Anwenderbericht

Fernwartung mit Sitzungsaufzeichnung und Genehmigungs-Workflow

Das Universitätsklinikum Leipzig vertraut bei Remote-Zugängen für externe Dienstleister auf das ISONA Fernwartungssystem

Universitätsklinikum Leipzig
Anstalt öffentlichen Rechts

Als Krankenhaus der Maximalversorgung deckt das Universitätsklinikum Leipzig (UKL) ein breites Spektrum medizinischer Leistungen ab. Mit rund 6.300 Beschäftigten und mehr als 1.400 Betten werden ambulant und stationär jährlich fast 400.000 Patienten behandelt. Dabei kommt modernste Technologie und Medizintechnik zum Einsatz – medizinische Geräte, Server und Steuerungssysteme, die für den Betrieb des Universitätsklinikums essentiell sind. Dazu zählen etwa auch Röntgengeräte, CTs, Ultraschallgeräte oder Systeme fürs das Patienten-Monitoring.

Universitätsklinikum Leipzig, Quelle: UKL

Um einerseits bei Ausfällen und Störungen solcher Geräte und Systeme schnelle Unterstützung leisten zu können, anderseits aber beispielsweise auch erforderliche Updates einfach und zeitnah vornehmen zu können, setzt das UKL vielfach auf die Möglichkeit des Fernzugriffs durch externe Dienstleister. Auf diese Weise können etwa Techniker oder Support-Mitarbeiter des jeweiligen Herstellers ohne langwierige Anfahrt Hilfestellung leisten.

Branchenspezifische Sicherheitsstandards

Bislang kamen dafür in erster Linie Remote-Zugänge auf VPN-Client-Basis zum Einsatz. Problematisch war hierbei allerdings, dass sich einmal eingerichtete Zugänge nicht zeitlich befristen ließen: Ein einmal eingerichteter Zugang war für den jeweiligen Dienstleister theoretisch dauerhaft nutzbar und damit ein potentielles Sicherheitsrisiko.

Ein fallweises Sperren und Entsperren der jeweiligen Zugänge wiederum erwies sich als nicht praktikabel: Spontane, nächtliche Notfall-Supporteinsätze wären nur durch entsprechende Freischaltung seitens des UKL-Administrationsteams möglich gewesen. Auch branchenspezifische Sicherheitsstandards und Richtlinien spielten eine Rolle, denn als Einrichtung der kritischen Infrastruktur unterliegt das Klinikum unter anderem der Vorgabe, Fernzugriffe stark zu reglementieren und zu protokollieren. Ein Zugriff soll außerdem nur für den tatsächlich benötigten Zeitraum möglich sein.

Auch eine Sitzungsaufzeichnung sollte umgesetzt werden

Um diese Anforderungen zu erfüllen und den Remote-Zugriff auf ein neues Level zu heben, prüften die UKL-Verantwortlichen verschiedene Lösungen und ließen sich unterschiedliche Ansätze präsentieren. Neben der Möglichkeit, den Fernzugriff zeitlich begrenzen zu können, musste künftig auch eine Protokollierung realisiert werden: „Wir wollten bei Bedarf nachvollziehen können, was genau ein Dienstleister eigentlich auf den Systemen gemacht hat und welche Änderungen vorgenommen wurden“, sagt Thomas Heid vom Informationsmanagement des UKL. „Es konnte früher durchaus einmal vorkommen, dass Nutzer von Anpassungen überrascht wurden oder nach Arbeiten durch Dritte etwas nicht mehr wie gewohnt funktionierte.“ Zu den weiteren Anforderungen zählte außerdem, eine möglichst schlanke und funktionale Lösung zu implementieren, die nicht mit unnötigen Zusatzfunktionen überladen ist.


Magnetresonanztomograph (MRT), Quelle: pixabay.com

Anwenderbericht

Nach gründlicher Sondierung des Marktes und einem Proof of Concept entschieden sich die Verantwortlichen des Leipziger Universitätsklinikums für die Zusammenarbeit mit ISONA und die Einführung einer Lösung auf Basis des ISONA Fernwartungssystems. Dieses wurde im Rahmen des Projekts an die besonderen Anforderungen des UKL angepasst. So konnte beispielsweise auf Basis des Automation WebCenters ein Ticketsystem für den Fernzugriff realisiert werden. Der sichere Remote-Zugang erfolgt über den Secure Automation WebClient. Ein weiteres Element der von ISONA umgesetzten Gesamtlösung ist die sogenannte „Mitschnittbox“, die die Aufzeichnung von Wartungs-Sitzungen ermöglicht. Da das neue System direkt in die bestehende IT-Infrastruktur des UKL integriert werden konnte, waren dort keine größeren Anpassungen notwendig. Gleichzeitig wurde eine Active-Directory-Kopplung eingerichtet, um den Authentifizierungsprozess zu vereinfachen: Bereits bestehende Nutzer können für den Loginvorgang ihre bekannten Daten verwenden.

