HANSER

Leseprobe

zu

„Informationssicherheit und Datenschutz – einfach & effektiv“

von Inge Hanschke

Print-ISBN: 978-3-446-45818-5
E-Book-ISBN: 978-3-446-45973-1
E-Pub-ISBN: 978-3-446-46300-4

Weitere Informationen und Bestellungen unter
http://www.hanser-fachbuch.de/978-3-446-45818-5
sowie im Buchhandel

Inhalt

Vorwort

Am besten erledigt man die Dinge systematisch.

Hesiod von Böotien (um 700 v. Chr.)

Anforderungen an die Informationssicherheit (u. a. ISO 27001 oder BSI), den Datenschutz (EU-Datenschutz-Grundverordnung) und Sicherheitsbedrohungen sowie die durch diese verursachten Schäden nehmen immer weiter zu. Ein in alle Planungs-, Entscheidungs- und Durchführungsprozesse verankertes, handhabbares und integriertes Managementinstrumentarium ist für deren nachhaltige Bewältigung notwendig. Im Buch werden sowohl die Herausforderungen adressiert als auch Hilfestellungen für eine systematische Gestaltung und nachhaltige Verankerung in der Organisation gegeben.

Im Buch werden sowohl die Anforderungen der EU-Datenschutz-Grundverordnung als auch die aus dem Kontext Informationssicherheit sowie wesentliche Normen und gesetzliche Regelungen eingeführt. Wegen der ständig zunehmenden Bedrohungslage im Cyberspace wird auch das Themenfeld Cyber-Security adressiert, um dessen wachsender Bedeutung gerecht zu werden. Cyber-Security beschreibt den Schutz vor technischen, organisatorischen und naturbedingten Bedrohungen, die die Sicherheit des Cyberspace inklusive Infrastruktur- und Datensicherheit gefährden. Es beinhaltet alle Konzepte und Maßnahmen, um Gefährdungen[1] zu erkennen, zu bewerten, zu verfolgen, vorzubeugen sowie Handlungs- und Funktionsfähigkeit möglichst schnell wiederherzustellen.

Neben den Herausforderungen für Datenschutz und Informationssicherheit finden Sie in diesem Buch sowohl Best-Practices für ein integriertes und ganzheitliches einfaches und effektives Management-Instrumentarium für Datenschutz und Informationssicherheit als auch einen Leitfaden, um Ihr individuelles Instrumentarium abzuleiten. Mithilfe eines

[1] Gefährdung = Bedrohung und Schwachstelle

Schritt-für-Schritt-Leitfadens werden Hilfestellungen für die individuelle Ableitung und für die Umsetzung gegeben. Die Schritte werden anhand von Beispielen erläutert.

Sowohl der Datenschutz als auch die Informationssicherheit, einschließlich der Cyber-Security, benötigen eine möglichst vollständige, konsistente und aktuelle Aufstellung aller Assets (fachliche und technische Werte des Unternehmens wie Geschäftsprozesse, Organisationsstrukturen, Applikationen, technische Bausteine und Configuration Items) für Analysen und Schutzbedarfsfeststellung.

So sind für den Datenschutz Informationen über die Verwendung von Daten (Geschäftsobjekte) in Prozessen oder Applikationen essenziell. Fragestellungen wie „Welche Prozesse oder Applikationen verwenden personenbezogene Daten in welcher Art und Weise?“ sind relevant. Auf Basis des Asset-Registers erfolgen zudem die Schutzbedarfsfeststellung und die Gefährdungsanalyse sowie die Analyse von Abhängigkeiten und Auswirkungen von technischen Schwachstellen (siehe Abschnitte 4.1 und 4.2).

Das Asset-Management kann maßgeblich durch Enterprise Architecture Management (EAM) und eine Configuration Management Database (CMDB) unterstützt werden. Durch die Kombination vom integrierten Managementsystem für Datenschutz und Informationssicherheit mit EAM und einer CMDB werden sowohl die Wirksamkeit als auch die Effizienz deutlich erhöht. Daher wird diesem Zusammenspiel ein eigenes Kapitel in diesem Buch gewidmet.

