Carl Schilling

Carl Schilling hat 2018 sein Abitur am Gymnasium Dresden Plauen erfolgreich abgelegt. Anschließend hat er an der Berufsakademie Sachsen – Staatliche Studienakademie Dresden sein Duales Bachelorstudium in der Fachrichtung Wirtschaftsinformatik begonnen und 2021 abgeschlossen. Sein Praxispartner war die Saxonia Systems AG, welche im Jahr 2019 durch Carl Zeiss Jena übernommen wurde und seitdem als Carl Zeiss Digital Innovation GmbH firmiert.

Kontakt: Carl.Schilling@hotmail.de

ISO 27001 im Home Office

Carl Schilling

Aufgrund der Covid 19-Pandemie, welche im Januar 2020 begann, wurden viele Betriebe geschlossen. Dies bezog sich vor allem auf Kultur und Gastronomie. Aber auch Unternehmen, welche Mitarbeiter haben, die nicht in direktem Kundenkontakt stehen, mussten Möglichkeiten finden ihre Mitarbeiter zu schützen. Die Lösung, welche der IT-Dienstleisterbranche aufgrund der Arbeitsbedingungen entgegenkam, war die Arbeit im „Home Office". Gleichermaßen gewann die ISO 27001-Norm an Bedeutung für Unternehmen in dieser Branche, was an steigenden Zahlen zertifizierter Unternehmen zu sehen ist. Daraus entstand das Thema für die Bachelorarbeit: „ISO 27001 im Home Office". Die Kernfrage ist, inwiefern eine ISO 27001-Zertifizierung für Unternehmen mit Mitarbeitern im Home Office möglich ist. Um diese Frage zu beantworten, wird zuerst geklärt, was die Arbeit im Home Office ausmacht und wie diese von der Telearbeit und dem mobilen Arbeiten abzugrenzen ist. Folgend wird auf die ISO 27001-Norm und deren Inhalt eingegangen. Dies dient als Grundlage zur Beantwortung der zentralen Frage.

The Covid19-pandemic, which began in January 2020, led to the temporary shutdown of many businesses. This concerned mainly companies in the cultural and gastronomic sectors. However, also companies with employees who have no direct contact with customers had to come up with ways to protect their employees. Remote work turned out to be the most suitable solution for the IT service provider industry and its particular working conditions. Similarly, the ISO 27001 standard gained importance for companies in this industry, which can be seen in the increasing number of certified companies. This leads to the topic for the bachelor thesis: "ISO 27001 in the home office". The key question is whether ISO 27001 certification is possible for companies with employees working remotely from home. In order to answer this question, clarification is first provided as to what constitutes work in a home office and how this is to be differentiated from teleworking and mobile working. This is followed by a discussion of the ISO 27001 standard and its contents. This serves as the basis for answering the central question.

Einleitung

Die Arbeit beschäftigt sich mit der ISO 27001 im Home Office. Dabei ist die Kernfrage, inwiefern eine Umsetzung dieser ISO-Norm für ein Unternehmen, welches als IT-Dienstleister tätig ist und Mitarbeiter im Home Office hat, möglich ist. Um diese Frage zu beantworten, wird zuvor definiert, was ein Home Office ist und was diese Arbeitsform ausmacht. Auch wird eine Abgrenzung des Begriffs zu der Telearbeit und dem mobilen Arbeiten durchgeführt. Dies soll als Grundlage und Verständnisklärung des Begriffs Home Office dienen. Folgend wird die ISO 27001-Norm betrachtet. Thematisiert werden dabei die Inhalte der ISO 27001-Norm selbst und inwiefern diese gegebenenfalls die Arbeit im Home Office bereits abdecken. Auch wird dabei der Zertifizierungsprozess betrachtet. Ziel dabei ist, zu klären, ob die ISO 27001-Norm so aufgebaut ist, dass sie theoretisch auch im Home Office Anwendung finden kann. Ausgehend von der Vermutung, dass ebendiese im Home Office angewendet werden kann, soll überprüft werden, ob seitens der Arbeit im Home Office eine Erfüllung der Anforderungen möglich ist.

