Die Welt | 15.12.12

Die große Datenunsicherheit

Die Spionageaffäre bei Minister Bahr wirft ein Schlaglicht auf grundlegende Missstände im Gesundheitswesen. Die gesamte Branche geht fahrlässig mit Patientenunterlagen um *Von Ulrich Clauß*

In Praxen, Apotheken und Kliniken ist der Datenschutz unterfinanziert, und Missbrauch wird Tür und Tor geöffnet

Das Bundesministerium für Gesundheit nimmt den Schutz Ihrer persönlichen Daten sehr ernst. Aus diesem Grunde haben wir Maßnahmen getroffen, die sicherstellen, dass die Vorschriften über den Datenschutz sowohl von uns als auch von unseren externen Dienstleistern beachtet werden." So steht es auf der Internetseite des Bundesgesundheitsministers. Doch seit der Maulwurfaffäre im Hause von Daniel Bahr (FDP) sind Zweifel an den Beteuerungen des Ministers angebracht.

Vor allem was die genannten externen Dienstleister angeht, hat Minister Bahr seit dieser Woche ein Problem. Und nicht nur er, sondern mit ihm die gesamte Branche. Nach Experteneinschätzung sind nicht nur die vom Gesundheitsminister, sondern ebenso die von Apothekern, Ärzten und Kliniken beauftragten externen EDV-Dienstleister das Sicherheitsrisiko Nummer eins.

So soll die Apothekenlobby mithilfe eines externen Dienstleisters einen Maulwurf ins Bundesgesundheitsministerium eingeschleust haben, der über zwei Jahre sensible Daten nach draußen schmuggelte – geheime Gesetzentwürfe, Referentenpapiere, E-Mails. Die Staatsanwaltschaft Berlin (Link: http://www.welt.de/themen/berlin-staedtereise/) ermittelt gegen einen freiberuflichen Pharma-Vertreter. Außerdem soll die Apotheker-Lobby in großem Stil personenbezogene Daten von Patienten missbraucht haben. Interessenten für solche Daten gibt es viele. Die Pharma-Industrie zum Beispiel ist bekannt für ihren Hunger nach Patientendaten und beschafft sich diese per Lieferverträgen sogar direkt von der Quelle: den Apotheken.

Der Daten-GAU im Gesundheitsministerium und seine Weiterungen werfen ein Schlaglicht auf unzulänglichen Datenschutz im gesamten Gesundheitssektor, wo nach Experteneinschätzung nicht nur an der Spitze des zuständigen Bundesministeriums merkwürdige Verhältnisse herrschen. "Im Gesundheitssektor werden nur ein bis zwei Prozent des Umsatzes für Informationstechnologie aufgewendet", sagt der Wirtschaftsinformatiker Thomas Jäschke vom Dortmunder Institut für Datensicherheit im Gesundheitsbereich der "Welt". In der Privatwirtschaft seien es durchschnittlich fünf Prozent. "Ich sehe da einen erheblichen Investitionsstau in der Branche." Jäschke leitet ein Institut für Datensicherheit im Gesundheitssektor und fungiert als Datenschutzbeauftragter von über 600 Arztpraxen. "Einige große externe Dienstleister arbeiten quer durch die Gesundheitsbranche, von der Apotheke über die Arztpraxen bis zur Betreuung von Großkliniken. Die Risiken, dass diese Daten verknüpft und unrechtmäßig weiter verwandt werden, sind sehr groß", warnt Jäschke. Auch sähe er bei "Zahnärzten und ihren kassenärztlichen Verbänden einen eklatanten Mangel an Konzepten für den Datenschutz".

Auch für Jean-Pierre Seifert, Professor für das Fachgebiet "Security in Telecommunications" an der TUBerlin, hat der in letzter Zeit bekannt gewordene millionenfache Missbrauch von Patientendaten seine Ursache beim fahrlässigen, wenn nicht sogar vorsätzlich lockeren Umgang von externen Dienstleistern mit Patientendaten. "Hier ist oftmals Tür und Tor für den Missbrauch geöffnet, auch durch den Kostendruck", sagt Seifert. "Ich halte es für unverantwortlich, unverschlüsselte Patientendaten von Apotheken und Arztpraxen an externe Dienstleister zu übermitteln. Generell ist die dezentrale Bewirtschaftung der Daten im Gesundheitsbereich mit großen Sicherheitsrisiken verbunden."

Auch in Kreisen der IT-Sicherheitsindustrie gilt der sorglose Umgang im Zusammenspiel mit ausgelagerter Datenwirtschaft als eines der Hauptrisiken für den Schutz von Patientendaten: "Wenn über Jahre große Datenmengen aus einem EDV-System entwendet wurden, wie das offenbar jetzt im Bundesgesundheitsministerium geschehen ist, dann lässt das unbedingt auf schwere Mängel bei der technischen Absicherung schließen", sagt Christian Vogt, Regional Director Deutschland (Link: http://www.welt.de/themen/deutschland-reisen/) und Niederlande bei Fortinet, dieser Zeitung. Die Firma ist ein großer IT-Sicherheitsdienstleister und Weltmarktführer bei multifunktionalen Firewalls. "Im Healthcare-Sektor haben wir es mit sehr heterogenen IT-Umgebungen zu tun. Da findet man auf der einen Seite Apothekenbetriebe vor, die noch mit Windows98 arbeiten, dem stehen modernste Großrechenanlagen bei Krankenhäusern und Krankenkassen gegenüber", so Vogt. Oft werde der Aufwand gescheut, Sicherungssysteme auf dem Stand der Technik zu installieren.

