Doktor 4.0[1]

Herausforderungen und Lösungsansätze für den Arzt im Cyberspace
www.doktor40.help

Dr. Philipp Amann, MSc
EUROPOL

Dr. Cornelius Granig
WGM Healthcare Services GmbH

Die Grenzen zwischen der Realität, dem ‚echten' Leben, und der "Virtuellen Realität" oder dem ‚Cyberspace' verschwinden nach und nach. Der technische Fortschritt hat dazu geführt, dass elektronische und Internet-fähige Geräte immer kleiner und leistungsfähiger werden und damit aus unserem privaten und beruflichen Leben nicht mehr wegzudenken sind.

Vor allem im Gesundheitswesen hält die vernetzte und vernetzende Technik immer stärker Einzug, nicht nur in Krankenhäusern und bei niedergelassenen Ärzten – in Österreich etwa durch die Einführung der elektronischen Gesundheitsakte ELGA – , sondern auch bei (potenziellen) Patienten, wo eine Vielzahl von smarten Geräten im Fitnessbereich, aber auch etwa für telemedizinische Zwecke zum Einsatz kommen. Während uns die diversen Geräte, die für unsere Vernetzung sorgen, im Regelfall noch umgeben, in der Hand gehalten oder am Körper getragen werden, gibt es in der Medizin auch eine Entwicklung hin zur immer stärkeren Integration z.B. in der Form von eingepflanzten Herzschrittmachern und Insulinpumpen oder smarten Kontaktlinsen.[2]

Auf der einen Seite dienen solche intelligenten Geräte der Überwachung und oft auch Optimierung der eigenen Gesundheit über die konstante Sammlung diverser Vitalwerte und deren regelmäßiger Auswertung.[3]

Auf der anderen Seite eröffnen diese zusätzlichen Daten auch neue Möglichkeiten in der Behandlung, vor allem im Bereich der Analyse, Diagnostik und Therapie chronisch Kranker. Abgesehen davon führt „Big Data", also die Sammlung und Auswertung großer Datenmengen, oft aus unterschiedlichen Quellen zu möglichen neuen Erkenntnissen oder zu besser abgestimmten Behandlungsmethoden.[4] Vor allem im zukunftsträchtigen Bereich der personalisierten Medizin oder Präzisionsmedizin,[5] also der Abstimmung von Behandlungsmethoden auf das individuelle genetische Profil eines Patienten, spielen große Datenmengen und da vor allem die Daten über die Genomsequenzierung eine bedeutende Rolle.

Das alles wird im deutschsprachigen Raum oft mit dem Begriff „Industrie 4.0" umschrieben, in Anlehnung an die vierte Stufe der industriellen Revolution. Gängige Begriffe im Englischen sind dafür

---

[1] Dieser Beitrag ist auf der Serviceplattform für Ärzte **www.doktor40.help** abrufbar und spiegelt ausschließlich die persönliche Meinung der Autoren wider .
[2] http://medicalfuturist.com/googles-amazing-digital-contact-lens-can-transform-diabetes-care/
[3] http://quantifiedself.com/
[4] https://www.technologyreview.com/s/519686/steve-jobs-left-a-legacy-on-personalized-medicine/
[5] http://derstandard.at/2000045378457-626/Forschung-fuer-massgeschneiderte-Medizin

Industrial Internet, Industrial Internet of Things oder nur *Internet of Things (IoT)*[6] also das Internet der Dinge. Speziell für den medizinischen Bereich hat sich auch der Begriff ***Internet of Medical Things***[7] etabliert.

Neben den vielen Möglichkeiten, die diese Entwicklungen bieten, entstehen damit vor allem auch für die Ärzteschaft viele Risiken und Herausforderungen. Neben zu erwartenden technischen und Softwareproblemen ist es auch die kriminelle Komponente, die in diesem Bereich Einzug hält. Patienten- und Gesundheitsdaten haben hier einen besonderen Stellenwert, neben der Krankengeschichte können das Adress- und Kontaktdaten, aber auch Kreditkarteninformationen oder genetische Profile sein.

