

Fernwartung weltweit: Zugänge per Internet schaffen die Voraussetzungen für den notwendigen umfangreichen und sicheren Datenaustausch.

Teleservice goes Internet

Kostengünstige und sichere Lösungen für die Fernwartung von Druckmaschinen

Der Druckmaschinen-Hersteller Koenig & Bauer rüstet seine Produkte mit mGuard-Produkten des Security-Spezialisten Innominat aus. Damit schafft er die Voraussetzungen zur sicheren Fernwartung per Internet.

Druckmaschinen bieten so ziemlich alle Eigenschaften, die einen Instandhalterjob interessant, herausfordernd und zuweilen sogar atemberaubend gestalten: Es sind teure und komplexe Anlagen, an deren Verfügbarkeit hohe Anforderungen gestellt werden. Denn nichts ist verderblicher als Neuigkeiten, deshalb arbeiten Druckereien meist nach sehr engen Produktionsplänen.

Zudem werden die Druckereiausrüstungen der großen Hersteller weltweit vertrieben, sind also oft sehr weit vom Herstellungsort installiert. Das Klischee vom ‚rasenden Servicetechniker‘, der mit Spezialwerkzeug, vor allem aber mit sei-

nem ganz speziellen Wissen als Troubleshooter durch die Welt jettet, um bei Kunden schnell Wunder zu wirken, hat hier eine seiner sehr realen Quellen. Allerdings sind Rat und Tat dieses Servicetechnikers nicht nur gut, sondern auch teuer, allein schon wegen des Reiseaufwandes.

Nicht zuletzt ist auch der Monteur vor Ort auf zusätzliche Informationen angewiesen. Er muss im einfachsten Fall beim Hersteller-Mutterhaus anfragen, er benötigt Auszüge aus Handbüchern, Stromlaufpläne oder einfach zusätzlichen Expertenrat.

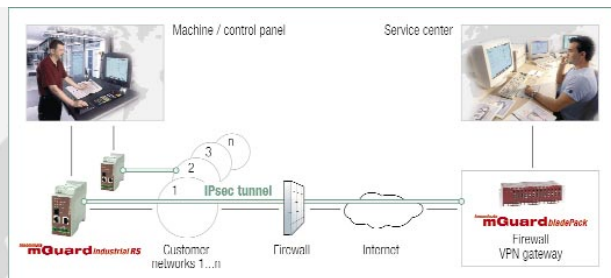
Wie bekommt er das alles? Im einfachsten Fall per Telefon und Fax, vielleicht über ISDN, wenn so etwas am Aufstellungsort der Maschine verfügbar ist. Und selbst wenn – ein Datendurchsatz von 128 kBit/s erlaubt am Ende auch nur einen beschränkten Informationsaustausch. Hinzu kommt, dass jedes Modem für das gesamte Netzwerk eines Unternehmens ein Sicherheitsrisiko darstellt. Direkt in ein Steuerungsnetzwerk einge-

bunden bildet es eine ‚Backdoor‘, die IT-Sicherheitsexperten nicht mehr bereit sind zu akzeptieren. Das gilt auch und nicht zuletzt für die Steuerungen von Druckmaschinen.

„Deshalb haben wir nach neuen Wegen der Fernwartung gesucht“, blickt Andreas Birkenfeld, Bereichsleiter Systemtechnik bei Koenig & Bauer, zurück und ergänzt: „Die Nutzung breitbandiger Inter-

Internetgestützte Virtual Private Networks eröffnen neue Perspektiven

net-Verbindungen bot sich geradezu an. Die Verbindungskosten sind hier kaum nennenswert. Der Datendurchsatz erreicht mehrere MBit/s bei xDSL-Internet, und es stehen Technologien wie Voice over IP – also Internet-Telefonie – oder das Streaming von Bild- und Videodaten zur Verfügung. Internetgestützte Virtual Private Networks (VPN) eröffnen völlig neue Service-Perspektiven.“ Für die



