DIGITAL HEALTH

Investoren lieben US-Firmen

2018 war in Sachen Risikofinanzierung bis dato das beste Jahr für Startups im Digital-Health-Geschäft.

Austin. Die globale Risikofinanzierung junger Digital-Health-Firmen hat 2018 einen neuen Rekordwert erreicht: Rund 9,5 Milliarden Dollar – 32 Prozent mehr als im Vorjahr – haben Venture-Capital-Geber in die Branche investiert, wie der US-Marktforscher Mercom Capital Group zu Wochenbeginn mitteilte. Einschließlich Schulden und Geldaufnahme über die Börsen sei die Unternehmensfinanzierung in Sachen Digital Health sogar um 58 Prozent auf 13 Milliarden Dollar geklettert. Damit hält der anhand der Mercom-Zahlen seit 2014 erkennbare starke Fördertrend an. Damals verzeichneten die texanischen Marktforscher im Jahreswechsel mehr als eine Verdoppelung der weltweiten Unternehmensfinanzierungen im Digital-Health-Sektor (von 2,2 auf 4,7 Milliarden Dollar).

Wenig überraschend floss mit 7,0 Milliarden Dollar der Löwenanteil 2018 in US-Unternehmen. Startups mit Sitz in anderen Ländern erhielten laut Mercom 2,5 Milliarden Dollar. Seit 2010 hätten Digital-Health-Anbieter damit insgesamt 35 Milliarden Dollar Anschubgelder aufgenommen und weitere 12 Milliarden mittels Schulden oder Kapitalerhöhungen und Börsengängen eingenommen.

Mengenmäßig würden Finanzierungsrunden nach wie vor Merger-Deals und Börsengänge „weit hinter sich lassen“, kommentiert Mercom-CEO Raj Prabhu. Ausstiegs-Vorhaben der Fondsgesellschaften stellten für die jungen Digital-Health-Unternehmen daher „weiterhin eine große Herausforderung dar“.

Am stärksten profitierten voriges Jahr von Risikokapital mit 2,1 Milliarden Dollar Startups, die sich mit Datenverarbeitung („Big Data“) befassen. An zweiter Stelle rangieren Entwickler von Gesundheits-Apps (1,3 Milliarden Dollar), und an dritter Anbieter telemedizinischer Konzepte (1,1 Milliarden). Kumuliert seit 2010 belegen allerdings App-Entwickler mit 4,9 Milliarden Dollar Platz 1. bei der Frühfinanzierung, gefolgt von Datensammlern (4,7 Milliarden Dollar) und Telemed-Anbietern (3,2 Milliarden).

Als größte Einzelinvestition weist Mercom für 2018 die 300 Millionen Dollar schwere Beteiligung von GlaxoSmithKline an dem kalifornischen Gendiagnostik-Anbieter 23andMe aus. Knapp dahinter mit 291 Millionen Dollar die Finanzierung der Telemed-Company American Well (u.a. Arztsuche oder Fernsprechstunde); die Geldgeber sind in Gänze nicht öffentlich gemacht worden. Anfang 2018 hatte das Bostoner Unternehmen eine Beteiligung der Allianz-Gruppe über 59 Millionen Dollar bekannt gegeben. Die drittgrößte Venture-Finanzierung erhielt mit 250 Millionen Dollar die Butterfly Network Inc., Anbieter einer cloudbasierten Ultraschalldiagnostik für Endverbraucher. Neben etlichen Venturefonds ist Mercom zufolge auch die Bill & Melinda Gates Stiftung bei Butterfly mit im Boot. *(cw)*

GASTBEITRAG

Wenn der Hacker die Kliniktechnik übernimmt

Bei Hackerangriffen auf Kliniksysteme sind viele Seiten betroffen: Patienten, Krankenhäuser und Gerätehersteller. Welche Sicherheitsrisiken bestehen - und welche Gegenmaßnahmen helfen im „Worst Case“?

Von Karolina Lange und Jonas Bördner

Die Vernetzung in Kliniken ist eine gute Sache – kann jedoch jederzeit ein Einfallstor für Hacker sein. © BEERKOFF/ ADOBE.STOCK.COM

Das Internet of Things (IoT) vernetzt physische Gegenstände mit virtueller Informationstechnik und findet im Gesundheitsbereich 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.

IoT optimiert Klinikprozesse

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.

Risiken bei Gesundheitsdaten

Eines ist klar: Gesundheitsbezogene Daten unterfallen täglich Cyberangriffen. 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 erstmal still, sind die finanziellen Folgen und möglichen Haftungsklagen im Vergleich dazu, dass auch Menschenleben auf dem Spiel stehen können, im Vergleich eher sekundär.

Welche Cyberangriffe drohen?

Das Problem beim IoT: Oft geschieht der unautorisierte Datenzugriff unbemerkt. 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.

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 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 und bequeme 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 immens, 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.

Geeignete Sicherheitsmaßnahmen für Kliniken können sein:

- **Segmentierung** von Daten und Netzwerk: Hilft, befallene Datenträger in Quarantäne zu schieben. Der externe Zugriff wird in Netzwerkprotokollen dokumentiert und ermöglicht eine Trennung der befallenen Daten vom Netzwerk selbst.
- **Firewalls** und Angrifferkennungssysteme (IDS): Helfen, den Angriff frühzeitig abzuwehren und das implementierte Risikomanagement umzusetzen. Dies geschieht etwa durch eine Monitoring- Plattform, die eine Übersicht über aktive (und inaktive) Datenträger und somit Interaktionsspielraum gibt.
- **Zugangsbeschränkungen** und Kontrolllisten: Schränken den Zugriff unberechtigter Dritter ein.

Karolina Lange ist Anwältin für Medizinrecht und berät Leistungserbringer, deren Träger sowie Arztpraxen, Ärztenetze und Krankenkassen.
Co-Autor Jonas Bördner ist als Wissenschaftler Mitarbeiter an der Goethe-Universität Frankfurt am Main tätig.