©Tierney – stock.adobe.com

Qualität erfordert sichere IT

Weiterentwicklung der ISO 9001 in Richtung eines sicheren IT-Einsatzes

Die Cybermafia hat gerade erst begonnen, den Angriff auf KMU zu starten, die 85 Prozent der deutschen Wirtschaft ausmachen. Die wenigsten dieser kleinen und mittleren Unternehmen haben ausreichende Ressourcen in Form von Wissen, Personal und geeigneten digitalen Strukturen, um ihre IT abzusichern. Daher bedarf es einer optimierten ISO 9001, die einen übergreifenden Ansatz von Qualität und Digitalisierung bietet und dazu anregt, sich mit den Risiken der Digitalisierung zu beschäftigen.

Christian Stahlbusch und Michael Redey

Heute betreibt jedes Unternehmen wichtige Verwaltungs-, Steuerungs-, Kommunikations- und Produktionsbereiche mittels IT-gestützter, digitaler Systeme und Technik (Hard- und Software). Der Begriff „IT“ (Information Technology) schließt Prozesse und Infrastrukturen mit ein. Die Qualitätssicherung dient der Erfüllung von Anforderungen seitens Kunden, Stakeholdern, gesetzlichen und behördlichen Institutionen, spricht also alle interessierten Parteien an und ist ein wesentliches Merkmal der QM-Norm ISO 9001.

Die Covid 19-Pandemie bringt den Unternehmen größere Einschränkungen als man je erwartet hätte. Diese Einschränkungen reichen in alle Prozesse hinein und erfordern zumindest eine gut funktionierende Kommunikation mit allen interessierten Parteien. Die IT musste in den meisten Unternehmen an diese neuen Pandemie-Anforderungen angepasst werden, um Homeoffice und Remote Work zu ermöglichen. Alleine die Anbindung der Homeoffice-Systeme verlangt nach Sicherheitsmaßnahmen um die Unternehmen vor Angriffen bzw. auch vor Schadsoftware zu schützen. Zudem zeigt sich in der Krise, wie wichtig durchgängige und stabile (interne und

externe) Kommunikationsketten bzw. leistungsfähige Internetplattformen (Marktplätze) sind. Dennoch ist auch hier der Grundsatz „Organisation vor Technik“ zu berücksichtigen.

Ohne eine Absicherung der relevanten Prozesse, Informationen, Verwaltungs-, Entwicklungs-, Steuerungs- und Produktionsanlagen scheitert der Qualitätsanspruch beim ersten Störfall. Die Auswirkungen von Datenverlust, -verfälschung oder -diebstahl sind mit enormem Imageverlust und finanziellen Schäden verbunden. Die Folgen können bis zum Totalausfall der Technik bzw. zum Konkurs eines Unternehmens führen, mindestens aber zu Beeinträchtigungen der Produktion und der gesamten Lieferkette .

Um aus Sicht der ISO 9001 den Aspekten Risikomanagement und Compliance mehr Aufmerksamkeit zu schenken, müssen auch neue IT bzw. die eingesetzten Produktionstechnologien und deren Prozesse bezogen auf die Sicherheit berücksichtigt werden. Unternehmen sollten also auch auf die Risiken und Gefahren angemessen reagieren können, die durch den Einsatz digitaler Produktions-, Steuerungs- und Verwaltungssysteme entstehen.

Daher sollte das Ziel verfolgt werden, Unternehmen intensiver auf die Dringlichkeit der Absicherung ihrer Infrastrukturen und IT bzw. ihrer eingesetzten Technologien, Prozesse sowie auf den Schutz von Unternehmenswerten (Daten, Produktionsanlagen, IT etc.) vorzubereiten.

Die Praxis zeigt aber immer wieder, dass vor allem kleine und mittlere Unternehmen gar nicht oder nur unzureichend auf die Digitalisierung vorbereitet sind. Das belegen u.a. aussagefähige Statistiken des Bundesamts für Informationssicherheit (BSI) und zunehmende Angriffe auf Unternehmen, Behörden sowie systemkritische Infrastrukturen (Krankenhäuser, Verwaltung etc.).

Zur Sensibilisierung der Unternehmen sollte die aktuell gültige Norm ISO 9001:2015 daher um weitere konkrete Anforderungen zur Absicherung der Unternehmen, der Anforderngen von Gesetzgeber und Kunden (Compliance) und zwingend um die Minimierung von Risiken erweitert werden. Uns ist bewusst, dass wir hiermit kein umfassendes Sicherheitssystem etablieren können, dennoch soll dies ein Anstoß zu weiteren Maßnahmen liefern (z. B. Zertifizierung nach ISO 27001).

