Holger Berens, Benjamin Bolzmann, Carl Dietzel, Lucia Ferrigno, Joachim Jakobs, Guido Johannes Lorc, Sascha Rösgen, Nikolaus Stapels

Bundesministerium für Gesundheit (BMG)
Herr Minister Jens Spahn
Friedrichstraße 108,

10117 Berlin

22. Januar 2019

Offener Brief

Sehr geehrter Herr Spahn,

die Unterzeichner dieses Briefs sorgen sich um die Sicherheit unseres Gesundheitswesens – und die der Patienten. Daher fordern wir eine Bildungsinitiative.

Unsere Sorge gründet auf diesen Entwicklungen:

Zwei Dutzend Kliniken in Nordrhein-Westfalen wurden 2016 von Cyberkriminellen nach der Verschlüsselung ihrer Kommunikationstechnik erpresst. Nicht einmal die Krankenhäuser selbst scheinen die notwendigen Konsequenzen daraus gezogen zu haben: Im November 2018 fiel die Klinik in Fürstenfeldbruck einem Verschlüsselungstrojaner zum Opfer – mit der Folge, dass zeitweise kein Computer zu gebrauchen war. Der Bayerische Datenschutzbeauftragte Professor Thomas Petry vermutet, dass die Klinik nur zufällig verseucht wurde, da kein Lösegeld gefordert wurde. Dieser Zufall wäre auch deshalb bemerkenswert, weil der Geschäftsführer der Klinik bis zu diesem Zeitpunkt eigenem Bekunden zufolge „gedacht“ hatte, dass sein Haus bezüglich Cybersicherheit „gut aufgestellt“ sei. Wie der Geschäftsführer zu diesem Gedanken kam, ist nicht bekannt; weitere Presseanfragen beantwortet die Klinik nicht. Es wirkt, als ob der Geschäftsführer einer Klinik mit 40.000 Patienten jährlich auf ein Risikomanagement verzichtet und sich stattdessen auf seinen Glauben verlässt.

Wenn eine ganze Klinik auf diese Weise „zufällig“ lahmgelegt werden kann, wird das Problem durch die Digitalisierung nicht kleiner: Das Internet der medizinischen Dinge – einschließlich „intelligenter“ (Krankenhaus-)Gebäude und (Kranken-)wagen, Computertomographen, Insulin- und Infusionspumpen künden davon. Nicht einmal Zahnbürsten bleiben davon verschont. Ganz nach dem Wunsch von Telekom-Chef Timotheus Höttges: „Alles wird vernetzt“. So werden viele Daten gewonnen und per künstlicher Intelligenz (kI) erschlossen; das ermöglicht nicht nur eine personalisierte Medizin, sondern womöglich demnächst auch das personalisierte 3D-Drucken menschlicher Organe, Nanoroboter in der Blutbahn, Chips im Gehirn und das Behandeln von Erbkrankheiten beim Facharzt für Humangenetik.

Die Stanford University School of Medicine glaubt gar an ein „Internet der Gene“: Jede Erbinformation eines jeden Menschen ließe sich dann einzeln verändern. Ähnlich engagiert ist die „Hamburg Brain School“ unterwegs; die hat sich die Vernetzung der "neurowissenschaftlichen Aktivitäten“ im Universitätsklinikum Eppendorf (UKE) „von der molekularen Ebene bis zur klinischen Forschung“ als Ziel gesetzt „und bietet

zahlreiche Schnittstellen mit neurowissenschaftlich aktiven Instituten der Universität Hamburg (insbesondere dem Psychologischen Institut). Es vereint aktuell mehr als 400 Wissenschaftler und Doktoranden aus 18 Instituten und Kliniken des UKE.“ Die Begeisterung über die Technik trübt den Beteiligten offenbar den Blick auf die Risiken – und die eigenen Fähigkeiten, damit umzugehen.

Der denkbare Diebstahl von Patientendaten ist das Eine: Sie lassen sich zum Beispiel an Kreditinstitute oder Versicherungen verkaufen. Und: In den „falschen Händen“ seien Patientendaten „grundsätzlich wertvoll“ – so eine Studie aus der Schweiz. In der Telekommunikationswirtschaft sollen Mitarbeiter bereits mit kompromittierendem Material erpresst werden; das Ziel: Die Herausgabe von Unternehmensinformationen. Alternativ könnten die Betroffenen womöglich als Saboteur angeworben werden.

