kontron

» Application Story «

KISS in Communications

Hochverfügbare Emb. Server für sichere Teleservices

Kontron KISS Server im Einsatz als High-End Firewall & VPN Gateway für industrielle Teleservices

Für die sichere Fernwartung und -diagnose von Maschinen und Anlagen via Internet hat Innominate eine hochverfügbare 19- Zoll Network Security Lösung entwickelt, die in Servicezentralen als High-End Firewall und VPN-Gateway zum Einsatz kommt. Dort bedient sie eingehende Anforderungen zum Aufbau von VPNs und hält dann diese sicheren Virtual Private Network Verbindungen zu den entfernten industriellen Systemen aufrecht. An diesen Knotenpunkt werden höchste Verfügbarkeitsanforderungen gestellt, da er für bis zu 1000 gleichzeitige VPN-Verbindungen verantwortlich ist. Die hierfür verwendete Serverhardware stammt von Kontron. Sie erfüllt Verfügbarkeitsanforderungen, wie sie sonst nur in Carrier-Grade Telekommunikationsplattformen zu finden sind. Dies jedoch zu industriegerechten Preisen.

Um Anlagenbetreiber zu unterstützen, stellen Hersteller von Maschinen und Anlagen immer häufiger auch Teleservices zur Fernwartung und zum Remote Monitoring bereit. Durch die weltumspannend möglichen Kommunikations¬verbindungen zwischen lokalen Bedienern und Experten in entfernten Servicezentralen können kostenintensive Einsätze vor Ort eingespart und Ausfallzeiten extrem reduziert werden. Zudem eröffnen die hohen Bandbreiten der zumeist schon an den Maschinen vorhandenen Ethernet-Schnittstellen neue, sehr effiziente Serviceperspektiven und damit Wettbewerbsvorteile, beispielsweise durch die Nutzung aktueller Internet-Technologien wie Voice-Over-IP und dem Streaming von Bild- und Videodaten.

Modems nicht mehr zeitgemäß

Seit Mitte der 90er Jahre und noch bis heute werden Teleservices größtenteils über Wählleitungen mit Analogmodems oder ISDN-Terminaladaptern erbracht. Neben dem hohen Aufwand für die Telefoninfrastruktur, den zusätzlichen Verbindungskosten und dem geringen Datendurchsatz haben Modemverbindungen zudem den Nachteil, dass jede einzelne Anbindung an das Telefonnetz als sogenannte „Backdoor“ auch ein zusätzliches Sicherheitsrisiko für das Unternehmensnetzwerk darstellt. Nicht zuletzt deshalb besteht in letzter Zeit ein starker Trend hin zu modernen, breitbandigen, durch VPN- und Firewall-Technologie gesicherten Internet-Verbindungen für solche Dienste. Da moderne Maschinen und Anlagen zumeist über Ethernet-Schnittstellen verfügen und häufig bereits in Unternehmensnetzwerke integriert sind, liegt es nahe, die Fernwartung der Anlagen über eine TCP/ IP-Internetverbindung via Ethernet zu realisieren. Die Nutzung von Internet-Verbindungen zur Fernwartung von Industrieanlagen und Maschinensystemen bringt gleich mehrere Vorteile: Der Aufwand für die Telefoninfrastruktur, welcher für den Teleservice via Modem für jede einzelne Maschine betrieben werden musste, entfällt. Zugleich fallen auch keine Verbindungskosten ins Ausland an und der Datendurchsatz wird enorm gesteigert. Und durch aktuelle Internet-Technologien wie Voice-over-IP und Streaming von Bild- und Videodaten ergeben sich zusätzlich neue, sehr effiziente Serviceperspektiven und damit Wettbewerbsvorteile.

Doch um von dieser schönen neuen Internetwelt auch auf Maschinenebene profitieren zu können, bedarf es zunächst einiger Sicherheitsvorkehrungen. Denn keine Maschine sollte ohne weiteres direkt aus dem Internet erreichbar und damit für Dritte technisch kompromittierbar sein. Um den gewünschten sicheren Zugriff auf Systeme, Maschinen und ganze Maschinenetze via TCP/IP zu ermöglichen, suchen Hersteller und Betreiber deshalb nach einer wirtschaftlichen Sicherheitslösung für Teleserviceanwendungen, die durch Verschlüsselungstechnik die Authentisierung, Vertraulichkeit und Integrität des Datenverkehrs gewährleistet und unerwünschten Datenverkehr durch Firewalls ausschließt. Im Idealfall sollte diese auch mit geringem Aufwand in die vorhandenen Netzwerkstrukturen integrierbar sein.

