1. Auflage

Ihr Plus:
36 Übersichten
26 Leitsätze

Informations-sicherheit *leicht gemacht* ✓

IT-Sicherheitsgesetz, NIS-Richtlinie und BSI-Gesetz

Alexander Deicke
Alexander Schinner
Dino Huber

Edition Wissenschaft & Praxis

DATAGROUP

Cyber-Bedrohungen kennen keine Pausen - Ihre Sicherheit auch nicht.

Cyberangriffe werden immer raffinierter, denn ein einziger Vorfall kann enorme Schäden verursachen.
Die Security Services von DATAGROUP bieten Ihnen ein starkes, skalierbares Schutznetzwerk, das Ihre IT jederzeit proaktiv absichert.

Security Operations Center (SOC) mit Echtzeit-Überwachung

24/7 Monitoring für maximale Reaktionsfähigkeit

Über **250 hochqualifizierte Sicherheitsexpert:innen**

Neueste Technologien für hochautomatisierte Detection and Response unter Einsatz von KI

CyberHelden werden durch den Partner gemacht, den sie wählen.

IT's that secure.

www.datagroup.de

Informationssicherheit – *leicht gemacht*

GELBE SERIE – *leicht gemacht*

Die *leicht gemacht*-Lehrbücher führen Studierende erfolgreich in die Fächer Recht (GELBE SERIE) und Steuern / Rechnungswesen (BLAUE SERIE) ein, indem sie besonderes Augenmerk auf didaktische Erfordernisse legen und die wichtigsten Grundlagen vermitteln. Die Bände richten sich insbesondere an Anfängerinnen und Anfänger ohne Vorkenntnisse und sind daher ideal für den Einstieg und zur Prüfungsvorbereitung.

Weitere spannende Bände unter:
www.leicht-gemacht.de

Informations-sicherheit *leicht gemacht* ✓

IT-Sicherheitsgesetz, NIS-Richtlinie und BSI-Gesetz

1. Auflage

von Alexander Deicke, Alexander Schinner und Dino Huber

Edition Wissenschaft & Praxis EWP

Bibliografische Information der Deutschen Nationalbibliothek

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

Umschlagbild: © Zocha_K – iStock

bei Duncker & Humblot GmbH, Berlin
Carl-Heinrich-Becker-Weg 9
12165 Berlin, Germany
E-Mail: info@duncker-humblot.de
Internet: https://www.duncker-humblot.de

Satz: Datagroup-Int SRL, Timişoara, România
Druck: Prime Rate Kft., Budapest, Ungarn
Gedruckt auf FSC-zertifiziertem Papier

leicht gemacht® ist ein eingetragenes Warenzeichen

ISBN 978-3-87440-412-9 (Print)
ISBN 978-3-87440-812-7 (E-Book)

Inhalt

Übersichten

Management Summary

In der heutigen digitalen Ära ist Informationssicherheit zu einem entscheidenden Anliegen für Unternehmen und Einzelpersonen geworden. Mit dem Anstieg von Cyberbedrohungen ist es wichtig, zu verstehen, was Informationssicherheit beinhaltet und wie sie verwaltet wird. Dieses kleine Buch hat zum Ziel, einen ersten Einblick in die Informationssicherheit zu geben, bemerkenswerte Beispiele für Cyberangriffe und deren Konsequenzen hervorzuheben und die relevanten rechtlichen Rahmenbedingungen in der EU und Deutschland zu diskutieren. Wir werden auch das Management der Informationssicherheit (z.B. über die Norm ISO27001:2022) untersuchen und einen Ausblick auf zukünftige Trends geben. All dies wird im größeren Kontext der ESG-Governance und des Datenschutzes betrachtet, um gezielt Synergien zu schaffen. Governance lässt sich bildlich als Dach eines Hauses verstehen, unter dem zentrale Bereiche wie Informationssicherheit, Datenschutz und Compliance angesiedelt sind. In manchen Organisationen zählen auch Risikomanagement und Legal als weitere tragende Strukturen dazu. Carl Crimi, kurz vor dem Abschluss des Jura-Studiums, möchte einmal Kommissar werden und im Bereich Cyberkriminalität arbeiten. Um sich ein besseres Bild von dem Thema und Beruf zu machen, befragt er Frank Nobody, einen Sicherheitsforscher und -berater.

Lektion 1: Was heißt sicher? Was ist unsicher?

