Podiumsdiskussion zu Cybersicherheit

Vor dem Hintergrund des Bekanntwerdens gravierender Sicherheitslücken in der sogenannten Telematikinfrastruktur (TI) für Arztpraxen, Kliniken und Krankenkassen fragen sich derzeit viele Ärzte, wie sie auch künftig den Schutz von vertraulichen Patientendaten sicherstellen können. Am 15. Januar 2020 fand im PresseClub München unter dem Titel „Wie lassen sich Emotet-Epidemien (Schadprogramme) im Gesundheitssektor verhindern?" eine Podiumsdiskussion zu diesem Thema statt. Daran nahmen neben Professor Dr. Siegfried Jedamzik, Geschäftsführer der Bayerischen TelemedAllianz, und Dr. Marc Maisch, Rechtsanwalt und Datenschutzbeauftragter, die Investigativ-Journalistin Sabina Wolf sowie der CEO der IT-Sicherheitsfirma hack-CARE, Viktor Mraz, teil. Die Diskussionsteilnehmer debattierten primär über die datenschutzrechtlichen Herausforderungen der Digitalisierung und praktische Lösungen für die Ärzteschaft.

Zuallererst merkte Jedamzik an, dass Kliniken, Arztpraxen und Apotheken eine besonders attraktive Beute für Hacker und Cyber-Kriminelle seien. Denn zum einen sei die IT-Sicherheitsinfrastruktur vieler dieser Einrichtungen nicht auf dem neuesten Stand, was sie zu einem leichten Ziel von Malware-Attacken (Schadprogramme) mache. Zum anderen seien Patientendaten auf dem Schwarzmarkt oft mehrere tausend Euro wert. Besonders interessant könnten solche Daten dabei für Versicherer und Werbeplattformen jeglicher Couleur sein. Durch die Einspeisung sensibler Patientendaten in ihr System könnten Werbeplattformen den Betroffenen etwa passgenau abgestimmte Werbeangebote machen. Versicherer hingegen könnten in Erwägung ziehen, von Bürgern und Versicherten höhere Beiträge zu verlangen oder ihnen den Abschluss einer Versicherung zu verweigern.

Äußerst gefährlich sei aber die Möglichkeit, dass durch Hackerangriffe sensible Geräte in Praxen oder Krankenhäusern ausfallen könnten. Vorstellbar sei etwa, dass durch eine Störung der IT computertomografische Scans nicht durchgeführt werden könnten, was zeitkritische Operationen deutlich erschweren oder sogar unmöglich machen könne. Schwerwiegende Konsequenzen könnten auch nicht zur Verfügung stehende bzw. von Hackern veränderte Patientendaten nach sich ziehen. Werde etwa die in den Daten festgehaltene vorgeschriebene Dosierung eines Medikaments verändert, könne das negative Auswirkungen auf den Gesundheitszustand des betroffenen Patienten haben.

Dies gelte es unbedingt durch eine gut ausgebaute IT-Sicherheitsinfrastruktur zu verhindern. Auch müsse das Personal von Praxen und Kliniken sowohl über die Strategien von Hackern als auch über die in der Datenschutzgrundverordnung (DSGVO) festgehaltenen aktuellen datenschutzrechtlichen Bestimmungen aufgeklärt werden. Ein Problem könne hierbei aber die bereits bestehende hohe Arbeitsbelastung von Ärzten darstellen: „Wenn ein Hausarzt jeden Tag 150 Patienten behandelt, liegt der Fokus nicht bei der DSGVO", merkte Jedamzik an.

Viktor Mraz fügte hinzu, dass auch das sogenannte Phishing ein großes Problem sei, das heißt Versuche von Hackern, über Malware wie zum Beispiel Trojaner an persönliche Daten eines Internetnutzers zu gelangen und daraufhin Identitätsdiebstahl zu begehen. Ein Hacker könne so zum Beispiel an das E-Mail-Passwort eines Arztes oder eines Medizinischen Fachangestellten gelangen und dann mit dessen E-Mail-Adresse mit Malware infizierte E-Mails versenden. Insofern mache jeder Arzt oder Medizinische Fachangestellte, der Phishing-Opfer werde, leicht Dutzende seiner Kollegen und Patienten zu Opfern, weil sie arglos E-Mails mit Anhängen öffnen würden, die von ihm zu stammen scheinen.

Viele Einrichtungen im Gesundheitswesen hätten noch nicht realisiert, dass die neuen Datenschutzregeln der EU eine Beweislastumkehr mit sich bringen würden. Mussten nach dem alten Bundesdatenschutzgesetz die Betroffenen nachweisen, dass ein Verstoß gegen den Datenschutz vorliegt, so müssen nun die Praxen oder Krankenhäuser beweisen, dass sie den Datenschutz befolgen. Im Zweifel könnten so hohe Schmerzensgelder und Schadensersatzansprüche fällig werden, sagte Maisch.

Ein anderer Punkt im Zusammenhang mit der DSGVO, der von mehreren Teilnehmern der Podiumsdiskussion angesprochen wurde, war das Thema Gesundheits-Apps.

Die Teilnehmer der Podiumsdiskussion stimmten überein, dass intensive Schulungen bei allen Mitarbeitern von Praxen und Kliniken eine erste wichtige Maßnahme seien, um die datenschutzrechtlichen Herausforderungen der Digitalisierung bewältigen zu können. Ferner sei es entscheidend, dass auch kleinere Praxen stets eine Checkliste führen würden, auf der Ansprechpartner aus der IT und Handlungsschritte notiert seien, um beim Eintreten eines IT-Notfalls sofort die notwendigen Maßnahmen einzuleiten.

Florian Wagle (BLÄK)