Foto: kachel_koeln - Fotolia.com

Mobilfunk mit entsprechendem Cyberschutz ist für Polizei und Rettungsdienste unverzichtbar.

Vor unbefugtem Zugriff und Manipulation schützen

Anwender, die sich auf ein reibungslos funktionierendes Kommunikationssystem verlassen müssen, benötigen Mobilfunk-Lösungen mit ausreichendem Cyberschutz.

THORSTEN ALTEMÖLLER

Ob Polizei, Rettungsdienste, Betreiber Kritischer Infrastrukturen oder industrielIe Produktionsbetriebe – sie alle nutzen Mobilfunk-Lösungen, die auf einen effektiven Cyberschutz angewiesen sind. Für diesen Zweck wurde Professioneller Mobilfunk (Professional Mobile Radio, PMR) als hochverfügbares, redundant ausgelegtes System einst entwickelt. PMR sollte in der Vergangenenheit jederzeit Sprachkommunikation ermöglichen, auch wenn die üblichen Richtfunkverbindungen gestört oder Leitungen durch Unfälle oder Brände beschädigt waren. PMR-Systeme sind dafür individuell auf die Bedürfnisse ihrer Anwender und deren betrieblichen beziehungsweise behördlichen Abläufe zugeschnitten. So ermöglichen sie es auch unter schwierigen Bedingungen in einem geschlossenen Netzwerk, etwa auf einem Firmengelände oder innerhalb einer spezifischen Nutzergruppe, wie der Betriebsfeuerwehr, zu kommunizieren.

> „In PMR-Systeme müssen robuste Sicherheitsmaßnahmen implementiert werden. “
>
> **Thorsten Altemöller,** Director Sales PMR bei der Telent GmbH

Mobilfunk vernetzt sich zunehmend

Die fortschreitende Digitalisierung verändert die Anforderungen an PMR-Systeme. Moderne Anwendungen wie Videotelefonie, IoT-Maschinen oder Augmented-Reality-Brillen müssen sich miteinander vernetzen und in hohem Maße Daten austauschen. Das bedeutet: PMR definiert sich nicht mehr als reines Sprachkommunikationssystem, denn es erfüllt mittlerweile die Anforderungen von schmalbandigen wie breitbandigen IP-basierten Systemen. Cybercrime spielt damit erstmals eine

Rolle. Ursprünglich war die PMR-Welt durch ihre proprietären Protokolle von außen kaum angreifbar. Doch damit verschiedene Geräte und Systeme, unabhängig von ihrem Hersteller oder ihrer spezifischen Hardware, miteinander und über das Internet kommunizieren können, wird mittlerweile einheitlich Internet Protocol (IP) verwendet. Ohne diese Standardisierung wären die Vernetzung von Geräten und die Übertragung von Datenpaketen zwischen verschiedenen Netzwerken wesentlich komplizierter und weniger zuverlässig. PMR wird dadurch – abhängig von Anwendung und Rolle in der Organisation – zum Bestandteil der IT oder OT (Operational Technology). Existieren dort Sicherheitslücken, eröffnet das Cyberkriminellen Zugang zu PMR-Systemen. Es führt kein Weg daran vorbei: In PMR-Systeme müssen robuste Sicherheitsmaßnahmen implementiert werden, um sie vor unbefugtem Zugriff und Manipulation zu schützen. Nur dann können sich Anwender auch zukünftig darauf verlassen, dass ihr Kommunikationssystem zu jeder Zeit und an jedem Ort funktioniert.

