AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

Ausgabe Juni 2016 | Seite 1

www.aok-verlag.info/ds-im-blick

INHALT

Windows 10: Wenn Datenschutz zur Einstellungsfrage wird

Das aktuellste Microsoft-Betriebssystem enthält bei der Erstinstallation zahlreiche datenschutzkritische Voreinstellungen. Ein Umstieg muss daher gut geplant werden.

Sven Venzke-Caprarese, Dr. Sebastian Ertel

Viele Gesundheitseinrichtungen werden sich derzeit mit der Frage beschäftigen, welches Betriebssystem sie in Zukunft einsetzen werden und wann der richtige Zeitpunkt für einen Umstieg ist. Insbesondere Einrichtungen, die bisher auf Windows 7 oder Windows 8.1 setzten, werden von Microsoft mit einer kostenlosen Upgrade-Möglichkeit auf Windows 10 zum Betriebssystemwechsel motiviert. Allzu viel Zeit lässt Microsoft allerdings nicht: Bis zum 29. Juli 2016 ist das kostenlose Upgrade möglich. Sofern diese Frist durch Microsoft nicht verlängert wird, ist jeder spätere Umstieg kostenpflichtig. Wir geben einen Überblick, für wen ein Wechsel sinnvoll sein kann und was dabei zu beachten ist.

Wechseln oder nicht?

Die Frage, ob und ggf. wann ein Betriebssystemwechsel sinnvoll ist, kann nicht allgemeingültig beantwortet werden. Grundsätzlich gilt, dass ein Betriebssystemwechsel unbedingt erfolgen sollte, sobald vom Hersteller keine Sicherheitsupdates mehr bereitgestellt werden. Dies ist z. B. für Windows XP und alle vorherigen Microsoft-Betriebssysteme der Fall. Hier ist ein Wechsel unbedingt angezeigt.

Doch auch wenn das von der Gesundheitseinrichtung verwendete Betriebssystem noch alle Sicherheitsupdates erhält, stellen sich weitere Fragen. So muss beachtet werden, wann die Sicherheitsupdates künftig eingestellt werden. Die Sicherheitsupdates für Windows Vista enden z. B. in einem knappen Jahr. Eine Wechselstrategie sollte daher bereits jetzt geplant werden. Für Be-

triebssysteme nach Windows Vista besteht im Hinblick auf den Ablauf der Sicherheitsupdates zwar noch Zeit. Ein Sonderfall ist hier jedoch Windows 7. Dieses Betriebssystem erhält zwar noch alle Sicherheitsupdates. Der sog. grundlegende bzw. Mainstreamsupport ist allerdings bereits Anfang 2015 abgelaufen. Konkret bedeutet dies, dass Windows 7 keine neuen Funktionen mehr erhalten wird und auch grundsätzlich keine Fehler mehr behoben werden.

Weile den vollen Support. Allerdings wurde in der Vergangenheit insbesondere die Bedienbarkeit des Betriebssystems kritisiert. Hier wartet Windows 10 in der Praxis mit deutlichen Verbesserungen auf.

Privacy by Default? Fehlanzeige!

Gesundheitseinrichtungen, die auf das aktuellste Microsoft-Betriebssystem setzen wollen, werden schnell feststellen, dass dieses nicht

Ab diesem Zeitpunkt gibt es für Windows keine Sicherheitsupdates mehr:

Windows XP	Seit dem 8. April 2014 werden keine Sicherheitsupdates mehr bereitgestellt. Ein Betriebssystemwechsel sollte daher bereits durchgeführt worden sein bzw. ist dringend zu empfehlen. Das Betriebssystem ist unsicher.
Windows Vista (Service Pack 2)	Windows Vista erhält keinen grundlegenden Support mehr und läuft aus. Sicherheitsupdates gibt es nur noch bis zum 11. April 2017.
Windows 7 (Service Pack 1)	Auch Windows 7 erhält keinen grundlegenden Support mehr. Sicherheitsupdates werden aber noch bis zum 14. Januar 2020 unterstützt.
Windows 8.1	Windows 8.1 erhält bis zum 9. Januar 2018 weiterhin den vollen Support. Sicherheitsupdates enden erst im Jahr 2023.
Windows 10	Windows 10 ist das aktuellste Microsoft-Betriebssystem und erhält bis ins Jahr 2020 ebenfalls den vollen Support. Sicherheitsupdates enden frühestens im Jahr 2025.