Methodik

Grundlage dieser Arbeit sind zwei zentrale Aspekte. Das Repertory Grid, welches der Definition und Abgrenzung des Begriffs Home Office dient und eine tiefgreifende Analyse des Inhalts der ISO 27001-Norm. Das Repertory Grid wurde aus folgenden Gründen gewählt: Es dient der Abgrenzung verschiedener Begriffe und zweigt gleichzeitig, dass diese Gemeinsamkeiten besitzen. Ist ein Repertory Grid korrekt umgesetzt, ist es selbst der Beweis, dass sich Begriffe vergleichen lassen und gleichzeitig die Grundlage für die Abgrenzung dieser. Die inhaltliche Analyse der ISO 27001 geschieht an ebendieser. Der Fokus dabei liegt auf Einschränkungen, die möglicherweise durch das Home Office aufgehoben bzw. die Arbeit im Home-Office nicht abgedeckt sind. Um die zentrale Frage zu klären, wird überprüft, inwiefern die Inhalte der ISO 27001-Norm die Arbeit abdecken und umgekehrt inwiefern eine Umsetzung dieser Anforderungen im Home Office möglich ist.

Home Office

Es wird oftmals von Home Office oder der Arbeit im Home Office gesprochen. Was jedoch genau dieser Begriff bedeutet, ist von Quelle zu Quelle verschieden. Kerninhalt ist jedoch immer das Arbeiten im Home Office. Um dies zu verdeutlichen, folgen Definitionen aus verschiedenen Quellen.
Im Anschluss daran wurde eine Definition verfasst, welche die Grundlagen der vorangegangenen enthält und somit die Basis für diese Arbeit darstellt.

„Home Office beschreibt den Arbeitsplatz im eigenen Wohnraum. Bei der Einrichtung dieses Arbeitsplatzes müssen Vorgaben durch das Unternehmen beachtet werden. Gesetzliche Vorgaben hinsichtlich der Einrichtung gibt es, aufgrund der fehlenden vertraglichen Festlegungen wie bei der Telearbeit, nicht."

Um auch die Begriffe Telearbeit und mobiles Arbeiten zu definieren, damit diese im Repertory Grid verwendet werden können, sind folgende Definitionen notwendig:
„Telearbeitsplätze sind vom Arbeitgeber fest eingerichtete Bildschirmarbeitsplätze im Privatbereich der Beschäftigten, für die der Arbeitgeber eine mit den Beschäftigten vereinbarte, wöchentliche Arbeitszeit und die Dauer der Einrichtung festgelegt hat. Ein Telearbeitsplatz ist vom Arbeitgeber erst dann eingerichtet, wenn Arbeitgeber und Beschäftigte die Bedingungen der Telearbeit arbeitsvertraglich oder im Rahmen einer Vereinbarung festgelegt haben und die benötigte Ausstattung des Telearbeitsplatzes mit Mobiliar, Arbeitsmitteln einschließlich der Kommunikationseinrichtungen durch den Arbeitgeber oder eine von ihm beauftragte Person im Privatbereich des Beschäftigten bereitgestellt und installiert ist."

„Mobiles Arbeiten [ist] nicht an den häuslichen Arbeitsplatz gebunden und ist auch weder durch eine Verordnung noch gesetzlich geregelt. Beschäftigte können vielmehr von unterschiedlichen Arbeitsorten über mobile Endgeräte wie Smartphones oder Laptops auf die Informations- und Kommunikationstechnik des Betriebs zugreifen."
Die Methodik des Repertory Grid zeigt sich wie folgt: Drei Begriffe werden hinsichtlich verschiedener Eigenschaften voneinander abgegrenzt. Dabei ist zu beachten, dass eine gewählte Eigenschaft immer auf zwei der Begriffe zutrifft und auf einen nicht. Somit wird bewiesen, dass die Begriffe vergleichbar sind, da sie Gemeinsamkeiten haben. Auch wird durch eine Eigenschaft immer eine Abgrenzung geschaffen. Folgend das Repertory Grid für die Begriffe Home Office, Telearbeit und mobile Arbeit. „1" bedeutet „trifft zu", „0" bedeutet „trifft nicht zu" und „0-1" bedeutet „trifft teilweise zu".

