"Ärztewoche" Nr. 06/2019 vom 07.02.2019 Seite 25
Ressort: Praxis

Schutz vor dem Daten-GAU

Informationstechnik. Bei Hackerattacken auf IT-Systeme in Krankenhäusern und Praxen sind viele Seiten betroffen: Patienten, Ärzte, Kliniken und Gerätehersteller. Neben Identitätsdiebstähle, Spionage, Manipulation und Erpressung kann im schlimmsten Fall auch ein Menschenleben auf dem Spiel stehen.

Das Internet of Things (IoT) vernetzt physische Gegenstände und virtuelle Informationstechnik miteinander. Im Gesundheitsbereich findet es Anwendung in der häuslichen Versorgung, dem klinischen Umfeld sowie bei präventiven Maßnahmen. Da das IoT eine vergleichbar neue Entwicklung ist und das Zusammenspiel der Komponenten weitestgehend automatisiert abläuft, ist es anfällig für Manipulationen. Dies stellt besondere Anforderungen an die Cybersicherheit und ist mit besonderen rechtlichen Herausforderungen verbunden.

Das IoT ermöglicht eine Interaktion zwischen Mensch und vernetzten elektronischen Systemen sowie zwischen den Systemen untereinander. Beim Healthcare IoT können Patienten, aber auch pflegebedürftige Senioren, beispielsweise via Ambient Assisted Living und Telemonitoring, in ihrem häuslichen Umfeld per Kamera und Sensoren überwacht werden. Die Versorgung kann dabei individuell angepasst werden. Eine enorme Entwicklung, wenn man bedenkt, dass die stationäre Versorgung von Patienten einer der größten Kostenpunkte im Gesundheitswesen ist und eine längere Pflege im häuslichen Umfeld zu Einsparungen im Milliardenbereich bei den Kostenträgern führen kann.

Prozessoptimierte Abläufe Auch bei der medizinischen Versorgung im klinischen Umfeld erhöht das IoT die Prozessoptimierung, beispielsweise durch vernetzte Medizingeräte. Handelt es sich um den richtigen Patienten? Ist das eingesetzte Medikament oder Medizingerät das Passende? Das IoT schlägt dabei den Bogen zur prozessoptimierten, digital gestützten Qualitätssicherung.

Auch die Diagnostik wie Langzeit-EKG-Untersuchungen übernimmt sehr wahrscheinlich zukünftig das IoT. Möglich, dass Menschen sich in ein "Digitales Medizinisches Versorgungszentrum" begeben, in dem gar keine Ärzte mehr anwesend sind. Bei der Bedienung der Medizingeräte werden sie vom einfühlsamen Personal freundlich unterstützt. Die Auswertung der Untersuchung nimmt eine Künstliche Intelligenz vor, und ein Arzt, dem die Diagnose zugeleitet wird, bespricht diese via telemedizinischer Anwendung und Fernbehandlung mit Ihnen. Klingt befremdlich? Die digitale Medizin wächst aus ihren Kinderschuhen heraus. Und mit ihr auch die regulatorischen und technischen Anforderungen.

Eines ist klar: Gesundheitsbezogene Daten sind täglich Cyberangriffen ausgesetzt. So wertvoll die Daten für ihre Anwender sind, so üben sie in gleichem Maße eine hohe Anziehungskraft auf Kriminelle aus. Das "Phishing" von gesundheitsbezogenen Daten ermöglicht es, in interne Prozesse einzugreifen, Daten für Identitätsdiebstähle auszuspionieren und zu manipulieren.

Hackern steht damit auch der Zugang zu erheblichem Erpressungspotenzial offen. Auch wenn Gesundheitsdaten nicht das primäre Ziel bei einem Cyberangriff sind, kann ein IoT-System der "wunde Punkt" und damit ein Einfallstor für einen Befall des gesamten Netzwerks des Krankenhauses oder der Arztpraxis -und damit zu ihrer Stilllegung - sein. Steht ein Gesundheitsbetrieb einmal still, sind die finanziellen Folgen und möglichen Haftungsklagen im Vergleich dazu, dass auch Menschenleben auf dem Spiel stehen können, im Vergleich eher sekundär.

Das Problem beim IoT ist, dass oft der unautorisierte Datenzugriff unbemerkt geschieht. Insbesondere bei Systemen, die nur untereinander kommunizieren und den Anwender nicht in den Datenaustausch mit einbeziehen, ist es ohne technische Überwachungsprogramme unmöglich, den externen unautorisierten Zugriff zu bemerken.

Welche Cyberangriffe drohen?

Ein Angriff kann demnach wie folgt aussehen: Die Malware greift via Schadsoftware in das IoT-Netzwerk ein, indem es die ungeschützten "Devices" fernsteuert. Das Tückische dabei ist: Ist das Netzwerk einmal infiltriert, breitet sich die Malware rasant und flächendeckend aus und kann auf bisher nicht befallene Dateien Einfluss nehmen. So können Hackerangriffe exponentiell mit der Anzahl der Dateien im Netzwerk zunehmen. Es droht der Daten-Gau. Um dem vorzubeugen - und auch zur Prävention von Haftungsklagen und Datenschutzrechtsverletzungen-, bedarf es technischer Vorkehrungen, die eine Datenüberwachung im IoT zulassen.

Diffizil gestaltet sich dabei die Kontrolle des Datenaustauschs. IoT-Datenträger sind auf eine einfache Handhabung und Benutzerfreundlichkeit ausgelegt und daher oft unverschlüsselt. Der Anwender wird zudem nicht bei unautorisiertem Zugriff

auf den Datenträger alarmiert. Man wiegt sich bei der Nutzung kleiner digitalen Gadgets in Sicherheit. Daher gilt es, die IoT-Datenträger und die sie umspannenden Netzwerke zu sichern. Eine Daten-und Netzwerksegmentierung ermöglicht die Trennung befallener Daten vom Netzwerk, Firewalls können Attacken frühzeitig abwehren und Zugangsbeschränkungen erlauben, den Zugriff von Dritten zu beschränken.

Gegenmaßnahmen im Worst Case Sollte es zum "Worst Case" kommen, gilt es, Ruhe zu bewahren. Die Netzwerkstrukturen der verschiedenen Akteure variieren sehr, daher fällt eine einheitliche Behandlung schwer. Im Idealfall sind die jeweiligen IoT-Datenträger in unterschiedlichen Netzwerken segmentiert, so dass die Cyberattacke sich nicht unmittelbar auf alle Datenträger ausbreiten kann. Zudem sollten sie passwortgeschützt sein. Hier empfiehlt es sich, ein Rotationssystem zu installieren, auf das mit gängigen Passwörtern nicht zugegriffen werden kann. Um effiziente Gegenmaßnahmen einzuleiten, muss sofort die IT benachrichtigt werden. Im Fall der Fälle sollte auch ein Anruf beim Rechtsanwalt des Vertrauens auf der Agenda stehen.

Die Autorin Karolina Lange, LL.M (Medizinrecht), ist als Rechtsanwältin in der Düsseldorfer Kanzlei Taylor Wessing auf die regulatorische Beratung im Gesundheitswesen spezialisiert. Co-Autor Jonas Bördner ist Wissenschaftlicher Mitarbeiter in der Kanzlei tätig.

Von Karolina Lange und Jonas Bördner/DÄZ

Quelle:	"Ärztewoche" Nr. 06/2019 vom 07.02.2019 Ressort: Praxis	Seite 25
Ressort:	Praxis	
Dokumentnummer:	065069082090084069087079 0 952019020701106706558806 8 070	