Gesundheitsdaten schützen

Das deutsche Bundesamt für die Sicherheit in der Informationstechnik hat im Hinblick auf die besondere Stellung von Gesundheitsdaten einen technischen Standard veröffentlicht, der sich mit der Sicherheit für digitale Gesundheitsanwendungen beschäftigt.

Während laufend über Datenlecks und Protokolle von privaten Telefon-Chats in den Medien berichtet wird, steigt die Sensibilität in der Bevölkerung, mobile Geräte besser abzusichern. Gleichzeitig nehmen Zahl und Form von Cyber-Angriffen auf Smartphones zu. Um solchen Situationen vorzubeugen, ist es wichtig, sich Gedanken über die Applikationen zu machen, die auf diesen Geräten installiert sind, und auch über die Daten, die man dort abspeichert. Fragestellungen rund um die Datenhaltung sollte jeder Anwender für sich selbst beantworten und gerade vor dem Hintergrund von Smartphonediebstählen sehen: Einerseits sind dann diese Daten nicht mehr im Zugriff des Benutzers – und falls er sie nur dort gespeichert hat, möglicherweise unwiederbringlich verloren. Andererseits ergibt sich für die Diebe die Möglichkeit, mit dem physischen Gerät Abfragen im Namen des Benutzers vor-

Arne Schönbohm: „Die Veröffentlichung sensibler Gesundheitsdaten lässt sich nicht ungeschehen machen."

zunehmen oder den Speicher der Geräte auszulesen. Die offene Architektur vieler mobiler Plattformen begünstigt auch den Einsatz von Schadsoftware (z. B. Trojaner), über die Login-Informationen ausgespäht werden können, um so an sensible Daten zu kommen.

Der Verlust sensibler Daten ist schon im Fall von Bankdaten sehr unangenehm, da hier Transaktionen zum Nachteil der Eigentümer der Geräte durchgeführt werden können. Noch problematischer ist der Abfluss von Gesundheitsdaten, da diese Informationen über Menschen enthalten können, die für sie sehr wesentlich und nicht für die Öffentlichkeit bestimmt sind.

Beispielsweise könnte es um Depressionen, Abtreibungen oder sexuell übertragbare Krankheiten gehen – alles in allem um Daten, deren Inhalte nach einer Veröffentlichung nicht mehr aus der Welt geschafft werden kann, und die ein ganzes Leben eines Menschen dann unheilvoll begleiten können.

Technische Richtlinie. Das *Bundesamt für die Sicherheit in der Informationstechnik (BSI, www.bsi.bund.de)* hat im Hinblick auf die besondere Stellung von Gesundheitsdaten vergangenes Jahr einen technischen Standard veröffentlicht, der sich mit der Sicherheit für di-