Hier setzt dieses Buch an. Das Buch liefert einerseits einen ganzheitlichen schlanken und handhabbaren Ordnungsrahmen und andererseits einen Schritt-für-Schritt-Leitfaden für die systematische maßgeschneiderte Ableitung Ihres individuellen Datenschutz- und Informationssicherheitsinstrumentariums sowie deren Operationalisierung durch direkt anwendbare Hilfestellungen.

München, im Herbst 2019

Inge Hanschke

Danksagung

Vielen Dank an die vielen Datenschutz- und Informationssicherheitsexperten und Kollegen aus befreundeten Unternehmen für den intensiven Austausch.

Danke an meine Diskussionspartner, Reviewer und Unterstützer, die durch wertvolle Kommentare und Feedback das Buch maßgeblich mitgestaltet haben. Hier sind insbesondere Sebastian Hanschke, Christiane Charrad und auch Frau Brigitte Bauer-Schiewek sowie Frau Irene Weilhart vom Hanser-Verlag für ihr wertvolles Feedback und ihre Unterstützung zu nennen.

Besonderen Dank an Jörg Krüger, meine Familie und Freunde, die mir den Rücken freigehalten haben und mich auch durch Feedback tatkräftig unterstützt haben.

Wegweiser durch dieses Buch

Die Gliederung des Buchs ist im folgenden Bild dargestellt. Sie können die Kapitel in der genannten Reihenfolge oder aber auch selektiv lesen. Sie sind inhaltlich in sich abgeschlossen.

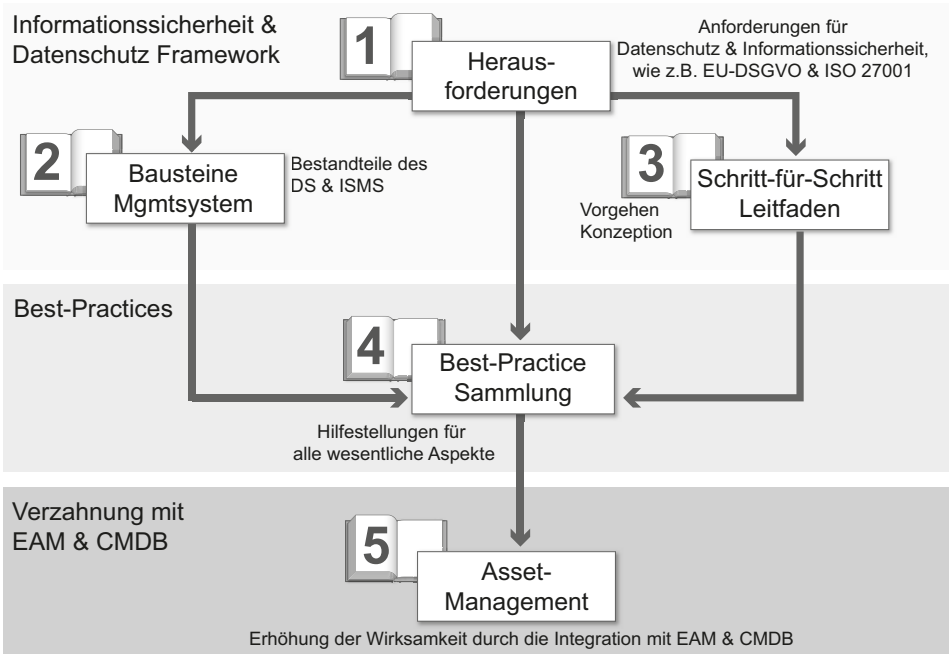

Bild 1 Kapitelstruktur

- Kapitel 1 erläutert die Herausforderungen im Datenschutz und in der Informationssicherheit mit allen relevanten Sicherheitsvorgaben, wie z. B. ISO 27001, IT-Grundschutz und EU-DSGVO sowie der Cyber-Security.
- Kapitel 2 skizziert die Bausteine eines integrierten Datenschutz- und Informationssicherheitssystems.
- In Kapitel 3 finden Sie den Schritt-für-Schritt-Leitfaden für die Konzeption Ihres integrierten Instrumentariums.
- Kapitel 4 liefert Ihnen eine Best-Practice-Sammlung zur Operationalisierung Ihres Instrumentariums.
- Kapitel 5 widmet sich dem Asset-Management mit Hilfe vom Enterprise Architecture Management und einer CMDB.

