GUTcert Interview

Digitale Gesundheitsanwendungen und Informationssicherheit

Im Oktober 2021 führte GUTcert-Mitarbeiterin Bozena Jakubowska im Nachgang zu einer Konferenz ein Interview zum Thema ISMS in der Medizinbranche mit Ulrich Wegener, Auditor bei der Berlin Cert und Wissenschaftler im Fachgebiet Medizintechnik.

Die letzten Jahre waren für die Medizinbranche sehr bedeutsam. Nicht nur die Folgen der Covid-Pandemie, auch oder vor allem die Automatisation fast aller Prozesse und der zunehmende Anteil an Künstlicher Intelligenz in allen Bereichen trugen dazu bei.

Während des Medical Devices Day beim Johner Institut wurde von Prof. Dr. Christian Johner angekündigt, dass mit fortschreitender Technologieentwicklung auch die formalen Anforderungen zunehmen werden – was bei vielen kleinen und mittelgroßen Unternehmen dazu führen wird, dass sie nach Möglichkeiten zu einer Kostensenkung suchen müssen. So werden wahrscheinlich fast 50% der Unternehmen die eigene Produktpalette reduzieren müssen, da das gesetzliche Einführen und Weiterentwickeln neuer Produkte schlicht zu teuer ist. Das allerdings wäre fatal und ein Schritt in die falsche Richtung, da gerade im Bereich Medizin ständig innovative Lösungen gefordert sind.

Eine der gesetzlichen Anforderungen bezieht sich auf Datensicherheit und Datenschutz von digitalen Gesundheitsanwendungen (DiGA): Alle Firmen, die sich mit digitalen Gesundheitsanwendungen beschäftigen, müssen ab dem 1. Januar 2022 über ein ISMS-Zertifikat verfügen.

Ulrich Wegener, Auditor bei der Berlin Cert und selbst seit Jahren in der Medizinbranche unterwegs, brachte in einem Gespräch mit unserer Mitarbeiterin Bózena Jakubowska Licht ins Dunkel: Er erläuterte, was wirklich angepasst werden muss, und wie man sich möglichst schmerzlos auf eine Zertifizierung des ISMS vorbereiten kann.

GC: Bei der Konferenz erfuhren wir von vielen Aspekten des Medizingeschäfts. Wie schätzen Sie die Lage der Branche ein?

Wegener: Die Branche ist durch die Einführung der Medical Device Regulation (MDR) noch immer in hohem Maß damit beschäftigt, ihre technische Dokumentation entweder für die neuen Vorgaben anzupassen oder Produkte vom Markt zu nehmen. Aber gerade kleine Firmen, die gemeinsam mit der MDR neu an den Markt kommen, können die neuen Anforderungen unvoreingenommen umsetzen.

GC: Die Digitale-Gesundheitsanwendungen-Verordnung ist ein Fakt. Was würden Sie Herstellern von digitalen medizinischen Produkten empfehlen? Welche Herausforderungen sehen Sie und wie kann man „smart" damit umgehen? Lässt das Gesetz eine gewisse Interpretationsfreiheit?

Wegener: Die Verordnung gibt ziemlich klare Hinweise darauf, was wie umzusetzen ist, damit eine DiGA auch als solche anerkannt wird und Erstattungsleistungen seitens der Kostenträger fließen. Insbesondere die Selbsterklärung nach Anlage I der Verordnung ist hier zu nennen. Das Fast-Track-Verfahren nach § 139e SGB V bietet den Herstellern digitaler Gesundheitsanwendungen eine transparente Möglichkeit, ihr Produkt zügig auf den Markt zu bringen.

Ihre Ansprechpartnerin:
Bozena Jakubowska
bozena.jakubowska@gut-cert.de
+49 30 2332021-65

GUTcert AFNOR Group
GUT Certifizierungsgesellschaft für Managementsysteme mbH
Umweltgutachter
Eichenstraße 3 b, 12435 Berlin

GUTcert Interview

GC: Was kann als Basis für das Umsetzen eines Informationssicherheits-Managementsystems (ISMS) dienen? Welche Unterschiede gibt es zwischen den Systemen und welche würden Sie empfehlen?

Wegener: Nach Punkt 1 der Basisanforderungen, die für alle digitalen Gesundheitsanwendungen gelten, muss der Hersteller die Frage beantworten, ob er ein Informationssicherheits-Managementsystem gemäß ISO/IEC 27000-Reihe, BSI-Standard 200-2 oder ein vergleichbares System umgesetzt hat und ob er auf Verlangen des Bundesinstituts für Arzneimittel und Medizinprodukte ein entsprechendes anerkanntes Zertifikat oder einen vergleichbaren Nachweis vorlegen kann.

Der Hersteller ist also frei in der Wahl des Systems. Empfehlen würde ich ein System der ISO/IEC 27000-Reihe denn es ist schlanker als andere: Der „Fragenkatalog" ist kleiner und auf das eigene Unternehmen anpassbar. Die ISO/IEC 27001 ist wie die EN ISO 13485 nach der High Level Structure geordnet und kann mit der EN ISO 27799 eine gute Ergänzung speziell für Gesundheitsanwendungen bieten.

