



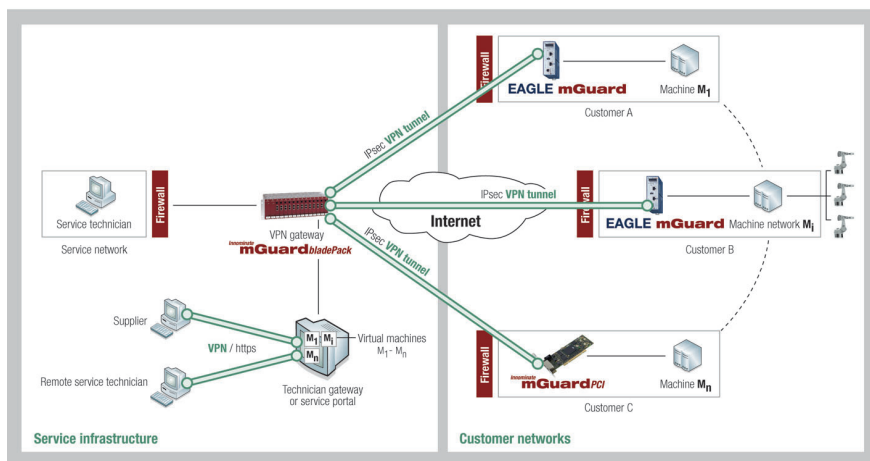
Teleservice goes Internet: sicher und skalierbar

Die Fernwartung von Maschinen und Anlagen kann über die meistens vorhandenen Internet-Zugänge auf eine preiswerte und breitbandige Plattform gestellt werden. Nachweislich sichere, für Anbieter und Betreiber leicht einzuführende Internet-Teleservice-Lösungen, die sich zentral verwalten und wirtschaftlich auf große Mengen anzubindender Systeme skalieren lassen, sind inzwischen verfügbar.

Ferndiagnose und Fernwartung industrieller Maschinen und Anlagen sind als Instrumente zur Reduktion von Servicekosten und Erhöhung der Verfügbarkeit seit Jahren anerkannt und verbreitet. Mit der zunehmenden Vernetzung von Maschinen und der Verfügbarkeit von Internet-Zugängen in diesem Umfeld wächst das Interesse, diese preiswerte und viel breitbandigere Infrastruktur anstelle traditioneller Modemverbindungen auch für den Teleservice zu nutzen. So erweisen sich nach Ansicht der Innominate Security Technologies AG die herkömmlich zu diesem Zweck genutzten Wahlverbindungen über Modems zunehmend als unwirtschaftlich, für die IT-Sicherheit problematisch und bezüglich Stabilität und Bandbreite ungenügend. Auch die Verfügbarkeit analoger Telefonleitungen im industriellen Umfeld und die Kompatibilität von Modems mit modernen TK-Anlagen werden als rückläufig gesehen. Statt dessen wolle der Kunde die Vorteile kostengünstiger Internet-Bandbreite und robuster TCP/IP-Verbindungen nutzen. Sie ermöglichen schnellere Downloads von Analyse- und Log-Daten, die Fähigkeit zum Upload umfangreicher Software-Updates und neue Dienste wie Internet-Telefonie (VoIP) oder der Übertragung von Kamerabildern (Streaming Video). Bislang bestand hier immer noch Unsicherheit, ob sich mit vertretbarem Aufwand ausreichend sichere Verbindungen zu hunderten oder gar tausenden von Maschinen über das notorisch unsichere Netz etablieren lassen. Die Kombination von Virtual Private Network (VPN) und Firewall-Technologien verpackt in einfach konfigurierbare und betreibbare Security Appliances macht es nun möglich.

Die Internet-Teleservice-Lösung

Innominate bietet auf Basis seiner Produktfamilie Mguard eine Lösung für die Fernwartung einzelner Maschinen und ganzer Anlagenetze über Internet. Sie umfasst



Teleservice-Szenario mit Innominat Mguard Security Appliances

VPN-Verbindungen, vom System im Betreiber-Netz ausgehend zum Teleservice Center inklusive einer konfliktfreien virtuellen Adressierung. Dabei stützt sie sich im Kern auf den offenen VPN-Standard IPsec (Internet Protocol Security). Das macht die Einführung minimal invasiv für Netzwerke und Firewalls der Betreiber, erhöht so deren Akzeptanz und reduziert gleichzeitig den Konfigurationsaufwand gegenüber bisher üblichen Ansätzen. Autarke Mguard Security Appliances in bzw. an jeder Maschine oder Anlage fungieren dabei als Träger der VPN- und Sicherheitsfunktionen. Durch ihren transparenten, von Innominat patentierten „Stealth Mode“ eignen sie sich auch zur Nachrüstung im Feld ohne Eingriffe in die zu wartenden Systeme oder deren umgebende Netzwerke vornehmen zu müssen. Firewall-Regeln beschränken den Datenverkehr durch die VPN-Tunnel auf zulässige Verbindungen und verhindern zugleich den unbefugten Zugriff über das zu wartende System hinaus ins Betreiber-Netz.

