Sicherheitsbericht 2018

Lagebild zur Informationssicherheit in der Telematikinfrastruktur

gematik

Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

EINLEITUNG

Der Austausch von medizinischen Informationen erfordert eine sichere, vertrauenswürdige digitale Infrastruktur. Für den sicheren Betrieb dieser bundesweit verfügbaren, sektorenübergreifenden Telematikinfrastruktur (TI) legt die gematik verbindliche Methoden und Verfahren fest, lässt Komponenten und Dienste der TI zu und überwacht als übergeordnete koordinierende Instanz den laufenden Betrieb der Anbieter und Hersteller. Ziel ist es, das erforderliche Datenschutz- und Sicherheitsniveau der TI kontinuierlich aufrechtzuerhalten.

Der gesetzliche Auftrag der gematik ist im Sozialgesetzbuch Fünftes Buch (SGB V) festgeschrieben.

Um dieser Verantwortung gerecht zu werden, hat die gematik ein koordinierendes Informationssicherheitsmanagementsystem etabliert. Es dient dazu, den sicheren Betrieb in der TI mit all ihren Komponenten und Diensten der Anbieter und Hersteller zu überwachen.

Die Telematikinfrastruktur wird als Kritische Infrastruktur in Deutschland geführt. Damit gehört die gematik zur öffentlich-privaten Kooperation zwischen den Betreibern Kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen, dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und dem Bundesamt für Sicherheit in der Informationstechnik (UP KRITIS).

Ein Meilenstein im Jahr 2018 war die erfolgreiche Auditierung des koordinierenden Informationssicherheitsmanagementsystems der TI gemäß der Norm ISO/IEC 27001. Das Zertifikat bestätigt, dass die gematik ihren gesetzlichen Auftrag erfüllt.

Mit dem Lagebild zur Informationssicherheit der TI gibt die gematik erstmals übergreifend Auskunft über den Stand der betrieblichen Sicherheit in der TI. Das Lagebild stützt sich auf die Ergebnisse des koordinierenden Informationssicherheitsmanagementsystems und seiner Funktionsbereiche gematik Computer Emergency Response Team der TI (gematik CERT TI), Auditprogramm-Management der TI und Notfallmanagement der TI.

Der vorliegende erste Bericht bildet den Zeitraum vom 1. Januar bis zum 31. Dezember 2018 ab.

Inhalt

DAS KOORDINIERENDE ISMS DER TI

Das koordinierende Informationssicherheitsmanagementsystem (koordinierendes ISMS) ist die zentrale Organisationsstruktur, um alle betrieblichen Aspekte der Informationssicherheit der Telematikinfrastruktur (TI) zu steuern. Es nimmt die Informationen der Funktionsbereiche gematik Computer Emergency Response Team der TI (gematik CERT TI), Auditprogramm-Management der TI und Notfallmanagement der TI auf, führt diese zusammen und stellt sie gegenüber den relevanten Interessengruppen in Form von konsolidierten Sicherheitsberichten dar. Außerdem stellt das koordinierende ISMS der TI den Funktionsbereichen Instrumente wie das Risikomanagement und das zentrale Tracking von Sicherheitsmaßnahmen zur Verfügung.

Innerhalb eines Informationssicherheitsmanagementsystems werden Verfahren und Regeln für einen definierten Geltungsbereich (z. B. eine Organisation) etabliert, um die Informationssicherheit kontinuierlich zu überwachen, aufrechtzuerhalten und fortlaufend zu verbessern.

Vorbereitung der ISO/IEC-27001-Zertifizierung. Das Jahr 2018 stand ganz im Zeichen der Vorbereitung und Durchführung der ISO/IEC-27001-Zertifizierung. Die relevanten Dokumente und Prozesse der Informationssicherheit wurden kontinuierlich weiterentwickelt. Die Zertifizierung des koordinierenden ISMS der gematik nach dem internationalen Standard für Informationssicherheit ISO/IEC 27001:2013 erfolgte nach einem Audit im vierten Quartal 2018 durch die KPMG Cert GmbH.

