



So sicher als wären Sie dabei

Absicherung von Tele-Service-Diensten

Die ersten beiden Teile dieser dreiteiligen Artikelreihe beschäftigten sich mit den organisatorischen Aspekten bei der Nutzung von Tele-Service-Diensten sowie den daraus abgeleiteten Anforderungen aus Sicht der IT-Security. In diesem dritten Teil wird eine in der Praxis erprobte Lösung zur Absicherung von Tele-Service-Diensten vorgestellt, die den Anforderungen der IT sowie denen der Produktionsabteilung gleichermaßen gerecht wird.

Aus den bisher dargestellten Verantwortlichkeiten und Zielen der IT und der Produktionsabteilung lassen sich einige Anforderungen definieren, die ein System erfüllen muss, um sichere Tele-Service-Verbindungen durch ein Firmennetz hindurch zu ermöglichen. Service- und Sicherheitsfunktion müssen voneinander getrennt sein, es müssen also separate Geräte für beide Zwecke eingesetzt werden. Die IT-Abteilung definiert die Sicherheitsrichtlinien für die Tele-Service-Verbindungen und parametrisiert und überwacht die für die Absicherung der Tele-Ser-

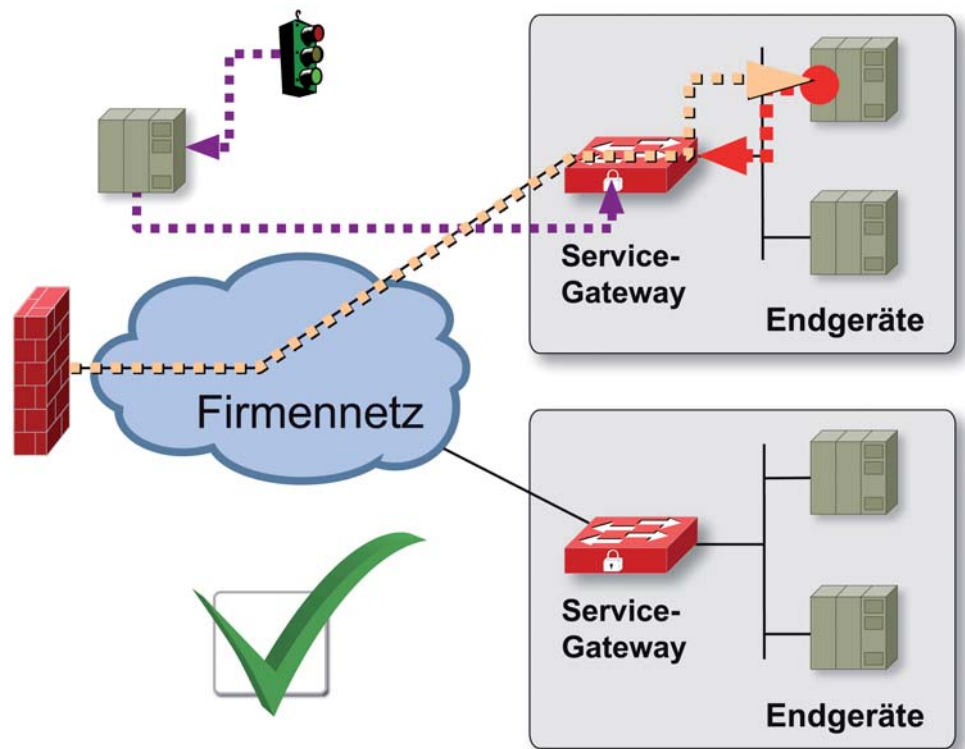
vice-Verbindungen verwendeten Geräte. Die Produktionsabteilung beziehungsweise der für den Prozess Verantwortliche kann eine von der IT-Abteilung parametrisierte Tele-Service-Verbindung in eigener Verantwortung freigeben oder sperren. Der aktuelle Zustand – „Freigegeben“, „Gesperrt“ oder „In Benutzung“ – aller Tele-Service-Verbindungen im Firmennetz wird zentral erfasst und dargestellt. Bei Bedarf kann eine Tele-Service-Verbindung direkt abgeschaltet und das Endgerät für die Zeit des Tele-Service-Zugriffs vollständig von anderen Geräten im Netzwerk abgeschottet werden.

