PRESSEMITTEILUNG

KI-basierte Alarmanlage für OT-Netzwerke

Operational Technology (OT)-Netzwerke sind zahlreichen Gefahren ausgesetzt. SSV hat eine auf KI-basierende adaptive Sensorik realisiert, die Cyberangriffe mittels Echtzeitüberwachung bereits in einer sehr frühen Phase automatisch erkennt und die Verantwortlichen alarmiert.

Hannover, im September 2024. Vernetzte Baugruppen in einem Operational Technology (OT)-Netzwerksegment sind aus Sicht der Cybersicherheit im Vergleich zu IT-Systemen überwiegend schwach geschützt. Bestenfalls existiert eine Perimeterschutzfunktion zwischen den einzelnen Netzwerksegmenten, beispielsweise eine Firewall. Die OT-Baugruppen selbst sind gegen Cyberangriffe relativ ungeschützt.

Mit einem neu entwickelten Embedded Intrusion Detection System (IDS) möchte SSV diesen sicherheitskritischen Zustand ändern. Dafür nutzt eine spezielle Anwendung - das IDS Data Exploration Tool (IDET) - Funktionen aus dem Bereich der künstlichen Intelligenz und des maschinellen Lernens (ML), um den Normalzustand der Kommunikationsbeziehungen in einem Netzwerksegment oder direkt an einer Geräteschnittstelle zu erlernen. Das IDET erzeugt dann ein plattformunabhängiges KI-Modell, das einer Inferenz Engine anschließend in Echtzeit die Anomalieerkennung in den Netzwerkdaten ermöglicht.

Henrike Gerbothe, die für diese Lösung zuständige SSV-Managerin erklärt: „Das IDS wird in die gewünschte Zielumgebung integriert und an den typischen Datenverkehr angepasst. Dazu bieten wir als Unterstützung einen Remote Expert Assistance Service, bei dem ein SSV-Experte gemeinsam mit dem Anwender über eine temporäre Lese-Zugriffsmöglichkeit auf das OT-Netzwerk die erforderlichen Verkehrsdaten als CSV-Datei erfasst, um damit das Embedded IDS zu trainieren und ein KI-Modell zu generieren. Anschließend wird ein zur Aufgabe passender IDS Sensor, z. B. ein Gateway, installiert und in Betrieb genommen."

Das SSV Embedded IDS ist wahlweise als lizenzierbare Softwarekomponente oder vorinstalliert in einer IDS Sensor Hardware ab sofort verfügbar. Neben dem IDET stehen darüber hinaus verschiedene Service Docker zur Verfügung, um automatische Updates und die Alarmweitergabe zu unterstützen.

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 „Deeply-Embedded-Integration" in die eigene Baugruppe zu ermög-lichen. Mit Hilfe dieser Technikbausteine werden nun verschiedene (I)OT/IT-Gateways für Cybersicherheits- und Wireless-Retrofit-Lösungen neu entwickelt.

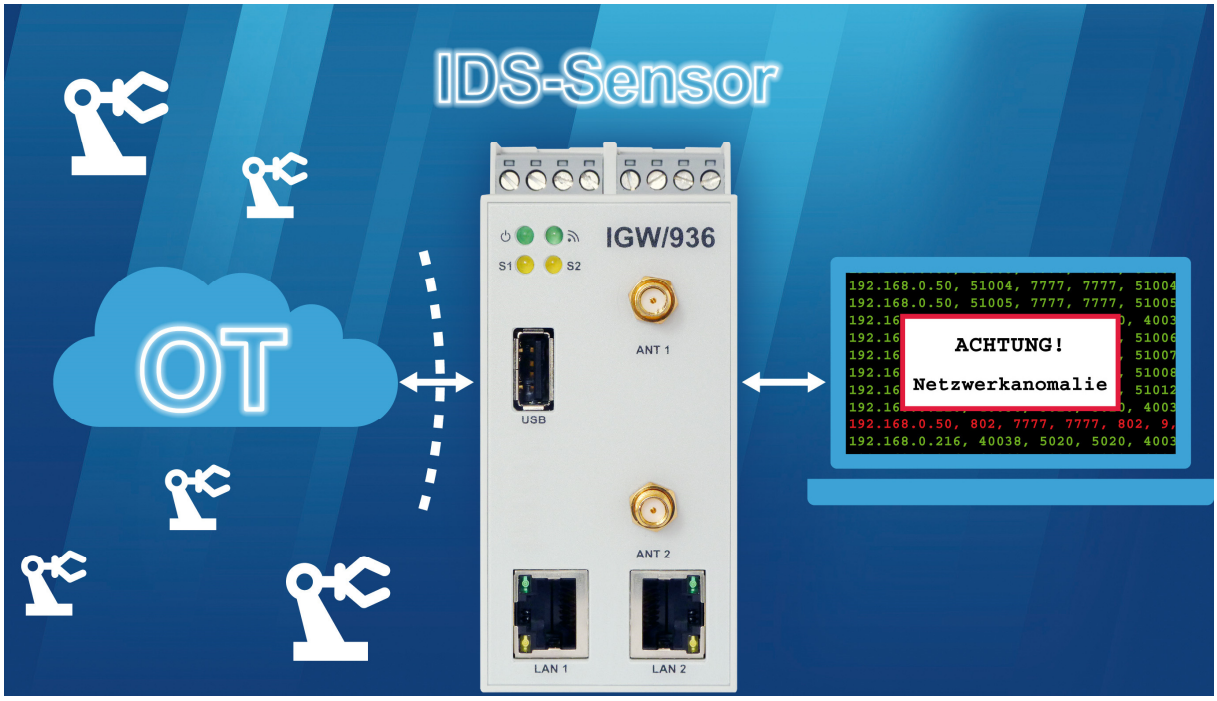
Bei Fragen wenden Sie sich bitte an:

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:
Vernetzte Baugruppen in einem Operational Technology (OT)-Netzwerksegment sind aus Sicht der Cybersicherheit im Vergleich zu IT-Systemen überwiegend schwach geschützt. Bestenfalls existiert zwischen den einzelnen Netzwerksegmenten eine Firewall. Die OT-Baugruppen selbst sind gegen Cyberangriffe relativ ungeschützt. Mit dem OT/IT-Gateway IGW/936A als Intrusion Detection System (IDS)-Sensor bietet SSV eine einfach zu handhabende Lösung, um Cyberangriffe und anormale Kommunikation innerhalb von OT-Netzen automatisch zu erkennen. Die dafür genutzte Echtzeitüberwachung basiert auf künstlicher Intelligenz (KI) und maschinellem Lernen (ML).