23/01/2014

EPR07/2014

www.enisa.europa.eu

Veraltete industrielle Steuerungssysteme für Energie, Wasser und Verkehr ohne ausreichende Cyber-Sicherheitskontrollen erfordern koordinierte Tauglichkeitsprüfungen auf EU-Ebene, sagt die EU Agentur für Netz- und Informationssicherheit ENISA

Heute veröffentlichte die EU Agentur für Netz- und Informationssicherheit ENISA einen neuen Bericht, um über die nächsten Schritte in Richtung einer koordinierten Prüfung der Leistungsfähigkeit der oft veralteten „Industrial Control Systems" (ICS) für die europäische Industrie zu beraten. Zu den wichtigsten Empfehlungen gehörten Prüfungen von ICS, welche ein Anliegen für alle EU-Mitgliedstaaten seien und ENISA zu folge auf EU-Ebenen behandelt werden könnte.

Heute werden IT häufig von industriellen Steuerungssystemen (z.B. SCADA) für Energie, Wasser und Verkehr eingesetzt. Diese werden verwendet, um die Effizienz zu verbessern, Kosteneinsparungen zu erzielen und die Automatisierung der Prozesse zu ermöglichen. Leider geht dies oft einher mit schlechter Planung, Mangel an Informationen, Sicherheitskonfigurationen sowie die Vereinigung von beidem: bereits bekannte und neue, unentdeckte oder noch nicht behobene "Zero-Day"-Schwachstellen in ICS / SCADA-Systemen.
ICS Systeme haben eine Lebensdauer von über 20 Jahren. Daher wurden sie traditionellerweise als unabhängige Systeme ohne ausreichende Sicherheitsanforderungen entworfen.
Folglich sind sie nicht gerüstet, um mit gegenwärtigen Bedrohungen umzugehen. Die Überwindung der heutigen Sicherheitslücken erfordert ein verlässliches Verständnis von Sicherheitsbelangen (d.h. Schwachstellen, ihre Herkunft, Häufigkeit, etc.). Die richtige Risikobewertung erfordert spezialisierte Werkzeuge und Methoden. Die Agentur betont, dass es eine starke Notwendigkeit nach einer bestimmten Strategie gibt, um die Ziele, die Mission und die Vision für eine Koordinationsfähigkeitsprüfung in der EU zu definieren.

Diese Studie untersucht, wie EU-Maßnahmen koordiniert werden können, um so eine Ebene einheitlicher, unabhängiger und vertrauenswürdiger ICS Testmöglichkeiten zu erreichen, die dann den derzeitigen Initiativen von Nutzen sein würden. Die Methodik umfasst Desktop-Forschung, eine Online-Umfrage und ausführliche Interviews mit 27 Experten aus der EU, den USA, Japan, Indien und Brasilien.

Die wichtigsten Ergebnisse und Empfehlungen

Diese Studie hat die 36 wichtigsten Ergebnisse und 7 Empfehlungen, sowohl für den öffentlichen als auch den privaten Sektor, herausgestellt, mit einem speziellen Fokus auf die EU-Behörde:

- 1. Die Schaffung einer Koordinationsfähigkeitsprüfung unter öffentlicher Europäischer Führung und einer starken Unterstützung durch die zuständigen öffentlichen, nationalen Behörden und dem privaten Sektor der EU
- 2. Die Einrichtung eines vertrauenswürdigen und fachlichen Vorstands, um eine Führung zu etablieren
- 3. Die Gründung oder Beteiligung von spezifischen Arbeitsgruppen

- 4. Bestimmung eines Finanzmodells, welches angesichts der Europäischen Lage geeignet ist
- 5. Durchführung einer Machbarkeitsstudie darüber, wie Tests organisiert werden sollten
- 6. Aufstellen von Kooperationsvereinbarungen mit anderen Organisationen, die sich mit ICS Sicherheiten befassen
- 7. Schaffung eines Wissensmanagement -Programms für ICS-Tests.

Der Executive Director von ENISA, Professor Udo Helmbrecht bemerkte: *"Es gibt eine offensichtliche Notwendigkeit, die Sicherheit in kritischen Informationsinfrastrukturen und ICS-System zu erhöhen; die Risiken nehmen zu, und sehr erfahrene Angreifer und Naturkatastrophen haben die Schwächen der Systeme gezeigt. Allen beteiligten öffentlichen und privaten Einrichtungen wird dringend empfohlen, diese Sicherheitsbedenken Ernst zu nehmen."*

Für den vollständigen Bericht
Hintergrund: EU Cyber Security Strategy **Für Interviews;** Ulf Bergström, Sprecher, ulf.bergstrom@enisa.europa.eu, Mobil: + 30 6948 460 143, oder Adrian Pauna, Experte, resilience@enisa.europa.eu

Übersetzung. Das Englische Original ist die einzige maßgebliche Fassung.
http://www.enisa.europa.eu/front-page/media/enisa-auf-deutsch
www.enisa.europa.eu