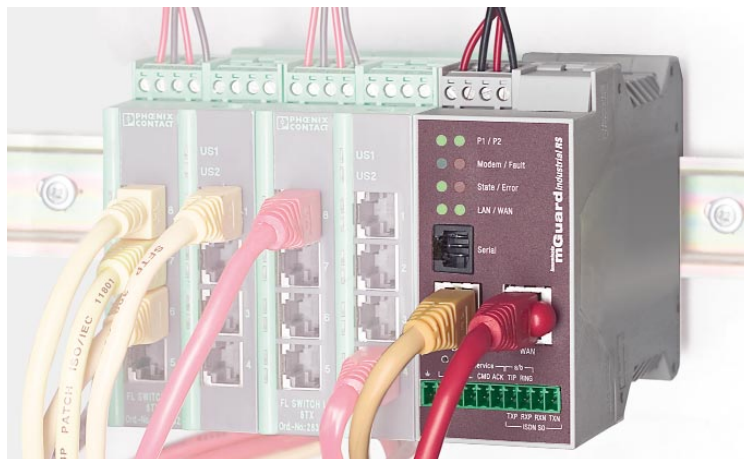
VPN-gesicherte Teleservice-Verbindung per Internet: Industrie-Firewalls sorgen für den kontrollierten Zugang in das Produktionsnetz.



Internet-Fernwartung der Druckmaschinen bei Koenig & Bauer entwickelte das auf industrielle Netzwerksicherheit spezialisierte Berliner Unternehmen Innominate schließlich eine integrierte Komplettlösung. Sie nutzt Standardtechnologien, die inzwischen auf dem Markt angeboten werden.

Ein wichtiges Merkmal dieses Systems besteht darin, dass die bisher übliche Abfolge bei Fernwartungsarbeiten umgekehrt wird. Bisher baute der Servicetechniker eine Verbindung zum System auf. Nach dem neuen ‚ausgehenden VPN-Konzept‘ kann nun der Verbindungsaufbau vom System hin zur Servicezentrale erfolgen. Dieser ‚feine Unterschied‘ ist entscheidend, öffnet er doch der Fernwartung den Weg über das Internet.

„Alle bisher vorhandenen Zugangsprobleme, die sich aus der Sicherheitspolitik der Betreiberfirmen von Maschinen und Ausrüstungen ergaben, lassen sich so mit einem Schlag lösen. Denn die ausgehenden Internet-Verbindungen werden nicht mehr durch die zentralen Unternehmens-Firewalls beeinträchtigt, sie sind entscheidend einfacher und entsprechend sicher zu administrieren“, beschreibt Torsten Rössel, Director Business Development bei Innominate, die für Koenig & Bauer umgesetzte Lösung.



mGuard industrial RS: Vielseitige Network Security Appliance für die Hutschiene mit optional integriertem Modem.

Als Hardware, mit der die Funktionen der so genannten mGuard-Technologie umgesetzt werden, dienen autarke Security Appliances. Diese elektronischen Module lassen sich in verschiedenen Bauformen in die zu wartenden Systeme integrieren. So stehen beispielsweise Geräte zur Verfügung, die auf DIN-Hutschienen im Schaltschrank einer Druckanlage oder als PCI-Steckkarten in den Steuerungsrechner einer Bogenoffsetmaschine eingebaut werden.

Als Gegenstelle im Servicezentrum von Koenig & Bauer wird ein skalierbares ‚Blade-Pack‘ installiert. Dieses kann bis

zu zwölf Blade-Einschübe in einem 19-Zoll-Chassis (3 HE) aufnehmen und so flexibel 250 bis 3 000 definierte sichere Teleservice-Verbindungen unterstützen. Die mGuard-Plattform arbeitet völlig eigenständig.

Die zur Fernwartung per Internet notwendigen Systeme lassen sich mit dieser Technik ohne großen Konfigurationsaufwand in jede Standard-Ethernet-Umgebung integrieren. Sie sind zu jedem Betriebssystem kompatibel und erfordern keinerlei Konfigurationsänderungen, weder am bestehenden Netzwerk noch am fernzuwartenden System.

Die Security-Funktionen

Mit Hilfe der in den Druckmaschinen von Koenig & Bauer eingesetzten dezentralen Security-Appliance lassen sich IP-basierte Netzwerk-Verbindungen zu industriellen Systemen und Anlagen zuverlässig absichern. Das geschieht mit Hilfe folgender Funktionen:

- Konfigurierbare Firewall zum Schutz vor unberechtigten Zugriffen und Verbindungen. Die Stateful Inspection Firewall untersucht ein- und ausgehende Datenpakete anhand der Ursprungs- und Zieladressen und blockiert unerwünschten Datenverkehr in beiden Richtungen.
- Flexibler Netzwerkbetrieb im Router-Modus zur Netztrennung oder im so genannten Stealth-Modus zur transparenten Integration in bestehende Netze. Im Stealth-Modus übernimmt die Appliance an ihrem externen Ethernet-Interface die Netzwerk-Adressen (MAC und IP) des zu schützenden Systems. Somit ist es selbst nicht zu erkennen und infolgedessen auch nicht angreifbar.
- VPN-Router (optional) für sichere Datenübertragung in öffentlichen Netze. Zum Einsatz kommen wahlweise eine hardware-beschleunigte DES-, 3DES- oder AES-Verschlüsselung und das standardisierte IPsec-Protokoll.
- Router- und Firewall-Redundanz (optional) für Industrial-Network-Security-Lösungen mit automatischem Master/Slave Failover.