Arbeitskreis Datenschutz und Informationssicherheit. Das koordinierende ISMS der TI organisiert zusammen mit dem koordinierenden Datenschutzmanagement der TI den Arbeitskreis Datenschutz und Informationssicherheit (AK DIS). Dieser Arbeitskreis trifft sich regelmäßig und tauscht sich mit Anbietern der TI über Datenschutz- und Informationssicherheitsaspekte aus. Die Abstimmung innerhalb des Arbeitskreises soll die Sicherheit des operativen Betriebs der TI unterstützen. Der AK DIS tagte im Jahr 2018 dreimal in den Geschäftsräumen der gematik.

DAS AUDITPROGRAMM-MANAGEMENT TI

Das Auditprogramm-Management für die Telematikinfrastruktur (TI) führt regelmäßig Audits bei Zulassungsnehmern durch, um zu prüfen, ob die Anforderungen hinsichtlich der Verfügbarkeit und Sicherheit der Betriebsleistung erfüllt werden.

Im Jahr 2018 wurden Audits bei den Betreibern der sogenannten Vertrauensanker der TI, den Anbietern von Institutionskarten bzw. elektronischen Praxisausweisen (SMC-B) und den Anbietern der zentralen Dienste durchgeführt.

Der Vertrauensanker, auch Root-CA oder Wurzel-Zertifikat, bildet die Basis der Public Key Infrastructure für die TI.

Es zeigte sich, dass die technischen und organisatorischen Maßnahmen der Betreiber und Anbieter ein angemessenes Schutzniveau gewährleisten und die spezifizierten Anforderungen der gematik eingehalten werden. Zudem wurden dezentrale Komponenten der TI einer zusätzlichen Sicherheitsanalyse unterzogen, um die Umsetzung des spezifizierten Sicherheitsniveaus zu verifizieren.

DAS GEMATIK CERT TI

Ziel des Computer Emergency Response Teams (CERT) der gematik zur Telematikinfrastruktur (TI) ist es, die operative Sicherheitslage der TI zu überwachen und, wenn erforderlich, Maßnahmen zur Wiederherstellung des notwendigen Sicherheitsniveaus zu koordinieren. Tritt ein Sicherheitsvorfall auf, übernimmt das gematik CERT TI die Koordination und Kommunikation zwischen den Anbietern der TI, dem Bundesamt für Sicherheit in der Informationstechnik und den Gesellschaftern der gematik.

Ein CERT ist ein Team von Sicherheitsexperten, die sich um die kontinuierliche Erkennung sowie die anschließende Analyse, Bewertung, Eskalation sowie Beseitigung von Schwachstellen und Sicherheitsvorfällen kümmern.

Regelmäßige Schwachstellenscans. Das gematik CERT TI überprüft in regelmäßigen Abständen mittels eines speziellen Scanners die Außenschnittstellen der TI (Schnittstellen, die vom Internet aus erreichbar sind) auf potenzielle Schwachstellen. Die Ergebnisse werden in Berichten zusammengefasst, durch das gematik CERT TI bewertet und dem jeweils verantwortlichen Anbieter zur Verfügung gestellt.

Es werden über 200 Schnittstellen mittels Schwachstellenscans regelmäßig überprüft. Hierbei wurden Schwachstellen in den folgenden Kategorien im Jahr 2018 erkannt:

- Konfigurationsfehler (z. B. offene nicht benötigte Ports)
- Zertifikatsfehler
- Veraltete Softwareversionen

Die ermittelten Schwachstellen wurden durch die Anbieter der TI in enger Abstimmung mit der gematik zeitnah behoben.

Schwachstellenmanagement. Aktuell bezieht das CERT TI der gematik Schwachstellenmeldungen aus verschiedenen Quellen; das sind rund 1200 Meldungen pro Monat. Diese werden hinsichtlich ihrer Relevanz für die Software, die in der TI eingesetzt wird, geprüft und bewertet.

Anbieter von TI-Produkten sind dazu verpflichtet, präventive Maßnahmen zu ergreifen, um technische Schwachstellen (Vulnerabilities) zu erkennen, zu analysieren und sodann geeignete Sicherheitsupdates durchzuführen. Dadurch sollen bekannte wie auch neue Bedrohungen möglichst frühzeitig beseitigt werden. Die Erkenntnisse des CERT dienen daher auch als Qualitätskontrolle.

