genua.



Software als Patient: ISO-27001-konforme Fernwartung der Krankenhaus-IT

Krankenhaus-IT verarbeitet hochsensible Daten, vom Klinikinformationssystem bis zur Software im OP. Warten externe Dienstleister diese Systeme aus der Ferne, braucht es klare Kontrolle. MKS IT hat die Fernwartung für die Klinken der St. Franziskus-Stiftung deshalb gemeinsam mit genua abgesichert und vereinheitlicht.

FERNWARTUNG DER KRANKENHAUS-IT

SecurITy made in Germany

Die St. Franziskus-Stiftung in Münster betreibt 15 Kliniken sowie weitere Einrichtungen von Bremen bis zum Ruhrgebiet, darunter ein KRITIS-relevantes Hospital. Im Klinikalltag müssen Dienstleister zahlreiche Applikationen remote warten und aktualisieren. Anlässlich einer ISO-27001-Zertifizierung stand die Stiftungstochter MKS IT, der Rechenzentrumsbetreiber der Gruppe, vor der Aufgabe, Fernwartungszugriffe zentral kontrollieren, überwachen und Session-Aufzeichnungen archivieren zu können.

Projekt-Steckbrief

Der Kunde:
MKS IT, der zentrale IT-Service-Provider des Klinikbetreibers St. Franziskus-Stiftung, Münster

Die Aufgabe:
KRITIS- und ISO-27001-konforme Steuerung, Kontrolle und Überwachung der Fernwartungszugriffe externer Dienstleister inklusive leicht durchsuchbarer Archivierung der Sessions

Die Lösung:
Für die St. Franziskus-Stiftung bedeutet die genua-Lösung einen messbaren Sicherheits- und Effizienzgewinn: ISO-27001- und KRITIS-konforme Kontrolle aller externen Zugriffe, durchsuchbare Session-Archive und ein reduziertes Firewall-Regelwerk (nur SSH/HTTPS). Der Personalaufwand sinkt um bis zu 50 % und Freischaltungen dauern nur noch 15 statt 30 Minuten.

Wer als Patient im Krankenhaus aufgenommen wird, hofft natürlich, dass Klinikpersonal und -technik ihm möglichst schnell wieder zur Genesung verhelfen. Was den wenigsten Patienten bewusst ist: Hinter den Kulissen sorgt eine aufwendige IT-Umgebung dafür, dass die Klinikprozesse reibungslos ablaufen.

Komplexe Krankenhaus-IT

Das Spektrum der Krankenhaus-IT reicht vom Klinikinformationssystem (KIS) für die zentrale Verwaltung, Steuerung und Dokumentation über Fachapplikationen wie Radiologie- oder Laborinformationssysteme (RIS, LIS) bis zum digitalen Bildarchiv und Kommunikationssystem (PACS). Hinzu kommt Software für Spezialgerätschaft etwa im OP oder Labor – eine komplexe Applikationslandschaft.

Deshalb bündelt die St. Franziskus-Stiftung den IT-Betrieb ihrer Häuser bei spezialisierten Tochterunternehmen: MKS IT mit zwölf IT- und vier IT-Sicherheits-Experten versorgt die Unternehmensgruppe von zwei Rechenzentren in Bremen aus mit zentralen IT Services. FACT IT betreut mit über 150 Fachleuten die IT der rund 15.000 Klinikmitarbeitenden vor Ort. Parallel dazu kümmert sich das Schwesterunternehmen FACT um die medizinische Betriebstechnik.

Die Fallhöhe bei Störungen ist groß: Pannen und Kompromittierungen können direkt auf die Patientenversorgung durchschlagen. Schließlich schrecken Cyberkriminelle nicht davor zurück, Kliniken mit Ransomware zu erpressen und dafür Abläufe über Monate zu blockieren.

Entsprechend hoch liegt die Messlatte für IT-Betrieb und IT-Sicherheit. Bei einem Haus der Gruppe sind die Anforderungen sogar gesetzlich festgeschrieben: Das St. Franziskus-Hospital in Münster zählt zur kritischen Infrastruktur (über 30.000 vollstationäre Fälle pro Jahr). Es muss daher die Vorgaben des neuen KRITIS-Dachgesetzes ebenso erfüllen wie die des Gesetzes zur Umsetzung der NIS-2-Richtlinie.