Das Betriebssystem ist im Begriff auszulaufen. Dies kann aus rein praktischen Gründen ebenfalls ein Grund zum Wechseln sein – insbesondere wenn der Wechsel auf das aktuellste Betriebssystem kostenlos ist. Schließlich spielen auch der Funktionsumfang, die Bedienbarkeit und die Kompatibilität mit vorhandenen Lösungen eine Rolle bei der Frage des Betriebssystemwechsels. Wer zum Beispiel Windows 8.1 einsetzt, erhält zwar noch eine ganze

nur Vorteile mit sich bringt. Zwar ist die Bedienbarkeit deutlich besser als bei Windows 8.1 und das Betriebssystem erhält noch über Jahre den vollen Support. Das Betriebssystem enthält aber zahlreiche Voreinstellungen, die eine ganze Menge Daten des Nutzers an Microsoft preisgeben.
Administratoren von Gesundheitseinrichtungen sind an dieser Stelle gefragt, die richtigen Einstellungen zu finden und diese über die gesamte Gesundheitseinrichtung anzuwenden. Hierbei ist es sinnvoll, die Einstellungen nicht manuell von Hand für jede Installation zu setzen, sondern diese über sog. Gruppenrichtlinien über alle Clients zu verteilen.

Datenschutz-Einstellungen anpassen

Anpassungsbedarf findet sich bereits in den Datenschutzeinstellungen von Windows 10. Zu finden sind diese im Startmenü unter „Einstellungen“, „Datenschutz“, „Allgemein“.
Hier sollte die sog. Werbungs-ID des Betriebssystems ausgeschaltet werden. Denn diese verfolgt lediglich den Zweck, den Nutzer wiederzuerkennen und anhand von vorherigen Aktivitäten, Suchvorgängen und Websitebesuchen mit personalisierter Werbung zu bespielen.
Darüber hinaus sollte eingestellt werden, dass keine Informationen zum Schreibverhalten an Microsoft gesendet werden. Denn ein Blick in die Microsoft-Datenschutzerklärung zeigt, dass sogar die über die Tastatur eingegebenen Wörter erfasst und an Microsoft gesendet werden können. Für Mitarbeiter in Gesundheitseinrichtungen kann dies einen Bruch der ärztlichen Schweigepflicht bedeuten.
Auch der Zugriff auf die Sprachliste sollte vor diesem Hintergrund deaktiviert werden.

Microsoft lässt Administratoren nicht ganz allein

Auch wenn die medienübergreifende Kritik an den Datenschutzvoreinstellungen von Windows 10 mehr als berechtigt ist, muss an dieser Stelle ehrlicherweise auch darauf

hingewiesen werden, dass Microsoft durchaus gute Hilfestellungen für Administratoren bietet. Unter diesem Link erläutert Microsoft nämlich detailliert, wie Administratoren die datenschutzkritischen „Telemetriedaten“ mit Wirkung für die gesamte Einrichtung in den Griff bekommen. Hierbei werden nicht nur die Einstellungen in der normalen Benutzeroberfläche angesprochen, sondern auch Möglichkeiten aufgezeigt, die Einstellungen einrichtungsweit mittels Gruppenrichtlinie oder Eintrag in der Registry vorzunehmen. Datenschutzbeauftragte, die den Einsatz von Windows 10 in der Gesundheitseinrichtung begleiten, sollten dieses Microsoft-Dokument Punkt für Punkt mit den zuständigen Administratoren bzw. Entscheidungsträgern durchgehen und die notwendigen Einstellungen abstimmen. Dabei zeigt sich dann auch schnell, wie sehr Gesundheitseinrichtungen aufpassen müssen, keine Einstellung zu vergessen.

Positionsdaten

Windows 10 ist sowohl für den Betrieb auf stationären als auch auf mobilen Geräten ausgelegt und verfügt daher über Funktionen zur Positionserkennung. Diese Funktion kann insbesondere für stationäre Geräte deaktiviert werden. Aber auch für mobile Geräte sollte die Deaktivierung in Betracht gezogen werden. Eine Speicherung des Positionsverlaufs kann im Extremfall nämlich mit der ärztlichen Schweigepflicht kollidieren.

