IT-SICHERHEIT FÜR DIE FERTIGUNGSAUTOMATION

VON JÜRGEN HÖFLING | juergen.hoefling@informationweek.de

Bei industriellen Fertigungsnetzwerken geht man mehr und mehr von angestammten Lösungen weg und orientiert sich an den Standards der Büro-EDV. Entsprechend müssen die Sicherheitsmechanismen angepasst werden.

Foto: MAN Nutzfahrzeuge

Die Welt der Fertigungsautomation ist längst keine sichere Oase mehr: »Uns sind Fälle aus der Praxis bekannt, wo ein Servicemann nicht nur die Maschine seines Arbeitgebers wartete, sondern gleichzeitig seinen Laptop zum Default-Gateway des Kundennetzes erhob und dadurch erheblichen Schaden anrichtete«, berichtet Dr. Klaus Zwerina, Marketingleiter beim schwäbischen Industrienetz-Spezialisten Hirschmann.

Waren die industriellen Fertigungsnetze lange Zeit eine Welt für sich, die keine Verbindung zur Bürowelt hatte, ist mittlerweile die Annäherung der beiden Welten in vollem Gange. Das gilt in doppeltem Sinn: zum einen gibt es immer mehr Verbindungen von Fertigungsautomation, Logistik und betriebswirtschaftlicher Standardsoftware (das Stichwort »RFID« mag hier genügen), zum anderen werden die spezifischen Betriebssysteme und Bussysteme der Fertigungsautomation in vielen Fällen durch aufgebohrte Versionen der aus der Bürowelt bekannten Standards wie Ethernet, TCP/IP und http abgelöst. Verteilte Automatisierungslösungen auf der Basis eines Internet-Browsers und http sind mittlerweile für viele Geräte in industriellen Umgebungen üblich.

STARKE VERWUNDBARKEIT

Die Frage nach der Sicherheit stellt sich hier dann sehr schnell. Dies gilt umso mehr, als die Fehlertoleranz von Ferti-

Die Mini-Firewall mGuard von Innominate wird »transparent« in das Netzwerk-Kabel zum PC eingeschleift oder als Karte in den Router integriert.

Foto: Innominate

gungssystemen in der Regel weitaus geringer ist als die vieler Bürosysteme, und das nicht nur im Echtzeitbereich. Wenn Schadprogramme wie SQL-Slammer beispielsweise im Nicht-Echtzeit-Bereich einen Leitrechner angreifen und die Bandbreite in Richtung der darunter liegenden Steuerrechner und Produktionsroboter deutlich drosseln, dann gehen letztere in Störung und die gesamte Produktionslinie ist lahmgelegt. In der vernetzten Bürowelt dagegen hat ein solcher Angriff auf die Verfügbarkeit zwar immer ärgerliche, aber nicht immer derart fatale Auswirkungen. »Selbst wenn man davon ausgeht, dass das Bürosystem ebenfalls in die Knie geht, verursacht eine abgeschaltete Produktionsstraße andere Verluste als beispielsweise der Ausfall des Mailservers«, sagt Stefan Strobel, Spezialist für IT-Sicherheit und Geschäftsführer von Cirosec in Heilbronn.

Foto: Hirschmann AG

KLAUS ZWERINA

»Wir kennen Fälle, wo ein Servicemann nicht nur die Maschine seines Auftraggebers wartete, sondern gleichzeitig seinen Laptop zum Default-Gateway des Kundennetzes erhob«

DR. KLAUS ZWERINA,
Marketingleiter, Hirschmann

Strobel zeigt im gleichen Atemzug die Problematik einer adäquaten Sicherheitslösung auf: »Maschinensteuerungen, Laborgeräte, aber auch Kassensysteme laufen in vielen Fällen auf älteren Windows-Systemen, bei denen nur mit immensem Aufwand ein Betriebssystem-Service-Pack eingespielt werden kann. Ein Beispiel für die Herausforderungen in Sachen IT-Sicherheit sind die sogenannten validierten Systeme, wie man sie in der Pharma-Branche findet. Diese Systeme befinden sich in einer Art eingefrorenem Zustand, der auf das genaueste dokumentiert ist. Auch nur eine kleine Änderung des Codes zieht einen sehr großen organisatorischen Aufwand nach sich«.

