TIMO KOB

DIGITAL HEALTHCARE

Zu Risiken und Nebenwirkungen ...

Bei allen Unbekannten, die die Digitalisierung für uns in den nächsten Jahren noch bereithalten wird, ist zumindest eines klar: Kaum eine Branche wird so gewaltigen Änderungen unterworfen sein wie die Medizin. Dies wird neue Heilungschancen betreffen; es wird Änderungen im Berufsbild bedeuten, wenn Krankheitsanalysen schneller und besser durch künstliche Intelligenz erstellt werden können, und es wird – siehe Health-Apps und deren absehbare Bedeutung für Krankenversicherungen – zu ethischen Fragestellungen kommen. Die Digitalisierung wird aber auch neue Gefahren bergen. Gefahren, die wir heute schon sehen, aber teilweise lange ignoriert haben, und Gefahren, die wir in den nächsten Jahren durch vermutlich zu sorg- und kritikloses Umsetzen der Möglichkeiten selbst noch neu hinzufügen.

Kaum eine Branche hat sich so lange der Digitalisierung verweigert wie die Medizin – teilweise aus Kostengründen, teilweise aber auch aus einer kultivierten Technikfeindlichkeit heraus; teilweise durchaus auch aus Sorge um die Vertraulichkeit von Patientendaten.

Dieser hieraus resultierende Mangel an Erfahrungen in Kombination mit dem nicht mehr aufzuhaltenden und mit brachialer Geschwindigkeit kommenden digitalen Wandel führt hier aber zu einer besonders bedrohlichen Gefahrensituation. Denn ein weiterer Faktor ändert sich ebenfalls gerade dramatisch: die Liste der potenziellen Täter.

Lange war es de facto der beste Schutz, dass es keine Tätergruppe gab, die eine besondere Bedrohung für die Gesundheitsbranche darstellte: Hacker waren pickelige Jungs, die mehr aus Spieltrieb und Geltungssucht denn aus klassisch kriminellen Motivlagen heraus agierten. Und auch die aufkommende Online-Kriminalität konzentrierte sich eher auf leichter zum finanziellen Vorteil der Täter ausnutzbare Branchen wie Banken und Online-Handel. Der Diebstahl von Patientenakten ist zwar für die Opfer nicht schön, aber für die Täter auch nur selten lukrativ. Gleiches gilt für die zweite Stoßrichtung neben der Spionage, die Sabotage: Natürlich ist es denkbar, Infrastrukturen lahmzulegen, aber warum sollte das jemand tun? Geld verdienen ließ sich damit jedenfalls nicht so einfach.

Der erste Warnschuss kam 2016 mit den Kryptotrojanern, am bekanntesten hier „Locky“ und 2017 „Wannacry“. Ein Warnschuss nicht nur, weil hier international auch Krankenhäuser betroffen waren, sondern weil hier ein Geschäftsmodell entstand, das der Sabotage eine kommerziell nutzbare Facette hinzufügte. Beunruhigend ist hier auch die überproportional hohe Betroffenheit von Krankenhäusern. All die Kryptotrojaner funktionieren als Geschäftsmodell im Normalfall nur, wenn die beiden ersten Regeln der IT-Sicherheit sträflich missachtet werden: Aktualisieren der Systeme zur Abwehr von Schadsoftware von Angreifern und regelmäßiges Backup zur schnellen Rückkehr in den geordneten Betrieb, wenn es doch passiert ist.

Wenn dies aber schon bei der klassischen Office-IT in vielen IT-Abteilungen der Gesundheitsbranche nicht gelingt, wie soll dann auf der zweiten Flanke der Digitalisierung, der Vernetzung von Medizintechnik, dies

Der Autor

Prof. Timo Kob ist Gründer des renommierten deutschen Sicherheitsberatungsunternehmens HiSolutions AG und Professor für Wirtschaftsschutz und Cybersecurity an der FH Campus Wien.

Seit 1992 berät Kob national und international Unternehmen, Behörden, Regierungen und Institutionen, darunter mehr als die Hälfte der DAX-Unternehmen, 75% der deutschen Top-20-Banken, das deutsche Bundesamt für Sicherheit und Informationstechnik (BSI), das Bundeskanzleramt Österreich, die OSZE, die europäische Agentur für Netzwerk- und Informationssicherheit (ENISA) u.v.m.

besser aussehen? Vor allem, weil die Lage hier deutlich komplizierter ist, wie es z. B. das herstellende Gewerbe unter dem Schlagwort Industrie 4.0 auch derzeit erfährt: Ist klassische IT (aber auch z. B. Smartphones) auf eine Nutzungsdauer von meist nur wenigen Jahren ausgelegt, so besitzen Maschinen und somit auch Medizintechnik meist einen längeren Lebenszyklus, sind aber zusätzlich auch noch deutlich schlechter auf den hohen Updatebedarf der Softwarekomponenten vorbereitet. Lücken bleiben so noch länger bestehen als schon in der klassischen IT und potenzieren sich oft im Laufe des Lebenszyklus.