Cortana

Windows 10 enthält ein relativ mächtiges Sprachassistenzsystem. Dieses überträgt jedoch die zur Spracherkennung erforderlichen Sprachdaten direkt an Microsoft. Zudem werden auch Kontakt- und Kalenderdaten übertragen. Insbesondere für Gesundheitseinrichtungen ist das Sprachassistenzsystem daher vor dem Hintergrund der ärztlichen Schweigepflicht grundsätzlich nicht nutzbar und sollte deaktiviert werden.

Kontoinformationen

Unter „Einstellungen“, „Datenschutz“, „Kontoinformationen“ kann der Nutzer bestimmten Apps einen Zugriff auf seine Kontoinformationen gewähren. Auch diese Einstellung sollte grundsätzlich deaktiviert werden.

Kontakte und Kalender, Anrufliste, E-Mail, Messaging

Gleiches gilt insgesamt für den Zugriff auf Kontakt- und Kalenderdaten, Anruflisten, E-Mails und Messagingdaten. Dieser Zugriff kann ebenfalls über die Datenschutzeinstellungen beeinflusst werden. Gesundheitseinrichtungen müssen an dieser Stelle unbedingt vermeiden, dass Daten, die beruflichen

Schweigepflichten unterliegen, versehentlich an unbefugte Dritte oder Cloud-Betreiber weitergebeben werden. Auch hier sollten daher möglichst restriktive Einstellungen getroffen und der Zugriff unterbunden werden.

Diagnosedaten

In der Standardeinstellung sendet Windows 10 eine Reihe von Diagnose- und Feedbackdaten an Microsoft. Diese sollten ebenfalls auf ein Minimum beschränkt werden.

Kontensynchronisation

Windows 10 enthält die Möglichkeit einer sogenannten Kontensynchronisation. Diese sollte jedoch grundsätzlich nicht genutzt werden, da u. a. auch Benutzerkennwörter von der Synchronisierung betroffen sind. Eine entsprechende Gruppenrichtlinie schafft hier Abhilfe.

WLAN-Optimierung

Windows 10 bietet Nutzern die Möglichkeit der „WLAN-Optimierung“. Hierzu gehört auch, dass Nutzer ihre WLAN-Zugangsdaten relativ einfach mit vorhandenen Kontakten oder sogar Facebook-„Freunden“ teilen können. Diese Möglichkeit findet sich etwas versteckt unter „Einstellungen“, „Netzwerk und Internet“, „WLAN“. Nutzer von Windows 10 können an dieser Stelle Windows 10 auch mit ihrem Facebook-Konto verbinden. Diese Möglichkeit sollte von den Administratoren der Gesundheitseinrichtung unterbunden werden. Ansonsten befinden sich schlimmstenfalls eine ganze Reihe unbekannter Nutzer im nichtöffentlichen Krankenhaus-WLAN.

Edge

Windows 10 enthält mit Microsoft Edge einen neuen Webbrowser, der den Internet Explorer ablösen soll. Über Gruppenrichtlinien können eine ganze Reihe sinnvoller Einstellungen vorgenommen werden.

So können z. B. die Funktionen zum automatischen Ausfüllen von Formularen und zur automatischen Kennwortspeicherung des Browsers deaktiviert werden. Eine genauere Analyse der möglichen Gruppenrichtlinien zeigt an dieser Stelle aber auch, wie bewusst Microsoft gegen das Prinzip „Privacy by Default“ verstößt. So enthält die entsprechende Gruppenrichtlinie die Möglichkeit festzulegen, ob Mitarbeiter „Do Not Track“-Header senden können. Hierbei handelt es sich um eine Möglichkeit, mit der sich Mitarbeiter vor Webtracking schützen könnten. In der Standardeinstellung verwehrt Microsoft den Mitarbeitern jedoch, diese Header überhaupt senden zu können. Die Möglichkeit sollte daher aktiviert werden.

Windows-Spotlight

Windows-Spotlight stellt nach Aussage von Microsoft verschiedene Hintergrundbilder und Texte auf dem Sperrbildschirm bereit. Was zunächst harmlos klingt, scheint jedoch von Microsoft auch als Möglichkeit genutzt zu werden, um personalisierte Werbung auf Sperrbildschirmen unterzubringen. Unsere Empfehlung: Deaktivieren.