Verschärfte Anforderungen durch ISO 27001

Bedrohungs- und Gesetzeslage erfordern also eine hochprofessionelle IT-Organisation. Die MKS IT ist seit 2022 ISO-27001-zertifiziert, der Rechenzentrumsbereich war es schon vorher. Ein Audit ergab, dass bei Kontrolle, Überwachung und Archivierung der Fernwartung noch Optimierungsspielraum bestand.

Im Klinikalltag treten immer wieder Trouble Tickets, Störungen oder Update-Bedarf auf. Externe IT-Dienstleister greifen dann remote auf die IT-Systeme zu, um Anwendungen zu warten bzw. zu aktualisieren. Je nach Standort und Applikation erfolgte das früher – wie branchenüblich – auf unterschiedliche

> „Die genubox ist sicherheitstechnisch genau das, was wir uns wünschen.“
>
> Daniel Siemer, Serviceleiter Rechenzentrum bei MKS IT

Weise: Mal griff der Dienstleister über ein Remote-Support-Tool zu, mal per RDP, mal per VPN. Eine zentrale Steuerung und Kontrolle aber war nur eingeschränkt möglich.

Seit 2019 war auch eine Fernwartung auf der Basis von genua im Einsatz. Der damalige MKS-IT-Geschäftsführer Oliver Seebass hatte sie auf einer Messe entdeckt und testweise installieren lassen. „Man hat gesehen: Die genubox ist sicherheitstechnisch genau das, was wir uns wünschen“, erinnert sich Daniel Siemer, Serviceleiter Rechenzentrum bei MKS IT.

Hochsichere Fernwartungsarchitektur

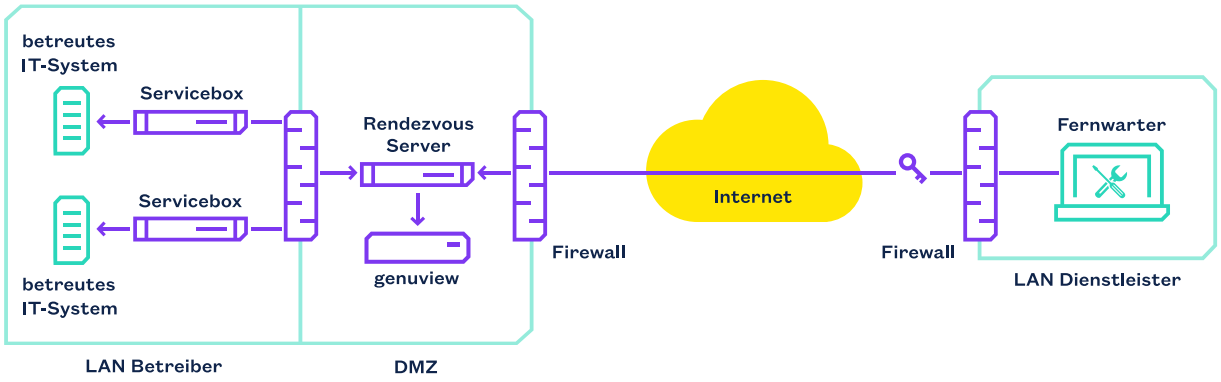
Denn die Architektur von genua unterscheidet sich grundlegend von anderen Verfahren: Ein Externer greift hier nicht über RDP oder VPN direkt auf das Zielsystem zu, weder nach Voranmeldung per E-Mail noch mittels dauerhafter Credentials. Vielmehr ist per SSH-Protokoll ein sogenannter Rendezvous Server zwischengeschaltet.

Ein Praxisbeispiel:

Ein Stationsarzt beanstandet per Trouble Ticket eine Applikationsstörung, FACT IT informiert den Softwareanbieter. Ein Techniker dieses Softwarehauses beantragt nun auf dem von MKS IT vorgegebenen Weg – früher per Interface des Rendezvous Servers, heute über eine benutzerfreundliche Web-Applikation – einen Fernzugang zum Rendezvous Server für eine bestimmte Anwendung und zu einem bestimmten Zeitpunkt.

