Abstract

Informationssicherheit ist in der heutigen Zeit ein sehr verbreitetes und viel diskutiertes Thema. Jeden Tag erreichen uns Nachrichten über verschiedene Angriffe, die zum Teil grosse und finanzstarke Firmen treffen und schädigen. Aufgrund dieser Vorkommnisse fragen sich viele Schweizer KMU, wie es um ihre Informationssicherheit steht und wie sie allenfalls zielgerichtet investieren könnten. Damit diese Fragen beantwortet werden können, muss die Informationssicherheit von Prozessen, Systemen und Organisation gemessen werden. Es gibt viele verschiedene Standards und Best-Practices–Sammlungen, wie z.B. ISO 2700X-Reihe, COBIT 5, ITIL V3 2011 oder BSI, die für die meisten Unternehmen nicht praktikabel sind, da die Einstiegshürden zu hoch sind. Das Ziel der Forschungsarbeit ist es, einen Ansatz in Form eines Frameworks zu entwickeln, mit dem ein KMU die Informationssicherheit eines Systems oder des ganzen Unternehmens messen kann. Der Ansatz muss einfach, schnell und günstig sein und so eine realistische Anwendung finden. Es wurden die Forschungsfragen gestellt, ob Informationssicherheit gemessen werden kann, wie sie gemessen werden kann und aus welchem Aspekt und wie ein Framework zum Messen der Informationssicherheit aussehen könnte. Als Forschungsvorgehen und Methodik wurde Design Science, genauer der Design Science Research Cycle nach Hevner et al. (2007) gewählt. Die drei Cycle Rigor, Design und Relevance wurden angewendet. Der Rigor Cycle bei der Untersuchung von bestehenden Standards und Best Practices sowie anderen Ansätzen, der Design Cycle bei der Entwicklung des Frameworks und der Relevance Cycle beim Proof of Concept in einem Unternehmen und zusätzlichen Experteninterviews. Die Forschungsarbeit hat gezeigt, dass die bestehenden Standards und Best Practices im Bereich der Messung von Informationssicherheit noch nicht viel zu bieten haben, aber eine gute Basis für die Massnahmenentwicklung bereitstellen. Die Gegenüberstellung hat ergeben, dass sich in der jetzigen Form kein Standard zur Messung der Informationssicherheit eignet. Die Messung stellt einen wichtigen Teil der Informationssicherheit dar, jedoch sind in diesem Bereich noch sehr viele Aspekte zu klären. Die Messmethode scheint mit dem GQM-Paradigma gefunden worden zu sein. Die Informationssicherheit lässt sich also tatsächlich messen und zwar am besten unter dem Effektivitätsaspekt. Dieses Paradigma ist auch der Kern des entwickelten Frameworks, wobei noch verschiedene Probleme bestehen bleiben. Der erste praktische Einsatz hat jedoch positive Ergebnisse geliefert. Ein Klärungsbedarf besteht weiterhin beim Begriff der Informationssicherheit, der noch nicht klar definiert zu sein scheint (Heinzmann, 2016). Allgemein sind sich die Experten nicht einig, wie mit dem Thema Messbarkeit von Informationssicherheit umgegangen werden soll.