Gängige Netzwerk-Firewalls können sicher mit kleinen Anpassungen auch in Fertigungsumgebungen eingesetzt werden. Weit mehr noch als in der Bürowelt befinden sich in der Fabrikautomation die größten Schwachstellen freilich nicht an den Netzübergängen, sondern im internen Bereich. Jede speicherprogrammierbare Steuerung, jeder Steuerrechner muss eigens geschützt werden. Die Gefahrenpunkte bei der Fernwartung von Maschinen und Anlagen über TCP/IP und http wurden zu Anfang schon erwähnt. »Hier ist nicht nur der Durchgriff des Servicetechnikers direkt auf die Maschine ein kritisches Element, das abgesichert werden muss, sondern auch die Tatsache, dass der Service-Mann eventuell auf die Systeme von Dutzenden von Kunden einen solchen Zugriff benötigt, eine entspre-

Foto: cirosec GmbH

STEFAN STROBEL

»Eine abgeschaltete Produktionsstraße verursacht weit höhere Verluste als beispielsweise der Ausfall eines Mailservers«.

STEFAN STROBEL,
Geschäftsführer von Cirosec in Heilbronn

WARTUNGSLÖSUNG BEI MAN NUTZFAHRZEUGE IN AUGSBURG

Matthias Stöckhert, Netzwerk-Administrator bei MAN Nutzfahrzeuge, beschreibt im Folgenden die Wartungs-Lösung des Unternehmens am Standort Augsburg:

»Bei MAN Nutzfahrzeuge sind zahlreiche Maschinen und EDV-Systeme im Einsatz, die von externen Dienstleistern gewartet werden. Für die effektive und schnelle Wartung benötigen diese Remote-Zugriff auf die Maschinen. MAN erlaubt jedoch aus Sicherheitsgründen keinen direkten Zugang aus dem Internet in das Unternehmensnetz, sondern lediglich auf die Server der Hochsicherheitszone (»Servernet-Securityzone«).

Der Rendezvous-Server, der auf einer GeNUBox von GeNUA läuft, steht in dieser »Servernet-Securityzone« Auf diesen Server können Dienstleister von außen zugreifen, und gleichzeitig können SSH-Tunnel von Innen aus dem Unternehmensnetz durch die Firewall GeNUgate zu dem »Treffpunkt« aufgebaut werden. Der Dienstleister meldet dabei seine Wartung telefonisch beim Netzwerk-Operating an. Daraufhin wird von Innen der SSH-Tunnel zum Rendezvous-Server aufgebaut. Danach hat der Dienstleister zehn Minuten Zeit, sich von Außen auf dem Server anzumelden.

Nach erfolgreicher Anmeldung kann der Dienstleister den SSH-Tunnel »rückwärts« nutzen und auf die Maschine oder das EDV-System zugreifen. Nach Abschluss der Wartung wird der Tunnel umgehend wieder abgebaut. Die Wartungs-Lösung ist seit einem Jahr im Einsatz und wird von rund 60 Dienstleistern regelmäßig genutzt. Neben der Firewall-Box wird lediglich ein SSH-Tool wie beispielsweise die Freeware Putty benötigen«.

→

chende wechselseitige Abschottung dieser Zugriffe aber nicht ohne Weiteres gewährleistet ist«, sagt Dr. Markus Harlander, Geschäftsführer beim Sicherheitsspezialisten GeNUA in Kirchheim bei München.

»TRANSPARENTE« INTEGRATION EINER MINI-FIREWALL

Entsprechende Lösungen zur Beschränkung der Kommunikation auf benötigte Partner und Protokolle können mit herkömmlichen Firewalls und einigen

Foto: Medusa Elektronik

Das Videoüberwachungssystem PICTRA enthält eine mGuard-Firewall in PCI-Kartenform.

trickreichen Mechanismen gelöst werden. Die Installation bei MAN Nutzfahrzeuge in Augsburg ist dafür ein gutes Beispiel (siehe Kasten S. 29). Eine Alternative sind spezielle Miniatur-Firewalls wie die mGuard-Reihe der Berliner Firma Innominate, die als eigenständige Boxen vor die betroffenen PCs geschaltet oder auch als »Firewall-PCI-Karte« in industrielle Netzwerk-Sicherheitsmodule wie die »EAGLE-Reihe« von Hirschmann integriert werden können. Das »schwäbische Adlerauge« ist beispielsweise bei einem Automobilhersteller im Einsatz und stellt dort dedizierte Serviceports bereit, welche die Zugriffsmöglichkeiten streng einschränken, zum Beispiel nur auf einen einzigen Roboter oder auf eine einzige Steuerung. Die Integration erfolgt dabei »transparent«, das heißt auf Layer-2, so dass sich die Topologie nicht ändert. Einen solchen Bridging-Modus sehen die meisten für industriellen Einsatz ausgelegten Firewalls vor, weil eine Layer-3-Integration, die mit der Änderung der IP-Adresse verbunden wäre, in der Regel nicht erwünscht ist.

