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**

# Neues Security-Whitepaper

**Hannover, 01. April 2019**: PI (PROFIBUS & PROFINET International) veröffentlicht ein neues Security Whitepaper, das die grundlegenden Konzepte für eine Absicherung des PROFINET-Protokolls dokumentiert. Das Whitepaper „Security-Erweiterungen für PROFINET“ soll dazu dienen, weitere Abstimmungsgespräche mit Anwendern, Integratoren aber auch Herstellern zu führen. Ziel dieser Diskussion ist ein abgestimmtes und tragfähiges Konzept, welches die industrielle Kommunikation mit PROFINET fit für die Anforderungen im Umfeld von Industrie 4.0 macht. Die Umsetzung wird zu einer Security-Spezifikation für PROFINET-Netze führen, die ergänzend zu der bereits seit mehr als 10 Jahren verfügbaren Security-Guideline bereitgestellt wird.

Die durchgängige Vernetzung im Unternehmen, die vertikale Integration und die Tendenz zu flacheren Systemhierarchien erfordern weiterreichende Ansätze für die IT-Sicherheit in der Produktion. Bisherige Konzepte, die in der Hauptsache auf eine Abschottung der Produktionsanlagen setzen, müssen durch neue Konzepte, die einen Schutz der Komponenten vorsehen, ergänzt werden.

Das aktuelle IT-Sicherheitskonzept für PROFINET geht von einem Defense-in-Depth Ansatz aus, wie er in der IEC 62443 beschrieben ist. Die Produktionsanlage wird dabei durch einen mehrstufigen Perimeter (u. a. Firewalls) insbesondere gegen Angriffe von außen geschützt. Darüber hinaus ist innerhalb der Anlage eine weitere Absicherung durch Unterteilung des Netzwerkes in Zonen möglich. Zusätzlich wird durch einen Security-Komponententest die Festigkeit der PROFINET-Komponenten gegen Überlastung in einem definierten Umfang sichergestellt. Dieses Konzept wird um organisatorische Maßnahmen in der Produktionsanlage im Rahmen eines Security-Management-Systems erweitert.

Die beschriebenen Schutzmaßnahmen für PROFINET entsprechen grundsätzlich dem heutigen Stand der Technik. Neue Anforderungen von Anwendern setzen jedoch einen weitergehenden Schutz auf Komponentenebene voraus, die geeignete Schutzmaßnahmen auf Protokollebene erfordern.

Das Whitepaper „Security-Erweiterungen für PROFINET“ beschreibt die neuen Security-Anforderungen, daraus abgeleitete Schutzziele und auf Basis der durchgeführten Analysen die wesentlichen Konzepte und Schutzmaßnahmen für ein PROFINET-System. Die Security-Arbeitsgruppe wird im nächsten Schritt Erweiterungen des PROFINET-Protokolls spezifizieren und es mit zusätzlichen kryptografischen Funktionen ertüchtigen, um Integrität, Authentizität und, sofern erforderlich, die Vertraulichkeit der Kommunikation auf Protokollebene sicherzustellen. Ziel ist, den technischen Aufwand für Anlagen mit einfachen Security-Anforderungen zu limitieren bei gleichzeitiger Wahrung der Rückwärtskompatibilität mit der Möglichkeit, das erweiterte Protokoll parallel zum bisherigen Protokoll in einem Netzwerk betreiben zu können.

Das Whitepaper liegt zum kostenlosen Download auf der PI-Webseite unter: <https://www.profibus.com/profinetsecurity>

\*\*\*

**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.