MDS MEDIZINISCHER DIENST DES SPITZENVERBANDES BUND DER KRANKENKASSEN

Aktuelles zu Auffälligkeiten bei Medizinprodukten

Essen, den 30.11.2018

Gefährliche Lücken bei der Cybersicherheit von Medizinprodukten

Menschen mit einem Herzschrittmacher oder einer Insulinpumpe müssen sich darauf verlassen können, dass die Geräte funktionieren und nicht von Unbefugten manipuliert werden können. Sicherheitsexperten einer US-amerikanischen IT-Firma fanden Lücken in der Datenkommunikation bei Herzschrittmachern und Insulinpumpen des Unternehmens Medtronic und stellten diese im August 2018 öffentlich vor.

Den Experten war es bei bestimmten Insulinpumpen gelungen, die vom Patienten genutzte Fernbedienung der Pumpen zu manipulieren. Die Insulingabe konnte in einem Ausmaß verändert werden, das zu einer unzureichenden Therapie des Blutzuckers mit ernsten gesundheitlichen Schäden führen kann[1]. Auch in den Datentransfer von einigen Herzschrittmachern konnten die Experten eingreifen und falsche Informationen einspielen. Damit hätten sie eine lebensbedrohliche Stimulierung des Herzens auslösen können[2].

Obwohl Medtronic laut Aussagen dieser Sicherheitsexperten bereits im Januar 2017 über die Sicherheitslücken informiert wurde, reagierte das Unternehmen erst im Juni 2018 öffentlich[3]. Medtronic begründete dies damit, dass die Gefahr einer Manipulation lediglich gering sei. Die amerikanische Kontrollbehörde FDA (U. S. Food and Drug Administration)[4] hat auf ihrer Internetseite Informationen von Medtronic zu diesen Sicherheitslücken sowie eigene Hinweise zum Thema Cyber-Sicherheit veröffentlicht. Auf der Internetseite der deutschen Aufsichtsbehörde, dem Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM), gibt es dazu bisher nur Informationen zur Insulinpumpe, nicht aber zu den Lücken bei den Herzschrittmachern.

Moderne Medizinprodukte werden zunehmend über Internet oder drahtlos (zum Beispiel über Bluetooth oder Funksignale) vernetzt, zum Beispiel um Daten der Geräte in und zwischen Gesundheitseinrichtungen schnell und einfach zu übertragen oder um Software zu aktualisieren. Aber auch Mess-Ergebnisse oder Patientendaten können auf diesem Weg an den Arzt oder die Ärztin übermittelt werden. Der Begriff der Telemedizin – ohne dass dieser exakt definiert ist – beschreibt dabei die drahtlose Fernübertragung von medizinischen Daten.

[1] https://www.medtronic.com/content/dam/medtronic-com/us-en/corporate/documents/Medtronic-MiniMed-Paradigm_Security-Bulletin_FINAL_080718.pdf
[2] https://www.deutschlandfunk.de/cyberkriminalitaet-bei-herzschrittmachern-hacker-machen.684.de.html?dram:article_id=425235
[3] https://www.medtronic.com/content/dam/medtronic-com/us-en/corporate/documents/Medtronic-MyCareLink-Security-Bulletin_FNL.pdf
[4] US Aufsichtsbehörde