Windows Store

Windows 10 verfügt über einen eigenen App-Store. Nutzer können hier Apps herunterladen und installieren. Um sicherzustellen, dass nur zugelassene Apps installiert sind, kann es durchaus sinnvoll sein, den Zugriff auf den Windows Store für Mitarbeiter über eine Gruppenrichtlinie zu deaktivieren. Die Möglichkeit, eine Black- oder Whitelist für bestimmte Apps zu hinterlegen, scheint jedoch nicht ohne weiteres gegeben zu sein.
Bessere Einstellungsmöglichkeiten bietet Microsoft über den sog. „Windows Store für Unternehmen“. Dieser setzt jedoch voraus, dass für alle Mitarbeiter ein Microsoft Azure Active Directory Konto angelegt wird. Die Mitarbeiterdaten landen somit in der Cloud.

Cloud Dienste

Insgesamt setzt Windows 10 an vielen Stellen auf eine Verknüpfung mit den Microsoft Cloud Diensten – insbesondere zum Microsoft Cloudspeicherdienst OneDrive. Diese Verknüpfung kann allerdings ebenfalls über entsprechende Gruppenrichtlinien deaktiviert werden.

Fazit

Kaum ein Betriebssystem von Microsoft verstieß bisher so konsequent gegen das Prinzip „Privacy by Default“ wie Windows 10. Zwar stellt Microsoft eine relativ gute Dokumentation für die datenschutzkonformen Nachjustierung zur Verfügung. Insbesondere im Bereich des Windows Stores zeichnen sich jedoch fehlende Einstellungsmöglichkeiten ab, sofern man nicht bereit ist, in die Microsoft Cloud zu wechseln. Zudem verbleibt am Ende das ungute Gefühl, doch noch eine Feinheit in den Einstellungsmöglichkeiten übersehen zu haben.

Mit dem Newsletter „Datenschutz im Blick“ greifen unsere Autoren Themen auf, die Sie über rechtliche und technische Fragen zu Datenschutz und Datensicherheit im Gesundheitswesen informieren. Dieser Service ist und bleibt für Sie kostenlos! Unsere Redaktion freut sich über jeden neuen Leser, denn damit zeigen Sie, dass dieses Angebot auf Interesse stößt. Deshalb eine Bitte:
Empfehlen Sie uns weiter!

Feedback, Anregungen oder auch **Fragen** können Sie gerne per Mail an **fachinfo@aok-verlag.de** übersenden.

Instant-Messenger im Gesundheitswesen

Der Messenger-Dienst WhatsApp machte in den vergangenen Monaten durch die Einführung einer Ende-zu-Ende-Verschlüsselung von sich reden. Durch diese soll die Kommunikation ausschließlich von den Gesprächspartnern, nicht aber von unbeteiligten Dritten und auch nicht von WhatsApp selbst gelesen werden können. Wird der Dienst dadurch auch im Gesundheitsbereich einsetzbar?

Dr. Sebastian Ertel, Sven Venzke-Caprarese

Messenger-Dienste?

Messenger-Dienste (auch Instant-Messenger) zeichnen sich dadurch aus, dass Nachrichten zwischen den Gesprächspartnern nicht über eine Telefon-, sondern eine kostengünstige Internetverbindung ausgetauscht werden.
Das Absenden einer Nachricht führt bei bestehender Internetverbindung zum unmittelbaren Empfang beim Empfänger. Ist eine Internetverbindung nicht verfügbar, erfolgt die Zustellung unmittelbar nach Aufbau einer solchen.
Die Kommunikation erfolgt fast ausschließlich über eine App, die auf den Smartphones der Teilnehmer installiert ist und die Daten über die Server des Diensteanbieters zwischen den Gesprächsteilnehmern austauscht.