System zur Kontrolle von Tele-Service-Diensten

Als Ergebnis aus diesen Anforderungen entstand das System zur Kontrolle von Tele-Service-Diensten, das im folgenden vorgestellt werden soll. Es besteht aus mehreren Komponenten. Die Verwaltungs- und Steuerungsfunktionen werden durch den zentralen Kontroll- und Monitoring Server (KMS) realisiert. Er verwaltet alle Serviceverbindungen zwischen den Tele-Service-Benutzern und den jeweiligen Endgeräten, das heißt den Start- und Zielpunkt einer Tele-Service-Verbindung

sowie die ihr zugeordneten dynamischen Filterregeln, in denen festgelegt ist, was erlaubt ist und was nicht. Hier wird ebenfalls hinterlegt, welcher Verantwortliche zur Freischaltung einer Tele-Service-Verbindung berechtigt ist. Der KMS hält ständige Verbindung zu den dezentral angeordneten Service-Gateways, überwacht deren Funktion und sendet an diese die Befehle zum Freischalten oder Sperren einer Service-Verbindung. Das Endgerät und die gesamte Service-Verbindung werden zyklisch auf korrekte Funktion und Verfügbarkeit geprüft. Dezentral, das heißt jeweils den Endgeräten zugeordnet, befinden sich die Service-Gateways. Ein Service-Gateway kann einem oder mehreren Endgeräten zugeordnet sein. Zu jedem Endgerät kann eine separate Service-Verbindung hergestellt werden. Das Service-Gateway hat Verbindung zum KMS und nimmt von ihm den Befehl zum Auf- oder Abbau einer Service-Verbindung entgegen. Eine Service-Verbindung besteht aus den Regeln, die definieren, welcher Datenverkehr zwischen dem Service-Rechner und dem Endgerät erlaubt ist und welcher nicht. Alternativ können die Tele-Service-Daten durch einen verschlüsselten Tunnel durch das Firmennetzwerk transportiert werden. Dies stellt die sicherste Methode für einen Tele-Service-Zugriff dar. Die auf Web-Technologien basierende graphische Benutzeroberfläche des KMS gibt dem Benutzer die Möglichkeit, je nach seiner im System festgelegten Funktion entweder Administrationaufgaben wahrzunehmen oder die ihm zugewiesenen Tele-Service-Verbindungen zu überwachen und zu steuern. Das System zur Kontrolle der Tele-Service-Dienste bedeutet einen geringeren administrativen Aufwand. Eine einheitliche IT-Policy ist über Templates für alle Geräte realisierbar, somit ist keine Änderung der bestehenden IP-Adressen der Maschinen erforderlich. Die Workflow-Orientierung drückt sich darin aus, dass eine Service-Verbindung durch den lokal Verantwortlichen freigeschaltet werden kann, verschiedene Endgeräte können unterschiedliche Verantwortliche haben. Die Verantwortung ist bei dem Kontrollsystem getrennt, Administration und Freischaltung erfolgen durch unterschiedliche Benutzer. Weitere Eckdaten sind:

- Herstellerunabhängig: einheitliche Lösung für Endgeräte unterschiedlicher Hersteller
- Sicher: dedizierter Zugang zu definiertem Endgerät, kein Zugang zum restlichen Netz
- Kontrolliert: Eine aktive freigeschaltete Verbindung kann jederzeit unterbrochen werden
- Zuverlässig: erfüllt die Anforderungen im industriellen und informationstechnischen Bereich



Dezentrale Service-Gateways schützen die Endgeräte und das Netzwerk.

