SICHERE AUTOMATISIERUNG

IT-Security in der Automation – Neuland oder Niemandsland?

Vom 26. bis 27. September 2005 fand in Köln die marcus evans-Konferenz „IT-Sicherheit in der Automation" statt. Besonderheiten und Sicherheitsanforderungen beim Einsatz von Ethernet und IT-Systemen im Umfeld industrieller Produktionsanlagen standen dabei im Vordergrund. Regina Berg-Jauernig sprach für GIT SICHERHEIT mit dem Leiter der Veranstaltung, Prof. Dr. Frithjof Klasen, Direktor des Instituts für Automation & Industrial IT der Fachhochschule Köln, über die Hintergründe und Ergebnisse der Konferenz.

Prof. Dr. Frithjof Klasen

GIT SICHERHEIT: Herr Professor Klasen, warum ist das Thema „IT-Sicherheit" derzeit ein so aktuelles Thema in automatisierten Produktionsumgebungen?

F. Klasen: Mit der zunehmenden Vernetzung industrieller Produktionsanlagen auf der Basis von Ethernet-TCP/IP bis in die Feldebene hinein steigt auch das Bedrohungsrisiko für die Automatisierungssysteme und Produktionsanlagen und lässt die Bedeutung von IT-Security-Aspekten sprunghaft ansteigen.

Wie ist es zu dieser Situation gekommen?

F. Klasen: Das war eigentlich vorhersehbar. Seit dem Ende der 90er Jahre wird der Einsatz von Ethernet in der Automation propagiert und gefordert – Ziel ist die Nutzung einer einheitlichen Infrastruktur und die Durchgängigkeit des Datenverkehrs zwischen allen Kommunikationsebenen.
Wir erleben bereits seit einigen Jahren drei wesentliche Trends: den Einsatz von Ethernet in der Automation, den verstärkten Einsatz der TCP/IP-Protokollfamilie und die zunehmende Verbreitung von windowsbasierten Lösungen in der Automation.
Bislang bestand die Produktion häufig aus Kommunikationsinseln. Die Kopplung an überlagerte Systeme erfolgte in der Regel durch einige wenige Systeme, die gleichzeitig auch Datenkonzentrator waren. Innerhalb der „Inseln" wurden häufig proprietäre, technologiespezifische Kommunikationsprotokolle eingesetzt – das Bedrohungspotential war damit eher gering. Durch die einheitliche Kommunikationsinfrastruktur wachsen diese Inseln jetzt zu Landschaften zusammen. Störungen und Bedrohungen sind damit nicht mehr lokal begrenzt und durch das Zusammenwachsen mit der Office-Welt steigen die Bedrohungen erheblich.

Wo liegt das Problem?

F. Klasen: Wir wollten einheitliche Kommunikationsinfrastrukturen und einheitliche Protokolle, um Lösungen der IT-Welt auch in der Automation einsetzen zu können. Jetzt werden wir damit konfrontiert, dass auch die Bedrohung der IT-Welt in die Automatisierungswelt einwirken – und damit die Verfügbarkeit von Produktionsanlagen beeinflussen.
Gleichzeitig sind aber die funktionalen Anforderungen und die Kommunikationsbeziehungen zwischen den Geräten und Systemen in der Automatisierungswelt wesentlich komplexer als in der Office- oder Corporate IT-Welt.
Wir wollten die gleiche Infrastruktur – hierfür sind jetzt Lösungen verfügbar. Die Security-Lösungen und Philosophien der IT-Welt sind aber nicht unmittelbar auf die Automatisierungswelt übertragbar. Mögliche Ansätze können daher entweder in der Weiterentwicklung und Anpassung bestehender Lösung der Corporate IT liegen oder in der Neuentwicklung von spezifischen Lösungen für die Automatisierungswelt. Beide Ansätze sind bei den am Markt verfügbaren Lösungen anzutreffen.

Was sind die spezifischen Anforderungen in der Automatisierungstechnik an Security-Lösungen?

