



So sicher als wären Sie dabei?

Organisatorische Aspekte von Tele-Service-Diensten

Die Voraussetzungen für die Kommunikation zwischen Maschine und Service-Arbeitsplatz sind durch das TCP/IP-Protokoll gegeben. Allein – aus Sicherheitsgründen werden Tele-Service-Dienste noch nicht allgemein akzeptiert. Das Unbehagen, die Aktivitäten des Service-Technikers nicht mehr im Blick zu haben und die wirtschaftlichen Konsequenzen, die daraus resultieren können, verhindern oft den produktiven Einsatz. Die Artikelreihe Tele-Service zeigt die Ursachen auf und diskutiert die Probleme.

Die sichere Umsetzung von Tele-Service-Dienstleistungen wird eine der Herausforderungen der Zukunft sein. Proaktive Schadenserkennung, Verlängerung der Wartungsintervalle durch Condition-Based-Monitoring und kürzere Reparaturzeiten durch Tele-Support ermöglichen eine höhere Wirtschaftlichkeit. Das ist ohne eine zuverlässige und vor allem sichere Infrastruktur für Tele-Service-Dienste nicht umsetzbar. Tele-Service-Dienste, das heißt Dienstleistungen, die den bedarfsweisen Zugriff auf Maschinen und Anlagen über heute meist digitale

Kommunikationswege, zum Beispiel auf Basis von TCP/IP, erfordern, liegen voll im Trend. Sei es das Auslesen von Messwertreihen zur Prozessoptimierung, sei es die Erfassung und Remote-Auswertung von Condition-Monitoring-Daten zur bedarfsorientierten Wartung, Remote-Support durch Fachpersonal des Lieferanten für das Bedienpersonal des Betreibers vor Ort, oder auch die Remote-Fehlersuche und -behebung; immer ist die direkte Kommunikation zwischen einem Servicearbeitsplatz des Servicetechnikers und der Maschine oder der Anlage erforderlich.

Neu ist der Weg: TCP/IP

Im Unterschied zur heute bereits häufig praktizierten und akzeptierten Kommunikation zwischen zwei Maschinen oder einer Anlage und einem Leitstand ist bei Tele-Service-Diensten der Kommunikationspartner in vielen Fällen ein externer Dienstleister, dessen Mitarbeiter nicht unmittelbar den organisatorischen Regeln und juristischen Grenzen des Betreibers unterworfen sind und auch nicht direkt in den Produktions-Prozess eingebunden sind. Nun sind die erwähnten Themengebiete nicht grund-

sätzlich neu. Schon seit vielen Jahren werden Daten in Maschinen erfasst, zum Beispiel über mechanische oder elektronische Schreiber, und anschließend an anderer Stelle ausgewertet. Oder es werden direkt an der Maschine Diagnosedaten mit einem Servicetool ausgelesen, die für die Fehlerdiagnose hilfreich sind. Neu ist der Weg, auf dem diese Daten vom Steuerrechner der Maschine zum Servicedienstleister gelangen sollen – nämlich aus Kosten- und Effizienz-Gründen direkt über die bereits vorhandenen TCP/IP-Infrastruktur wie Prozess-Netze und Internet-Verbindungen.

Sicherheit ist erforderlich

Die Akzeptanz und praktische Anwendbarkeit von Tele-Service-Diensten auf Seiten des Betreibers hängen entscheidend davon ab, ob es gelingt, für diese das gleiche Sicherheitsniveau wie für herkömmliche Service-Dienstleistungen zu etablieren. Deshalb ist es an dieser Stelle hilfreich, die wichtigs-

ten Sicherheitsaspekte zu betrachten, die für Tele-Service Dienste relevant sind:

- **Prozess-Sicherheit**
Wartungsarbeiten oder Tätigkeiten an der Maschine oder Anlage dürfen den Produktions- oder Fertigungsprozess nicht beeinträchtigen und dürfen nur durchgeführt werden, wenn sie von den Maschinen- oder Anlagenverantwortlichen freigegeben wurden.
- **Personen-(Arbeits-)Sicherheit**
Wartungsarbeiten oder Tätigkeiten an der Maschine oder Anlage dürfen nicht zur Gefährdung für Leib und Leben des Service-Personals führen und dürfen nur an gesicherten und freigegebenen Maschinen durchgeführt werden.
- **Informations-Sicherheit**
Durch Wartungsarbeiten oder Tätigkeiten an einer Maschine oder Anlage dürfen keine für den Betreiber wirtschaftlich oder anderweitig sensiblen Daten, sei es aus dem Fertigungsprozess selbst oder aus anderen Bereichen, an Dritte gelangen und es darf keine Möglichkeit bestehen, dass diese Daten durch Dritte verfälscht werden.

