Vorwort zur zehnten Auflage

Geschätzte Leserinnen und Leser

Die Digitalisierung schreitet weiter voran. Immer grössere Teile unseres wirtschaftlichen Handelns und unseres Alltags verlagert sich in den virtuellen Raum – den Cyberspace. Dies bringt viele Vorteile mit sich, insbesondere für KMU, bei welchen Optimierungen in der Leistungserbringung zwingend notwendig sind um sich gegen allenfalls grössere Marktteilnehmer mit mehr freien Mitteln zu behaupten. Zum Beispiel können trotz unterschiedlichen Standorten, welche lokale Vorteile nutzen, Entscheide welche die ganze Firma betreffen ohne wesentliche Verzögerung oder teure Reisen gefällt und umgesetzt werden. Arbeitsschritte können stärker dezentralisiert und trotzdem abgestimmt gehalten werden, was wiederum in geringeren Produktionskosten oder schnellerer Time to Market resultiert. Es ergeben sich neue Marketing- und Absatzkanäle, oder gar ganz neue Märkte. Und der Einsatz von künstlicher Intelligenz erlaubt es sogar, dass sich zum Beispiel Fertigungsstrassen selbständig optimieren. Dies nur einige Vorteile.

Trotz all den Vorteilen die sich durch die Digitalisierung bieten, transferieren sich aber auch Risiken in den Cyberspace oder es entstehen gar ganz Neue. Die Basis, damit der Cyberspace möglichst gewinnbringend genutzt werden kann ist jedoch, dass die Risiken einerseits fassbar sind und andererseits in Einklang mit dem eigenen Risikoappetit gebracht werden können. Weiter geht es darum, beim Eintritt eines Cyberrisikos möglichst effizient die negativen Effekte zu beschränken und schnell wieder operativ zu sein. Cybervorfälle lassen sich nie ganz ausschliessen.

Die Informationssicherheit spielt eine zentrale Rolle ob eine Firma langfristig erfolgreich sein kann oder nicht. Einerseits, ist es die Verantwortung der Geschäftsleitung, des Verwaltungsrates und des höheren Managements den Risikoappetit des jeweiligen Verantwortungsbereiches zu definieren und laufend zu überprüfen. Dort wo das Risiko nicht akzeptabel ist, müssen diese Entscheidungsträger dann Investitionen in die Umsetzung von Massnahmen tätigen und deren Effektivität überprüfen. Nur so kann eine Firma resilient sein und trotzdem ökonomisch agieren. Im vorliegenden Buch werden Instrumente zum Management der Informationssicherheit vorgestellt. Die beschriebenen Methoden und Mittel ermöglichen es, von der Technik über die Geschäftsprozesse bis hin zu der Steuerung und Überprüfung auf den obersten Verantwortungsstufen stringente und auf die Unternehmensbedürfnisse angepasste Massnahmen umzusetzen.

Andererseits spielen immer mehr auch rechtliche Aspekte eine wichtige Rolle. Datenschutz ist ein zentraler Aspekt, wenn es darum geht, das Vertrauen der Kunden zu gewinnen und auch zu behalten. Aber auch Compliance und Governance Anforderungen die es – speziell im Zusammenhang mit Finanztransaktionen – zu beachten gilt dürfen nicht unterschätzt werden. Und dann muss man natürlich auch gegenüber seinen Lieferanten die rechtlichen Aspekte und Haftungspflichten bezüglich Vorfällen entsprechend adressieren.

Nicht zu Letzt thematisiert dieses Buch auch die technische und organisatorische Informationssicherheit. Der Kern der Sache, wenn man so will – ist doch die Technik und der Umgang mit ihr zentral in der Digitalisierung.

Das Zusammenbringen dieser Aspekte in einem Buch liefert eine gute Basis, damit Sie in ihrer Funktion ihre Unternehmung sicherer machen können. Gleichzeitig hilft das Buch auch ein Verständnis für Themen der Informationssicherheit, welche vielleicht nicht direkt im eigenen Aufgabenfeld liegen zu fassen und vor allem – und das ist das wichtigste – die Zusammenhänge der verschiedenen Aspekte der Informationssicherheit zu verstehen. Denn am Schluss ist Informationssicherheit immer ein Querschnittsthema, das die ganze Unternehmung betrifft und immer im Kontext der Geschäftstätigkeit gesamtheitlich betrachtet werden muss.

Ich wünsche Ihnen viel Spass bei der Lektüre.

Florian Schütz

Direktor Bundesamt für Cybersicherheit