Ein Mitarbeiter von FACT IT schaltet, ebenfalls bequem per Web-App, eine SSH-Verbindung zwischen Applikations- und Rendezvous Server frei. Hierbei wird die Benutzeroberfläche des Zielsystems auf dem Rendezvous Server nur gespiegelt. Dadurch ist ein Direktzugang von außen auf die Krankenhaus-IT ausgeschlossen und die Steuerung der Fernzugänge bleibt unter der Kontrolle von MKS IT.

Das sorgt für höchstmögliche Sicherheit.



Hochsichere Fernwartungsarchitektur mit SSH-basiertem Rendezvous Server, der externe Zugriffe kontrolliert vermittelt und einen direkten Zugang zur Krankenhaus-IT verhindert. Je nach Einsatzszenario der Lösung kann der Rendezvous Server bei Bedarf auch beim Fernwarter in einer DMZ platziert und von diesem betrieben werden.

Zentralisierung und Standardisierung

Deshalb nahm sich MKS IT vor, Fernwartungsvorgänge auf genua-Technik zu standardisieren. „Wir haben uns schon lange einen möglichst einfachen Weg gewünscht, die Fernwartung zentral freizuschalten und zu kontrollieren“, erinnert sich Serviceleiter Siemer. Insbesondere das Security-Team drängte zur Eile: Es wollte potenziell unkontrollierte Fernzugänge der Remote-Support-Tools möglichst bald stillgelegt wissen, ebenso die RDP- und VPN-Zugänge.

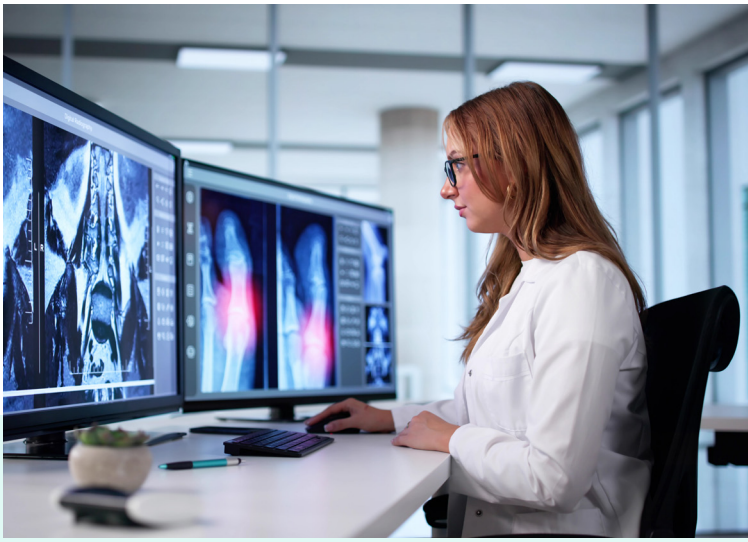
Siemers oberstes Ziel: gemäß ISO 27001 sicherzustellen, dass Externe nur zu vorgegebenen Zeiten und nur auf freigegebene Systeme zugreifen können. Auch wollte er – eine weitere ISO-Anforderung – auditierbar nachweisen, wer wann Zugang zu welchem IT System hatte. Dazu galt es, die Session-Aufzeichnungen leicht durchsuchbar zu archivieren.

Daniel Siemers Team erweiterte die genua-Lösung zur einheitlichen Struktur für alle fünf Regionen der Klinikgruppe: die Regionen Nord (Bremen mit den beiden Rechenzentren), Münster 1 und 2, südliches Münsterland sowie Rhein-Ruhr. Das Projekt begann im Januar 2025 mit einem Zwei-Tages-Workshop. Danach implementierten genua und MKS IT gemeinsam die Rendezvous Server und Serviceboxen in den Rechenzentren.

Den Rollout der übrigen physischen und virtuellen Geräte übernahm MKS IT großteils selbst. Pro Region implementierte das Projektteam am jeweils größten Klinikstandort je einen Rendezvous Server und eine genubox als Hardware-Appliances, in Bremen je ein Appliance-Paar pro Rechenzentrum. Für kleinere Standorte nahm es zehn virtualisierte Serviceboxen hinzu.

