



# Service via Internet

Angesichts eines Exportanteils von 83 % ist das Thema Teleservice für den Druckmaschinen-Hersteller Koenig & Bauer von essenzieller Bedeutung. Wo Modem- und ISDN-Verbindungen den Anforderungen nicht mehr gerecht werden, sollen künftig breitbandige Internet-Verbindungen neue Möglichkeiten in punkto sicherer Fernwartung eröffnen.

**D**er eng verzahnte Produktionsplan einer Druckerei macht die Verfügbarkeit der Druckanlagen zum wichtigen Wettbewerbskriterium. Ungeplante Standzeiten können sich kein Verlag und keine Druckerei leisten. Für die Service-Abteilung des Druckmaschinenherstellers heißt das, Fehlerpotenziale möglichst frühzeitig zu entdecken und so Störfälle zu vermeiden. Eine enorme Herausforderung bei den zahlreichen, weltweit verteilten Anlagen von Koenig & Bauer.

Die fränkische Unternehmensgruppe hat bereits sehr früh die Möglichkeiten der

Ferndiagnose und Fernwartung (Teleservice) über Modemverbindungen genutzt, um die Verfügbarkeit der installierten Anlagen zu gewährleisten und gleichzeitig die Kosten für Service und Wartung zu reduzieren. Durch die zunehmende Funktionalität der Drucksysteme ist die bisherige Praxis des Teleservice aufgrund des Datendurchsatzes von 64 beziehungsweise 128 kBit/s beim Einsatz von ISDN-Verbindungen mittlerweile an ihre Grenzen gestoßen. Außerdem sind der Aufwand für die Telefon-Infrastruktur, die hohen Verbindungskosten und nicht zuletzt das Si-

## Der Anwender

Die Firma Koenig & Bauer (KBA) hat eine lange Tradition. Bereits 1814 druckte die neu entwickelte Zylinderdruckmaschine von Friedrich Koenig zum ersten Mal die Londoner Tageszeitung „The Times“ mit Dampfmaschinenkraft. Heute verfügt die Unternehmensgruppe mit Stammsitz im fränkischen Würzburg über eine breite Produktpalette an Druckmaschinen für die Bereiche Bogenoffset, Digital-Bogenoffset, Rollenoffset, Rollentiefdruck, Zeitungsdruck, Flexodruck, Telefonbuchdruck, Wertpapierdruck und Blechdruck sowie industrielle Kennzeichnungssysteme (Inkjet-, Heißpräge- und Lasertechnik). Mit 8300 Mitarbeitern und einem Jahresumsatz von 1,7 Mrd. Euro zählt das Unternehmen weltweit zu den größten Herstellern von Druckanlagen.



cherheitsrisiko, das jedes Modem für das gesamte Netzwerk eines Unternehmens darstellt, Nachteile, die der Druckmaschinen-Hersteller nicht länger akzeptieren wollte. „Ergo haben wir nach neuen Wegen der Fernwartung gesucht“, blickt Andreas Birkenfeld, Bereichsleiter Systemtechnik bei Koenig & Bauer, zurück und ergänzt: „Die Nutzung breitbandiger Internet-Verbindungen bot sich geradezu an, weil die Verbindungskosten kaum nennenswert sind, der Datendurchsatz von den bisher verfügbaren 64/128 kBit/s auf bis zu mehrere MBit/s bei xDSL-Internet steigt und Technologien wie Voice-over-IP – also Internet-Telefonie – oder das Streaming von Bild- und Videodaten neue Service-Perspektiven eröffnen.“

### Der Lösungsansatz

Die Umsetzung der Internet-Fernwartung erfolgte schließlich auf der Grundlage einer integrierten Komplettlösung basierend auf Standard-Technologien durch das auf industrielle Netzwerksicherheit spezialisierte Berliner Unternehmen Innominate. Das Konzept dieser Lösung besteht zunächst darin, dass der Ansatz für den

Verbindungsaufbau von Fernwartungs-Services im Vergleich zu bisher üblichen Konzepten umgekehrt wurde: Musste bisher eine Verbindung vom Servicetechniker zum System aufgebaut werden – also eine beim Endkunden eingehende Verbindung –, wird beim „ausgehenden VPN-Konzept“ die Verbindung vom System zu einer Servicezentrale – also eine vom Endkunden ausgehende Verbindung – hergestellt. Dies öffnet der Fernwartung den Weg über das Internet. „Alle bisherigen Zugangsprobleme aufgrund von firmeninternen Sicherheits-Policies und zentralen Unternehmens-Firewalls sind mit einem Schlag gelöst, denn ausgehende Internet-Verbindungen sind entscheidend einfacher und entsprechend sicher zu administrieren,“ beschreibt Torsten Rössel, Director Business Development bei Innominate, den bei Koenig & Bauer realisierten Ansatz.

