PRESSEMITTEILUNG

OT/IT-Gateway ermöglicht virtuelles Patchen

Durch neue rechtliche Rahmenbedingungen erhält die Cybersicherheit der Operation Technology (OT) einen völlig neuen Stellenwert. Dazu gehört in Zukunft auch die Verpflichtung, erkannte Schwachstellen durch Software-Updates zu beheben. Ist das nicht möglich, lässt sich mit dem IGW/936A von SSV ein virtueller Patch realisieren, um externe Zugriffe auf Schwachstellen in OT-Baugruppen zu unterbinden.

Hannover, im September 2023. Verschiedene neue EU-Regelwerke zur Informationstechnik sowie Änderungen zur Produkthaftung erfordern ein Umdenken hinsichtlich der OT-Cybersecurity. Aus diesen Vorgaben lässt sich ableiten, dass in Zukunft anlassbezogene Software-Updates zur Fehler- und Schwachstellenbeseitigung für Produktanbieter verpflichtend werden. Aber auch die Betreiber von IT- und OT-Infrastrukturen sind gefordert. Sie müssen mit Hilfe geeigneter Cybersicherheits-Management-Prozesse systematisch nach potenziellen Schwachstellen suchen und diese beheben.

In der vernetzten Automatisierung existieren diesbezüglich allerdings weitere Herausforderungen. Zum einen lässt sich nicht jede Baugruppe innerhalb eines OT-Netzwerks im Bedarfsfall durch einen Software-Update auf den neuesten Stand bringen. Die Ursachen dafür sind unterschiedlich. Teilweise werden von den Herstellern einfach keine Updates entwickelt. In einigen Fällen stehen auf Grund der End-of-Support-Problematik keine aktuellen Software-Patches zur Verfügung. Vielfach sind solche Updates technisch auch gar nicht vorgesehen bzw. auf Grund der Baugruppenkonstruktion unmöglich. Zum anderen gibt es für die Betreiber von Maschinen und Anlagen aber auch verschiedene funktionale Gründe, die gegen Software-Updates oder den Austausch bestimmter Baugruppen sprechen. Dazu gehören z. B. Echtzeitaspekte, die Maschinensicherheit, bestimmte Vertragsbedingungen mit Haftungsausschluss bei Veränderungen usw.

Mit dem IGW/936A hat SSV ein spezielles Gateway für Cyber-sichere OT/IT-Integrationsaufgaben entwickelt. Es ist als Infrastrukturbaugruppe zur Domänenbildung bzw. Domänenisolation zwischen Ethernet-basierten IT-Netzwerken sowie Maschinen und Anlagen vorgesehen. Zum Lieferumfang gehört eine Patch-Management-Server-Software, um in der Gateway-Laufzeitumgebung virtuelle Software-Updates zum Schließen der Sicherheitslücken einzelner OT-Systeme zu aktivieren. Darüber hinaus unterstützen weitere Gateway-Funktionen die sichere OT/IT-Vernetzung für Baugruppen mit fehlender Verschlüsselung, unzureichender Authentifizierung sowie fehlenden Datenintegritätsmerkmalen. Über optionale Sensoren eignet sich ein IGW/936A auch für zusätzliche Überwachungsaufgaben hinsichtlich der jeweiligen Anwendungsumgebung.

Jürgen Fitschen, der für das Produktkonzept zuständige F&E-Manager bei SSV, erklärt: „Bei der Konzeption der IGW/936A-Hardware- und Softwarefunktionen haben wir uns nicht nur auf den Zugriffsschutz der OT-Netzwerkschnittstellen konzentriert, sondern über externe Sensoren auch den Zutritt zu Schaltschränken sowie Manipulationen der Umgebungsbedingungen in die zu überwachenden Parameter einbezogen. Dadurch ergibt sich ein dreidimensionaler Cybersicherheitsansatz für Automatisierungsumgebungen, auf Wunsch auch mit einer NSL-Meldeschnittstelle zu externen Alarmzentralen.“

Über SSV Software Systems:
SSV Software Systems 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 Hardware-baugruppen und Systeme für den Industrieeinsatz. Der Anwendungsschwerpunkt liegt dabei im Bereich der industriellen M2M- und IoT-Kommunikation. Zu den neusten Entwicklungen gehört eine Produktfamilie für „vollständig datenbasierte Embedded-Systems-Funktionen“. Dabei werden sowohl die Hardware-CAD-Daten als auch Quellcodes für das Betriebssystem und die Firmware an den Anwender übergeben, um eine „Deely-Embedded-Integration“ in die eigene Baugruppe zu ermög-lichen. Mit Hilfe dieser Technikbausteine werden nun verschiedene OT/IT-Gateways für Cybersicherheits-Retrofit-Lösungen neu entwickelt.

Bei Fragen wenden Sie sich bitte an:

SSV Software Systems GmbH
Werner Bührig
Dünenweg 5
D-30419 Hannover

E-Mail: wbu@ssv-embedded.de
Tel.: +49 511 40000-22
Fax: +49 511 40000-40
Website: www.ssv-embedded.de
LinkedIn: www.linkedin.com/company/ssv-software-systems

Das zugehörige Bildmaterial dieser Pressemitteilung finden Sie zum Download auf unserer Website www.ssv-embedded.de.

Bildmaterial:

Bildunterschrift:
Sicherheitslücken in vernetzten Baugruppen und Systemen werden in der Regel über Software-Updates geschlossen. In der vernetzten Automatisierung ist ein solcher Patch-Vorgang für OT-Baugruppen aber nicht immer möglich. In einigen Fällen stehen einfach keine Updates zur Verfügung. Teilweise ist ein Software-Patch auch auf Grund der Anlagensicherheit unmöglich. In einer solchen Situation ist ein virtueller Patch für das externe IGW/936A OT/IT Gateway eine Retrofit-Alternative, um externe Zugriffe auf die Sicherheitslücken bestimmter Baugruppen innerhalb einer OT-Domäne zu unterbinden.