Doch beim Umbau der PMR-Architektur sollte der zweite Schritt nicht vor dem ersten erfolgen – so wichtig Cyberschutz auch ist. Zunächst muss die Frage geklärt werden, mit welcher Technologie die traditionell mit Schmalband ausgelegten Systeme zukünftig betrieben werden. Seit private 5G-Campuslösungen als lokale, abgegrenzte Netze mit eigenen Frequenzen für Industrieunternehmen und Organisationen verfügbar sind, gewinnt Breitband-PMR an Bedeutung. Wer eine bestehende PMR-Lösung in ein Breitbandsystem integrieren möchte, steht vor einem komplexen Prozess, der sorgfältig geplant und umgesetzt werden muss. Dabei gilt es, kein Geld für bisherige Investitionen zu verbrennen, sondern vorhandene digitale Funkkommunikationssysteme wie Tetra (Terrestrial Trunked Radio) und DMR (Digital Mobile Radio) mit Breitbandtechnologien zu einer interoperationalen Kommunikationslösung zu verbinden. Wie so etwas aussehen kann, zeigt sich an einem aktuellen Projekt in einem unterirdischen Abbaugebiet, in dem ein neues Tetra-System implementiert wird, da das Unternehmen eine zuverlässige Sprachtechnologie benötigt. Zur Verbindung mit einem privaten LTE-Netzwerk, das breitbandige Anwendungen ermöglicht, wird ein Gateway genutzt. Diese kombinierte Funklösung wird dann über eine Strecke von mehr als 30 Kilometern über eine optische Repeaterlösung verteilt. Um wie in diesem Fall ein zeitgemäßes Kommunikationssystem in eine bestehende Umgebung zu integrieren, ist viel Fachwissen im Aufbau und Betrieb von Netzwerken im Bereich PMR sowie in angrenzenden Technologien gefragt. Mit diesem Know-how, das erfahrene Systemintegratoren wie beispielsweise Telent besitzen, werden die Stärken und Schwächen verschiedener Technologien bewertet und für die individuellen Anforderungen passend kombiniert.

„Um in den anspruchsvollen, technologisch schnelllebigen Umgebungen der Zukunft weiterhin zuverlässig und hochverfügbar über PMR zu kommunizieren, müssen sich die Systeme fortentwickeln, um IoT- und Multimedia-Anwendungen einzubinden."

Breites Spektrum an Cyberschutz-Services

Ist die Entscheidung gefallen, wie bestehende PMR-Systeme durch die Integration von 5G und LTE weiterentwickelt werden, ist neben dem komplexen Migrationsprozess der Aufbau eines robusten Cyberschutzes wichtig. Auch dafür gibt es nicht die eine Universallösung, sondern ein breites Angebot an Managed Services. Die Dienstleistungen decken verschiedene Aspekte der Cybersicherheit ab, wie Firewall-Management, Endpunkt-Sicherheit oder Patch-Management. In Security Operations Center (SOC) übernehmen Cybersecurity-Experten mithilfe spezieller Tools die Echtzeitüberwachung und reagieren auf Sicherheitsereignisse. Bisher gibt es erst wenige SOC für OT. Der Schutz gemischter IT/OT-Infrastrukturen ist anspruchsvoll, da neben Kenntnissen in IT-Sicherheit ein umfassendes Verständnis der Strukturen in der Betriebstechnologie und ihrer Automatisierungs-, Prozess- und Netzleittechnik unerlässlich ist. Telent führt dieses interdisziplinäre Know-how in dem neuen Serviceangebot, SOC-as-a-Service, zusammen. Das Team integriert, analysiert und überwacht im Auftrag seiner Kunden die gesamte IT/OT-Infrastruktur einschließlich der PMR-Bereiche. Mithilfe eines Security Information and Event Management (SIEM) werden große Datenmengen ausgewertet, um relevante Sicherheitsvorfälle zu identifizieren. Technischen Tools sind im Kampf gegen Cyberkriminalität wichtig.

Um in den anspruchsvollen, technologisch schnelllebigen Umgebungen der Zukunft weiterhin zuverlässig und hochverfügbar über PMR zu kommunizieren, müssen sich die Systeme fortentwickeln, um IoT- und Multimedia-Anwendungen einzubinden. Deren Nutzung kann eine Verbindung zum Internet voraussetzen, wodurch das Risiko von Cyberangriffen ebenso steigt wie durch mögliche Sicherheitslücken der verwendeten Technologien und Geräte. Ohne angemessene Sicherheitsmaßnahmen besteht die Gefahr von Manipulationen und Unterbrechungen durch Cyberangriffe, was die Integrität und Zuverlässigkeit der Kommunikation gefährdet. Der Wandel der PMR-Welt von Schmalband hin zu Breitband wird deswegen nur erfolgreich gelingen, wenn PMR-Lösungen bestens gegen Cyberkriminalität geschützt werden. ■

Telent GmbH:
www.telent.de