Um diesen Aspekten Genüge zu tun, sind organisatorische, technische und personelle Maßnahmen zu treffen. Der Nachweis über die eingeführten Prozesse ist durch eine entsprechende Zertifizierung, zum Beispiel nach ISO 9001, zu dokumentieren und wird durch die unterschiedlichen Regelwerke zur Bewertung eines Unternehmens, etwa Basel II oder SOX, gefordert. Bevor im Detail festgelegt werden kann, welche Bedingungen von sicheren Tele-Service-Diensten erfüllt werden müssen, scheint es zweckmäßig, darzustellen, wie bei heutigen Service-Diensten, die nicht remote abgewickelt werden, verfahren wird. Die in vielen Firmen etablierten Abläufe und Prozeduren, die je nach Sicherheitsbedürfnis der jeweiligen Produktion mehr oder weniger stark ausgeprägt sind, werden im folgenden Beispiel exemplarisch am Ablauf eines Wartungseinsatzes durch externes Service-Personal an einer Maschine im Verantwortungsbereich eines Betreibers dargestellt.



Industrieunternehmen sind besser gegen unberechtigten Zutritt gesichert als manche Grenze. Trifft ein Service-Techniker an der Werkspforte ein, werden Identität und Auftraggeber geprüft. Dann muss der Techniker an den Einsatzort gelangen. Je nach Sensibilität des Unternehmens vertraut man ihm oder er wird durch einen Mitarbeiter der Werksicherheit bis zum Einsatzort begleitet.

Bildquelle: sxc.hu

Ein herkömmlicher Einsatz

Nachdem ein Fehler an der Maschine durch den Verantwortlichen festgestellt wurde, erfolgt die Benachrichtigung des externen Service-Personals, entweder telefonisch oder über E-Mail, SMS oder ähnliche Kommunikationswege. Wenn das externe Service-Personal an der Werkspforte eintrifft, wird dort deren Identität geprüft und festgehalten. Gegebenenfalls wird geprüft, ob schon eine Anforderung für einen Service-Einsatz vorliegt. Zumindest wird bei dem Verantwortlichen nachgefragt. Sind Identität und die anfordernde Stelle bestätigt, muss das Service-Personal an den Einsatzort gelangen. Je nach Sensibilität des Unternehmens vertraut man dabei dem Service-Personal („Gehen sie nur, sie kennen ja den Weg.“) oder – im anderen Extrem – werden diese durch einen Mitarbeiter der Werksicherheit bis zum Einsatzort begleitet. Ist der Einsatzort erreicht, erfolgt die Einweisung des externen Service-Personals durch den

für den Fertigungsprozess oder die Maschinen verantwortlichen Mitarbeiter des Betreibers. Dieser trägt die Verantwortung dafür, dass sich die Maschine in einem sicheren Zustand befindet und Wartungsarbeiten durchgeführt werden dürfen. Während der Wartungsarbeiten an der Maschine muss durch geeignete Maßnahmen sichergestellt sein, dass das externe Service-Personal nur an der freigegebenen Maschine arbeitet und sich nicht unkontrolliert an andere Orte innerhalb des Werkes begibt. Dies könnte durch eine direkte Beaufsichtigung durch einen Mitarbeiter, eine räumliche Absperrung anderer Anlagen- beziehungsweise Gebäudeteile oder aber durch eine indirekte Überwachung, zum Beispiel mit Videokameras, erfolgen. Rein organisatorische Regelungen zwischen dem Auftraggeber und dem Service-Unternehmen oder blindes Vertrauen dürften im Zweifelsfall, das heißt wenn es zu einem Zwischenfall mit Folgen in einem der oben erwähnten Sicherheits-Bereiche gekommen