Praktischer Einsatz Bundesweite Infrastruktur

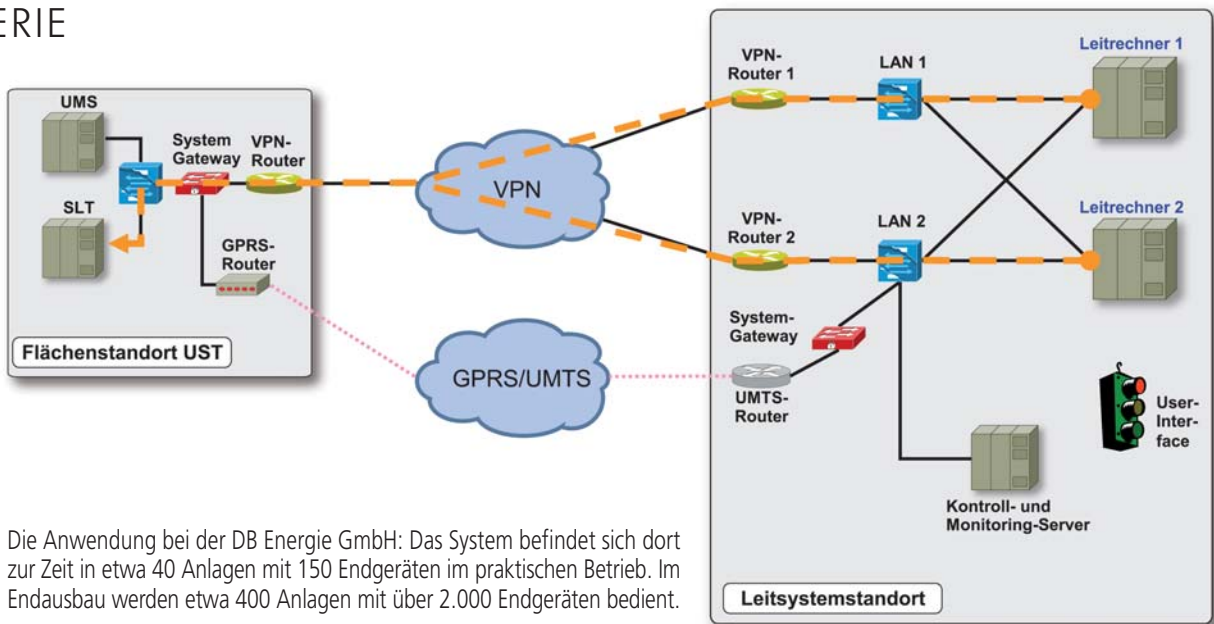
Die DB Energie betreut als unabhängiger Energiemanager der Bahn eines der größten Energiearten-übergreifenden Portfolios in Deutschland. Sie verfügt unter anderem über eine bundesweite Infrastruktur zur Stromversorgung von mobilen und stationären Verbrauchern und betreibt zu diesem Zweck eigene Hoch- und Mittelspannungsnetze. Das System befindet sich dort zur Zeit in etwa 40 Anlagen mit 150 Endgeräten im praktischen Betrieb. Im Endausbau werden etwa 400 Anlagen mit über 2.000 Endgeräten bedient. Die geschalteten Service-Tunnel dienen dazu, die Daten für die Steuerung der elektrischen Energieversorgung bei Ausfall des kabelgebundenen Hauptwegs für die Endgeräte transparent über eine Funkverbindung zu transportieren. Die dafür verwendeten Komponenten und Verfahren sind mit denen der hier beschriebenen Lösung identisch: Vor den Endgeräten befinden sich die in diesem Fall System-Gateways genannten dezentralen Komponenten. Das zentrale System-Gateway dient als Gegenstelle für den IPSec-Tunnel aus der Unterstation. Durch den Kontroll und Monitoring-Server werden alle relevanten Komponenten, angefangen von den Funk-Routern über die System-Gateways bis hin zu den Endgeräten überwacht. Das Personal in der



Der Energiemanager DB Energie

Seit 2001 ist die DB Energie Eisenbahninfrastrukturunternehmen mit Know-how und modernsten Steuerungsinstrumenten unter einem Dach. Hierzu gehört auch eine eigene Infrastruktur zur Versorgung des Bahnnetzes. Für Bahnen, Industrie, Gewerbe und öffentliche Auftraggeber bietet das Leistungsspektrum ein einfaches Handling auch komplexer Energiefragen, erzeugerunabhängige Beratung sowie zuverlässige in der Energieversorgung.

TELE-SERVICE SERIE



Die Anwendung bei der DB Energie GmbH: Das System befindet sich dort zur Zeit in etwa 40 Anlagen mit 150 Endgeräten im praktischen Betrieb. Im Endausbau werden etwa 400 Anlagen mit über 2.000 Endgeräten bedient.

Leitstelle kann bei Bedarf, das heißt wenn der Hauptweg ausgefallen ist, diesen Tunnel aktivieren. Die Daten gelangen dann über Funk zu den Leitrechnern.

