

# Sicher vom Servicetechniker bis zum Endgerät

## Vollständige Kontrolle aller Fernwartungsverbindungen im eigenen Produktions- und Firmennetzwerk



Bild 1: Sicher vom Servicetechniker bis zum Endgerät (Quelle: Kayser-Threde GmbH; aboutpixel.de@svair)

**Fernwartung über das Internet – von jedem Ort der Welt Zugriff auf jedes Endgerät der Welt – für die einen die Wirklichkeit gewordene Vision der unbegrenzten Möglichkeiten der Internet-Kommunikation – für die anderen eine unakzeptable Bedrohung. Welche Positionen stehen sich hier scheinbar unvereinbar gegenüber? Der folgende Beitrag zeigt eine integrierte Lösung zum Aufbau und zur Kontrolle von Fernwartungsverbindungen aus dem Internet in ein Firmennetzwerk, welche die Anforderungen der IT und der Automatisierungstechnik gleichermaßen berücksichtigt.**

**B**eginnen wir mit einem Beispiel: Es soll eine neue Maschine für den Produktionsbereich angeschafft werden (z.B. CNC-Fräse, Schweißroboter usw.). Weil der Steuerungsrechner der Maschine Daten mit anderen Rechnern im Netz des Kunden austauschen muss, z.B. einem Parametrier-Arbeitsplatz, ist bei der Installation eine Verbindung mit dem Produktionsnetz vorgesehen, welches wiederum, mehr oder weniger abgesichert, mit dem Firmennetz des Kunden verbunden ist. Analysen haben ergeben, dass viele Fehler, für die bisher ein Servicetechniker vor Ort geholt wurde, auch aus der Ferne diagnostiziert und beseitigt werden können, sofern der Servicetechniker über eine Verbindung zur Steuerung der Maschine verfügt. Deshalb soll eine solche Verbindung realisiert werden. Zwei grundsätzliche Lösungen stehen für diese Serviceverbindung zur Verfügung:

- Ein separates Modem an der Ma-

schine, über das sich der Lieferant direkt einwählt

- Eine Verbindung vom Lieferanten über das Internet und die Firewall in das Netz des Kunden bis zur Maschine

Bisher wurde im Allgemeinen die erste Lösung realisiert, da es sich um ein schon seit Jahren verfügbares Verfahren handelt, die Technik relativ einfach und bekannt ist und sich so nicht zuletzt die Beteiligung der IT-Abteilung meist vermeiden lässt. Dass es in der Regel laut IT-Policy grundsätzlich verboten ist, ein Gerät an das Firmennetzwerk anzuschließen, wenn gleichzeitig eine separate Einwahlmöglichkeit vorhanden ist, wird manchmal schlicht übersehen oder aber auch im Interesse der Servicequalität und der Verfügbarkeit der Maschine ignoriert (Bild 2). Die zweite Variante böte dagegen eine ganze Reihe von Vorteilen: Kein separater Telefonanschluss für jede Maschine, keine Modems, die nicht funktionieren, wenn man sie braucht, weil sie

nicht überwacht werden, keine langsamen Datenverbindungen. Dank moderner DSL-Technik ist die Anbindung einer Firma an das Internet heute mit mehreren Mbit/s 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 unverständliche IT-Policy, meist eine lange Liste der Anforderungen, die die Maschine bzw. ihr Steuerungsrechner erfüllen müsste: aktueller Virenschutz, aktivierte Firewall, Benutzerauthentifizierung der Servicetechniker über die IT-Infrastruktur, regelmäßige Security-Updates der Software usw. Und im Übrigen verlangt die IT-Abteilung die vollständige Kontrolle über alle Service-Verbindungen. Legt der Ver-

