admeritia

Community-Projekt "Top 20 Secure PLC Coding Practices":

Am 15.06. werden erstmals sichere Programmierpraktiken für Steuerungen (SPS) veröffentlicht

Am Dienstag, 15. Juni 2021, werden erstmals "Secure Coding Practices" für speicherprogrammierbare Steuerungen (SPS) veröffentlicht. Solche Programmierprinzipien, die helfen, Security zu berücksichtigen, sind gängig für IT-Software, aber für das Programmieren von SPSen gab es so etwas bislang nicht.

SPSen kommen überall zum Einsatz, wo Maschinen und Anlagen gesteuert und geregelt werden. "Secure Coding Practices" für SPSen sind daher insbesondere für die Absicherung von kritischen Infrastrukturen (etwa Stromversorger, Wasserversorger und Nahrungsmittelproduzenten) relevant, die in Deutschland durch das gerade verabschiedete IT-Sicherheitsgesetz 2.0 stärker reguliert worden sind.

Die "Top 20 Secure PLC Coding Practices" sind das Ergebnis eines internationalen Community-Projekts, für das alle Mitarbeitenden ehrenamtlich tätig waren.

Nach über einem Jahr Arbeit steht das Projektergebnis nun ab 15.06.2021, 15 Uhr MESZ, auf https://www.plc-security.com **zum kostenfreien Download zur Verfügung**.

Es enthält eine zweiseitige Zusammenfassung aller 20 "Programmierpraktiken" sowie weitergehende Informationen auf bis zu vier Seiten je "Practice", eine Anleitung, Hintergrundinformationen, Security-Nutzen, Implementierungsbeispiele und Referenzen auf verwandte Standards und Frameworks.

Ziel des Projekts

Das Dokument ist frei verfügbar und mit einer maximal freigiebigen Lizenz ausgestattet, die jegliche Weiterverwendung, Kopie und Nutzung für kommerzielle und nicht-kommerzielle Zwecke erlaubt. Der Wunsch der Projektinitiatoren und des Projektteams ist es, das bislang fehlende Wissen über sichere Programmierung von SPSen zu verbreiten und fest im Wissensschatz von SPS-Programmierern, -Nutzern und -Herstellern zu verankern. Die Secure Coding Practices könnten in Informationssicherheits-Managementsystemen, Leitlinien für die sichere Systementwicklung sowie in Anforderungen für Lieferanten genutzt werden.

Das Dokument darf und soll daher genutzt und kommentiert werden - es wird ein Kommentarformular auf der Projektwebsite zur Verfügung stehen. Vor allem das Feedback von Anwendern und Herstellern von SPSen ist ausdrücklich erwünscht. Die "Top 20 Secure PLC Coding Practices" sollen regelmäßig aktualisiert werden.

Als weitere Zusammenarbeit ist unter anderem mit einem Team der US-amerikanischen Organisation MITRE geplant, das analog zur bekannten, ebenfalls bei MITRE entwickelten "Common Vulnerability Enumeration" (CVE) eine "Common Weakness Enumeration" (CWE) erarbeitet. SPSen fehlen auch dort. Auch wird es voraussichtlich Trainingsangebote zu den Top 20 Secure PLC Coding Practices geben.

Hintergrund und Entstehung

Initiiert wurde das Community-Projekt nach einem Konferenzbeitrag von Jake Brodsky (https://www.youtube.com/watch?v=JtsyyTfSP1I) zur ICS-Security-Konferenz S4 im Januar 2020 durch den Konferenzleiter Dale Peterson. Die Leitung des Projekts übernahmen Sarah Fluchs, CTO des auf

industrielle IT-Security spezialisierten deutschen Beratungsunternehmens admeritia, und Vivek Ponnada, tätig für General Electric Canada.
Das Projekt wurde mit Infrastruktur unterstützt von der Dale Peterson und S4xEvents, der ISA Global Cybersecurity Alliance und der Firma admeritia GmbH, die auch die Webseite des Projekts mit der Liste der Top 20 Secure PLC Coding Practices und weiterführenden Informationen betreibt.

Für Experten der industriellen Security ist schon lange klar, dass SPSen zu den verwundbarsten Komponenten in automatisierten Anlagen gehören. Es gibt zahlreiche Berichte über Schwachstellen und inhärent unsichere Features in Steuerungen, die nicht zuletzt für die bekannten Security-Vorfälle Stuxnet oder Triton / Trisis ausgenutzt wurden. Dem gegenüber steht jedoch wenig Konkretes, um SPSen sicherer zu machen.

Dementsprechend war die Resonanz auf das Community-Projekt von Anfang an groß: Auf der eigens für das Projekt erstellten öffentlichen Plattform (top20.isa.org) registrierten sich knapp 1000 Nutzer, reichten Secure Coding Practices ein, kommentierten die Einreichungen und wählten die Top 20 der wichtigsten Programmierpraktiken aus. Die Zielgruppe des Projekts sind SPS-Programmierer. Auch von deutschen Integratoren, Betreibern und Verbänden aus dem Kontext der Automatisierungstechnik waren Mitglieder an der Erstellung beteiligt.

Weiterführende Informationen

- **Blogpost zur Projektvision:** https://fluchsfriction.medium.com/security-f%C3%BCr-die-sps-programmierung-6b7af27343e8 (29.07.2020)
- **Blogpost zur Erklärung der nun veröffentlichten Version:** unter https://fluchsfriction.medium.com/ (verfügbar ab 15.06., 15 Uhr)
- **Twitter-Account des Projekts:** https://twitter.com/secureplc
- **Projektwebsite:** https://plc-security.com (verfügbar ab 15.06., 15 Uhr)

Ansprechpartner

Wenn Sie weitere Texte, Logos / Bilder, Hintergrundinformationen oder Aussagen aus dem Projektteam benötigen, wenden Sie sich gern an unsere Ansprechpartner:

INHALTLICHES:

- Sarah Fluchs, CTO, Projektleitung Top 20 Secure PLC Coding Practices
- Sarah.fluchs@admeritia.de
- +49 2173 20363-0

ORGANISATORISCHES:

- Matthias Müller, Head of Marketing
- matthias.mueller@admeritia.de
- +49 2173 20363-0