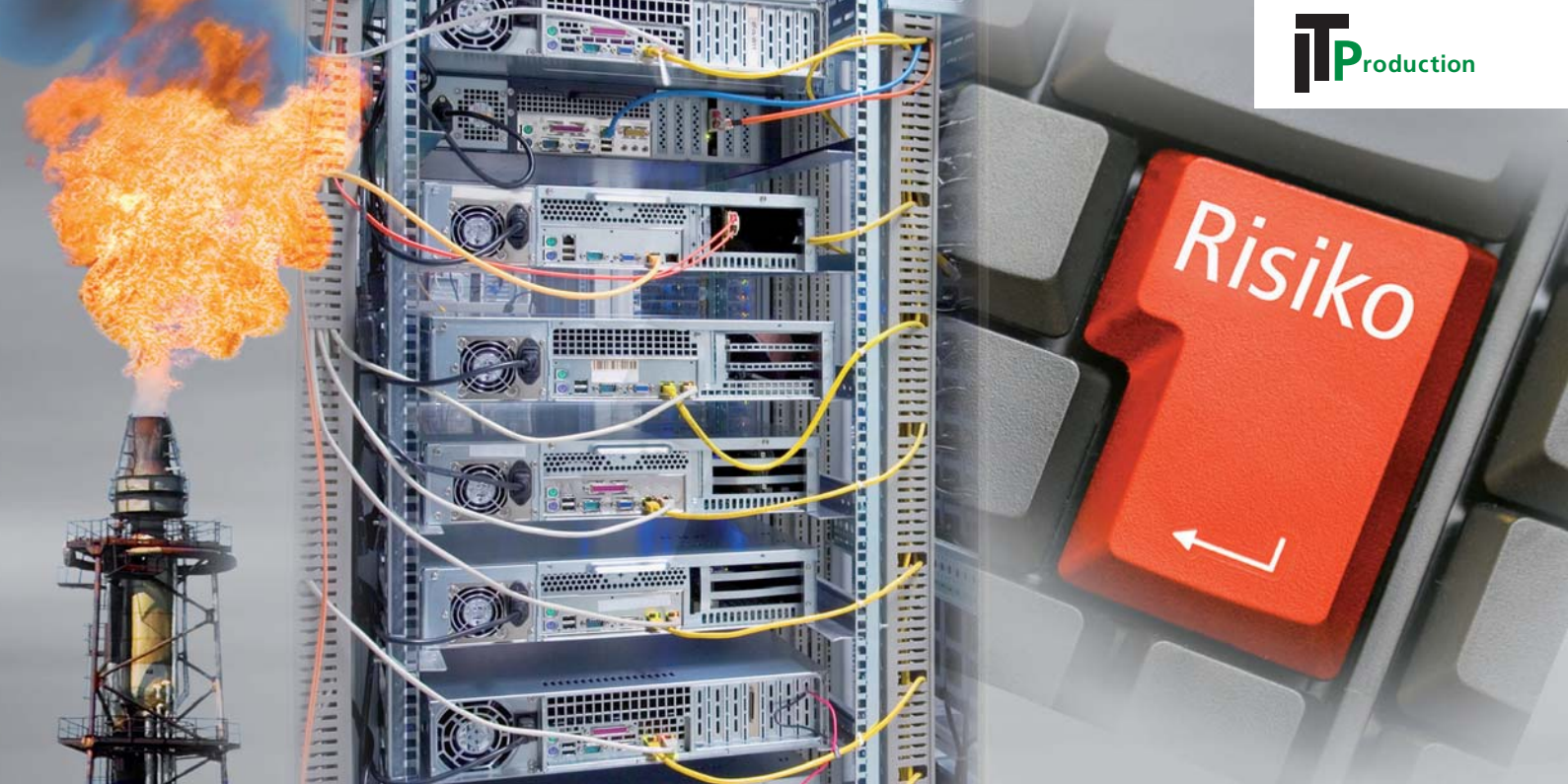
ist, der Aufsichtspflicht des Auftraggebers nicht genügen. Ist die Arbeit des Service-Personals abgeschlossen, so kontrolliert der Verantwortliche die korrekte Ausführung der Arbeiten und bestätigt diese. Das externe Personal begibt sich, mehr oder weniger begleitet, an die Pforte. Dort wird das Verlassen des Werksgeländes dokumentiert.

Zertifizierte Prozeduren

Zusammengefasst haben die beschriebenen Abläufe und Prozeduren das Ziel, alle Risiken, die aus dem Einsatz von externem Service-Personal für das Unternehmen des Auftraggebers entstehen könnten, zu minimieren und auf ein akzeptables Maß zu begrenzen. Als Nachweis muss der Auftraggeber zumindest folgende Frage jederzeit beantworten können: „Wer hat wann was wo und eventuell auch wie gemacht?“ Und hier beginnt nun das Dilemma bei den Tele-Service-Diensten. Während sich die Aspekte der Prozess- und Arbeits-Sicherheit durch die Übertragung heute bereits vorhandener Prozeduren auch für Tele-Service-Dienste beherrschen lassen, gilt dies nicht für den Bereich der Informations-Sicherheit. Durch die für die Tele-Service-Dienste notwendige Kommunikation durch das Firmennetz hindurch bis direkt in die Maschine werden durch die bisher unzureichenden Sicherheitsvorkehrungen „Tür und Tor“ für neue, inakzeptable Gefährdungen geöffnet. Mit der Einführung von Tele-Service-Diensten und damit dem Übergang vom realen zum virtuellen Servicetechniker verschieben sich innerhalb der Organisation des Kunden bisher klar geregelte Verantwortungen: Wer kontrolliert, wer auf welchem Weg in die Firma gelangt? Und wer sorgt dafür, dass dieser keinen Schaden anrichtet? Aus diesem Grund kann die Einführung von Tele-Service-Diensten auch nicht die Aufgabe einer einzelnen Fachabteilung sein, sondern muss durch das übergeordnete Management begleitet und koordiniert werden. Warum genau Tele-Service-Dienste eine Bedrohung für die Informations-Sicherheit darstellen, welche Fachabteilungen bei der Einführung betroffen sind und wie eine konkrete Lösung, die den unterschiedlichen Anforderungen gerecht wird, aussehen muss, erfahren Sie in der nächsten Folge. ■

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

www.kayser-threde.com



So sicher als wären Sie dabei?

