



Ein Fast Response Center für die Energiewende

Für die Energiewirtschaft wird die Verfügbarkeit von energietechnischen Einrichtungen immer wichtiger. Deshalb arbeiten Betreiber und Dienstleister seit Jahren mit Fernwartung. Doch durch die steigende Komplexität der Netze und die zunehmende Bedrohung durch Cyberangriffe rückt die Sicherheit solcher Systeme zunehmend in den Fokus. Wie Fernwartung sicher und effizient betrieben werden kann, zeigt das Beispiel des Grid Automation Service von Hitachi Energy: Dort werden zwischen 80 und 100 Support Cases pro Monat bearbeitet, viele davon mit einem Remote-Zugang.

SICHERE FERNWARTUNG

von Frank Jablonski, freier Journalist

Es ist vielleicht das erste Mal seit der Industrialisierung, dass sich eine wesentliche Säule der Wirtschaft in Deutschland so dramatisch verändert, wie derzeit die Energielandschaft. Gleich mehrere parallele Treiber beschleunigen den Wandel: Vom Ausstieg aus der Kernenergie, über die Gasmangellage zu Beginn des russischen Angriffskrieges auf die Ukraine bis hin zum Klimawandel führen diese Ereignisse in der Summe zu einem noch nie dagewesenen Wachstum bei dezentralen Energiequellen und neuen, dezentralen Verteilnetzen. Und mit ihnen wachsen die Anforderungen an Stromproduzenten, Netzbetreiber und Zulieferer.

Projekt-Steckbrief

Der Kunde:

Hitachi Energy mit Hauptsitz in der Schweiz plant und realisiert Umspannwerke, Hochspannungs-Gleichstrom-Übertragungs-Verbindungen, Transformatoren-Stationen und zahlreiche weitere Anlagen der Energieversorgung.

Die Aufgabe:

Unterstützung von Hitachi-Kunden weltweit, die Support bei Alarmen und Fehlfunktionen oder Szenarien der Maschinenüberwachung, der Ferndiagnose oder des Remote Access benötigen.

Die Lösung:

genubox sichert den Fernzugriff auf die Kunden-Anlagen und erlaubt dem Anwender die vollständige Verbindungskontrolle in sein Netzwerk.

Einer der Technologieführer in der Energiewirtschaft ist Hitachi Energy

Das Unternehmen mit Hauptsitz in der Schweiz beschäftigt rund 45.000 Mitarbeiter in 90 Ländern und erwirtschaftet ein Geschäftsvolumen von rund 13 Milliarden US-Dollar Umsatz.

Kunden aus den Bereichen Energie, Industrie und Infrastruktur stehen alle vor derselben Herausforderung: In einer immer komplexer werdenden Welt die Energiewende hin zu einer klimaneutralen Zukunft voranzutreiben, ohne den Überblick zu verlieren. Das geht nur mit intelligenten Konzepten, eingebettet in eine sichere, weitgehend automatisierte und digitalisierte Struktur.

„Wir entwickeln das Energiesystem unserer Kunden weiter, um sie nachhaltiger, flexibler und sicherer zu machen und gleichzeitig mit wirtschaftlichen, ökologischen und sozialen Werten in Einklang zu bringen“, sagt Michael Joos. Er ist Chef des Collaborative

Operations Center, kurz COC, in Baden in der Schweiz. „Die Automatisierung und Flexibilisierung steht bei unserer Geschäftseinheit Grid Automation besonders im Vordergrund. Für unsere Kunden wird dabei ein Aspekt immer wichtiger: Die Verfügbarkeit der Anlagen und Netze“, ergänzt Joos.

Um diese zu maximieren, konzentriert sich Hitachi Energy mit seinem Grid Automation Service auf sechs Leistungsfelder:

- Intelligente Ersatzteilverhaltung und -versorgung
- Software- und Firmware-Unterstützung
- Maßgeschneiderte Schulungen
- Werkzeuge und Knowhow für eine präventive Instandhaltung
- Cyber-Security-Lösungen und
- Schnelle und flexible Unterstützung im Service-Fall.



Einrichtungen der Energieversorgung zählen zur kritischen Infrastruktur. Für Fernwartungszugriffe innerhalb seines Grid Automation Services vertraut Hitachi Energy auf die genubox-Technologie von genua.

Mehr als 40 Engineering- und Servicezentren liegen strategisch günstig um den Globus verteilt, um diese Themen zu bearbeiten und die Automatisierungs- und Kommunikationssysteme der Anwender aus mehr als 140 Ländern am Laufen zu halten. Geräte- und Systemschulungen sorgen dafür, dass das Betriebspersonal schnell und effizient reagieren kann. Wo das nicht reicht, identifizieren und analysieren Joos und seine Kollegen die Ursachen von Geräteausfällen und schlagen effektive Maßnahmen vor. Sie beraten in Bezug auf Ersatzteile, Upgrades und Nachrüstungen oder auch zu Fragen der Cybersicherheit.