Beim telemedizinischen Einsatz von Herzschrittmachern oder Defibrillatoren werden Informationen vom Implantat (Patienten) an die Arztpraxis übermittelt. Der Weg führt von einem Patienten/Home-Monitor (auch als Transmitter bezeichnet), der sich zu Hause in der Nähe des Patienten befinden muss, über das firmeneigene Netzwerk mit einem entsprechenden Server des Implantate-Herstellers zur Arztpraxis. Der Home-Monitor muss beim Patienten an eine passende Datenleitung (Telefon, Mobilnetz, Breitbandnetz, WLAN) angeschlossen sein. Auf diesem Weg können sowohl Daten zum Status der Funktionsfähigkeit des Implantats (zum Beispiel Batteriestatus) aber auch Daten zum Gesundheitszustand des Herzens (zum Beispiel Arrhythmien) übermittelt werden. In umgekehrter Richtung können aber auch Programm-Aktualisierungen durch den Hersteller für den Transmitter vorgenommen werden[5,6]. Diese Verbindungen sollten über geräteindividuelle Kennwörter sicher verschlüsselt sein. Hier liegt die Sicherheitslücke bei dem Home-Monitor von Medtronic[7], über die nicht-autorisierte Personen sich Zugriff verschaffen und manipulierte Daten in das Netzwerk einschleusen könnten[8].

Sicherheitsprobleme wiesen auch Geräte von Medtronic auf, mit denen Ärzte im Rahmen der Kontrolle ihrer Patienten, deren Herzschrittmacher bei Bedarf programmieren können. Diese Geräte erhalten automatische Updates über das Hersteller-Netzwerk. In diese Datenübertragung können Personen unberechtigt eingreifen und damit auf das Programmiergerät des Arztes. Denkbar ist zudem, dass über diesen Zugang auch das Implantat des Patienten manipuliert werden kann. Auf Grund dieser Sicherheitslücke hat Medtronic das Aufspielen von Updates über das Medtronic-Netzwerk deaktiviert. Updates können jetzt nur noch vor Ort in der Arzt-Praxis über eine USB-Verbindung aufgespielt werden[9].

Auch andere Hersteller haben mit Problemen bei der Cybersicherheit zu kämpfen. Das Unternehmen St. Jude Medical (zu Abbott gehörend) informierte 2017 über Lücken in seinem telemedizinischen System, dem firmeneigenen Merlin.net, welches zum Datentransfer der St. Jude Herzschrittmacher- und Defibrillatormodelle dient. Im Januar 2017 wurde bekannt, dass sich Fremdpersonen Zugriff auf den Merlin@home-Transmitter verschaffen können. Damit wäre es ihnen möglich, die Programmierung des Implantates zu verändern oder eine vorzeitige Batterieentleerung durch übermäßig häufigen Funkkontakt mit dem Implantat hervorzurufen. St. Jude Medical entwickelte daraufhin mehrere Aktualisierungen der Software (Sicherheits-Patches), um die Sicherheitslücke zu schließen und einen Fremdeingriff über das Internet oder die Funkverbindung zum Implantat zu verhindern[10]. Allerdings konnte das Update nur für aktuelle Modelle erstellt werden. Für ältere Modelle (Modellreihen *Current* und *Promote*) war dies aus technischen Gründen nicht möglich[11].

[5] https://www.bfarm.de/SharedDocs/Kundeninfos/DE/01/2017/00310-17_kundeninfo_de.pdf?__blob=publicationFile&v=2
[6] https://www.medtronic.com/content/dam/medtronic-com/de-de/patients/documents/reveal-mycarelink/pb-mycarelink-non-wireless.pdf
[7] Telemedizinisches Netz Carelink, Transmitter Modellnr. MyCareLink Patient Monitor 24950 und 24952
[8] https://www.medtronic.com/content/dam/medtronic-com/us-en/corporate/documents/Medtronic-Rios-MCL_Security-Bulletin_080718-FINAL.pdf
[9] https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm623184.htm
[10] https://www.bfarm.de/SharedDocs/Kundeninfos/DE/01/2017/08528-17_kundeninfo_de.pdf?__blob=publicationFile&v=1
[11] https://www.bfarm.de/SharedDocs/Kundeninfos/DE/01/2018/04572-18_kundeninfo_de.pdf?__blob=publicationFile&v=2