Monitoring. Im Jahr 2018 wurden im gematik CERT TI erste Lösungen zur kontinuierlichen Sicherheitsüberwachung der TI entwickelt und in Betrieb genommen. Diese Tools verifizieren fortlaufend die Verfügbarkeit und Korrektheit von Zertifikatssperrlisten. Zusätzlich werden die Erreichbarkeit, die korrekte Konfiguration und die Gültigkeit der benötigten Schnittstellen der TI und der TI-nahen Dienste im Internet dargestellt.

Weiterhin nutzt das CERT der gematik frei verfügbare, offene Quellen (Open Source Intelligence), um Informationen bezüglich der TI auszuwerten. Beispielsweise werden regelmäßig externe und öffentlich erreichbare HTTPS-Schnittstellen der TI sowie Systeme, welche für den Betrieb der TI notwendig sind, hinsichtlich der verwendeten TLS-Zertifikate geprüft. Die kontinuierliche Beobachtung von (sozialen) Medien dient dazu, neue Bedrohungen und Schwachstellen sowie deren Ausnutzbarkeit (Exploits) schnell zu erkennen und, falls sie für die TI relevant sind, rasch zu reagieren.

Vernetzung. Um den Austausch und die Vernetzung mit anderen CERTs zu fördern, trat die gematik im vierten Quartal 2018 dem europäischen CERT-Verbund „Trusted Introducer“ bei. Im November 2018 nahm das CERT TI der gematik außerdem als Gast am Treffen des deutschen CERT-Verbunds teil und hatte die Gelegenheit, sich dort vorzustellen. Weiterhin fanden 2018 mehrere Treffen mit verschiedenen nationalen CERTs auf Arbeitsebene statt.

DAS NOTFALLMANAGEMENT TI

Aufgabe des Notfallmanagements der Telematikinfrastruktur (TI) ist es, die Eintrittswahrscheinlichkeit oder Schadensschwere von Notfällen im Kontext der TI zu verringern, indem es Risiken frühzeitig erkennt und bewertet sowie anbieterübergreifende notfallvorbeugende Maßnahmen etabliert. Tritt dennoch ein Notfall ein, sollen die zwischen den beteiligten Anbietern und der gematik abgestimmten Handlungen die Auswirkungen und Schäden minimieren.

Kommunikation. Die Krisenkommunikation der gematik unterstützt das Notfallmanagement TI bei Maßnahmen zur Vorsorge wie auch bei der Bewältigung und Nachbereitung von Notfällen. Aufgabe der Krisenkommunikation ist es, dabei zu unterstützen, dass relevante Informationen zum Ereignis für die Beteiligten und Betroffenen inhaltlich konsistent sind, dass die Beteiligten und Betroffenen wahrheitsgemäße Informationen über das Ereignis erhalten und dass die relevanten Informationen zum Ereignis selbst und zur Einordnung der Verantwortlichkeiten der Öffentlichkeit zugänglich gemacht werden. Auch die Krisenkommunikation erfolgt stets in enger Abstimmung mit den Gesellschaftern der gematik und dem Bundesministerium für Gesundheit.

Notfallübungen. Im Jahr 2018 wurden verschiedene Notfallübungen, teils mit Beteiligung von Anbietern der TI, durchgeführt. Für die Übungen wurden entsprechende Drehbücher erstellt und im Anschluss ebenso Verbesserungspotenziale abgeleitet.

Folgende Ziele wurden durch die Notfallübungen im Jahr 2018 erreicht:

- Überprüfung von Alarmierungsketten
- Zusammenarbeit der verschiedenen Akteure im Notfall
- Verifikation von Wiederherstellungsplänen, Checklisten und Merkblättern
- Prüfung der Nutzbarkeit technischer Hilfsmittel

Begleitung von Störungen. Im ersten und zweiten Quartal 2018 kam es kurzzeitig zu größeren Einschränkungen der TI-Verfügbarkeit.