Rollout mit Gegenwind

Der Rollout stieß zunächst auf Gegenwind: Manche lokale Administratoren waren nicht glücklich damit, etablierte Abläufe zu ändern. Und einige externe Support-Techniker monierten, man könne nun kein „Copy & Paste“ mehr nutzen und keine Dateien direkt auf Zielsysteme übertragen. Beides erfordere nun einen „Umweg“ über den Rendezvous Server – doch genau dies ist eben der Kern der genua-Architektur, um die Fernwartung kontrollierbar und sicherer zu machen.



Im Hintergrund sorgt eine aufwendige IT-Umgebung dafür, dass der Klinikalltag reibungslos funktioniert.

„Trotz vereinzelter Kritik von Anwenderseite waren das Rechenzentrums- und das Security-Team von MKS IT aufgrund der zentralen Kontrolle der Fernzugriffssicherheit mit den erzielten Verbesserungen sehr zufrieden“, berichtet System- und Netzwerkadministrator Jeff Fischer, der zusammen mit Daniel Siemer das genubox-Projekt betreut hat. „Unser größter IT-Partner, Dedalus Healthcare, kannte das Konzept der hochsicheren Fernwartung bereits. Bei den übrigen Dienstleistern ist die Akzeptanz stark gestiegen, seit wir beim Rendezvous Server auf das Web-Portal umgestellt haben.“ Denn so können die Techniker ein Web-Interface verwenden, wie sie es von anderen Fernwartungstools her kennen.

Zeitersparnis und Kostenkontrolle

Heute wird die genua-Lösung intensiv genutzt. Im Rechenzentrum gibt es laut Jeff Fischer zehn bis 20 Fernwartungszugriffe pro Tag, in größeren Kliniken im Schnitt ein bis zwei. Den IT-Fachleuten von MKS IT und FACT IT bringt der neue Workflow eine deutliche Erleichterung: „Wir haben weniger Personalaufwand, weil man die Sessions nicht mehr aktiv betreuen muss. Und Freischaltungen dauern nun nur noch 15 statt 30 Minuten – eine Zeitersparnis von 50 Prozent“, freut sich Siemer.

Auch das Security-Team profitiert. „Für die IT-Security ist von Vorteil, dass wir nun ein deutlich schlankeres Firewall-Regelwerk haben“, sagt Siemer. Früher musste man Firewall-Regeln je nach Fernwartungstool individuell anpassen. Die genua-Geräte hingegen kommunizieren untereinander nur per SSH. Nach außen sind daher lediglich SSH und HTTPS freizuschalten.

MKS IT zeichnet die Fernwartungsvorgänge auf und kontrolliert sie stichprobenartig. So lässt sich auch die Ursache leichter ermitteln, wenn beim Support Probleme auftreten. Siemer nennt ein Beispiel: Beim internen Dokumentenmanagement werden Dokumente per Website-Aufruf für Mitarbeiter der Stiftung freigegeben. Diese Website war eines Tages nicht mehr aufrufbar. Anhand der Aufzeichnung ließ sich nachvollziehen, dass die Störung auf eine Fernwartung zurückging, die kurz vorher erfolgt war. In einem anderen Fall belegte die Aufzeichnung, dass ein Techniker mehr Arbeit als tatsächlich geleistet abgerechnet hatte.

„Wir haben weniger Personalaufwand, weil man die Sessions nicht mehr aktiv betreuen muss. Und Freischaltungen dauern nun nur noch 15 statt 30 Minuten – eine Zeitersparnis von 50 Prozent.“

Daniel Siemer
Serviceleiter Rechenzentrum bei MKS IT

Wachsendes Archiv einfach durchsuchen

Angesichts eines stetig wachsenden Archivs aufgezeichneter Fernwartungen erwies es sich als nicht mehr praktikabel, Aufzeichnungen einfach in einem Dateiverzeichnis abzulegen: Die Suche wurde zu zeitraubend.

So ergänzte MKS IT die Lösung um genuview 2.0, genuas Add-on zur Verwaltung von Videoaufzeichnungen. genuview speichert alle Fernwartungsaufzeichnungen in einem Langzeitarchiv und ermöglicht per Web-Interface, bei der Suche nach Datum zu filtern. „Das ist deutlich komfortabler als die Suche anhand der langen Dateinamen, in denen man vorher eine Session aufstöbern musste“, so Siemer. Ein weiterer Vorteil: Die Dateifreigabe war nur im Rechenzentrum erreichbar, das Web-Portal hingegen steht unternehmensweit zur Verfügung.

