Stellungnahme zu „Telematikinfrastruktur und NSA-Überwachungsskandal“

Berlin, 18.09.2013

Die vielen Medienberichte über das Ausspähen von Bürgerinnen und Bürgern bzw. das Brechen von Verschlüsselungsverfahren beispielsweise durch den amerikanischen Geheimdienst NSA haben bundesweit Fragen zur Sicherheit von gespeicherten Daten ausgelöst. Auch Heilberufler, die tagtäglich mit sensiblen Daten von Patienten umgehen und diese schützen wollen, sind verunsichert.

Als Kompetenzzentrum für Datenschutz und Informationstechnik in einem vernetzten Gesundheitswesen ist die gematik vom NSA-Skandal nicht überrascht worden. Dieser ist vielmehr ein Beleg für Vorgehensweisen von Geheimdiensten, über die IT-Sicherheitsexperten schon lange spekuliert haben. Der Skandal bestätigt zudem, dass die Telematikinfrastruktur (TI) als geschützte Kommunikations- und Sicherheitsinfrastruktur im deutschen Gesundheitswesen dringend benötigt wird. Das Gesundheitswesen braucht die TI als wirksamen Schutz sensibler Patientendaten und als Schutzinstrument gegen den Datenzugriff von Unbefugten. Die Telematikinfrastruktur ist noch wichtiger geworden, um den Patientinnen und Patienten die Sicherheit zu geben, dass ihre Daten geschützt sind und sie ihr Recht auf informationelle Selbstbestimmung jederzeit wahrnehmen können.

1. NSA und andere Geheimdienste „brechen“ Verschlüsselungsverfahren

Bei Geheimdiensten kann im Allgemeinen nicht davon gesprochen werden, dass diese moderne kryptographische Verschlüsselungsverfahren „brechen“. Vielmehr nutzen sie Schwachstellen bei der Umsetzung von Verschlüsselungsverfahren in konkreten Produkten wie etwa ungenügend „zufällige“ Zufallsgeneratoren. Mitunter wirken Geheimdienste auch darauf hin, dass IT-Produkthersteller solche „Fehler“ bewusst einbauen, um diese für die Geheimdienste nutzbar zu machen. Der ehemalige NSA-Mitarbeiter Edward Snowden selbst formuliert im Interview mit der englischen Tageszeitung „The Guardian“: „Verschlüsselung funktioniert. Sauber implementierte, starke Verschlüsselung ist eines der wenigen Dinge, auf die man sich noch verlassen kann.“

Die Sicherheit der personenbezogenen medizinischen Daten in der Telematikinfrastruktur hängt demnach davon ab, dass die starken kryptographischen Verfahren korrekt in sicherheitsgeprüfte Komponenten implementiert werden.

Alle Sicherheitsmechanismen sind immer wieder verschiedenen Hackerangriffen ausgesetzt. Um sich diesen anzupassen, müssen Sicherheitsmechanismen zum Schutz gegen potenzielle Angreifer laufend technisch weiterentwickelt werden. Die einzelnen Maßnahmen werden stets für eine bestimmte Zeit geplant. Das System der Telematikinfrastruktur ist aus technischer Sicht auf fortlaufende Anpassung und Erweiterung ausgelegt.

Die Sicherheitsarchitektur der Telematikinfrastruktur basiert unter anderem auf folgenden Annahmen:

- In der Telematikinfrastruktur werden nur moderne, starke kryptographische Verfahren verwendet. Die in der TI verwendeten kryptographischen Verfahren werden durch das BSI mittels der Technischen Richtlinie 03116 für eCard-Projekte der Bundesregierung vorgegeben. Damit können die verwendeten kryptographischen Verfahren nicht gebrochen werden, da diese zu jeder Zeit an den aktuellen Stand der technischen Forschung angepasst sind.

Die Kryptologen des BSI sind für die Arbeit der gematik maßgeblich. Darüber hinaus verfolgt die gematik auch eigenverantwortlich die wissenschaftliche Fachdiskussion beispielsweise zu den Entwicklungen in der Kryptoanalyse.

- Die kryptographischen Verfahren in den Komponenten der TI werden korrekt implementiert. Denn alle Komponenten, die mit der Verschlüsselung bzw. Entschlüsselung betraut sind, wie etwa die elektronische Gesundheitskarte (eGK), der Heilberufsausweis (HBA) oder der Konnektor, werden durch das BSI nach sogenannten „Common Criteria“ (gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik) evaluiert.
  Die Komponenten behaupten also nicht nur, dass sie über eine korrekte kryptographische Implementierung verfügen, sie werden dahingehend auch durch das BSI im Rahmen der „Common Criteria“ (CC)-Evaluation überprüft.

