In Kooperation mit

genua.

T Security

Sichere Fernwartung

mit Magenta Secure Industrial Remote Access Service (MSIRAS)

Connecting your world.

INHALTSVERZEICHNIS

ZUSAMMENFASSUNG

In der Fertigungs- und Prozessindustrie sind externe Zugänge für Wartungszwecke weit verbreitet. Zunehmende Automatisierung und Digitalisierung haben die Komplexität der Anlagen und Systeme steigen lassen – und die Nachfrage nach Remote-Lösungen für die Fernwartung durch Hersteller und externe Dienstleister erhöht. Cyberkriminelle wissen das: Laut BSI zählt das Eindringen über solche Fernwartungszugänge zu den besonders kritischen und am häufigsten auftretenden Bedrohungen für die Anlagensicherheit – mit steigender Tendenz.

Fernwartung mit MSIRAS sicher gestalten

Nicht zuletzt deswegen hat die EU die NIS-2-Richtlinie zur Stärkung der Cybersicherheit verabschiedet. Anfang 2026 ist sie als nationales deutsches Gesetz in Kraft getreten. Dies und die zunehmenden Schäden durch Cyberkriminalität treiben die Nachfrage nach sicheren Fernwartungslösungen und begleitenden Managed Services. Magenta Secure Industrial Remote Access Service, kurz MSIRAS, adressiert diesen Bedarf: In der vertrauenswürdigen Gesamtlösung „Made in Germany“ führen die Deutsche Telekom Security GmbH und die genua GmbH ihre Expertise zusammen.

MSIRAS zeichnet sich aus durch

- die hochsichere, für den Einsatz in der Industrie konzipierte **Fernwartungslösung genubox** mit der zentralen Management Lösung genucenter,
- eine vertrauenswürdige, **in Deutschland gehostete Virtual Private Cloud (VPC)**,
- umfassende **Managed Security Services** sowie
- ein hohes Maß an **Souveränität**: Hardware, Software, Verschlüsselung und Betrieb stammen aus Deutschland

MSIRAS kombiniert für den sicheren Fernwartungszugang Expertenwissen, Hard- und Software sowie eine dedizierte Virtualisierungsumgebung für jeden Kunden. Dazu gehören die Rendezvous-Server genubox von genua mit dem zugehörigen Central Management System genucenter und die Virtual Private Cloud (VPC) innerhalb der T Cloud Public.

Die VPC ist innerhalb der Cloud komplett von den Instanzen anderer Mandanten getrennt. Die Rendezvous-Architektur von genubox stellt sicher, dass ausschließlich authentisierte Anwender Zugriff auf vorher spezifizierte Dienste und Zielsysteme erhalten. Zusätzlicher Schutz entsteht dadurch, dass der Zugriff nur zu einem vereinbarten Zeitpunkt und für einen vorgegebenen Zeitraum in einem begrenzten Anlagenbereich (z.B. einer Maschine) stattfinden darf. Dazu nutzt genubox ein feingranulares, ausgereiftes Rechte- und Rollensystem. Daher eignet sich MSIRAS für eine sehr gezielte Zugriffssteuerung bis hin zur Implementierung von Zero-Trust-Konzepten. Die Lösung ermöglicht ferner eine SIEM-Anbindung und bietet Logging-Funktionen sowie eine Video-Aufzeichnungsfunktion für eine revisionsoptimierte Dokumentation aller Wartungsarbeiten.

MSIRAS auf Basis von genubox unterstützt den Anwender bei der zentralen Verwaltung von Fernwartungszugängen mit vollständiger Kontrolle über Wartungsaktion, Zugriffszeitpunkt, Ziel und die zugreifende Instanz. Betreiber können die Fernwartungslösung je nach Anforderungen komplett an die Deutsche Telekom Security auslagern oder im Rahmen eines Shared Managements über einen separaten Management-Tunnel teilweise selbst übernehmen.

[1] Siehe auch SANS five critical controls for ICS: https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls

Die Herausforderung:

CYBERSICHERHEIT IM INDUSTRIELLEN UMFELD

Kontrolle zurückholen, souverän agieren

Die Deutsche Telekom Security GmbH und die in München ansässige genua GmbH bieten eine gemeinsame IT-Sicherheitslösung für Industrie-Unternehmen in Deutschland an: MSIRAS.

75% der vom Digitalverband Bitkom befragten Unternehmen sind bereits Opfer von digitalem Diebstahl ihrer Geschäftsdaten geworden. Deutlich mehr als zwei Drittel musste bereits digitale Sabotage in ihrem Betrieb erleben und bei 60% wurden E-Mails mitgelesen oder andere Kommunikationsformen ausspioniert. Dieser wirtschaftliche Schaden summiert sich auf 267 Milliarden Euro pro Jahr. Geld, das nicht für Innovation, Instandhaltung oder Ausbildung zur Verfügung steht.