Kurze Reaktionszeiten gefragt

Zeit ist Geld. Diesen Spruch hat jeder Anwender im Hinterkopf, wenn es in der Anlage klemmt. Herzstück für eine schnelle Fehlerbehebung und Ursachenanalyse ist die Customer-Connect-Center-Systematik, bei der jeder Kunde zum passenden Berater geroutet wird. Dragan Klisarić, Global COC Manager und somit verantwortlich für alle Collaborative Operations

Center weltweit, beschreibt den Aufbau: „Vergleichbar zu unserem COC hier in Baden gibt es sechs weitere Zentren, die so in den unterschiedlichen Zeitzonen platziert sind, dass unsere Experten rund um die Uhr ansprechbar sind. Im Support-Netzwerk arbeiten alle zusammen, wir tauschen Know-how untereinander aus und arbeiten nach dem Follow-the-Sun-Konzept zusammen.“

Viele Kunden, vor allem der kritischen Infrastruktur, nutzen Service Level Agreements, in denen sehr schnelle Antwortzeiten definiert sind. Je nach Vertrag können das ein, zwei Stunden sein, bis hin zu einem First Response von 15 Minuten. „Um solche Antwortzeiten zu erreichen, müssen verschiedene Bedingungen erfüllt sein. Zunächst einmal arbeiten wir zusammen mit den lokalen Einheiten. Sie kennen die Anlagen bereits sehr gut und müssen sich nicht erst langwierig einarbeiten. Wenn uns ein Kunde anruft, müssen wir nicht erst nachschauen, was der von uns gekauft haben könnte. Sondern wir wissen ganz genau, wer auf der anderen Seite sitzt, was sein System ist und wo die Probleme liegen könnten“, sagt Klisarić.

„Früher standen wir in der Warte, um an die Netzwerke zu kommen. Heute wird alles digital erfasst und der Zugang mithilfe intelligenter Sicherheitslösungen wie genubox über das Internet erledigt.“

Michael Joos, Chef des Collaborative Operations Center,
Hitachi Energy

Der Blick in die Anlage

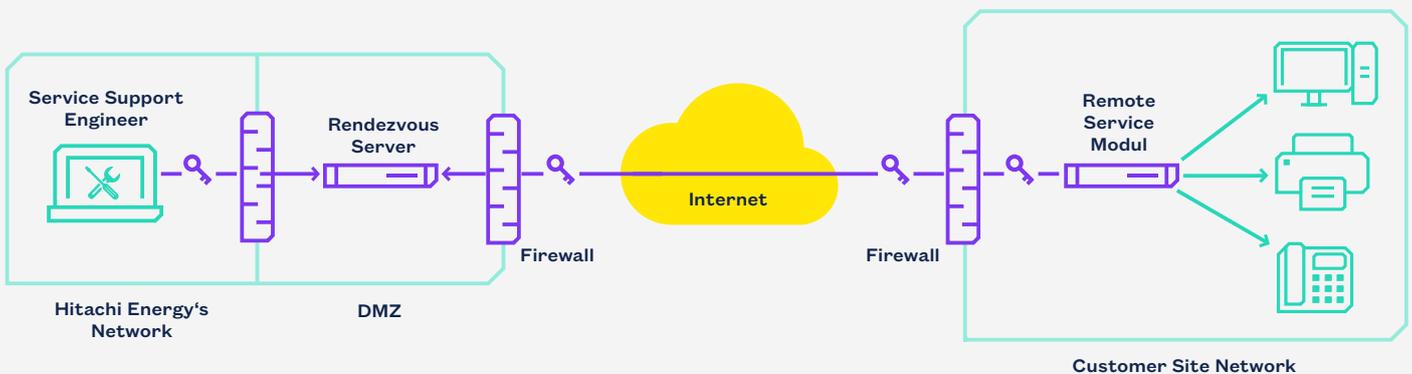
Um den Anwendern bei einem Notfall schnell helfen zu können, sind die Ingenieure und Techniker im Support darauf angewiesen, sehr schnell Informationen zu bekommen. Wie sieht es im System aus, welche Alarme gibt es, wie lauten Events in Logbüchern, können Informationen schnell heruntergeladen werden, Logfiles, Störschreiber-Einträge – das sind typische Fragen, die früher per Telefon und über E-Mail geklärt werden mussten. „Diese Zeiten sind glücklicherweise vorbei“ sagt Joos und ergänzt: „Das Entscheidende ist, dass wir heute eine sichere Möglichkeit haben, direkt auf das Kundensystem zuzugreifen. Unsere Service Level Agreements definieren, wer kann zugreifen, wann kann zugegriffen werden, auf welche Systeme kann man zugreifen. Dass das Ganze sicher abläuft, dafür sorgt unser Partner genua mit der genubox.“

Das Tochterunternehmen der deutschen Bundesdruckerei-Gruppe ist ein IT-Security-Unternehmen und Experte, wenn es darum geht, komplexe und

kritische, digitale Infrastrukturen zu schützen. Neben der Beratung und Software-Anwendungen ist es auch spezielle Hardware, mit der der entfernte Zugriff auf Anlagen sicher realisiert werden kann.