Tele-Service-Dienste aus Sicht der IT-Security

Der erste Teil dieser dreiteiligen Artikelreihe beschäftigt sich mit den organisatorischen Aspekten der Nutzung von Tele-Service-Diensten. Im vorliegenden zweiten Teil soll der Frage nachgegangen werden, welche Fachabteilungen von der Einführung der Tele-Service-Dienste betroffen sind, welche Anforderungen sie haben und worin das Gefährdungspotenzial der Dienste für die IT-Infrastruktur des Unternehmens liegt.

Als Grundlage für die weitere Betrachtung des Themas soll zu Beginn an einem Beispiel die grundsätzliche Problematik aufgezeigt werden. Es wird eine neue Maschine oder Gerät im produktiven Bereich angeschafft, zum Beispiel eine Druckmaschine, eine Drehbank oder ein visuelles Inspektionssystem. Weil der Steuerungsrechner des Gerätes Daten mit anderen Rechnern im Netz des Kunden austauschen muss, zum Beispiel einem Parametrier-Arbeitsplatz oder der zentralen Prozess-Steuerung, ist eine Verbindung mit dem Produktionsnetz notwendig, welches wiederum, mehr oder weniger abgesichert, mit dem Büronetzwerk des Kunden verbunden ist. Viele Fehler, für die sich bisher ein Servicetechniker zum Einsatz vor Ort begeben musste, kann er aber auch aus der Ferne diagnostizieren und beseitigen, sofern eine Service-Verbindung zur Rechner Einheit der Maschine oder dem Gerät vorhanden ist. Auch die Inbetriebnahme vereinfacht sich erheblich, weil der Techniker vor Ort schnell und unkompliziert durch Spezialisten des Lieferanten unterstützt werden kann, zum Beispiel bei der Feh-

lersuche oder mit einem Software-Update. Deshalb soll eine solche Verbindung realisiert werden. Zwei grundsätzliche Lösungen stehen für diese Serviceverbindung zur Verfügung. Entweder wählt sich der Lieferant über ein separates Modem direkt an der Maschine beziehungsweise dem Endgerät ein, zur Auswahl stehen analog, ISDN oder GPRS/UMTS, oder es wird eine Verbindung vom Lieferanten über das Internet und die zentrale Firewall in das Netz des Kunden bis zur Maschine beziehungsweise zum Endgerät geschaffen. Bisher wurde im Allgemeinen die Modem-Lösung realisiert, da dieses Verfahren schon seit Jahren verfügbar und die Technik relativ einfach und bekannt ist. Nicht zuletzt lässt sich so, frei nach dem Motto: „Was sie nicht weiß, macht sie nicht heiß“, die Beteiligung der IT-Abteilung meist vermeiden. Übrigens ist es in der Regel laut – durchaus vorhandener – IT-Policy grundsätzlich verboten, ein Gerät an das Firmennetzwerk anzuschließen, wenn gleichzeitig eine separate Einwahlmöglichkeit vorhanden ist. Wenn dieser Umstand nicht manchmal schlicht übersehen wird, wird er auch im Interesse

der Servicequalität und der Verfügbarkeit der Maschine ignoriert. Die Internet-Variante bietet gegenüber dem Modem eine ganze Reihe von Vorteilen. Nicht jede Maschine braucht einen separaten Telefonanschluss, kein Modem kann mehr gerade dann ausfallen, wenn es gebraucht wird, weil die Geräte nicht überwacht werden, auch ist das Problem der langsamen Datenverbindungen ausgeräumt. Dank moderner DSL-Technik ist die Anbindung einer Firma an das Internet heute mit mehreren Megabit pro Sekunde möglich und ein Teil davon ließe sich durchaus für die Fernwartung verwenden. Setzt sich der für die Maschine oder den Produktionsbereich Verantwortliche mit der IT-Abteilung in Verbindung, um die Möglichkeit einer solchen Verbindung zu besprechen, so erhält er neben dem Verweis auf die für ihn weitgehend unpraktikable, weil überwiegend an den normalen Büroprozessen ausgerichtete IT-Policy meist eine lange Liste der Anforderungen, die die Maschine beziehungsweise ihr Steuerungsrechner erfüllen sollen. Verlangt werden ein aktueller Virens Scanner, eine aktivierte Firewall, Benutzerauthentifizierung der Servicetechniker über die IT-Infrastruktur, regelmäßige Security-Updates der Software und einiges mehr. Mit Sicherheit wird die IT-Abteilung dann auch noch die vollständige Kontrolle über alle Service-Verbindungen einfordern. Legt der Verantwortliche die Liste dem Lieferanten vor, winkt dieser meist umgehend ab. Die Steuerungsrechner sind auf die für die Funktion der Maschine erforderlichen Bedürfnisse hin optimiert, eine zusätzliche Berücksichtigung aller Sicherheitsaspekte wäre technisch aufwändig und wirtschaftlich nicht sinnvoll. Wie lassen sich die scheinbar unvereinbaren Bedürfnisse der Produktionsabteilung und der IT-Abteilung unter einen Hut bringen?