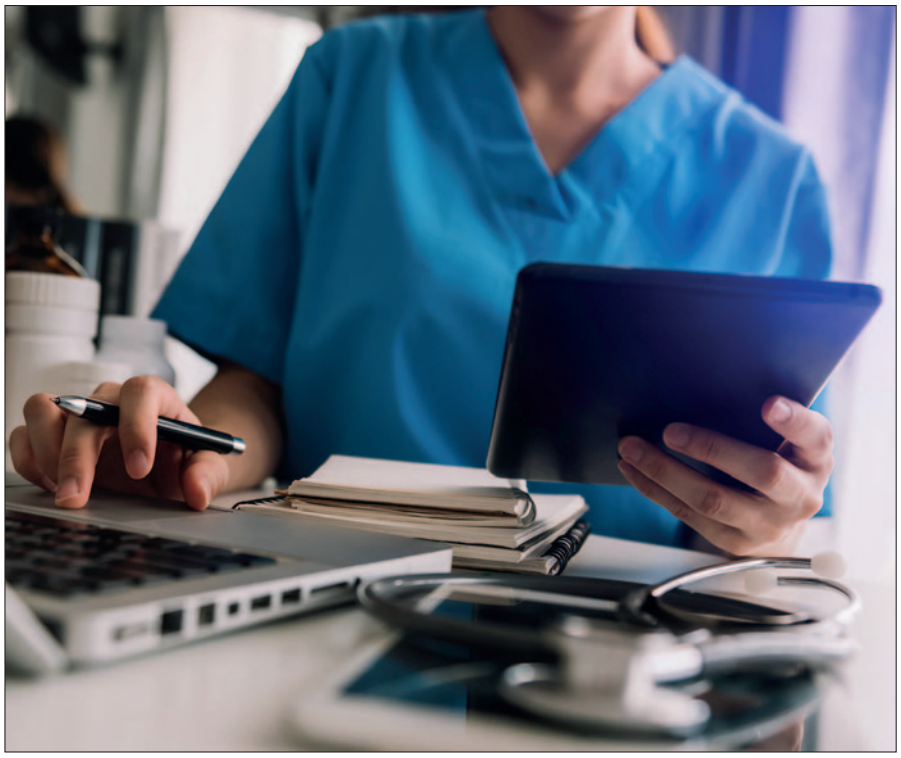
TECHNISCHE RICHTLINIE

Prüfkriterien

In der Richtlinie geht es um Aspekte der Vertraulichkeit, Integrität und Verfügbarkeit von mobilen Gesundheitsanwendungen. Dazu werden Prüfkriterien vorgeschlagen, nach denen die Entwickler und Hersteller schon vor der Inbetriebnahme in Form einer Checkliste die wichtigsten Fragestellungen abarbeiten können – hier einige der Fragen:

- Was ist der Zweck der Anwendung und wie werden dafür personenbezogene Daten verarbeitet?
- Wird der Benutzer über diese Datenverarbeitung detailliert zumindest bei der erstmaligen Inbetriebnahme informiert?
- Kommt es über den primären Zweck der Anwendung hinaus zu einer weiteren Verarbeitung von sensiblen Daten?
- Wie wird der Benutzer darauf hingewiesen, wenn neue personenbezogene Daten erfasst oder verarbeitet werden?
- Wie wird sichergestellt, dass bei Nichtzustimmung des Benutzers keine Datenerfassung oder Datenverarbeitung erfolgt?
- Was passiert, wenn der Benutzer seine Einwilligung zur Datenverarbeitung zurückzieht?
- Wie werden die Daten am Endgerät und am Server sicher gelöscht?
- Gibt es Funktionalitäten für die Teilung von Daten mit Dritten und wie wird der Benutzer hier einbezogen, um seine ausdrückliche Zustimmung zu geben (Opt-in-Verfahren)?
- Wurde der gesamte Datenlebenszyklus (Erhebung, Verarbeitung, Speicherung, Löschung) von sensiblen Daten bei der Entwicklung und im Betrieb abgebildet?
- Für welche Plattformen wurde die Anwendung entwickelt und wie wurden die jeweils immanenten Sicherheitsfragestellungen behandelt?
- Wurde die Anwendung als Webservice gestaltet oder ist sie als native Anwendung für *iOS* oder *Android*-Geräte verfügbar?
- Welche Bibliotheken oder Anwendungs-Frameworks von Drittherstellern werden genutzt und wie ist sichergestellt, dass diese nur den primären Anwendungsfall unterstützen und darüber hinaus keine personenbezogenen Daten verwenden?
- Welche Form der sicheren Anmeldung wurde für die Anwendung gewählt, so dass ein Authentizitäts- und Integritätsschutz besteht?
- Welche Verbindungen gibt es zwischen der Anwendung und Serversystemen, auf denen Transaktionen ausgeführt oder Daten gelesen oder gespeichert werden?
- Wie verbindet sich die Anwendung mit Serversystemen und welche Sicherheitsvorkehrungen sind eingebaut (z. B. verschlüsselter Verbindungsaufbau)?
- Sind die verwendeten kryptographischen Verfahren ausreichend und ist sichergestellt, dass für Backups der Endgeräte keine unverschlüsselten sensiblen Daten oder kryptographisches Schlüsselmaterial zur Verfügung stehen?

Foto: Kurt Hickisch



Die „Technische Richtlinie“ des BSI enthält Prüfkriterien für die IT-Sicherheit von mobilen digitalen Gesundheitsanwendungen.

gitale Gesundheitsanwendungen beschäftigt. BSI-Präsident Arne Schönbohm schrieb dazu im April 2020: „Sensible Gesundheitsdaten verdienen einen besonderen Schutz. Sowohl das Smartphone der Nutzerinnen und Nutzer als auch die Hintergrundanwendungen aufseiten der Anbieter müssen daher ein Mindestmaß an Sicherheit vorweisen können. Denn die Veröffentlichung sensibler Daten wie Pulsfrequenz, Schlafrhythmus oder Medikationspläne, lässt sich nicht ungeschehen machen. Hier kann nicht, wie im Falle eines Missbrauchs beim Online-Banking, der Fehlbetrag zurückgebucht werden.