F. Klasen: Nutzt man die Möglichkeiten der verfügbaren Technologien beider Welten, so sind in der Automatisierungstechnik die Kommunikationsbeziehungen zwischen den Geräten und Systemen inhomogener und komplexer. Es stel-

len sich zusätzliche Anforderungen wie z.B. die Echtzeitfähigkeit der Kommunikation. Anders als in der Bürowelt oder auch der Prozessindustrie ist die Anzahl der embedded Systeme in der Fertigungsautomatisierung sehr groß, die nicht ohne größeren Aufwand mit Updates nachgerüstet werden können. Das Einspielen von Security-Patches, wie es in der IT-Welt gang und gäbe ist – kommt hier praktisch nicht in Frage.
Darüber hinaus ist derzeit zu beobachten, dass die Intelligenz der Systeme in die Feldgeräteebene wandert, womit die Anzahl der Kommunikationsteilnehmer steigt und darüber hinaus auch Funktionen von Kommunikationsinfrastrukturkomponenten wie z.B. Switches in diese Feldgeräte verlagert werden. Damit steigt die Anzahl der zu managenden Geräte und Systeme ganz erheblich und als Folge werden in den Automatisierungsprotokollen zunehmend Managementfunktionen für die Parametrierung und Verwaltung dieser Geräte implementiert – letztlich auch um die Produktionsanlagen in der Projektierungs- und Inbetriebnahmephase autonom betreiben zu können.

Kommen wir zurück zu der Veranstaltung – von welchen Teilnehmern wurde die Veranstaltung besucht?

F. Klasen: Die Veranstaltung richtete sich an Unternehmen der produzierenden Industrie. Teilnehmer und Referenten kamen überwiegend aus Anwenderunternehmen, so dass die Betreibersicht im Vordergrund der Diskussionen stand – bewusst weniger die Sicht von Lösungsanbietern. Die Veranstaltung war im Sinne einer B2B-Konferenz angelegt. Die Referenten berichteten über Lösungen in ihren eigenen Unternehmen. Die Teilnehmer kamen sowohl aus dem Bereich Corporate IT und Netzwerkbetrieb als auch aus dem Produktionsbereich.

Welche Themen wurden diskutiert?

F. Klasen: Die Referenten stellten Strategien, Konzepte und konkrete Maßnahmen zum Management und Schutz von Netzwerken und IT-Systemen im Produktionsumfeld vor. Das wohl am häufigsten verwendete Wort an den beiden Tagen war „Patch-Management" – ein Zeichen dafür, dass die Beiträge von Seiten der Referenten eher aus der Sicht der IT-Welt dargestellt wurden. Häufig endete der Verantwortungsbereich der dargestellten Lösung dann auch an der Grenze zur Produktionsanlage. Lösungen aus dem Bereich der Automatisierungstechnik sind zwar auch am Markt verfügbar – Erfahrungen damit liegen bei den Betreibern selber aber erst seit relativ kurzer Zeit vor.

Gibt es denn überhaupt Lösungsansätze?

F. Klasen: Das hängt natürlich davon ab, welche Bedrohungsszenarien man denn überhaupt betrachtet. Im Großen und Ganzen konzentrieren sich die Lösungen derzeit auf eine sinnvolle Abgrenzung von Produktionsbereichen bis herunter zur Absicherung von Einzelgeräten. Auch die „Härtung" von Einzelgeräten spielt eine zunehmend wichtige Rolle. Und in die Normung kommt Bewegung – einige wichtige nationale und internationale Gruppen arbeiten derzeit an Entwürfen für Normen im Security-Bereich. Darüber hinaus werden von Nutzerorganisationen wie der IAONA oder der PNO Security-Policies, -richtlinien und Merkmalkataloge veröffentlicht.

Sprechen IT-Leute und Automatisierer überhaupt dieselbe Sprache?

