



Sichere Fernwartung im Gesundheitswesen

Management Summary

Im Gesundheitswesen stehen optimale Versorgung und bestmöglicher Schutz von Patienten im Fokus. IT-Sicherheit hat dabei einen hohen Stellenwert. Strikte gesetzliche Anforderungen an Zuverlässigkeit und Datenschutz stehen einer zunehmenden Vernetzung und damit digitalen Verwundbarkeit gegenüber. Die sichere Fernwartungslösung von genua kann hier einen wertvollen Beitrag leisten, Störungen von medizinischen Geräten frühzeitig zu erkennen und schnell zu beheben.

Im Gesundheitswesen hat ein Paradigmenwechsel stattgefunden: Eine rasant zunehmende Vernetzung der IT-Infrastruktur führt zu immer offeneren und damit immer schützenswerteren IT-Systemen. Medizingeräte (z. B. in Kliniken) sichern das Überleben von Patienten. Medizinisches Fachpersonal muss daher auf eine absolute Zuverlässigkeit und damit Verfügbarkeit dieser Geräte vertrauen. Mussten Medizingerätehersteller und IT-Spezialisten im Gesundheitswesen früher eine präventive Störungsbehebung in geschlossenen Systemlandschaften gewährleisten, so sehen sie sich heute durch die Vernetzung mit Herausforderungen wie Hackern und Malware konfrontiert. Manipulation von Medizingeräten kann Menschenleben bedrohen. Darüber hinaus besteht die Gefahr, dass höchst vertrauliche Patientendaten in unbefugte Hände gelangen. Hier stehen Medizingerätehersteller vor der Aufgabe, ein Höchstmaß an IT-Sicherheit zu gewährleisten.

Doch wie verbindet man die Vernetzung sensibler Geräte mit hoher Sicherheit und gleichzeitiger Anwenderfreundlichkeit?

Hier erhalten Sie einen Überblick, wie Medizingerätehersteller die Vorteile vernetzter medizinischer IT-Landschaften mit der Fernwartungslösung von genua nutzen können.

Von zentraler Bedeutung ist dabei der Schutz des Netzwerks von Kunden (Krankenhäuser, medizinische Spezial-einrichtungen usw.) nach hohen Sicherheitsstandards, wie z. B. den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Risiken durch Fernwartung

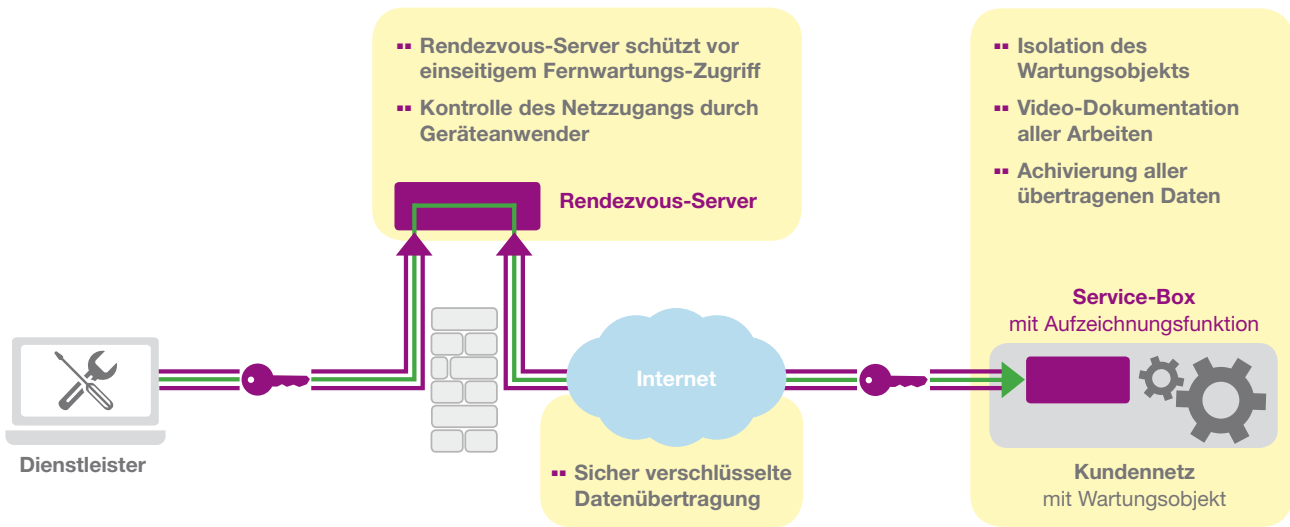
Der Einsatz einer Fernwartungslösung bringt viele Vorteile, folgende Risiken sprechen allerdings dagegen:

