IT-Support spielt zentrale Rolle bei der Erhöhung der Sicherheit für Server, Netzwerke und Daten

Digitalisierung als Risikofaktor

Bild: Kadmy/Fotolia

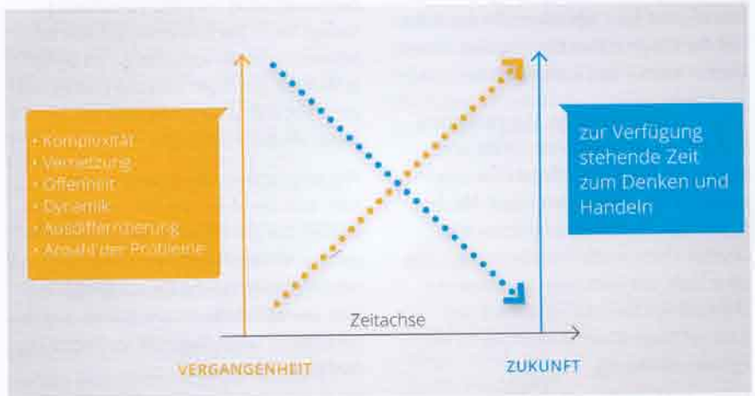
Durch das E-Health-Gesetz und den bundesweiten Aufbau einer Telematikinfrastruktur erhält der IT-Support von Gesundheitseinrichtungen weitere verantwortungsvolle Aufgaben.

Die Digitalisierung hält Einzug im Gesundheitswesen – ob mit elektronischen Patientendaten oder durch die Vernetzung von IT und Medizintechnik. Krankenhäuser und andere medizinische Einrichtungen stehen vor der Herausforderung, die Sicherheit der Daten und Systeme zu gewährleisten. Der IT-Support spielt dabei eine zentrale Rolle.

Medizinische Geräte übertragen Vitalparameter an die mobilen Geräte der Ärzte, Serviceroboter entlasten das Pflegepersonal bei schweren körperlichen Arbeiten und dank der elektronischen Patientenakte sind Informationen zur Krankengeschichte schneller verfügbar. Smarte Technologien halten Einzug in den Krankenhäusern, das Smart Hospital ist nicht mehr nur wohlklingende Zukunftsmusik. Spätestens mit der elektronischen Gesundheitskarte ist die Digitalisierung in der Gesundheitsbranche angekommen.
Durch die bundesweite Einführung der Telematikinfrastruktur im Rahmen des E-Health-Gesetzes wird sie Fahrt aufnehmen. Für die daran angeschlossenen Institutionen bedeutet dies höchste Anforderungen an die Datensicherheit, denn es gilt, hochsensible Patientendaten zu schützen – eine Herausforderung für Krankenhäuser und andere medizinische Einrichtungen. Ein guter IT-Support ist deshalb wichtiger denn je.

Digitalisierung lässt Sicherheitsanforderungen steigen

Der IT-Support sorgt für den reibungslosen Betrieb der IT-Infrastruktur im Krankenhaus. Neben der Datensicherheit als zentrales Thema stehen wachsende Datenbestände, das Einbinden privater Geräte der Mitarbeiter (Boyd – Bring your own device) oder die Vernetzung von IT und Medizintechnik an der Tagesordnung. Hinzu kommen die Support-Bedürfnisse, die beispielsweise das Internet der Dinge mit sich bringt. Denn ein Smart Hospital kann nur funktionieren, wenn die IT zuverlässig läuft und auf dem aktuellen Stand der Technik gehalten wird. Dafür werden zum einen IT-Spezialisten und zum anderen Tools benötigt, die die Arbeit des IT-Supports sinnvoll unterstützen. Viele IT-Probleme können heute per Fernzugriff gelöst werden. Insbesondere kleinere medizinische Einrichtungen leisten sich deshalb keinen eigenen IT-Support mehr oder setzen auf eine Kombination aus hauseigener IT-Abteilung und externen Dienstleistern mit der benötigten Fachexpertise.
Die Fernwartung ergänzt schon seit Jahren den klassischen Besuch vor Ort. Üblicherweise kommt dafür ein Fernwartungsprogramm zum Einsatz, mit dem der IT-Supporter mittels Desktop-Sharing auf das System des Krankenhauses oder einzelne PCs zugreifen kann. Das funktioniert mit neueren Fernwartungswerkzeugen quasi konfigurationsfrei. Beide Seiten, der IT-Support und der zu wartende Rechner, müssen lediglich die Software installiert haben.