Quer durch Wirtschaft und Verwaltung sind unzählige Organisationen betroffen. Gleichzeitig verschieben sich die Verhältnisse zugunsten der kriminellen Angreifer: Automatisierung, Digitalisierung und vernetzte (I)IoT nehmen zu, und kaum eine Maschine oder ein Messgerät kommt noch ohne Netzwerkzugang in die Betriebe. Zudem müssen Angreifer durch den Einsatz von KI-Tools bei ihren Angriffen immer weniger Automatisierung-Know-how besitzen, um „erfolgreich“ zu sein. Hierbei kommen statt Schadsoftware immer öfter normale Engineering-Werkzeuge zum Einsatz. Dies erschwert das Erkennen solcher Angriffe.

Der Hintergrund wird bei einem Blick in die Fertigungshallen und Produktionsanlagen deutlich. Betriebs- und Geschäftsleiter müssen Anlagen und Prozesse stetig optimieren und vor allem rund um die Uhr am Laufen halten. Die Folge ist: Anlagen werden immer komplexer. Über Automatisierung und Digitalisierung wird versucht, dem Fachkräftemangel zu begegnen und Kostenstrukturen im Griff zu behalten. Beispiel Predictive Maintenance: Um Ausfallzeiten so gering wie möglich zu halten, werden mehr und mehr Assets mithilfe von intelligenter Software überwacht und noch vor einem sich abzeichnenden Ausfall gewartet. Aber auch bei der klassischen Wartung sowie bei Sicherheitsupdates, Fehlermeldungen oder defekten Bauteilen sind aufgrund der Komplexität der Geräte immer häufiger die Experten des Herstellers gefragt.

Schnelle Instandhaltung durch Fernzugriff

Damit die wenigen, verfügbaren Fachkräfte die Probleme schnell und ohne Reisetätigkeit analysieren und beheben können, ist oft ein administrativer Zugriff von außen auf die Anlagen notwendig. Einige Fehler lassen sich zum Beispiel durch korrigierte Einstellungen oder ein Firmware-Update lösen. Komplexere Eingriffe können per Fernzugriff analysiert und eine Ersatzteilbeschaffung effizient vorbereitet sowie die Instandsetzung angeleitet werden. Hier bieten viele Hersteller eigene Lösungen und Service-Pläne bis hin zu Pay-per-Use- oder Equipment-as-a-Service-Modellen an, die einen Zugriff von außen auf Maschine und Anlage z.B. über eine IoT-Plattform voraussetzen.

Werden detaillierte Prozessdaten und Geräteparameter zur Analyse an eine externe KI gesendet (Open-Loop-Szenario), müssen diese vor Diebstahl und unautorisierter Manipulation geschützt werden. Aus der Sicht des Anwenders wird ein weiteres wesentliches Problem deutlich: Angesichts der vielen unterschiedlichen Lieferanten ist es praktisch unmöglich, alle externen Fernwartungssysteme zu bewerten und ihre Sicherheitsstandards zu überwachen. Jeder einzelne Hersteller mit einem solchen System müsste in Abständen überprüft werden. Ist die Lösung sorgfältig konfiguriert? Wird sie regelmäßig aktualisiert und überwacht? Ist der Zugriff auf die Fernwartung beschränkt und werden sämtliche Daten verschlüsselt übertragen? Angesichts der beschriebenen Sicherheitslage sollten alle diese Fragen mit Ja beantwortet werden können.

Phishing-Attacken öffnen Einfallstore

Zwar finden viele Angriffe auf OT-Assets indirekt über die IT-Systeme der Firmen statt. Jedoch sind es oft die Fernwartungszugänge, die als initialer Angriffsvektor genutzt werden. Besonders, wenn es sich um „historisch gewachsene“ Provisorien handelt, die rund um die Uhr aktiv sind und zudem noch schlecht oder gar nicht überwacht werden. Nicht selten sind es VPN-Lösungen, die ohne Beschränkung im IT- oder OT-Netzwerk existieren. Eingerichtet in der Not eines Anlagenstillstandes, um einen Fehler mit externer Hilfe schnell und in gutem Glauben zu beheben. Nach Phishing-Attacken öffnen unsichere Remote-Zugänge weitere typische Einfallstore wie infizierte Engineering-Workstations, Laptops oder mobile Datenträger. Experten beobachten zudem Lieferkettenangriffe. Hier hat sich der Kriminelle über den Umweg eines Angriffs auf die Software des Lieferanten Zugang zur eigentlichen Produktionsanlage verschafft.

Die schlechte Nachricht lautet: Die Angriffe werden immer ausgefeilter und die Kriminellen lernen dazu. Strukturen, Logiken und Bezeichnungen sind kein Hoheitswissen mehr. Auch künstliche Intelligenz hilft leider, komplexer werdende Angriffe zu strukturieren und fehlendes OT-Know-How auszugleichen. Auch ist mittlerweile gut dokumentiert, dass unfreundliche staatliche Stellen Angriffe mit Personal und Ressourcen unterstützen – man spricht mittlerweile von Cyber-Warfare, also kriegsähnlichen Zuständen im virtuellen Raum. Die Dringlichkeit beim Thema Cybersicherheit für die Produktion und kritische Infrastruktur nimmt daher rasant zu.

Das hat auch die Europäische Union erkannt und in ihrer zweiten Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2) den verpflichtenden Schutz kritischer Infrastrukturen angeordnet. Unternehmen und Organisationen aus den Bereichen Energie, Wasser, Verkehr, Gesundheit, Banken und digitale Infrastruktur müssen seit Oktober 2024 auch in Deutschland Mindeststandards für Cybersicherheit einhalten. Bei Verstößen drohen empfindliche Strafen: Bußgelder bis zu 10 Millionen Euro oder 2% des Jahresumsatzes und sogar die persönliche Haftung der Geschäftsleitung stehen auf dem Spiel.

Checkliste: NIS-2-ready werden

- *prüfen, ob das Unternehmen unter NIS-2-Zuständigkeit fällt*
- *Verantwortlichkeiten und Zuständigkeiten inhouse klären*
- *Cybersicherheitsmaßnahmen auf Lücken prüfen (lassen)*
- *Prozesse zur Vorfallserkennung und -meldung etablieren*
- *externe Dienstleister bewerten und absichern*
- *Kontakt zur Aufsichtsbehörde vorbereiten (z.B. BSI)*

Um Unternehmen in Deutschland, Europa und darüber hinaus, Kosten und Ärger zu ersparen, bietet die Deutsche Telekom Security (DTS) auf Basis der Technologie von genua ein Dienstleistungsangebot für die industrielle Fernwartung an. Das vorliegende Whitepaper beschreibt die Funktionsweise von MSIRAS (Magenta Security Industrial Remote Access Service). Kernkomponente der Lösung ist die genubox. Sie stellt sicher, dass nur befugte Personen Zugriff auf sensible industrielle Netze erhalten. In Deutschland und speziell für industrielle Umgebungen entwickelt, erfüllt sie alle Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) an eine sichere Fernwartung.

NIS-2 stellt dezidierte Anforderungen an Betriebe

Bereich	Anforderungen unter NIS-2
Risikomanagement	Identifikation und Absicherung von IT- und OT-Systemen
IT-Sicherheitstechnologien	Firewalls, Zugangskontrollen, Verschlüsselung, Backup, Monitoring
Incident-Response	Verfahren zur Reaktion auf Sicherheitsvorfälle
Meldung von Vorfällen	Erste Meldung schwerwiegender Cybervorfälle innerhalb von 24 Stunden
Business Continuity	Notfallpläne, Wiederherstellungsverfahren
Lieferketten-Sicherheit	Absicherung von Dienstleistern und Partnern
Governance	Verantwortung der Unternehmensleitung, z.B. durch Aufsichtspflichten
Dokumentation & Audits	Nachweisbarkeit der Sicherheitsmaßnahmen

DIE LÖSUNG:

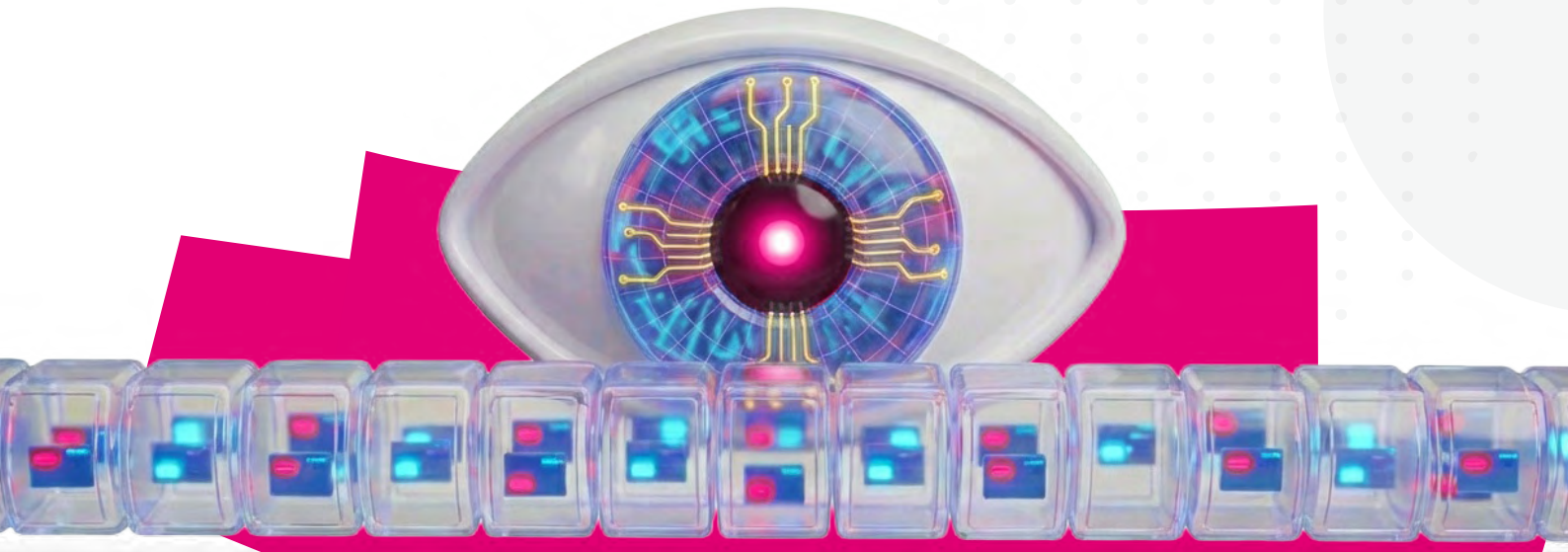
MSIRAS – Mehrwert durch Kooperation

Die Säulen der Sicherheit

Cybersicherheit ist kein Sprint: Lösungen, die Betriebe im Zusammenhang mit der Fernwartung adäquat absichern, müssen aus verschiedenen Säulen bestehen. Dazu gehört eine Multi-Faktor-Authentifizierung der Nutzer ebenso wie granulare Zugriffsrechte jedes einzelnen Teilnehmers und die Isolation des Fernwartungsziels. Nur notwendige Tätigkeiten und nur die Bereiche in der Anlage, die zur Erfüllung einer Aufgabe notwendig sind, sollen auch erreichbar sein. Dass ein langer Atem gefragt ist, zeigt auch ein weiterer wichtiger Punkt: Die revisionssichere und datenschutzkonforme Aufzeichnung der Tätigkeiten während des Fernzugriffs. Ein Punkt, der in der pharmazeutischen Industrie schon lange gelebt wird und in anderen KRITIS-Bereichen vermehrt Einzug hält.

Ein weiterer Aspekt ist die Vergangenheitsbewältigung: Die Betriebe sollten unbedingt alte, nicht mehr genutzte oder provisorische Zugänge identifizieren und sukzessive auf eine konforme Lösung migrieren. Diese „historischen“ oder „vergessenen“ Zugänge müssen zeitnah zurückgebaut werden, da gerade solche vergessenen Zugänge in der Vergangenheit erfolgreiche Angriffspfade für den initialen Schritt von Angreifern waren.

Unternehmen vor allem aus den KRITIS-Bereichen können sich nicht mehr erlauben, das Thema der Cybersicherheit nicht auf höchstem Niveau zu betreiben. Dafür sind die Risiken zu hoch. Und die Bedrohungen wachsen: KI-basierte und automatisierte Angriffsszenarien werden stark zunehmen, prognostizieren Experten. Und auch der Einsatz von Quantencomputern für strafbare Zwecke dürfte wahrscheinlicher werden.



Empfehlungen des BSI erfüllt

Angesichts der drohenden Schäden durch Cyberangriffe und der möglichen Strafen im Zusammenhang z.B. mit der NIS-2-Regulierung wählen viele Unternehmen die hochsichere Fernwartungslösung genubox. Sie wurde von den IT-Sicherheitsspezialisten der genua GmbH – ein Unternehmen der Bundesdruckerei-Gruppe – speziell für industrielle Umgebungen entwickelt. Zusammen mit dem genucenter, das wie eine Leitstelle für ein Netzwerk aus Sicherheitsgeräten fungiert, erfüllt sie alle Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) an eine sichere Fernwartung. Beide Produkte sind als virtuelle Maschinen für den Betrieb im eigenen Rechenzentrum oder in Cloud-Umgebungen erhältlich.

Für diejenigen Betriebe, die auch bei Planung, Einrichtung, Migration von Legacy-Lösungen und Betrieb Unterstützung von Sicherheitsexpertinnen und -experten nutzen möchten, bietet sich das neue Managed-Service-Paket für die sichere Fernwartung in der Industrie (Industrial RAS) an. Es kombiniert die sicheren Fernwartungslösungen von genua mit begleitenden Managed Services der Deutschen Telekom Security GmbH.

> ***Mit MSIRAS können Unternehmen schnell eine Grundschutz-konforme Fernwartung aufbauen, deren Infrastruktur von der Cloud bis hin zur Schnittstelle am Kundenstandort vollständig von der Telekom betrieben wird.***
>
> - Markus Maier, Product Owner für Industrieprodukte bei genua

Leistungsangebot von MSIRAS

Der Magenta Secure Industrial Remote Access Service – kurz MSIRAS – implementiert für Anwender dedizierte, virtuelle genua Komponenten der Lösung in einem deutschen Rechenzentrum der Telekom. Diese VPC (Virtual Private Cloud) Instanz erfüllt höchste Datenschutzstandards und garantiert DSGVO-konforme Sicherheit – frei von außereuropäischen Einflüssen. Durch georedundante Rechenzentren, höchste Verfügbarkeitsstandards und regelmäßige unabhängige Prüfungen bietet sie maximale Betriebssicherheit.

Zum Managed Service MSIRAS gehören darüber hinaus folgende Leistungen für die unterschiedlichen Phasen eines Projektes:

- Fachvertrieb/Presales: Expertinnen und Experten beraten, wie eine Lösung aussehen könnte, erstellen ein Grobkonzept und geben Vorschläge für Größe und Ausgestaltung der Services.
- Durchführung von Proof of Concepts: An einem Pilot-Standort kann die Lösung testweise betrieben werden.
- Planung: In dieser Phase wird die Integration durch das Projektmanagement vorbereitet.
- Installation: Sowohl bei der Konfiguration, als auch beim Cloud-Deployment und der On-site-Installation stehen Fachkräfte der Deutschen Telekom zur Verfügung.
- Dabei haben Anwender die Wahl zwischen zwei Service-Leveln:
  - S72 bietet eine Terminvereinbarung innerhalb von acht Stunden und eine Entstörfrist innerhalb 72 Stunden. Das entspricht einer 99,17%igen Verfügbarkeit im Jahr.
  - Noch schneller ist der S24-Service-Level, der 24/7 eine Terminvereinbarung innerhalb von zwei Stunden und eine Entstörfrist innerhalb 24 Stunden bietet. Das entspricht 99,72% Verfügbarkeit im Jahr.

Der technische Kern:

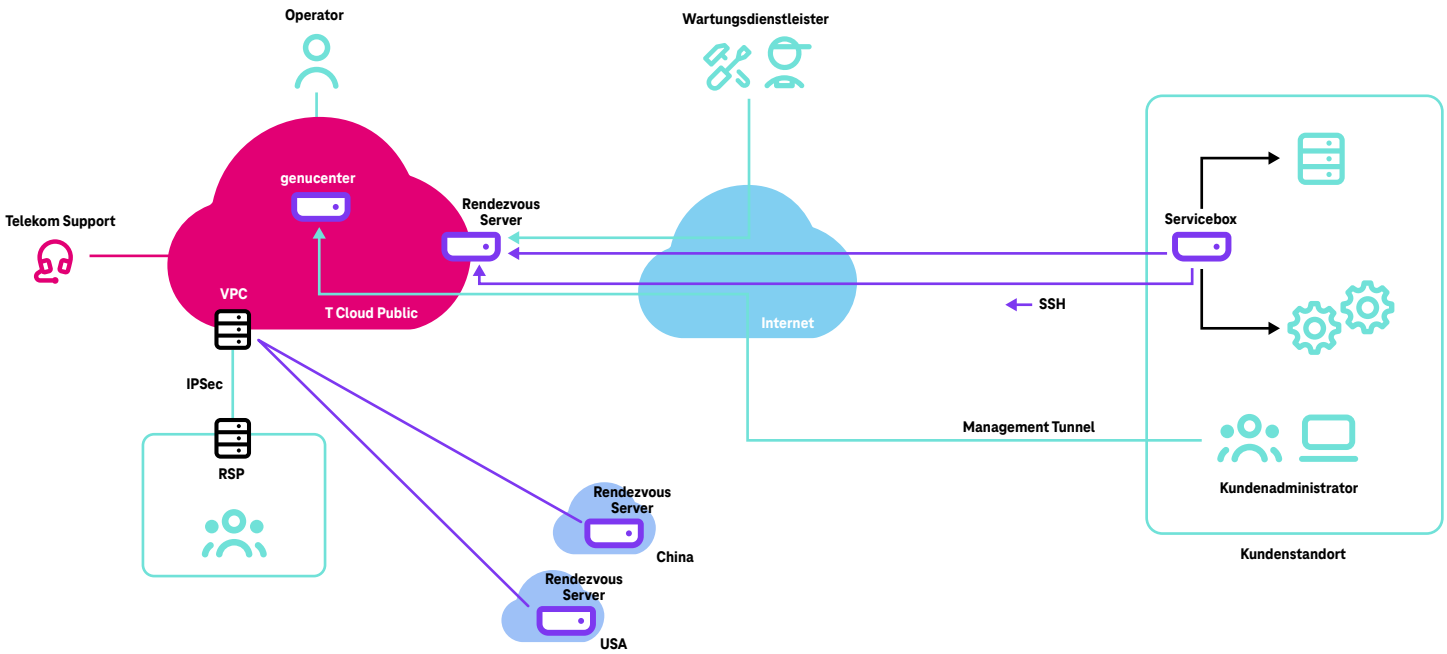
GENUBOX UND GENUCENTER

Die Rollenverteilung bei MSIRAS ist klar geregelt. Die Deutsche Telekom Security unterstützt mit ihren mehr als 1.800 Sicherheitsexpertinnen und -experten Kunden je nach Anforderungen bei der Realisierung des Fernzugriffs – von der Grobplanung der Architektur und Prüfung der Standortvoraussetzung über die Integrationsplanung und Migration bis hin zum Betrieb inklusive CERT-Management und Überwachung.

Die Rendezvous-Lösung von genua bildet den technischen Kern des Konzeptes. Sie stellt sicher, dass es keine einseitigen Zugriffe vom externen Fernwartungs-Dienstleister gibt. Verbindungen in die Anlage zur Analyse oder Wartung müssen über einen Rendezvous-Server abgewickelt werden, der in einer sogenannten demilitarisierten Zone (DMZ) implementiert wird. Zu diesem Treffpunkt bauen der externe Instandhalter und ein Verantwortlicher auf Seite des Betreibers, auf Anfrage, eine Verbindung auf. Mit diesem aktiven Schritt des Anwenders entsteht die durchgängige Verbindung, die zum Informationsfluss der Wartungszwecke notwendig ist. Maschinenwerte und Fehlermeldungen können anschließend ausgelesen und bearbeitet werden. Dabei bleibt der Zugriff zeitlich und räumlich beschränkt. Der externe Service bewegt sich nur im zuvor definierten Zielsystem und Rollenbild. Hierzu nutzt genua das robuste und sichere SSH-Protokoll.

Security-by-design

Vorbeugen ist besser als Nachsorgen. Aus diesem Grund verfolgt der genua-Ansatz das Security-by-Design-Prinzip. Dabei wird die sichere Architektur mit den dazu gehörigen Abläufen und Verhaltens- und Bedienregeln in der ersten Konzeptphase festgelegt und in alle Aspekte der weiteren Entwicklung eingebunden. So entsteht eine Einheit aus technischen Schutzmaßnahmen und organisatorischen Prozessen und Prinzipien. Durch diese Maßnahmen wird sichergestellt, dass potenzielle Schwachstellen frühzeitig erkannt und behoben werden. Im Ergebnis laufen die Systeme stabil und zukunftssicher; Risiken werden minimiert und Daten geschützt.



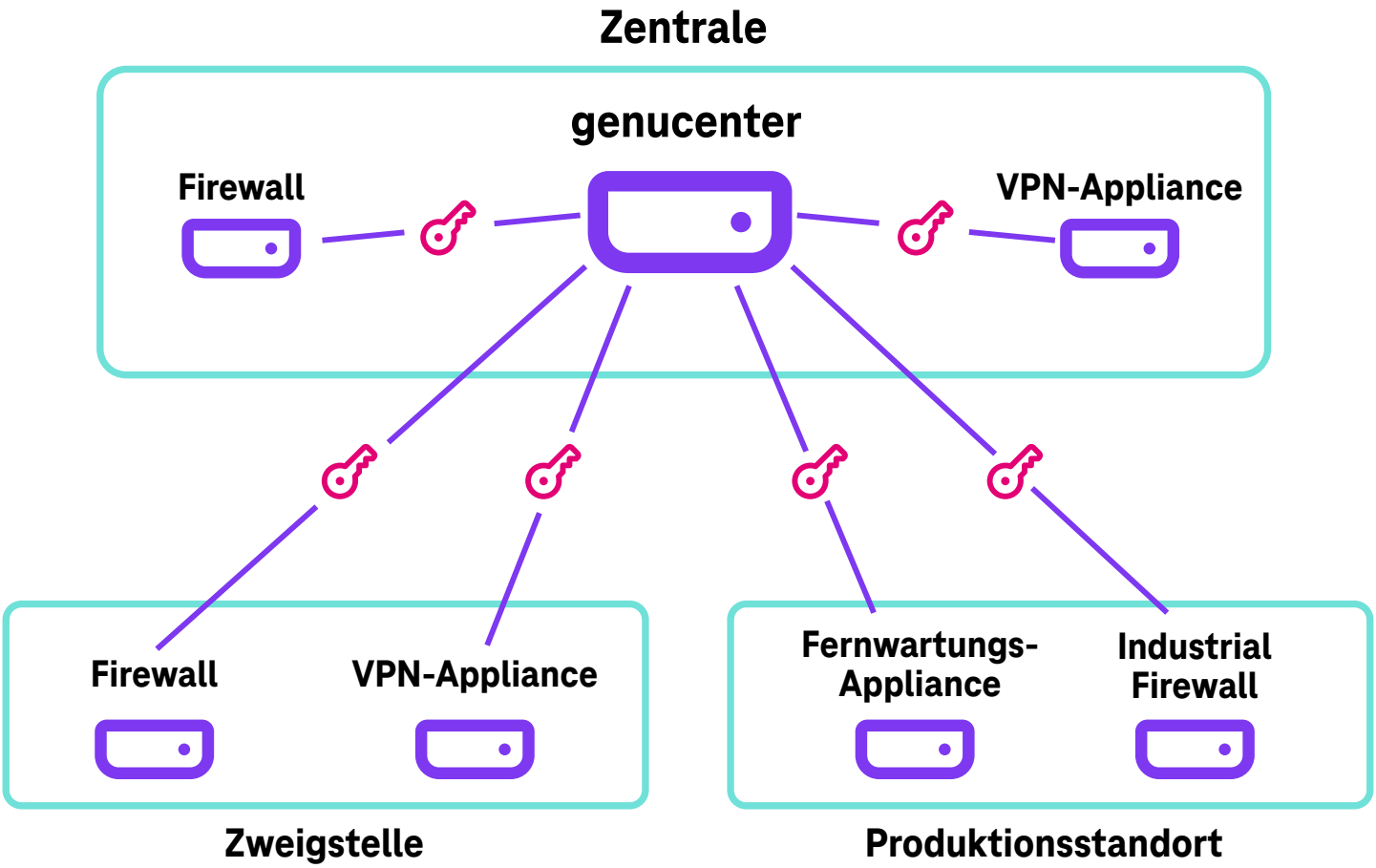
Schematischer Ablauf einer Fernwartung: Der Wartungsdienstleister darf nach Freigabe durch den Operator im Rendevouz-Server über die Servicebox auf die zu wartende Maschine zugreifen.

Komplexe Strukturen übersichtlich darstellen

Die Central Management Station (CMS) genucenter ist die Steuerzentrale im MSIRAS-Konzept. Sie hilft den Verantwortlichen, den Überblick zu behalten und mit einfach formulierten Fernwartungsregeln, die komplexen technischen Vorgänge der Plattform wie zum Beispiel die Verteilung der kryptographischen Schlüssel oder die lokale Konfiguration der Firewall-Regeln an den dezentralen Standorten, effizient und sicher zu verwalten. Statt jedes Gerät einzeln zu konfigurieren, kann man von einem zentralen Ort aus Updates einspielen, Einstellungen vornehmen, Geräte überwachen, Störungen erkennen und Berichte erzeugen.

Ein wichtiges Merkmal von genucenter ist das hierarchische Management. Auch komplexe Strukturen werden granular abgebildet. Von der Firmenzentrale bis hinunter zu einzelnen Abteilungen an verschiedenen Standorten wird die Berechtigungsstruktur nach ihrem Organigramm dargestellt.
Für die unterschiedlichen Bereiche können individuelle Benutzerrechte definiert werden, z.B. welche Engineering-Rolle mit welchen Rechten auf bestimmet OT-Assets, zu welchen Zeiten zugreifen darf.

Alternativ können Systeme in einer Baumstruktur zusammengefasst werden, um Konfigurationen ohne großen Aufwand zu vererben. Darüber hinaus können unternehmensweite Regeln festgelegt werden. Die zentrale und übersichtliche Verwaltung hilft, auch komplexe Regelwerke kontrolliert durchzusetzen, ohne die Verfügbarkeit der Produktion zu gefährden.



Struktur des genucenters: Firewalls und Zugriffe auch komplexer Strukturen können zentral verwaltet werden.

DAS ABLAUFBEISPIEL:

Sichere Wartung mit Remote Access Service

Der sichere Wartungsvorgang läuft nach einem klaren Muster ab: Nachdem im Vorfeld Rechte und Aufgaben geklärt wurden, baut der Wartungsdienstleister im betrieblichen Wartungsfall zunächst mit dem RAS-Service über das Internet mit Hilfe der Secure-Fernwartung-App einen gesicherten SSH-Tunnel zu einem Treffpunkt im System (dem Rendezvous Server) auf. Dieser virtuelle Ort wird beispielsweise in der T Cloud Public bereitgestellt. Die Verbindung ist verschlüsselt und über eine Zweifaktor-Authentifizierung vor unbefugtem Zugriff gesichert. Zwar kann das Treffen auch ohne App stattfinden, z.B. unter Nutzung des nativen SSH-Protokolls, doch bietet sich die Windows-Anwendung zur einfacheren Bedienung an. Die App hilft sowohl dem Wartungsdienstleister als auch dem Operator bzw. Maschinen-Administrator dabei, die Fernwartungsbeziehung zu starten, zu verwalten und zu beenden.

Die jeweilige Konfiguration des Fernwartungseinsatzes wird zentral auf genucenter ausgeführt, dem Central Management System. Auch dieses läuft auf der T Cloud Public. Um die Aufwände auf Seiten der Nutzerinnen und Nutzer so gering wie möglich zu halten, bietet genucenter zudem die Möglichkeit, sich über Identity Provider (IdP) wie Microsoft Active Directory, Keycloak, Okta oder Azure AD anzumelden. Im IdP sind Benutzerinformationen, Gruppenzugehörigkeit, Rollen und Berechtigungen hinterlegt und verwaltet. Nach erfolgreicher Anmeldung gibt der IdP eine digitale Bestätigung weiter, z.B. in Form eines OIDC-Tokens.

Neben den Software-Komponenten in der VPC gehört zur MSIRAS auch die Implementierung der Hardware genubox (im Schaubild Servicebox genannt). Im Netzwerk des Anwenders wird sie für die zu betreuenden Systeme installiert. An dieser Hardware werden Fernwartungsverbindungen zum Netzwerk bzw. zur zu wartenden Industrieanlage terminiert.

Nach beendeter Arbeit, oder auch live während des Zugriffs, kann der Operator darüber hinaus per Videoaufzeichnung die Arbeiten nachvollziehen und so überwachen. Falls etwas nicht korrekt ablaufen sollte, ist er jederzeit in der Lage, die Zugriffsrechte wieder zu entziehen.