GC: Demnach sollte das Einführen eines ISMS bei Unternehmen, die bereits ein ISO 13485 Zertifikat halten, ein wenig leichter sein. Gibt es etwas dabei, auf das man besonders achten sollte?

Wegener: Als Hersteller eines Medizinprodukts ist man mit der EN ISO 13485 vertraut, was liegt also näher, als ein integriertes Managementsystem zu schaffen und die ISO/IEC 27001 an das Qualitätsmanagementhandbuch (QMH) der EN ISO 13485 anzubinden? Dabei ist es wichtig zu erwähnen, dass die ISO/IEC 27001 kein QMH kennt. Wichtige Punkte sind hier die Risikoanalyse, /die aber keinen schrecken sollte, der die EN ISO 14971 beherrscht, und die „Erklärung der Anwendbarkeit", also der Nachweis, durch welche Maßnahmen der Schutz der Werte vor bestimmten Bedrohungen erreicht wird. Diese Erklärung ist Grundlage des Zertifikats.

GC: Welche Vorgehensweise würden Sie einem Hersteller empfehlen? Und wie lange dauert das Einführen eines ISMS?

Wegener: Wenn man die Idee hat, eine DiGA zu entwickeln und noch keine Berührung mit der EN ISO 13485 hatte, dann sollte man sich zunächst mit der ISO/IEC 27001 beschäftigen, um ein Gespür für die Norm zu bekommen: Sie ist relativ leichte Kost.

Die EN ISO 13485 bringt einen ganzen Strauß weiterer Normen mit, selbst wenn man sich vermeintlich nur auf die Entwicklung einer DiGA konzentriert. Hier kann man aber mit dem „Blick durch die Brille" der ISO/IEC 27001 relativ leicht deren Aspekte in die zu beschreibenden Prozesse der EN ISO 13485 integrieren. Dabei wird einem auffallen, wie klein der Fokus ist, den die EN ISO 13485 auf IT-Sicherheit selbst legt. Ein Nebeneffekt könnte zudem sein, dass einem klar wird, wie einfach alle Aspekte der DSGVO mit einem ISMS zu greifen sind. Die ISO/IEC 27001 ist für mich das Managementsystem für die DSGVO.

Sie fragten nach der Dauer der Einführung: Nun, bei einem kleinen Unternehmen ist man in ein paar Monaten durch, gefestigte Strukturen benötigen leider mehr Zeit, z. B. für die realistische Analyse des Ist-Zustandes als Grundlage für die Risikobewertung.

Ihre Ansprechpartnerin:
Bozena Jakubowska
bozena.jakubowska@gut-cert.de
+49 30 2332021-65

GUTcert AFNOR Group
GUT Certifizierungsgesellschaft für Managementsysteme mbH
Umweltgutachter
Eichenstraße 3 b, 12435 Berlin

GUTcert Interview

GC: Kennen Sie vielleicht noch andere Hilfsmittel, die bei der Umsetzung eines ISMS in der Medizinbranche hilfreich sein können?

Wegener: Aktuell haben wir eine Checkliste erarbeitet, anhand derer jeder Interessierte prüfen kann, ob das etablierte ISMS die Mindestanforderungen an ein System nach ISO/IEC 27001 erfüllt. Die Checkliste kann aber keine Risikoanalyse ersetzen, hier werden wir aber demnächst in einem Leitfaden weitere Hinweise geben können.

GC: Welches Feedback bekommen Sie von den Unternehmen?

Wegener: Die Einführung eines weiteren Managementsystems wird häufig zunächst als Bürde empfunden. Wenn aber der Gedanke eines integrierten Systems verfängt, dann rücken die Vorteile in den Vordergrund der Betrachtung. Ist der Wert eines Managementsystems für die Anforderungen der DSGVO erstmal erkannt, dann hat man den Damm durchbrochen. Bisher hat sich das Feedback immer ins Positive gewandelt.

GC: Welche Rolle spielt für Sie die Zertifizierungsbranche?

Wegener: Die Digitalen Gesundheitsanwendungen starten in einer Zeit, in der die Branche unter der Einführung der MDR ächzt – es gibt bereits einen Stau bei den benannten Stellen für die MDR. Zusätzlich wird nun noch ein Mehrbedarf bei den akkreditierten Stellen für die ISO/IEC 27001 generiert und weitere Zertifizierungen im Bereich der IT-Sicherheit werden in der nächsten Zeit kommen.

So ist leider absehbar, dass Medizinprodukte oft nicht zu dem Zeitpunkt verfügbar sein werden, wo sie für den Menschen gebraucht werden. Hier kann man der Zertifizierungsbranche keinen Vorwurf machen, denn ein Aufwuchs ist nicht so schnell geschaffen, wie ein Fast-Tack einer DiGA.

WIR WOLLEN GEMEINSAM BESSER WERDEN.

Ulrich Wegener
Auditor ISO13485:2016, Wissenschaftler im Fachgebiet Medizintechnik

Bozena Jakubowska
Produktmanagerin ISMS, GUTcert

Ihre Ansprechpartnerin:
Bozena Jakubowska
bozena.jakubowska@gut-cert.de
+49 30 2332021-65

GUT Certifizierungsgesellschaft für Managementsysteme mbH
Umweltgutachter
Eichenstraße 3 b, 12435 Berlin