Impressum

mt | medizintechnik

erscheint 6-mal jährlich
140. Jahrgang / Ausgabe 3.2020

Schwerpunktthema
Cybersicherheit, DSGVO

Redaktion
Iris Bings | bings@mt-medizintechnik.de
Markus Kemm | kemm.markus@mt-medizintechnik.de

Unter Mitarbeit von
Frank J. Schmitz | schmitz@mt-medizintechnik.de

Redaktion www.mt-medizintechnik.de
Mirjam Bauer | bauer@mt-medizintechnik.de

Redaktionsbeirat
C. Backhaus | claus.backhaus@fh-muenster.de
C. Bulitta | c.bulitta@oth-aw.de
H.-D. Dejon | HansDieter.Dejon@t-online.de
M. Fiebich | fiebich@web.de
G. Haufe | buero@ibhaufe.de
D. Hochmann | david.hochmann@fh-muenster.de
J. Held | juergen.held@hfg-gmuend.de
A. Keller | andreas.keller@tu-ilmenau.de
M. Kindler | manfred.kindler@fbmt.de
M. Regner | maic.regner@uniklinikum-dresden.de
R. Stender | rstender@prosystem-nsf.com

Verlag
TÜV Media GmbH
Am Grauen Stein 1, 51105 Köln
Postfach 903060, 51123 Köln
Tel.: 0221/806-3535, Fax: 0221/806-3510
tuev-media@de.tuv.com
www.tuev-media.de
Geschäftsführerin: Gabriele Landes

Koordination
Dr. Benita Herder | benita.herder@de.tuv.com
Tel.: 0221/806-3517

Anzeigenverwaltung
Speitkamp Werbe- und Verlagsgesellschaft
Stephan Speitkamp | tuev@wa-sp.de
Tel.: 02407/916266

Satz: DSV, Bernd Meier, Stockhausen

Druck: Medienhaus Plump GmbH, Rheinbreitbach

Bezugs- und Lieferbedingungen
Jahresabonnement Inland: 69,90 EUR zzgl. Versandkosten.
Einzelheft: 15,– EUR zzgl. Versandkosten.
Studentenabonnement: 30,– EUR zzgl. Versandkosten.
Preisänderungen vorbehalten.
Kündigung: bis 6 Wochen zum Ende eines Kalenderjahres schriftlich an den Verlag. Inlandspreise inkl. MwSt. Der Abonnementspreis wird jährlich im Voraus in Rechnung gestellt oder bei Teilnahme am Lastschriftverfahren jährlich abgebucht.
Bei Nichterscheinen der Zeitschrift ohne Verschulden des Verlages oder infolge höherer Gewalt entfällt für den Verlag jegliche Lieferpflicht. – Anzeigenpreise nach Tarif vom 1.1.2020. Informationen und Angebote über Netzwerklizenzen erhalten Sie beim Verlag direkt. – Mit der Annahme von Originalbeiträgen zur Veröffentlichung erwirbt der Verlag das uneingeschränkte Verfügungsrecht.

Titelfoto
Quelle: © www.stock.adobe.com/envfx

Hinweis für Autoren
Unter: www.mt-medizintechnik.de/Kontakt;
Manuskripte sind einzusenden an:
redaktion@mt-medizintechnik.de

G 8770 F
ISSN 0344-9416

Quelle: © www.stock.adobe.com/envfx

Schwerpunktthema
Cybersicherheit, DSGVO

Internetsicherheit und Datenschutz – wichtiger denn je!

Die Informations- und Kommunikationstechnologie (IKT) ist eine der zurzeit wichtigsten Schlüsseltechnologien und gewinnt auch im Gesundheitswesen mit seinen mehr als fünf Millionen Beschäftigten zunehmend an Bedeutung. Digitale Technologien helfen uns, die Herausforderungen, vor denen jetzt alle Gesundheitssysteme der Welt stehen, zu lösen. Sie ermöglichen eine bessere und effizientere Versorgung und einen breiteren Zugang zu medizinischer Expertise, insbesondere auch in abgelegenen Regionen. Auch neue Formen einer besseren Betreuung von Patienten im häuslichen Umfeld können mit ihr realisiert werden.
Eine weitere Schlüsseltechnologie für die Zukunft ist die künstliche Intelligenz (KI). Sie wird dazu beitragen, die aktuellen Herausforderungen des Gesundheitswesens zu meistern, die Qualität der medizinischen Versorgung zu steigern und das Gesundheitswesen gleichzeitig finanzierbar zu halten. Gerade in der Diagnostik verspricht die künstliche Intelligenz große Erfolge – sie wird dafür sorgen, dass Diagnosen präziser und schneller erstellt werden können.

