Mit Sicherheit Mobil:
Die Nutzung mobiler Geräte stellt Herausforderungen an Datenschutz und -sicherheit im Klinikalltag

Agnes Gawlik, Marcel Winandy
Horst Görtz Institut für IT-Sicherheit, Ruhr-Universität Bochum

Smartphones und Tablet-Rechner ermöglichen eine einfache Handhabung, um Patientendaten flexibel erfassen und bearbeiten zu können. Die Anwendungen (Apps) sind mittlerweile zahlreich und vielfältig (z.B. über 700 medizinische Apps für Android im Google Play Store). So spielen viele Einrichtungen mit dem Gedanken, derartige mobile Systeme in ihre IT-Landschaft einzubinden, andere haben bereits damit begonnen. Jedoch gilt es zu bedenken, dass die Betriebssysteme dieser Geräte nicht für den Einsatz mit hohem Schutzbedarf für sensible Daten (wie Patientendaten) konzipiert sind. Betriebssysteme wie iOS oder Android bringen zwar eine Reihe von Sicherheitsfunktionen mit, die sich für viele Anforderungen gut einsetzen und zum Teil auch zentral managen lassen. Durch den Einsatz mehrerer Anwendungen auf demselben Gerät und die vielfältigen Kommunikationsmöglichkeiten bleiben dennoch einige Bedrohungen hinsichtlich der Datensicherheit bestehen. Neuartige, verbesserte Sicherheitsmechanismen für Mobilgeräte können eine technische Unterstützung geben, um nicht allein auf organisatorische Maßnahmen zurückgreifen zu müssen.

Sicherheitsanforderungen für Mobilgeräte

Die Speicherung und Bearbeitung von patientenbezogenen Daten muss auf Mobilgeräten die üblichen Anforderungen nach Integrität und Vertraulichkeit der Daten gewährleisten. Der gesetzliche Datenschutz und die Wahrung des Patientengeheimnisses erfordern zusätzliche Maßnahmen für den Einsatz von Mobilgeräten. Diese Geräte können sich aufgrund ihrer Mobilität nicht nur mit verschiedenen Netzwerken verbinden (WLAN, Bluetooth, etc.), sondern auch physisch in falsche Hände geraten, z.B. durch Diebstahl. IT-Systeme, die allein auf Zugriffskontrolle und Berechtigungsmechanismen zum Schutz der Daten setzen, laufen Gefahr, dass sensible Daten auf den Mobilgeräten gespeichert bleiben, auch wenn diese nicht mehr mit dem IT-System der Gesundheitseinrichtung verbunden sind. Hier muss explizit geprüft werden, ob der Hersteller der medizinischen Apps Daten auf dem Gerät speichert oder nur zur Bearbeitung und Einsichtnahme anzeigt. Wenn sensitive Daten gespeichert werden, muss sichergestellt werden, dass diese in geeigneter Weise verschlüsselt auf dem Gerät abgelegt werden.

Ein weiteres Problem betrifft die gleichzeitige Nutzung mehrerer verschiedener Apps auf demselben Gerät. Einige (medizinische) Apps greifen ggf. nur auf interne IT-Systeme über gesicherte Netzwerkverbindungen zu (lokales WLAN oder VPN). Andere Apps erfordern jedoch den Zugang zu offenen Netzen, d.h. Internet (z.B. für Recherche-Zwecke). Die Sicherheitsmechanismen von mobilen Betriebssystemen erlauben zwar die Einschränkung von Berechtigungen von Apps (z.B. Zugriff auf Internet oder die Kontakte), bei Zugang zu offenen Netzen besteht jedoch die Gefahr, dass durch Schadsoftware oder Software-Angriffe die Berechtigungen umgangen oder unzulässigerweise erhöht werden [1]. Wenn das medizinische

