Ihr Ansprechpartner:

Barbara Weber

Barbara.Weber@profibus.com

 +49 721 9658-549

**P R E S S E M I T T E I L U N G**

# Weitere Schutzmaßnahmen ergänzen bewährtes IT-Sicherheitskonzept für PROFINET

**Karlsruhe, 17. September 2020:** Schon sehr früh - parallel mit den ersten PROFINET-Spezifikationen - veröffentlichte PI ein umfassendes Security-Konzept, das in mehreren Schritten weiter detailliert und angepasst wurde. Dabei reicht es nicht, Anlagennetze und Automatisierungskomponenten zu schützen, sondern die eingesetzten Schutzmechanismen und Konzepte dürfen den laufenden Produktionsbetrieb nicht stören. Zudem müssen Schutzkonzepte einfach umsetzbar und bezahlbar bleiben. Der wichtigste Aspekt ist jedoch, dass die Konzepte immer wieder an die aktuellen Entwicklungen angepasst werden müssen. PI hat nun sein IT-Sicherheitskonzept ergänzt.

Das IT-Sicherheitskonzept für PROFINET geht von einem Defense-in-Depth-Ansatz aus. Dabei wird die Produktionsanlage durch einen mehrstufigen Perimeter (u. a. Firewalls) gegen Angriffe, insbesondere von außen, geschützt. Darüber hinaus ist innerhalb der Anlage eine weitere Absicherung durch Unterteilung in Zonen unter Einsatz von Firewalls möglich. Zusätzlich wird durch einen Security-Komponententest die Festigkeit der PROFINET-Komponenten gegen Überlastung in einem definierten Umfang sichergestellt. Dieses Konzept wird durch organisatorische Maßnahmen in der Produktionsanlage im Rahmen eines Security-Management-Systems unterstützt.

Allerdings ist Security ein Thema, das permanent an die aktuelle Entwicklung angepasst werden muss und daher nie abgeschlossen ist. Dies gilt insbesondere vor dem Hintergrund der zunehmenden Vernetzung von Produktionsanlagen. So sorgt der Einsatz von PROFINET-Komponenten mit Mehrwert, also z. B. Web- oder OPC-Kommunikation, für eine vermehrte, direkte Kommunikation mit übergeordneten Systemen außerhalb der Sicherheitszone. Gleichzeitig wird eine Trennung von PROFINET-Netzwerken immer schwieriger.

Außerdem werden die Netzwerke größer, so dass immer mehr Komponenten zu einem Netzwerk verbunden werden und miteinander interagieren. Ein erfolgreicher Angriff auf ein einzelnes (PC-) System innerhalb einer solchen Zelle umgeht daher Vorab-Schutzmaßnahmen. Auch behindern weit verteilte Anlagen den physischen Schutz von Netzwerken und Zugangspunkten. Dadurch können unbefugte Personen Zugang zum PROFINET-Netzwerk erhalten.

Aus diesem Grund müssen bisherige Konzepte, die in der Hauptsache auf eine Abschottung der Produktionsanlagen setzen, durch neue Konzepte, die einen Schutz innerhalb der Zelle ermöglichen, ergänzt werden. PI hat daher die bisherigen Maßnahmen durch weitergehende Schutzmaßnahmen erweitert. Dazu gehören ein Credential Management, z. B. für eine Authentifizierung der Geräte, und eine End-to-End-Security-Erweiterung für die PROFINET-Kommunikation als Konfigurationsoption. Da nicht jede Anwendung die gleichen Sicherheitsanforderungen stellt, wurden bei PROFINET drei Sicherheitsklassen definiert.

Weitere technische Details und Praxisbeispiele finden sich im Industrie 4.0 Highlight „Security“ unter <https://www.profibus.com/technology/industrie-40/>. Diese Kampagne auf der PI-Webseite greift aktuelle Themen, Fragestellungen und Trends aus Industrie 4.0-Anwendungen auf, damit der Anwender diese leicht in die Praxis umsetzen und realisieren kann.

\*\*\*

# Grafik: PI hat sein Sicherheitskonzept für PROFINET um weitere Schutzmaßnahmen ergänzt.

****

**Pressekontakt:**

PI (PROFIBUS & PROFINET International)

PROFIBUS Nutzerorganisation e. V.

Barbara Weber

#### Haid-und-Neu-Str. 7

#### D-76131 Karlsruhe

Tel.: 07 21 /96 58 - 5 49

#### Fax: 07 21 / 96 58 - 5 89

Barbara.Weber@profibus.com

<http://www.PROFIBUS.com>

Der Text dieser Pressemitteilung liegt unter [www.profibus.com](http://www.profibus.com) zum Download für Sie bereit.