}essentials{

Inge Hanschke

Informationssicherheit und Datenschutz systematisch und nachhaltig gestalten

Eine kompakte Einführung in die Praxis

2. Auflage

Springer Vieweg

essentials

essentials liefern aktuelles Wissen in konzentrierter Form. Die Essenz dessen, worauf es als „State-of-the-Art“ in der gegenwärtigen Fachdiskussion oder in der Praxis ankommt. *essentials* informieren schnell, unkompliziert und verständlich

- als Einführung in ein aktuelles Thema aus Ihrem Fachgebiet
- als Einstieg in ein für Sie noch unbekanntes Themenfeld
- als Einblick, um zum Thema mitreden zu können

Die Bücher in elektronischer und gedruckter Form bringen das Expertenwissen von Springer-Fachautoren kompakt zur Darstellung. Sie sind besonders für die Nutzung als eBook auf Tablet-PCs, eBook-Readern und Smartphones geeignet. *essentials:* Wissensbausteine aus den Wirtschafts-, Sozial- und Geisteswissenschaften, aus Technik und Naturwissenschaften sowie aus Medizin, Psychologie und Gesundheitsberufen. Von renommierten Autoren aller Springer-Verlagsmarken.

Weitere Bände in der Reihe http://www.springer.com/series/13088

Inge Hanschke

Informationssicherheit und Datenschutz systematisch und nachhaltig gestalten

Eine kompakte Einführung in die Praxis

2., korrigierte Auflage

Springer Vieweg

Inge Hanschke
München, Deutschland

ISSN 2197-6708 ISSN 2197-6716 (electronic)
essentials
ISBN 978-3-658-28698-9 ISBN 978-3-658-28699-6 (eBook)
https://doi.org/10.1007/978-3-658-28699-6

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

Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Was Sie in diesem *essential* finden können

- Begriffsdefinitionen aus dem Kontext Informationssicherheit und Datenschutz
- Herausforderungen von Informationssicherheit und Datenschutz
- Bestandteile und Leitfaden für den Aufbau und Betrieb eines integrierten Managementsystems für Informationssicherheit und Datenschutz

Inhaltsverzeichnis

Einleitung

1

Wer die Freiheit aufgibt, um Sicherheit zu gewinnen, wird am Ende beides verlieren.

Benjamin Franklin

1.1 Introduction

Das Leben im 21. Jahrhundert ist von der Durchdringung von Informations- und Kommunikationstechnik in allen Lebensbereichen geprägt. Kaum ein Geschäftsprozess kommt mehr ohne IT-Unterstützung aus. Mit zunehmender Digitalisierung nimmt die horizontale und vertikale Vernetzung immer weiter zu. Die hohe Durchdringung erhöht gleichzeitig die Abhängigkeit und die Anfälligkeit für die kontinuierlich zunehmenden Sicherheitsbedrohungen, zum Beispiel im Kontext von Cyber-Security.

Nicht verfügbare Systeme, Datenpannen, manipulierte, missbräuchlich verwendete, mutwillig zerstörte oder kompromittierte Daten können für Unternehmen zu ernsthaften rechtlichen oder wirtschaftlichen Konsequenzen führen. Beispiele sind Massen-E-Mails mit Viren oder eine Datenpanne, bei der im Unternehmen gespeicherte Daten an die Öffentlichkeit gelangen. Ein weiteres Beispiel ist die Unterbrechung in einer Lieferkette in einer Just-in-time (JIT) Fertigung, aufgrund eines Systemabsturzes, der zu einem Produktionsstillstand führt, da wesentliche Rohstoffe oder Teile nicht angefordert werden und damit fehlen.

Informationssicherheit und Datenschutz sind daher unerlässlich, um sowohl personenbezogene Daten als auch Geschäfts- und Unternehmensgeheimnisse zu schützen und einen zuverlässigen Geschäftsbetrieb zu gewährleisten.

I. Hanschke, *Informationssicherheit und Datenschutz systematisch und nachhaltig gestalten,* essentials, https://doi.org/10.1007/978-3-658-28699-6_1

▶ Die **Informationssicherheit** zielt auf den angemessenen Schutz von Informationen und IT-Systemen insbesondere in Bezug auf alle festgelegten Schutzziele, wie Vertraulichkeit, Integrität und Verfügbarkeit, ab. So soll insbesondere ein unbefugter Zugriff oder Manipulation von Daten verhindert und soweit möglich vorgebeugt werden, um daraus resultierende wirtschaftliche Schäden zu verhindern. Bei den Daten ist es unerheblich, ob diese einen Personenbezug haben oder nicht. Informationen können sowohl auf Papier oder in IT-Systemen vorliegen.

▶ **IT-Sicherheit** adressiert als Teilbereich der Informationssicherheit den Schutz elektronisch gespeicherter Informationen und deren Verarbeitung inklusive Funktionssicherheit, also das fehlerfreie Funktionieren und die Zuverlässigkeit der IT-Systeme. Hier müssen auch Systeme einbezogen werden, die häufig nicht unmittelbar als IT-Systeme wahrgenommen werden, wie Steuerungs- (ICS) oder IoT-Systeme. Die IT-Sicherheit ist also Bestandteil der Informationssicherheit. Das Aktionsfeld der klassischen IT-Sicherheit wird bei der Cyber-Sicherheit auf den gesamten Cyber-Raum ausgeweitet.

▶ Unter **Datenschutz** wird primär der Schutz personenbezogener Daten vor missbräuchlicher Verwendung und Datenverarbeitung verstanden, um das Recht des Einzelnen auf informationelle Selbstbestimmung zu stärken.

Externe Vorgaben erzwingen durch Gesetze, Regulatoren und Normen angemessene Sicherheitsmaßnahmen. Vorstände und Geschäftsführer haften persönlich für Versäumnisse und mangelnde Risikovorsorge. Durch die geänderte Gesetzeslage fallen zudem hohe Bußgelder bei Datenpannen im Kontext der EU-DSGVO an.

Es stellt sich also nicht die Frage, ob man Informationssicherheit und Datenschutz in seinem Unternehmen adressiert, sondern nur wann und in welchem Umfang. Für letzteres stellt sich die Frage: Wann ist man hinreichend sicher? Hierauf gibt es eine einfache Antwort: Systeme sind hinreichend sicher, wenn der Aufwand eines Angreifers dessen Nutzen erheblich übersteigt. Widerstandsfähige Systeme überstehen absichtliche Angriffe ohne inakzeptablen Schaden für das Unternehmen.

Schutz ist kein Selbstzweck, sondern es ist so viel Schutz notwendig, um einen kontinuierlichen Geschäftsbetrieb, Reputationserhalt, Kundenbindung und allgemein die Unternehmensziele zu erreichen. So dürfen z. B. Hackerangriffe nicht zum Ausfall von Kernsystemen führen. Hinreichend ist hierbei das Schlüsselwort. Denn eine übertriebene Absicherung ist unsinnig teuer oder