

Rohde & Schwarz Cybersecurity: Neue Sicherheitslösung mit Modbus-Protokoll-Dekodierung für Firewalls in der Industrie 4.0

Modbus-Protokolle sind in der Industrie der Kommunikationsstandard. Die zunehmende Vernetzung mit dem Internet in Folge von Industrie 4.0 macht das Protokoll allerdings zum Einfallstor für Cyber-Angriffe. Da dem Kommunikationsprotokoll spezielle Sicherheitsmaßnahmen fehlen, können Angreifer SCADA, ICS und andere auf Modbus-Protokollkommunikation basierende Industriesysteme einfach unterwandern und die Kontrolle über kritische Infrastrukturen übernehmen. Rohde & Schwarz Cybersecurity bietet ab sofort eine IT-Sicherheitslösung, die die Modbus-Protokollkommunikation absichert und Industrial Internet of Things (IIoT) gegen Cyber-Angriffe und Spionage schützt. Firewall-Anbieter, die die Lösung in ihre Sicherheitsprodukte einbetten, können den Anforderungen des Industrie-4.0-Marktes begegnen.

Leipzig, 20. April 2017. Rohde & Schwarz Cybersecurity, führender Hersteller von IT-Sicherheitslösungen für Unternehmen und Behörden, hat sein zentrales Netzwerkanalyse-Tool, die Deep Packet Inspection (DPI) Engine R&S PACE 2, um eine Funktionalität zur Modbus-Protokoll-Dekodierung erweitert. Die DPI Engine ermöglicht ab sofort die Erkennung und Extrahierung von Modbus-Inhalten und -Metadaten. Anbieter von Sicherheitsprodukten wie Firewalls oder Gateways können durch die feingranulare Analyse der Modbus-Protokollkommunikation Gefahren erkennen. Dadurch ist es möglich, Angriffe und Fehlkonfigurationen in SCADA- oder ICS-Umgebungen zu verhindern. Diese zusätzliche Sicherheitsfunktion verbessert bisherige Lösungen und macht sie bereit für die Anforderungen der Industrie 4.0.

„Firewall-Anbieter können die Deep Packet Inspection Engine in ihre Sicherheitsprodukte einbetten, um den Inhalt einer industriellen Protokollkommunikation zu untersuchen“, so Dirk Czepluch, VP der Business Units Network Analytics und Network Protection bei Rohde & Schwarz Cybersecurity. „Da die DPI Engine Inhalts- und Metadaten von Modbus erkennt und extrahiert, können Firewall-Hersteller detailliertere Regeln sowie Filter für einzelne Felder und Werte bestimmen, die für IT-Administratoren wichtig sind. Auf diese Weise können sie kontrollieren, wer mit dem Gerät kommunizieren darf, welche Art von Kommunikation erlaubt ist und natürlich Cyber-Angriffe und Spionage abwehren“, fügt Czepluch hinzu.

In der Energiebranche werden Strom-, Verkehrs- und Wassersysteme durch SCADA, CIS oder ICS betrieben. Es ist daher unabdingbar, dass die Schwachstellen in der Modbus-Protokollkommunikation geschlossen werden. Ein Angriff auf solche Systeme und Netzwerke könnte die Stromversorgung ganzer Regionen stilllegen oder kritische Systeme und Produktionsanlagen stören.

Die Entwicklung von Modbus-basierten Industriesystemen und -netzwerken konzentriert sich auf Verlässlichkeit, Verfügbarkeit und Geschwindigkeit. Da die Systeme jedoch für isolierte Umgebungen konzipiert sind, wurde ihre Sicherheit nicht berücksichtigt. Insbesondere fehlen dem Modbus-Protokoll gängige Sicherheitsmechanismen wie Authentifizierung, Vertraulichkeit und Integrität. Dadurch wird das Protokoll grundsätzlich unsicher und anfällig für Angriffe.

Modbus ist ein Protokoll der Anwendungsschicht, das für die Client/Server-Kommunikation zwischen Geräten sorgt, die mit unterschiedlichen Arten von Bussen oder Netzwerken verbunden sind. So messen beispielsweise SCADA-Systeme (Supervisory Control and Data Acquisition) oder Industriesteuersysteme die Temperatur und Luftfeuchtigkeit und geben die Messwerte mithilfe des Modbus-Protokolls an einen Computer weiter.

Unter <https://ipoque.com/solutions> erfahren Sie, wie Anbieter von IT-Sicherheitslösungen die DPI-Engine **R&S@PACE 2** nutzen, um ihre Netzwerksicherheitsprodukte weiter zu verbessern und ihren Kunden noch mehr Vorteile zu bieten.

Pressekontakt:

Christine Lorenz, Telefon: +49 34159403062, E-Mail: christine.lorenz@rohde-schwarz.com

Rohde & Schwarz Cybersecurity

Das IT-Sicherheitsunternehmen Rohde & Schwarz Cybersecurity schützt Unternehmen und öffentliche Institutionen weltweit vor Cyber-Angriffen. Mit hochsicheren Verschlüsselungslösungen, Next-Generation-Firewalls sowie Software für Netzwerkanalyse und Endpoint-Security entwickelt und produziert das Unternehmen technisch führende Lösungen für die Informations- und Netzwerksicherheit. Das Angebot der mehrfach ausgezeichneten und zertifizierten IT-Sicherheitslösungen reicht von kompakten All-in-one-Produkten bis zu individuellen Lösungen für kritische Infrastrukturen. Mit der Übernahme der DenyAll umfasst das Portfolio nun auch Firewalls und Schwachstellen-Scanner für geschäftskritische Web-Anwendungen. Im Zentrum der Entwicklung von vertrauenswürdigen IT-Lösungen steht der Ansatz „Security by Design“, durch den Cyber-Angriffe proaktiv statt reaktiv verhindert werden. Knapp 450 Mitarbeiter sind an den Standorten in Deutschland, Frankreich und Dänemark tätig.

Rohde & Schwarz

Der Technologiekonzern Rohde & Schwarz bietet innovative Lösungen auf allen Feldern der drahtlosen Kommunikationstechnik. Außerdem sorgt er für Sicherheit in der Informationstechnik. Vor mehr als 80 Jahren gegründet, unterhält das selbstständige Unternehmen ein engmaschiges Vertriebs- und Servicenetz mit Niederlassungen und Vertretungen in mehr als 70 Ländern. Zum 30. Juni 2016 betrug die Zahl der Mitarbeiterinnen und Mitarbeiter rund 10.000. Der Konzern erwirtschaftete im Geschäftsjahr 2015/2016 (Juli bis Juni) einen Umsatz von rund 1,92 Milliarden Euro. Der Firmensitz ist in Deutschland (München), in Asien und Amerika steuern starke regionale Hubs die Geschäfte.

R&S® ist eingetragenes Warenzeichen der Firma Rohde & Schwarz GmbH & Co. KG.