Eigenschaft	Arbeit im Home Office	Telear-beit	Mobiles Arbeiten
Fester Arbeitsstandort	1	0	0
Gesetzliche Vorgaben zu diesem Begriff	0	1	1
Beschreibung einer Arbeitsart	1	1	1
Beschreibung für den Arbeitsort/das Arbeiten von Zuhause	1	1	0
Gleiche Arbeits-bedingungen für Mitarbeiter:innen	1	1	0
Arbeitsplatz im Unternehmen	0	0-1	0-1
Verschiedene Formen	0	1	1

Tabelle 1: Repertory Grid (Quelle: Eigene Darstellung)

Dem Repertory Grid ist zu entnehmen, dass eine einfache Abgrenzung dieser Begriffe nicht trivial ist, da sie sich in verschiedenen Bereichen überschneiden. Alle drei Begriffe beschreiben nach den Definitionen in dieser Arbeit eine Arbeitsart. Jedoch kann dies schon in verschiedenen Definitionen abweichen. Eine Gemeinsamkeit aller ist, dass der Arbeitsplatz nicht im Unternehmen sein muss. Bei der Telearbeit und dem mobilen Arbeiten kann es jedoch vorkommen, dass die Arbeit teilweise im Unternehmensgebäude durchgeführt wird. Home Office und Telearbeit können nach verschiedenen Definitionen auch als gleicher Begriff gewertet werden. Wichtig für die Abgrenzung zur mobilen Arbeit ist, dass diese von überall stattfinden kann und keinen festen Standort hat. Bei der Arbeit im Home Office hingegen ist dieser Standort festgeschrieben, und zwar ist es der Wohnsitz der entsprechenden Mitarbeiter. Ein weiterer Unterschied zwischen der Arbeit im Home Office und den anderen beiden Begriffen ist, dass nur bei Home Office genau bekannt ist, wie die Arbeitsform ist. Sowohl bei der Telearbeit als auch bei dem mobilen Arbeiten ist dies nicht der Fall. Das liegt daran, dass die beiden Begriffe jeweils in verschiedene Formen dieser Arbeitsweise unterteilt werden können.

ISO 27001

Die ISO 27001 gehört zur Familie der ISO 27000-Normen. Die Norm 27000 gibt für die 27001 und andere 270XX Normen (wobei X eine Ziffer darstellt) die Rahmenbedingungen vor. Die ISO 27001 selbst gibt die Anforderungen an ein Informationssicherheitsmanagementsystem vor. Ihr Inhalt besteht aus den Kapiteln Einleitung, Anwendungsbereich, Normative Verweisungen, Begriffe, Kontext der Organisation, Führung, Planung, Unterstützung, Betrieb, Bewertung der Leistung, Verbesserung. Die Analyse aller Kapitel ergab, dass die Anforderungen der ISO 27001 so formuliert sind, dass sie auch in der Arbeit im Home Office Anwendung finden. Seitens der Norm ist eine Umsetzung möglich. Der Zertifizierungsprozess, bestehend aus der Audit-Vorbereitung, dem Stufe 1-Audit, dem Stufe 2-Audit und der Entscheidung über die Zertifizierung, muss jedoch noch angepasst werden. Das Stufe 1-Audit ist gleichermaßen umsetzbar, da es sich hierbei um eine Analyse der Dokumentation des erstellten Informationssicherheitsmanagementsystems handelt. Diese Dokumente werden der Prüfstelle übergeben und ausgewertet. Das Stufe 2-Audit dient der Überprüfung, ob die dokumentierten Vorgaben auch so umgesetzt werden. Dabei sind die Prüfer in das Unternehmen gekommen und haben das Unternehmensgebäude vor Ort inspiziert und Befragungen der Mitarbeiter durchgeführt. Sind die Mitarbeiter jedoch im Home Office, ist eine Überprüfung der Büros nicht nur sehr umständlich, sondern rechtlich auch nicht erlaubt. Zudem muss eine Befragung der Mitarbeiter vorher geplant werden, um diese auch zu erreichen und nicht ihren Arbeitsprozess zu stören. Ist dieses Audit durchgeführt, wird entschieden, ob das Unternehmen eine Zertifizierung erhält. Dabei gibt es die Möglichkeiten, dass zu viele Mängel vorhanden waren, um eine Zertifizierung auszustellen, dass einige Mängel vorhanden waren, aber eine Zertifizierung ausgestellt wurde mit der Auflage, diese Mängel zu beheben oder dass eine Zertifizierung ohne Feststellung von Mängeln erteilt wird.