Jedes Kapitel enthält darüber hinaus zahlreiche Literaturhinweise als Empfehlung für die Vertiefung des jeweiligen Themas.

Wer sollte dieses Buch lesen?

Das Buch adressiert alle Personengruppen im Kontext Informationssicherheit und Datenschutz, die „Kümmerer“ und die „Betroffenen“, wie z. B. der Datenschutz- oder Informationssicherheitsbeauftragte sowie die Bereiche Infrastruktur, Organisation, Personal, Technik und Notfallvorsorge. Folgende Personengruppen werden besonders adressiert:

- *Chief Information Security Officer (CISO), Informationssicherheitsbeauftragter (ISB), Beauftragte für IT-Sicherheit, Bereichs- oder Projektsicherheitsbeauftragter*
  - Wie kann das ISMS initiiert, implementiert und überwacht werden?
  - Welche Sicherheitsanforderungen bestehen? Welche Normen, wie z. B. ISO 27001, sind für das Unternehmen relevant?
  - Wie werden Sicherheitsziele und Geltungsbereich festgelegt?
  - Welche Sicherheitsmaßnahmen sind zur Umsetzung der Anforderungen erforderlich?
  - Welche Dokumente sind unter welchen Vorgaben verpflichtend? Welche Inhalte haben die Dokumente, wie z. B. die Informationssicherheitsleitlinie? Wie können diese handhabbar gestaltet werden?
  - Wie muss eine Sicherheitsorganisation für den jeweiligen Kontext gestaltet werden?
  - Wie sieht ein Sicherheitskonzept aus? Welche Best-Practices gibt es hierzu?
  - Wie kann wirksam ein Instrumentarium aufgebaut und betrieben werden?
  - Wie erfolgt die Erstellung von Plänen zur Umsetzung und Kontrolle von Sicherheitsmaßnahmen?
  - Wie kann die Wirksamkeit überprüft werden?
  - Wie kann ein ausreichendes Sicherheitsniveau definiert und implementiert werden?
  - Wie kann Informationssicherheit effizient und effektiv kontinuierlich sichergestellt werden?
  - In welche Prozesse, wie z. B. Risikomanagement, und organisatorische Strukturen muss sich das Instrumentarium verzahnen? Auf welche Art und Weise?
- *Datenschutzbeauftragte (DSB)*
  - Wie kann der Datenschutzbeauftragte der obersten Leitungsebene bei der Wahrung der Persönlichkeitsrechte und der Vermeidung von Zwischenfällen, die dem Ansehen des Unternehmens schaden, unterstützen?
  - Wie sieht ein Datenschutzkonzept aus?
  - Welche Dokumente/Meldewege sind verpflichtend? Welche Inhalte und Struktur haben diese Dokumente? Wie können diese handhabbar gestaltet werden?
  - Welche technischen und organisatorischen Maßnahmen sind relevant für die Umsetzung des Datenschutzkonzepts? Wie kann deren Wirksamkeit überprüft werden?
  - Welche organisatorischen Voraussetzungen müssen geschaffen werden?
  - Wie kann ein ausreichendes Datenschutzniveau definiert und implementiert werden?
  - Wie kann Datenschutz effizient und effektiv kontinuierlich sichergestellt werden?
  - In welche Prozesse, wie z. B. Risikomanagement, muss sich das Instrumentarium verzahnen? Auf welche Art und Weise?