„genubox ist die Antwort auf die berechtigten Sicherheitsfragen unserer Kunden“, sagt Joos. „Sie löst unsere Herausforderungen in Bezug auf Remote-Engineering, Cyber Security, Anlagen-Zugriff aus der Ferne, oder Anbindung ans Internet. Wir nutzen sie als Servicebox und als Plattform für unterschiedliche Funktionalitäten.“

Wenn alle Wartungsverbindungen über die genubox laufen, ist die Anlage sicher und Anwender behalten die volle Kontrolle. Der Zugriff von außen erfolgt port- bzw. anwendungsgenau auf das vom Rest der Anlage isolierte Zielsystem. Es stehen dezidierte Rendezvous-Punkte zur Verfügung. Sie liegen beispielsweise in der Cloud oder in der sogenannten demilitarisierten Zone. Das sind Computer, die zwischen zwei Netzwerken liegen und diese durch strenge Zugriffsregeln voneinander abgrenzen.



Struktur der Fernwartung bei Hitachi Energy: Ohne die Lösung von genua wäre hier kein sicherer Zugang von außen zur Kundenanlagen möglich. Pro Monat werden zwischen 80 und 100 Support-Cases bearbeitet – etwa 5 % davon remote.

Alle Zugriffe stets im Blick

Dennoch: „Im Kundengespräch stellt sich immer wieder die Frage: Ist das sicher genug? Auch in Fällen, in denen wir unsere Partner davon überzeugen konnten, dass die Systematik sicher ist und dass sich bedeutende Vorteile ergeben, bleibt nicht selten Unsicherheit bestehen. Das geht so weit, dass der Anlagenzugriff auf einzelne Hitachi-Energy-Kollegen beschränkt ist, sonst darf niemand aus der Ferne in die Anlage“, sagt Joos. Auch hier bietet die verwendete Software und Authentifizierungslogik eine Lösung: Gängige Identitäts- und Zugriffsmanagementsysteme können angebunden werden und somit Benutzer und ihre Rechte einfach und zentral verwaltet werden.

Hilfreich für sehr sensible Bereiche ist neben der Verbindungskontrolle das Monitoring: Anwender können mithilfe von genubox sämtliche Wartungsarbeiten live über die Bedienoberfläche mitverfol-

gen und Videomitschnitte zur revisionsoptimierten Dokumentation erstellen. So sind Wartungsaktion, Zugriffszeitpunkt, Ziel und zugreifende Instanz in Echtzeit überwacht und zu jeder Zeit dokumentiert.

„Wir sind sehr zufrieden mit der genua-Technik und der Zusammenarbeit mit den Kollegen. Durch die Nutzung stellen wir gegenüber unseren Kunden sicher, dass der Remote Access nur durch autorisiertes Personal erfolgt, und können eine schnelle Reaktion zeigen, die den Namen ‚Rapid Response‘ verdient“, sagt Klisaric.

Mit Hilfe von genubox kann der Geschäftsbereich Grid Automation der Hitachi Energy seine Servicevereinbarungen auf die Bedürfnisse der Kunden zuschneiden. In Notfällen oder bei geplanten Betriebsunterbrechungen werden Reparaturen so zügig erledigt, damit die betroffene Anlage schnell wieder ihren Platz im Stromnetz und der Energiewende einnehmen kann.

„Es ist nicht nur Service, für den wir stehen, uns treibt auch das Thema Sustainability an.“

Dragan Klisaric, Global COC Manager, Hitachi Energy



Sichere Fernwartung – IT-Security made in Germany



Verschiedene Szenarien möglich

genubox vereint Fernzugriff, VPN-Zugang und Firewalling. Die Lösung ist zentral verwaltbar und erlaubt dem Anwender die vollständige Verbindungskontrolle in sein Netzwerk. Das Basismodul sichert mit seinen kryptografischen Grundfunktionen die wesentlichen Zugriffsarten ab. Das Applikationsmodul als Anwendungsplattform optimiert den sicheren Anlagenzugriff mithilfe individueller Einstellungen. So werden Szenarien der Maschinenüberwachung, der Ferndiagnose oder des Remote Access ermöglicht. Komplexe Tunnel für Application Service Providing wie Präventiv-Wartungssysteme sind ebenfalls denkbar. Messwerte und Zustandsinformationen können aufgezeichnet, verschlüsselt und in bestimmten Intervallen an den Wartungsdienstleister versendet werden.

Weitere Informationen:

www.genua.de/fernwartung



0325-04-DE

Über genua

Die genua GmbH sichert sensitive IT-Netzwerke im Public- und im Enterprise-Sektor, bei KRITIS-Organisationen und in der geheimhaltungsbetreuten Industrie mit hochsicheren und skalierbaren Cyber-Security-Lösungen. Dabei fokussiert sich das Unternehmen auf den umfassenden Schutz von Netzwerken sowie auf die interne Netzwerksicherheit für IT und OT. Das Lösungsspektrum umfasst Firewalls und Gateways, VPNs, Fernwartungssysteme, interne Netzwerksicherheit und Cloud Security bis hin zu Remote-Access-Lösungen für mobiles Arbeiten.

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 in 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

