

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 Rechnereinheit 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.

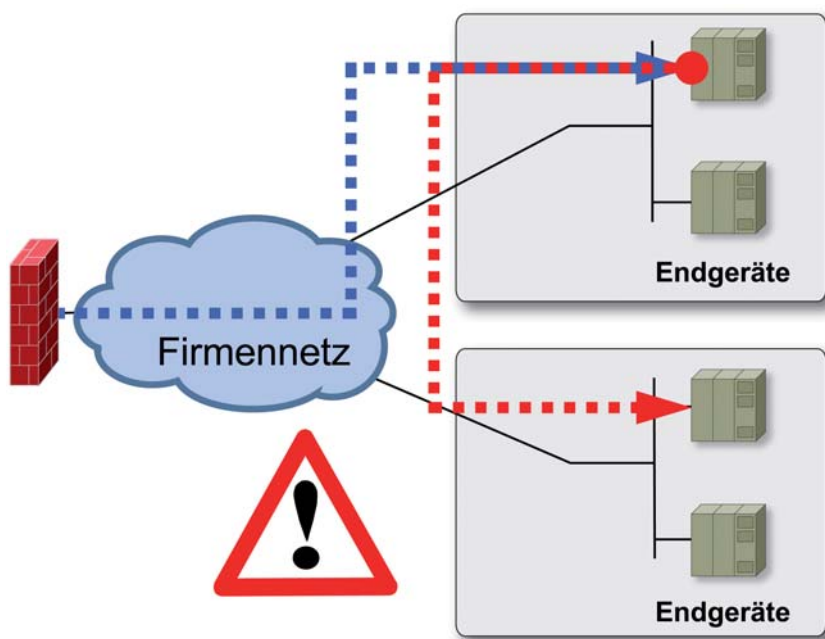
Anforderungen aus Sicht der IT-Abteilung

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 berechnete Mitarbeiter an diesen PCs anmelden können und die Sicherheitseinstellungen so sicher wie möglich sind.

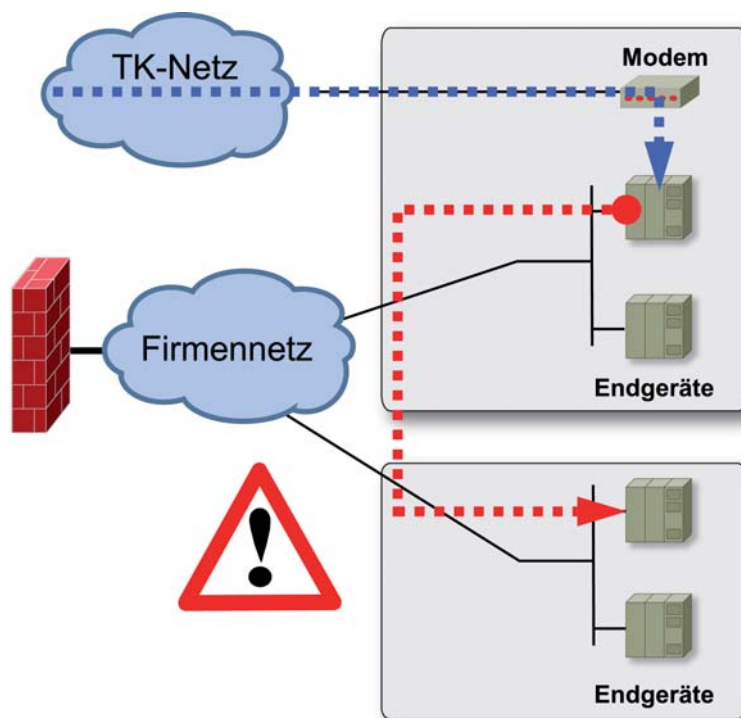
Auf einem Steuerungsrechner ist dies aber weder möglich noch sinnvoll, da sein Aufgabenschwerpunkt an anderer Stelle liegt. Zudem meldet sich der Servicetechniker meist als Administrator an diesem Rechner an, weil er für seine Serviceaufgaben eben gerade Zugriff auf alle Ebenen des Betriebssystems benötigt. 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.