- *Betriebsrat*
  - Wie können die Mitbestimmungsrechte gewahrt werden?
  - Wie können Mitarbeiter vor Sanktionen geschützt werden?
  - Wie können Mitarbeiter vor unklaren Regelungen und einschränkenden Maßnahmen geschützt werden?
- *Oberste Leitungsebene („Informationssicherheit und Datenschutz ist Chefsache")*
  - Ist ein ISMS im Wettbewerb ein Vorteil oder ein Hygienefaktor?
  - Wie können die Unternehmenswerte hinreichend gesichert werden?
  - Wie können die Unternehmensrisiken und persönlichen Risiken beherrscht werden?
  - Wie können Informationssicherheit und Datenschutz hinreichend umgesetzt werden? Mit welcher Organisation? Ohne zu viele Aufwände? Ohne zu viele Formalismen? Wie viele Rollen und Ressourcen sind notwendig?
  - Welche Aufgaben bestehen für die oberste Leitungsebene? Welche Aufgaben können delegiert werden? Welche Verantwortung verbleibt?
- *Leiter Organisation und Führungskräfte*
  - Welche organisatorischen Voraussetzungen müssen für Informationssicherheit und Datenschutz geschaffen werden?
  - Welche organisatorischen und personellen Anforderungen bestehen und wie können diese durch angemessene Sicherheitsmaßnahmen umgesetzt werden?
  - Wie können Datenschutz- und Informationssicherheitsrisiken in das unternehmensübergreifende Risikomanagement integriert werden?
- *Einkauf*
  - Wie kann das Sicherheitsrisiko durch Lieferanten gesenkt werden? Wie können Auftragnehmer zu den für das Unternehmen festgelegten Sicherheits- und Datenschutzrichtlinien verpflichtet und in geeigneter Weise zur Einhaltung „gezwungen" werden?
  - Wie stellt man sicher, dass der Auftragnehmer bei erkennbaren Mängeln und Risiken eingesetzter Sicherheitsmaßnahmen den Auftraggeber unverzüglich informiert?
  - Wie kann der Aufwand bei der Lieferanten-Auditierung reduziert werden?
- *Fachverantwortliche für Geschäftsprozesse und Fachverfahren*
  - Wie können die geschäftliche Relevanz/Kritikalität der verarbeitenden Informationen, der Verarbeitungen und deren Schutzbedarf festgelegt werden?
  - Welche Sicherheits- und Kontrollmaßnahmen sind zur Verwaltung und zum Schutz der im Verantwortungsbereich befindlichen Informationen zu implementieren?
  - Wie können durch den Fachverantwortlichen der Zugang zu Informationen sowie der Umfang und die Art der Autorisierung in den Verarbeitungen definiert werden? Was ist dabei zu berücksichtigen? Wie ist die Autorisierung zu dokumentieren?
  - Welche Informationen haben welche geschäftliche Relevanz und wie können diese adäquat geschützt werden?
  - Welche Aufbewahrungsfristen müssen entsprechend der gesetzlichen Vorschriften eingehalten werden?

- *Mitarbeiter*
  - Welche Verhaltensregeln gibt es im Kontext Informationssicherheit und Datenschutz?
  - Was muss beachtet werden? Wo findet man die jeweils gültige Richtlinie und Verfahrensanweisung?
- *IT-Verantwortliche*
  - Welche Richtlinien und Verfahrensanweisungen sind für sichere IT-Unterstützung der Geschäftsprozesse relevant? Wie können diese mit den vorhandenen IT-Prozessen integriert werden?
  - Wie können IT-Servicemanagement und Informationssicherheit zusammenwirken?
  - Wie sollte eine ordnungsgemäße IT-Administration erfolgen? Welche Verhaltensregeln und Sicherheitshinweise sollten für Administratoren festgelegt werden?
  - Wie können über Sicherheitsgateways oder Firewalls Schutzzonen erstellt werden? Welche sind erforderlich?
  - Wie kann ein hinreichender Virenschutz zum Schutz vor Schadprogrammen erreicht werden?
  - Wie kann die Notfallvorsorge aussehen?
  - Was ist bei der Datensicherung zu beachten?
  - Welche Daten sind zu archivieren? Welche Aufbewahrungsfristen gelten?
  - Wie kann die sichere Nutzung von E-Mail und Groupware gewährleistet werden?
  - Was ist bei Outsourcing und externen Dienstleistern zu beachten?

Webseite zum Buch

Weitergehende Informationen zum Buch finden Sie auf den Webseiten https://Lean42.com und https://LeanISMS.de, außerdem unter https://www.hanser-fachbuch.de/978-3-446-45818-5. Auf dieser Buchdetailseite klicken Sie auf die Registerkarte Links.

Stichwortverzeichnis