Hauptbedrohungen im Cyberspace

Für Europa lassen sich aufgrund von Industriedaten und relevanten Forschungsergebnissen aus polizeilicher Sicht die Bedrohungen in verschiedene Bereiche einteilen, wovon hier nur zwei besonders relevante beschrieben werden sollen:[8]

Ransomware:

Hierbei handelt sich um eine Schadsoftware, welche Computer und andere elektronische Geräte wie z.B. Smart-TVs befällt und die Daten, die darauf gespeichert sind, verschlüsselt. Der Betroffene wird dann aufgefordert, Lösegeld, meist in einer Kryptowährung wie Bitcoin[9] zu bezahlen. Wird der Aufforderung innerhalb eines relativ kurz gesetzten Zeitintervalls nicht Folge geleistet, wird der Schlüssel zum Entschlüsseln der Daten gelöscht, was den Zugriff auf die Daten meist für immer versperrt. Betroffen von dieser Art der Erpressung sind Einzelpersonen sowie Unternehmen jeder Größe, wobei auch Krankenhäuser oft Ziel von Attacken sind.[10] Zum Beispiel wurde im März 2016 das Hollywood Presbyterian Medical Center in den USA mit Ransomware lahmgelegt, die wesentliche IT-Systeme verschlüsselte. Als Folge waren Mitarbeiter gezwungen, so lange papierbasiert zu arbeiten, bis das Management die Entscheidung traf, den Kriminellen die geforderte Geldsumme zu überweisen, um wieder Zugriff auf alle IT-Systeme und Daten zu haben.

Krimineller Missbrauch von Daten

Daten haben sich zu einem Hauptgut im kriminellen Onlinehandel entwickelt, mit einem deutlichen Trend zu höheren Preisen für personenbezogene Daten im Vergleich z.B. zu gestohlenen oder gefälschten Kreditkarten. Und obwohl es oft nur die spektakulären Fälle sind, die in den Medien Erwähnung finden, sind auch viele kleine und mittlere Betriebe (KMU) von diesen Angriffen

[6] http://www.rockwellautomation.com/de_DE/news/blog/detail.page?pagetitle=Internet-der-Dinge-Industrie-4.0-%7C-Blog&content_type=blog&docid=526c90d2ccdbe09d0111e26c62ad4948
[7] http://www.technewsworld.com/story/83654.html
[8] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016
[9] http://www.coindesk.com/information/what-is-bitcoin/
[10] http://www.beckershospitalreview.com/healthcare-information-technology/hospitals-are-hit-with-88-of-all-ransomware-attacks.html

betroffen, was auch darauf zurückzuführen ist, dass bei diesen Unternehmen oft das Bewusstsein für die Notwendigkeit und die Ressourcen für einen adäquaten Schutz fehlen.

Neben der Industrialisierung und Kommerzialisierung der Cyberkriminalität sind es vor allem die wachsende Anzahl an mit dem Internet verbundenen Geräten – das Internet der Dinge – und die daraus resultierende Komplexität, gepaart mit unzureichenden oder nicht vorhandenen Sicherheitsmaßnahmen, die Kriminellen immer mehr Angriffsmöglichkeiten bieten.[11]

Herausforderungen und Lösungsansätze für den Arzt – Doktor 4.0

Um mit internetbasierten Geräten zu arbeiten, bedarf es neben der entsprechenden Ausbildung auch eines technischen Grundwissens und der notwendigen Ausstattung. Voraussetzung ist freilich die Akzeptanz bei Ärzten und Patienten, solche medizinischen Geräte einzusetzen. Doch neben dem Risiko des Datendiebstahls besteht durch Sicherheitslücken in telemedizinischen Anwendungen die Gefahr von falschen klinischen Entscheidungen oder auch von direkter Manipulation der Funktionsweise solcher Geräte durch unbefugte Personen. Daraus können nicht nur Gesundheitsprobleme für die betroffenen Patienten resultieren, sondern auch Rechtsstreitigkeiten und finanzielle Sanktionen.

