PMeV NETZWERK SICHERE KOMMUNIKATION
KOMPAKT Nr. 8/2019

PMeV widmet sich einsatz- und sicherheitskritischen Breitbandapplikationen

Der PMeV – Netzwerk Sichere Kommunikation hat eine Plattform für einsatz- und sicherheitskritische Breitbandapplikationen gegründet, die sich unter anderem mit der Standardisierung einer Leitstellenschnittstelle befasst. In dem Gremium sind namhafte Unternehmen aus der Branche für sicherheitskritische Kommunikation und bedeutende Anwender aus dem Bereich der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) vertreten. „Künftig werden sich durch die Einführung neuer Technologien die technischen Anforderungen an professionelle Leitstellensysteme enorm verändern. Dabei ist die Leitstellenschnittstelle von besonderer Bedeutung für die Einführung eines missionskritischen Breitbandnetzes-Netzes (4G/5G) für die BOS in Deutschland“, erklärt Volker Hartwein, stellvertretender PMeV-Vorsitzender und Leiter des Fachbereichs Leitstellen.

Leitstellen: In Zukunft mit standardisierten Schnittstellen zu 4G/5G

Foto: Frequentis

Schnittstelle zwischen Leitstellen und Systemen

Das „3rd Generation Partnership Project“ (3GPP), eine weltweite Kooperation von Gremien für die Standardisierung im Mobilfunk und federführend bei der Standardisierung von 4G und 5G, sieht die Funktionalität einer Leitstelle als Erweiterung der Funktionen und Merkmale des sogenannten UE-Clients (User Equipment) vor. Im Wesentlichen wäre die Leitstelle ein „Benutzer“ mit entsprechend erweiterten Berechtigungen und Befugnissen. Dabei wird jedoch nicht auf die besonderen Leistungsmerkmale komplexer Leitstellen einsatzkritischer Anwendungen eingegangen.

Da aber die Einführung missionskritischer 4G/5G-Systeme früher oder später vollzogen werden wird – erste Projekte sind derzeit bereits in Planung – ist aus Sicht des PMeV der Zeitpunkt gekommen, dieser insbesondere für professionelle Anwender aus den Sicherheitsbehörden so wichtigen Schnittstelle mehr Aufmerksamkeit zu widmen.

Kompetenzträger auch für Breitbandapplikationen

Einsatz- und sicherheitskritische Breitbandapplikationen gewinnen im Markt für Professionellen Mobilfunk und sicherheitskritische Kommunikation mehr und mehr an Bedeutung. Mit der Etablierung der Plattform zeigt sich der PMeV entschlossen, diese Entwicklung mit zu gestalten: „Wir wollen erster Ansprechpartner und Kompetenzträger für alle relevanten Themen der einsatz- und sicherheitskritischen Kommunikation sein“, erklärt der PMeV-Vorsitzende Bernhard Klinger.

Für den PMeV ist die Erweiterung seines Themenspektrums von besonderer Bedeutung. Die Thematisierung einsatz- und sicherheitskritischer Breitbandapplikationen fügt sich somit in das PMeV-Vorhaben ein, sich als Kompetenzträger für alle wichtigen Bereiche der sicheren Kommunikation zu positionieren. „Der PMeV“, so Bernhard Klinger, „greift neue und wichtige Entwicklungen in themenzentrierten Fachbereichen auf. Das schafft attraktive Plattformen für unsere Mitglieder und ein Höchstmaß an Flexibilität bei der Behandlung neuer Themen.“

PMeV - Netzwerk sichere Kommunikation
Professioneller Mobilfunk e. V. • Schönhauser Allee 10-11 • 10119 Berlin
Vorsitzender: Hytera Mobilfunk GmbH • Bernhard Klinger
Redaktion: Jochen Müller • Kommunikation & Public Affairs • Hobsweg 78 • 53125 Bonn
www.pmev.de • mueller@pmev.de

PMeV gründet Fachbereich Cybersecurity

Der PMeV – Netzwerk Sichere Kommunikation hat einen Fachbereich Cybersecurity gegründet. In der konstituierenden Sitzung wählten die Vertreter der PMeV-Mitgliedsunternehmen Nico Werner (telent GmbH) einstimmig zum Vorsitzenden des Fachbereichs. Mit der Gründung dieses Fachbereichs trägt der PMeV der hohen Bedeutung des Themas Cybersecurity für die sicherheitskritische Kommunikation und somit für die PMeV-Mitglieder Rechnung.

„Die Unternehmen beschäftigen sich immer intensiver mit Cybersecurity – sei es bei Leitstellen, im Hinblick auf 5G oder auch im direkten Umfeld des Professionellen Mobilfunks (PMR). Allerdings fehlen uns derzeit noch spezielle Anforderungen oder Lösungen, die für unsere Branche optimiert sind. Mit der Gründung des neuen Fachbereichs wollen wir dies ändern“, erklärt Nico Werner.

Cybersecurity als Kernaufgabe des PMeV

Erklärtes Ziel des PMeV ist es, das Bewusstsein dafür zu schaffen, dass sichere Kommunikationssysteme für Einsatz- und Rettungskräfte, Betreiber kritischer Infrastrukturen und die Industrie entscheidend zur Aufrechterhaltung der Sicherheit und Versorgung unserer Gesellschaft beitragen. „Um die Sicherheit dieser Kommunikationssysteme auch in Zukunft zu gewährleisten, muss Cybersecurity höchste Priorität bei Betreibern und Verantwortlichen der professionellen mobilen Kommunikation haben. Diese Arbeit im Interesse der Anwender sicherheitskritischer Kommunikation mitzugestalten, voranzutreiben und zu koordinieren ist eine Kernaufgabe des Verbandes“, sagt Bernhard Klinger, Vorsitzender des PMeV.

Egal auf welcher technologischen Plattform die Vernetzung von Anlagen und Systemen in Zukunft realisiert werden wird, ohne die Berücksichtigung der Cybersecurity wird man den Anforderungen sicherheitskritischer Anwender nicht gerecht werden können. Deshalb differenzieren diese Anwender beim Schlagwort Internet of Things (IoT) unter anderem zwischen Industrial Internet of Things (IIoT) oder Life Saving Internet of Things (LSIoT) und bringen so die Kritikalität der Anwendung zum Ausdruck.

Nico Werner Foto: telent

Umfassender Schutz der vernetzten Systeme

Um den umfassenden Schutz von Kommunikations- und Informationssystemen zu gewährleisten, geht Cybersecurity weit über herkömmliche Computer- und Netzwerksicherheit hinaus. Ungeachtet der Vorteile und Leistungsfähigkeit des professionellen Mobilfunks dürfen die Gefahren nicht unterschätzt werden, die sich etwa durch ein einzelnes vernetztes Gerät oder offene Hardware- oder Softwareschnittstellen (wie USB und API) auftun, die im ungeschützten Zustand Angreifern als Einfallstor in Unternehmen dienen. Ein gesamtheitliches Sicherheitskonzept ist zudem Basis für Prozessoptimierung sowie Resilienz.