



Halle 9
Stand 532



Bild 1: Ob im Schaltschrank auf der Hutschiene oder als PCI-Karte direkt im Industrie-PC: mGuard Security Appliances sorgen für die sichere Anbindung von Maschinen und Anlagen an das Remote Services Portal.

Sichere Fernwartung durch Cloud Computing: Remote Services Portal aus der Wolke

Interessenten an einer zeitgemäß Internet-basierten Fernwartungslösung steht ein neuer Dienst zur Verfügung: das mGuard Remote Services Portal von Innominate. Im Verbund mit den bewährten mGuard Security Appliances als VPN Routern für Maschinen und Anlagen im Feld ermöglicht dies sichere Fernwartungsverbindungen ohne lange Lernkurve und ohne Investitionen in die eigene zentrale Infrastruktur.

Der Umfang und Anteil von Software an der Wertschöpfung und Komplexität industrieller Maschinen und Anlagen nimmt seit Jahren zu. Entsprechend erwarten ihre Betreiber, dass die Fähigkeiten der Hersteller und Integratoren zum Remote Support ihrer Systeme mit dieser Entwicklung Schritt halten. Leistungsfähige Teleservice-Angebote auf Basis breitbandiger VPN-Verbindungen (Virtual Private Networks) über das Internet anstelle traditioneller Modem-Einwählverfahren werden daher immer mehr zum allgemein akzeptierten und geforderten Standard. So konnten zahlreiche namhafte Unternehmen des Maschinen- und Anlagenbaus in den letzten Jahren auf Basis des von Innominate empfohlenen Sicherheitskonzepts und der ausschließlichen Nutzung ausgehender VPN-Verbindungen unter Kontrolle der Betreiber neue Internet-basierte Teleservice-Lösungen erfolgreich einführen und mit positiven Erfahrungen bei ihren Kunden positionieren.

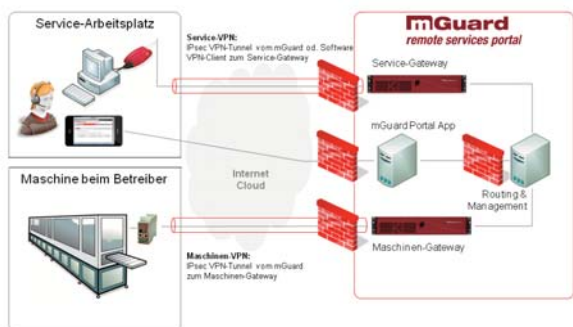


Bild 2: Das Remote Services Portal: mit betriebsbereit vorkonfigurierten Security Routern und Web-basierter Bedienung haben Anwender die Fernwartung ihrer Maschinen und Anlagen im Griff.

Aller Anfang ist schwer

Für den Einstieg in die Nutzung dieser modernen Technologien sind jedoch zunächst einige Hürden zu überwinden. Insbesondere zum vollständigen Eigenbetrieb einer Gesamtlösung ist Know-how in Sachen Vernetzung und Sicherheit erforderlich und eine geeignete IT-Infrastruktur aufzubauen und vorzuhalten. Gerade für die Startphase, wenn es erst einmal nur um die Evaluierung geeigneter Produkte und Lösungen und dann um einen Pilotversuch mit wenigen ersten Maschinen geht, können diese Hürden selbst für größere Unternehmen abschreckend hoch sein. Für kleine und mittelgroße Hersteller des Maschinen- und Anlagenbaus mit durchschnittlich nur ein bis drei oder vier neu ausgelie-

Bild 3: Struktur-Diagramm des Remote Services Portals: Anwender sehen ihre angebundenen Maschinen und Anlagen unter deren realen IP Adressen, das Portal kümmert sich um eindeutiges Routing der Verbindungen.



ferten Systemen pro Monat ist die Wirtschaftlichkeit einer selbst realisierten und betriebenen Lösung sogar dauerhaft infrage gestellt. Die typischen Herausforderungen beginnen schon bei der Komplexität der eigenen IT-Umgebung und - Organisation. Es sind Internet-Zugänge und öffentliche IP-Adressen für eigene VPN-Gateways zu beschaffen, Feldgeräte und Gateways für den Aufbau der VPNs zu konfigurieren und mit einer geeigneten Software Schlüsselpaare und digitale Zertifikate für die so gesicherten Verbindungen zu erzeugen – das allein ist recht aufwendig für einen Neueinsteiger. Noch kniffliger wird es beim Thema eindeutige Adressierung und Routen. Da die Maschinen und Anlagen eines Herstellers sehr häufig die immer gleichen IP Adressräume in ihren internen Netzwerken nutzen, lassen sie sich infolge der daraus resultierenden Adresskonflikte nicht so ohne weiteres per VPN zu einem gemeinsamen zentralen Gateway verbinden. Ein Ansatz, dieses Problem zu überwinden, ist die Abbildung der identischen realen Adressen des Maschinennetzes auf jeweils eindeutige virtuelle Netzwerke durch eine sogenannte 1:1 NAT-Funktion des VPN-Routers. Ein tatsächlicher Zugriff über diese virtuellen Adressen ist aber zum einen für die Service-Techniker nicht komfortabel, da sie dann ständig zwei Sichten auf die Maschine und ihr Netz-