Vor allem die verteilte Datenwirtschaft im Gesundheitssektor ist das Problem. In Arztpraxen und Apotheken, wo die hochsensiblen Patientendaten als Erstes anfallen, herrschen zum Teil sehr bedenkliche Zustände. "Gehen Sie mal in eine normale Arztpraxis, da muss bei mehr als zehn Angestellten ein Datenschutzbeauftragter bestellt werden, das macht doch kaum jemand. Bestenfalls wird einer Sprechstundenhilfe auf die Schulter geklopft und gesagt: Du machst das jetzt. Das sind meine Erfahrungen", berichtet Medizininformatiker Jäschke. Dazu komme die Mentalität der Ärzte. "Ärzte sehen sich mehrheitlich nicht als Unternehmer und schaffen keine geordnete betriebswirtschaftliche Basis in ihrem Betrieb. Das geht oftmals auf Kosten von Datenschutz und Datensicherheit", so Jäschke. Zum Beispiel würden Patientendaten zumeist unverschlüsselt in den Praxen gespeichert. "Bei den häufigen Einbrüchen in Arztpraxen gelangen also oftmals höchst sensible Daten in falsche Hände."

Offizielle Statistiken über Datenschutzvergehen und -missbrauch im deutschen Gesundheitssektor gibt es nicht. Die zahlreichen Einzelfälle in jüngster Zeit haben jedoch die Datenschutzbeauftragten der Länder alarmiert. Sie wollen sich die Branche nun endlich etwas genauer anschauen. So untersuchte der rheinland-pfälzische Landesbeauftragte für den Datenschutz, Edgar Wagner, den Datenschutz bei Versandapotheken. In nahezu allen Fällen sei der Einsatz von Passwörtern mangelhaft und der Anmeldevorgang deshalb nicht sicher, stellte er fest. Der Hamburger Datenschutzbeauftragte stellte in mehreren Fällen mangelnden Datenschutz in Kliniken fest. Gemeinsam erarbeiteten die Landesdatenschützer inzwischen Rahmenrichtlinien für den Datenschutz in Kliniken. Nach überwiegender Einschätzung der von dieser Zeitung befragten Experten würde bislang praktisch kein Großklinikum oder Krankenhaus in Deutschland diesen Anforderungen genügen.

Versäumnisse und Handlungsbedarf stellen die Experten auch bei Verbänden und Standesvertretungen der Branche fest. So haben es die Apothekerverbände der Länder bis heute nicht fertiggebracht, eine bundeseinheitliche verbandstechnische Regelung für den Umgang mit Patientendaten zu erarbeiten. "Die Unkenntnis über den Umgang mit sensiblen, personenbezogenen Daten, wie sie in Apotheken vorliegen, unterstützt die Möglichkeiten des Verstoßes gegen geltendes Datenschutzrecht durch Apotheker und Mitarbeiter", stellt dazu Möritz Görmann fest, externer Datenschutzbeauftragter und Geschäftsführer der CTM-COM GmbH für "Datenschutz und IT-Sicherheit". Er betreut 50 mittelständische Apothekenbetriebe in Hessen, Bayern und Rheinland-Pfalz. "Die Apotheker liefern oft ihre Daten unverschlüsselt und inklusive der personenbezogenen Anteile an externe Dienstleister zur Weiterverarbeitung, damit ist die Kontrolle über diese Daten in keiner Weise mehr gegeben", pflichtet ihm Medizininformatiker Jäschke bei.

Aufmerksamkeit in der Branche ist durch den beispiellosen Fall von Politikspionage beim Gesundheitsminister jedenfalls hergestellt, nach Experteneinschätzung kein Einzelfall. "Der aktuelle Fall dürfte erst der Anfang sein. Ich halte es für sehr wahrscheinlich, dass an zahlreichen Stellen in der politischen Administration Datenlecks vorliegen. Die allermeisten Fälle werden allerdings nicht öffentlich – wie auch in der Privatwirtschaft", sagt Sebastian Schreiber, Geschäftsführer des IT-Sicherheitsdienstleisters Syss GmbH, der "Welt". Offenbar wird erst aus Fehlern gelernt – beim Minister wie in der Apotheke. "Jeder Betrieb wird so lange sorglos mit den Patientendaten umgehen, bis etwas schiefgeht. Es muss immer erst einmal knallen, bevor etwas passiert", sagt TU-Professor Seifert. Geknallt hat es nun, zumindest beim Minister. Die Frage ist, ob man auch im Rest der Gesundheitsbranche den Schuss gehört hat.