Auslesen des Telefonbuches

Die Identifizierung der Nutzer erfolgt in der Regel über die Mobilfunknummer des Telefons.
Nach Freigabe des Telefonbuches werden sämtliche dort hinterlegten Mobilfunknummern auf den Server des Betreibers übertragen. Bei WhatsApp bedeutet das eine Speicherung in den USA. Unklar ist, ob dabei lediglich Mobilfunknummern oder das gesamte Telefonbuch (inklusive Namen, E-Mail-Adressen, Anschriften, Geburtstage) ausgelesen wird. Eine sich anbahnende Kommunikation kann dadurch aufgebaut und den Teilnehmern zugeordnet werden.
Laut der FAQ von WhatsApp ist auch eine Nutzung des Messenger-Dienstes möglich, wenn der Zugriff auf das Telefonbuch nicht freigegeben wurde. Diese ist allerdings stark eingeschränkt:

- Nachrichten von anderen WhatsApp Benutzern und Gruppen können empfangen und
- WhatsApp-Einstellungen geändert werden.

Nicht möglich ist hingegen:

- Kontaktnamen sehen,
- einen neuen (Gruppen-) Chat oder eine Broadcast-Liste beginnen,
- die Favoriten sehen.

Die Funktionalität bei fehlendem Zugriff auf das Telefonbuch ist daher so eingeschränkt, dass eine effektive Nutzung kaum möglich ist.
Im Gegensatz dazu ist eine Verwendung des Messenger-Dienstes Threema auch ohne Telefonbuchfreigabe möglich. In diesem Fall muss der Nutzer die Kontakte manuell durch Eingabe der ID oder Scan des QR-Codes hinzufügen.

Ende-zu-Ende-Verschlüsselung

Bei der Ende-zu-Ende-Verschlüsselung (E2E) werden die Kommunikationsinhalte auf Senderseite ver- und erst beim Empfänger wieder entschlüsselt. Nicht verschlüsselt werden hingegen die Metadaten. Die Verschlüsselung basiert auf einem asymmetrischen Kryptosystem. Hierbei wird – vereinfacht dargestellt – per Zufallsprinzip ein Schlüsselpaar, bestehend aus einem öffentlichen und einem privaten Schlüssel, erzeugt. Der private Schlüssel ist streng geheim zu halten und darf nicht weitergegeben werden. Im Gegensatz dazu muss der öffentliche Schlüssel (der eigentlich ein „offenes Schloss“ darstellt) bekanntgegeben werden, da dieser für die Verschlüsselung der Nachricht benötigt wird. Will der Versender eine Nachricht verschlüsseln, nimmt er sich das öffentlich verfügbare Schloss des Nachrichtenempfängers, verschließt damit die Nachricht und versendet diese anschließend. Der Empfänger kann als einziger mit seinem geheimen privaten Schlüssel das Schloss öffnen, also entschlüsseln, und die Nachricht lesen.

Kommunikationsinhalte „Metadaten“

Zu den Kommunikationsinhalten gehören sämtliche Informationen, die mittels einer Nachricht ausgetauscht werden können:

- Texte
- Bild- und Tondateien
- Dokumente

Ein Zugriff auf diese Daten ist bis auf den Inhaber des privaten Schlüssels jedem verwehrt. Auch dem Anbieter des Messenger-Dienstes ist ein Zugriff nicht möglich.

Nicht verschlüsselt werden hingegen die sogenannten Metadaten, also die Begleitdaten der Kommunikation:

- Kommunikationsteilnehmer
- Zeitpunkt der Kommunikation (Datum und Uhrzeit)
- Umfang der Kommunikation (wie oft und mit welchem Datenvolumen).

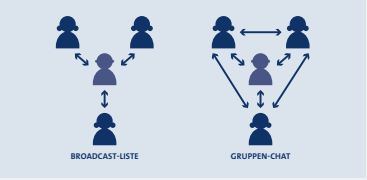
Was genau mit diesen Daten beim Anbieter des Messenger-Dienstes passiert, ist unklar. Denkbar wäre sowohl eine unverzügliche Löschung als auch eine langfristige Speicherung. Gespeicherte Daten wecken irgendwann immer den Wunsch nach einer späteren Auswertung.

Von der Problematik der Metadaten abgesehen, sind die Daten einer Kommunikation durch WhatsApp technisch gut abgesichert.

Und der Datenschutz?

Eine Kommunikation mit Patienten über einen Messenger-Dienst ist vorab mit diesen abzustimmen. Im Falle von WhatsApp (Datenübermittlung in die USA) bedarf es sogar einer expliziten Einwilligung. Durch diese wird die Weitergabe der Telefonbuchdaten in ein Land ohne angemessenes Datenschutzniveau legitimiert.