Anforderungen aus Sicht der Produktion

Das oberste Ziel der Produktionsabteilung ist die funktionierende Produktion beziehungsweise der funktionierende Prozess. Eine defekte Maschine oder Steuerung, die den gesamten Produktionsprozess blockiert, ist der größte anzunehmende Unfall und muss so schnell wie möglich beseitigt werden. Der für den Prozess respektive die Produktion Verantwortliche muss die Störungsbeseitigung einleiten und schnell alle notwendigen Aktionen durchführen können, damit der Servicetechniker Zugriff auf die Maschine erhält. Er ist der Einzige, der letztendlich entscheiden kann, ob aus betrieblicher Sicht an einer Maschine oder einem Gerät Wartungsarbeiten durchgeführt werden dürfen. Eine zeitaufwändige Einbeziehung weiterer, nur indirekt an der Störungsbeseitigung beteiligten Abteilungen, etwa der IT-Abteilung zur Freischaltung einer Serviceverbindung, ist aus Zeit- und Verfügbarkeitsgründen im Regelfall nicht vorteilhaft. Der Prozess muss gegebenenfalls 24 Stunden an sieben Tagen in der Woche verfügbar sein. Primär sollte sich der Fokus damit auf die Zuverlässigkeit sowie einfache und schnelle Nutzbarkeit einer Serviceverbindung richten.

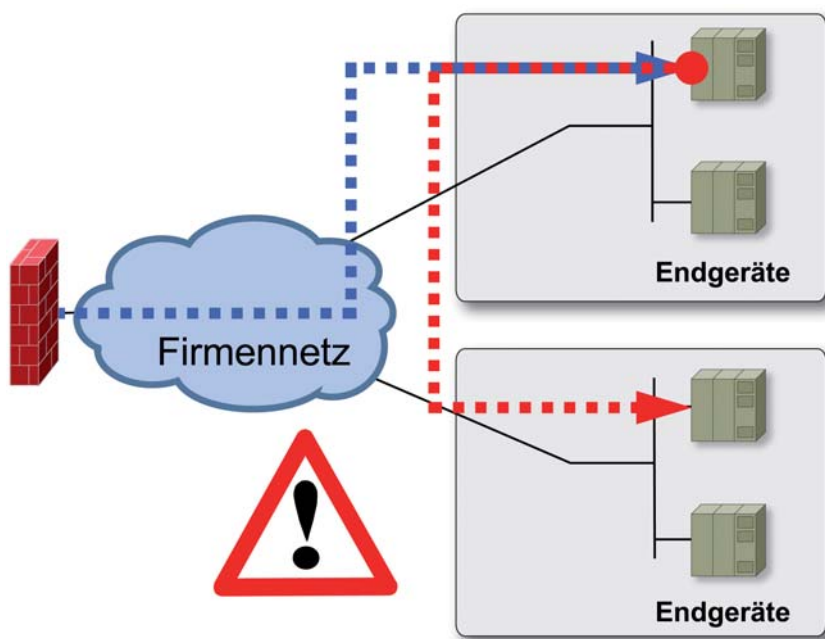
Anforderungen aus Sicht der IT-Abteilung

Die IT-Abteilung betreibt das Firmennetzwerk und bietet die IT-Dienstleistungen wie E-Mail, Datei- und Druckserver, SAP oder Internetzugang an. Oberste Priorität hat ein sicheres und funktionierendes Netzwerk als Basis für den Geschäftsbetrieb. Da Firmennetzwerke heute meist auf Internet-Technologien basieren, hat die IT-Abteilung in der Regel von der Geschäftsführung die Verantwortung für die Minimierung aller Risiken, die aus der Kommunikation über die Netzwerke resultieren können. Die Prinzipien der Integrität, Authentizität und Vertraulichkeit zu wahren, ist das Gebot. Im vorliegenden Fall bedeutet dies, dass Informationen, die an beliebiger Stelle im Netzwerk verfügbar sind, ausschließlich Personen zu-

gänglich sein dürfen, deren Berechtigung zweifelsfrei nachgewiesen ist, und die Möglichkeit auszuschließen, dass Dritte diese Informationen mitlesen oder verändern können. Mit dem zunehmenden Einsatz der Internet-Technologien auch im Bereich der Automatisierungstechnik und der Prozesssteuerung, zum Beispiel Ethernet/IP-basierte Feldbussysteme, TCP/IP-Kommunikation zwischen Maschine und Leitstelle, weitet sich der Verantwortungsbereich der IT-Abteilung aus, oft ohne dass sie die notwendigen Kenntnisse über den Produktionsprozess besitzt. Das vorrangige Anliegen der IT-Abteilung ist die Einhaltung der in der IT-Policy festgelegten Randbedingungen und Verfahren, die sich an den Erfordernissen der Bürovernetzung orientieren und deshalb selten den Anforderungen der Automatisierung und Prozess-Steuerung genügen.