Die Komplexität der Informationstechnologie steigt zusehends und die für Support-Aufgaben zur Verfügung stehende Zeit wird geringer. Geeignete Tools und leistungsfähige Dienstleister sind ein Ausweg aus dieser Zwickmühle. Bild: pcvisit Software

Zugriff auf krankenhausinternes System

Eine für den Support in Krankenhäusern wichtige Funktion bietet die Fernwartungssoftware pcvisit 15.0. Vor allem für gemischte Teams aus hausinternem IT-Support und externen Fachleuten kann der ‚einfache Fernzugriff' mit Berechtigungskonzepten interessant sein. Mit ihm können Verantwortliche über ein zentrales Portal, das auch alle anderen Teammitglieder als Einstieg nutzen, verschiedene Zugriffsberechtigungen einrichten und verwalten.

Uwe Rummel, Vorstand pcvisit Software: „Als Anbieter von Fernwartungssoftware für kleine und mittelgroße IT-Supporter-Teams kennen wir die Sorgen und wissen, dass der Aufgabenbereich des IT-Supports im Krankenhaus wachsen wird." Bild: pcvisit Software

Damit entfällt die sicherheitstechnisch bedenkliche Weitergabe von Passwörtern, und der Verantwortliche erhält einen transparenten Überblick über die vergebenen Zugriffsrechte. Die Zugriffe werden zudem zu Dokumentationszwecken automatisch erfasst. Dies dient einerseits der Absicherung, dass niemand anonym zugreift, andererseits können die Zugriffe auch als Nachweis für ausgeführte Arbeiten herangezogen werden.
Mit abgestuften Zugangs- und Konfigurationsrechten sowie temporären Zugängen wird die Arbeit mit externen Fachleuten zusätzlich vereinfacht. Die zu wartenden Computer werden mit der Software übersichtlich in Ordnerstrukturen dargestellt und verwaltet. IT-Supporter im Team bekommen individuell nur die Ordner angezeigt, für die sie vom Verantwortlichen eine Zugriffsberechtigung erhalten haben. Und auch die PC-Nutzer können sehen, wer konkret Zugriff auf ihre Rechner hat und wer nicht.

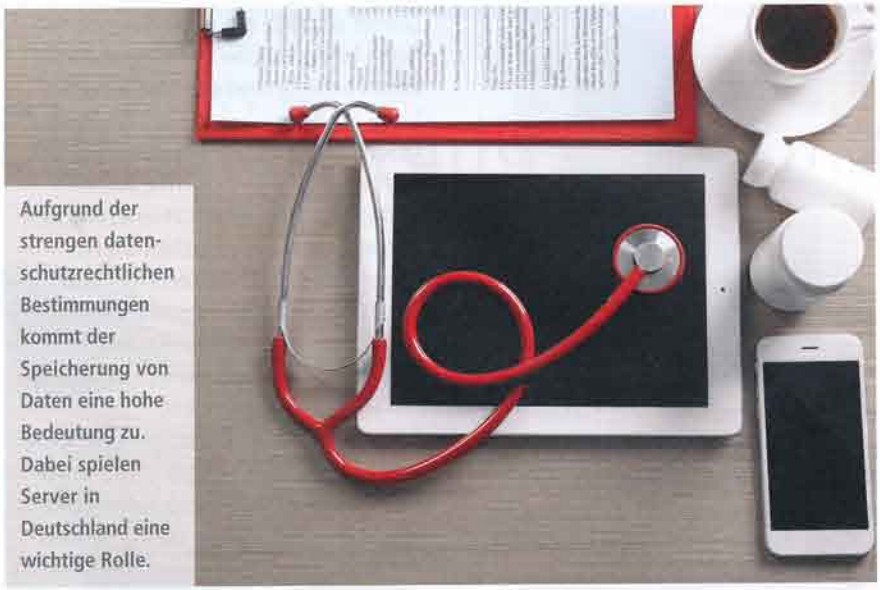


Bild: Africa Studio/Fotolia

Aufgrund der strengen datenschutzrechtlichen Bestimmungen kommt der Speicherung von Daten eine hohe Bedeutung zu. Dabei spielen Server in Deutschland eine wichtige Rolle.

Beim Thema Sicherheit vertrauen Krankenhausmitarbeiter auf den IT-Support. Nur wie steht es um die Datensicherheit bei der vom Support genutzten Software? Fakt ist: Der IT-Support in den Einrichtungen bewegt und speichert zum Teil hochsensible Daten, die eigenen und die der Krankenhäuser. Die Sicherheit dieser Daten ist deshalb von besonderem Belang.

