6/12/2013

EPR/18/013
www.enisa.europa.eu

Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) betont die Notwendigkeit eines besseren Schutzes von SCADA-Systemen

Wie lange können wir es uns noch leisten, sensible IT-Infrastrukturen mit nicht gepatchten SCADA-Systemen zu verwenden, fragt die Europäische Agentur für Netz- und Informationssicherheit (ENISA). ENISA argumentiert, dass die EU und ihre Mitgliedstaaten verpflichtendes Patch-Management einführen könnten, um somit Sicherheitslücken zu überbrücken, Cyber-Attacken abzuschwächen und für die Gesellschaft wichtige Infrastruktur zu schützen.

Ein großer Teil der sensiblen Infrastruktur in Europa kann in den Bereichen Energie, Beförderungsmittel und Wasserversorgung gefunden werden. Diese Infrastrukturen sind weitgehend von sogenannten SCADA-Systemen (Supervisory Control and Data Acquisition gemanaged (eine Unterkategorie von Industriellen Steuerungssystemen (ICS)). Die SCADA-Technologie hat sich im letzten Jahrzehnt maßgeblich entwickelt und von einzelnen abgeschlossenen Systemen wegbewegt. Heutzutage operieren SCADA-Technologien in offenen Architekturen und mit Hilfe von Standardtechnologien, welche stark mit anderen Netzwerken sowie dem Internet verbunden sind.

- Als Konsequenz zu diesen Veränderungen sind SCADA-Systeme nun verstärkt für Attacken von außerhalb des Systems angreifbar.
- Zurzeit sind die bedeutendsten Probleme mit Patching der Fehlerrate (60%)[1] und der Nichtexistenz des Patchens an sich; weniger als 50% der 364 als kritisch eingestuften, öffentlichen Infrastrukturen hatten Patches[2] für SCADA zur Verfügung.

ENSIA hat verschiedene Best Practices und Empfehlungen herausgestellt, welche den Sicherheitsstatus von SCADA-Systemen durch Patchings maßgeblich verbessern. Anbei sind einige Beispiele:

- Kompensierende Kontrollen:
  - Eine Verstärkung der Verteidigung durch Netzwerkeinteilung um vertrauenswürdige Zonen aufzubauen, welche durch Zugangskontrollen miteinander kommunizieren;
- Eine Verbesserung des SCADA-Systems durch das Entfernen von unnötigen Leistungen;
- Patch-Management und Dienstleistungsverträge:
  - Eigentümer sollten auch einen Dienstleistungsvertrag für das Patch-Management aufstellen und somit klar die Verpflichtungen des Verkäufers und des Konsumenten im Patch-Managementprozess festlegen;
  - Eigentümer sollten immer ihre eigenen Tests, entweder virtuell oder durch ein separates System durchführen.
  - Zertifizierte Systeme sollten nochmals ratifiziert werden, nachdem ein Patch angewendet wurde.

---

[1] *„In 2011, ICS-CERT hatte eine Fehlerrate von 60% bei Patches welche bekanntgegebene Schwachstelle in Kontrollsystemen beheben sollten.")*

[2] *Weniger als 50% der 364 von ICS-CERT identifizierten Schwachstellen hatten Patches zur Verfügung." (SCADA Security Scientific Symposium (S4) Jänner 2012, McBride)*

Der Geschäftsführer der ENISA, Professor Udo Helmbrecht, kommentierte: *„Obwohl Patch-Management nicht eine Wunderwaffe ist, mit der alle SCADA-Sicherheitsprobleme gelöst werden können, ist es doch von großer Bedeutung, dass Unternehmen über eine Patch-Managementpolitik verfügen. Die Europäische Union und ihre Mitgliedstaaten könnten das Bewusstsein für Patch-Management stärken, indem sie die Bedeutung des Patch-Managements bei der Neudefinierung von Gerätvorschriften betonen.“*

Zum vollständigen Report
Hintergrundinformationen: EU Cyber Security Strategy,
Für Interviews; Ulf Bergström, Sprecher, ulf.bergstrom@enisa.europa.eu, Mobiltelefon: + 30 6948 460 143, oder Adrian Pauna, Experte, adrian.pauna@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