-info_i02_isb-profil.pdf.

- Grundlegendes Wissen über die Aufgaben und Abläufe der Behörde (interdisziplinäres Denken)
- Erfahrung im Projektmanagement (vorzugsweise mit Kenntnissen über Risikoanalysen)
- Hohes Maß an Fortbildungsbereitschaft
- Selbstständiges Arbeiten
- Analytische Fähigkeiten
- Kooperations- und Teamfähigkeit
- Durchsetzungsvermögen
- Kommunikationsgeschick.

Zum erforderlichen IT-Fachwissen zählt das Landesamt:

- Sicherheitstechniken für IT-Systeme wie Firewalls und Antivirenprogramme
- Netzwerktechnik
- Absicherung von Endgeräten (z. B. PCs, Smartphones).

In einer Klage zur Eingruppierung einer IT-Sicherheitsbeauftragten in bestimmte Lohngruppen des Tarifvertrags der Länder (TVÜ-Länder) hat das Bundesarbeitsgericht (BAG) entschieden, dass die Tätigkeit eines IT-SiBe kein Hochschulstudium voraussetzt (BAG, Urt. v. 14.09.2016 – 4 AZR 964/13). Entscheidend war aber im BAG-Fall die Aufgabenbeschreibung der klagenden IT-SiBe in deren Arbeitsvertrag. Je nach Aufgabe ist ein passendes Hochschulstudium jedenfalls sinnvoll, um die notwendige Qualifikation zu erwerben bzw. nachzuweisen. Zahlreiche Hochschulen bieten z. B. IT-Sicherheit oder zumindest zentrale Elemente daraus als Studiengang an.[10]

Zusammenfassung: Die Tätigkeit als ISB oder IT-SiBe setzt einen Auftrag voraus. Der Auftrag ist von der obersten Leitungsebene derjenigen Organisation zu erteilen, in der der ISB/IT-SiBe tätig werden soll. Leistungsumfang und erforderliche Ressourcen sind sinnvollerweise in einem Vertrag zwischen ISB/IT-SiBe und der Organisation festzulegen. Für die Praxis hilfreich kann zudem eine Bestellungsurkunde sein, mit der der ISB/IT-SiBe seinen Auftrag anderen Personen gegenüber nachweisen kann.

Die notwendigen Qualifikationen eines ISB/IT-SiBe ergeben sich aus seinen Aufgaben.

10 Es gibt verschiedene Organisationen, die Kenntnisse für ISB und IT-SiBe vermitteln, z. B. die IHKs, TÜV, Dekra, VDI usw. Fraglich ist allerdings, ob Schnellkurse von wenigen Tagen die nötigen vertieften Kompetenzen auf technischer und rechtlicher Ebene vermitteln können. Solche Angebote sind daher vor allem dann sinnvoll, wenn die Betreffenden schon Vorkenntnisse mitbringen.

Für ISB und IT-SiBe ist wichtig, dass sie die Aufgabe nur übernehmen, wenn die Voraussetzungen dafür gegeben sind, insbesondere wenn die Organisationsleitung ausreichende Ressourcen zur Erledigung der Aufgaben bereitstellt und der ISB/IT-SiBe die notwendigen Qualifikationen bereits erworben hat oder die Organisation ausreichend Gelegenheit zur Fortbildung schafft.

1.6. Erwartungen an die Beauftragten

Aus den vielschichtigen Aufgaben von ISB und IT-SiBe können sich hohe Erwartungshaltungen verschiedener Beteiligter ergeben.

Aus Sicht der **Leitung der Organisation** führt die Beauftragung von ISB bzw. IT-SiBe zu einer **Delegation** bei der Aufgabe der Informations- bzw. IT-Sicherheit. Die Delegation kann zu der Erwartung führen, die Organisationsleitung habe die Informations- und IT-Sicherheit an den ISB/IT-SiBe übertragen und sei diese Aufgabe nun los. Diese Erwartung ist falsch. ISB und IT-SiBe müssen ihr entgegentreten. Wer Aufgaben delegiert, muss auch deren Erledigung überprüfen.[11] Die Bestellung eines ISB/IT-SiBe führt also nicht dazu, dass sich die Organisationsleitung der Aufgabe der Informations- und IT-Sicherheit entziehen kann. **Informations- und IT-Sicherheit** gehört zur Existenzsicherung der Organisation und bleibt eine **Kernaufgabe der Leitung**. ISB und IT-SiBe unterstützen die Leitung dabei und tragen jeweils auf ihrer Organisationsebene Verantwortung. Dies gilt auch dann, wenn die Organisation eine sogenannte „horizontale Delegation" vorgenommen und die Informationssicherheit einem von mehreren Geschäftsführern übertragen hat (wie es bei einer „C-Level-Struktur" vorkommen kann, siehe oben Ziffer 1.3). Wer als Geschäftsführer ISB/IT-SiBe ist, trägt damit zwar höhere Verantwortung, aber die übrigen Leitungsorgane sind nicht davon entbunden, sich zu vergewissern, ob und wie die Aufgaben der Informations- und IT-Sicherheit erledigt sind.

