genua.

Fernwartung für KRITIS: Mit Sicherheit machbar

Fernwartung für eine kritische Infrastruktur (KRITIS)? Eine heikle Sache. Die IT-Systeme der Deutschen Rentenversicherung verarbeiten Medizin- und Sozialdaten und sind als KRITIS klassifiziert. Die Deutsche Rentenversicherung zeigt, wie Fernwartung machbar ist, die höchsten Sicherheitsanforderungen genügen muss.

Teile der IT-Systeme der Deutschen Rentenversicherung sind als kritische Infrastruktur (KRITIS) klassifiziert und haben einen besonders hohen Schutzbedarf.

von Martin Ortgies, freier Journalist

SecurITy made in Germany

„In unserem Organisationsbereich möchten etwa 50 verschiedene Hersteller via Internet auf installierte Systeme zugreifen, um diese aus der Ferne zu warten. Das ist unter KRITIS-Bedingungen eine große sicherheitstechnische Herausforderung“, beschreibt Tobias Birk, Leiter des Security-Bereichs der Deutschen Rentenversicherung Baden-Württemberg (Dt.Re.Vers.) die Ausgangssituation.

Die Träger der Deutschen Rentenversicherung (im Einzelnen: Nordbayern, Bayern-Süd, Schwaben, Rheinland-Pfalz, Hessen, Saarland, Baden-Württemberg) betreiben in Würzburg ein gemeinschaftliches Rechenzentrum. Dieses versorgt die auf fünf Bundesländer verteilten Träger mit einer Vielzahl an Regionalzentren, Außenstellen, sozialmedizinischen Dienststellen sowie Rehakliniken und Therapiezentren. An diesen Standorten werden unterschiedlichste IT- und Techniklösungen betrieben, von der Laborausstattung in Kliniken über die Aufzugssteuerung in der Gebäudetechnik bis zur Office-IT für die Versichertenadministration.

Projekt-Steckbrief

Der Kunde:
Deutsche Rentenversicherung, Betreiber eines gemeinschaftlichen Rechenzentrums in Würzburg

Die Aufgabe:
Sichere Fernwartung von IT-Systemen, die als kritische Infrastrukturen (KRITIS) eingestuft sind

Die Lösung:
Fernwartungslösung mit Rendezvous-Konzept von genua

Kritische Bereiche des IT-Systems müssen ganz besonders geschützt werden

„Wir benötigen eine sichere Lösung, vergleichbar der in der analogen Welt“, nennt Birk die Herausforderung. Er erläutert dies am Beispiel des Vor-Ort-Einsatzes von Service-Technikern, wie er früher üblich war. Der Techniker musste sich persönlich zunächst beim Empfang melden. Ein IT-Mitarbeiter der Deutschen Rentenversicherung überprüfte seine Identität und Berechtigung und begleitete ihn zur Anlage. Jeder Schritt des Technikers wurde persönlich überwacht. „Unberechtigte Personen hatten keine Chance. Auch wenn sie es über den Parkplatz bis zum Empfang geschafft hatten, konnten sie nicht unkontrolliert in das gut abgesicherte Haus hinein“, formuliert der IT-Security-Spezialist den Anspruch für eine sichere Fernwartungslösung.

Anforderung eines KRITIS-Unternehmens

„Fernwartung über externe Netze oder durch Dritte ist besonders kritisch“, so das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Kapitel „Absicherung von Fernwartung“ des IT-Grundschutz-Katalogs. Das 2015 in Kraft getretene Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) schreibt KRITIS-Betreibern vor, die IT-Sicherheit nach dem „Stand der Technik“ umzusetzen. Das BSI benennt Grundregeln zur Absicherung von Fernwartungszugängen und beschreibt notwendige Sicherheitsfunktionen, die erfüllt werden sollten. „Die BSI-Regeln waren für uns die Grundlage des Pflichtenhefts der Fernwartungslösung. Auf die revisionsopitimierte Aufzeichnung auch per Video und die Umsetzung eines Vier-Augen-Prinzips haben wir besonderen Wert gelegt. Außerdem soll unser Mitarbeiter die Fernwartungs-Session jederzeit unterbrechen können“, listet Birk die Forderungen auf.

Es wurde zunächst unter Einbeziehung eines externen neutralen Dienstleisters eine Marktanalyse und Bewertung relevanter Fernwartungslösungen durchgeführt. Am Ende blieben zwei Anbieter zur Auswahl. In einem Proof of Concept wurden die Lösungen der beiden Anbieter unter realen Bedingungen mit drei Mandanten simuliert und ca. drei Monate lang intensiv getestet. Der PoC wurde nach der üblichen Kooperationsmethode im Rechenzentrums-Würzburg-Verbund der Deutschen Rentenversicherung gemeinsam von der IT der Dt.Re.Vers. Baden-Württemberg und den Spezialisten der Dt.Re.Vers. Rheinland-Pfalz und Bayern-Süd durchgeführt.

Die Fernwartungslösung genubox bietet ein hohes Sicherheitsniveau, eine einfache Integration sowie eine komfortable Administration.