2. Konsequenzen des NSA-Skandals für die Telematikinfrastruktur

Aus dem aktuell aufgedeckten NSA-Skandal ergeben sich keine unmittelbaren Konsequenzen für das Projekt „elektronische Gesundheitskarte und Telematikinfrastruktur“. Denn Datenschutz und Informationssicherheit hatten bis heute und haben auch in Zukunft höchste Priorität bei dem Aufbau und dem Betrieb der Telematikinfrastruktur. Die gematik ist dabei nach wie vor der geltenden Gesetzeslage verpflichtet. So heißt es beispielsweise in § 291b, Absatz 1 SGB V: *Die gematik hat „die Interessen von Patientinnen und Patienten zu wahren und die Einhaltung der Vorschriften zum Schutz personenbezogener Daten sicherzustellen.“*

In einer aktuellen Stellungnahme vom 13. September 2013 hat das Bundesamt für Sicherheit in der Informationstechnik die Sicherheit der in der Telematikinfrastruktur gespeicherten Daten bestätigt. Sämtliche Sicherheitsvorgaben des BSI für das Gesundheitswesen wie beispielsweise die BSI-Richtlinie TR-03116 werden in den gematik-Spezifikationen berücksichtigt. Um das notwendige Sicherheitsniveau zu erhalten, müssen zudem folgende Vorgaben weiterhin eingehalten werden:

- „Die Sicherheitsleistung der eingesetzten Produkte bzw. zu migrierenden Bestandsanwendungen und -netze muss vor Einsatz in der TI von unabhängigen Instanzen überprüft und bestätigt werden. Dazu müssen auch eindeutige Verantwortlichkeiten (organisatorisch, ggf. auch haftungsrechtlich) vorab zugewiesen werden.
- Das Schlüsselmanagement für den Einsatz der kryptographischen Verfahren in der TI muss überprüfbar den für die PKI der TI definierten Anforderungen entsprechen. Die Güte der verwendeten Schlüssel muss sichergestellt sein.
- Die kryptographischen Vorgaben aus der TR-03116-1 müssen umgesetzt werden. Die Überwachung des Betriebs innerhalb der TI muss auf Grundlage von ISO/IEC 27001 erfolgen, um auf Probleme zeitnah reagieren zu können.
- Datenknoten, die in die TI führen, müssen überwacht werden. Eine ungesicherte Datenverbindung in Netze außerhalb der TI erzeugt Sicherheitsrisiken.

Weitere Anforderungen an die TI zur weiteren Aufrechterhaltung eines hohen Sicherheitsniveaus in der TI

- Einhaltung der in den Spezifikationen der gematik und den Technischen Richtlinien und Schutzprofilen des BSI für die Telematikinfrastruktur gestellten Sicherheitsvorgaben.

- Gewährleistung der Sicherheit der in die TI zu migrierenden Bestandsanwendungen und –netze auf ein den Sicherheitsanforderungen der TI entsprechendes Niveau.
- Eindeutige Zuordnung der Verantwortlichkeiten für die Sicherheit der in die TI zu integrierenden Bestandsanwendungen und -netze.“

Zusatzinformationen

Weitere gute Gründe für die Telematikinfrastruktur
Im Gesundheitswesen werden nach wie vor Unterlagen auf dem Postweg und per Fax versendet oder unverschlüsselt per Email verschickt. Das Risiko ist also groß, dass Unberechtigte Einblicke in Daten von Patienten erhalten. Denn auch Geräte wie Fax, Kopierer und Scanner, die auf einer elektronischen Kommunikation wie dem Internet basieren, können ausgespäht werden. Das Ausspähen solcher Geräte fällt technisch leicht, da die analoge Datenübertragung immer mehr einer digitalen weicht und zunehmend das Internet-Protokoll (IP) verwendet wird. Technisch wesentlich aufwendiger sind hingegen die Analyse und das Zusammenführen von Daten. Das ist in der Telematikinfrastruktur (TI) ausgeschlossen, da die Daten zu keiner Zeit unverschlüsselt vorliegen. Ein potenzieller Angreifer könnte die Daten demnach auch nicht auswerten.