Die containerisierte Anwendung genuview 2.0 läuft im Kubernetes-Cluster. Siemer besitzt eine Kubernetes-Zertifizierung und konnte deshalb auch dieses Add-on selbst einführen: „Ich habe der Dokumentation schnell entnommen, dass die Implementierung recht einfach ist“, erinnert er sich. „Es waren nur zwei Tage Aufwand, bis die ersten Aufzeichnungen liefen.“ Dabei ging er sogar einen Sonderweg: Er wollte das Langzeitarchiv per NFS mit dem Kubernetes-Cluster verbinden, was nicht vorgesehen war. „Wir haben das an unsere Speicherbedürfnisse angepasst und unsere Erkenntnisse an genua zurückgespielt, damit auch andere davon profitieren können“, erzählt er.

Reibungsloser Alltag

Unterstützung im Betrieb benötigt Siemers Team kaum: „Wir hatten erst einen Support Case, aufgrund einer Anfrage aus einem Standort“, berichtet er. „Da mussten wir erst die Support-Kontaktdaten raussuchen.“

Einmal meldete sich Jeff Fischer bei genua: Laut einem Penetration-Test lief auf den genuboxen ein veralteter SSH-Server. Dies erwies sich schnell als Fehlalarm: genua nutzt eine eigene, gehärtete SSH-Version, nicht die Standardvariante.

Der konzernweite Rollout der Lösung ist fast abgeschlossen: Alle Regionen sind angebunden, nur ein paar virtuelle genuboxen stehen noch aus. „Der überwiegende Konsens bei uns im Hause ist, dass die genubox, der Rendezvous Server und genuview 2.0 eine sinnvolle Lösung sind“, resümiert Daniel Siemer. Deshalb will MKS IT die Lösung auch an allen Standorten etablieren, die noch hinzukommen, so wie die kürzlich akquirierten VKKD-Kliniken aus Düsseldorf. In Zukunft will MKS IT zudem die Medizintechnik in die Fernwartung einbinden.

Dass gelegentlich ein Dienstleister reklamiert, er könne keine Skripte direkt übertragen, betrachtet Siemer als notwendige Folge einer hochsicheren Fernwartungsarchitektur. Denn ein hohes Maß an Sicherheit ist eben immer etwas unbequemer – wie ein Fahrradhelm oder der Sicherheitsgurt im Auto. Aber es sind eben Helm und Gurt, die dafür sorgen, dass man nicht unnötig schnell als Patient in einer Klinik der St. Franziskus Stiftung landet.

Weitere Informationen:

genua.de/genubox

1126-01-DE

Über genua

Mit ihren in Deutschland entwickelten und produzierten IT-Sicherheitslösungen ist die genua GmbH eine Wegbereiterin für digitale Souveränität. Behörden, geheimschutzbetreute Organisationen und KRITIS-Unternehmen vertrauen auf genua zum Schutz ihrer kritischen und hochsensiblen digitalen Infrastrukturen.

genuas Portfolio umfasst hochsichere, Backdoor-freie und skalierbare IT-Security-Produkte wie Firewalls, Gateways, quantenresiliente VPNs, Fernwartungssysteme und Komplettlösungen für VS-NfD-konformes mobiles Arbeiten. Viele Produkte sind auch als virtualisierte Variante für eine flexible Cloud-Integration verfügbar. Regelmäßige Zertifizierungen und Zulassungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) belegen das hohe Sicherheits- und Qualitätsniveau.

Mit ihren rund 500 Mitarbeitenden ist die genua GmbH Teil der Bundesdruckerei-Gruppe. Das Unternehmen ist vom BSI als „Qualifizierter Hersteller“ eingestuft und mit seinen Produkten im Kaufhaus des Bundes gelistet. Zu den Kunden zählen u. a. BMW, die Bundeswehr, das THW und die Würth-Gruppe.

Teil der Bundesdruckerei-Gruppe

genua GmbH

Domagkstraße 7 | 85551 Kirchheim bei München
+49 89 991950-0 | info@genua.de | www.genua.de