Fazit Das Firmen-Netz bleibt sicher

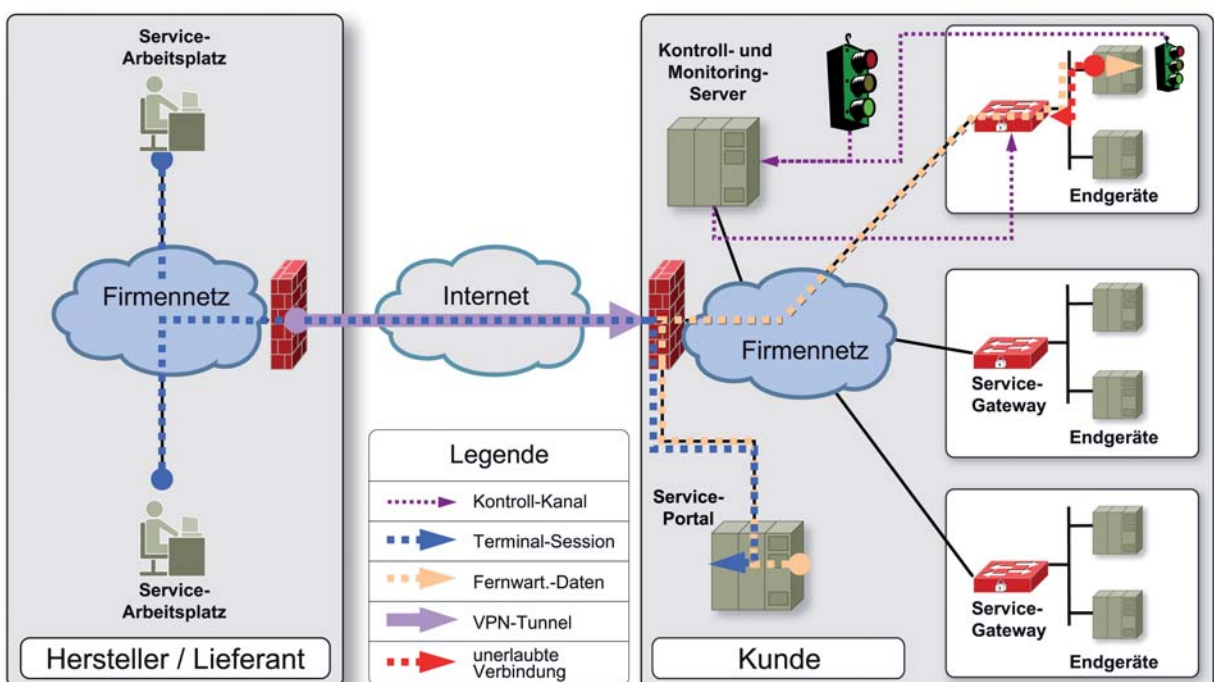
Das System weist mehrere einzigartige Eigenschaften auf, die in dieser Kombination bis jetzt nicht am Markt zu finden sind. Zum Beispiel lässt es sich jederzeit auch in bereits vorhandene Infrastrukturen integrieren, ohne dass an den existierenden Geräten Änderungen an der Netzwerkkonfiguration vorgenommen werden müssen. Die Sicher-

ung der Service-Verbindung erfolgt direkt bis zum Endgerät und nicht nur bis zur Firewall am Eingang des Firmennetzes. Das Firmennetz bleibt sicher. Die Sicherheitsrichtlinien für eine Serviceverbindung können zentral festgelegt und kontrolliert werden. Die Freischaltung einer Serviceverbindung erfolgt prozessorientiert durch den Anlagen- oder Prozess-Verantwortlichen. Ein Endgerät kann während der Serviceaktivitäten komplett vom restlichen Netz abgeschottet werden oder es lässt sich zumindest der ausgehende Datenverkehr protokollieren. Mit diesem Ansatz ist es möglich, Tele-Service-Zugänge für Lieferanten durch das Firmennetz des Kunden hindurch zu realisieren, die

den Sicherheits-Anforderungen der IT-Abteilung und den Anforderungen an die praktische Handhabung durch die Produktionsabteilung in gleichem Maße gerecht werden. Damit wird es erstmals möglich, die großen Vorteile, die eine durchgehende Tele-Service-Verbindung zwischen Lieferanten und Kunden bietet, konsequent zu nutzen. ■

Autor Matthias Wunderskirchner ist bei der Kayser-Threde GmbH verantwortlich für den Produktbereich „Industrial-Network Security-Solutions“.

www.kayser-threde.com



Sichere und zuverlässige Kontrolle von Tele-Service-Diensten im Firmennetzwerk durch zentrale und dezentrale Komponenten