In beiden Fällen unterstützte das Notfallmanagement durch vorbereitete Eskalationsprozeduren und Pläne die schnelle anbieterübergreifende Ursachenanalyse sowie die Wiederherstellung der Verfügbarkeit. Dies umfasste sowohl die Moderation und Unterstützung der Anbieter bei der Ursachenanalyse als auch die Auf- und Nachbereitung der Ereignisse. Die Sicherheit der TI war zu keiner Zeit gefährdet.

Versichertenstammdaten-Management: Grundsätzlich sind auch bei einer Störung der Online-Anbindung an die TI das Einlesen der elektronischen Gesundheitskarte und die Übertragung in das Primärsystem möglich (gültiger Prüfnachweis für die Abrechnung des Leistungserbringers).

AUSBLICK

Im Jahr 2019 soll der Rollout der TI abgeschlossen werden und die ersten medizinischen Anwendungen im Feld stattfinden. Das bedeutet eine große Herausforderung für die betriebliche Sicherheit in der TI.

Gleichzeitig bleibt die Gefährdungslage durch zunehmend professionell agierende Angreifer unverändert hoch. Daher wird die gematik die bereits etablierten Prozesse dazu nutzen, das Sicherheitsniveau aufrechtzuerhalten bzw. weiter zu verbessern.

Im koordinierenden ISMS wird der Fokus darauf liegen, die Abweichungen, die sich aus dem ISO/IEC-27001-Zertifizierungsaudit ergeben haben, zu beseitigen und die übergreifende Dokumentationsqualität zu verbessern.

Im Bereich des Auditprogramms werden 2019 mehr Audits und Sicherheitsanalysen stattfinden, da die Zahl der zugelassenen Anbieter und Hersteller der TI gestiegen ist.

Im Notfallmanagement sollen vermehrt übergreifende Übungen mit TI-Anbietern durchgeführt werden, um im Ernstfall eine bestmögliche anbieterübergreifende Zusammenarbeit zu gewährleisten.

Das gematik CERT TI wird 2019 die Schwachstellenanalyse auf weitere Anbieter und Schnittstellen ausweiten und das Security Monitoring ausbauen. Ziel ist es, das operative Sicherheitsniveau noch effizienter kontinuierlich zu überwachen.

ABKÜRZUNGSVERZEICHNIS

AK DIS	Arbeitskreis Datenschutz und Informationssicherheit
CERT	Computer Emergency Response Team
ISMS	Informationssicherheitsmanagementsystem
ISO/IEC 27001	internationaler Standard für Informationssicherheit (ISO/IEC 27001:2013)
SMC-B	Security Module Card Typ B (Institutionskarte, Praxisausweis)
TI	Telematikinfrastruktur
TLS	Transport Layer Security
UP KRITIS	öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen

IMPRESSUM

gematik – Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH
Friedrichstraße 136
10117 Berlin

Tel.: +49 30 400 41-0
Fax: +49 30 400 41-111

info@gematik.de
www.gematik.de

Geschäftsführer: Alexander Beyer

Stand: Januar 2019

Bildnachweis: Titel: © iStock/malerapaso

Hinweis zum Text: Zugunsten des Leseflusses wird in dieser Publikation meist die männliche Form verwendet. Wir bitten, dies nicht als Zeichen einer geschlechtsspezifischen Wertung zu deuten.

Disclaimer

Alle im Bericht enthaltenen Angaben und Informationen wurden von der gematik – Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH sorgfältig recherchiert und geprüft. Trotz aller Sorgfalt können Fehler nicht vollständig ausgeschlossen werden und sich insbesondere Sachverhalte zwischen Erstellung und Veröffentlichung verändert haben. Eine Garantie oder Haftung für Richtigkeit, Vollständigkeit und Aktualität der Inhalte dieses Berichts kann daher nicht übernommen werden. Die gematik – Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH haftet nicht für direkte oder indirekte Schäden, einschließlich entgangenen Gewinns, die aufgrund von oder in Verbindung mit Informationen entstehen, die in diesem Bericht enthalten sind.

Geschützte Namen oder eingetragene Marken unterliegen uneingeschränkt den Bestimmungen des Kennzeichenrechts und sind Eigentum der jeweiligen juristischen oder natürlichen Personen, auch dann, wenn hierauf nicht gesondert hingewiesen wird.