- **Safety:** Gefährdung von Leib und Leben
- **Datenschutz:** Hochsensible Patientendaten fließen ab
- **Schadsoftware:** Eingeschleuste Malware verbreitet sich im Netzwerk des Medizingerätebetreibers
- **Kosten:** Durch Cyber-Angriff auf ein Krankenhaus oder eine medizinische Facheinrichtung entstehen Schäden
- **Kontrolle:** Bei Schäden sind Haftungsfragen strittig
- **Usability:** Prozesse im Handling medizinischer Geräte werden komplizierter

Wir zeigen im Folgenden, inwieweit sich die genannten Vorbehalte ausräumen lassen.

Die Lösung: Fernwartung mit genua

Sichere Fernwartung medizinischer Geräte




1. Cyber-Angriffe vermeiden

Herausforderung	Fernwartungslösung von genua
<p>Wird Fernwartung nicht sicher durchgeführt, z. B. aufgrund unzureichender Identifizierung und Authentifizierung der Dienstleister, entstehen Einfallstore in die medizinische IT-Landschaft. Treten auf diese Weise z. B. Schäden durch Cyber-Angriffe ein, können wichtige Medizingeräte manipuliert werden bzw. ausfallen. Es besteht die Gefahr, dass die Gesundheit von Patienten bedroht ist.</p>	<ul style="list-style-type: none"> •• Fokus auf Sicherheit und Hochverfügbarkeit •• Authentifizierung und Verschlüsselung •• Zugriffsbeschränkung auf Wartungsobjekt •• Medizingerätebetreiber hat vollständige Kontrolle über Wartungsprozess und Netzöffnung •• Sicherheits-Patches für alle Fernwartungskomponenten zentral verteilbar
<p>Ihr Vorteil: Bestmögliche Absicherung Ihrer medizinischen Geräte in einer offenen IT-Landschaft. ✓</p>	


2. Sensible Patientendaten schützen

Herausforderung	Fernwartungslösung von genua
<p>Fernwartung eröffnet Dritten einen potenziellen Zugang zum Netzwerk Ihrer Kunden. Das Auslesen hochsensibler Patientendaten wird grundsätzlich möglich, zudem werden diese gegebenenfalls via Internet zur Leitstelle des Dienstleisters transferiert und damit auf ihrem Weg ausspähbar. Dies ist bei sensiblen Daten und strengen gesetzlichen Regularien (BDSG, GDSG, StGB) absolut inakzeptabel.</p>	<ul style="list-style-type: none"> •• Gewährleistung von Vertraulichkeit •• Kontrollierter und ausschließlicher Zugriff auf Ihr fernzuwartendes Medizingerät, ein Zugriff nicht autorisierter Dritter über dieses Netzsegment hinaus ist versperrt •• Hochsichere Datenverschlüsselung •• Unterstützung des Risikomanagements (MPG und DIN EN ISO 14971)
<p>Ihr Vorteil: Der Schutz sensibler Patientendaten hat zu jedem Zeitpunkt höchste Priorität. ✓</p>	


3. Ausbreitung von Schadsoftware verhindern

Herausforderung	Fernwartungslösung von genua
Fernwartung erfordert eine Öffnung des Ziel-Netzwerks. Damit entsteht die Gefahr der absichtlichen oder unbeabsichtigten Einschleusung von Schadsoftware durch Dienstleister oder Angreifer. Ohne Schutzmaßnahmen kann sich Malware ungehindert im gesamten IT-Netz des Kunden ausbreiten, Daten ausspionieren, Steuerungssysteme manipulieren und zentrale medizinische Versorgungsgeräte lahmlegen.	<ul style="list-style-type: none">■ Verschlüsselung, Authentifizierung und Zugriffskontrolle■ Eingeschleuste Schadsoftware ist in einem Netzsegment des Wartungsobjekts eingekapselt■ Durch USB-Sticks verursachte Infektionen sind auf ein Netzsegment begrenzt und können dort untersucht und behoben werden
Ihr Vorteil: Gefahr für die IT-Landschaft Ihrer Kunden wird auf ein Minimum begrenzt. 	