Eine Rundum-Sicherheitslösung für Unternehmensnetze

Eine solche Sicherheitslösung bietet Innominate, Spezialist für Network Security Appliances, mit seinem mGuard Produktportfolio. Eine Innovation dieser integrierten Komplettlösung auf Basis bewährter Standard-Technologien besteht darin, den Ansatz für die Durchführung von Fernwartungsservices umzukehren: musste bisher eine Verbindung vom Servicetechniker zum System aufgebaut werden, wird beim mGuard Teleservice-Konzept von Innominate die Verbindung vom System zum Service hergestellt. Der Verbindungsaufbau zur Maschine wird somit nicht mehr von außen initiiert, sondern beginnt bei der Maschine als ausgehende Verbindung zu einer vorher definierten Gegenstelle. Damit werden typische Zugangsprobleme aufgrund von Sicherheits-Policies und Firewalls gelöst, da ausgehende Internet-Verbindungen mit fest definierten VPN-Tunnelpartnern entscheidend einfacher und sicherer zu administrieren sind. Das mGuard Konzept wurde speziell für den Einsatz im industriellen Umfeld entwickelt und kombiniert die Eigenschaften einer sogenannten Stateful Inspection Firewall, die eingehende und ausgehende Datenpakete anhand vordefinierter Regeln überwacht, mit der Möglichkeit einer sicheren und vertraulichen Kommunikation über verschlüsselte Virtual Private Network Verbindungen (VPNs).

Für jede Anlage die passende Lösung

Um Netzwerke, Produktionszellen oder einzelne Automatisierungsgeräte zu schützen, stellt Innominate mit dem mGuard Portfolio verschiedene Network Security Appliances bereit, die einfach in Ethernet-basierte Produktionsnetzwerke integrierbar sind. Feldtaugliche mGuard Komponenten werden beispielsweise als externe Hutschienengeräte oder PCI-Karten zur Integration in die dezentralen Systeme bereit gestellt. Eine interessante Bauformvariante für 19-Zoll Umgebungen und hohe Verfügbarkeitsanforderungen ist darüber hinaus das mGuard bladePack. Mit redundanter Stromversorgung und Hot-Swap-fähigen Blade-Einschüben kann dieses bis zu zwölf Systeme oder Subnetze individuell vernetzen und absichern und als VPN-Gateway von 250 bis 3000 VPN-Tunneln skaliert werden.

Allen Geräten gemeinsam ist neben einem integrierten WebGUI zur lokalen Administration die Fähigkeit zum zentralen Management durch den Innominate Device Manager (IDM). Dieser bietet einen Vorlagen-Mechanismus, mit dem Anwender zentral alle ihre mGuard Geräte höchst effizient konfigurieren und verwalten können. Ist die feldseitige Installation abgeschlossen, können die Geräte auf einzelne Anforderung oder permanent VPN-Verbindungen zu den zentralen Servicepunkten

von Teleservice-Anbietern aufbauen. In der Regel erfolgt dies unter Kontrolle des Maschinen- oder Anlagenbetreibers, der den Teleservicedienst so nach Bedarf nutzen und den Verbindungszustand jederzeit überwachen kann. Um eine VPN-Verbindung aufbauen zu können, bedarf es natürlich auch einer Gegenstelle auf der zentralen Serviceseite. Genau für solche Gegenstellen hat Innominate nun ein neues System entwickelt, um diesen zentralen Knotenpunkt für die Verbindungen zu großen Mengen von Feldgeräten noch effizienter zu gestalten (vgl. Photo. 1).