Hardwaretechnisch basiert die so genannte mGuard-Technologie auf autarken Security-Appliances, die in verschiedenen Bauformen in die zu wartenden Systeme integriert werden – etwa als Hutschienengerät im Schaltschrank einer Druckanlage



△  
mGuard-PCI im integrierbaren PCI-Kartenformat für den Einsatz in Industrie-PCs und PC-basierten Steuerungen, wie sie zum Beispiel für die serienmäßige Teleservice-Ausrüstung von Bogenoffsetmaschinen bei KBA geplant sind.



Entwicklungsmuster der neuen Remote-Service-Appliance von Innominate für die Montage auf der Hutschiene: Das Gerät bietet neben der Standard-Ethernet-Schnittstelle optional integrierte Analog- oder ISDN-Modems. Diese Optionen erlauben Maschinen und Anlagen eine einfache Migration von traditioneller Modem-basierter hin zu moderner Fernwartung via Internet.

Geräten eigenständig heruntergeladen und aktiviert werden (Pull-Verfahren).

Durch eine ausgefeilte Vorlagen- und Vererbungstechnik, intelligente Verwaltung virtueller Adress-Pools und eine integrierte Certificate Authority zur Erzeugung der VPN-Zertifikate lässt sich mit dem IDM ein hoher Automatisierungsgrad bei der Konfiguration und Inbetriebnahme einzelner Geräte erzielen. Diese Elemente ermöglichen auch eine praxisnahe Arbeitsteilung. Wenige IT-Security-Administratoren mit tieferer Expertise gestalten dabei die Vorlagen mit den komplexeren, sicherheitsrelevanten Bestandteilen, während eine größere Zahl von Technikern schon nach kurzer Einweisung entsprechende Geräte mithilfe der Vorlagen auslieferungsreif konfektionieren und in Betrieb nehmen kann.

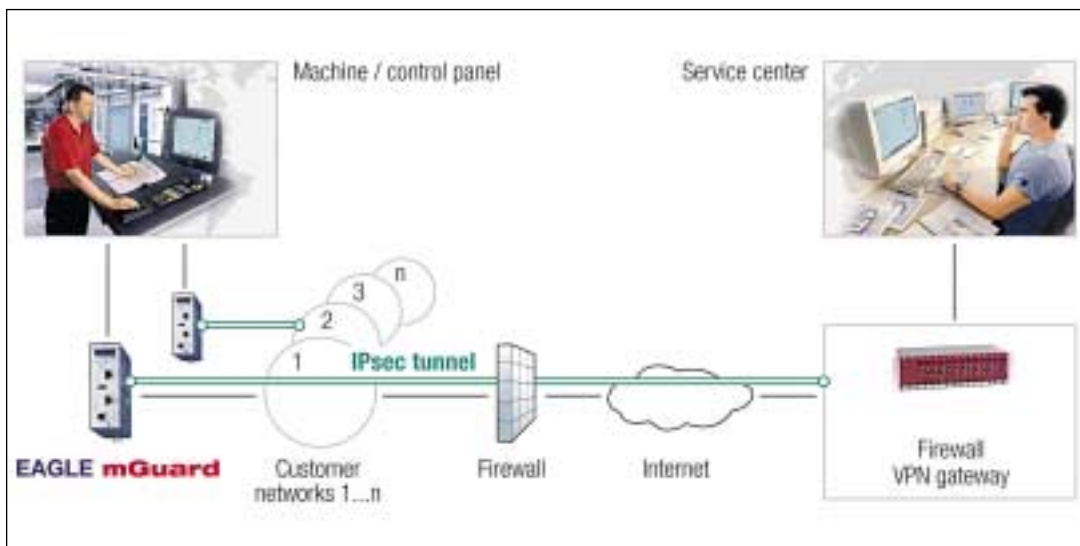
oder als PCI-Steckkarten in den Steuerungsrechner einer Bogenoffsetmaschine. Als Gegenstelle kommt im Servicezentrum von Koenig & Bauer ein skalierbares „Blade-Pack“ zum Einsatz, das bis zu zwölf Blade-Einschübe in einem 19-Zoll-Chassis (3 HE) aufnehmen und so flexibel 250 bis 3000 definierte sichere Teleservice-Verbindungen unterstützen kann. Die mGuard-Plattform arbeitet komplett eigenständig. Die entsprechenden Systeme lassen sich daher ohne großen Konfigurationsaufwand in jede Standard-Ethernet-Umgebung integrieren, sind zu jedem Betriebssystem kompatibel und erfordern keinerlei Konfigurationsänderungen – weder am bestehenden Netzwerk noch am fernzuwartenden System. Die Sicherheit der Teleservice-Verbindung wird durch VPN-Technologie (Virtual Private Network) auf Basis des IPsec-Standards garantiert. Dabei kann die (De-)Aktivierung der VPN-Tunnel durch den

Endkunden kontrolliert und die zulässige Kommunikation durch Firewall-Regeln gezielt auf das gewünschte, notwendige Maß beschränkt werden.

