Hinweise zum Anschluss der Konnektoren für die Telematik-Infrastruktur in den Arztpraxen

Alle Arztpraxen, die an der vertragsärztlichen Versorgung teilnehmen, mussten bis zum 30. Juni 2019 in ihren Praxen die technischen Einrichtungen für den Zugang zur Telematik-Infrastruktur (TI) installieren. Für die Anbindung einer Arztpraxis an die TI ist u. a. ein Konnektor notwendig. Dem Landesbeauftragten für den Datenschutz Sachsen-Anhalt ist bekannt geworden, dass es bei dem Anschluss dieser Konnektoren in Einzelfällen zu technischen Problemen bzw. erheblichen Risiken für die Sicherheit der Daten in den betroffenen Arztpraxen gekommen ist. Aus diesem aktuellen Anlass gibt der Landesbeauftragte die folgenden Hinweise:

Gesundheitsdaten stehen als besondere Kategorien personenbezogener Daten unter erhöhtem Schutz (Art. 9 Abs. 1 DS-GVO, § 203 Abs. 1 StGB). Dies muss sich auch in den technischen und organisatorischen Maßnahmen gemäß Art. 24, 25 und 32 DS-GVO widerspiegeln.

Der Konnektor ist ein von der Gematik zertifizierter vorkonfigurierter VPN-Router, der den daran angeschlossenen Geräten (i. d. R. Kartenleser und Praxis-PCs) den verschlüsselten Zugang zur TI über einen herkömmlichen Internetzugang (z. B. DSL) ermöglicht. Alle Geräte, die direkt an diesem Konnektor angeschlossen sind, haben ausschließlich Zugang zur TI und nicht mehr zum allgemeinen Internet; dies verhindern Firewallregeln im Konnektor. Damit soll erwirkt werden, dass die Geräte am Konnektor lediglich TI-Funktionalitäten umsetzen und nicht gleichzeitig im Internet aktiv sind und so unbemerkt Schadsoftware heruntergeladen werden könnte, die dann den Zugang zur TI ausspionieren könnte.

Diese serielle Anbindung an die TI (oder auch **Reihenbetrieb** des Konnektors) ist für Arztpraxen geeignet, die sonst keine weiteren Sicherheitsvorkehrungen treffen können und keine fortlaufende Betreuung durch einen qualifizierten IT-Dienstleister beanspruchen oder die mit der Anbindung an die TI auch initial an das Internet angeschlossen werden. In dieser Konstellation kann zusätzlich ein abgesicherter Internetzugang (Secure Internet Services - SIS) über die TI kostenpflichtig gebucht werden.

Werden bei diesem Reihenbetrieb keine SIS bei der TI dazu gebucht, verfügt der Praxisrechner hinter dem Konnektor nicht über einen Internetzugang, kann keine Webseiten aufrufen und auch keine Sicherheits- und Softwareupdates durchführen, obwohl die Arztpraxis technisch über einen Internetzugang verfügt. Arztpraxen mit vorhandener Netzwerkinfrastruktur und mehreren Praxis-PCs und Arbeitsstationen entscheiden sich daher mitunter dazu, den Konnektor im Parallelbetrieb zu betreiben.

Im **Parallelbetrieb** wird der Konnektor gleichrangig neben allen anderen Geräten im Praxisnetzwerk betrieben. Die anderen Geräte, wie Praxis-PCs, können dann wahlweise direkt über den Internet-Router (z. B. DSL) auf das Internet zugreifen und auch gleichzeitig über den Konnektor auf die TI.

Der Parallelbetrieb wird von der Gematik nur dann empfohlen, wenn ein bereits vorhandenes und gut ausgebautes Praxisnetzwerk hinreichend gegen Sicherheitsvorfälle geschützt ist. Dazu gehören nicht nur lückenlos konfigurierte Firewall-Einstellungen sondern auch

regelmäßige Router-, Betriebssystem- und Softwareupdates, restriktive Benutzerkonten, ein geschützter Netzwerkzugang (MAC-Adress-Filterung), Abschottung aller Netzwerkkomponenten aus dem Zugangsbereich der Patienten, Whitelists für erlaubte Internetseiten, umfangreiche Antivirenprogramme, restriktive Konfiguration des WLANs und vieles mehr.

Es gibt keine verbindliche Vorgabe der Gematik, wann der Reihenbetrieb und wann der Parallelbetrieb einzurichten ist, weder an die Arztpraxen noch an die IT-Dienstleister vor Ort. Der Parallelbetrieb ist zwar mit höheren Risiken verbunden, gewährt der Arztpraxis allerdings flexiblere Möglichkeiten bei der Internet- und PC-Nutzung.

Wenn nun ein IT-Dienstleister den Anschluss an die TI für eine Praxis einrichtet, kann es passieren, dass der Konnektor keine Verbindung zur TI herstellen kann, da die Router-Firewall nur bestimmte Verbindungsports nach außen zulässt. In diesem Fall ist vorstellbar, dass ein (möglicherweise unerfahrener) IT-Dienstleister die Firewall-Funktionalität des Routers vollständig deaktiviert. Wenn diese Konstellation im Parallelbetrieb auftritt, würde ein zusätzliches Risiko entstehen. Angreifer aus dem Internet und auch Schadsoftware hätten bessere Chancen, das Praxisnetz zu kompromittieren. Daher ergeht folgende Empfehlung an Arztpraxen:

Falls dies nicht bereits bekannt ist, sollte sich die Arztpraxis von Ihrem Dienstleister bestätigen lassen, ob die Anbindung des Konnektors im Reihenbetrieb oder im Parallelbetrieb erfolgt ist. Dazu kann das Muster-Installationsprotokoll „Sichere TI-Installation“ dienen, dass die Gematik kürzlich veröffentlicht hat. Es ist u. a. für Ärzte gedacht, um die fachgerechte Beratung und Installation beim Anschluss an die Telematikinfrastruktur zu prüfen bzw. die entsprechenden Informationen vom Dienstleister einzufordern.

Außerdem sollte die Arztpraxis überprüfen, ob die Firewall des Praxis-Routers durchgehend aktiviert war. Diese Prüfung kann mit Hilfe des heise-Netzwerkchecks (https://www.heise.de/security/dienste/Netzwerkcheck-2114.html) durchgeführt werden. Von einer deaktivierten Firewall ist generell abzuraten, eine Kombination aus deaktivierter Firewall und Parallelbetrieb des Konnektors birgt ein noch höheres Risiko für IT-Angriffe in sich und muss unbedingt vermieden werden.

Generell sollte der Parallelbetrieb durch weitere umfangreiche Sicherheitsmaßnahmen (siehe oben) abgesichert werden. Falls keine entsprechenden Kapazitäten vorhanden sind, jedoch nicht auf einen Internetzugang der Praxis-PCs mit TI-Anbindung verzichtet werden kann, sollte vom IT-Dienstleister der Reihenbetrieb eingerichtet und bei der Gematik der über die TI abgesicherte Internetdienst SIS gebucht werden.

Herausgeber:
Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt
Leiterstr. 9, 39104 Magdeburg

Tel.: (0391) 81803-0
poststelle@lfd.sachsen-anhalt.de
www.datenschutz.sachsen-anhalt.de

SACHSEN-ANHALT
Landesbeauftragter für den Datenschutz