Verbesserungsvorschlag für eine weiterentwickelte ISO 9001

Wir haben darum einen Vorschlag zur Optimierung der ISO 9001:202x erarbeitet. Dieser wurde Mitte September 2020 dem DIN-Normenausschuss Qualitätsmanagement, Statistik und Zertifizierungsgrundlagen (NQSZ) NA 147-00-01 AA „Qualitätsmanagement“ zur Prüfung und Aufnahme vorgelegt. Hier die einzelnen Themen:

Compliance

Sofern gesetzliche oder vertragliche Anforderungen bestehen, gilt es diese kurz und knapp zu formulieren und zu dokumentieren. Neben den Vorgaben zur Einhaltung sind auch die Konsequenzen von Verletzungen der Compliance zu dokumentieren. Zudem müssen Audits die Einhaltung von Verträgen bzw. Internen und externen Richtlinien und Vorgaben sicherstellen.

Dafür ist die Einordnung der eingesetzten Technologie (IT-, Produktions-, Überwachungs-, Steuerungs-, Verwaltungs- und Kommunikationstechnik und deren Infrastrukturen und Prozesse) nach ihrer Wertigkeit und Bedeutung notwendig. Alle wichtigen Technologien sind zu erfassen und ihre Bedeutung ist zu dokumentieren, etwa auf einer Skala von 1 bis 5. Neben der Wichtigkeit sollten auch der Zweck und die Zielerreichung einer Technik beschrieben werden.

Risikomanagement und Ziele

Hier geht es um die Ermittlung von Risiken für und aus dem Einsatz von IT (inkl. Infrastrukturen und Prozesse) im Unternehmen. Für die jeweilige digitale Technik sind die Risiken zu ermitteln, welche sich durch den Betrieb ergeben können. Das Risiko ist zu bewerten und Maßnahmen zur Beseitigung bzw. Minderung des Risikos zu beschreiben (Risikomanagement). Zudem müssen Risiken von den Verantwortlichen für die jeweilige Technik und ggf. von der Geschäftsleitung getragen und verantwortet werden. Änderungen an einer eingesetzten Technik muss daher auch geplant, getestet und abgenommen werden. Ebenso muss ggf. eine neue Risikoanalyse, -bewertung und -übernahme erfolgen.

Die Risikobetrachtung ist zu dokumentieren. Schutzziele sind abzuleiten und ebenfalls zu dokumentieren. Hier können Standards für das Risikomanagement angewandt werden, die die ISO 9001:2015 heute schon im Ansatz fordert.

Infrastruktur, Prozessumgebung und Information

Hier wird die Ermittlung des individuellen Schutzniveaus und -bedarfs der jeweiligen Technik adressiert. Auf Basis der Bedeutung einer Technik ist das Schutzniveau und der Schutzbedarf zu ermitteln. Außerdem sind dafür geeignete Maßnahmen zu realisieren, zu dokumentieren und zu überwachen. Dazu sind auch die gespeicherten und zu verarbeitenden Daten im Interesse der Parteien zu berücksichtigen.

Planung von Änderungen, Steuerung und Überprüfung

Der Einsatz von IT bedarf u.a. einer Planung und Dokumentation wichtiger technischer Funktionen im Sinne nachvollziehbarer Beschreibungen für die Betreiber und Bediener. Dazu zählen Anforderungen und Einsatz, Handhabung, Wartungsbedarf, »»

Besonderheiten etc. Die Antrags- und Genehmigungs-, sowie Einführungsstufen der IT unterliegen geregelten und dokumentierten Prozessen. Die Dokumentation muss für Dritte nachvollziehbare und verständliche Aussagen enthalten.

Organisation der Wartung

Hier geht es um die Festlegung des Wartungsbedarfs und -umfangs, um Termine, Firmen, Verträge, um interessierte Parteien, die Steuerung nichtkonformer Prozesse, die Ableitung und Dokumentation der gesetzlichen und vertraglichen Anforderungen an die jeweilige IT inklusive der Konsequenzen bei Störungen oder Ausfällen. Für die Behebung von Störungen, Ersatzstellungen und Wartungsaktivitäten sollten mit Partnern Verträge geschlossen werden, in denen u.a. auch die Reaktionszeiten und Kommunikationswege festgelegt sind.

Verbesserung

Verbesserung beschreibt die Maßnahmen zur Behebung von aktuellen Störfällen und Fehlern zur Schadensbegrenzung. Dazu gehört auch die Abwehr und Wiederaufnahme der Produktion bzw. Verarbeitung.

Richtlinien

Erstens geht es um Richtlinien für die Anschaffung, den Aufbau, den sicheren Betrieb, die Pflege und Wartung der IT. Für die Anschaffungs- und Infrastrukturmaßnahmen sind Ressourcen zu planen und bereitzustellen (Changemanagement).

Zweitens geht es um die Dokumentation von internen und externen Vorgaben aus Regelwerken für die Implementierung und Nutzung von IT. Die internen Prozesse müssen die Vorgaben und deren Umsetzung gemäß den Anforderungen aller Parteien sicherstellen. Diesbezüglich sind auch Schulungen sowie dokumentierte Vorgaben (Richtlinien, Anweisungen etc.) u.a. auch als Nachweis (im Sinne der Compliance) erforderlich.

