

InformationWeek

Das Praxismagazin für CIOs und IT-Manager

3 | 8. März 2007

SONDERDRUCK FÜR NETVIEWER

SICHERE TUNNEL FÜR DIE FERNWARTUNG

VON JÜRGEN HÖFLING |
juergen.hoefling@informationweek.de

Durch die Verwendung IP-basierter Netze entstehen in Fertigungsumgebungen neue Möglichkeiten, aber auch neue Sicherheitsprobleme. Fernwartungsverbindungen stehen hierbei an vorderster Stelle. Das Lösungsspektrum ist durchaus unterschiedlich.

Foto: Reinhard Kurzendörfer



»Der Bereich der Fernwartung spielt bei der Zusammenführung von Büro-IT und Fertigungs-IT die Vorreiterrolle«.

PETER DÖLLING,
Vorstand Defense

Jahrzehnte lang waren Büro-IT und die IT der Fertigungswelt Paralleluniversen ohne große technische und organisatorische Berührungspunkte. Das Internetprotokoll bringt sie jetzt zusammen. »Der Bereich der Fernwartung spielt dabei die Vorreiterrolle«, sagt Peter Dölling, Vorstand beim Systemintegrator Defense, der auf Fragen der IT-Sicherheit im Fertigungsbereich spezialisiert ist. Sicherheit ist dort in der Tat ein wichtiges Thema geworden, denn die neue Offenheit mit all ihren Produktivitätsvorteilen hat natürlich ihren Preis. Auf einmal ist nämlich die bisher durch proprietäre Bussysteme abgeschottete Welt der Industrie-PCs, speicherprogrammierbaren Steuerungen und Fertigungsroboter all den Angriffsszenarien ausgesetzt, die wir aus der Büro-IT schon lange kennen.

RENDEZVOUS IM GRENZNETZ

Dass Fernwartung quasi der Türöffner für industrielle IP-Verbindungen ist, liegt nicht zuletzt an der Komplexität und Globalität der heutigen Fertigungs- und Logistikprozesse. Viele Maschinen sind schwer zugänglich und oft weit entfernt vom Fachpersonal. Fernwartung ist dann eine sehr kosteneffiziente Möglichkeit, die wenigen Spezialisten, die man hat, an die Maschine zu bringen, ohne sie zu Flugreisen von Tausenden von Kilometern zwingen zu müssen.

Diese Vorteile sind aber nicht ohne einige Problemchen zu haben: So ist nicht nur der Durchgriff eines Servicetechnikers direkt auf einen Leitrechner oder gar direkt auf die Maschine ein kritisches Element, das abgesichert werden muss, sondern auch die Tatsache, dass »der Service-Mann eventuell auf den Systemen von Dutzenden von Kunden einen ebensolchen Zugriff benötigt, eine entsprechende wechselseitige Abschottung dieser Zugriffe aber nicht ohne Weiteres gewährleistet ist«, gibt Dr. Markus Harlander, Geschäftsführer beim Sicherheitsspezialisten GeNUA zu bedenken.

Um diesen Fallstricken zu entgehen, haben sich Harlanders Techniker eine

recht komplexe Konstruktion ausgedacht, die unter anderem bei MAN Diesel und MAN Roland Druckmaschinen zum Einsatz kommt. In der Grenznetzzone steht ein sogenannter Rendezvous-Server. Auf diesen kann der Servicetechniker von außen zugreifen und gleichzeitig können SSH-Tunnel von innen aus dem Unternehmensnetz aufgebaut werden. Der zeitlich eng begrenzte SSH-Tunnel wird nur nach telefonischer Anmeldung des Servicetechnikers aufgebaut und kann dann von diesem in umgekehrter Richtung, also in Richtung der zu wartenden Maschine, benutzt werden.

IPSEC-WARTUNGSTUNNEL

Anders als GeNUA setzt die Berliner Innominate ganz auf einen VPN-Tunnel unter IPSec. Die hauseigene Sicherheitsbox mGuard unterstützt dabei »anders als herkömmliche IPSec-VPN-Appliances die Anwendung von Stateful-Inspection-Firewall-Regeln innerhalb von VPN-Tunneln«, unterstreicht Innominate-Marketier Andreas Beierer. Damit könne der Verkehr durch den Tunnel auf die gewünschten beziehungsweise notwendigen Ziele, Protokolle und Richtungen beschränkt werden. Gleichzeitig sei durch die hundert-

prozentige IPSec-Konformität aber auch das Zusammenspiel mit IPSec-konformen VPN-Gateways anderer Hersteller als zentraler Gegenstelle gewährleistet. Lediglich ausgehende Verbindungen zum Servicezentrum-Gateway über die beiden UDP-Ports 500 und 4500 müssten zugelassen werden. Denn ähnlich wie bei GeNUA werden auch beim Innominate-Konzept die VPN-Verbindungen von der Maschine zur Servicezentrale ausgelöst.