Lösung von genua setzt sich durch

Die Entscheidung fiel zugunsten der Fernwartungslösung des deutschen IT-Sicherheitsunternehmens genua GmbH. Die Tests hatten bestätigt, dass die Lösung alle Musskriterien erfüllt und sich auch im Betrieb bewährt.

Zentrales Sicherheitselement der Lösung von genua ist das sogenannte Rendezvous-Konzept. Dabei werden keine einseitigen Fernwartungszugriffe in das Netz der Dt.Re.Vers. erlaubt. Alle externen Verbindungen erfolgen über einen Rendezvous-Server, der in einer Demilitarisierten Zone (DMZ) installiert ist. Sowohl der externe Wartungstechniker als auch der interne Mitarbeiter der Dt.Re.Vers. bauen zu einem verabredeten Zeitpunkt Verbindungen zum Server auf. Diese werden als stark verschlüsselte und authentisierte Punkt-zu-Punkt-Verbindungen über einen VPN-Tunnel erzeugt. Erst mit dem Rendezvous auf dem Server entsteht die durchgängige Wartungsverbindung. Eine direkte Netzkoppelung findet nicht statt. Durch die Rendezvous-Lösung behält die Dt.Re.Vers. die vollständige Kontrolle über die Wartungszugriffe in ihre Netze.

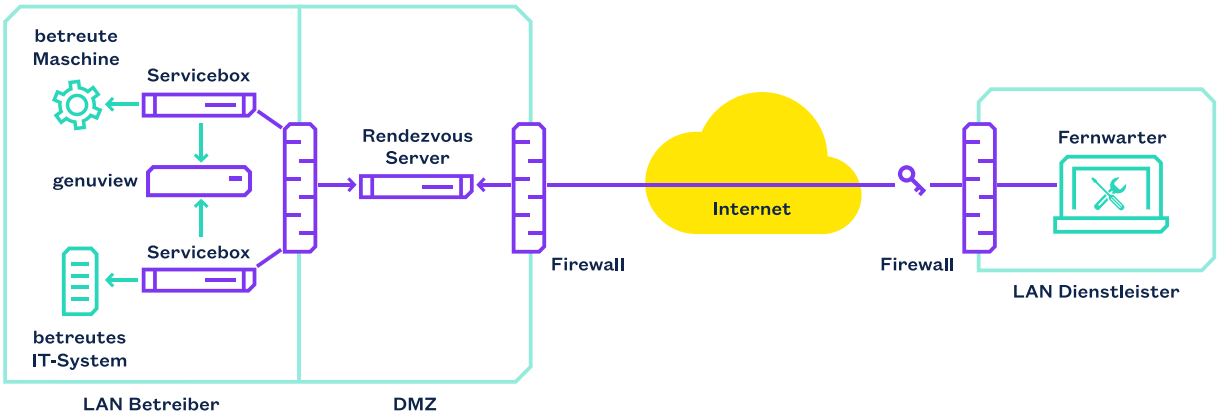
Einheitliche und durchgängige Lösung

Die Implementierung der Fernwartungslösung erfolgte zusammen mit genua und wurde innerhalb von zwei Wochen umgesetzt. Dabei konnten die vorkonfigurierten und getesteten Elemente aus dem Proof of Concept übernommen werden. „Mit dem genucenter als Management-Station administrieren wir alle Fernwartungs-Elemente an einer zentralen Stelle. So ist es relativ einfach, den Status im Blick zu behalten oder zusätzliche Hardware einzubinden“, berichtet Tobias Birk. Der IT-Security-Spezialist arbeitet in Stuttgart, das Rechenzentrum befindet sich in Würzburg und die „fernzuwartenden Systeme“ befinden sich in Bayern, Baden-Württemberg, Rheinland-Pfalz, Saarland und Hessen.

Die Daten von ca. 4 Mio. Versicherten der Deutschen Rentenversicherung Baden-Württemberg werden gut geschützt. Die Fernwartungslösung von genua hat sich in der Praxis als schnell, zuverlässig und sicher bewährt.

Für diese verteilten Strukturen benötigte die Dt.Re.Vers. ein differenziertes Rollenkonzept, um die Erfordernisse mehrerer rechtlich eigenständiger Nutzer erfüllen zu können. Auch die unterschiedlichen Sicherheitsbeauftragten sollten bei einem Audit nur Zugriff auf die Daten ihres Mandanten erhalten. Für die Vervollständigung der Fernwartungslösung hatte die Dt.Re.Vers. noch weitere Remote-Desktop-Anforderungen. Dazu gehörte die Möglichkeit, die Option eines Datentransfers konfigurierbar zu gestalten, um hier flexibel zu sein. „genua hat die Change Requests angenommen und nach unseren Wünschen umgesetzt“, so Birk. „Die Unterstützung und der Support von genua sind gut. Bei Bedarf haben wir immer einen Ansprechpartner und nicht nur ein anonymes Web-Ticket-System. Wenn es dringend ist, können wir weitere Eskalationsstufen nutzen.“

