Bayerischer Landtag

19. Wahlperiode 11.02.2025 Drucksache 19/4538

Schriftliche Anfrage

der Abgeordneten **Roland Magerl, Andreas Winhart, Matthias Vogler, Elena Roon, Franz Schmid AfD**
vom 25.11.2024

Cybersicherheit von Herzimplantaten

Die Staatsregierung wird gefragt:

Antwort

des Staatsministeriums für Umwelt und Verbraucherschutz im Einvernehmen mit dem Staatsministerium für Gesundheit, Pflege und Prävention
vom 08.01.2025

1.1 Werden Patienten, die ein Herzimplantat erhalten, derzeit standardmäßig über die Cyberrisiken informiert?

1.2 Welche Maßnahmen sind geplant, um sicherzustellen, dass alle Patienten zukünftig über diese Risiken aufgeklärt werden?

1.3 Falls keine Maßnahmen geplant sind, warum nicht (bitte begründen)?

Zu den Fragen 1.1 bis 1.3 teilt das dafür verantwortliche Staatsministerium für Gesundheit, Pflege und Prävention (StMGP) Folgendes mit:

Die AfD verkennt, dass es in Deutschland keine Staatsmedizin gibt. Die Staatsregierung überwacht nicht die berufliche Tätigkeit von Ärztinnen und Ärzten. Diese üben einen freien Beruf aus und sind für ihr Tun selbst verantwortlich. Hierbei unterliegen sie einem engen Netzwerk an zivil-, straf- und berufsrechtlichen Regelungen.

Ärztinnen und Ärzte sind nach § 630e Bürgerliches Gesetzbuch (BGB) verpflichtet, den Patienten vor jeder ärztlichen Maßnahme über die damit verbundenen Umstände, Risiken, Alternativen und möglichen Folgen aufzuklären. Die Einwilligung des Patienten in einen medizinischen Eingriff ist nur nach ordnungsgemäßer Aufklärung wirksam.

2.1 Ist die Aufnahme von Cyberrisikofaktoren in die Einwilligungserklärung der Patienten bereits vorgesehen?

2.2 Falls nein, warum nicht (bitte begründen)?

2.3 Wie wird sichergestellt, dass diese Informationen regelmäßig aktualisiert werden, wenn neue Risikoinformationen verfügbar werden?

Zu den Fragen 2.1 bis 2.3 teilt das dafür verantwortliche StMGP Folgendes mit:

Siehe Frage 1. Ärztinnen und Ärzte sind verpflichtet, Patienten im Rahmen der Aufklärung vor einem medizinischen Eingriff auch über Risikofaktoren auf der Basis aktueller wissenschaftlicher Erkenntnisse zu informieren. Der Arzt hat seine Kenntnisse eigenverantwortlich auf dem neuesten Stand der Wissenschaft zu halten. Hat ein Patient infolge einer Sorgfaltspflichtverletzung oder eines Behandlungsfehlers des behandelnden Arztes einen Gesundheitsschaden erlitten, sind entsprechende Ansprüche gegen den Arzt (insbesondere Schadensersatz, Schmerzensgeld) vom Patienten vor den Zivilgerichten geltend zu machen.

3.1 Welche Schutzmaßnahmen werden ergriffen, um Herzimplantate vor Cyberangriffen zu schützen?

Ein Medizinprodukt muss unter Berücksichtigung seiner Zweckbestimmung den in Anhang I der Verordnung (EU) 2017/745 über Medizinprodukte festgelegten für das Produkt geltenden grundlegenden Sicherheits- und Leistungsanforderungen genügen. Für die Einhaltung und Gewährleistung der grundlegenden Sicherheits- und Leistungsanforderungen ist der Hersteller verantwortlich (Art. 10 Abs. 1 Verordnung (EU) 2017/745).

3.2 Falls keine Maßnahmen geplant sind, warum nicht (bitte begründen)?

Siehe Antwort zu Frage 3.1.