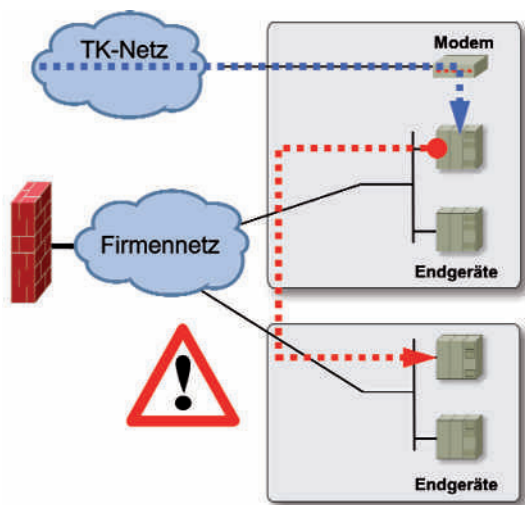


Bild 2: Modems an der Maschine gefährden das Firmennetzwerk.

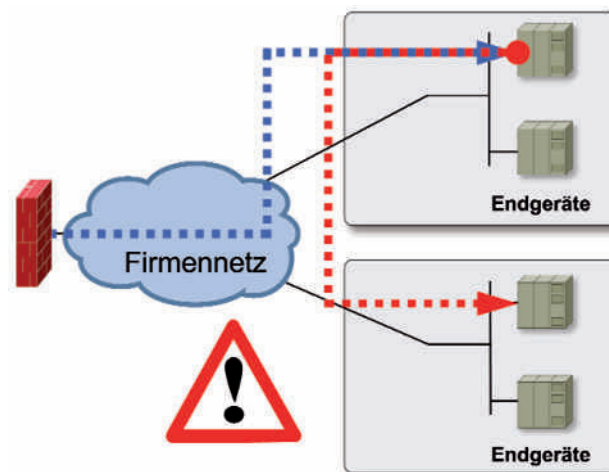


Bild 3: Direkte Serviceverbindungen sind im Firmennetzwerk unkontrollierbar.

antwortliche 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 wirtschaftlich nicht sinnvoll. Wie lassen sich nun die scheinbar unvereinbaren Bedürfnisse der Produktionsabteilung und der IT-Abteilung unter einen Hut bringen? Das oberste Ziel der Produktionsabteilung ist die funktionierende Produktion. Eine defekte Maschine, die den gesamten Produktionsprozess blockiert, ist der größte anzunehmende Unfall und muss so schnell wie möglich beseitigt werden. Die IT-Abteilung betreibt das Firmennetzwerk und bietet die IT-Dienstleistungen (E-Mail, Datei- und Druckserver, SAP, Internetzugang usw.) an. Oberste Priorität hat ein sicheres und funktionierendes Netzwerk als Basis für den Geschäftsbetrieb. Warum aber stellt ein Servicezugang zum Steuerungsrechner einer Maschine überhaupt ein Sicherheitsrisiko für das Firmennetz dar, an dem die Maschine angeschlossen ist? Die Ursache liegt im Aufbau der Steuerungsrechner moderner Maschinen. 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 einen industrietauglichen PC. 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. Im Firmennetz und auf den Büro-PCs sorgt die IT-Abteilung dafür, dass sich nur 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. Die unkontrollierbaren Kommunikationsmöglichkeiten von einem Steuerungsrechner in das Firmennetz in Verbindung mit einem Servicezugang, egal ob über ein zentrales Service-Portal an der Firewall oder direkt realisiert, stellt eine möglichen Bedrohung für das Firmennetzwerk dar, der keine IT-Abteilung zustimmen kann (Bild 3). Aus den oben dargestellten Zielen der Beteiligten lassen sich einige Anforderungen definieren, die ein System erfüllen muss, um eine hoch sichere Fernwartung durch das Firmennetz hindurch zu ermöglichen:

- Service- und Sicherheitsfunktion müssen voneinander getrennt sein
- Die IT-Abteilung legt die Sicherheitsrichtlinien für Serviceverbindungen fest
- Die IT-Abteilung parametriert und überwacht die für die Absicherung der Service-Verbindung verwendeten Geräte
- Die Produktionsabteilung, bzw. der für die Maschine Verantwortliche, kann eine von der IT-Abteilung parametrierte Serviceverbindung in eigener Verantwortung freigeben oder sperren
- Der aktuelle Zustand ('freigegeben', 'gesperrt' oder 'in Benutzung') aller Serviceverbindungen im Firmennetz wird zentral erfasst und dargestellt
- Im Notfall kann – auch durch die IT-Abteilung – eine Service-Verbindung direkt abgeschaltet werden
- Bei Bedarf kann das Endgerät für die Zeit des Service-Zugriffs vollständig von anderen Geräten im Netzwerk abgeschottet werden
- Auf Anforderung werden Service-Verbindungen zentral protokolliert

Das hier vorgestellte System zur Fernwartungskontrolle (Bild 4) erfüllt diese Anforderungen. Es besteht aus zentralen und dezentralen Komponenten. Der zentrale Kontroll- und Monitoring-Server stellt die Benutzeroberfläche für die Benutzer zur Verfügung. Er nimmt Kommandos zum Freigeben oder Sperren einer Serviceverbindung entgegen und leitet sie an das zuständige Service-Gateway weiter. Er stellt den aktuellen Zustand der

Verbindungen dar und sammelt die protokollierten Informationen. Er verwaltet in seiner Datenbank alle für das System relevanten Informationen. Über ihn können die Service-Gateways parametriert werden. Die vom Kontroll- und Monitoring-Server bereitgestellte Benutzeroberfläche kann auf dem Browser eines beliebigen Rechners dargestellt werden. Die einzelnen Benutzer haben unterschiedliche Funktionen, z.B. Administrator oder Verantwortlicher für die Freigabe einer Serviceverbindung zu einer Maschine. Dezentrale Service-Gateways kontrollieren den Datenverkehr zu einem Endgerät, z.B. einem Steuerrechner. Sie können für das Endgerät transparent in den Datenverkehr eingeschleift werden, sind also auch nachträglich ohne Änderung der IP-Adressen am Endgerät einsetzbar. Die Kontrolle findet auf Ebene der IP-Verbindungen statt und verfügt über die Möglichkeiten einer Stateful-Inspection Firewall. Um Service-Verbindungen freizugeben oder zu sperren, können die Regeln manuell dynamisch aktiviert oder deaktiviert werden. Ein zentrales Service-Portal kann, muss aber nicht vorhanden sein. Hier besteht bei Bedarf eine zusätzliche Möglich-

# Sichere Automation

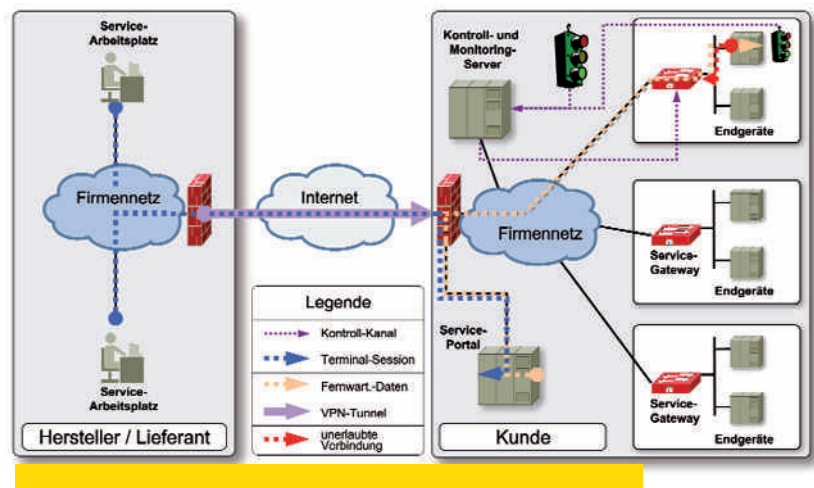


Bild 4: Sichere und zuverlässige dynamische Fernwartungskontrolle im Firmennetzwerk durch zentrale und dezentrale Komponenten.