Neues Firewall- & VPN-Gateway ergänzt die mGuard-Familie

Der neue Innominate mGuard centerport im 19-Zoll-Format erfüllt alle High-End-Firewall- und VPN-Gateway-Funktionen, die man für eine sichere Anbindung sehr vieler dezentraler Feldgeräte benötigt. Vorteilhaft bei dem neuen System ist, dass alle VPN-Verbindungen über eine einzige öffentliche IP-Adresse geroutet werden. Beim bislang verfügbaren modularen mGuard bladePack waren dazu noch bis zu zwölf IP-Adressen erforderlich, also jeweils eine IP-Adresse pro Blade-Steckplatz. Konfiguration und Administration sind dadurch beim mGuard centerport deutlich einfacher, da man sich um das Load-Balancing zwischen verschiedenen Gateway-Adressen keine Gedanken machen muss und nur eine öffentliche IP-Adresse benötigt wird. Ferner werden statt Fast Ethernet (100 MBit/s) nun Gigabit Ethernet (1.000 MBit/s) Schnittstellen eingesetzt, über welche der mGuard centerport 1.000 gleichzeitig aktive VPN-Tunnel aufrecht erhalten kann und dabei einen verschlüsselten Datendurchsatz von 300 MBit/s erreicht – die gut vierfache Leistung eines mGuard blades. Der mGuard centerport ist voll kompatibel zu allen mGuard VPN Feldgeräten und dem Innominate Device Manager, wodurch sich Integration und Einrichtung denkbar einfach gestalten. Hardwareseitig genügt es, das Servicenetzwerk mit dem rückseitig ausgeführten LAN-Port zu verbinden und den WAN-Port mit einem Internet-Zugang zu versorgen. Über zwei redundante Netzteile mit Strom versorgt, kann das Gateway nach seiner Erstinbetriebnahme über das integrierte Webinterface fortan hochautomatisiert über den Innominate Device Manager verwaltet werden. Und sollte das System einmal neu gestartet werden, sind die bis zu 1.000 VPN-Tunnel dank der hohen Systemperformance in weniger als 5 Minuten wieder aufgebaut, was höchste Verfügbarkeit für Teleserviceanwendungen gewährleistet.

„Six nines“ im Visier

Für die neue 19-Zoll Lösung, die als Knotenpunkt im Unternehmensnetzwerk den Teleservice und damit die Verfügbarkeit zahlreicher Maschinen und Anlagen gewährleistet, wurden hohe Anforderungen an die Hardware gestellt: Das System sollte zum einen eine hohe Performance bieten, um die bis zu 1000 VPN-Tunnel auch effizient und ohne spürbare Zeitverzögerungen zu handhaben. Zum anderen sollten die hochperformanten Systeme auch Bestwerte in Bezug auf MTBF (Mean Time Between Failures) aufweisen, denn an eine solche Serverplattform werden Anforderungen gestellt, die mit denen von Carrier-Grade Telekom-Netzen vergleichbar sind. Zwar ist es nicht immer erforderlich, dass die Systeme redundant ausgelegt werden oder Hot-Swap Baugruppen besitzen, doch in Hinblick auf die Qualität der verwendeten Komponenten und des Boarddesigns suchte man nach einer Lösung, die auf höchste Verfügbarkeiten ausgelegt ist und beispielsweise ein redundantes Netzteil sowie RAID-Festplattensupport bietet, um so die anfälligsten Komponenten in Computersystemen höchst ausfallsicher zu machen. „Ideale Voraussetzungen liefern Systeme, die an Verfügbarkeiten von 99,9999 Prozent