Foto: GeNUA mbH

MARKUS HARLANDER

»Fernwartungs-Zugriffe auf Steuerungsrechner und Produktionsroboter müssen hermetisch abgesichert werden«

DR. MARKUS HARLANDER, Geschäftsführer von GeNUA

OFT DIE LETZTE RETTUNG

Der Vorteil einer Mini-Firewall-Lösung gegenüber einer »Personal Firewall«-Software besteht darin, dass der zu schützende PC nicht angefasst werden muss. Die Miniatur-Firewall wird als eigenständiges System nur in das Netzwerk-Kabel zum PC eingeschleift oder in den Router integriert und ändert nichts an der Software oder der Konfiguration der genannten übergeordneten Geräte.

Miniatur-Firewalls wie mGuard sind oft die letzte sinnvolle Schutz-Möglichkeit, wenn keine weitere Software auf die Zielsysteme installiert werden kann oder wenn die betroffenen Systeme auf verschiedene Netze verteilt sind, so dass es nicht möglich ist, sie mit einer herkömmlichen gemeinsamen Netzwerk-Firewall zu schützen.

GERÄTESCHUTZ DURCH HOSTBASIERTES IPS

Eine mGuard-PCI-Karte hat beispielsweise die MEDUSA Elektronik GmbH in ihr digitales Videoüberwachungssystem PICTRA integriert, das bei Banken und an Flughäfen, aber eben auch in der Industrie eingesetzt wird. »Durch die Kombination PICTRA und mGuard können unsere Kunden über eine gesicherte Verbindung in alle Filialen live hineinsehen«, sagt Frank Schlürscheid, Technischer Direktor bei MEDUSA.

Einen neuen Sicherheits-Ansatz stellen die sogenannten hostbasierten IPS-Systeme dar (siehe Kasten S. 30). Dazu müssen die zu schützenden Systeme einmal angefasst werden, da ein Host-IPS als Software auf dem Endgerät installiert wird. Danach jedoch sind keine Änderungen oder Aktualisierungen mehr notwendig. »Ein gutes Host-IPS bietet eine Prävention, die nicht von Muster-Updates abhängt und die Systeme gegen Würmer und Angreifer sichert, selbst wenn die Zielsysteme nicht gepatcht werden können«, sagt Cirosec-Geschäftsführer Stefan Strobel.

GeNUA-Geschäftsführer Markus Harlander sieht durchaus die Meriten solcher neuen Ansätze in Sachen »Innere Sicherheit«, meint aber, dass solche Systeme derzeit im Bereich der Fertigungsautomatisierung »noch nicht im Fokus der Anwender« sind. ■

SO FUNKTIONIERT EIN HOST-IPS

Ein hostbasiertes IPS kontrolliert die Ressourcen-Zugriffe aller Programme, die auf dem System ablaufen. Jeder Zugriff auf eine Datei der Festplatte, auf einen Registry-Eintrag, auf das Netzwerk oder ein externes Gerät kann dabei mit einem gelernten Normal-Profil verglichen werden. Falls ein Wurm oder auch ein Hacker es schaffen würden, eine Schwachstelle des Systems auszunutzen, würde das Host-IPS verhindern, dass der Wurm die Kontrolle über das System erlangt und weiteren Schaden anrichtet. Auch das Filtern von TCP/IP-Verbindungen, wie man es von einer Firewall kennt, kann mit einem Host-IPS realisiert werden. Während Virenscanner häufig keine Option sind, da sie die Systeme zu sehr bremsen, bringen Host-IPS-Produkte sehr viel weniger Performance-Probleme mit sich, da sie nicht wie ein Virenscanner die Inhalte aller Daten gegen Tausende von Mustern vergleichen müssen. Host-IPS filtern meist nur die Zugriffe als solche, nicht aber die übertragenen Inhalte.