19. Dez. 2011

www.enisa.europa.eu

Industrielle Steuerungssysteme: Empfehlungen für Europa und Mitgliedsländer

ENISA, die Europäische Agentur für Cybersicherheit, hat heute die Ergebnisse einer Studie über die Sicherheit von industriellen Steuerungssystemen (Industrial Control Systems, ICS) veröffentlicht. Der Bericht beschreibt die aktuelle Situation hinsichtlich der ICS-Sicherheit und empfiehlt sieben Verbesserungsmöglichkeiten.

Industrielle Steuerungssysteme (Industrial Control Systems, ICS) sind Steuerungs- und Kontrollnetzwerke und Systeme, die zur Unterstützung industrieller Verfahren entwickelt wurden. Diese Systeme werden zur Überwachung und Kontrolle unterschiedlicher Verfahren und Tätigkeiten genutzt, wie Gas- und Stromversorgung, Wasser- und Ölaufbereitung und Eisenbahnverkehr.

In den letzten zehn Jahren verzeichneten diese Systeme eine beträchtliche Anzahl von Störfällen. Dazu gehört der „Stuxnet"-Angriff, bei dem möglicherweise maßgeschneiderte Schadsoftware dazu verwendet wurde, nukleare Steuerungssysteme im Iran anzugreifen, und die vor Kurzem ‚aktualisierte Variante' dieser Schadsoftware, DuQu. Diese Störfälle haben ICS-Nutzer sehr verunsichert.

2011 hat sich die ENISA mit den wichtigsten Bedenken in Bezug auf ICS-Sicherheit beschäftigt und paneuropäische und internationale Initiativen dazu erarbeitet. Zu den beteiligten Interessengruppen gehören Anbieter von ICS-Sicherheits-Tools und -Dienstleistungen, Hersteller von ICS-Software/-Hardware, Infrastrukturbetreiber, öffentliche Körperschaften, Normungsgremien, Hochschulen sowie der Bereich Forschung und Entwicklung.

Der Abschlussbericht schlägt in Bezug auf die Verbesserung aktueller Initiativen und die Verstärkung von Kooperationen sieben praktische und wirksame Empfehlungen für ICS-Akteure aus dem öffentlichen und privaten Sektor vor. Die Empfehlungen fordern die Bildung nationaler und paneuropäischer Strategien zur ICS-Sicherheit, ein Handbuch für bewährte Praktiken bei ICS-Sicherheit, Forschungsaktivitäten und die Einführung eines gemeinsamen Tests hinsichtlich der Reaktionsfähigkeit auf ICS-Computer-Notfälle.

„Echte Sicherheit für industrielle Steuerungssysteme kann nur durch gemeinsame Bemühungen erreicht werden, die sich durch Kooperation, Wissensaustausch und

*gegenseitiges Verständnis **aller** involvierter Interessengruppen auszeichnet",* so Rafal Leszczyna, Verfasser des Berichts.

Professor Udo Helmbrecht, Geschäftsführender Direktor von ENISA, fügte hinzu:

„Stuxnet hat das Sicherheitsproblem industrieller Steuerungssysteme bekannt gemacht. Unsere Studie zeigt deutlich, dass in diesem Bereich von allen relevanten Interessengruppen noch viel getan werden muss. Wir hoffen, dass unsere sieben Empfehlungen zu bedeutenden Verbesserungen führen werden."

Hintergrund: Im April 2007 führte der Rat der Europäischen Union ein Europäisches Programm für den Schutz kritischer Infrastrukturen (EPSKI) ein. Das Schlüsselelement des EPSKI ist die Direktive zur Identifikation und Bestimmung von kritischen Infrastrukturen in Europa. Parallel dazu wurden im Rahmen der Digitalen Agenda für Europa (DAE) und des CIIP-Aktionsplans Informationen über Sicherheitsangelegenheiten bei wichtigen Infrastrukturen in Europa herausgegeben. Die Ergebnisse der ENISA-Studie wurden während eines Workshops im September 2011 in Barcelona bestätigt.

Vollständiger Bericht

Ansprechpartner für Interviews: Ulf Bergstrom, Pressesprecher ENISA, press@enisa.europa.eu, Mobil: + 30-6948-460-143

http://www.enisa.europa.eu/front-page/media/enisa-auf-deutsch

Übersetzung**. Das Englische Original** ist die einzige maßgebliche Fassung.