Informationsflut erfordert Regulative

Aber im Zuge der zunehmenden Digitalisierung im Gesundheitswesen wächst auch der Umfang der Informationen, die für die Steuerung und Überwachung der Patienten verwendet werden. Für die Gestaltung des Gesundheitswesens muss es gelingen, diese Datenschätze nachvollziehbar zu erschließen, zu überprüfen und vor unbefugtem Zugriff zu schützen.
Ziel muss es sein, in der Zukunft valide Daten zu nutzen, um Zusammenhänge aufzuzeigen und Ansätze zu finden, wie Krankheiten und Risiken besser identifiziert werden können. Präventionen und Therapien lassen sich dann frühzeitiger einleiten.
Dabei sind neben den technologischen Anforderungen an die Interoperabilität auch mögliche Anpassungen datenschutzrechtlicher Regelungen und die Diskussion gesellschaftlich akzeptierter Weiterentwicklungen der Rahmenbedingungen zu berücksichtigen. Umso wichtiger ist es, dass es stets aktuelle regulatorische und normative Anforderungen an die Sicherheit und Leistung solcher IKT-Systeme und Medizinprodukte im Gesundheitswesen gibt.

Veraltete Normen und Sicherheitslücken

Bedingt durch die COVID-19-Pandemie wurde am 23. April 2020, unter vielen weiteren Notfallverordnungen, die Verordnung (EU) 2020/561 des europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) 2017/745 über Medizinprodukte unterzeichnet. Es bedurfte also einer Pandemie, um die lang ersehnte Verschiebung des Geltungsbeginns einiger Bestimmungen der Verordnung (EU) 2017/745 um ein Jahr auf den 26. Mai 2021 politisch durchzusetzen.
Die meisten Wirtschaftsakteure, Benannten Stellen und Behörden begrüßen die Verlängerung der Übergangszeit um ein Jahr. Aber es gibt auch kritische Stimmen, gerade zum Thema Sicherheit und Leistung von Medizinprodukten. Wenn man sich die am 24. März 2020 veröffentlichte Liste über die harmonisierten Normen für Medizinprodukte zur Umsetzung der jetzt noch bis zum 26. Mai 2021 gültigen Richtlinie 93/42/EWG ansieht, sind diese kritischen Stimmen berechtigt. Hier wird auf Normen verwiesen, die teilweise älter als 20 Jahre sind und sicherlich nicht mehr den Stand der Technik beschreiben. Diese veralteten Normen dürfen die Hersteller von Medizinprodukten bis zum 26. Mai 2021 nun jedoch weiterhin anwenden und behaupten, ihr Produkt erfülle die Anforderungen an Sicherheit, Leistung und den Stand der Technik. Dabei fehlen weiterhin harmonisierte Normen zu aktuell wichtigen Themen wie Künstliche Intelligenz, Gesundheitssoftware, Internetsicherheit (Cybersecurity) und Datenschutz in der Medizintechnik.
Wo bekommen die Hersteller jetzt die nötigen Informationen und Anleitungen her, um den tatsächlichen Stand der Technik zu berücksichtigen und für die Sicherheit und Leistung ihrer Medizinprodukte und Dienstleistungen gewissenhaft Verantwortung zu übernehmen? Diese Frage stellt sich nicht von ungefähr, denn bereits jetzt nutzen Cyberkriminelle die COVID-19-Pandemie, um ihre Malware möglichst effizient mit Phishing-Mails zu verbreiten: Die beiden Sicherheitsfirmen Sophos und Kaspersky entdeckten bereits Anfang März 2020 einen stetigen Anstieg an Phishing-Mails mit Bezug auf COVID-19. Cyberkriminelle versuchen, sich die Krise zunutze zu machen, indem sie schädliche Dateien in E-Mails einschleusen, die einen vermeintlichen Bezug zu Corona haben oder vortäuschen, dass sie von Behörden oder öffentlichen Organisationen, wie zum Beispiel der WHO, versendet wurden.
Aber nicht nur die Hersteller von Medizinprodukten sind betroffen, sondern auch die zuständigen Überwachungsbehörden, Benannten Stellen und Labore benötigen diese wichtigen Informationen und Anleitungen für die sichere Prüfung und Überwachung von Medizinprodukten.