Viel bedrohlicher ist jedoch, dass Patientendaten auch manipulationsanfällig sein könnten: Der Sicherheitsdienstleister Kaspersky will weltweit „mehr als tausend“ medizinische Geräte gefunden haben, auf die übers Internet zugegriffen werden kann. Wissenschaftler behaupten, sie könnten über die Infrastruktur von Herzschrittmacher-Herstellern Schadsoftware auf implantierte Geräte einschleusen. Dann könnte der Herzschrittmacher angeregt werden, seinem Träger 830 Volt Schläge mit tödlichen Konsequenzen zu verpassen. 2017 erhielten Herzschrittmacher-Patienten von Abbott ein Update aufs Herz; nach Angaben der Firma allein 12.000 in Deutschland. Ursache dafür waren wohl drei Software-Fehler; einem davon hat die US-Bundesregierung einen „hohen“ Schweregrad verpasst. Eine Amerikanische Kongressabgeordnete befürchtet jedoch, dass „Millionen“ solcher verwundbarer Geräte „in unseren Körpern implantiert“ sein könnten.

Die Leistungsfähigkeit der Informationstechnik ist also Segen und Fluch gleichermaßen: „Automatisierung schafft neue Angriffsflächen“, warnt die Computerwoche. Außerdem senkt die wachsende Leistungsfähigkeit die Kosten für die Angreifer. Umgekehrt explodieren die Gewinne: Zwischen 2015 und 2021 sollen sie sich weltweit von 3 auf 6 Billionen (!) US-Dollar verdoppeln.

Unklar ist dabei nur, ob dabei auch schon die künftig verfügbare Leistungsfähigkeit berücksichtigt ist: Das ZDF befürchtet „Angriffe mit Künstlicher Intelligenz“. Der Russische Präsident Wladimir Putin ist gar der Ansicht, wer bei künstlicher Intelligenz in Führung gehe, „wird die Welt beherrschen“. Vermutlich ist keine künstliche Intelligenz notwendig, um eine Zielperson gefügig zu machen, wenn der Angreifer Zugang zu seinen medizinischen Daten oder seinen implantierten Geräten haben sollte. Schädlich wäre sie aber auch nicht.

Das Dänische Centre For Cyber Security hat sich mit den Angreifertypen beschäftigt: Die Bedrohung des Gesundheitswesens durch Geheimdienste sei „sehr hoch“. Sehr hoch sei auch die durch die Datenkriminalität. Klingt plausibel: Eine einzelne Patientenakte bringt auf dem Markt bereits 300 bis 500 US-Dollar. Die Blutgruppe lässt sich eben nicht so leicht austauschen wie die Kreditkarte. Und viele Mitarbeiter sollen bereit sein, Patientendaten für 500,- bis 1000,- US-Dollar zu verkaufen. Je nachdem wieviel tausend Patientenakten in einer solchen Datenbank enthalten sind, winkt eine stolze Gewinnspanne. Die Bedrohung durch Cyberterroristen halten die Dänischen Forscher für gering; interessant ist die Begründung: Terroristen hätten wohl Interesse an Patientendaten, es mangele ihnen jedoch am Wissen, diese für ihre Zwecke zu verwenden. Wobei – so viel Wissen ist nicht einmal erforderlich, um Terror zu verbreiten: Vor zwei Jahren wurde eine Liste mit 8700 Personen veröffentlicht und gefordert: „Tötet sie, wo immer ihr sie findet!“

Andere „Innentäter“ wollen einfach nur gegen die Kommerzialisierung des Gesundheitswesens protestieren – Daten von 300 Kliniken des Krankenhauszweckverbands Rheinland sollen deshalb ins Netz geraten sein. Noch eine Ursache: Gedankenlosigkeit! Ein Klinik-Mitarbeiter aus der EDV-Abteilung soll bei einer Raucherpause ein Datensicherungsband vergessen haben. Es soll mehr als hunderttausend Patientendatensätze enthalten haben.

Seit Mai 2018 haftet der Verantwortliche/Auftragsverarbeiter nach der Datenschutzgrundverordnung (DSGVO) für Schäden, wenn er nicht nachweisen kann „dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist“. Dabei ist es der Verordnung zufolge unerheblich, ob diese Schäden „unbeabsichtigt“ oder „unrechtmäßig“ entstanden sind. Der Verantwortliche soll dazu die Risiken systematisch erfassen, bewerten und entsprechende Maßnahmen ergreifen, um seine Datenverarbeitung nach dem „Stand der Technik“ zu schützen;

Das Justizministerium definiert den Begriff so: „Stand der Technik ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, der nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlich vorgegebenen Zieles gesichert erscheinen lässt. Verfahren, Einrichtungen und Betriebsweisen […] müssen sich in der Praxis bewährt haben oder sollten – wenn dies noch nicht der Fall ist – möglichst im Betrieb mit Erfolg erprobt worden sein“. Der Regierung ist also das Beste grade gut genug, was der Markt an technischen und organisatorischen Maßnahmen (TOM) hergibt.