Auch der Innsbrucker Konnektivitätsspezialist Phion setzt bei Fernwartungslösungen auf das IPSec-Protokoll beziehungsweise IPSec over https. Letzteres bietet verschiedene Vorteile, sagt Wieland Alge, Gründer und Geschäftsführer. Er nennt in diesem Zusammen-

durch das Maschinenpersonal abhängig gemacht werden«.

WARTUNGSTUNNEL IN DER APPLIKATION

In bestehende Firewalls und andere Sicherungsgeräte integriert sich das Fernsteuerungsprogramm »Remote admin« aus der Online-Konferenz-Suite von Netviewer des gleichnamigen Karlsruher Unternehmens. »Die Verbindung von einem Unternehmens-Client zu einem Server wird über ein eigenes Verfahren abgewickelt, das auf http aufsetzt«, sagt Jürgen Daunis, Leiter Presales bei den Karlsruhern. Netviewer lässt sich nach Daunis' Darstellung von jedem Unternehmen einsetzen, das Internetzugang hat. Dazu muss ein kleines Programm auf den

denden Dienstfahrten«, erklärt EDV-Systembetreuer Joachim Kiwitz. Das Zentrum für Medien und IT-Support ist für die komplette IT-Ausstattung der 102 Schulen im Landkreis zuständig. Das Aufgabenspektrum reicht von der einfachen Fehlerbehebung bis zu umfangreichen Migrationsprojekten.

FERNWARTUNG PER MAUSKLIK UNTERBRECHEN

Ebenfalls auf eigenen Protokollen baut der Fernzugriff von NTRglobal auf. Die Eigenmechanismen setzen auf dem TCP/IP-Protokoll-Verbund auf. Laut Deutschland-Chef Michael Kessler kann NTRglobal »256-bit-verschlüsselte Verbindungen über jeden beliebigen Port herstellen, ganz wie der Kunde will«. Der Servicetechniker könne im Übrigen



»Auf Wunsch kann auch bei Phion der Wartungszugang von einer (zeitlich begrenzten) expliziten Freischaltung durch das Maschinenpersonal abhängig sein«.

STEFAN GASTEIGER vom Phion-Partner Infracore Gendorf



»Bei uns macht die Applikation selbst einen Tunnel auf. Das ist viel einfacher und mindestens genau so sicher wie ein IPSec-Tunnel«.

JÜRGEN DAUNIS, Technischer Manager bei Netviewer

hang »die Möglichkeit, einen Wartungstunnel über einen Proxy hinweg (zum Beispiel aus einem Firmensitz heraus) aufzubauen oder auch die bessere Nutzbarkeit in Ländern mit problematischen Internetverbindungen«. Im Gegensatz zu GeNUA oder Innominate wird bei Phion die Verbindung vom Servicetechniker zur Maschine geschaltet, doch wird der »eingehende Verkehr auf das absolut Notwendige begrenzt«, erklärt Stefan Gasteiger vom Phion-Partner Infracore Gendorf und meint: »Auch der VPN-Client auf dem Endgerät hat eine Firewall integriert, deren Regelsatz bei der Online-Verarbeitung zur Maschine zentral vorgegeben wird. So findet also eine doppelte Filterung des eingehenden Verkehrs statt«. Auf Wunsch kann auch bei Phion der Wartungszugang von einer (zeitlich begrenzten) expliziten Freischaltung

abgesetzten Geräten aufgespielt werden. Der Servicetechniker muss auf seinem Gerät nichts installieren. Im Fernwartungsfall starte er, so Daunis, sein Steuerungsprogramm auf dem Wartungsrechner, melde sich mit seinen Zugangsdaten an und bekomme dann die zu wartenden Maschinen angezeigt, die für ihn relevant seien. »Im Gegensatz zu einem IPSec-Tunnel, der aus Sicherheitsgründen dann wieder mit entsprechenden Tools nur für bestimmte Applikationen freigegeben wird, macht Netviewer von vornherein nur in der Applikation selbst einen Tunnel auf, das ist viel einfacher und mindestens genauso sicher«, sagt Jürgen Daunis.

Im hessischen Main-Kinzig-Kreispart das Zentrum für Medien und IT-Support durch den Einsatz von Netviewer als Fernwartungsinstrument »rund die Hälfte aller sonst notwendig wer-

erst nach der Autorisierung durch den Kunden auf dessen PC zugreifen und mit der Fernwartung beginnen. Der Kunde sei immer Herr der Lage, sagt Kessler. Er habe nach Beginn der Sitzung zu jeder Zeit die Möglichkeit, die Fernwartung per Mausclick zu unterbrechen oder gänzlich zu stoppen. Darüber hinaus könne die gesamte Sitzung in einem Textprotokoll oder auch als Videomitschnitt aufgezeichnet werden.

Alle hier vorgestellten Vorgehensweisen haben letztlich ein hohes Sicherheitsniveau, wenn die Einstellungen korrekt vorgenommen werden und die Arbeitsabläufe stimmen. Die Unterschiede liegen vor allem in der Verwendung von Standards und in der Art, wie diese verwendet werden. Hier muss jeder Anwender für sich entscheiden, wieviel Offenheit er in seinem Umfeld benötigt. ■