Der Gesetzgeber hat sich bewusst für die TI, einer spezifischen Kommunikations- und Sicherheitsinfrastruktur, als Basis für die digitale und sektorübergreifende Vernetzung im Gesundheitswesen entschieden. Diese ist nicht mit dem ungeschützten Internet vergleichbar. Im Unterschied zum Internet, auf das jeder weltweit zugreifen kann, herrschen in der TI klare „Verkehrsregeln“, deren Einhaltung von der gematik GmbH überwacht wird. Ein wichtiges Ziel ist, Hackerangriffe zu erschweren und damit den Datenschutz im Gesundheitswesen zu stärken.

In der TI werden medizinische Daten nicht nur während der Übertragung durch moderne Verschlüsselungsverfahren geschützt, sondern liegen dort zu keinem Zeitpunkt unverschlüsselt vor. Lediglich in einer vertrauenswürdigen Umgebung, bspw. einer Arztpraxis, in der die Daten wie bisher für die Patientenversorgung verwendet werden, werden die verschlüsselten Daten abgerufen und wieder entschlüsselt.

Da die dafür notwendigen Schlüssel ausschließlich auf den jeweiligen personenbezogenen elektronischen Gesundheitskarten (eGK) und Heilberufsausweisen (HBA) bzw. institutionsbezogenen Karten gespeichert und ausschließlich mittels dieser Karten nutzbar sind, ist eine Entschlüsselung durch unberechtigte Dritte und entsprechend des Forschungsstandes in der Kryptologie (Verschlüsselungsverfahren und Angriffe auf diese Verfahren) ausgeschlossen. Das heißt, ein erfolgreicher Hackerangriff brächte dem Angreifer keine verwertbaren Daten. Er würde nur sehr stark verschlüsselte Daten finden, die er nicht entschlüsseln und keinem bestimmten Versicherten zuordnen kann.

Fakt ist zudem, alle vertraulichen Daten werden an unterschiedlichen Orten gespeichert. Auch müssen sich die Zugriffsberechtigten authentifizieren, nachdem der Versicherte dem Zugriff zugestimmt hat. Es werden ausschließlich verschlüsselte Daten übertragen.

(Rechtlich) festgelegte Lese- und Zugriffsrechte:
Für den Zugriff auf die in der Telematikinfrastruktur gespeicherten medizinischen Gesundheitsdaten gilt das sogenannte Zwei-Schlüssel-Prinzip. Demzufolge ist es nur

einem Heilberufler möglich auf die Daten zuzugreifen, wenn sein elektronischer Heilberufsausweis – der 1. Schlüssel – und die persönliche elektronische Gesundheitskarte des Versicherten – 2. Schlüssel – in das Kartenlesegerät eingebracht werden und sowohl der Heilberufler als auch der Versicherte seine PIN eingeben.

Einzig der lesende Zugriff auf die Notfalldaten ist ohne Eingabe der PIN möglich. Der Versicherte muss der Ablage und dem Auslesen der Notfalldaten im Notfall jedoch zuvor schriftlich zugestimmt haben. Der Heilberufsausweis ist eine Chipkarte, mit dem sich Angehörige der Heilberufe gegenüber der Telematikinfrastruktur ausweisen. Die Heilberufler sind verpflichtet, sich bei jedem Zugriff auf medizinische Daten über die elektronische Gesundheitskarte mit ihrem Heilberufsausweis zu authentifizieren. Ohne diese Legitimation ist es nicht möglich, medizinische Daten zu lesen, zu speichern oder zu ergänzen.

Ein Zugriff auf die auf Wunsch des Versicherten in der Telematikinfrastruktur gespeicherten medizinischen Gesundheitsdaten ist ohne dessen Zustimmung nicht möglich. Der Versicherte erteilt diese Zustimmung entweder durch Eingabe seiner PIN oder durch das Ausstellen einer Zugriffsberechtigung für einen bestimmten Heilberufler.

Für die in der Telematikinfrastruktur mittels der elektronischen Gesundheitskarte des Versicherten erhobenen, verarbeiteten und genutzten personenbezogenen Daten legt § 291a SGB V darüber hinaus rechtliche Rahmenbedingungen fest:

Die Verarbeitung von medizinischen Informationen in den Anwendungen der Telematikinfrastruktur gemäß § 291a Abs.3 SGB V ist für den Patienten freiwillig. Der Patient hat in den sogenannten freiwilligen Anwendungen die Datenhoheit für sämtliche enthaltenen Gesundheitsdaten. Das heißt, die Daten dürfen nur nach ausdrücklicher Zustimmung des Patienten zu dessen medizinischer Versorgung genutzt werden. Patienten autorisieren mittels ihrer PIN zum Zugriff auf ihre Daten.

