

17.10.2019

Antwort

der Landesregierung

auf die Kleine Anfrage 2994 vom 19. September 2019
des Abgeordneten Matthi Bolte-Richter BÜNDNIS 90/DIE GRÜNEN
Drucksache 17/7454

Patientendaten ungeschützt im Netz – was passiert in NRW?

Vorbemerkung der Kleinen Anfrage

Der Bayerische Rundfunk meldete am 17. September 2019, dass Millionen von Patientendaten ungeschützt im Internet zugänglich gewesen seien.¹ Hierbei handle es sich beispielsweise um Brustkrebscreenings, Wirbelsäulenbilder und Röntgenaufnahmen. Diese seien verknüpft mit personenbezogenen Daten wie Geburtsdatum, Vor- und Nachname, Termin der Untersuchung und Informationen über den behandelnden Arzt oder die Behandlung selbst.

Aus Deutschland besonders betroffen sind dem Bericht zufolge Daten aus Bayern und Nordrhein-Westfalen.

Der Minister für Arbeit, Gesundheit und Soziales hat die Kleine Anfrage 2994 mit Schreiben vom 17. Oktober 2019 namens der Landesregierung im Einvernehmen mit dem Minister des Innern sowie dem Minister für Wirtschaft, Innovation, Digitalisierung und Energie beantwortet.

1. Welche Informationen liegen der Landesregierung über den Sachverhalt vor?

Das Ministerium für Arbeit, Gesundheit und Soziales wurde am 17. September 2019 über eine Presseanfrage mit Bezug auf die Veröffentlichung der Rheinischen Post (https://rp-online.de/nrw/staedte/kempen/datenleck-millionen-von-patientendaten-ungeschuetzt-krankenhaus-kempen-betroffen_aid-45882501) auf den Sachverhalt aufmerksam.

Daraufhin wurde von Seiten des Ministeriums unverzüglich eine Stellungnahme des Hospitals zum Heiligen Geist eingeholt.

¹ Quelle: <https://www.br.de/nachrichten/deutschland-welt/millionenfach-patientendaten-ungeschuetzt-im-netz,RcF09BW>

Datum des Originals: 17.10.2019/Ausgegeben: 23.10.2019

Die Geschäftsführung des Krankenhauses versicherte, dass keine Patientendaten aus den EDV-Systemen der Hospital zum Heiligen Geist GmbH & Co. KG offen im Internet zugänglich waren und sind. Das Krankenhaus habe umfangreiche Vorkehrungen zur Datensicherheit getroffen und keinen unerlaubten Zugriff auf seine Systeme feststellen können.

Hinsichtlich der in der Presse geäußerten Verdachtsmomente auf einen möglichen Datenschutzverstoß bezogen auf die radiologische Gemeinschaftspraxis in Kempen liegt keine Zuständigkeit der Landesregierung vor. Die unabhängige Landesbeauftragte für Datenschutz und Informationsfreiheit ist eingeschaltet worden.

2. *Wie viele Patientinnen und Patienten aus Nordrhein-Westfalen sind nach Kenntnis der Landesregierung betroffen?*

Zusätzlich zu den in den öffentlichen Medien bekannt gemachten Informationen liegen der Landesregierung keine weiteren Kenntnisse zu dem Sachverhalt vor. Daher kann die Frage nach der Anzahl der betroffenen Patientinnen und Patienten nicht beantwortet werden.

3. *Durch welche Maßnahmen wurden die Betroffenen von wem informiert?*

Die Verarbeitung und der Verkehr personenbezogener Daten unterliegen der Datenschutz-Grundverordnung, welche auch die Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person regelt. Die Landesregierung ist in diesen Prozess nicht eingebunden.

4. *Welche konkreten Maßnahmen für einen besseren Schutz von Gesundheitsdaten beabsichtigt die Landesregierung, auf Bundes- und Landesebene mit welchem Zeithorizont zu unternehmen?*

Die Verantwortung für die sichere Speicherung der Patientendaten in den EDV-Systemen der Krankenhäuser und Arztpraxen, so genannte Primärsysteme, obliegt der jeweiligen Einrichtung. Krankenhäuser mit mindestens 30.000 vollstationären Fällen im Jahr sind gemäß der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung) verpflichtet, organisatorische und technische Vorkehrungen zu treffen, um ihre IT-Systeme auf den Stand der Technik zu bringen.

Die Krankenhäuser im Geltungsbereich der BSI-Kritisverordnung sind außerdem verpflichtet, erhebliche Störungen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Das BSI wertet die gemeldeten Informationen aus und stellt diese anderen Betreibern sogenannter Kritischer Infrastrukturen sowie den zuständigen Behörden zur Verfügung. Damit soll das Informationsniveau und Know-how bei den Betreibern insgesamt erhöht und damit die Sicherheit verbessert werden.

Mit der Einführung der elektronischen Patientenakte werden vergleichbare Patientendaten künftig auch über die Telematikinfrastuktur (TI) übertragen und bei den Betreibern der Patientenakten verschlüsselt gespeichert. Die Spezifikationen der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) sind so gestaltet, dass sowohl die Daten selbst als auch die Transportwege bis zu den Krankenhäusern und Arztpraxen verschlüsselt sind und ein Zugriff auf die Daten nur nach vorheriger Einwilligung durch den Versicherten möglich ist.

Die Schnittstellen der TI zum Internet werden nach Aussage der gematik kontinuierlich mittels Schwachstellenscans überwacht, um unberechtigte Zugriffe unmittelbar zu erkennen und in Abstimmung mit dem betriebsverantwortlichen Anbieter sofortige Gegenmaßnahmen zu ergreifen. Zusätzlich werden die Anbieter der Dienste der TI vor Ort regelmäßig mittels Audits hinsichtlich der implementierten Sicherheitsmaßnahmen und deren Wirksamkeit überprüft. Daneben sollen zusätzlich Tests beauftragt werden, um zu verifizieren, ob die Systeme auch gegen professionelle Angriffe ausreichend geschützt sind.