Doch das ist noch lang nicht alles: Die Verordnung brummt dem Verantwortlichen eine „Rechenschaftspflicht“ auf; er muss nicht nur für Sicherheit sorgen, sondern auch noch nachweisen können, dass er Datensicherheit und Datenschutz gewährleistet. Defacto bedeutet das „Sicherheit 4.0“ fürs vernetzte Gesundheitswesen – dazu sind technische, organisatorische und Bildungsmaßnahmen notwendig: Wir müssen -- flächendeckend, systematisch, proaktiv! -- investieren in Sicherheits-/Notfallkonzepte, physikalischen Einbruchschutz, elektronische Signaturen, kryptographische Verschlüsselungen, IAM-/SIEM-Systeme, rollenspezifische Bildung für Alle, herstellerunabhängige, (nach Möglichkeit dynamische) Gütesiegel für die Wolke sowie Produkte/Dienstleistungen/"Apps" und Penetrationstests. Dabei bitte den Stand der Technik nicht vergessen – vielfach ist das künstliche Intelligenz, denn kI soll auch Wege finden, die dem Menschen auf den „ersten Blick“ verborgen bleiben.

Das gilt – der Vernetzung sei Dank! – nicht nur für die Heilberufe, – einschließlich Apotheken, medizinischen Laboren, die „Physiotherapie 4.0“ und skypende (!) Logopäden, sondern auch für die Entwickler von (Branchen-)software, Krankenversicherer (und ihrem Aussendienst!), Krankenhausbetreiber, die Betreiber von Krankenwagen-Flotten (und ihren Werkstätten), die Hersteller medizinischer Geräte sowie Anbieter „personalisierter“ Medikamente, Lebens- und Nahrungsergänzungsmittel.

Vielfach ist dabei mit „hohen Risiken“ zu rechnen – die verlangen dann nach einer Datenschutzfolgenabschätzung (DSFA). Diese enthält dem Gesetzgeber zufolge „zumindest Folgendes:

1. „eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

2. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
3. eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen […] und
4. die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird."

Der Verband forschender Arzneimittelhersteller (VfA) fordert eine solche DSFA „vor der umfangreichen Verarbeitung aller Gesundheitsdaten". Davon wären dann wohl alle 190.000 Arztpraxen in Deutschland betroffen. Wer meint, dass sie/er nicht zum Kreis der Verpflichteten gehört, sollte sich eine gute Begründung dafür überlegen.

Soweit zum SOLL. Tatsächlich sollen 90 Prozent der kleinen Unternehmen keinerlei Datensicherungsmaßnahmen ergriffen haben – berichtet Healthcare Informatics im Januar 2019 unter Berufung auf eine Studie der US-Bundesregierung.

Datensicherungsmaßnahmen müssten sich allein schon auf die Personalauswahl auswirken – dass das nicht der Fall ist, beweist eine Facharztpraxis für Humangenetik in einer Stellenanzeige; die geforderte Qualifikation: „Kompetenzen in NGS, MLPA, Bioinformatik, EDV, und mit guten Englischkenntnissen". Von Kenntnissen über „Risikomanagement" oder gar „Datenschutzfolgenabschätzung" ist da keine Rede. Das bedeutet: Dieser Praxisinhaber legt Wert darauf, die Leistungsfähigkeit der Technik bis zum Anschlag zu nutzen. Womöglich hängt der scheinbare Bewusstseinsmangel des Arztes mit einer mangelhaften Weiterbildung zusammen. Die Bayerische Landesärztekammer verlangt in ihrer 79 seitigen Weiterbildungsordnung im Oktober 2017 kurz und bündig: „Datensicherheit und Datenschutz in der Medizin: Rechtliche Vorschriften; Prinzipien und Maßnahmen zur Gewährleistung des Datenschutzes". Risiken? Datenschutzfolgenabschätzung??