3.3 Gibt es regelmäßige Sicherheitsüberprüfungen der eingesetzten Technologien?

Hersteller von Medizinprodukten sind gemäß Art. 10 der Verordnung (EU) 2017/745 im Rahmen ihres Qualitätsmanagements zur Aufstellung, Anwendung und Aufrechterhaltung eines Systems zur Überwachung nach dem Inverkehrbringen gemäß Art. 83 der Verordnung (EU) 2017/745 verpflichtet. Zusätzlich benötigen die Hersteller ein Verfahren für die Meldung von schwerwiegenden Vorkommnissen und Sicherheitskorrekturmaßnahmen im Feld im Rahmen der Vigilanz. Auch das Management korrektiver und präventiver Maßnahmen und die Überprüfung ihrer Wirksamkeit sowie Verfahren zur Überwachung und Messung der Ergebnisse, Datenanalyse und Produktverbesserung sind hierbei verpflichtend.

Der Hersteller ist ebenfalls verpflichtet, im Rahmen seiner Überwachungstätigkeit nach dem Inverkehrbringen ggf. neue Risiken zu ermitteln, diese zu bewerten und entsprechende Maßnahmen einzuleiten. Die Verfahren der zuvor genannten Überwachungstätigkeiten des Herstellers werden im Rahmen der Herstellerüberwachung durch die Aufsichtsbehörden der Länder geprüft.

Schwerwiegende Vorkommnisse müssen innerhalb der in der Verordnung (EU) 2017/745 festgelegten Fristen an das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) gemeldet werden.

4.1 Gibt es bereits dokumentierte Fälle von Cyberangriffen auf Herzimplantate und, wenn ja, wie wurden diese Vorfälle gehandhabt?

Zum jetzigen Zeitpunkt ist im Zuständigkeitsbereich der bayerischen Aufsichtsbehörden für deren Hersteller und Bevollmächtigte kein Fall bekannt.

4.2 Welche spezifischen Cyberrisiken bestehen für verschiedene Arten von Herzimplantaten (z. B. Herzschrittmacher, Defibrillatoren)?

Die Risiken eines Cyberangriffs auf Herzimplantate sind abhängig von verschiedensten Faktoren wie Hersteller, Produkt, Soft- und Hardwarestand, Funktechnologie und weiteren und müssen vom Hersteller im Zuge des Risikomanagements bewertet werden. Anschließend muss der Hersteller geeignete Maßnahmen einleiten und umsetzen.

4.3 Wie werden Ärzte und medizinisches Personal in Bezug auf die Cybersicherheit von Herzimplantaten geschult?

Dazu teilt das dafür verantwortliche StMGP Folgendes mit:

Die ärztliche Fort- und Weiterbildung ist keine staatliche Aufgabe, sondern liegt in der Zuständigkeit der ärztlichen Selbstverwaltung.

Ärztinnen und Ärzte sind berufsrechtlich verpflichtet, sich in dem Umfang beruflich fortzubilden, wie es zur Erhaltung und Entwicklung der zu ihrer Berufsausübung erforderlichen Fachkenntnisse notwendig ist. Jede Ärztin und jeder Arzt entscheidet dabei eigenverantwortlich, in welchem Umfang und zu welchen Inhalten Fortbildungsveranstaltungen besucht werden. Denn letztlich haftet jede Ärztin und jeder Arzt für die ordnungsgemäße Durchführung ärztlicher Eingriffe auf Basis der aktuellen wissenschaftlichen Erkenntnisse.

Über die Cybersicherheit von Medizinprodukten informiert u. a. das BfArM auf seiner Homepage: www.bfarm.de[1]

Maßnahmenempfehlungen zur IT-Sicherheit werden auch auf den Webseiten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Verfügung gestellt. Dabei befasst sich der Expertenkreis CyberMed als Zusammenschluss von Vertretern von Industrie, Anwendern und Behörden mit dem Thema Cybersicherheit von Medizintechnik: www.allianz-fuer-cybersicherheit.de[2]

5.1 Welche Rolle spielen Hersteller von Herzimplantaten bei der Sicherstellung der Cybersicherheit ihrer Produkte?

Von den Herstellern wird ein Risikomanagementsystem wie in Anhang I Abschnitt 3 der Verordnung (EU) 2017/745 beschrieben eingerichtet, dokumentiert, angewandt und aufrechterhalten (Art. 10 Abs. 2 Verordnung [EU] 2017/745). Im Übrigen wird auf die Antwort zu Frage 3.1 verwiesen.