Sicherheitsschwachstellen können mannigfaltige Ursachen haben, die nicht nur in der Komplexität und Heterogenität von IoT-Systemen liegen, sondern auch im unzureichenden Management von Software-Updates und dem Umgang mit bekannten Software-Schwachstellen, speziell für den Zeitraum zwischen deren Bekanntwerden und der Auslieferung der Fehlerbehebung. Aufgrund von Ressourcenbeschränkungen in Bezug auf Speicher, Batterie und Rechenleistung haben sich gerade internetbasierte Geräte als schwieriger zu schützen herausgestellt.[12]

Beispiele für bekannte Risiken reichen von angreifbaren Herzschrittmachern, Insulinpumpen zu Infusionssystemen[13] und Operationsrobotern:[14]

So wurde etwa im August 2016 von St. Jude, einem amerikanischen Hersteller von Herzschrittmachern, ein Software-Update verfügbar gemacht, das potentielle Angriffspunkte für Hacker über die Funkfernsteuerung des Geräts behob.

Im Oktober 2016 wies Johnson & Johnson auf eine Sicherheitslücke bei einer seiner Insulinpumpen hin, die auch über die Fernbedienung bestand, und einen Angreifer theoretisch in die Lage versetzten konnte, die Insulinzufuhr zu beeinflussen. In diesem Fall wurden rund 114.000 Patienten kontaktiert.[15]

---

[11] http://www.spiegel.de/netzwelt/web/deutsche-telekom-stoerung-war-misslungener-botnet-angriff-a-1123544.html

[12] Cybersecurity and the Internet of Things – a Law Enforcement Perspective, https://www.cybersecurityraad.nl/binaries/Report%20European%20Foresight%20Cyber%20Security%202016_tcm56-102235.pdf

[13] http://www.zdnet.de/88237212/infusionssysteme-in-us-krankenhaeusern-angeblich-manipulierbar/

[14] https://www.technologyreview.com/s/537001/security-experts-hack-teleoperated-surgical-robot/

[15] http://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUSKCN12411L

Aber auch im Verbraucherbereich wie zum Beispiel bei Fitness- und Aktivitäts-Trackern gibt es bekannte Risiken.[16]

Cybersicherheit der Patienten sowie des Arztes

Sowohl der Arzt als auch der Patient sind interessante Angriffsziele für Hacker und andere Kriminelle.

In diesem Zusammenhang stellt sich die Frage, inwieweit der Arzt auch für laufende Updates der internetbasierten Geräte und damit für Cybersicherheit aber auch die physische Sicherheit von Patienten mit verantwortlich ist. In Anlehnung an das Johnson & Johnson Beispiel, kann man sich also leicht zukünftige Szenarien vorstellen, wo der Arzt als Teil des Patientengesprächs auch die letzten Updates und Sicherheitsmaßnahmen für diese und ähnliche vernetzte medizinische Geräte empfehlen muss und unter Umständen sogar einspielen kann. Der Arzt würde somit einen wichtigen Beitrag zur "*Endpoint Security*" leisten.

Für den Arzt gilt es, im Zuge seines Risikomanagements, durch die Umsetzung relevanter Richtlinien[17] und Gesetzesvorlagen sowie Standards, das eigene Risikoprofil zu ermitteln und geeignete Maßnahmen zur Risikovermeidung und –verminderung zu treffen, wobei es sich hier typischerweise um einen kontinuierlichen Prozess handelt.

Schutz von Patientendaten auch hinsichtlich der relevanten Regelungen auf EU-Ebene.

Zum Schutz der Patientendaten gehören definierte Prozesse zur Bearbeitung der Daten, Verschlüsselung von Daten, Zugriffskontrolle und Authentifizierung sowie das Aufzeichnen aller Zugriffe. Zusätzlich sind z.B. für den Fall einer Datenschutzpanne und eines Datendiebstahls Vorkehrungen zu treffen, auch unter Berücksichtigung der relevanten Verordnungen und Direktiven auf EU-Ebene, wobei vor allem die folgenden drei Maßnahmenregelwerke zu erwähnen sind:

<u>Datenschutz-Grundverordnung[18]</u>

Die Datenschutz-Grundverordnung, welche im Jahr 2018 EU-weit in Kraft getreten ist, brachte nicht nur mehr Rechte für Privatpersonen (z.B. das Recht auf Datenlöschung), sondern auch weitreichende Änderungen bei betrieblichen Datenanwendungen. Durch die Regelungen am es zu einer Vereinheitlichung der europäischen Datenschutznormen - mit vielen Vorteilen, insbesondere für kleine und mittlere Unternehmen (KMU), durch geringere Kosten und weniger Verwaltungsaufwand.