Vergleich:

MSIRAS VS. KLASSISCHE VPN

Kriterium	VPN-Zugang (klassisch, z.B. OpenVPN/IPSec)	Magenta Security Industrial RAS (MSIRAS)
Sicherheitsniveau	Abhängig von Konfiguration; Angriffsfläche bei offenen Ports	Sehr hoch, vor allem durch das Zero-Trust-Prinzip, verbindungsinitiierte Kommunikation und genubox als sicherer Anker
Verbindungsaufbau	Manuell oder automatisch, meist über öffentliche IP oder dynamische DNS und Portweiterleitung (die ein Sicherheitsrisiko darstellen können)	Outbound-only: Es werden keine Ports geöffnet, die Verbindung wird von der genubox als Rendevouz-Server von innen heraus aufgebaut, es gibt keine offene Eingangsverbindung
Zugriffskontrolle	Meist über Benutzername und Passwort oder Zertifikate	Granulare Zugriffssteuerung auf einzelne Anlagen, Nutzer, Zeitfenster; Rollen- und Rechtekonzept
Auditierbarkeit & Logging	Eingeschränkt oder abhängig vom VPN-Server	Lückenloses Protokollieren aller Fernzugriffe, revisionssicher und DSGVO-konform
IT-Sicherheitsintegration	Eigenverantwortung (Firewall, Updates, etc.)	Gemanagt durch Telekom Security inkl. regelmäßiger Wartung und Updates
Industrie- & OT-Kompatibilität	Oft schwierig bei komplexen Netzwerken: da nur die IP-Ebene getunnelt wird (Layer 3), funktionieren bestimmte industriell genutzte Protokolle z.B. zur Maschinensteuerung nicht	Speziell für OT-Netzwerke konzipiert; unterstützt auch komplexe industrielle Protokolle
Skalierbarkeit	Ja, aber mit Aufwand verbunden, da Zertifikate und Nutzerprofile angelegt und gepflegt werden müssen	Zentral verwaltbar, mandantenfähig, leicht skalierbar für viele Nutzer und Standorte
Zugriffsfreigabe	Oft dauerhafter Zugang	Temporäre, genehmigungsbasierte Freigaben durch Anlagenbetreiber möglich
Endgeräte-Anforderungen	VPN-Client erforderlich	Webbasierter Zugriff möglich, zusätzliche Clients bei Bedarf (z.B. für Maschinenhersteller)
Hosting und Betrieb	Kann auf interner Hardware oder in der Cloud betrieben werden. Im Eigenbetrieb verantwortlich für Installation, Updates, Nutzerverwaltung, Sicherheitskonfiguration und Überwachung/ Wartung	Gehostet in deutschen Rechenzentren der Telekom, mandantenfähig, leicht erweiterbar über das zentrale Management, 24/7-Support von Experten
Kostenmodell	Geringe Lizenzkosten, aber hoher interner Aufwand	Monatliche/jährliche Gebühren, service-basiert, spart interne IT-Kosten

MIT SICHERHEIT ZUM ERFOLG

MSIRAS unterstützt Sie dabei, eine KRITIS/NIS-2-konforme Fernwartung aufzubauen. Die Partner genua GmbH und Deutsche Telekom Security GmbH ergänzen sich dabei zu einem Full-Security-Paket.

Ihre Vorteile auf einen Blick:

- Fernzugriff, VPN und Firewalling in einer Lösung
- Zentrale Verwaltung mit jederzeit vollständiger Kontrolle über Wartungsaktion, Zugriffszeitpunkt, Ziel und zugreifende Instanz
- Hohe Betriebssicherheit durch Bestätigung der Verbindungsaufnahme von innen, z.B. per Windows-App oder Schlüsselschalter (über potentialfreien Schaltkontakt an der genubox)
- Sicherheitsniveau an Bedarf anpassbar, „offener“ und fortlaufender Zugriff bis hin zu vollständiger Kontrolle
- Ausgefeiltes Corporate-ready Rechte- und Rollensystem für hunderte Fernwarter weltweit
- Höchste Sicherheit und Kontrolle durch portgenauen Zugriff auf das vom Rest der Anlage isolierte Zielsystem sowie Rendezvous-Punkt in der DMZ oder in der Cloud
- Video-Aufzeichnungsfunktion und Logging
- Vertrauenswürdige, in Deutschland gehostete Virtual Private Cloud (VPC)
- Unterstützung von Planung, Integration und Migration bis hin zu Betrieb inkl. CERT-Management
- Umfassende Managed Security Services: Konfiguration der Fernwartungslösung kann komplett an die Deutsche Telekom Security ausgelagert werden

> *Im Jahr 2025 wurden in der Produktion mehr Sicherheitsvorfälle durch schlecht implementierte oder überwachte Remote-Zugänge verursacht, als durch Ransomware-Vorfälle. Dabei sind robuste, funktionierende Lösungsarchitekturen für einen sicheren Remote-Zugriff seit Jahren bekannt. Das Problem ist also kein technisches – wir müssen uns verstärkt um die organisatorische Seite kümmern.*
>
> - Bernd Jäger, Practice Lead Industrial & IoT Security, Deutsche Telekom

Setzen Sie auf sichere Fernwartung!

Gern beraten wir Sie dazu, wie Sie sichere Fernwartung implementieren können. Weitere Informationen zu OT Security finden Sie auch hier.

Kontakt
security.dialog@telekom.de
security.telekom.de

Herausgeber
Deutsche Telekom Security GmbH
Office Port 1
Friedrich-Ebert-Allee 71–77
53113 Bonn

Connecting your world.

Deutsche Telekom Security GmbH | 03/2026