Sofern mit einer Nachricht (z. B. Terminverschiebungen oder -absagen) mehrere Patienten angesprochen werden sollen, ist zwingend auf einen Gruppen-Chat zu verzichten und die weniger bekannte Broadcast-Funktion zu verwenden. Diese zeichnet aus, dass der Versender einer Nachricht diese an eine Vielzahl von Empfängern schickt. Die Empfänger sehen jedoch nicht, wem ebenfalls die Nachricht zugestellt wurde. Eine Rückantwort wird ebenfalls nur dem ursprünglichen Versender zugestellt. Im Gegensatz hierzu ist bei einem Gruppen-Chat jedes Gruppenmitglied erkennbar, ebenso jede Nachricht, egal wer diese versandt hat. Zudem sind die Telefonnummern und individuellen Profildaten (Status, Profilbild, zuletzt online) der anderen Teilnehmer sichtbar.



Ärztliche Schweigepflicht?

Auch wenn die Kommunikationsinhalte verschlüsselt sind, besteht die Gefahr, dass unbefugte Dritte über das (Dienst-) Handy des Arbeitnehmers Zugriff auf die Kommunikationsinhalte nehmen können. Insoweit bedarf es weiterer Maßnahmen zur Datensicherheit (siehe unten).

Unabhängig davon stellt sich die Frage eines Verstoßes gegen die ärztliche Schweigepflicht hinsichtlich der Verarbeitung von Meta- und Telefonbuchdaten. Wie bereits in der Märzausgabe dargestellt, unterliegt bereits der Umstand, dass man sich in medizinische Behandlung begeben hat, der ärztlichen Schweigepflicht. Inwieweit dieser Aspekt relevant ist, hängt wiederum davon ab, welche Daten tatsächlich auf dem Server des Anbieters gespeichert werden. Aus der Kombination „Telefonnummer und Metadaten“ wird kaum eine medizinisch relevante Verknüpfung vermutet werden können, da eine Zuordnung der Mobilfunknummer zu einem Berufsgeheimnisträger wenig wahrscheinlich ist. Werden hingegen auch Name, Firma, E-Mail-Adresse, Postanschrift und ggf. Notizen zum Telefonkontakt gespeichert, können durchaus entsprechende Rückschlüsse gezogen werden.

Bei der Auswahl des einzusetzenden Dienstes sollte der Aspekt der Wahrung der ärztlichen Schweigepflicht eine wesentliche Rolle einnehmen.

Noch mehr Datensicherheit?

Bisher wurde nur die Datensicherheit beim Anbieter des Messenger-Dienstes besprochen. Der Arbeitgeber bzw. der jeweilige Mitarbeiter muss jedoch seinerseits auch Maßnahmen zur Gewährleistung der Sicherheit der Daten treffen.

- **Private Geräte:**
  Die Kommunikation sollte keinesfalls auf privaten Geräten über den privaten Account des Mitarbeiters erfolgen. Scheidet der Mitarbeiter aus dem Unternehmen aus, hat der Arbeitgeber keine Möglichkeit, auf die Daten zuzugreifen bzw. deren Löschung zu veranlassen. Darüber hinaus hat der Arbeitgeber keine Möglichkeit, weitere Sicherheitsmaßnahmen (hierzu gleich) auf dem Gerät zu „erzwingen“.

- **Gerätesperre:**
  Sowohl Gerät als auch Messenger-Dienst (sofern dies unterstützt wird) sind mit einer PIN-Sperre zu versehen. Hierdurch wird es Unbefugten zumindest erschwert, auf die Kommunikationsdaten zuzugreifen.
- **Dokumente/ Fotos:**
  Der Versand von Fotos und Dokumenten ist zu untersagen. Der Empfang ist auf ein absolutes Mindestmaß zu reduzieren. Erhaltene oder versandte Dokumente sind unverzüglich von den Geräten, aus der ggf. im Hintergrund laufenden Cloud und aus dem Messenger zu löschen. Je nachdem wie der Messenger-Dienst konfiguriert ist, werden empfangene Dokumente auf dem Gerät in den entsprechenden Ordnern (Fotos, Videos, etc.) abgelegt und von dort unter Umständen in die Cloud des Geräteinhabers weitergeleitet. Zumindest Letzteres kann bei WhatsApp dadurch ausgeschlossen werden, dass die Funktion „Empfangenes Sichern“ (Einstellungen Chats) deaktiviert ist.