Notfallmanagement, Notfallpläne und -übungen

Regelungen zur Behandlung von Notfällen und Störungen der IT-Technik, sowie die Bereitstellung von Ersatztechnik und Infrastruktur, inklusive erforderlicher Ausstattung, Ersatzstellung für wichtige Einrichtungen der Infrastruktur (Kühlung, Be- beziehungsweise. Entwässerung, unterbrechungsfreie Stromversorgung, Technik und Know-how). Auch hier helfen standardisierte Vorgehensweisen, um entsprechende Maßnahmen zu ergreifen.

Rollen, Wissen, Kompetenz und Bewusstsein

Festlegung von direkten Verantwortlichen und Vertretern inkl. deren Befugnisse für IT und Prozesse. Schulungen aller beteiligten Parteien (ggf. auch Externe). Funktions- und Stellenbeschreibungen sind heute Routinen, die diese Anforderungen unterstützen. Im Hinblick auf die Einführung und Weiterentwicklung der Technik muss die Weiterbildung auch aktuelle Sicherheitsstandards vermitteln (s. Richtlinien)

Nachhaltigkeit und Ressourcen

Nachhaltigkeit beinhaltet ein bewusstes, verantwortungsvolles Handeln, welches die vorhandenen Ressourcen schont. Es geht um die Anpassung:

- der eingesetzten Ressourcen,
- der internen und externen Abläufe unter Berücksichtigung von Vorgabenm
- der logistischen und administrativen Abläufe sowie
- der Arbeitsplätze und Arbeitsbedingungen

Zunächst sind alle Aspekte zu analysieren, um sie dann optimal anzupassen. Ein Blick ins Unternehmen sollte zeigen, welche Ressourcen hier hauptsächlich eingesetzt werden, für die sich Risiken ergeben bzw. die Risiken verursachen können (z.B. die Ausstattung der Arbeitsplätze oder Arbeitsprozesse). Diese sollten ergonomisch und notwendige Wege kurz sein. Der wertschöpfende Nutzen der vorhandenen Flächen sollte berücksichtigt werden.

Am Beginn einer digitalen Ära

Unausgereifte oder veränderte Systeme, Prozesse und Technik sind potenzielle Einfallstore für Cyberkriminelle. Sie wollen Daten kompromittieren, verschlüsseln, erpressen, abgreifen und an unseriöse Marktbegleiter weiterverkaufen. Betroffene Unternehmen verschwenden Unsummen an Geld und Ressourcen, um verschlüsselte Daten zu rekonstruieren, Erpresser ermitteln zu lassen, Lieferausfälle zu kompensieren und befallene IT zu bereinigen. Von den Nachwirkungen im Sinne der DSGVO und Strafgesetzen ganz zu schweigen, denn bei Verletzungen der Compliance werden drastische Bußgelder bzw. Strafen mit Abführung der Gewinne verhängt.

Wir stehen heute noch am Anfang einer sich rapide ändernden Gesellschaft, die ohne Digitalisierung die Corona-bedingten Einschränkungen in den Unternehmen nicht bewältigen kann. Die Cybermafia hat gerade erst begonnen, den Angriff auf KMU zu starten. Ohne eine ausreichend abgesicherte IT wird künftig kein Unternehmen mehr in der Lage sein, seinen Zweck zu erfüllen, Qualität zu liefern und die Lieferkette aufrecht zu erhalten.

Eine optimierte ISO 9001 könnte neben anderen etablierten Normen auch ein Mittel sein, um dieses Ziel zu erreichen und den Weg zu einer sichereren Digitalisierung zu ebnen. ■

INFORMATION & SERVICE

VORGESCHICHTE

Am 2.10.2020 tagte der DIN-Normenausschuss NA 147–00–01 AA „Qualitätsmanagement". Die Autoren hatten in einer Web-Konferenz die Möglichkeit, ihren Optimierungsvorschlag dem DIN-Normenausschuss NA 147–00–01 AA „Qualitätsmanagement" vorzustellen. Der eingereichte Vorschlag wurde durch das DIN-Gremium vorbewertet. Für den Fall, dass eine Revision der ISO 9001:2015 durch das ISO-Gremium TC 176 beschlossen wird und die erste Revision der ISO 9001:202x als Draft vorliegt, kann dieser Vorschlag weiter ausgearbeitet und konkretisiert beim DIN eingereicht werden.

AUTOREN

Christian Stahlbusch ist seit 2011 Leitender Auditor in der Zertifizierung von Managementsystemen für diverse Standards, u. a. ISO 9001 und BSIG §8a Kritis V bei der TÜV Nord Cert GmbH, Hagen.
Michael Redey ist freiberuflicher Revisor, Auditor, Berater und externer Datenschützer . Er unterstützt Firmen bei der Einführung und dem Betrieb der Informationssicherheitssysteme nach ISO 27001 und deren Zertifizierung bis in den Bereich Kritischer Infrastrukturen (KRITIS).

KONTAKT

Christian Stahlbusch
T 02508 1889
team-iso9001–202x@e-mail.de