Die Sicherheit der Teleservice-Verbindung wird durch VPN-Technologie auf Basis des IPsec-Standards garantiert. Dabei kann der Endkunde das Öffnen und Schließen der VPN-Tunnel steuern und die zulässige Kommunikation mit Hilfe von Firewall-Regeln gezielt auf das gewünschte, notwendige Maß beschränken. Um eine Internet-Teleservice-Lösung mit hunderten oder gar tausenden angebundener Systeme wirtschaftlich betreiben zu können, muss unbedingt die Möglichkeit der umfassenden Gerätesteuerung von einer zentralen Plattform aus bestehen. Der Innominat Device Manager (IDM) stellt eine solche Plattform mit Client/Server-Architektur dar. Alle Leistungsmerkmale und Einstellungen der Security-Appliances lassen sich damit beim Roll out für die Inbetriebnahme von Teleservice-Verbindungen zentral konfigurieren und verwalten.

Es ist auch möglich, während des laufenden Betriebs Updates von Firmware und Konfigurationsänderungen der Geräte vorzunehmen. Diese können bei be-

stehender Teleservice-Verbindung aufgespielt (Push-Verfahren) oder von den Geräten eigenständig heruntergeladen werden (Pull-Verfahren). Mit Hilfe des IDM lässt sich die Konfiguration und Inbetriebnahme einzelner Geräte stark automatisieren. Dafür sorgen ausgefeilte Vorlagen, sichere Vererbungstechniken, die intelligente Verwaltung der virtuellen

Änderungen am Ethernet oder am System sind nicht notwendig

Adress-Pools sowie die integrierte Certificate Authority zur Erzeugung der VPN-Zertifikate. Diese Elemente ermöglichen auch eine praxisnahe Arbeitsteilung: Wenige hoch qualifizierte IT-Security-Administratoren gestalten dabei die Vorlagen mit den komplexeren, sicherheitsrelevanten Bestandteilen. Eine größere Anzahl von Technikern ist dann bereits nach kurzer Einweisung in der Lage, die Geräte mithilfe der Vorlagen auslieferungsfähig zu konfigurieren und in Betrieb zu nehmen.

Koenig & Bauer hatte in der Pilotphase weltweit mehr als 20 Druckanlagen mit der mGuard-Komplettlösung ausgerüstet, um Erfahrungen mit dem Internet-basierten Teleservice zu sammeln. Unter anderem wurde dabei ein Formblatt entwickelt, mit dessen Hilfe sich das IT-Umfeld und die besonderen Anforderungen der Kunden spezifizieren lassen.

Auf diese Weise wird es möglich, Konfiguration, Funktionstest und Abnahme der Appliance bereits im Werk vorzunehmen. Vor Ort braucht der Monteur dann im Idealfall das System nur noch mit Datenleitung und Versorgungsspannung zu verbinden. Durch die weitgehend standardisierte Konfiguration der Appliances reduziert sich der administrative Aufwand auf ein Minimum.

„Bei guter Vorbereitung können wir per Plug&Play installieren“

„Bei ausreichender Vorklärung durch den Kunden können wir sogar eine echte Plug&Play-Installation erreichen“, schätzt Birkenfeld ein. Und auch zu den künftigen Möglichkeiten der Lösung gibt es schon konkrete Vorstellungen: „Wir denken, dass es sinnvoll ist, den Device Manager um Monitoring-Funktionalität für die laufende Zustandsüberwachung und Logging-Funktionalität für die Aufzeichnung von Ereignissen zu erweitern.“ Innominat hat diese Anregungen bereits in die Roadmap für die weitere Produktentwicklung einfließen lassen.

Nach erfolgreichem Abschluss der Pilotphase setzt Koenig & Bauer in seinen Systemen inzwischen serienmäßig mGuard-Devices für den Internet-Teleservice ein. Auch bereits bestehende Systeme im Feld sollen mit der Technologie nachgerüstet werden.

Innominat Security Technologies AG,
Tel: 030 63923300,
Mail: troessel@innominate.com,
www.innominate.de