Funktionen für das Aktivieren und Deaktivieren der Teleservice-Verbindung lassen sich auf einfache Weise in die Bedienober-

flächen von Leitständen und Steuerungen integrieren. Der Betreiber hat so volle Kontrolle über die Verfügbarkeit der Verbindung. Neben stationären Teleservice-Arbeitsplätzen können über ein zentrales Techniker-Gateway auch mobile Service-Mitarbeiter und Zulieferer einen kontrollierbaren, sicheren Zugriff auf Anlagen mit aktiver Fernwartungsverbindung erhalten.

Optional kann die Lösung über ein Service Portal implementiert werden, das unter Einsatz von Virtualisierungs-Software die Notebooks und PC der Service-Techniker von den Netzwerkverbindungen zwischen Teleservice und ferngewarteten Systemen isoliert. Eine virtuelle Maschine auf dem zentral gepflegten Portal Server wird damit zum eigentlichen Teleservice-Arbeitsplatz; der Rechner des Technikers stellt nur noch ein Fenster auf dieser virtuellen Arbeitsumgebung bereit, ohne selbst mit dem Zielsystem verbunden zu sein. Das Risiko einer Ausbreitung von Schad-Software von insbesondere mobilen, schwerer gegen Infektionen schützenden Geräten auf die gewarteten Systeme (und umgekehrt) wird dadurch eingedämmt.



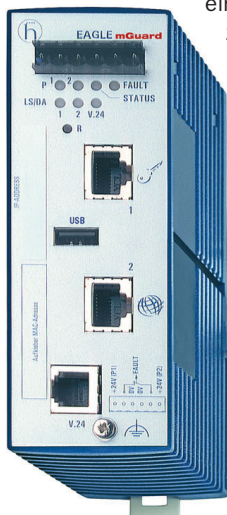
Teleservice in Safety-kritischen Umgebungen

Beim Betrieb Safety-kritischer Anlagen ist die Einhaltung entsprechender Unfallverhütungsvorschriften erforderlich, um die Gesundheit oder gar das Leben von Menschen nicht zu gefährden. Dies gilt umso mehr bei der Bedienung von Maschinen im Rahmen des Teleservice aus der Ferne, da sich der Bediener nicht mit eigenen Augen und Ohren vor Ort an der Anlage befindet. In diesen Fällen benötigt der Teleservice-Techniker einen autorisierten Partner vor Ort, der sich von der Einhaltung aller Sicherheitsvorschriften an der Anlage vergewissert, bevor ein Zugriff per Teleservice ermöglicht wird. Im Interesse der Prozesssicherheit und für den Schadens- und Haftungsfall muss die Identität der handelnden Personen zweifelsfrei feststellbar sein und dokumentiert werden.

Die Authentifikation von Bedienern und die Protokollierung von Zugriffen sind daher wesentliche Elemente einer Teleservice-Lösung für Safety-kritische Umgebungen. Dafür können an beiden Enden der Teleservice-Verbindung USB-basierte kryptografische Token („eToken“) mit starker 2-Faktor-Authentifikation nach dem Prinzip „Besitz

Andreas Beierer ist Director Marketing & Alliances und Torsten Rössel ist Director Business Development bei der Innominate Security Technologies AG in Berlin.

und Wissen“ eingesetzt werden. Die Token tragen in sich ein eindeutiges Zertifikat (Besitz), dessen Benutzung durch eine PIN (Wissen) freigeschaltet werden muss. Sowohl der Teleservice-Techniker als auch sein Safety-verantwortlicher Partner vor Ort müssen sich gegenüber dem (virtuellen) Service-Arbeitsplatz bzw. der Anlagensteuerung mit diesem Verfahren authentifizieren, damit eine Fernverbindung zustande kommt. Authentifikation, Verbindungsdauer sowie gegebenen-