Der grundsätzlich zugriffsberechtigte Personenkreis auf die mittels der eGK erhobenen Daten, wie beispielsweise Ärzte, Zahnärzte und Apotheker, ist in den Absätzen 4 und 5a des § 291a SGB V festgelegt. Doch sind diese Personengruppen nicht pauschal zum Zugriff berechtigt, sondern müssen durch den Patienten dazu berechtigt werden. Darüber hinaus hat der Patient, gemäß § 291a Abs.4 und Abs.5b SGB V, selbst das Recht, auf seine personenbezogenen Daten zuzugreifen.

In § 291a Abs. 5 und Abs. 5a SGB V sind ferner die Bedingungen für den Zugriff auf die Daten nach § 291a Abs.3 Satz 1 SGB V, also auf die medizinische Daten freiwilliger Anwendungen, rechtlich verankert. So darf der Zugriff nur in Verbindung mit einem elektronischen Heilberufsausweis eines zugriffsberechtigten Heilberuflers erfolgen. Der Patient hat (s.o.) grundsätzlich das Recht auf die Daten zuzugreifen, die seine Person betreffen, allerdings auch nur „in Verbindung mit einem Heilberufsausweis“. Das soll Patienten vor einer Nötigungssituation schützen: Ohne Mitwirkung einer dem Wohl der Patientinnen und Patienten besonders verpflichteten Berufsgruppe können Patienten keine Daten offenbaren. Selbst dann nicht, wenn sie dazu etwa durch ihren Arbeitgeber oder ein Versicherungsunternehmen gedrängt werden.

Schließlich müssen die Zugriffe auf die medizinischen Daten des Versicherten gemäß § 291a Abs. 6 SGB V registriert werden. Dabei ist sicherzustellen, dass mindestens die letzten 50 Zugriffe für Zwecke der Datenschutzkontrolle protokolliert werden. Dadurch

lässt sich zuverlässig zurückverfolgen, wer wann von seinem Zugriffsrecht, das der Patient erteilt hat, Gebrauch gemacht hat. Die Protokolldaten selbst unterliegen allein der Hoheit des Patienten.

Alle Maßnahmen stellen deshalb ein Höchstmaß an Schutz für die personenbezogenen medizinischen Daten sicher. Sämtliche medizinischen Anwendungen basieren darüber hinaus auf Freiwilligkeit. Versicherte können sich also auch dafür entscheiden, die eGK ausschließlich als Versicherungsnachweis zu nutzen. Der Versicherte ist und bleibt also Herr seiner Daten.

Sicherheit durch leistungsfähige kryptographische Verfahren
Die sensiblen medizinischen Daten werden mittels moderner kryptographischer Verfahren geschützt. Diese Verfahren wurden von unabhängigen Wissenschaftlern entwickelt und über mehrere Jahre auf ihre Wirksamkeit hin untersucht. Während diese Verschlüsselungsverfahren die Daten in einem Maße verändern, dass Unbefugte die Daten nicht lesen können, schützen Signaturverfahren darüber hinaus die Daten vor unberechtigter Veränderung oder einem unzulässigen Austausch. Authentisierungsprotokolle erlauben zudem eine sichere Zugriffskontrolle auf Daten.

Notwendig für die meisten kryptographischen Verfahren sind Schlüssel, die in der Regel aus einer zufällig gewählten und nicht erratbaren enormen Zahlenmenge bestehen.

Über das Sicherheitsniveau der eingesetzten kryptographischen Verfahren entscheiden unter anderem:

- *Schlüssellänge und -qualität*
  Ein kryptographischer Schlüssel besteht in der Regel aus einer zufällig gewählten und nicht erratbaren enormen Zahlenmenge. Die Schlüssel beispielsweise für eine qualifizierte elektronische Signatur, mit der digitale Dokumente rechtskräftig digital unterschrieben werden können, haben jeweils eine Länge von 2048 Bit. Das ist eine Zahl mit mehr als 600 Dezimalziffern.

  Die Mindestlängen der Schlüssel für die TI legt das Bundesamt für Sicherheit in der Informationstechnik (BSI) fest. Das BSI orientiert sich dabei am aktuellen Stand von Wissenschaft und Technik. Das BSI veröffentlicht auch Vorgaben für die Zufallszahlenerzeugung, damit zufällig erzeugte Schlüssel wirklich zufällig – also nicht erratbar oder berechenbar – sind.