Exkurs: Vorratsdatenspeicherung

In einer aktuellen Entschließung des Bundesrates (Drucksache 88/16) vom 22. April 2016 wurde sich dafür ausgesprochen, Messenger-Dienste, die bislang nicht dem Telekommunikationsgesetz (TKG) unterliegen, über eine Gesetzesänderung im TKG mitzuregeln. In diesem Fall könnten die Metadaten unter Umständen auch der Vorratsdatenspeicherung unterliegen. In diesem Fall wäre der Einsatz der Instant-Messenger erneut auf den Prüfstand zu stellen.

Fazit

Messenger-Dienste können datenschutzkonform und unter Beachtung der ärztlichen Schweigepflicht in Gesundheitseinrichtungen eingesetzt werden, wenn bestimmte Voraussetzungen erfüllt sind (siehe Checkliste). Der Patient muss über etwaige Risiken aufgeklärt werden und, je nach eingesetztem Messenger-Dienst, in dessen Einsatz einwilligen (z. B. Datentransfer in die USA). Bei der Auswahl und der Einführung sollte der Datenschutzbeauftragte frühzeitig eingebunden werden.

CHECKLISTE

Bietet der Anbieter eine Ende-zu-Ende-Verschlüsselung?	Ja ■	Nein ■
Werden Metadaten sofort gelöscht?	Ja ■	Nein ■
Werden Daten des Telefonbuches auf den Servern des Anbieters gespeichert werden?	Ja ■	Nein ■
Ist eine Nutzung des Dienstes auch ohne Auslesen des Telefonbuches möglich?	Ja ■	Nein ■
Soll der Messenger auf privaten Geräten der Beschäftigten eingesetzt werden?	Ja ■	Nein ■
Sind die dienstlichen Geräte mit speziellen Zugriffsschutzmaßnahmen (z. B: PIN) versehen?	Ja ■	Nein ■
Sind der Umgang mit Dokumenten und Fotos sowie die Speicherung von Daten in einer Cloud geregelt?	Ja ■	Nein ■
Finden regelmäßige Prüfungen der Einhaltung der Vorgaben statt?	Ja ■	Nein ■

Sicherheit von Krankenhausnetzen und Medizingeräten in der Kritik

Im Januar 2016 stellten Sicherheitsforscher auf der Usenix Enigma Konferenz dar, welcher Stand der IT-Sicherheit aus ihrer Sicht in amerikanischen Krankenhäusern immer noch zu finden ist und wie (un-)sicher viele Medizingeräte eigentlich sind. Berichtet wurde in diesem Zusammenhang u. a. von einem MRT-Gerät, welches bei einem Netzwerkscan durch das Betriebssystem Windows 95 auffiel. Bei einer späteren Besprechung des Netzwerkscans stellte sich heraus, dass das MRT-Gerät nur mit dieser veralteten Windows-Version betrieben werden konnte und zu allen anderen Betriebssystemen inkompatibel war. Was hätte das Krankenhaus vor dem Hintergrund der hohen Anschaffungskosten des MRT-Geräts an dieser Stelle also tun können? Zumindest wäre die Erstellung eines separaten Sicherheitskonzepts für den Weiterbetrieb des MRT-Gerätes unter Verwendung von Windows 95 erforderlich gewesen. Im Rahmen der Erstellung des Sicherheitskonzepts wäre das Krankenhaus vermutlich zu dem Ergebnis gekommen, dass das MRT-Gerät nur dann weiterbtrieben werden darf, wenn es vom sonstigen Netzwerk des Krankenhauses separiert wird. Bei einem normalen Netzwerkscan hätte das MRT-Gerät daher gar nicht auftauchen dürfen.

Die Sicherheit von Krankenhausnetzen war vor einigen Jahren übrigens auch Teil eines Vortrags auf dem 31C3 mit dem Titel „Security Nightmares“. Im Fazit wurde festgestellt, dass man eins nicht machen sollte, wenn man als Patient im Krankenhaus liegt: „Nmap benutzen“. Bei Nmap handelt es sich übrigens um einen Netzwerkscanner, der auch von professionellen Penetrationstestern genutzt wird, um sich einen Überblick über ein bestehendes Netz, dessen Dienste und Schwachstellen zu verschaffen.

