

Schadsoftware macht auch vor der Automatisierung nicht halt

Beliebig umsteuern und normale Wirklichkeit nur vortäuschen

Die erste Anwenderkonferenz der Innominate Security Technologies zu industrieller Netzwerksicherheit und sicheren Remote Services stieß mit einem aktuellen Vortragsprogramm auf großen Zuspruch. Im Folgenden ein Auszug daraus.



70 Nutzer und Interessenten der mGuard Technologie aus dem Maschinen- und Anlagenbau folgten der Einladung Innominates zum Firmensitz nach Berlin Adlershof



Innominate Vorstand Dirk Seewald vergleicht die Unternehmenssicherheit mit der Arbeit eines Pförtners

Stimmte kraftvoll ein: Dr. Sandro Gaycken, Cybersecurity-Forscher an der FU Berlin schilderte den Teilnehmern mit seinem Leitvortrag „Post-Stuxnet Industrial Security – Die Welt im Cyberwar?“ die global veränderte Sicherheitslage. Etwa wie Regierungen, Militärs und Geheimdienste weltweit Cyberwaffen als äußerst probates und selbst bei Kosten in zweistelliger Millionenhöhe preiswertes Mittel erkennen, um die kritischen Infrastrukturen und Wirtschaftsunternehmen anderer Staaten mit modernen Informationsgesellschaften IT-gestützt zu erkunden und empfindlich zu treffen. Nach seiner Einschätzung haben Staat und Wirtschaft noch einen weiten Weg vor sich, um für eine angemessene Entnetzung kritischer Einheiten, bezahlbarer Informationstechnik, den Aufbau sicherer Organisationen und Produktionssysteme sowie Maßnahmen zur Abwehr von Angriffen durch Insider zu sorgen.

Im zweiten Leitvortrag „Inside Stuxnet – Analyse einer industriellen Malware und ihrer

Folgen“ führte Ralph Langner, CEO des Hamburger Beratungsunternehmens Langner Communications den Teilnehmern vor Augen, mit welcher Raffinesse und Perfektion die im Juni 2010 erstmals entdeckte industrielle Schadsoftware Stuxnet ihr Ziel verfolgte und erreichte. Schon der sogenannte Dropper-Anteil zur Infiltration und Infektion von Windows PC über USB-Medien und LAN verfügte über ungewöhnliche Komplexität und Aggressivität. Der Payload-Anteil, gewissermaßen der digitale Sprengkopf von Stuxnet, stellt allerdings alles bislang Gesehene in den Schatten. So gelang es dem Wurm, speicherprogrammierbare Steuerungen und zugehörige Projekte mit circa 15 000 Zeilen schadhaftem SPS-Programmcode verborgen zu infiltrieren. Dazu wurden von den Entwicklern der Schadsoftware aufwendig bislang wenig bekannte Möglichkeiten in Simatic S7 Steuerungen genutzt, u.a. das Überladen von System Function Calls und die Manipulation der Abbildung zwischen physikalischen und logischen Ein-

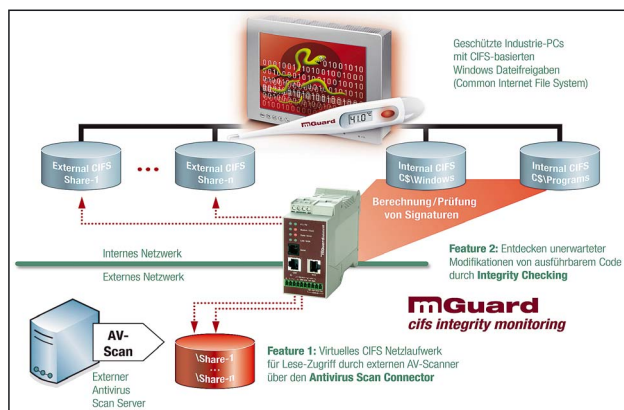
und Ausgängen in beiden Richtungen. So wird es möglich, einen physikalischen Prozess nach Belieben umzusteuern und gleichzeitig der Visualisierung am Leitstand eine ganz andere, „normale“ Wirklichkeit vorzugaukeln. Besonders bedrohlich: Die meisten der mit Stuxnet bekannt gewordenen Angriffstechniken lassen sich – und das sogar durch Werkzeuge automatisiert – von weit weniger versierten Nachahmungsstätern in neuer Schadsoftware wiederverwenden. Stuxnet-Derivate, die deutlich unspezifischer eine erheblich größere Zahl von Zielen schädigen könnten, werden daher als sehr wahrscheinlich befürchtet. Und sie werden auf eine Automatisierungslandschaft treffen, in der man vergleichbar wirksame Security Maßnahmen, wie sie in der Office-IT längst üblich sind, bis noch meist vergeblich sucht. Wie sich ein großes Fertigungsunternehmen diesen Herausforderungen stellt, erklärte Enrico Puppe, zuständig für die Sicherheit der produktionsnahen IT bei der Volkswagen AG