Leitfaden. Mit der Technischen Richtlinie stellt das *BSI* als die Cyber-Sicherheitsbehörde des Bundes einen wichtigen Leitfaden zur Verfügung, damit die Anwendungen das erforderliche IT-Sicherheitsniveau erreichen können.“ In die Ausarbeitung der Richtlinie des *BSI* ist viel Know-how aus dem Bereich der Bekämpfung von Computerkriminalität und Softwareentwicklung eingeflossen. Jeder Hersteller oder Betreiber von mobilen Gesundheitsanwendungen, der sensible personenbezogene Daten erfasst oder bearbeitet (z. B. in Apps in Zusammenhang mit der Corona-Pandemiebekämpfung, mobile Impfpässe, mobile Gesundheitsakte) sollte diese laufend beachten und regelmäßig durch externe Spezialisten überprüfen lassen.

Dabei geht es nicht um ganz neue Themen, sondern um grundlegende Fragen der Computersicherheit. Gemeint sind damit Funktionalitäten wie die Zwei-Faktor-Authentifizierung, verschlüsselte Übertragung und sichere Löschung von Daten, die eigentlich in jeder modernen IT-Anwendung beachtet und vorgesehen werden sollten.

Nur mit der Fokussierung auf maximalen Datenschutz und maximale Sicherheit kann verhindert werden, dass Menschen, die Opfer von Computerkriminalität werden, nicht ihr ganzes Leben lang unter den Folgen der Veröffentlichung von persönlichen Gesundheitsdaten zu leiden haben. Das wäre eine Schattenseite der Digitalisierung.

Cornelius Granig

Der Autor ist ein österreichischer Unternehmensberater und Buchautor. Er leitet bei der internationalen Beratungsfirma Grant Thornton die Bereiche Cyber Security, Compliance und Krisenmanagement.

Risikobewertung von Wanderwegen

In den Bergen bleibt oft kein Stein auf dem anderen. Gründe sind die Klimaerwärmung, die zum Abtauen der Gletscher und Lockerung des Gerölls führen oder heftige Regenfälle. Immer öfter werden Bergwege für Wanderer aufgrund erhöhter Steinschlaggefahr gesperrt.

Wegehalter haften für die Sicherheit ihres Weges. Das ist im ABGB (Allgemeines Bürgerliches Gesetzbuch) in § 1319a geregelt. Verunglückt ein Wanderer aufgrund eines Steinschlags, kann er den Wegehalter klagen. Haftung droht einem Wegehalter in Österreich nur bei grober Fahrlässigkeit oder Vorsatz. Um das Risiko von Naturgefahren auf Wanderwegen besser einzuschätzen, entwickelte eine Expertengruppe aus Vertretern des Landes Tirol, des *Österreichischen Alpenvereins* und des *Kuratoriums für Alpine Sicherheit* einen Risikorechner: das Analyse-Tool R.A.G.N.A.R. (Risiko Analyse Gravitativer Naturgefahren im Alpinen Raum).

Das Tool ermöglicht Wegehaltern, das Todesfallrisiko auf einem bestimmten Wanderweg einzuschätzen. In die Risikobewertung fließen unter anderem die Häufigkeit und Schwere von Naturgefahren, die Personenfrequenz und die Expositionszeit ein. Ist das Risiko durch Naturgefahren zu hoch, muss der Weg gesperrt werden.

Der RAGNAR-Online-Rechner ist nicht nur für Wegehalter nützlich, er bietet Wanderern und Bergsteigern die Möglichkeit, sich mit den Anforderungen der verschiedenen Wegekategorien und der damit verbundenen Eigenverantwortung auf interaktive Weise auseinanderzusetzen.

Der Online-Rechner wird von lokalen Expertinnen und Experten und einem Sachverständigen angewandt; er ist auf der Homepage des Landes Tirol verfügbar *(www.bergwelt-miteinander.at/ragnar)*

RAGNAR soll nicht nur in Tirol und Österreich verwendet werden, sondern ist auch als künftiges Euregio-Projekt gemeinsam mit Südtirol und dem Trentino geplant.

FOTO: MRMOHOCK/STOCK.ADOBE.COM