Risikobetrachtung von Serviceverbindungen

Warum aber stellt ein Servicezugang zum Steuerungsrechner einer Maschine oder eines Gerätes überhaupt ein Sicherheitsrisiko für das Netzwerk dar, an dem das Gerät angeschlossen ist? Die Ursache liegt im Aufbau der Steuerungsrechner moderner Anlagen. Diese verfügen heute fast immer über ein Betriebssystem, meist eine Windows- oder Linux-Variante. Im Prinzip handelt es sich deshalb bei den aktuellen Steuerungsrechnern um industrietaugliche PCs, und genau wie normale Büro-PCs haben auch diese Rechner die Möglichkeit, mit anderen Rechnern über das Netzwerk zu kommunizieren, wenn dies nicht explizit verhindert wird. Ein Servicezugang



Direkte Service-Verbindungen sind im Produktivnetz unkontrollierbar.

auf einen Steuerungsrechner impliziert damit die Möglichkeit, von diesem Rechner aus auf andere Rechner innerhalb des Produktivnetzes zuzugreifen. Weil in den meisten Fällen innerhalb der Netze keine weiteren Abschottungen oder Überwachungen existieren, wird dies auch nicht bemerkt (siehe Bild oben auf dieser Seite). Im Firmennetz und auf den Büro-PCs sorgt die IT-Abteilung dafür, dass sich nur berechtigte Mitarbeiter an diesen PCs anmelden können und die Sicherheitseinstellungen so sicher wie möglich sind.

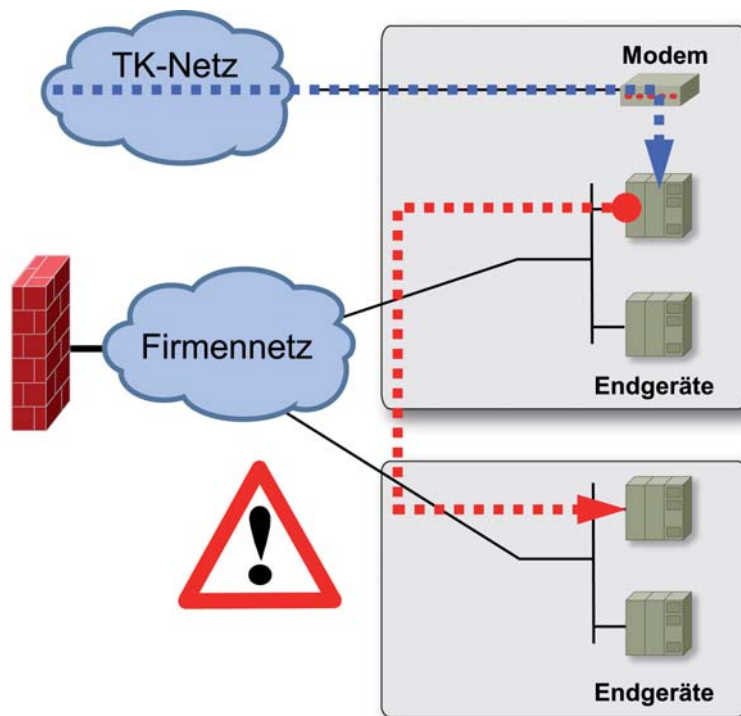
Auf einem Steuerungsrechner ist dies aber weder möglich noch sinnvoll, da sein Aufgabenschwerpunkt an anderer Stelle liegt. Zudem meldet sich der Servicetechniker meist als Administrator an diesem Rechner an, weil er für seine Serviceaufgaben eben gerade Zugriff auf alle Ebenen des Betriebssystems benötigt. Deshalb unterliegt er in seinen Handlungen keinerlei Einschränkungen durch das Betriebssystem und kann insbesondere alle Netzwerkdienste des Steuerungsrechners nutzen. Dies stellt einen gravierenden Unterschied zu normalen Büro-Arbeitsplätzen dar, hier arbeiten die Benutzer immer mit eingeschränkten Rechten und haben keine Möglichkeit, unerlaubte Netzwerkverbindungen aufzubauen. Ein weiterer Unterschied ist die Tatsache, dass die Servicetechniker des Lieferanten nicht der eigenen Firma angehören, also auch nicht den IT-Richtlinien des eigenen Unternehmens verpflichtet sind. Hier sind jeweils individuelle Vereinbarungen mit dem Lieferanten zu treffen und natürlich zu überwachen. Die unkontrollierbaren Kommunikationsmöglichkeiten von einem Steuerungsrechner in das Produktiv- oder Büronetz in Verbindung mit einem Servicezugang, egal ob über ein zentrales Service-Portal an der Firewall oder direkt realisiert, stellt ein mögliches Risiko für diese Netzwerke dar und erfordert eine sehr genaue Abwägung der Vor- und Nachteile.