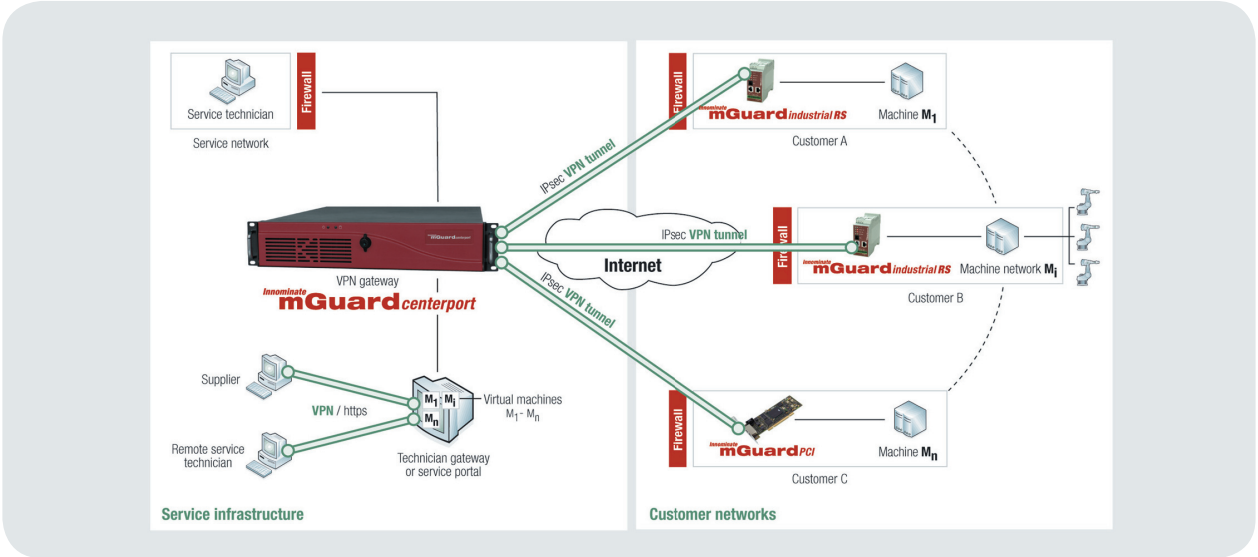

Photo 1: Effiziente Serviceinfrastrukturen: Der auf Basis des Industrieservers Kontron KISS 2U entwickelte mGuard centerport bedient als zentrales Gateway die von mGuard Feldgeräten eingehenden Anforderungen zum Aufbau von VPNs und unterhält gesicherte Virtual Private Network Verbindungen zu einer Vielzahl verteilter industrieller Systeme.

heranreichen, also Six Nines bieten“, stellt Torsten Rössel, Director Business Development bei Innominate, fest. „Eine bezahlbare Lösung in diese Richtung haben wir gesucht.“

Systemhardware und Baugruppen aus einer Hand

Entschieden hat sich Innominate für die KISS-Serverfamilie (Kontron Industrial Silent Server) von Kontron, die auch in der Netzleittechnik von Energie-versorgungsunternehmen, in der Leittechnik für den Schienenverkehr, in der Medizintechnik oder gar in Kernkraftwerken zum Einsatz kommt und entsprechend hochverfügbar sein muss. Dank Intel AMT Support können sie sogar optional auch mit In-Band sowie Out-Of-Band Monitoring Funktionen ausgerüstet werden und damit bis auf Hot-Swap-Fähigkeit der Baugruppen nahezu alle Anforderungen erfüllen, wie sie auch in Carrier-Grade Telekommunikationsnetzwerken gestellt werden. Für Innominate ausgerüstet mit redundantem Netzteil, Gigabit Ethernet und Intel® Core™2 Quad Prozessor ist der 19-Zoll / 2HE Server KISS 2U einer der derzeit kleinsten und schnellsten Hochverfügbarkeits-Server für langzeitverfügbare und robust auszulegende Applikationen. Dass man sich für eine Hardwareplattform von Kontron entschied, hatte nach Angaben von Torsten Rössel, Director Business Development bei Innominate, mehrere Gründe: „Kontron ist für uns ein namhafter und als Lieferant unseres Mutterkonzerns Phoenix Contact bereits bewährter Hersteller von Industrie-PCs. Wichtige Aspekte waren aber auch eine geeignete Modellpalette mit Skalierbarkeit nach oben und unten, die mögliche Gestaltung des Systems als OEM-Produkt mit eigenem Branding, die längerfristige Verfügbarkeit einer genau spezifizierten Hardware-Konfiguration, die Produkt-Qualität und der lokale Support durch einen deutschen Hersteller.“ Für Innominate wurde der Server von Kontron individuell mit einem platzsparenden PICMG 1.3 Slotboard, einer High-Performance Backplane, 4 Port Gigabit Ethernet-Karte und einem kundenspezifischen Frontdesign ausgestattet. Das System und alle Baugruppen kommen bei Kontron aus einer Hand, was beste Kompatibilität und Zuverlässigkeit des Gesamtsystems gewährleistet. Die MTBF liegt bei 50.000 Stunden, was in etwa 5,7 Jahren Dauereinsatz entspricht. Zudem ist der Server mindestens 5 Jahre bei Kontron verfügbar. So wird eine homogene Hardwarestruktur ermöglicht, was im Servicefall für Innominate besonders effizient ist und zudem die Investitionen in die kunden-spezifische Hardwareplattform besonders sicher macht.

Kontron KISS 2U Server

Individuell konfigurierbar Kontron KISS 2U Industrieserver werden von Innominate als spezifisch und hochverfügbar ausgelegte OEM-Plattform für High-End Firewalls & VPN Gateways genutzt. Als COTS-Systeme sind die Kontron KISS-2U Server individuell mit PICMG 1.3 und PICMG 1.0 Slotboards oder Flex-ATX Motherboards bestückt und entsprechend besonders flexibel ausbaubar. Besonders dicht gepackt und damit platzsparend sind PICMG 1.x Konfigurationen mit bis zu fünf Erweiterungskarten. Im Standardausbau mit Flex-ATX Motherboards sind zwei PCI Erweiterungskarten möglich.