Für Krankenhäuser und Arztpraxen ist vor allem der Bereich der Datenschutz-Folgenabschätzung ser wichtig, die dann verpflichtend ist, wenn durch die Datenverarbeitung ein hohes Risiko für Betroffene entsteht, oder die Beschreibung der notwendigen Schritte bei einer Datenschutzpanne oder bei Datenverlust.

[16] https://www.theregister.co.uk/2015/10/21/fitbit_hack/
[17] FDA Richtlinien, IEC/TR 80001-2-2, IEC/TR 80001-2-8, ISO 27000
[18] https://www.wko.at/Content.Node/branchen/oe/sparte_iuc/Werbung-und-Marktkommunikation/EU-Datenschutz-Grundverordnung-(GVO).html

NIS-Direktive zur Netzwerks- und Informationssystems-Sicherheit[19]

Diese Direktive, zielt darauf ab, einheitliche Regelungen zur Sicherung von Netzwerken und Informationssystemen in den EU-Mitgliedsstaaten zu schaffen. Neben einer Reihe von Maßnahmen sieht die Direktive auch eine Meldepflicht für IT‑Vorfälle für Betreiber kritischer Infrastrukturen inklusive dem Gesundheitswesen vor, mit entsprechendem Handlungspotential u.a. für Betreiber von Krankenanstalten.

International, aber auch auf EU-Ebene gibt es einige relevante Initiativen, Maßnahmen und Richtlinien, wie zum Beispiel zur Cybersicherheit in medizinischen Geräten[20] oder Bestrebungen, ein Cybersicherheit-Zertifizierungsrichtwerk sowie ein Kennzeichnungsschema für die Sicherheit von ICT-Produkten zu entwickeln.

Für Anwender im medizinischen Bereich wäre eine Aus- und Weiterbildung zur Bewusstseinsschaffung, aber auch hinsichtlich konkreter, insbesondere zum Schutz sensibler Daten zu setzender Maßnahmen, dringend notwendig.

Whistleblower-Richtlinie

Die derzeit noch in Ausarbeitung befindliche Whistleblower-Richtlinie wird EU-weit in zwei Jahren Geltung haben und alle Firmen und Organisationen betreffen, die mehr als 50 Mitarbeiter haben. Diese müssen eine gesicherte Kommunikation für die anonym bleibenden Hinweisgeber ermöglichen und dürfen nicht gegen sie vorgehen. Das Management von Hinweisgebern bietet die große Chance, mehr über organisationsinternes Fehlverhalten und ggf. sogar Gesetzesverstöße zu erfahren und gegen diese vorzugehen.

Die Autoren:

Dr. Philipp Amann ist der Leiter der Strategieabteilung des Europäischen Zentrums zur Bekämpfung der Cyberkriminalität (EC3) von EUROPOL in Den Haag. Die operativen und strategischen Schwerpunkte des EC3s sind die Bekämpfung der High-Tech-Kriminalität, des Betrugs im Zahlungsverkehr und der sexuellen Ausbeutung von Kindern im Internet.

Dr. Cornelius Granig ist leitet die österreichische Beratungsfirma WGM Healthcare Services GmbH, die Dienstleistungen für Ärzte, Krankenhäuser und andere Gesundheitsdienstanbieter anbietet. Er befasst sich seit vielen Jahren mit Cyber-Security, Digitalisierung und Korruptionsbekämpfung und war in den letzten Jahren als Geschäftsführer bei den internationalen Technologiekonzernen IBM und Siemens tätig. Sein Fachbuch zum Thema Computerkriminalität mit dem Titel “Darknet: Die Welt im Schatten der Computerkriminalität" erschien 2019 im Verlag Kremayr & Scheriau.

[19] http://www.consilium.europa.eu/de/policies/cyber-security/
[20] https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm