zeitschrift für automation und security

Nr.3 · September 2012 · ISSN 2193-8555

IT-Security und Security für Systeme
der Automatisierungs-, Leit- und Steuertechnik

Interview mit Ramon Mörl, Geschäftsführer itWatch GmbH Seite 9

# "Industrie vernachlässigt SCADA-Sicherheit"

Angriffe stoppen Seite 28

## Malwareschutz für die Produktion

Unterbrechungsfrei produzieren

## USV schützt gegen Stromausfälle

Seite 20

Seite 16

Apps in der Industrie:

## Warum Experten jetzt zum Handeln raten

Seite 34

Ramon Mörl, Geschäftsführer itWatch GmbH

# „Industrie vernachlässigt SCADA-Sicherheit"

**a+s:** *Herr Mörl, Schadsoftware wie Stuxnet und Duqu hat IT-Security in der Automatisierungstechnik stärker in den Vordergrund gerückt. Aus Ihrer Erfahrung heraus, würden Sie sagen, dass die beiden Schadprogramme für viele Unternehmen der erste Anlass waren, sich überhaupt mit dem Thema zu befassen?*

**Mörl:** Unsere vielen Gespräche mit Anwenderunternehmen auf den verschiedenen Fachmessen bestätigen leider die Tatsache, dass die Firmen bislang viel zu lax mit der IT-Sicherheit in der Automatisierungstechnik umgegangen sind und erst die verschiedenen Vorfälle Sensibilität geschaffen haben. Anwenderunternehmen entscheiden selbst in ihrem Risikomanagement und der Kosten-Nutzen-Analyse über den Reifegrad ihrer Systeme. Die itWatch-Lösung kann beispielsweise jede kritische Applikation in einer eigenen gesicherten Umgebung ablaufen lassen und zudem jede Datei, die auf ein System kommt oder dieses verlässt, einer Inhaltskontrolle unterziehen und die richtige Aktion, wie Blockieren, Protokollieren oder Verschlüsseln einleiten.

**Seit 1987 ist Ramon Mörl als Berater in Fragen der IT-Sicherheit tätig. Für Firmen wie HP, IBM, Siemens, ICL und Bull übernahm er leitende Tätigkeiten in Projekten in Belgien, Schweiz, USA und weiteren Ländern. Als unabhängiger Evaluator und Berater der Europäischen Union war er vor allem im Bereich der ECMA und ISO-Standards für die IT-Sicherheit tätig. Seit 2002 bringt der Dipl.-Informatiker seine Erfahrungen in die itWatch GmbH als Geschäftsführer ein.**

*Ramon Mörl, Geschäftsführer der itWatch GmbH, München*

**a+s:** *Wenn Sie mit Kunden im Bereich Automatisierung sprechen, finden Sie dann schon ein Konzept für die IT-Sicherheit vor oder gibt es praktisch keine Strategie zum Schutz der Produktionssysteme vor Schadsoftware und anderen IT-Bedrohungen?*

**Mörl:** Wie immer im Leben gibt es auch hier nicht nur schwarz oder weiß. Unternehmen haben meistens eine mehr oder weniger gut ausgebaute Sicherheitsstrategie zum Schutz ihrer Produktionssysteme. Trotzdem treffen wir auch heute noch Anwenderfirmen, die ihre vormals isolierten Rechner relativ ungeschützt ins Internet bringen und sich auch über weitere Angriffsvektoren keine Gedanken machen. Gerade aber die Tatsache, dass die Produktionssysteme zunehmend vernetzt werden und auch über mobile Datenträger in den Datenaustausch mit einbezogen werden, zeigt die Notwendigkeit für standardisierte IT-Sicherheitslösungen. Neue Herausforderungen entstehen, da die in der Produktionswelt verbauten Systeme oftmals alt sind und keinem regelmäßigen Patch-Management unterliegen. Unserer Einschätzung nach hinkt der Markt für IT-Sicherheit von SCADA- und Automatisierungssystemen um bis zu zehn Jahre hinter dem IT-Markt hinterher.

**a+s:** *Sind die Firmen schon soweit, dass man das Sicherheitsniveau mithilfe von Produkten erhöhen kann, oder müssen erst Prozesse und Awareness angepasst werden?*

**Mörl:** Gerade im Bereich SCADA und Automatisierung muss nicht der Anwender oder die Betreiberorganisation selbst IT-Sicherheitswissen sammeln. Es geht vornehmlich um Produkte und Anlagen, die im besten Fall die adäquate Sicherheit schon in sich tragen oder mit geeigneten Checklisten ausgeliefert werden sollten, was noch für den sicheren Betrieb auf baulicher Seite bereitgestellt werden sollte. Die modernen Angriffe haben auch gezeigt, dass Prozesse, organisatorische Lösungen und Awareness-Maßnahmen immer mit technischen Lösungen unterlegt werden müssen. Die vernetzten Systeme und die vorhandenen offenen, standardisierten Schnittstellen wie USB, Bluetooth, SCSI etc. bieten natürlich einerseits hohen Nutzen, stellen aber andererseits auch Schwachstellen dar, die es zu kontrollieren gilt.