Fazit: Risiken vermeiden

Es lässt sich festhalten: Tele-Service-Dienste eröffnen ein großes Potential, um neue Service-Dienstleistungen wirtschaftlich zu realisieren. Ohne weitere Maßnahmen aber ergeben sich daraus unkalkulierbare Risiken für die IT-Infrastruktur und damit den gesamten Geschäftsprozess eines Unternehmens. Oder würden Sie, um das Bild aus dem ersten Teil dieser Artikelreihe aufzugreifen, einem gegebenenfalls sogar externen Service-Mitarbeiter den vollkommen unkontrollierten und unbeobachteten Zugang zu allen Räumen Ihres Unternehmens gewähren? Bei Tele-Service-Diensten entspricht dies häufig noch der Realität, ohne dass sich die Beteiligten, vor allem aus dem Produktionsbereich, dieser Tatsache bewusst sind. Wie eine konkrete Lösung aussieht, die sowohl den Anforderungen der Produktions- als auch der IT-Abteilung genügt und die auch wirklich den Anspruch erfüllt, Tele-Service-Dienste so sicher zu machen „als wären Sie dabei“, beschreibt der dritte und letzte Teil dieser Reihe. ■

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

www.kayser-threde.com



Ein Modem am Endgerät gefährdet das Netzwerk.



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-

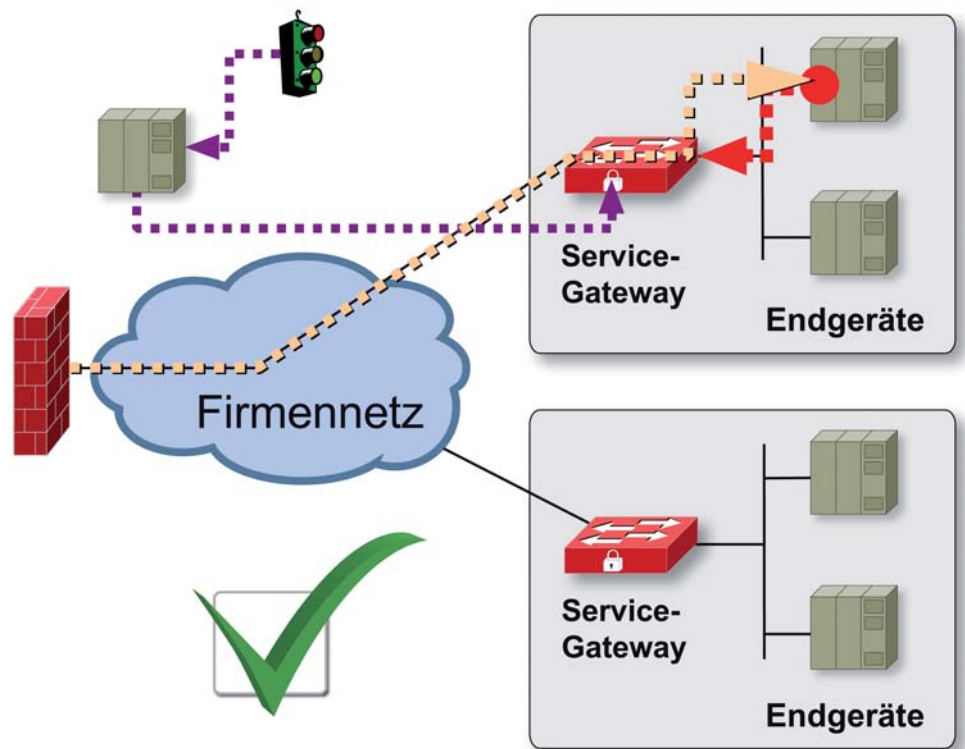
vice-Verbindungen verwendeten Geräte. Die Produktionsabteilung beziehungsweise der für den Prozess Verantwortliche kann eine von der IT-Abteilung parametrisierte Tele-Service-Verbindung in eigener Verantwortung freigeben oder sperren. Der aktuelle Zustand – „Freigegeben“, „Gesperrt“ oder „In Benutzung“ – 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