Beispiele von Mguard-Produktvarianten zur Montage auf DIN-Hutschienen und im integrierbaren PCI-Kartenformat

Neuheiten zur Hannover Messe

Erweiterter Support für PKI und Zertifikate

Neue Software-Versionen der Mguard Security Appliances und des Innominate Device Managers (IDM) bieten jetzt eine vervollständigte Unterstützung für Standard PKI (Public Key Infrastructure) mit X.509-Zertifikaten und RSA Keys. Insbesondere die zentralen Mguard VPN Gateways in Teleservice-Szenarien können dadurch mit einer einzigen so genannten Tunnel Group Definition für eine hoch skalierbare Zahl möglicher VPN-Verbindungen konfiguriert werden. Digitale Zertifikate lassen sich nun auch zur passwortlosen, automatischen Authentifikation von Benutzern an den Mguard Web Interfaces und Command Line-Interfaces nutzen.

Management und Update von Firmware-Versionen

Der IDM kann nun auch Populationen von Mguard Appliances mit

gemischten Firmware-Ständen verwalten und kontrollierte Firmware-Updates im Push- und Pull-Verfahren durchführen.

Gruppierung von Firewall-Regeln, erweiterter Modem-Support, Quality of Service (QoS)

Firewall-Regeln können jetzt frei gruppiert und in solchen Gruppen selektiv (de-)aktiviert werden. Zugriffsrechte sind so etwa von einem Leitstand aus nach Bedarf dynamisch veränderbar. Erweiterter Modem-Support erlaubt nun auch abgehende Wählverbindungen und VPN über die serielle Schnittstelle. Dies eröffnet unter anderem Redundanz- und Failover-Lösungen für den Internet Teleservice bei Störungen der Ethernet-basierten Internet-Verbindung. Neue QoS-Funktionen unterstützen eine gezielte Priorisierung von Datenströmen bei schmalbandigen Verbindungen.

falls auch durchgeführte Aktionen werden zum späteren Nachweis protokolliert.

Schlüsselement: zentrales Management

Für die wirtschaftliche Skalierbarkeit einer Internet-Teleservice-Lösung auf hunderte oder gar tausende angebundener Systeme ist die Fähigkeit zum umfassenden Geräte-Management von einer zentralen Plattform aus unabdingbar. Der Innominate Device Manager (IDM) stellt eine solche Plattform mit Client/Server-Architektur dar. Alle Leistungsmerkmale und Einstellungen der Mguard Security Appliances können damit beim Roll-out für die Inbetriebnahme von Teleservice-Verbindungen zentral konfiguriert und verwaltet werden. Kontrollierte Updates von Firmware und Konfiguration der Geräte sind im laufenden Betrieb möglich und können bei bestehender Teleservice-Verbindung aufgespielt (Push-Verfahren) oder von den Geräten eigenständig heruntergeladen und aktiviert werden (Pull-Verfahren).

Durch das Anlegen von ausgefeilten, mehrstufigen Vorlagen (Vererbungstechnik), die intelligente Verwaltung virtueller Adresspools und eine integrierte Certificate Authority zur Erzeugung der VPN-Zertifikate wird mit dem IDM ein hoher Automatisierungsgrad bei der Konfiguration und Inbetriebnahme einzelner Geräte erzielt. Diese Elemente ermöglichen auch eine praxisnahe Arbeitsteilung. Wenige IT-Security-Administratoren mit tieferer Expertise gestalten die Vorlagen mit den komplexeren, sicherheitsrelevanten Bestandteilen, während eine größere Zahl von Technikern schon nach kurzer Einweisung Mguard-Geräte mithilfe der Vorlagen auslieferungsfähig konfektionieren und in Betrieb nehmen kann, sind die Erfahrungen des deutschen Spezialisten für industrielle Netzwerksicherheit.

Fazit

Der Trend zur Ablösung herkömmlicher Modem-Wählverbindungen für den Teleservice durch Internet- und VPN-basierte Lösungen ist klar motiviert und erkennbar. Die resultierenden Anforderungen sind heute erfüllbar und der Übergang hat bereits begonnen. Innominate bietet auf Basis seiner industrietauglichen Mguard Security Appliances und des Innominate Device Managers eine sichere, zentral verwaltbare und technisch-wirtschaftlich skalierbare Lösung, maßgeschneidert auf die Bedürfnisse des Maschinen- und Anlagenbaus und seiner Kunden.

Andreas Beierer, Torsten Rössel