4. Kontrolle behalten

Herausforderung	Fernwartungslösung von genua
Fernwartung erfordert Vertrauen gegenüber Dritten. Krankenhäuser und andere medizinische Gerätebetreiber müssen ihr IT-Netzwerk für Medizingerätehersteller und Dienstleister öffnen, die Monitoring- und Wartungs-Dienste an hochverfügbaren und komplexen Geräten erbringen. Treten Schäden an den fernbetreuten medizinischen Systemen auf, stellt sich schnell die Frage nach der Haftung. Können Sie die Fernwartungsarbeiten nicht detailliert nachvollziehen und vor allem nachweisen, wird es Ihnen schwerfallen, in einem Rechtsstreit die notwendigen Beweise vorzulegen.	<ul style="list-style-type: none">■ Größtmögliche Transparenz für Medizingerätebetreiber und Dienstleister■ Umfassende Logging-Funktionen■ Videoaufzeichnung aller Vorgänge während des Fernwartungsvorgangs■ Mitverfolgen aller Wartungszugriffe in Echtzeit■ Archivierung von Videos sowie übertragenen und ausgeführten Wartungsprogrammen
Ihr Vorteil: Zugriffe sind revisionssicher nachvollziehbar, die Beweislage jederzeit eindeutig. 	

5. Usability und komfortable Administration gewährleisten

Herausforderung	Fernwartungslösung von genua
Fernwartung und deren Absicherung erfordern zusätzliche IT-Komponenten im Netzwerk von Medizingerätebetreibern. IT-Infrastrukturen werden noch komplexer und für Mitarbeiter entstehen Barrieren – die Störanfälligkeit steigt, die Usability sinkt. Damit wird zusätzliches, speziell qualifiziertes Fachpersonal erforderlich, das die Fernwartungslösung administriert.	<ul style="list-style-type: none">■ Einfache Integration in bestehende IT-Landschaften Ihrer Kunden■ Management Station ermöglicht zentrale Administration■ Komfortable Fernwartungs-App■ Vorkonfigurierbare Abläufe für medizinisches Personal und externe Dienstleister■ Session wird mit wenigen Mausklicks freigegeben, durchgeführt und abgeschlossen
Ihr Vorteil: Einfache Bedienung, Trainings zur Fernwartungslösung sind nicht erforderlich. 	



Weitere Informationen

Checkliste BSI-Empfehlungen für sichere Fernwartung

Die Fernwartungslösung von genua erfüllt alle Sicherheitsempfehlungen des BSI.

<https://www.genua.de/download/bsi-fernwartung.pdf>

Über genua

genua ist ein deutscher Spezialist für IT-Sicherheit. Seit der Firmengründung 1992 beschäftigen wir uns mit der Absicherung von Netzwerken und bieten hochwertige Lösungen. Unser Leistungsspektrum umfasst die Absicherung sensibler Schnittstellen im Behörden- und Industriebereich bis hin zur Vernetzung hochkritischer Infrastrukturen, die zuverlässig verschlüsselte Datenkommunikation via Internet, Fernwartungssysteme sowie Remote Access-Lösungen für mobile Mitarbeiter und Home Offices. Unsere Lösungen werden in Deutschland entwickelt und produziert. Viele Firmen und Behörden setzen auf Lösungen von genua zum Schutz ihrer IT. genua ist ein Unternehmen der Bundesdruckerei-Gruppe.

SecurITy
made
in
Germany

So erreichen Sie uns:

genua gmbh, Domagkstraße 7, 85551 Kirchheim bei München

tel +49 89 991950-0, fax +49 89 991950-999, info@genua.de

www.genublog.de, www.genua.de