Sicherheit durch hauseigenen Support und deutsche Server

Der Datenschutz ist über die Grenzen der Gesundheitsbranche hinaus in Deutschland ein viel diskutiertes Thema. Bisher ist ungeklärt, ob Daten, die über amerikanische Server laufen, von den US-Behörden eingesehen werden können oder nicht. Die Gesetzgebung dazu hängt noch in der Schwebe. Die europäischen Datenschutzbeauftragten möchten ein akzeptables Schutzniveau für europäische Daten aushandeln. Nicht alle Beobachter sind sich jedoch einig, ob diese Bemühungen fruchten werden. Aktuell ist es deshalb ratsam, Support-Lösungen zu wählen, bei denen die Daten Deutschland zu keinem Zeitpunkt verlassen. Deutschland leistet sich eines der strengsten Datenschutzgesetze weltweit. Medizinischen Einrichtungen, die den Schutz kritischer Patientendaten gewährleisten müssen, kommt es deshalb entgegen, wenn der Dienstleister denselben strengen Restriktionen unterliegt wie sie selbst. Fernwartungssysteme, die ausschließlich über deutsche Server kommunizieren, unterliegen dem deutschen Datenschutzgesetz. Der Serverstandort des Anbieters wird relevant, sobald sein Dienst als Software as a Service (SaaS) auf seinem Server ausgeführt wird. Noch mehr Sicherheit bieten Softwarelösungen, die autark auf dem hauseigenen Server betrieben werden können. IT-Supporter, die das Fernwartungshosting auf diese Weise vollständig selbst verantworten möchten, können die Fernwartung beispielswiese mit dem Angebot ‚Private Server' von pcvisit über einen eigenen Verbindungsserver betreiben. Das so in die Infrastruktur des Krankenhauses intergierte Fernwartungshosting ermöglicht die volle Kontrolle über Verbindungen, Daten und Updates.

Interne Risikofaktoren

IT-Supporter in Krankenhäusern helfen Mitarbeitern, die in den seltensten Fällen so technikaffin sind, dass sie die Risiken der Digitalisierung realistisch einschätzen können. Die Unsicherheit des Personals im Umgang mit neuen Technologien ist eine Sicherheitsfrage für jede Einrichtung. Obwohl regelmäßig davor gewarnt wird, E-Mail-Anhänge unbekannter Absender zu öffnen, wird es immer Mitarbeiter geben, die doch unüberlegt klicken und damit unerwünschter Schadsoftware Einlass in das hausinterne System gewähren.
Es ist deshalb Aufgabe der IT, dafür Sorge zu tragen, dass solche Szenarien nicht zur Katastrophe werden. Mit Sicherheitstools kann der IT-Support Bedrohungen schneller erkennen und darauf reagieren. Regelmäßige Sicherheits- und Stabilitäts-Updates sollten zu den Standardmaßnahmen gehören, um die Angreifbarkeit der IT-Strukturen zu minimieren. Veraltete medizintechnische Geräte, für die es keine Updates mehr gibt, sind deshalb eine Sicherheitslücke für Krankenhäuser. Auch hier ist es Aufgabe der IT, die Kompatibilität der Hardware mit der Software im Blick zu behalten – vorausschauend vor der Anschaffung und auch später.

Die Grenzen verschwimmen

Die Digitalisierung bietet enorme Chancen für das Gesundheitswesen. Der Aufgabenbereich des IT-Supports wird mit den technologischen Veränderungen im Krankenhaus wachsen. Die Grenzen zwischen dem Supporter, der sich am Arbeitsplatz darum kümmert, dass der Monitor funktioniert, und dem Admin, der für die sichere Übertragung sensibler Patientendaten zwischen den medizinischen Einrichtungen sorgt, verschwimmen. Beide Bereiche werden weiterhin auch in einem Smart Hospital gebraucht. Die ständige Verfügbarkeit der IT-Systeme und deren Sicherheit können jedoch zum geschäftskritischen Faktor werden. Dem IT-Support kommt eine zentrale Rolle als IT-Sicherheitsbeauftragter zuteil. Er wird künftig noch mehr in den Mittelpunkt der strategischen Planung von Krankenhäusern rücken.

Uwe Rummel

Kontakt

pcvisit Software AG
Elisabeth Kaminsky
Leitung Kundenberatung
Tel.: +49 351 892559-47
elisabeth.kaminsky@pcvisit.de
www.pcvisit.de