OEM Security Appliances

Kundenspezifische Network Security Appliances auf Basis der vorgestellten Innominate mGuard und Kontron KISS Technologien sind als weitere OEM-Varianten realisierbar. Interessiert? Sprechen Sie uns an!

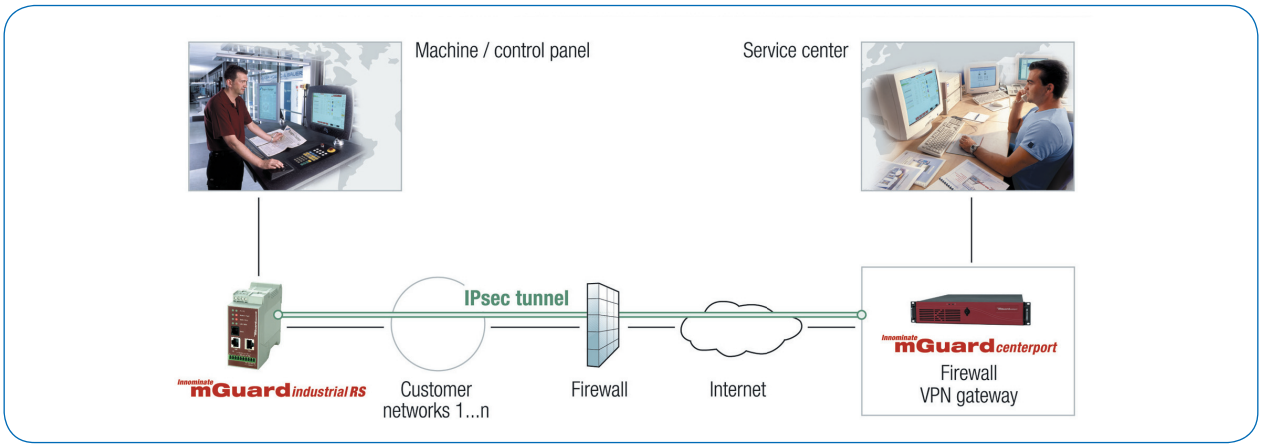

Abb. 2: Skalierbar verbunden: Dank des neuen mGuard centerport können Servicezentralen und Condition Monitoring Dienste über verschlüsselte VPN-Tunnel mit bis zu 1000 weltweit verteilten Systemen gleichzeitig verbunden sein.

Über Innominate Security Technologies AG

Innominate, ein Phoenix Contact Unternehmen, ist führender Hersteller von Komponenten und Lösungen für die kontrollierte und gesicherte Kommunikation in industriellen Netzwerken. Kerngeschäftsfelder sind die Absicherung vernetzter industrieller Systeme und die sichere Fernwartung von Maschinen und Anlagen über das Internet. Die Innominate mGuard Netzwerksicherheitsgeräte verfügen über Router, Firewall, Virtual Private Network (VPN) sowie Quality of Service (QoS) Funktionalitäten und unterstützen bei Intrusion Detection und Antiviren-Schutz. Ergänzt wird das mGuard Portfolio durch eine hoch skalierbare Device Management Software. Produkte von Innominate werden unter der Marke mGuard von Systemintegratoren sowie über OEM-Partner weltweit vertrieben.

Weitere Informationen finden Sie unter **www.innominate.de**

About Kontron

Kontron is a global leader in embedded computing technology. With more than 40% of its employees in research and development, Kontron creates many of the standards that drive the world's embedded computing platforms. Kontron's product longevity, local engineering and support, and value-added services, helps create a sustainable and viable embedded solution for OEMs and system integrators.

Kontron works closely with its customers on their embedded application-ready platforms and custom solutions, enabling them to focus on their core competencies. The result is an accelerated time-to-market, reduced total-cost-of-ownership and an improved overall application with leading-edge, highly-reliable embedded technology.

Kontron is listed on the German TecDAX stock exchanges under the symbol "KBC". For more information, please visit: **www.kontron.com**

CORPORATE OFFICES

Europe, Middle East & Africa
Lise-Meitner-Str. 3-5
86156 Augsburg
Germany
Tel.: +49 (0) 821 4086-0
Fax: +49 (0) 821 4086 111
sales@kontron.com

North America
14118 Stowe Drive
Poway, CA 92064-7147
USA
Tel.: +1 888 294 4558
Fax: +1 858 677 0898
info@us.kontron.com

Asia Pacific
17 Building,Block #1, ABP.
188 Southern West 4th Ring Road
Beijing 100070, P.R.China
Tel.: +86 10 63751188
Fax: +86 10 83682438
info@kontron.cn