werk im Kopf bzw. vor sich in der Dokumentation haben müssen: die reale, für welche die Maschine zu projektieren ist, und die virtuelle, über welche man aus der Ferne mit ihr kommuniziert. Er ist zum anderen auch in vielen Fällen technisch gar nicht möglich, weil die zum Teleservice eingesetzten Werkzeuge – wie z.B. ältere Versionen der Step 7 Projektierungs-Software Simatic Manager – zu einer solchen Unterscheidung zwischen realer und virtueller Adressierung gar nicht in der Lage sind. Beides führt zu der Anforderung, dass der Anwender einer Fernwartungslösung die angeschlossenen Systeme unter ihren realen IP-Adressen sehen und ansprechen können sollte, so als wäre er vor Ort mit ihnen verbunden. Da es zu diesen Adressen infolge ihrer mehrfachen Verwendung in verschiedenen Maschinen aber meist keine eindeutige Route gibt, wird irgendein zusätzlicher Mechanismus zur eindeutigen Auswahl des Zielsystems benötigt, über den der Anwender definieren kann, auf welche Maschine er in einer Sitzung mit diesen mehrdeutigen Adressen denn nun zugreifen möchte. An dieser Stelle reift die Einsicht, dass VPN Gateways allein für die komfortable Nutzung von Fernverbindungen durch den Service oftmals nicht ausreichend sind und Bedarf nach einer weiteren Unterstützung auf Applikationsebene besteht.

Bedarf nach Portal-Lösungen aus der Cloud

Prinzipiell kann diese Unterstützung durch eine beim Anwender installierte Software (einen Fat Client) erfolgen, wie das insbesondere bei einigen auf OpenVPN basierenden Lösungen am Markt auch der Fall ist. Dies bringt allerdings Abhängigkeiten von den Plattformen und Betriebssystemen der Anwender und die üblichen Probleme mit der Pflege und Aktualisierung verteilter Software-Installationen mit sich. Außerdem sind Lösungen, die sich vorrangig auf das Client-seitig definierte Routing verlassen, anfälliger für Manipulationsversuche. Eine Portal-Lösung mit zentralem Server und Web-basierter Benutzeroberfläche erscheint daher als geeignetere, erstrebenswerte Lösung. Deren Eigenentwicklung ist für kleine und mittlere Unternehmen des Maschinen- und Anlagenbaus aber in der Regel mit einem zu hohen Aufwand verbunden. Um der großen Zahl dieser Firmen dennoch modernste Technolo-



Bild 4: Die aktuelle Generation von Hutschienengeräten mGuard rs2000 und mGuard rs4000 aus den Field und Factory Lines ist durch Konfigurationsspeicherung auf SD-Karten einfach mit dem Remote Services Portal in Betrieb zu nehmen.

gie für sichere Remote Services auf einfachste Art und Weise zu erschließen, hat Innominate daher das mGuard Remote Services Portal entwickelt. Ganz im aktuellen Trend hin zum Cloud Computing stellt die Hosting Edition dieses Portals VPN Infrastruktur, webbasierte Bedienoberfläche und Konfigurationen für die beteiligten mGuard Feldgeräte als Managed Service bereit. In Abkürzungen und Sprachgebrauch der IT-Branche gesagt also IaaS und SaaS: Infrastructure & Software as a Service. Das Portal wird in einem Internet Rechenzentrum mit hoher Verfügbarkeit betrieben und erspart seinen Anwendern so Investitionen und Betriebsaufwand für eine eigene Teleservice-Zentrale. Nach Registrierung und Vertragsabschluss für einen Mandanten kann dessen primärer Administrator weitere Benutzerkonten und Service-Arbeitsplätze für seine Kollegen im Portal einrichten. Neu anzubindende Maschinen und Anlagen können strukturiert nach Betreibern und Standorten in Form einer typischen Stammdatenkarte erfasst und dann ihre VPN-Anbindung zum Portal beauftragt werden. Nach Auftragsbearbeitung steht die betriebsbereite Konfiguration für das an der Maschine eingesetzte Feldgerät über das Portal zum Download bereit. Elegant gestaltet sich der Einsatz des Remote Services Portals in Verbindung mit den neuen Security Appliances der mGuard Field und Factory Lines, welche über entsprechend bespielte SD-Karten sogar ohne Netzwerkzugang zur Benutzeroberfläche konfiguriert werden können. Den Online-Status ihrer Maschinen und Service-Arbeitsplätze haben Anwender über das Portal im Blick. Dabei werden die vorrangig aktuell zum Portal verbundenen Maschinen als erste präsentiert.

Service-Sitzungen auf einer Maschine werden über das Portal gestartet und zeitlich protokolliert.

Einfaches Geschäftsmodell

Ein einfaches Geschäftsmodell erlaubt dem Anwender, die Nutzung des Portals bedarfsgerecht zu skalieren. Je Anbindung eines Service-Arbeitsplatzes bzw. einer Maschine an das Portal ist über den Kauf und die Einlösung sogenannter Voucher eine Art von Prepaid-Laufzeitvertrag mit kalenderjährlicher Verlängerung abzuschließen. Dabei war es Innominate wichtig, kein reines Self-Service Portal zu schaffen, das den Anwender mit der Technik alleine lässt. Vielmehr erfolgt die Konfiguration der eingesetzten Feldgeräte durch Personal im Portal Service und ist ebenso wie die Nutzung einer Portal Support Hotline in den Ersteinrichtungs- und Nutzungsgebühren enthalten. So entsteht eine Cloud-basierte 'Plug-n-Protect' Lösung. Gerade bei kleinen und mittleren Volumina von jährlich neu anzubindenden Maschinen ist der Eigenbetrieb einer Lösung zu vergleichbaren Kosten kaum möglich. ■

www.innominate.com



*Autor: Torsten Rösse,
Director Business Development
Innominate Security
Technologies AG*