**a+s:** *Was ist Ihrer Ansicht nach der Grund dafür, dass IT-Security im Produktionsumfeld in vielen Unternehmen so lange vernachlässigt wurde?*

**Mörl:** Zum einen ist hier bestimmt die alte Weisheit „never touch a running system“ ein Verhinderer für den adäquaten Schutz gegen neue Angriffstechniken. Zum anderen ist aber auch die trügerische Annahme vorhanden, dass die größte Gefahr von den Anwendern ausgeht und auf den Produktionssystemen ja keine echten Anwender ihren täglichen IT-Aufgaben nachgehen.

**a+s:** *Sicherheit ist ein integraler Bestandteil in allen Anlagen der Automatisierungstechnik, allerdings eher unter dem Aspekt der Arbeits- und Maschinensicherheit (Safety). Gibt es Ihnen bekannte Ansätze, wo die beiden Bereiche in einem gemeinsamen Framework kombiniert werden?*

**Mörl:** Für die so genannte Safety gibt es aus verständlichen Gründen viele Sicherheitsnormen (VDMA, ZVEI) für die Umsetzung, da ja die Gesundheit von Personen betroffen sein kann. Der IT-Sicherheitsbedarf hingegen ist eher unternehmensindividuell. Mit dem IT-Grundschutzhandbuch des BSI gibt es aber auch hier standardisierte Maßnahmenkataloge. In der medizinischen Welt ist zum Beispiel über den HIPAA-Standard schon ein Versuch einer Integration gemacht worden. Wie immer muss aber die Priorität zwischen dem sicheren Funktionieren (also der Safety), der Verfügbarkeit des Systems und der Vertraulichkeit und Integrität der Daten und Komponenten individuell – auch in Notfallplänen – abgebildet werden.

**a+s:** *Sehen Sie, was die IT-Sicherheit angeht, prinzipbedingte Probleme in der Automatisierungstechnik, die sich nicht lösen lassen, ohne etablierte Paradigmen in Frage zu stellen?*

**Mörl:** Nein, es gibt keine unlösbaren Probleme. Sehr wohl sind aber Themen wie Echtzeitbehandlung, andere Werte im Risikomanagement und Prioritäten der Prozesse strukturell unterschiedlich.

**a+s:** *Sollte es nicht einfacher sein, IT-Sicherheit in einer Produktionsumgebung herzustellen, als in einem Büro? Schließlich haben die Benutzer normalerweise nichts mit dem IT-System zu tun, was über die bloße Bedienung der Applikation hinausgeht. Internetzugang kann grundsätzlich (für Nicht-Admins) ausgeschlossen werden, das physische Gerät kann man abschotten (alle Ports hinter Blenden), Softwareinstallation darf nur der Admin vornehmen. Eigentlich ideale Bedingungen, oder?*

**Mörl:** Das möchte man prinzipiell meinen, stellt dann aber in der Realität fest, dass die „Moderne“ bereits Einzug gehalten hat. Messdaten werden trotz Verbots über mobile Datenträger abgezogen und Programme installiert, der Wartungszugang aus Kostengründen über Internet zur Verfügung gestellt. Das geht bis zur Peer-to-Peer-Vernetzung über ungesicherte Funkschnittstellen. Wir nehmen einen schleichenden Vorgang wahr, der von der Innovation in der IT profitieren möchte, aber bei dem Risikomanagement eben die IT-Sicherheit häufig vergisst.

**a+s:** *Die Produktionstechnik nutzt mittlerweile zahlreiche Konzepte und Systeme aus dem Netzwerkbereich: x86 PCs für die Hutschiene, WLAN und Ethernet als Transportmedium, Router und VPN-Gateways als Infrastruktur. Haben Sie den Eindruck, dass die Hersteller, die solche, speziell für den Bereich Automatisierung entwickelte Produkte anbieten, den Sicherheitsaspekt ausreichend bedienen?*

**Mörl:** Oft geht es bei diesen Systemen nur um Funktionsfähigkeit und hohe Verfügbarkeit. Die Vertraulichkeit von Daten und – noch wichtiger – die Integrität der Systeme spielt hier eine nachgelagerte Rolle. Sicherlich gibt es in größeren Firmen IT-Sicherheitsbeauftragte, denen die PC-Technik in der Produktion nicht entgangen sein kann. Nur sind sie hierfür oft nicht verantwortlich. Die Produktion und die darin verbaute IT liegt in anderen Händen als die „normale“ Büro-Kommunikation. Auch wenn bereits verfügbare Sicherheitsprodukte den Bedarf optimal abdecken können, so mangelt es oft an den Kontakten zu diesen Personen. Diese Plattform möchten wir auf der it-sa – Deutschlands größter IT-Sicherheitsmesse – für alle Teilnehmer bieten.