

Bild 1: Skalierbar verbunden: Dank des mGuard centerport können Servicezentralen und Condition Monitoring Dienste über verschlüsselte VPN-Tunnel mit bis zu 1.000 weltweit verteilten Systemen gleichzeitig verbunden sein.



Sicherer Teleservice

Hochverfügbare Embedded Server

Halle 9
Stand D18

Für die sichere Fernwartung und -diagnose von Maschinen und Anlagen via Internet hat Innominate eine hochverfügbare 19" 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. Dieser Knotenpunkt ist für bis zu 1.000 gleichzeitige VPN-Verbindungen verantwortlich. 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 Kommunikationsverbindungen 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. 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 Maschinennetze 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 uner-

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, effiziente Serviceperspektiven und damit Wettbewerbsvorteile.

wünschten 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).

Individuelle Lösungen

Um Netzwerke, Produktionszellen oder einzelne Automatisierungsgereäte 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 z.B. als externe Hutschienengeräte oder PCI-Karten zur Integration in die dezentralen Systeme bereit gestellt. Eine interessante Bauformvariante für 19"-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 Manage-

ment durch den Innominate Device Manager (IDM). Dieser bietet einen Vorlagen-Mechanismus, mit dem Anwender zentral alle ihre mGuard Geräte 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.

Firewall- & VPN-Gateway ergänzt die mGuard-Familie

Der neue Innominate mGuard centerport im 19"-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 automatisiert 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 fünf Minuten wieder aufgebaut, was eine hohe Verfügbarkeit für Teleserviceanwendungen gewährleistet.

'Six nines' im Visier

Für die neue 19"-Lösung, die als Knotenpunkt im Unternehmensnetzwerk des Teleservice und damit die Verfügbarkeit zahlreicher Ma-

schinen und Anlagen gewährleistet, wurden hohe Anforderungen an die Hardware gestellt: Das System sollte zum einen eine hohe Performance bieten, um die bis zu 1.000 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



Bild 2: 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 flexibel ausbaubar. 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.

in Hinblick auf die Qualität der verwendeten Komponenten und des Boarddesigns suchte man nach einer Lösung, die auf hohe Verfügbarkeiten ausgelegt ist und z.B. ein redundantes Netzteil sowie RAID-Festplattensupport bietet, um so die anfälligsten Komponenten in Computersystemen ausfallsicher zu machen. „Ideale Voraussetzungen liefern Systeme, die an Verfügbarkeiten von 99,9999% heranreichen, also 'Six Nines' bieten“, stellt Torsten Rössel, Director Business

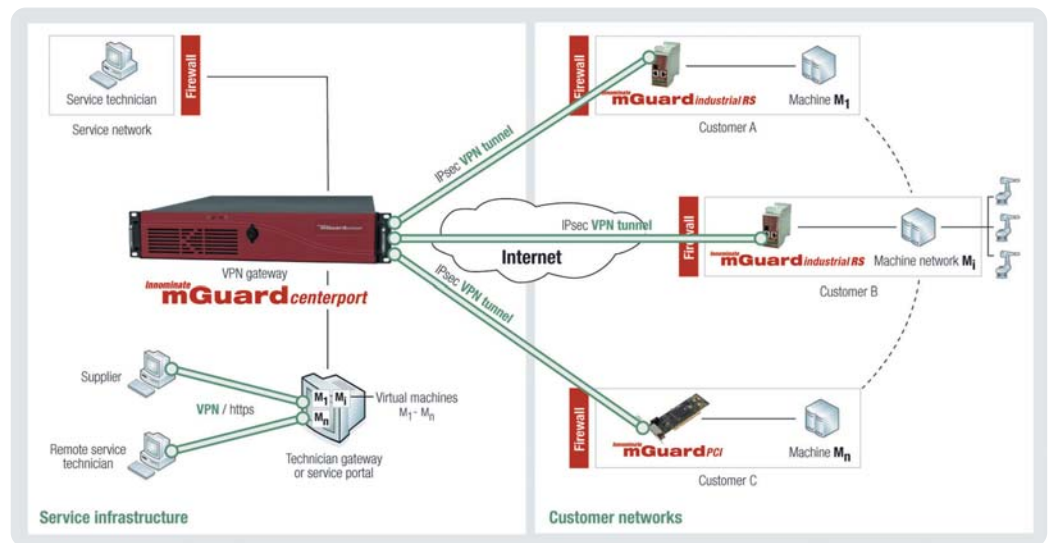


Bild 3: Effiziente Serviceinfrastrukturen: Der auf Basis des Industrieressers Kontron KISS 2U entwickelte mGuard centerport bedient als zentrales Gateway die von mGuard Feldgeräten eingehenden Anforderungen zum Aufbau von VPNs und unterhält gesicherte Virtual Private Network Verbindungen zu einer Vielzahl verteilter industrieller Systeme.

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 Energieversorgungsunternehmen, 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 Core2 Quad Prozessor ist der 19" / 2HE Server KISS 2U einer der derzeit kleinsten und schnellsten Hochverfügbarkeits-Server für langzeitverfügbare und robust auszuführende Applikationen. Dass man sich für eine Hardwareplattform von Kontron entschied, hatte nach Angaben von Torsten Rössel, 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 die Standardkonfiguration des Innominate centerports wurde der Server von Kontron individuell mit einem kundenspezifischen Frontdesign, einem platzsparenden PICMG 1.3 Slotboard, einer High-Performance Backplane sowie einer 4 Port Gigabit Ethernet-Karte ausgerüstet. Neben dieser Standardkonfiguration können aber auch kundenspezifische Varianten mit einer veränderten Hardwarekonfiguration umgesetzt werden. Das System und alle Baugruppen kommen bei Kontron aus einer Hand, was die Kompatibilität und Zuverlässigkeit des Gesamtsystems gewährleistet. Die MTBF liegt bei 50.000h, was in etwa 5,7 Jahren Dauereinsatz entspricht. Zudem ist der Server mindestens fünf Jahre bei Kontron verfügbar. So wird eine homogene Hardwarestruktur ermöglicht, was im Servicefall für Innominate effizient ist und zudem die Investitionen in die kundenspezifische Hardwareplattform besonders sicher macht. ■

www.kontron.de



Autor: Günter Dumsky,
Director Systems & Boards, Kontron