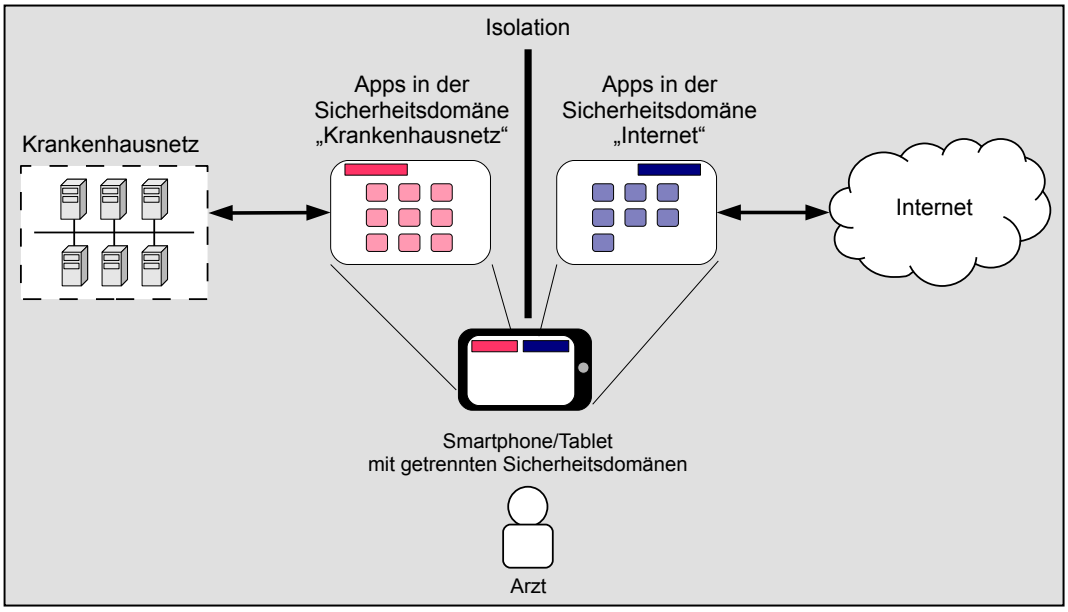

Abbildung 1: Sicherheitsdomänen für mobile Apps

Personal dann noch ihre eigenen Mobilgeräte für die Nutzung in der Gesundheitseinrichtung verwenden („Bring Your Own Device“), potenzieren sich die Probleme, da mit einer Vielzahl weiterer (nichtmedizinischer) Apps auf den Geräten zu rechnen ist. Verstärkte organisatorische Maßnahmen können helfen [2], wünschenswert wäre jedoch eine technische Unterstützung.

Lösungsmöglichkeit: Sicherheitsdomänen

Das Ziel ist eine sichere Integration von vertrauenswürdigen mobilen Endgeräten in die jeweilige IT-Infrastruktur. Das Konzept der Sicherheitsdomänen kann hierbei helfen. Dabei werden die Apps jeweils einer Sicherheitsdomäne zugeordnet, z.B. „Internet“ und „Krankenhausnetz“. Apps, die zur Domäne „Internet“ gehören, können sich mit offenen Netzen verbinden, während Apps der Domäne „Krankenhausnetz“ sich nur über eine gesicherte VPN-Verbindung in die interne IT verbinden können. Alle Apps können jeweils nur auf Daten zugreifen oder mit anderen Apps kommunizieren, die auch zu derselben Domäne gehören. D.h. Apps der Domäne „Internet“ sind niemals in der Lage auf Patientendaten zuzugreifen. Für jede Domäne werden getrennte Kontakte und Email-Konten verwaltet, der Zugang zu Telefondiensten oder SMS kann ebenfalls pro Domäne beschränkt werden. Damit lässt sich z.B. eine Konfiguration für Krankenhaus-Szenarien erstellen, in der nur konkret definierte und von der IT-Abteilung zugelassene Apps in der Krankenhaus-Domäne laufen. Alle Daten auf dem Mobilgerät werden vom Betriebssystem automatisch und transparent so verschlüsselt gespeichert, dass sie jeweils nur in ihrer zugehörigen Domäne lesbar sind. Zudem lassen sich die Domänenzugehörigkeit der Apps sowie die Sicherheitseinstellungen und Schlüsselverwaltung jeder Domäne zentral verwalten und über entsprechende Sicherheitsregeln verbindlich an alle in die IT eingebundenen Mobilgeräte übertragen. Das grundlegende Prinzip dieser Sicherheitsdomänen für medizinische Anwendungen wurde bereits im Rahmen des vom Land NRW und der EU teilgeförderten Projektes RUBTrust/MediTrust [3] erprobt und bereits für Mobilgeräte wie Laptops entwickelt. Ähnliche Techniken zur Bereitstellung isolierter Sicherheitsdomänen für Smartphones findet man beispielsweise bei

BizzTrust/TrustedMobile von der Sirrix AG und Fraunhofer SIT [4], der Android Knox-Plattform von Samsung [5] sowie in BlackBerry Balance [6].

Fazit

Der Einsatz von Mobilgeräten im Gesundheitsbereich stellt eine Herausforderung an den Datenschutz und die Datensicherheit dar. Handelsübliche Betriebssysteme für Smartphones und Tablet-Rechner können diese Anforderungen nicht ohne Weiteres erfüllen. Die Aufteilung von Apps und deren Daten auf Mobilgeräten in isolierte Sicherheitsbereiche stellt eine Lösung dar, um medizinische Daten vor unerlaubtem Zugriff, z.B. aus dem Internet, zu schützen. Jetzt liegt es an der Industrie, entsprechende Produkte bereitzustellen, und an den IT-Verantwortlichen in Krankenhäusern, diese Systeme einzusetzen.

Literatur

[1] L. Davi, A. Dmitrienko, A.-R. Sadeghi, M. Winandy: „Privilege Escalation Attacks on Android“, Information Security, 13th International Conference, ISC 2010, LNCS 6531/2011, Springer 2011, S. 346-360.

[2] O. Pramann, B. Garz, U.-V. Albrecht: „Bring your own device – private Smartphones im Krankenhaus – Haftungsrisiken und –prävention“, E-HEALTH-COM 02/2013, S. 26-30.

[3] Projekt RUBTrust/MediTrust. http://www.rubtrust-meditrust.de (30.09.2013)

[4] Sirrix AG security technologies, TrustedMobile BizzTrust, (20.10.2013), http://www.sirrix.de/content/pages/trustedmobile.htm

[5] Samsung KNOX, A New Solution for Work and Play, (20.10.2013), http://www.samsung.com/global/business/mobile/solution/security/samsung-knox

[6] BlackBerry, Balance technology, (20.10.2013) http://us.blackberry.com/business/software/blackberry-balance.html