Pressemitteilung

Hannover, Juli 2014

Zugriff durch Identifikation

Webschnittstellen zur Gerätekonfiguration sind typische Schwachstellen für Cyber-Angriffe. Über einen elektronischen Hardware-Serviceschlüssel, den SSV Security-Dongle SEC/1, lässt sich dieses Problem lösen.

Durch das Internet der Dinge (IoT), Cyber-Physical Systems und Industrie 4.0 wird die Anzahl der vernetzten Baugruppen in der Automatisierung in den nächsten Jahren sehr stark wachsen. Da praktisch jedes System zumindest eine webbasierte Benutzerschnittstelle (Konfigurationsoberfläche) für Inbetriebnahme- und Serviceaufgaben besitzt, steigt auch die Anzahl möglicher Angriffspunkte. Schon die Abfrage einer einfachen Benutzername/Passwort-Kombination stellt ein erhebliches Sicherheitsrisiko dar, da potenzielle Angreifer diese schnell herausfinden und sich Zugang verschaffen können. Aus Expertensicht besteht beim Schutz dieser Schnittstellen deshalb akuter Handlungsbedarf.

Mit dem Security-Dongle SEC/1 präsentiert SSV nun eine praxistaugliche Lösung zum Schutz webbasierter Konfigurationsoberflächen in der Automatisierung. Der SEC/1 besitzt eine typische kompakte Dongle-Bauform und ist mit RS-232- oder USB-Schnittstelle erhältlich. Steckt ein zugriffsberechtigter Mitarbeiter den SEC/1 auf die entsprechende Schnittstelle einer Automatisierungsbaugruppe, erfolgt eine abhörsichere Challenge/Response-Authentifizierung. Erst nach erfolgreicher Identifikation und der anschließenden Prüfung von Benutzername/Passwort ist ein Zugriff auf die webbasierte Konfigurationsoberfläche der jeweiligen Baugruppe möglich.

Neben dem reinen Zugriffsschutz eignet sich der Security-Dongle allerdings auch für die Umsetzung von „Principle of least Privilege (POLP)“-Konzepten. Dabei werden einem bestimmten Benutzer nach erfolgreicher Identifikation lediglich die speziell für ihn geltenden Freigaben in der Konfigurationssoftware eingeräumt und somit beispielsweise nur die minimal notwendigen Zugriffsrechte erteilt, bzw. spezielle Konfigurationsseiten angezeigt. POLP-Lösungen helfen so sehr effektiv teure Fehlbedienungen zu vermeiden, da ein Benutzer lediglich auf jene Gerätefunktionen Zugriff erhält, für die er auch geschult wurde. Das größte Sicherheitsrisiko bei vernetzten Automatisierungsbaugruppen ist dadurch schnell gebannt.

Der Security-Dongle SEC/1 ist ab sofort zusammen mit einem speziellen Sicherheits-Setup als Standardzubehör für die Remote Access Gateways IGW/922 und IGW/925 verfügbar. Selbstverständlich kann dieser aber auch nachträglich an andere Baugruppen angepasst werden. Für interessierte Gerätehersteller bietet SSV auf Anfrage ein entsprechendes Integrations-Kit an. Mit diesem lassen sich auch bestehende Systeme mit einem entsprechenden Zugriffsschutz nachrüsten.

Den Text sowie das zugehörige Bildmaterial dieser Pressemitteilung finden Sie zum Download auf unserer Webseite www.ssv-embedded.de

Informationen zu SSV Software Systems:

Die SSV Software Systems GmbH wurde 1981 in Hannover als Entwicklungsdienstleister für Mikroprozessoranwendungen in der Logistik und Automatisierung gegründet. Seit Anfang der 90er Jahre entwickelt und produziert das Unternehmen eigene Hardwarebaugruppen und Systeme für den Industrieeinsatz.
Der Anwendungsschwerpunkt liegt dabei im Bereich der industriellen HMI- und M2M-Kommunikation. Zu den neuesten Entwicklungen gehören komplette Lösungsbausteine für kommunikationsintensive Embedded-System-Anwendungen, Security Gateways und -Server sowie Fernzugriffslösungen für dezentrale Energieerzeuger.

Informationen

SSV Software Systems GmbH
Susanne Mundrzik
Dünenweg 5
D-30419 Hannover
E-Mail: smu@ssv-embedded.de
Tel.: +49(511) 40 00 042
Fax: +49(511) 40 00 040
www.ssv-embedded.de

Pressekontakt

SSV Software Systems GmbH
Jörg Neumann
Dünenweg 5
D-30419 Hannover
E-Mail: jne@ssv-embedded.de
Tel.: +49(511) 40 00 013
Fax: +49(511) 40 00 040
www.ssv-embedded.de