Home-Office ohne Security?

Erschwerend kommt hinzu, dass im Zuge der Pandemie in kürzester Zeit eine Vielzahl von Arbeitsplätzen im privaten Umfeld nachgebildet werden mussten, um Betriebsabläufe weiterhin aufrechtzuerhalten. Während technisch gut aufgestellte Organisationen, Benannte Stellen und Behörden ihre Mitarbeiter mit professionellem IT-Equipment ausgestattet und umfangreich geschult haben, wird jetzt – ohne Risikobewertung – das Heimnetzwerk und eigene Hardware verwendet, um personenbezogene oder gar Patientendaten zu bearbeiten. Bei solchen spontanen Lösungen für mobiles Arbeiten können in der Regel nicht alle Anforderungen für IT-Sicherheit vollständig umgesetzt werden. Schnelle und stabile Netzwerkanschlüsse, der Aufbau von VPN-Lösungen sowie die Anschaffung

geeigneter Hardware lassen sich nur schwer zeitnah bewerkstelligen. Also bleiben die IT-Sicherheit und der Datenschutz definitiv auf der Strecke. Datenschutzbeauftragte stehen hier vor einer der größten Herausforderungen seit der Veröffentlichung der Datenschutzgrundverordnung (DSGVO) im Mai 2016. Es war noch nie einfacher, mit krimineller Energie an geheime bzw. geschützte Daten heranzukommen oder Softwareanwendungen zu manipulieren, denn welches Home-Office ist schon nach ISO 27001 zertifiziert?

Leitlinien und Lösungen

Die von der europäischen Kommission eingesetzte Medical Device Coordination Group (MDCG) veröffentlicht fleißig nicht gesetzlich verbindliche („non-binding") Leitlinien zur Umsetzung der Anforderungen der Verordnung (EU) 2017/745. Als eine gute Informationsquelle zum Thema Cybersecurity in der Medizintechnik hat sich die MDCG-Leitlinie MDCG 2019-16 herausgestellt. Da aber einige Inhalte – zum Teil leider nicht vollständig – aus dem AMII-Papier *TIR57:2016 – Cybersecurity in Medical Devices* übernommen wurden, möchte ich Ihnen an dieser Stelle empfehlen, zusätzlich diese Guideline zu lesen.
Im April 2020 wurde darüber hinaus eine Leitlinie für die Benannten Stellen (MDCG 2020-4) veröffentlicht, die sich mit dem Thema Remote Audits (Fernaudits) während der COVID-19-Pandemie und Reisebeschränkungen beschäftigt. Remote Audits bieten die Möglichkeit, herkömmliche Auditmethoden zu ergänzen oder zu ersetzen und dabei Reisekosten und Zeit für An- und Abreise einzusparen. Zudem können potenzielle Risiken, die mit Vor-Ort-Audits verbunden sind, wie zum Beispiel die Kontamination von Arbeitsbereichen oder Sicherheitsrisiken für Auditoren, verringert werden. Angesichts der zunehmenden technischen Lösungen ergeben sich vielfältige Möglichkeiten zur Integration von computergestützten Auditverfahren in bestehende Auditprogramme. Remote Audits sind besonders sinnvoll, wenn ein Unternehmen mehrere Standorte hat oder wenn die Vor-Ort-Auditierung mit Problemen verbunden ist, wie die aktuellen Reisebeschränkungen schmerzhaft demonstrieren, oder auch wenn gesundheitliche oder produktbezogene Risiken vorliegen.
Aber um störungsfreie und effektive Remote Audits durchführen zu können, bedarf es einer sehr guten Vorbereitung. Dies betrifft insbesondere die Bereitstellung einer funktionsfähigen, zuverlässigen und sicheren technischen Infrastruktur in Verbindung mit der notwendigen Kompetenz bei Auditoren und Inspektoren. Denn welcher Hersteller möchte gerne seinen Abweichungsbericht oder die Technische Dokumentation seiner Medizinprodukte im Internet wiederfinden?

Ich wünsche Ihnen viel Freude beim Lesen dieser Ausgabe. Bleiben Sie gesund!

Randolph Stender
NSF PROSYSTEM GmbH