5.2 Gibt es Kooperationen mit IT-Sicherheitsfirmen, um die Sicherheit von Herzimplantaten zu verbessern?

Für die Einhaltung und Gewährleistung der grundlegenden Sicherheits- und Leistungsanforderungen ist der Hersteller verantwortlich (Art. 10 Abs. 1 Verordnung [EU] 2017/745). Im Übrigen wird auf die Antwort zu Frage 3.1 verwiesen.

5.3 Wie wird die Kommunikation zwischen Herzimplantaten und externen Geräten (z. B. Home-Monitoring-Systemen) gesichert?

Die Absicherung der Kommunikation zwischen verschiedenen Geräten erfolgt in Abhängigkeit vom Produkt und der verwendeten Funktechnologie. Dabei kommen verschiedenste Maßnahmen zum Einsatz, darunter z. B. Verschlüsselung, Authentifizierung, sichere Kanäle, Zugriffskontrollen, Einschränkung der Reichweite (Nahfeld), standardisierte Sicherheitsprotokolle oder die Anwendung von Normen.

---

1 https://www.bfarm.de/DE/Medizinprodukte/Aufgaben/Risikobewertung-und-Forschung/Cybersicherheit/_node.html

2 https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Netzwerk-Formate/Veranstaltungen-und-Austausch/Expertenkreise/CyberMed/cybermed_node.html

Die Marktüberwachung im Bereich der Richtlinie 2014/30/EU über die elektromagnetische Verträglichkeit und der Richtlinie 2014/53/EU über die Bereitstellung von Funkanlagen auf dem Markt obliegt der Bundesnetzagentur.

6.1 Welche gesetzlichen Regelungen gibt es derzeit in Bayern oder Deutschland, die die Cybersicherheit von medizinischen Implantaten betreffen?

Gesetzliche Anforderungen für Medizinprodukte sind auf europäischer Ebene in der Verordnung (EU) 2017/745 geregelt und gelten damit einheitlich für alle Mitgliedstaaten. Dazu ergänzend ist national das Medizinprodukte-Durchführungsgesetz einzuhalten.

6.2 Wie wird die Öffentlichkeit über die potenziellen Cyberrisiken von Herzimplantaten informiert?

Das BfArM veröffentlicht Informationen über Risiken, die von Medizinprodukten ausgehen. Sicherheitsanweisungen im Feld, die von einem Hersteller im Zusammenhang mit einer Sicherheitskorrekturmaßnahme im Feld an Anwender und Kunden übermittelt wurden, werden zusätzlich auf der Homepage des BfArM bereitgestellt: www.bfarm.de[3]

6.3 Welche Forschung wird aktuell betrieben, um die Cybersicherheit von Herzimplantaten zu verbessern?

Aktuelle Projekte des BSI im Bereich der Medizintechnik finden sich unter: www.bsi.bund.de[4]

7.1 Gibt es internationale Standards, die bei der Sicherstellung der Cybersicherheit von Herzimplantaten berücksichtigt werden?

Eine nicht abschließende Auflistung anwendbarer internationaler Standards: ISO 15408, UL 2900, ISO 13485, ISO 14971, IEC 60601-1, IEC 62304, IEC 80001-1, ISO 14971, IEC 62304, IEC 82304, AAMI TIR 57, UL2900-2-1, ISO 27001

7.2 Wie wird die Zusammenarbeit zwischen verschiedenen Gesundheitsinstitutionen und Behörden bei der Bewältigung von Cyberrisiken koordiniert?

