iXactly

Jacqueline Naumann

Die ganze Härte der ISO 27001

Ihr Kampf als Informationssicherheits-beauftragter (ISB)

Kommunikation Dokumentenlenkung Sicherheitsbereiche Ressourcen
Transport Politik Audit ISMS Scope Beweismittel Hochverfügbarkeit Drucker
Kontext Richtlinien Vertraulichkeit Betriebsmittel Monitoring Freigabe

2022

Kurzüberblick

Liebe Leserin, lieber Leser,

vielen Dank, dass Sie sich für dieses Buch entschieden haben.

Informationssicherheit ist immer ein brennendes Thema, das vor allem durch das IT-Sicherheitsgesetz 2.0 und die ISO/IEC 27001:2022 noch einmal für viele Organisationen an Fahrt aufgenommen hat.

Ich hoffe, ich kann Ihnen, liebe Informationssicherheitsbeauftragte und lieber Informationssicherheitsbeauftragter mit diesem Buch wertvolle Praxisbeispiele bieten, die Sie für Ihre Aufgaben nutzen können.

Herzlichst, Ihre Jacqueline Naumann
Trainerin, Beraterin, Auditorin

iXactly ist Ihr Dienstleister für Seminare, Beratung und Audits für Ihr ISMS.

Gostritzer Straße 63, 01217 Dresden www.ixactly.com

Vielen Dank
an Florentine Naumann für die Illustrationen im Buch!

Inhalt

Ihre Aufgaben als ISB sind nicht immer einfach

Ihr Kampf als ISB

1 Einleitung

Nach Ihrer Ernennung oder Berufung zum Informationssicherheitsbeauftragten mussten Sie sicherlich so einige Kämpfe austragen. Alle ISBs, mit denen ich bisher gesprochen habe, bestätigten mir dies.

ISO/IEC 27001 Kap. 10.2 Fortlaufende Verbesserung

Einige leiden in ihrer Rolle, andere hingegen sehen die Herausforderungen, die ein ISMS-Aufbau mit sich bringt als Chancen.

Auch wenn Sie glauben, Ihr ISMS vollständig aufgebaut zu haben, erlaubt Ihnen die ISO/IEC 27001 gar keine Fertigstellung. Die Norm-Anforderung dazu finden Sie im »Kapitel 10.2 Fortlaufende Verbesserung«. Das heißt, die Norm fordert uns auf, das ISMS in seiner Ausprägung fortlaufend weiter zu verbessern.

Mit diesem Buch will ich Ihnen deshalb wieder eine Reihe Praxisbeispiele vorstellen, anhand derer Sie möglicherweise neuen Input für Ihre Verbesserungen erhalten. Die größte Herausforderung besteht ab dem Jahr 2022 mit der Neuausgabe der ISO/IEC 27002 und deren vollständig überarbeiteten Struktur der Sicherheitsmaßnahmen. Das

führt zu einem geänderten »Anhang A« in der ISO/IEC 27001.

1.1 Bekanntmachung mit unserem Buch-ISB

Leser des ersten Bandes kennen unseren Buch-ISB und seine Mitmenschen bereits. Für alle anderen, die mit diesem Band in die Reihe »*Die ganze Härte der ISO 27001*« einsteigen, werden die Personen des Buches in den folgenden Zeilen kurz erläutert.

Im Buch werden viele Praxisbeispiele aus tatsächlich stattgefundenen Episoden wiedergegeben. Um die Anonymität zu gewährleisten, nutze ich sogenannte »schwarze Schafe«, denen ich alle Kuriositäten unterschiebe.

Mein schwarzes Schaf für unsere fiktive Organisation T34M heißt im Buch T34M-L34D. Bei T34M handelt es sich um eine fiktive Organisation, die unter anderem Nachrichten produziert sowie zu den KRITIS (kritische Infrastrukturen) im Bereich Medien zählt, von denen das IT-Sicherheitsgesetz fordert, ein ISMS aufzubauen.

Bei dem ISB, der im Buch interviewt wird oder einfach Tatsachen erzählt, handelt es sich um T34M-L34D.

Die Organisation hatte bei ihrer Gründung Freude daran, die Buchstaben E durch 3 und A durch 4 zu ersetzen, so wie es einige angehende Hacker in der Sprache Leet tun.

T34M-L34D steht stellverstretend für hunderte Kunden, Kollegen, Mitarbeiter und Seminarteilnehmer, mit denen ich in den mittlerweile über zwanzig Jahren gesprochen oder denen ich einfach nur zuge-hört habe.

T34M-L34Ds Erzählungen sind Praxisbeispiele, die Ihnen, in Ihrer Rolle als ISB zeigen sollen, dass sich in allen Organisationen teilweise recht kuriose Begebenheiten bezüglich Informationssicherheit ereignen.

T34M-BO$$ ist die oberste Leitung von T34M. Er kommt relativ wenig zu Wort, da T34M-L34D als ISB alle Aufgaben und Themen auf seinem Tisch hat und bearbeiten muss.

T34M-ADMIN ist als Administrator bei T34M beschäftigt.

T34M-EXTERNER ist ein fiktiver Dienstleister, dem alle Zitate von echten Dienstleistern untergeschoben werden.

1.2 Anonymität

Die vielen Zitate von Kunden, Lieferanten, externen Dienstleistern, ehemaligen Kollegen und auch Seminarteilnehmern sind anonymisiert. Für den Fall, dass der einen Leserin oder dem anderen Leser ein Zitat bekannt vorkommt, möchte ich anmerken, dass viele Herausforderungen nicht nur bei einer Organisation anzutreffen sind und sich deshalb Zitate auch ähneln können. Kein Leser muss in Sorge geraten, wenn er meint, sich in einem Zitat wiedererkannt zu haben. Die gesammelten Zitate umfassen einen zeitlichen Rahmen von über zwanzig Jahren.

1.3 Die Schwert-Symbolik

Das Cover des ersten Bandes zeigte ein Schwert, das noch aus dem Stein gezogen werden musste. Sie als damals neuer ISB zogen Ihr Schwert aus dem Stein, wie einst König

Artus sein Schwert Caliburn, um sich seiner neuen Aufgabe zu stellen.

Ihr eigenes Schwert steht nun kampfbereit auf einem steinigen Weg. Lesen Sie nun, wie es anderen ISBs auf ihren Wegen ergangen ist.

Viel Spaß beim Lesen und Lernen!