genua.

VS-NfD-Fernwartung

Hochsicherer Fernzugriff auf eingestufte Netze

Behörden und geheimschutzbetreute Unternehmen übertragen die Pflege von Systemen zunehmend an deren Hersteller, spezialisierte Fernwartungsdienstleister oder andere Standorte, um verschiedene Vorteile zu realisieren. Bei externen Zugriffen in eingestufte Netze sind jedoch besondere Vorkehrungen zu treffen, um Cyber-Risiken zu vermeiden.

Secur|Ty made in Germany

Secur|Ty made in EU

Anforderungen an eine hochsichere Fernwartung

Bei der Fernwartung in VS-NfD-Netze sind die Regularien der Verschlusssachenanweisung des Bundesministeriums des Innern und für Heimat (BMI) zu erfüllen. Bei der Übertragung von VS-NfD-Daten fordern diese den Einsatz von Produkten, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für VS-NfD zugelassen wurden.

Weiterhin definieren die BSI-Grundschutzkataloge Architekturvorschläge für die Fernwartung von IT-Systemen. Darunter fallen die Vermeidung einer dauerhaften Netzverbindung sowie die Möglichkeit zur Überwachung der Fernwartungsvorgänge.

Die Rendezvous-Fernwartungslösung

Mit der Rendezvous-Fernwartungslösung für VS-NfD-Netze können diese Anforderungen zuverlässig erfüllt werden:

- Innerhalb eines vereinbarten Wartungszeitfensters kann ein vom Betreiber vollständig kontrollierter Zugriff nur auf das Zielsystem erfolgen.
- Dazu baut der Fernwarter eine VS-NfD-verschlüsselte Verbindung zur Fernwartungsplattform von genua auf.
- Der sichere Zugriff wird über einen Rendezvous Server realisiert, der keinen einseitigen Wartungszugriff auf das Zielsystem zulässt.
- Aus dem Kundennetz wird jetzt ebenfalls eine Verbindung zum Rendezvous Server aufgebaut, beispielsweise von einem Administrator.
- Erst wenn es zum Rendezvous kommt, kann der Fernwarter die jetzt durchgängige Verbindung zum Zielsystem nutzen.

Da der Administrator in der Behörde/im geheimschutzbetreuten Unternehmen den Zugriff in jedem Fall autorisieren muss, hat er stets die vollständige Kontrolle, wer wann auf das Zielsystem im VS-NfD-Netz zugreift.