Hersteller, Bevollmächtigte und Importeure, aber auch Anwender und Betreiber sind verpflichtet, Vorkommnisse an das BfArM zu melden. Das BfArM führt daraufhin eine Risikobewertung durch und legt mit dem Hersteller geeignete Maßnahmen und den zeitlichen Ablauf fest. Die Aufsichtsbehörden der Länder unterstützen das BfArM und überwachen die Abarbeitung der Maßnahmen.

Weiterführende Informationen finden sich beim BfArM: www.bfarm.de[5]

---

3 https://www.bfarm.de/DE/Medizinprodukte/Aufgaben/Risikobewertung-und-Forschung/Cybersicherheit/_node.html

4 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/E-Health/Medizintechnik/Projekte/projekte_node.html

5 https://www.bfarm.de/DE/Medizinprodukte/Antraege-und-Meldungen/Vorkommnis-melden/_node.html

7.3 Welche Maßnahmen werden ergriffen, um die Vertraulichkeit und Integrität der Daten, die von Herzimplantaten gesammelt werden, zu schützen?

Dazu teilt das dafür verantwortliche StMGP Folgendes mit:

Ärztinnen und Ärzte sind verpflichtet, Patientendaten vertraulich zu behandeln. Die allgemeinen Grundsätze des Datenschutzrechts, einschließlich der besonderen Vorschriften für Gesundheitsdaten, gelten selbstverständlich auch für Ärztinnen und Ärzte. Jede Ärztin und jeder Arzt hat eigenverantwortlich sicherzustellen, dass die datenschutzrechtlichen Anforderungen an den Schutz der Patientendaten (sei es in Papierform oder auf elektronischen Datenträgern) jederzeit gewahrt werden. Bei Verstößen gegen datenschutzrechtliche Vorgaben kann ein Patient ggf. Schadensersatzansprüche gegen den Arzt geltend machen oder eine Beschwerde beim Landesamt für Datenschutzaufsicht einreichen.

8.1 Gibt es spezielle Notfallpläne für den Fall eines Cyberangriffs auf Herzimplantate?

Dazu teilt das dafür verantwortliche StMGP mit:

Hierzu liegen dem StMGP keine Informationen vor.

8.2 Wie wird sichergestellt, dass ältere Herzimplantate, die möglicherweise weniger sicher sind, regelmäßig überprüft und ggf. aktualisiert werden?

Hierzu wird auf die Antwort zu Frage 3.3 verwiesen.

8.3 Welche Unterstützung erhalten Patienten, die sich Sorgen über die Cybersicherheit ihrer Herzimplantate machen?

Dazu teilt das dafür verantwortliche StMGP Folgendes mit:

In den ESC Pocket Guidelines der European Society of Cardiology (ESC) und der Deutschen Gesellschaft für Kardiologie zur Schrittmacher- und kardiale Resynchronisationstherapie wird als Ziel der Nachsorge die Gewährleistung der Patientensicherheit aufgeführt. Dabei besteht die Möglichkeit einer telemedizinischen Nachsorge als auch einer Fernüberwachung. Ansprechpartner für die Patienten sind die behandelnden Kardiologinnen und Kardiologen.

Hinweise des Landtagsamts

Zitate werden weder inhaltlich noch formal überprüft. Die korrekte Zitierweise liegt in der Verantwortung der Fragestellerin bzw. des Fragestellers sowie der Staatsregierung.

Zur Vereinfachung der Lesbarkeit können Internetadressen verkürzt dargestellt sein. Die vollständige Internetadresse ist als Hyperlink hinterlegt und in der digitalen Version des Dokuments direkt aufrufbar. Zusätzlich ist diese als Fußnote vollständig dargestellt.

Drucksachen, Plenarprotokolle sowie die Tagesordnungen der Vollversammlung und der Ausschüsse sind im Internet unter www.bayern.landtag.de/parlament/dokumente abrufbar.

Die aktuelle Sitzungsübersicht steht unter www.bayern.landtag.de/aktuelles/sitzungen zur Verfügung.