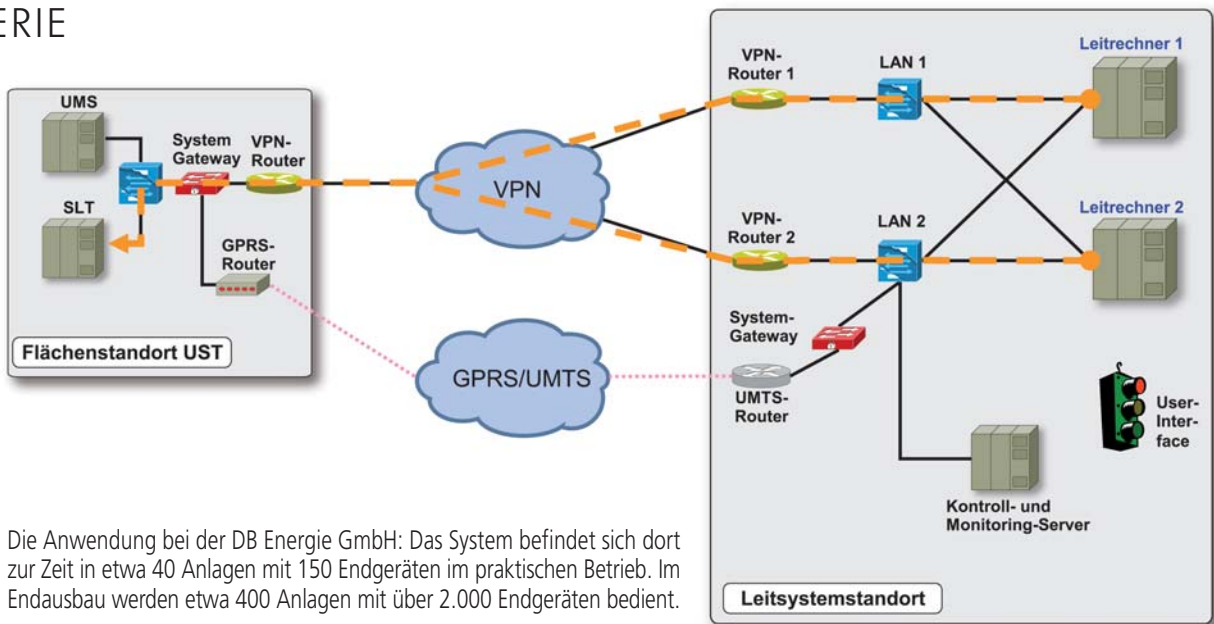
Die DB Energie betreut als unabhängiger Energiemanager der Bahn eines der größten Energiearten-übergreifenden Portfolios in Deutschland. Sie verfügt unter anderem über eine bundesweite Infrastruktur zur Stromversorgung von mobilen und stationären Verbrauchern und betreibt zu diesem Zweck eigene Hoch- 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

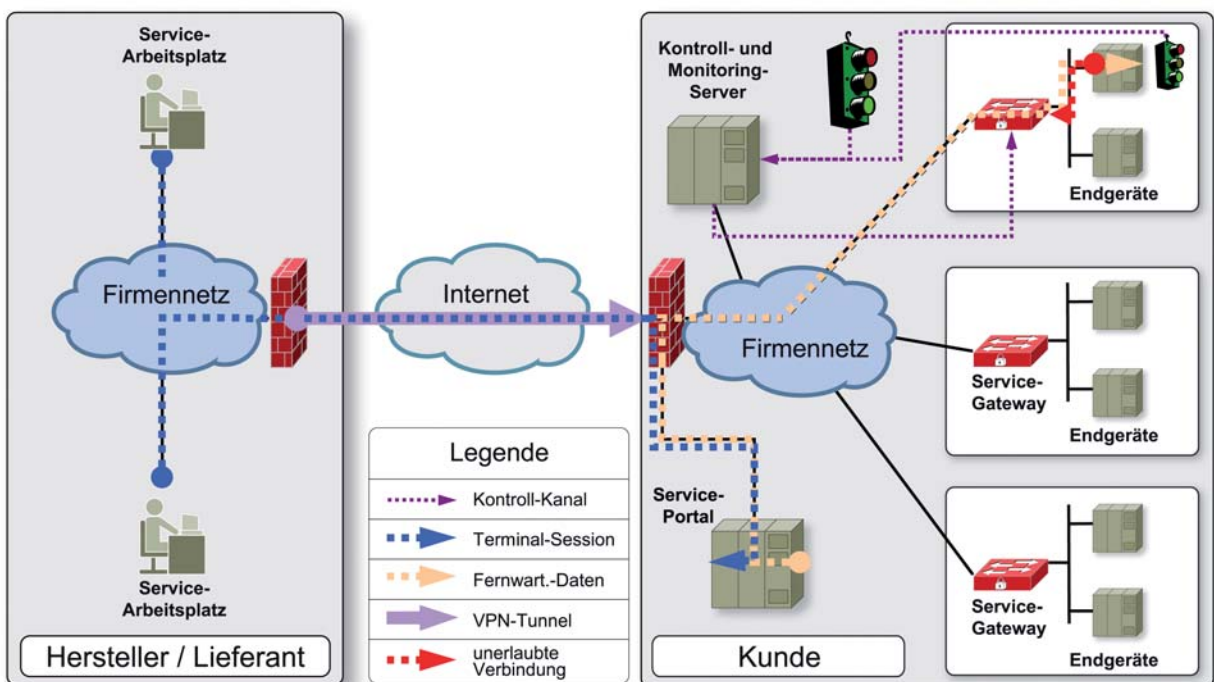
Das System weist mehrere einzigartige Eigenschaften auf, die in dieser Kombination bis jetzt nicht am Markt zu finden sind. Zum Beispiel lässt es sich jederzeit auch in bereits vorhandene Infrastrukturen integrieren, ohne dass an den existierenden Geräten Änderungen an der Netzwerkkonfiguration vorgenommen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