Nutzfahrzeuge. Regelmäßig werden dort zum Beispiel Profinet Audits sowie Labortests und Gefährdungsanalysen bei Bekanntwerden neuer Verwundbarkeiten durchgeführt. Ein um Konsens bemühtes, von Beginn an kooperatives Vorgehen von Herstellern, Systemintegratoren, Anlagenplaner, Betreiber und dessen Sicherheitsorganisation hat sich als Schlüssel zum Erfolg bewährt. Als technische Maßnahmen konnten so unter anderem Firewalls und Intrusion Protection Systeme (IPS) implementiert, Systeme und Applikationen gehärtet (Stichwort „minimale Maschinen“), Berechtigungskonzepte konzipiert und eingehalten sowie ein Monitoring und Reporting mit automatischer Eskalation etabliert werden. Ergänzt werden diese durch

gration und Fernwartung von Maschinen und Anlagen in Betreiber-netzen abdecken, bieten die mGuard rs2000 Geräte der Field Line künftig eine weniger komplexe, preisgünstige Alternative für die sichere Fernverbindung zu Feldsystemen über Internet und VPN. Erste TX/TX-Modelle beider Linien mit 2 Ethernet-Ports sind inzwischen verfügbar, Varianten mit Mobilfunk-Routern und integrierten Switches werden folgen. Auch für die mGuard PCI Karte und den bereits angekündigten mGuard delta sind Nachfolgemodelle auf Basis der mGuard core2 Architektur in Vorbereitung beziehungsweise bereits in Entwicklung.

Ebenfalls eingegangen wurde auf die jüngsten Innovationen im Bereich der mGuard

Firmware (Releases 7.1 bis 7.4). Dazu zählen insbesondere das Easy Initial Setup Verfahren, die neue High Availability Option mit Firewall- und VPN-Redundanz sowie das CIFS Integrity Monitoring Verfahren. Letzteres stellt eine interessante, industrietaugliche und nachrüstbare Alternative zu lokal installierter Antivirus- und Whitelisting-Software dar, welche ohne externe Zuführung von Malware-Signaturen und deren ständiges Update auskommt und bei-



Die mGuard core2 Plattform ist Basis der neuen Generation von Hutschienen-montierbaren Sicherheitsapplikationen Bilder: Innominate

organisatorische Maßnahmen wie Security-Richtlinien, Trainings, Notfallpläne und sichere Fernwartungszugänge.

Eine Präsentation zu den aktuellen Produktentwicklungen bei Innominate und der weiteren mGuard Roadmap sowie ein offenes Forum unter dem Motto „Was Sie schon immer mal über mGuard wissen wollten ...“ bildeten den Abschluss der Konferenz. Vorgestellt wurden insbesondere das zukunftssichere neue mGuard core2 Plattform Design und seine Mehrwerte für kommende mGuard Produkte und OEMs. Es ist Basis der neuen Generation von Hutschienen-montierbaren Sicherheitsapplikationen der mGuard Field und Factory Lines, die sich unter anderem durch Metallgehäuse, einen auf -20 bis +60°C erweiterten Temperaturbereich und die Nutzung wechselbarer SD-Karten als Konfigurationsspeicher auszeichnen.

Während die mGuard rs4000 Geräte der Factory Line dabei weiterhin umfassende Security-Funktionen bereit stellen und damit auch anspruchsvolle Szenarien wie die Inte-

spielsweise Stuxnet-Infektionen zuverlässig erkennt.

Ein besonderes Highlight der mGuard Roadmap ist das „HyperSecured“-Konzept zu den Trendthemen Virtualisierung und Hardware-Konsolidierung. Es erlaubt OEM, in kostensensitiven Embedded Applikationen, die keine eigene physische Security Appliance zulassen, einen vollwertigen mGuard als virtuelle Appliance mit weiteren virtuellen Maschinen (SPS, HMI, etc.) auf einer Hardware-Plattform mit Hypervisor zu integrieren. Als Machbarkeitsstudie hatte Innominate bereits im vierten Quartal 2010 gemeinsam mit den Partnern KW-Software und Wind River einen HyperSecured PLC realisiert und demonstriert. Wind River plant inzwischen eine Pre-Packaged Solution zum HyperSecured-Konzept mit virtuellem mGuard auf PowerPC-Basis (P2o2o) und WR Hypervisor.

■ **Torsten Rössel**

Innominate Security Technologies, Berlin