Informationssicherheit und Datenschutz in Steuerbüros: Herausforderungen und Maßnahmen

Bachelorarbeit

zur Erlangung des akademischen Grades „Bachelor of Science (B.Sc.)“
im Studiengang Wirtschaftswissenschaft der
Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: Lehmann-Bues Vorname: Emily

[redacted] [redacted] [redacted] [redacted]

Prüfer: Prof. Dr. Michael H. Breitner

Alfeld, den 26.07.2021

INHALTSVERZEICHNIS

1. Einleitung

Die Sicherheit von wertvollen persönlichen Informationen und der Schutz persönlicher beziehungsweise personenbezogener Daten spielen im jetzigen Zeitalter weltweiter Vernetzung und Digitalisierung eine immer größere und bedeutende Rolle.
Hacker- beziehungsweise Cyberangriffe, die große Unternehmen und staatliche Institutionen in den Fokus nehmen und zum Verlust von Informationen oder zum völligen Stillstand des Geschäftsbetriebs führen, lassen die Gefahren deutlich in den Vordergrund treten. Die Nutzung personenbezogener Daten zur Manipulation von Wahlen, das gezielte Ausspionieren von Reportern und Politikern verdeutlichen die Notwendigkeit des Schutzes von persönlichen Daten.

Die Begriffe Informationssicherheit, Datenschutz und IT-Sicherheit verschwimmen in der Wahrnehmung der Öffentlichkeit oftmals miteinander. Gesetzliche Regelungen und die unternehmerische Verantwortung und Pflicht zum Schutz des eigenen Betriebes vor Schaden sind oftmals unklar und werden undifferenziert mit IT-Sicherheit gleichgesetzt.
Schnell wird klar, dass ein solch komplexer und verantwortungsvoller Aufgabenbereich von Fachleuten übernommen werden sollte. Unternehmen investieren in ihre IT-Sicherheit und denken es ist das gleiche wie Informationssicherheit: Unternehmen und Behörden unterscheiden nicht gut genug zwischen IT- und Informationssicherheit[1].
Letztlich steht hinter allem die Notwendigkeit Risiken für eine Unternehmung und eine unternehmerische Handlung einzuschätzen, zu bewerten und angemessene und wirksame Maßnahmen gegen fiktive und aber auch reale Bedrohungen zu ergreifen.

Das gilt im privaten Bereich zum Schutz der eigenen Informationen, aber umso mehr für Unternehmen, wie zum Beispiel die in dieser folgenden Forschungsarbeit untersuchten Steuerbüros. Gerade in Steuerbüros stellen Informationen die Basis der unternehmerischen Arbeit und die eigentlichen Unternehmenswerte dar, die es gilt zu schützen. Bei einem Verlust oder der ungewollten Offenlegung von Mandantendaten drohen hohe Bußgelder oder der Vertrauensverlust von Seiten der Mandanten, was letztendlich das gesamte Geschäftsmodell der Steuerberatung gefährdet und zur Verletzung von Berufspflichten führt.

[1] Vgl. Kilian, *Einführung in Informationssicherheitssysteme(I): Begriffsbestimmung und Standards*, 2006, S. 651

Um am Ende dieser vorliegenden Forschungsarbeit ein aussagekräftiges und konkretes Ergebnis zu erhalten habe ich folgende zwei Forschungsfragen aufgestellt:

1. Wie ist die IT-Infrastruktur in deutschen mittelständischen Steuerbüros aufgebaut?

2. Welche Maßnahmen wurden in deutschen mittelständischen Steuerbüros ergriffen um den Schutz personenbezogener Daten (Datenschutz) sicherzustellen?

Zur Beantwortung dieser Forschungsfragen werden im ersten Teil dieser Arbeit zunächst die gesetzlichen Vorgaben und Regelungen zur Informationssicherheit und zum Datenschutz erläutert. Außerdem wurde ein Fragebogen an 31 mittelständische Steuerbüros verteilt, mit dem sich die Forschungsfragen äußerst konkret beantworten lassen.

7. Zusammenfassung und Ausblick

Ziel dieser vorliegenden Forschungsarbeit war es, aufzuzeigen, wie die Anforderungen an die Informationssicherheit und die gesetzlichen Vorgaben der Datenschutzgrundverordnung in deutschen mittelständischen Steuerbüros umgesetzt wurden.