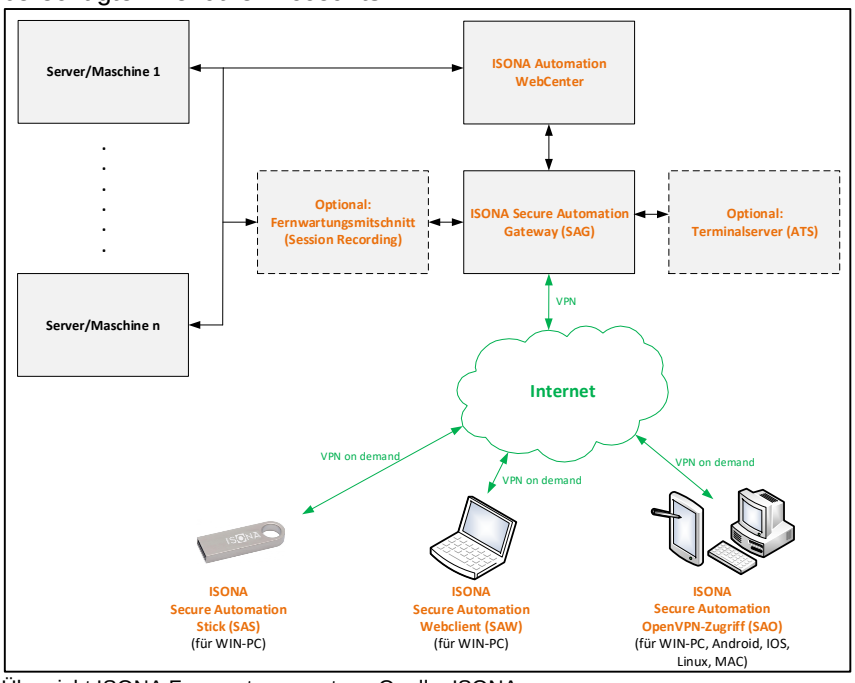
Ticket-basierter Genehmigungsprozess

Beim Fernzugriff für externe Dienstleister deckt das UKL mit dem neuen System bewusst zwei Varianten ab. Den Standard bildet für die meisten Zugriffe eine Ticket-basierte Lösung. Je nachdem, wer den Zugriff beantragt, wird über entsprechende E-Mail-Verteiler der jeweilige Personenkreis innerhalb des UKL über den Zugriffswunsch informiert. Dieser kann dann für ein bestimmtes Zeitfenster genehmigt werden und erfolgt über ein One-Time-Passwort (OTP), welches dem anfragenden Dienstleister per E-Mail übermittelt wird. Die Tickets enthalten dabei Details wie etwa die Zielsysteme und die erlaubten Zugriffsports oder die berechtigten Benutzer-Accounts.

„Unser Ziel ist grundsätzlich, dass möglichst viele externe Dienstleister beim Fernzugriff die Variante mit Genehmigungsprozess nutzen“, erklärt Heid. „Selbstverständlich gibt es aber Sonderfälle, bei denen wir aus praktischen Gründen auch weiterhin auf einen per 2-Faktor-Authentisierung abgesicherten Rund-um-die-Uhr-Zugang ohne vorgeschalteten Genehmigungsprozess setzen werden. Dies ist beispielsweise dann erforderlich, wenn zu jedem Zeitpunkt bei Störungen ein Zugriff auf kritische Systeme möglich sein muss.“

Umstellung der bestehenden VPN-Zugänge

Nach der Integration des neuen Fernwartungssystems von ISONA hat das UKL die Migrationsphase gestartet, in der bestehende VPN-Zugänge auf die neue Lösung umgestellt werden. Hinsichtlich der Sitzungsaufzeichnung ist eine Archivierung der Log-Dateien für sechs Monate geplant, um Vorgänge bei Bedarf nachvollziehen zu können. Die Reaktionen auf Kundenseite fallen positiv aus – auch deshalb, weil das neue Fernwartungssystem sich mit beliebigen Browsern nutzen lässt und Dienstleister somit zusätzliche Flexibilität gewonnen haben. Und auch auf Seiten der Technik fällt das Fazit sehr zufrieden aus: „Die ISONA-Lösung ermöglicht es uns, die Anforderungen umzusetzen, die der branchenspezifische Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus vorgibt. Gleichzeitig haben wir eine Lösung realisiert, die zum einen den Anforderungen unserer externen Dienstleister entspricht, zum anderen aber auch den Genehmigungs- und Freischaltprozess für Fernzugriffe in unserem Haus deutlich optimiert und vereinfacht hat.“



Übersicht ISONA Fernwartungssystem, Quelle: ISONA

ISONA GmbH
Sant-Ambrogio-Ring 13a
D-55276 Oppenheim

Telefon +49 6133 / 509098-0
Telefax +49 6133 / 509098-98
E-Mail info@isona.de
Internet www.isona.de