keit, die Servicemitarbeiter explizit zu authentifizieren und gegebenenfalls kontrollierte Service-Arbeitsplätze zu realisieren. Merkmale des Systems zur Kontrolle der Fernwartungsverbindungen:

- **Einfach:** geringer administrativer Aufwand, einheitliche IT-Policy über Templates für alle Geräte realisierbar, keine Änderung der bestehenden IP-Adressen der Maschinen erforderlich
- **Work-flow orientiert:** eine Serviceverbindung kann durch den lokal Verantwortlichen freigeschaltet werden, verschiedene Endgeräte können unterschiedliche Verantwortliche haben
- **Getrennte Verantwortung:** Administration und Freischaltung erfolgen durch unterschiedliche Benutzer
- **Endgeräte unabhängig:** einheitliche Lösung für Endgeräte unterschiedlicher Hersteller
- **Sicher:** dedizierter Zugang zu definiertem Endgerät, kein Zugang zum restlichen Netz
- **Kontrolliert:** Aktive freigeschaltete Verbindung kann jederzeit unterbrochen werden, Netzwerk-Aktivitäten sind protokollierbar
- **Zuverlässig:** genügt den Anforderungen im industriellen und informationstechnischen Bereich

## Aufbau und Funktionsweise

Das System zur Fernwartungskontrolle besteht aus mehreren Komponenten. Die Verwaltungs- und Steuerungsfunktionen werden durch den zentralen Kontroll- und Monitoring-Server realisiert. Er verwaltet

alle Serviceverbindungen zwischen den Service-Benutzern und den jeweiligen Endgeräten, d.h. den Start- und Zielpunkt einer Serviceverbindung sowie die ihr zugeordneten dynamischen Filterregeln. Hier wird ebenfalls hinterlegt, welcher Verantwortliche zur Freischaltung einer Serviceverbindung berechtigt ist. Er hält ständige Verbindung zu den dezentral angeordneten Service-Gateways, überwacht deren Funktion und sendet an sie die Befehle zum Freischalten oder Sperren einer Serviceverbindung. Die von den Service-Gateways erfassten und gesendeten LOG-Informationen werden gespeichert und zur Auswertung verfügbar gemacht. Gleichzeitig werden das Endgerät und die gesamte Service-Verbindung zyklisch auf korrekte Funktion und Verfügbarkeit geprüft, damit ein Ausfall frühzeitig, d.h. möglichst bevor die Verbindung benötigt wird, beseitigt werden kann. Dezentral, d.h. jeweils den Endgeräten zugeordnet, befinden sich die Service-Gateways (Bild 5). Ein Service-Gateway kann einem oder mehreren Endgeräten zugeordnet sein. Zu jedem Endgerät kann eine separate Service-Verbindung hergestellt werden. Das Netz-

werk hinter einem Service-Gateway stellt einen Vertrauensbereich dar, die Endgeräte in diesem Bereich sind nicht gegeneinander abgeschottet. Das Service-Gateway hält die Kontroll-Verbindung zum zentralen Kontroll- und Monitoring-Server und nimmt von ihm den Befehl zum Aufbau einer Service-Verbindung entgegen. Auf Anforderung protokolliert es die festgelegten Datenverbindungen mit und sendet die erfassten Daten an den Kontroll- und Monitoring-Server. Eine Service-Verbindung besteht aus zwei Komponenten, zum einen den Regeln, die definieren, welcher Datenverkehr zwischen dem Service-Rechner und dem Endgerät erlaubt ist, zum anderen können Regeln angegeben werden, die für die Zeit einer aktiven Service-Verbindung explizit Datenverkehr vom Endgerät in das restliche Firmennetz verbieten. Die grafische Benutzeroberfläche als dritte Komponente des Systems gibt den Benutzern die Möglichkeit, mit dem System zu interagieren. Es handelt sich um eine html-basierte Oberfläche, die durch einen Web-Browser eines beliebigen Rechners dargestellt werden kann. Je nach seiner im System festgelegten