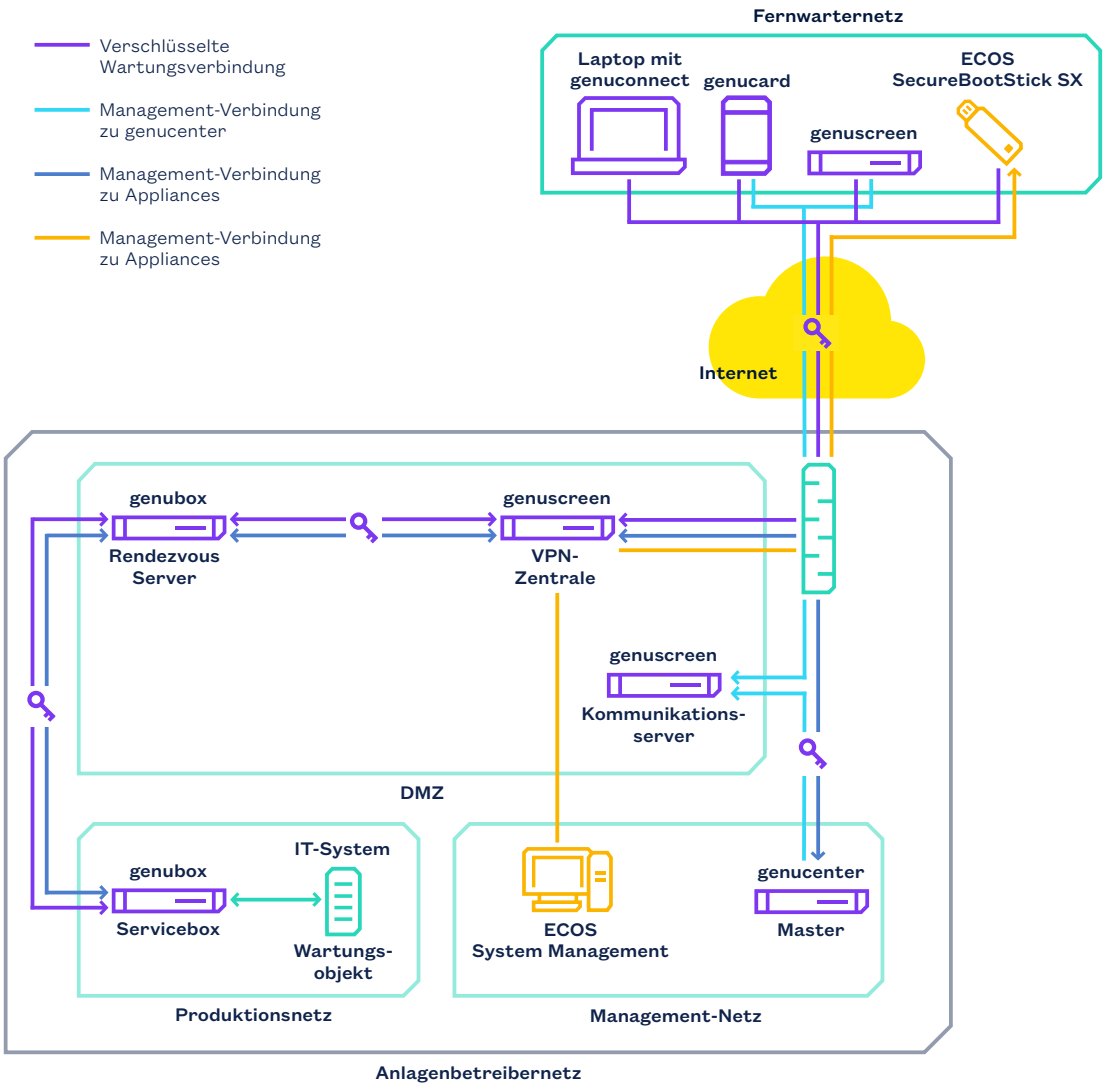
Fernzugriff – flexibel und sicher

Entsteht Wartungsbedarf, der aus logistischen Gründen nicht vor Ort erbracht werden kann, stellt Fernwartung eine flexible und praktische Lösung für Systembetreiber und Fernwarter dar. Je nach Situation und Schutzbedarf sind allerdings hohe Anforderungen an die IT-Sicherheit zu beachten.

Zugelassene Fernwartungs-Clients

Für den hochsicheren Zugriff verfügt der Fernwarter über ein Endgerät, mit dem er einen VS-NfD-IPsec-Tunnel zur Gegenstelle, der Firewall & VPN-Appliance genuscreen, aufbaut. genua bietet verschiedene Clients mit BSI-Zulassung:

- **genuconnect:** VPN Software Client für geschützte Verbindungen von Laptops und Tablets mit MS Windows
- **genucard:** Personal Security Device zur sicheren Konnektivität für alle Endgeräte
- **genuscreen:** Firewall & VPN-Appliance zur sicheren Anbindung von Liegenschaften und mobilen Standorten mit mehreren Arbeitsplätzen
- **ECOS SecureBootStick SX:** „Plug & Play"-Sicherheitslösung für einen flexiblen Einsatz



Überblick: Komponenten und Verbindungen bei Fernwartung in ein VS-NfD-Netz

Ablauf der sicheren Fernwartung im Überblick

Für die direkte Verbindung von genuscreen (Gegenstelle zum Fernwartungs-Client) und Rendezvous Server wird ein SSH-VPN verwendet. Dieses stellt eine Verschlüsselung der kompletten Strecke zwischen dem Fernwartungs-Client und dem Rendezvous Server sicher. Im Gegensatz zu einem klassischen VPN, das Site-to-Site- (Netzwerk-zu-Netzwerk) oder Host-to-Host-Beziehungen bereitstellt, wird bei einem SSH-VPN nur der Zugriff auf bestimmte Anwendungen/Dienste (Ports) gewährt.

Der Rendezvous Server dient als Vermittlungsstelle zwischen dem Fernwarter und dem Zielsystem. Fernwartungsverbindungen müssen immer von innen autorisiert und aufgebaut werden. Dazu wird eine sogenannte Servicebox verwendet: Sie fungiert als Schnittstelle zum Zielsystem und baut innerhalb des VS-NfD-Netzes ebenfalls eine verschlüsselte Verbindung zum Rendezvous Server auf.

Zusätzlich dient die Servicebox als Paketfilter und schützt vor unerwünschten Netzwerkzugriffen auf die Wartungsobjekte. Durch die Möglichkeit, einen Viren-Scanner einzubinden, lassen sich die vom Fernwarter gesendeten Daten überprüfen und Schäden durch Malware vermeiden.

Die Wartungsverbindungen werden durch einen autorisierten Operator beispielsweise mithilfe der zentralen Management-Lösung genucenter oder eines Schlüsselschalters freigegeben.

Ein Fernwarter hat somit nur bei Bedarf und gewährleisteter Autorisierung Zugriff auf das Zielsystem im sensiblen Netzwerk.

Konfiguration, Steuerung und Überwachung aller Netzwerkzugriffe erfolgen über die zentrale Management-Lösung genucenter. Da diese im VS-NfD-Einsatz nicht direkt an ein unsicheres Netzwerk wie das Internet angebunden werden darf, ist die Zwischenschaltung eines Kommunikationsservers erforderlich.

Support von Zero-Trust-Konzepten

Die Fernwartungslösung von genua unterstützt Zero-Trust-Konzepte. In diesem Zusammenhang übernimmt der Rendezvous Server die Rolle des Software-defined Perimeter und erlaubt externen authentisierten Anwendern den Zugriff auf spezifische Dienste hinter dem Perimeter. Wesentliche Sicherheitsfunktionen der Fernwartungslösung von genua:

- VS-NfD-verschlüsselter Tunnel zwischen Client und Software-defined Perimeter
- Flexible Zugriffskontrolle am Software-defined Perimeter basierend auf Identität und Ablaufumgebung
- Priviledged Access mit ausgefeiltem Mandanten-, Rollen- und Rechtekonzept

Weitere Informationen:

www.genua.de/genubox

Über genua

Die genua GmbH ist ein Enabler der digitalen Transformation. Wir sichern sensible IT-Netzwerke im Public- und 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 eine Tochtergesellschaft der Bundesdruckerei-Gruppe. Mit mehr als 350 Mitarbeitern 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
T +49 89 991950-0 | E info@genua.de | www.genua.de