softScheck
we identify vulnerabilities others don't

Pressemitteilung

Industrie 4.0 Security

Sankt Augustin, 7. Januar 2013

Die IT-Sicherheitsberatung softScheck GmbH hat einen 5-stufige Prozess zur Absicherung von Industriesteuerungen entwickelt und wird ihn auf der BITKOM-Veranstaltung ‚Industrie 4.0' am 9. Januar in Berlin vorstellen.

Bisher wird von Unternehmen und Behörden fälschlicherweise nur versucht, die vielfältigen Angriffe zu erkennen. Unberücksichtigt bleibt dabei, dass jedem erfolgreichen Angriff unverzichtbar eine Sicherheitslücke zugrunde liegt, die der Angriff ausnutzt. Angriffe werden unmöglich, wenn die jeweils ausgenutzte Sicherheitslücke identifiziert und behoben wird!

Der Prozess, in dem bisher nicht-erkannte Sicherheitslücken identifiziert werden: **Zero-Day-Vulnerabilities**, besteht aus den folgenden 5 Stufen:

1. **Threat Modeling**: Review and Evaluation of Software Security Architectures to identify Vulnerabilities
2. **Static Source Code Analysis**
3. **Penetration Testing** to check on already known Vulnerabilities
4. **Dynamic Analysis - Fuzzing**: Review and Evaluation of the executable, compiled file – no Source Code necessary
5. **Explorative Testing** and manual Code Auditing

Das **BSI und das ICS-CERT warnen vor zunehmenden Angriffen auf Industriesteuerungen**, speicherprogrammierbare Steuerungen / Programmable Logic Controller (SPS/PLC). Allein mit dem Verfahren Threat Modeling wurden von softScheck in einer Stichprobe aus 15 Projekten aus dem Bereich Industriesteuerungsanlagen ca. 1.000 Threats identifiziert - darunter ca. 100 hoch-kritische, bisher nicht-erkannte Sicherheitslücken. Wirkungsvoll ist auch das Verfahren Dynamic Analysis: Fuzzing, das mit bis zu 50 (!) Tools sehr erfolgreich eingesetzt wird. Das BSI listet die konkreten Bedrohungen: „Industrial Control System Security - Top 10 Bedrohungen" (ICSS-Top 10). Die von softScheck eingesetzten Verfahren werden u.a. vom Bundesamt für Informationssicherheit (BSI) unterstützt.

Über softScheck

Die softScheck GmbH hat sich in den letzten Jahren als Alleinstellungsmerkmal in Europa mit der kostengünstigen Identifizierung bisher nicht-erkannter Sicherheitslücken (**Zero-Day-Vulnerabilities**) in jeder Art Software (und auch Hardware) neue, attraktive Wachstumsfelder erschlossen: In Anwendungssoftware (Webapplications, ERP, ERM, CRM, SCM, E-Business, CIM etc.) und Netzwerk-Protokollen, Embedded Systems und Industrial Control Systems (ICS), Manufacturing Execution Systems - Produktionsleitsysteme mit MES, SCADA (Leittechnik und –systeme), SPS bis zur Feldebene, im Smart Grid (z.B. Smart Meter Gateway), Cyber Physical Systems, M2M, Industrie 4.0, in Apps und Applets für smart and mobile Devices, im Cloud Computing und auch in Hardware.

softScheck führt regelmäßig **Sicherheitsprüfungen** von Software und Hardware durch. Daneben bietet softScheck selbstverständlich auch die klassische IT-Sicherheitsberatung an vom Grundschutz (ISO 27000-Familie) bis hin zur Hochsicherheit in der Informationsverarbeitung (Redundanz und Diversität) – auch mit Consulting, Coaching und Forensics.

Kontakt:

Anja Wallikewitz
Tel.: 02241 – 255 43 – 11
Fax: 02241 – 255 43 – 29
anja.wallikewitz@softScheck.com

softScheck GmbH
Bonner Straße 108
53757 Sankt Augustin
www.softScheck.com