Eine vergleichbare Erwartung können die **Beschäftigten** einer Organisation entwickeln. Die Bestellung eines ISB/IT-SiBe kann die Vorstellung hervorrufen, Beschäftigte müssten sich nicht mehr um Informations- und IT-Sicherheit kümmern. Dies gilt umso mehr, als konkrete Sicherheitsmaß-

11 Das Kammergericht Berlin (Urt. v. 09.10.1998 – 14 U 4823/96) hat zwei Geschäftsführer zum Schadensersatz verurteilt, weil deren Mitarbeiter Betrugsgeschäfte tätigten. Die Geschäftsführung hatte die Mitarbeiter bevollmächtigt, aber nicht kontrolliert, ob sie auftragsgemäß handelten.

nahmen scheinbar einer nutzerfreundlichen Bedienung von Betriebsmitteln (insbesondere IT) entgegenstehen.

Diese Erwartung ist mehrfach falsch. Weder steht Nutzerfreundlichkeit der IT-Sicherheit entgegen, noch kann ein ISB/IT-SiBe ohne die Unterstützung der Mitarbeiter erfolgreich sein. Ein ISB/IT-SiBe organisiert die Geschäftsprozesse, um das Sicherheitsniveau zu erreichen, welches die Organisationsleitung vorgegeben hat. Die Beschäftigten sind angehalten, die definierten Maßnahmen umzusetzen, dazu geben ISB und IT-SiBe Empfehlungen und Handlungsanweisungen, können Gefahren erläutern und weitere Hinweise an die Hand geben. Dabei dürfen sie aber keine Angst vor der IT-Nutzung erzeugen, sondern müssen Sicherheit im Umgang mit der IT vermitteln.

Kunden und sonstige Kommunikationspartner der Organisation erwarten, dass der ISB bzw. IT-SiBe dafür sorgt, dass deren Informationen dort sicher sind. Außerdem erwarten sie, dass sie sich bei der Kommunikation mit der Organisation keine Malware oder sonstige Sicherheitsrisiken „einfangen". Insbesondere die Vermeidung von Schwachstellen in Software dient auch dem Interesse der Allgemeinheit, weil deren Verbreitung stets Angriffsfläche für Kriminelle bietet. Dies kann nicht nur die Organisation betreffen, sondern jeden IT-Nutzer. Diese Erwartungen mögen berechtigt sein, richten sich aber nicht an den ISB/IT-SiBe, sondern an die Organisation selbst.

Aufsichtsbehörden der Organisation (unten Ziffer 4) erwarten vom ISB/IT-SiBe, dass die Organisation ihre Sicherheitspflichten erfüllt. Der ISB/IT-SiBe ist zudem Ansprechpartner der Behörden, der sie auch über Störfälle („Incidents") informiert. Die Kommunikation mit Aufsichtsbehörden gehört zwar zu den typischen anlassbezogenen Aufgaben des ISB/IT-SiBe, er führt diese Aufgaben aber nicht im Auftrag der Aufsichtsbehörden aus, sondern er bleibt der Organisation verpflichtet, die ihn mit der Informations- bzw. IT-Sicherheit beauftragt hat.

Schließlich sind auch die eigenen Erwartungen des ISB/IT-SiBe relevant (**Selbstverständnis**). Welches Sicherheitsniveau halte ich für richtig und weicht dies von den Erwartungen der Organisationsleitung ab?

Fühle ich mich meinem Auftraggeber oder der Informations- und IT-Sicherheit im Allgemeinen verpflichtet?

Welche Wirkungen will ich mit meinen Maßnahmen bei der Organisation erreichen?

Geht es um effektive Informations- und IT-Sicherheit oder erschöpft sich die Tätigkeit darin, Richtlinien und Dokumentationswerke zu schaffen mit dem Ziel, sich selbst und die Organisation von Verantwortung zu entlasten?

Zusammenfassung: Die Erwartungen an IT-SiBe und ISB können vielschichtig sein. Denn die IT- und Informationssicherheit einer Organisation betreffen die Organisationsleitung, deren Beschäftigte, Kunden und sonstige Kommunikationspartner. Auch die Aufsichtsbehörden einer Organisation haben eigene Erwartungen.

ISB/IT-SiBe haben sich von den Erwartungen abzugrenzen. Maßgeblich hierfür ist der Auftrag, den sie von der Organisationsleitung erhalten haben.