Seit Oktober 2018 prüft die Aufsichtsbehörde in Ansbach acht Bayerische Arztpraxen, wie sie sich vor Erpressungstrojanern schützen. In ihrem zweiseitigen Fragebogen wollen die Datenschützer vom Amt wissen: „Führen Sie regelmäßige automatisierte Backups Ihrer Patientendaten durch?", „Ist das Praxisverwaltungssystem (PVS) an das Internet angeschlossen?" und „Ist bekannt, dass bei einem erfolgreichen Angriff durch einen Verschlüsselungstrojaner eine Meldung beim Bayerischen Landesamt für Datenschutzaufsicht durchgeführt werden muss?" Die Erwartungen der Behörde sind offenbar so bescheiden, dass sie sich dezidierte Fragen zum Risikomanagement gleich geschenkt hat.

Erlauben sich Praxisinhaber, Geschäftsleitung und andere Verantwortliche hier Patzer, riskieren sie Geldbußen und Schadenersatzforderungen seitens der Betroffenen: 400.000 Euro soll eine Klinik in Portugal berappen, weil ihr Berechtigungsmanagement mangelhaft gewesen sein soll.

Das kann die Bonität des Unternehmens belasten. Die Verantwortlichen müssen schließlich damit rechnen, dass sie vom Arbeitgeber persönlich für den Schaden haftbar gemacht werden. Eine Erfahrung die kürzlich frühere Vorstandsmitglieder einer Österreichischen Aktiengesellschaft machen mussten: Für einen Schaden in Höhe von

54 Millionen Euro sollten sie 10 Millionen Euro zurückzahlen. Der Vorwurf: Die Beklagten hätten "in ihren Funktionen die Einrichtung eines angemessenen internen Kontrollsystems (IKS) verabsäumt und die Pflicht zur kollegialen Zusammenarbeit und Überwachung verletzt". Unbekannt ist, ob die früheren Vorstandsmitglieder grade flüssig sind. Interessant ist da ein Blogbeitrag der Anwaltskanzlei Flick Gocke Schaumburg: „Aufsichtsräte müssen Schadensersatzansprüche gegen Vorstandsmitglieder auch dann verfolgen, wenn dadurch zugleich ihre eigene Pflichtverletzung offenkundig wird und damit auch eine Aufsichtsratshaftung droht“.

Und nicht zuletzt sinkt der Börsenkurs am Tag des Bekanntwerdens einer Datenpanne um durchschnittlich 5 Prozent. Umgekehrt profitieren Unternehmen davon, wenn sie in ein Dateschutzmanagement-System investieren. Das kann man sich dann noch dazu zertifizieren lassen. Vor Jahren veröffentlichte der Bitkom eine Broschüre über „Betriebssichere Rechenzentren“ – darin wird behauptet, eine Zertifizierung brächte auch eine „Verbesserung des Rankings und der Kreditwürdigkeit“ mit sich. Das gilt wohl nicht nur für Rechenzentren.

Schließlich müssen wir unser Bildungswesen aktualisieren: Die künftig im Gesundheitswesen tätigen verantwortlichen Ärzte, Ingenieurinnen, Informatiker, Psychologinnen und Kaufleute werden vielfach hohe Risiken eingehen (müssen). Diese Menschen sollten wohl bereits während ihres Studiums lernen, wie mit Risiken umzugehen ist, wie DSFA durchzuführen sind, wie Institutionen und Prozesse verantwortungsbewusst organisiert werden können, sodass ihr jeweiliges (nicht-akademisches) Personal in der Lage versetzt wird, Patienten/Versicherte samt ihren Daten angemessen zu schützen. Unklar ist jedoch, woher wir viele Tausend Menschen nehmen wollen, die dieses Wissen vermitteln. Wir müssen jetzt darüber reden, wie wir diesen Zustand verbessern!

Gesundheit für 2019 wünschen Ihnen

Holger Berens
Vorstandsvorsitzender Bundesverband für den Schutz Kritischer Infrastrukturen (BSKI e.V.)

Benjamin Bolzmann
Betrieblicher Datenschutzbeauftragter,
TRUECARE IT- und Projektmanagement GmbH

Carl Dietzel,
Sachverständiger für Datenschutz und Datensicherheit

Lucia Ferrigno,
Wirtschaftsjuristin, Datenschutzauditorin und externe Datenschutzbeauftragte

Joachim Jakobs, Freier Journalist

Guido Johannes Lorc
Production Manager Gateway Service Platform (Smartmetering) T-Systems International GmbH

Sascha Rösgen
Datenschutz-& IT-Sicherheitsbeauftragter

Nikolaus Stapels
VdS Fachberater für Cyber Security (Norm 3473)