F. Klasen: In den Unternehmen gibt es kaum Mitarbeiter, die in beiden Welten zu Hause sind und beide Welten gleich gut kennen. Die Verständigung ist dann auch nicht ganz einfach, weil durchaus unterschiedliche Ziele verfolgt werden. Ein IT-Bereich in einem Unternehmen ist an einer Optimierung und einer möglichst einheitlichen Managementstruktur der IT-Systeme interessiert – aus dieser Sicht ist der Bereich der vernetzten Produktion kompliziert und unattraktiv. Für die Produktion hat dagegen die Verfügbarkeit der Fertigungsanlagen oberste Priorität. Wie die Zusammenarbeit der beiden Bereiche in den Unternehmen erfolgt, ist aber sehr unterschiedlich. Es stellt sich auch die Frage, ob der tradierte organisatorische Zuschnitt dieser Bereiche noch angemessen ist.
Jedenfalls könnten beide Bereiche eine Menge voneinander lernen.

Informationsportal IT-Security

Das Institut für Automation & Industrial IT (AIT) der Fachhochschule Köln unterstützt Unternehmen beim Einsatz von IT-Lösungen in der Automatisierungstechnik und der Produktion. Aus Anlass des Kongresses „IT-Sicherheit in der Automation" wird derzeit ein Informationsportal aufgebaut und betreut, das sich gezielt dem Thema IT-Security in der Automation widmet (www.security-in-automation.com). Fragen, Anregungen, Beiträge und Meinungen zu diesem Thema und dem vorliegenden Artikel senden Sie bitte an: klasen@gm.fh-koeln.de.

Mit welchen Fragen bzw. Anregungen oder „Hausaufgaben" haben die Teilnehmer nach der Veranstaltung den Heimweg angetreten?

F. Klasen: Die Klärung der Grenzen der Verantwortlichkeit, den Ausgleich des Wissensdefizits zwischen der IT-Welt und der Automatisierungswelt und die Frage der Ressourcen!

Hat eine Annäherung der beiden Welten im Rahmen der Veranstaltung stattgefunden?

F. Klasen: Ich glaube, dass den Teilnehmern die Vielschichtigkeit des Themas IT-Security in der Automation deutlich geworden ist. Klar geworden ist auch, dass man keine Patentrezepte erwarten kann. Eine Lösung hat nicht nur Technologieaspekte zu berücksichtigen – Security-Maßnahmen umfassen immer auch Prozesse und Personen. Unternehmens-Policies und Anwendungsaspekte sind daher genauso wichtig. Klar geworden ist: Produkte und Technologien sind weder das alleinige Problem noch die alleinige Lösung!

Prof. Dr. Frithjof Klasen
Institut für Automation & Industrial IT
Fachhochschule Köln

Easy Info • 281

Höhere Systemverfügbarkeit im Industrial Ethernet

Innominate Security hat den Funktionsumfang ihrer Firewall-Lösung MGuard um zahlreiche Features erweitert. Die neue Softwareversion MGuard 3.0 kommt in der Industrie-Firewall und beim Racksystem BladePack zum Einsatz, das die Schnittstellen zwischen Fertigungs- und Büronetzwerken schützt. Zehn neue Firewall-Features erhöhen ab sofort die Verfügbarkeit der gesicherten Systeme. Durch den Einzug offener Standards wie TCP/IP und Ethernet in die Welt der Produktionsautomatisierung werden diese Netzwerke auch anfällig für Viren, Würmer oder andere Schadprogramme. Das Unternehmen setzt mit seiner Produktreihe auf die Strategie der „device attached security". Das bedeutet, dass jedes System oder sinnvoll zusammengefasste Systemgruppe mit je einer eigenen Firewall einzeln abgesichert wird.

Easy Info • 282

Cybercrime in TK-und IT-Systemen

Wie sich Unternehmen wirkungsvoll gegen kriminelle Lausch- und Online-attacken schützen können, zeigt die NRW-Landesinitiative „secure-it.nrw" am 15.02.06 in Bonn mit dem kostenfreien Workshop „Wirtschaftsspionage und Abhörsicherheit". Von Wanzen und Abhörschutz über „man in the middle-Attacken" bis hin zu Mobile Security und WLAN-Sniffing erläutern Experten mit praktischen Vorführungen die größten Risiken und geben Tipps, wie sich Unternehmen wappnen können. Der Workshop findet von 14-18 Uhr in den Räumen der Deutschen Telekom statt; teilnehmen können alle interessierten Unternehmen. Weitere Infos und Anmeldung unter: www.secure-it.nrw.de

Easy Info • 283