  Der Heilberufsausweis ist immer mit Schlüsseln für die qualifizierte elektronische Signatur ausgestattet. Notfalldaten können so rechtssicher und für Unbefugte unveränderbar, digital unterschrieben werden. Der Unterzeichner kann damit zu jeder Zeit eindeutig festgestellt werden. HBA und eGK enthalten Schlüssel für eine sichere Authentisierung und für eine sichere Ende-zu-Ende-Verschlüsselung. So kann erreicht werden, dass nur Personen auf Daten in der TI zugreifen können, die dazu auch berechtigt sind.

- *Verwendete Verschlüsselungsmethoden in der TI:*
  Bei einem symmetrischen Verfahren werden zwischen Sender und Empfänger nur gleiche Schlüssel sowohl für die Ver- als auch für die Entschlüsselung benutzt, die beiden bekannt sind. Bei der Aktualisierung der Versichertenstammdaten zwischen der elektronischen Gesundheitskarte und dem Kartenmanagementsystem der Krankenkassen werden symmetrische Verfahren

verwendet. Dabei wird ein vertraulicher und authentischer Kanal aufgebaut, über den die Daten sicher und für Dritte weder lesbar noch von diesen veränderbar übertragen werden.

Bei einem asymmetrischen Verfahren sorgen zwei getrennte, aber eng zusammenhängende Schlüssel (ein öffentlicher und ein privater) für die Ver- und Entschlüsselung, wie zum Beispiel bei der Kommunikation von Konnektor und Fachdiensten des Versichertenstammdatenmanagements. Bei diesem Verfahren werden Daten mittels des sogenannten öffentlichen Schlüssels für einen bestimmten Empfänger verschlüsselt. Der Empfänger muss Inhaber eines privaten Schlüssels sein, der den Schlüsselinhaber als rechtmäßigen Empfänger der Daten ausweist. Nur mittels des privaten Schlüssels können die verschlüsselten Daten entschlüsselt werden.

Hybride Verfahren stellen eine Kombination aus dem symmetrischen und dem asymmetrischen Verfahren dar. Solch eine Kombination ist sinnvoll, um Vorteile von symmetrischen und asymmetrischen Verfahren zu vereinigen. Asymmetrische Verfahren sind (je nach Verfahren) ca. 400-mal so langsam bei der Entschlüsselung wie symmetrische Verfahren. Symmetrische Verfahren kennen keine öffentlichen Schlüssel, die in der TI leicht verteilt werden können.

Ein hybrides Verfahren wird beispielsweise bei der Dokumentenverschlüsselung mittels des im Vergabeverfahren zum Online-Rollout (Stufe1) ausgeschriebenen Konnektors verwendet.

Möchte ein Arzt einem anderen Arzt etwa ein Ende-zu-Ende-verschlüsseltes PDF-Dokument schicken, so wird das Dokument zunächst mittels eines zufällig gewählten symmetrischen Schlüssels chiffriert. Dies geht sehr schnell und der verwendete Schlüssel ist sehr viel kleiner als das Dokument. Der symmetrische Schlüssel wird dann mittels des öffentlichen Schlüssels des Empfängers verschlüsselt. Durch die Public-Key-Infrastructure (PKI) der TI und die sicheren Kartenherausgabeprozesse ist sichergestellt, dass nur der Empfänger den notwendigen privaten Schlüssel für die Entschlüsselung des symmetrischen Schlüssels besitzt. Dieser befindet sich einzig auf dem Heilberufsausweis des Empfängers. Mit dem Entschlüsseln – quasi dem „Auspacken“ – des symmetrischen Schlüssels bringt der Empfänger diesen in Erfahrung und kann so das damit verschlüsselte Dokument symmetrisch entschlüsseln.

Sicherheit durch Anpassung

Das BSI überprüft regelmäßig, ob die verwendeten kryptographischen Maßnahmen die gespeicherten Daten noch ausreichend vor dem Zugriff Unbefugter schützen. Im Bedarfsfall werden die Maßnahmen geändert. Nur Verfahren, die in der Technischen Richtlinie 03116-1 des BSI als sicherheitstechnisch geeignet bewertet werden, dürfen in der Telematikinfrastruktur verwendet werden.
Die TR-03116 wird mindestens einmal jährlich aktualisiert und dem Stand von Wissenschaft und Technik angepasst. Die Komponenten der TI passen sich diesen Veränderungen kontinuierlich an, so dass sichergestellt ist, dass stets die leistungsstärksten bzw. sichersten kryptographischen Verfahren zum Schutz von personenbezogenen medizinischen Daten verwendet werden. Das ist auch der Grund, weshalb die elektronische Gesundheitskarte, der Heilberufsausweis und die Institutionskarte (SMC-B) alle sechs Jahre ausgetauscht werden.