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) ist eine solche Plattform mit Client/Server-Architektur. Alle Leistungsmerkmale und Einstellungen der Security-Appliances lassen sich damit beim Roll-Out für die Inbetriebnahme von Teleservice-Verbindungen zentral konfigurieren und verwalten. 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

## Erste Erfahrungen

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 ein Formblatt entwickelt, um das IT-Umfeld und die besonderen Anforderungen der Kunden zu spezifizieren. Auf dieser Basis lassen sich Konfiguration, Funktionstest und Abnahme der Appliance bereits im Werk vornehmen. Vor Ort braucht der Monteur das System im Idealfall nur noch mit Datenleitung und Versorgungsspannung zu verbinden. Durch die weitgehend standardisierte Konfiguration der Appliances reduziert



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

sich der administrative Aufwand auf ein Minimum. „Bei ausreichender fachlicher Vorklärung durch den Kunden können wir sogar eine echte Plug&Play-Installation erreichen“ – so die Erfahrung von Andreas Birkenfeld. Auch was die zukünftigen Möglichkeiten der Lösung betrifft, gibt es schon konkrete Vorstellungen: „Wir halten die Aufnahme von Monitoring-Funktionalität zur laufenden Zustandsüberwachung und Logging-Funktionalität für die Aufzeichnung von Ereignissen für sinnvolle Erweiterungen des Device Managers“. Innominate hat



**Andreas Birkenfeld, Koenig & Bauer:**  
 „Über die gesteigerte Bandbreite der sicheren Verbindung via Internet können wir dem Kunden erweiterte Dienstleistungen auf dem Gebiet der Fernwartung anbieten.“

diese Anregungen bereits in die Roadmap für die weitere Produktentwicklung einfließen lassen. Nach erfolgreich verlaufener Pilotphase ist bei Koenig & Bauer in Zukunft der serienmäßige Einsatz von mGuard-Devices geplant und in einem zweiten Schritt die Nachrüstung bereits bestehender Systeme.

Im Zusammenhang mit der eigentlichen Fernwartungsapplikation plant Koenig & Bauer, die Secure-Service-Portal-Lösung des Braunschweiger Unternehmens DS Data Systems einzusetzen. Dabei handelt es sich um eine Plattform, über die komplexe Remote-Services sicher über Internet-Verbindungen abgewickelt werden können. Der Service-Mitarbeiter autorisiert sich dabei beim zentralen Service-Portal und wählt nur noch den Kunden und die Anlage aus. Alle individuellen Vorgaben der Kunden sind zentral gespeichert.

Das Service-Portal bietet dabei eine zentrale Administration auch über die heterogenen Netzwerke verschiedener Anlagenbetreiber und verfügt über Sicherheitsmechanismen, die nach ISO 27001/IT-Grundschutz vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert sind. Ein optionales Feature der Portal-Lösung von DS Data Systems ist die Möglichkeit, auf Knopfdruck eine Verbindung von Seiten der zu wartenden Anlage oder Maschine aufzubauen. Dabei kann der Betreiber über eine Datenbank bestimmen, wann seine Maschinen gewartet werden dürfen.

gh

## Die Security-Funktionen

Die in den Druckmaschinen von Koenig & Bauer eingesetzte, dezentrale Security-Appliance vereint diverse Funktionen, um IP-basierte Netzwerk-Verbindungen zu industriellen Systemen und Anlagen zuverlässig abzusichern:

- ▷ 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 und ist dadurch selbst nicht zu erkennen und infolgedessen auch nicht angreifbar.
- ▷ VPN-Router (optional) für sichere Datenübertragung über öffentliche Netze. Zum Einsatz kommen wahlweise eine hardware-beschleunigte DES-, 3DES- oder AES-Verschlüsselung und das standardisierte IPsec-Protokoll.
- ▷ Router- und Firewall-Redundanz (optional) für hochverfügbare Industrial-Network-Security-Lösungen mit automatischem Master/Slave Failover.