Auch hier gab es aber bisher zwei schützende Aspekte: Zum einen hatte natürlich keiner der lange dominierenden Freizeithacker die entsprechende Technik, um Angriffe zu erproben, zum anderen galt auch hier die klassische Frage: Welcher Täter hätte denn etwas von einem solchen Angriff? Doch die Welt hat sich geändert – und nicht unbedingt nur zum Guten.

Unsere Fokussierung auf Cyberkriminalität – und damit das dominierende Motiv des finanziellen Gewinns – ist nicht länger gültig. Durch die immer realistischer werdenden Gefahren des Cyberterrorismus und des Cyberwars steigen einerseits die finanziellen Möglichkeiten der Angreifer, und diese müssen durch die wechselnde Motivlage – weg vom direkten eigenen Gewinn, hin zur reinen Schädigung des Feindes – noch nicht einmal durch die Taten refinanziert werden. Und spätestens hier, wenn die Gesellschaft an sich in den Fokus der Täter rückt und diese Täter nicht mehr nur fiktionale Möglichkeiten, sondern konkrete Realität sind, rückt das Gesundheitswesen als auch emotional für die Gesellschaft und deren Funktionieren eine herausragende Bedeutung besitzende Branche in den Fokus. Kein Wunder also, wenn dieses Segment in den Regulierungsbemühungen für Cybersicherheit in kritischen Infrastrukturen eine hervorgehobene Bedeutung erhält.

Und Disruption ist kein Thema, das nur für Start-ups von Bedeutung ist: Auch Terrorismus erfindet sich neu und wird neue Schlachtfelder für sich entdecken; Schlachtfelder, die die Militärs bereits besetzen, Schlachtfelder, die noch schwerer zu verteidigen sind, aber maximale Aufmerksamkeit garantieren.

Wir dürfen uns nicht täuschen: Auch wenn uns NSA-Skandal oder CIA-Spionagetool-Leaks auf den ersten Blick glauben lassen, dass enormer Aufwand und hohes Fachwissen nötig sind, um avancierte Einbrüche in Computersysteme vorzunehmen, so ist die Einstiegsbarriere für diese Schlachtfelder deutlich niedriger als erhofft.

Und wir dürfen uns nicht täuschen: Auch wenn uns NSA-Skandal oder CIA-Spionagetool-Leaks auf den ersten Blick glauben lassen, dass enormer Aufwand und hohes Fachwissen nötig sind, um avancierte Einbrüche in Computersysteme vorzunehmen, so ist die „Einstiegsbarriere“ für diese Schlachtfelder deutlich niedriger, als von uns erhofft.

Einerseits zeigen schon die Social-Media-Aktivitäten des IS, dass ein mittelalterliches Weltbild nicht zwingend auch zu technischer Inkompetenz führt. So war etwa der berüchtigte IS-Henker „Jihadi John“ Absolvent der Informatik an der University of Westminster.

Auf der anderen Seite ist es sehr einfach und kostengünstig, sich das nötige Know-how im Darknet einzukaufen. Wir wären also gut beraten, bei unseren Bemühungen um sinnvolle und notwendige Digitalisierung auch den Schutz vor Cyberterrorismus von Anfang an mitzudenken. Mitdenken heißt: Vernetzung sinnvoll einsetzen statt „anything goes“. Eine in Hackerkreisen beliebte Regel ist „Adamas Law“ (nicht ganz szeneuntypisch benannt nach einer fiktiven Figur aus der Fernsehserie „Kampfstern Galactica“). Diese Regel lautet: „If it can kill you, don’t connect it to the network!“ Wenn auch in der Summe vielleicht zu apodiktisch formuliert, so steckt doch einiges in dieser These, was man sich aus Expertensicht in der Praxis wünschen würde. Steht wirklich immer ein ausreichender Nutzen den Gefahren gegenüber, überfordern meine Technologiesprünge nicht die Kompetenz und Reife meiner Organisation – sollte ich lieber einen Zwischenschritt einrichten? Bin ich auch für den Fall des Falles technisch und organisatorisch in der Lage, eine solche Krise zu bewältigen?

Das sind Fragen, die sich grundsätzlich alle Anwender stellen sollten. In einem Segment, wo Technik aber so eine starke Auswirkung auf Leib und Leben hat, ist dies im wahrsten Sinne des Wortes von existenzieller Bedeutung!