Bisher sind keine Fälle öffentlich bekannt, bei denen Personen durch die oben genannten Sicherheitslücken geschädigt wurden. Beispiele aus der Gesundheitsversorgung zeigen jedoch, wie aktuell und relevant das Thema ist. 2017 wurde das Virus „Wannacry“ in IT-Systeme von britischen Krankenhäusern eingeschleust. Das Virus verschlüsselte darin gespeicherte Daten, sodass diese nicht mehr lesbar waren. Es kam zu erheblichen Störungen und Verzögerungen bei der Behandlung von Patienten[12]. Ferner wurden Fälle bekannt, bei denen eine Schadsoftware in Geräte eingeschleust wurde, mit denen im Krankenhaus die Herzaktivität von Säuglingen überwacht wird. Eigentlich war der Computerwurm zur Spionage von Kreditkarteninformationen programmiert worden, gelangte aber über das Krankenhausnetzwerk auch in die medizinischen Geräte. Dort führte er quasi als „Nebenwirkung“ zum Neustart (Reboots) der Herzmonitore, sodass deren Überwachungsfunktion nicht sicher gewährleistet war[13].

Wie oben beschrieben wurde von Medtronic das Risiko eines relevanten Cybereingriffes – zum Beispiel auf kardiologische Implantate – als gering eingestuft. Begründet wird dies unter anderem damit, dass die entdeckten Sicherheitslücken den Zugriff auf einzelne Geräte vor Ort betreffen. Die genauen Datenflüsse der firmeneigenen Netzwerke sind aber intransparent. Deshalb ist nicht klar, welche Schäden eine von Unbefugten eingeschleuste Software anrichten könnte. Es drängt sich die Frage nach der Cybersicherheit der firmeneigenen Server auf. Insbesondere die Frage, ob gegebenenfalls über den Server ein genereller Zugriff auf Patienten-Monitore und Implantate möglich ist – vergleichbar dem Zugriff auf die Monitore in Arztpraxen, deren Datenverkehr zum Medtronic-Server stark eingeschränkt wurde.

Unabhängige Prüfungen und Zertifizierungen der Serversicherheit könnten hier einen verbindlichen Standard schaffen. In Deutschland ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Stelle, bei der Firmen entsprechende Netzwerkstrukturen und Server zertifizieren lassen können.

Die Notwendigkeit von mehr Cybersicherheit im medizinischen Umfeld haben auch deutsche Behörden erkannt. Das BSI hat dazu im Mai 2018 die Empfehlung „Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte“ veröffentlicht[14]. Das BfArM hat auf seiner Homepage zu diesem Thema eine eigene Rubrik eingerichtet, unter anderem zu „Maßnahmen von Herstellern mit Bezug Cybersicherheit“[15]. Zudem hat das BfArM im Juni 2018 eine öffentliche Konferenz zum Thema „Cybersicherheit von Medizinprodukten“ durchgeführt. Die Konferenz verdeutlichte eindrucksvoll die Herausforderungen, die das Thema Cybersicherheit an alle Beteiligten stellt und die unverzüglich angegangen werden müssen. Insbesondere Hersteller sind in der Verantwortung, ihre Produkte sicher zu gestalten. Der IT-Sektor ist hochdynamisch und entwickelt sich ständig weiter. Das gilt auch für Schadsoftware. Des-

[12] http://www.spiegel.de/wirtschaft/unternehmen/cyber-crime-wie-gefaehrdet-sind-deutsche-krankenhaeuser-a-1148763.html
[13] https://www.dicardiology.com/article/raising-bar-medical-device-cyber-security
[14] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_132.pdf?__blob=publicationFile&v=6
[15] https://www.bfarm.de/DE/Medizinprodukte/RisikoerfassungUndBewertung/Cybersicherheit/kundeninfos_cybersicherheit_node.html

Weiterer relevanter Link
https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf

halb müssen Medizinprodukte mit Internetanbindung bei Markteintritt aber auch während ihrer gesamten Lebensdauer immer wieder auf mögliche neue Gefährdungen hin geprüft und angepasst werden.