E-Health-Gesetz

Anfang Dezember 2015 wurde das E-Health-Gesetz vom Bundestag beschlossen und ist zum Jahreswechsel in Kraft getreten. Durch dieses wird die bundesweite Einführung der Telematik-Infrastruktur vorangetrieben. Beginn der Einführung ist Mitte 2016. Ziel ist die Schaffung einer flächendeckenden Telematik-Infrastruktur für Arztpraxen und Krankenhäuser innerhalb von zwei Jahren. Insgesamt soll das Gesetz die gesetzlichen Grundlagen für ein modernes Stammdatenmanagement schaffen und die Speicherung von Notfalldaten und Medikationsplan auf der Versichertenkarte ermöglichen. Darüber hinaus sollen auch elektronische Arztbriefe und die elektronische Patientenakte und die Telemedizin gefördert werden.

Aus datenschutzrechtlicher Sicht wurde dem E-Health-Gesetz insbesondere in der Anfangsphase erhebliche Kritik entgegengebracht. An vielen Stellen wurde daher nachgebessert:

- **Dezentrale Datenspeicherung**
  Die Speicherung der Daten erfolgt nicht an einem einzigen Ort, sondern ist über verschiedene verteilt. Der Vorteil hierbei ist, dass im Falle einer Überwindung der Zugriffsschranken nicht sämtliche Daten des Betroffenen erfasst sind.
- **Bessere Transparenz**
  Patienten können ab 2018 veranlassen, dass ihre auf der Gesundheitskarte gespeicherten Daten in ein elektronisches Patientenfach aufgenommen werden und dort auch weitere Daten hinterlegen. Hierdurch ist es dem Betroffenen möglich, sich über Diagnose und Therapie detailliert zu informieren.
- **Betroffenenrechte**
  Das elektronische Patientenfach ermöglicht dem Betroffenen, die Wahrung seiner Rechte auf Auskunft, Berichtigung oder Löschung (Sperrung) effektiv wahrzunehmen.
- **Datenschutzrecht**
  Sämtliche durch das E-Health-Gesetz geregelten Datenverarbeitungsvorgänge bzw. veranlassten Regelungen bzw. Richtlinien unterliegen der vorherigen Kontrolle des Bundesbeauftragten für den Datenschutz.

gesundheit | versorgung | kommunikation – für diese Begriffe steht die gevko. Mit S3C, unserer IT-Schnittstelle für Versorgungsverträge, vernetzen wir die gesetzlichen Krankenkassen mit den Leistungserbringern, um eine effiziente Abbildung und Abwicklung, u.a. von Selektivverträgen zu ermöglichen. Auf diese Weise sorgen wir dafür, dass die Vertragsinhalte im Praxisalltag ankommen und sowohl Patienten als auch Ärzte von den Vorteilen der Einzelverträge in vollem Umfang profitieren.

gesundheit | versorgung | kommunikation heißt auch unser Newsletter, mit dem wir regelmäßig über Neuigkeiten rund um die Themen S3C-Schnittstelle und IT-gestütztes Versorgungsmanagement informieren. Wir stellen Ihnen aktuelle Projekte und Projektvorhaben der gevko, Neuerungen aus unserer Produktschmiede und deren Anwendungsmöglichkeiten und -vorteile in der Praxis sowie Veranstaltungen und aktuelle Trends und Themen im Gesundheitswesen, in der Softwareindustrie und in der Politik vor.

Interessiert? Dann abonnieren Sie kostenlos unseren Newsletter
gesundheit | versorgung | kommunikation unter http://www.gevko.de/de/newsletter/.

Datenschutz im Gesundheitswesen

Grundlagenwissen – Praxislösungen – Entscheidungshilfen

2 Ordner mit Register im Format DIN A5,
ca. 1.300 Seiten Inhalt
ISBN: 978-3-553-43000-5
Preis 179.- inkl. MwSt.

Uneingeschränkter Online-Zugriff auf alle Arbeitshilfen inkl. 3-4 kostenpflichtige Nachtragslieferungen pro Jahr zum Preis von jeweils 74,90 Euro inkl. MwSt. und versandkostenfreier Zusendung im Inland.