Fall 1

„Danke, Frank, dass du dir die Zeit nimmst, mir das alles zu erklären. Ich bin echt verwirrt", beginnt Carl. „Mein Informatiklehrer meint, ich müsse unbedingt alles verschlüsseln, denn das sei viel sicherer. Mein Nachbar – der studiert Informatik – behauptet, sein Linux sei deutlich sicherer als mein Windows. Mein Onkel, zugegebenermaßen mit leichten Schwurblertendenzen, wiederum warnt mich ständig, Onlinebanking sei total unsicher." Carl holt tief Luft. „Dann erzählt mir einer, WhatsApp sei unsicher, der nächste sagt, alle Messenger seien unsicher, weil die NSA mitliest, und der Dritte meint, genau das sei die einzige sichere Art zu kommunizieren. In der Werbung heißt es, ich brauche unbedingt supertolle, aber sündhaft teure Sicherheitssoftware, ohne die ich im Netz verloren bin. Und dann schreibt dieser eine Blogger, dass gerade diese Software alles unsicher mache und sowieso nur modernes **Schlangenöl** sei. Was heißt das denn überhaupt? Ich versteh's einfach nicht mehr." Er sieht Frank fragend an „Sicher! Unsicher! Meinen die überhaupt alle dasselbe? Oder reden die komplett aneinander vorbei?"

Frank holt tief Luft, schaut Carl ruhig an und meint: „Okay, erst mal zum Thema Schlangenöl. Das steht einfach für eine wirkungslose Sicherheitslösung. Der Begriff kommt ursprünglich aus der Medizin: Vor allem im ‚Wilden Westen' verkauften **Quacksalber** angebliche Wundermittel, die sie als ‚Snake Oil' anpriesen. Das sollte gegen alles helfen, aber in Wahrheit gab es aber überhaupt kein echtes Öl aus Schlangen, das irgendeine Wirkung gehabt hätte. In der Informatik gibt es ganz viele solche bildhaften Begriffe, oft bedient man sich auch bei der Sprache des Militärs, das ist alles ein bisschen wie ein Insiderwitz, macht das Verständnis aber nicht leichter. Mir ist auch klar, was dich so verwirrt, denn das, was du da erzählst, ist ja tatsächlich ein ziemliches Durcheinander. Das liegt insbesondere daran, dass alle von Sicherheit sprechen, aber oft etwas völlig Unterschiedliches darunter verstehen."

Er lehnt sich zurück. „Lass es mich erklären. Wir müssen wirklich ganz am Anfang anfangen, so, wie du es schon richtig vermutet hast. Und zwar mit der Frage: Was bedeutet das Wort **Sicherheit** eigentlich?" Er macht eine kurze Pause: „Denn wenn wir das nicht klären, reden wir weiter aneinander vorbei – so wie dein Lehrer, dein Mitbewohner, dein Onkel und die Leute aus der Werbung."

Frank nickt. „Also, Carl, wenn wir von **Sicherheit** sprechen, dann meinen wir meistens: **etwas soll vor Schaden bewahrt werden**. Aber was genau das bedeutet, hängt davon ab, was wir vor welcher Bedrohung schützen wollen. Stell dir vor, du hast einen Rucksack. Du willst, dass niemand etwas daraus klaut – also schließt du ihn an der Hochschule in deinem Spind ein. Oder du willst sicherstellen, dass dein Tablet nicht beschädigt wird – also suchst du dir einen Rucksack mit einem gepolsterten Fach. Oder du willst, dass nur du an deine Unterlagen kommst – also machst du ein Schloss an die Klappe. Siehst du, Carl – in jedem der Beispiele hast du etwas anderes schützen wollen: einmal vor Diebstahl, einmal vor Beschädigung, einmal vor unbefugtem Zugriff. Und jedes Mal sah die Lösung anders aus."

Er schaut Carl an. „Genau so funktioniert das auch in der Informationssicherheit. Wenn wir von **Sicherheit** sprechen, dann reicht es nicht, einfach zu sagen: ‚Es soll sicher sein.' Wir müssen uns immer fragen: **Was** soll eigentlich geschützt werden? Und **wovor**? Und genau dafür gibt es in der IT klare Begriffe. Wir nennen sie die **Schutzziele der Informationssicherheit**."

Frank nimmt sich sein Tablet und zeichnet ein Dreieck, die Ecken beschriftet er mit drei Begriffen:

- Vertraulichkeit
- Integrität
- Verfügbarkeit

„Diese drei nennt man die **Schutzziele der Informationssicherheit**. Sie bilden das Fundament. Wenn jemand von ‚IT-Sicherheit' redet, dann meint er in Wirklichkeit fast immer eines oder mehrere davon."

Er zeigt auf das erste Wort: „**Vertraulichkeit** bedeutet, dass nur die richtigen Personen auf eine Information zugreifen dürfen und alle anderen nicht. Stell dir dein Bankkonto vor: du willst, dass niemand außer dir den Kontostand sieht oder deine Überweisungen mitliest."

Dann fährt er mit dem zweiten Punkt fort: „**Integrität** heißt, dass Informationen nicht unbemerkt verändert werden dürfen. Dein Kontostand