ISO 27001 im Home Office

Es stellt sich heraus, dass durch die Arbeitsweise der Arbeit im Home Office neue Risiken entstehen, zu denen Maßnahmen gefunden werden müssen. Diese Risiken richtig zu identifizieren und die Maßnahmen entsprechend zu gestalten, ist aktuell noch eine Herausforderung. Das liegt daran, dass die Arbeit im Home Office erst seit kurzer Zeit so intensiv genutzt und umgesetzt wird. Es gibt für die in dieser Arbeit genannten Problemkonstellationen mögliche Lösungen, um die Anforderungen zu erfüllen. Wird Home-Office-Arbeit länger von verschiedenen Firmen umgesetzt, so kann sich auch ein Standard für die Umsetzung dieser Arbeitsweise herausbilden. Zukünftig können Unternehmen, welche Zertifizierungen anbieten, sich auch auf das Thema Home Office für diese spezialisieren. Dadurch wird den Unternehmen geholfen, Lösungen für die dadurch entstehenden Anforderungen zu finden. Auch ist es möglich, dass eine ISO-Zertifizierung mit Mitarbeitern im Home Office möglich ist, jedoch durch die neuen, noch teilweise unbekannten Bedingungen einen Mehraufwand für Unternehmen darstellt. Wird sich die Arbeit weiterhin in diese Richtung entwickeln, so werden sich auch Standards für die Arbeit im Home Office bilden. Diese werden dann zur Folge haben, dass eine Zertifizierung unter diesen Arbeitsumständen nicht nur möglich, sondern auch ohne den großen Mehraufwand, wie er jetzt existiert, umsetzbar ist. Zukünftig können Unternehmen untersuchen, wie die Arbeitsbedingungen in der Home-Office-Arbeit sind. Basierend darauf können Unternehmensprozesse so angepasst werden, dass diese auch für Mitarbeiter im Home Office umsetzbar sind. Eine weitere Möglichkeit kann eine Vereinbarung sein mit verbindlichen Vorgaben und Standards, welche die Mitarbeiter bei der Arbeit im Home-Office umsetzen müssen.

Literatur:

§ 2 ArbStättV – Einzelnorm, in: https://www.gesetze-im-internet.de/arbst_ttv_2004/__2.html (abgerufen am 11.06.2021).

Deutsches Institut für Normung, Entstehung einer Norm, in: https://www.din.de/de/ueber-normen-und-standards/din-norm (abgerufen am 17.04.2021).

Homeoffice in: https://www.arbeitszeit-klug-gestalten.de/alles-zu-arbeitszeitgestaltung/arbeitszeitmodelle-im-ueberblick/homeoffice/?L=0 (abgerufen am 11.06.2021).

International Standardisation Organisation, About us, Members, in: https://www.iso.org/members.html (abgerufen am 10.06.2021).

International Standardisation Organisation, DIN ISO/IEC 27001.

International Standardisation Organisation, ISO/IEC 27000:2018.

International Standardisation Organisation, ISO/IEC 27005:2018-07: International Standardisation Organisation.

Kraus, S.; Grzech-Sukalo, H.; Rieder, K. (2020): Mobile Arbeit – Home-Office, Dienstreisen, Außendienst – was ist wirklich belastend?, in: Z. Arb. Wiss. 74.

Kühl, S.; Strodtholz, P.; Taffertshofer, A., (Hg.) (2009:) Handbuch Methoden der Organisationsforschung, Quantitative und qualitative Methoden, 1. Auflage, Wiesbaden: Springer.

Lanwehr, R.; Mayer, J. (2018): People Analytics im Profifußball, Wiesbaden: Springer Fachmedien.

Rump, J.; Eilers, S. (2019): Arbeitszeitpolitik, Berlin, Heidelberg: Springer