Windows 10 und Datenschutz in der Arztpraxis

Es ist nicht ungewöhnlich, dass Software durch neuere Versionen ersetzt wird. Der Stand der Technik und Wissenschaft entwickelt sich weiter und passt sich neuen Anforderungen an. Die Unterstützung des Herstellers für veraltete Software-Versionen wird irgendwann eingestellt, sodass diese auf moderner Hardware oft nicht mehr laufen oder deren Einsatz aufgrund von – in der Informatik unvermeidlichen – Sicherheitsproblemen nicht mehr guten Gewissens vertretbar ist.

Ungewöhnlich intensiv sind aber in letzter Zeit Diskussionen über das neueste Betriebssystem Windows 10 von Microsoft. Insbesondere der Aspekt des Datenschutzes wird dabei kontrovers thematisiert. Ärztliche Kollegen sind hier besonders sensibilisiert, weil sie die Daten ihrer Patienten schützen müssen.

In der Kritik stehen hauptsächlich die tiefe Integration des Betriebssystems mit Cloud-Diensten des Herstellers sowie Hilfsfunktionen, wie die digitale Assistentin „Cortana", die dafür erforderliche Spracherkennung oder die Handschrifterkennung. Gemeinsames Merkmal der kritisch diskutierten Punkte ist, dass eine Datenübertragung vom lokalen Rechner zu Diensten des Herstellers stattfindet oder Daten gleich in der Cloud (zum Beispiel bei MS-Office 365) gespeichert werden. Sie ist integraler Teil einer Dienstleistung (Speicherung in der Cloud und Bereitstellung zu Synchronisationszwecken) oder für den Betrieb von Hilfsfunktionen erforderlich (Spracherkennung, Handschrifterkennung, Cortana). Welche Daten wofür übertragen werden, beschreibt Microsoft in einer Datenschutzerklärung [1, 2]. Fairerweise muss man anmerken, dass solche Funktionen auch in anderen Produkten und Betriebssystemen seit längerer Zeit üblich und offenbar von den meisten Anwendern erwünscht sind (siehe Siri oder Apple-Cloud bei iOS und Mac OS X, Dropbox, Android oder Google-Dienste). Trotzdem dürfen Patientendaten eine Arztpraxis ungewollt oder gar unbemerkt nicht verlassen. Ein externer IT-Dienstleister darf keinen Zugriff auf Patientendaten erhalten.

Die Frage, die sich hier stellt, ist, ob unter dieser Maßgabe ein Betrieb von Windows 10 in einer Arztpraxis vertretbar ist.

Fakt ist, dass Windows in der Standard-Konfiguration („Expresseinstellungen" bei der Installation) für oben genannte Cloud- und Komfort-Funktionen Daten an Microsoft bzw. in eine öffentliche Cloud überträgt. Ob auch patientenrelevante (Meta-)Daten dabei sind, kann nicht mit Sicherheit geklärt oder ausgeschlossen werden. Diese Datenübertragungen können aber vom Anwender „abgeschaltet" werden.

Ob und zum Teil welche Daten der Rechner überträgt, lässt sich in den Datenschutz- und Konten-Einstellungen von Windows regeln. Eine Einführung in die Thematik kann im Internet unter www.heise.de [3] nachgelesen werden. Sehr empfehlenswert ist die Analyse des Landesbeauftragten für den Datenschutz Baden-Württemberg mit allen relevanten Einstellungen inklusive Empfehlungen für einen datenschutzfreundlichen Betrieb von Windows 10 [4].

Eine Datenübertragung kann nur dann erfolgen, wenn ein Rechner mit dem Internet verbunden ist. Für die Informationssicherheit in der Arztpraxis sind die Empfehlungen der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung maßgeblich, insbesondere die „Technische Anlage" [5]. Darin wird gefordert, dass eine direkte Verbindung eines Patientendaten führenden Systems mit dem Internet nicht hergestellt werden darf. Der Betrieb von Windows 10 in einer isolierten Umgebung ist also ohnehin ratsam. Sichere Verbindungen in geschützten Netzen sind unter definierten Voraussetzungen zulässig. Hier kann ein Kollege allerdings in ein Dilemma geraten. Einerseits ist die regelmäßige Aktualisierung des Betriebssystems und der Praxis-Software – auch aus Sicherheitsaspekten – notwendig. Andererseits bekommt man solche Sicherheits- und Programmupdates über das Internet. Es wäre sinnvoll, wenn zumindest Updates der Praxis-Software oder eine gegebenenfalls unvermeidbare Fernwartung über ein geschütztes Netz (zum Beispiel das „Sichere Netz" der Kassenärztlichen Vereinigungen oder ein sicheres Netz des PVS-Herstellers) erfolgen. Für Aktualisierungen des Betriebssystems gibt es die Möglichkeit, Updates über einen vom Praxisnetz zunächst isolierten Rechner ohne Patientendaten herunterzuladen und diese dann im lokalen Netz zu verteilen (Stichwort: Windows Server Update Services – WSUS; offline).

Ein Betriebssystem hat naturgemäß vollen Zugriff auf alle Daten, die in einem Rechner gespeichert sind. Ein gewisses Maß an Vertrauen an das Betriebssystem und den Hersteller ist daher erforderlich. Nach gegenwärtigem Kenntnisstand gibt es zwar viele Diskussionen, jedoch keine fundierten, objektiven Belege, die auf einen Vertrauensbruch seitens des Herstellers hindeuten würden. Im Gegenteil: die eingesetzten Sicherheitsmechanismen, wie sie in den Zertifizierungsdokumenten von Windows 10 beschrieben werden, entsprechen dem gegenwärtigen Stand der Wissenschaft und Technik [6]. Eher dürfte also Malware für Ärger sorgen, wenn man die einschlägigen Empfehlungen zur Informationssicherheit in der Arztpraxis nicht beachtet.

Das Literaturverzeichnis kann beim Verfasser angefordert oder im Internet unter www.bayerisches-aerzteblatt.de (Aktuelles Heft) abgerufen werden.

Autor

Professor Dr. med. Georgios Raptis,
Informatik/E-Health,
Fakultät Informatik und Mathematik,
Ostbayerische Technische Hochschule
Regensburg, Prüfeninger Straße 58,
93049 Regensburg