Die beteiligten Mitarbeiter der Dt.Re.Vers. mussten sich zunächst mit dem neuen System vertraut machen. Der Tenor war schließlich sehr positiv, weil die neue Lösung für alle Anwendungen einheitlich ist. Die Vielfalt an Methoden und Bedienoberflächen entfällt. Zusätzlich kann jeder Admin für seinen Bereich notwendige Details anpassen. So kann der Aufbau der SSH-Verbindung über Tools wie Putty oder einen Viewer von genua erfolgen. Der externe Wartungszugriff lässt sich über die Central Management Station zudem auf bestimmte Bereiche oder einzelne Systeme einschränken. Auch zeitlich kann die Nutzung auf definierte Tageszeiten beschränkt werden. Schließlich besteht die Möglichkeit, die Fernwartungs-Session in der Dauer zu beschränken. „Das ist wie früher die Kontrolle durch den Wachdienst. Wir definieren ein elektronisches Wachbuch und wissen jederzeit, wer noch anwesend ist und was der macht“, fasst Birk die Möglichkeiten zusammen.



Mit der Fernwartungslösung von genua erfolgen alle externen Verbindungen über einen Rendezvous-Server, der in einer Demilitarisierten Zone (DMZ) installiert ist. Eine Netzkoppelung findet nicht statt.

Gemeinsamer Betrieb der Lösung

Der Betrieb dieser zentralen Lösung erfolgt innerhalb der Region Süd Südwest der Dt.Re.Vers. bzw. im RZW-Verbund gemäß dem hier vorherrschenden Kooperationsmodell. Dies bedeutet konkret, dass sich die Dt.Re.Vers. BW und die Dt.Re.Vers. Rheinland-Pfalz den Betrieb teilen. Der Kontakt zu den externen Herstellern und Dienstleistern wird über einen Single Point of Contact zur Verfügung gestellt. Das Konzept ist völlig transparent. Alle autorisierten Benutzer sind in einer Auftragsdatenbank registriert. Hier ist auch hinterlegt, welche Berechtigungen sie jeweils haben.

Die externen Partner reagierten auf die neue Lösung zunächst sehr zurückhaltend. Der Hinweis auf die KRITIS-Anforderungen sorgte für mehr Verständnis. Schließlich konnte die extrem schlanke Lösung überzeugen. „Hersteller und IT-Dienstleister müssen keine zusätzliche Software installieren. Sie laden einen „portable Client“ herunter, spielen in diesem Client die seitens der Dt.Re.Vers. vordefinierte Konfiguration ein und der Client ist funktionstüchtig. Das war es schon“, so Birk.

Eine sichere Lösung für alle KRITIS-Anforderungen

Die Lösung mit dem Rendezvous-Konzept zur Einbindung externer Zugriffe hat sich bei der Dt.Re.Vers. in der Praxis als schnell, zuverlässig und sicher bewährt. Die Sicherheit aus der analogen Welt konnte erfolgreich auf die KRITIS-Infrastruktur übertragen werden.

„Die Fernwartungslösung ist einfach und sicher. Und wenn es einfach ist, wird es auch akzeptiert. Selbst wenn der Laptop eines externen Service-Technikers gestohlen wird, schafft er es sinngemäß nur bis auf den Parkplatz vor dem Gebäude. Das Innere des Gebäudes selbst ist sicher. Das ist Security by Default“, gibt der Leiter des Dt.Re.Vers.-Firewall-Kompetenzteams eine gute Bewertung der Security-Lösung.

Foto: Deutsche Rentenversicherung Baden-Württemberg Pressestelle

Beratungsgespräch in der Deutschen Rentenversicherung

Weitere Informationen:

www.genua.de/fernwartung

1023-14-DE

Über genua

Die genua GmbH ist Enabler der digitalen Transformation. Wir sichern sensible IT-Netzwerke im Public- und im Enterprise-Sektor, bei KRITIS-Organisationen und in der geheimschutzbetreuten Industrie mit hochsicheren und skalierbaren Cyber-Security-Lösungen. Dabei fokussiert sich die genua GmbH auf den umfassenden Schutz von Netzwerken, Kommunikation und interner Netzwerksicherheit für IT und OT. Das Lösungsspektrum umfasst Firewalls & Gateways, VPNs, Fernwartungssysteme, interne Netzwerksicherheit und Cloud Security sowie Remote-Access-Lösungen für mobile Mitarbeiter und Home Offices.

Die genua GmbH ist ein Unternehmen der Bundesdruckerei-Gruppe. Mit mehr als 400 Mitarbeitenden entwickelt und produziert sie IT-Security-Lösungen ausschließlich in Deutschland. Seit der Unternehmensgründung 1992 belegen regelmäßige Zertifizierungen und Zulassungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) den hohen Sicherheits- und Qualitätsanspruch der Produkte. Zu den Kunden zählen u. a. Arvato Systems, BMW, die Bundeswehr, das THW sowie die Würth-Gruppe.

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