Dafür wurden zunächst die einzelnen Themen *Informationssicherheit, Informationssicherheitsmanagement, Datenschutz* und *Risikomanagement* beschrieben.
Das grundlegende Prinzip der Informationssicherheit beruht auf dem Schutz der drei Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität. Dies bezieht sich sowohl auf analoge als auch digitalisierte Informationen.
Das Informationssicherheitsmanagement, sprich das Management, welches für die Sicherstellung der Informationssicherheit verantwortlich ist, gehört untrennbar zu den Organisationspflichten eines Unternehmers. Hierfür ist der PDCA-Zyklus ein gängiges Hilfsmittel, um den Prozess beziehungsweise den Lebenszyklus der Informationssicherheit zu beschreiben. In vier Phasen wird das Informationssicherheitsmanagement geplant und konzeptioniert, die Planung umgesetzt, die Zielerreichung kontrolliert und überwacht und schließlich optimiert und verbessert.
Um die Anforderungen an den Datenschutz und den damit verbundenen Schutz personenbezogener Daten vor Dritten bestmöglich umzusetzen und zu gewährleisten, gibt der Gesetzgeber ein Mindestmaß an Methoden und Maßnahmen vor, die sogenannten TOMS.
Das Risikomanagement ist vermutlich die Kernaufgabe eines Managements in Bezug auf Informationssicherheit und Datenschutz. Erst durch eine Risikoanalyse und eine Visualisierung der identifizierten Risiken in Form einer Risikomatrix lassen sich die Schwachstellen des bisherigen Informationssicherheitsmanagements und der Anforderungen an den Datenschutz feststellen. Durch das Ergreifen von geeigneten und wirtschaftlich sinnvollen Maßnahmen soll der Eintritt von Risiken bzw. das Ausmaß potenzieller Schäden reduziert oder zumindest die Eintrittswahrscheinlichkeit verringert werden.

Im Folgenden wurde der gesetzliche Rahmen in Form von Gesetzen und Standards definiert und abgesteckt.
Dabei wurde deutlich, dass es seit langer Zeit schon gesetzliche Vorgaben an den Datenschutz gibt. Seit dem Jahr 2000 und der Unterzeichnung der EU-

Grundrechtecharta wurde der Datenschutz zum Grundrecht für alle in der EU lebenden Menschen. Eine Konkretisierung und Hilfe zur einheitlichen Umsetzung bietet seit 2016 die EU-Datenschutzgrundverordnung. Diese regelt den Umgang mit und die Verarbeitung von personenbezogener Daten EU-weit für alle Mitgliedsstaaten. Sie lässt jedoch an manchen Stellen die Ausarbeitung offen und bietet den Mitgliedsstaaten die Möglichkeit durch nationales Recht zu ergänzen. Dies hat Deutschland in Form des Bundesdatenschutzgesetztes (BDSG) getan.
Im Gegensatz zu diesen lange existierenden nationalen und EU-weiten Gesetzen gibt es erst seit dem Jahr 2015 in Form des IT-Sicherheitsgesetzes eine gesetzliche Regelung bezüglich der Informationssicherheit an sich und deren Geltungsbereich. Die zunehmenden Bedrohungen durch die kritischen Infrastrukturen (KRITIS), die das öffentliche Leben aufrechterhalten, machte dieses Gesetz notwendig.
Außerdem bildeten sich sowohl auf nationaler als auch auf internationaler Ebene sogenannte Standards, die Hilfeleistungen im Umgang mit dem Informationssicherheitsmanagement, durch den BSI-Standard 200-1 oder aber auch bei der Umsetzung der Anforderungen an den IT-Grundschutz, durch den BSI-Standard 200-2 bieten. Auf nationaler Ebene werden diese Standards durch das Bundesamt für Sicherheit und Informationstechnik zusammengetragen. International werden die Standards durch die Organisation mit dem Namen ISO verfasst.

Aufgrund der vielfältigen Tätigkeiten eines Steuerbüros und des ständigen Umgangs und Verarbeitung von Daten, wurde im Folgenden die aktuelle Umsetzung der Anforderungen an die Informationssicherheit und an den Datenschutz anhand eines Fragebogens in Steuerbüros untersucht, analysiert und an geeigneten Stellen mit den gesetzlichen Vorgaben in Beziehung gesetzt. An dieser Stelle wurde deutlich, dass der Großteil der Steuerbüros auf die Dienste der DATEV-Anwendungen zurückgreift. Dieser zertifizierte Dienstleister stellt seinerseits zum einen die IT-Sicherheit und den Datenschutz im eigenen Bereich sicher. Jedoch wurden auch Schwachstellen zum Beispiel in Form der zum Teil fehlenden Firewall zur Absicherung der eigenen internen IT-Infrastruktur deutlich. Insbesondere wurde aber deutlich, dass der Faktor Mensch als Risikofaktor für die Informationssicherheit noch nicht ausreichend erkannt wurde, so dass entsprechende Schulungen noch nicht zum Standard gehören.

Die vorliegende Forschungsarbeit und der ausgewertete Fragebogen kann jedoch nicht jede Schwachstelle zufriedenstellend hinterfragen. Dafür reicht der vorgegebene Rahmen nicht aus. Vielmehr kann nur die aktuelle Situation dargestellt und Schwachstellen benannt werden, die optimiert und verbessert werden sollten.
Um die Schwachstellen in deutschen mittelständischen Steuerbüros weiterführend detailliert zu hinterfragen, bedarf es weiteren Forschungsarbeiten.