PMeV NETZWERK SICHERE KOMMUNIKATION
KOMPAKT Nr. 8/2018

Cybersecurity trifft PMR: Netzwerke und Infrastrukturen sichern ist Chefsache

Von Nico Werner*

Wer bei Cybersecurity nur an einen modernen Begriff für IT-Sicherheit denkt, ist sich der Dimension des Themas nicht bewusst. Um den umfassenden Schutz von Kommunikations- und Informationssystemen zu gewährleisten, geht Cybersecurity weit über herkömmliche Computer- und Netzwerksicherheit hinaus. Ungeachtet der unbestreitbaren Vorteile und Leistungsfähigkeit des Professional Mobile Radio (PMR), 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. Es hat daher oberste Priorität bei Betreibern und Verantwortlichen für die PMR-Kommunikation.

Cybersecurity umfasst sowohl den Schutz von Kommunikationsanlagen und IT-Infrastrukturen sowie Serverräumen und Data Centern als auch Maßnahmen gegen Schadsoftware und die Sicherung von Mobilgeräten und vernetzten Maschinen. Der Einsatz von Standard-Software wie Betriebssystemen oder IP-basierten Applikationen für das Management bzw. den Betrieb von PMR-Netzen bietet einerseits wirtschaftliche und technische Vorteile, birgt aber andererseits mindestens genauso viele Gefahren. Die Digitalisierung und die Anbindung an das Internet der Dinge tangieren PMR-Systeme und bringen neben der Einsatzvielfalt auch zusätzliche Risiken mit sich.

Ein Beispiel ist das sogenannte „Cryptojacking“, das aus den englischen Begriffen „Cryptocurrency“ (deutsch:

Neu im PMeV:

KAITEC GmbH – Ingenieurleistungen für Nachrichten- und Übertragungstechnik

KAITEC Ingenieurleistungen für Nachrichten- und Übertragungstechnik

Matthias Lampe

KAITEC entwickelt und produziert seit über 15 Jahren kundenspezifische Lösungen im Bereich der Funkkommunikation. Das Unternehmen legt dabei den Fokus unter anderem auf den Bereich Objektfunk. Installation, Inbetriebnahme und Service der KAITEC-Produkte erfolgen deutschlandweit über qualifizierte Systempartner. Weiterhin bietet KAITEC Consultingdienstleistungen in allen Bereichen der Funkkommunikation an - insbesondere für den Objektfunk und für flächendeckende Funknetze.

Zu den kundenspezifischen Lösungen, die KAITEC anbietet, zählen u.a. Hardwarelösungen für den Objektfunk (2m, TMO, TMOa, DMO), Aktiv-Sendekoppler und Tablet Messsysteme. Im Bereich des Project Engineering & Consulting bietet das Unternehmen Strategieberatung das Unternehmen Strategieberatung und Lösungskonzepte, Systemplanung, Funkplanung, Vergabeunterstützung, Test und Messungen, Trouble Shooting, Schulungen, Training, Projektmanagement, Bauüberwachung und Abnahme.

Zu den Kunden der KAITEC zählen u.a. BOS-Anwender, Industrieunternehmen, Energieversorger und Straßenbetriebe. Sitz des Unternehmens ist Hösbach in der Nähe von Aschaffenburg.

www.kaitec-gmbh.de
matthias.lampe@kaitec-gmbh.de

Kryptowährung) und „Hijacking“ (deutsch: Entführung) gebildet wird. Diese Art des Angriffs ist bei Cyberkriminellen sehr beliebt. Sie „kapern“ Betriebssysteme, Server oder Browser mit dem Ziel, Computer für unerwünschtes Cryptocoin Mining, also das Schürfen digitaler Währungen, zu missbrauchen.

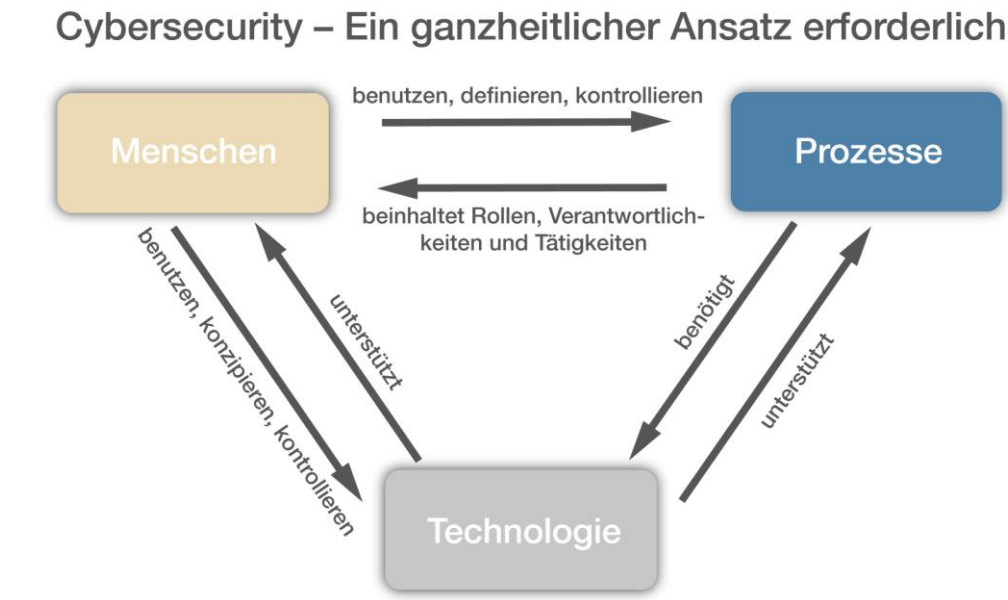
Ein Szenario ist der Aufbau eines Botnetzwerks aus zahlreichen vernetzten Geräten, darunter auch PMR-Systeme, über die Rechenpower entzogen werden kann. Während Angreifer einen minimalen Kostenaufwand haben, ist der reputative und wirtschaftliche Schaden auf Seiten der Betroffenen umso höher. Gefährlich daran ist, dass auch technisch nicht versierte Personen wie ehemalige Mitarbeiter oder Bewerber über diesen Weg z.B. die Möglichkeit haben, einem Unternehmen be-wusst zu schaden. Unternehmen, die sich gegen Angriffe wie diese schützen wollen, sind mit einigen Anforde-rungen konfrontiert, die aber unter dem Strich klare Vorteile mit sich bringen.

Herausforderungen und Vorteile auf einen Blick

Wer sich mit Maßnahmen für Cybersecurity oder Datenschutz befasst, stößt unweigerlich auf einige gesetzliche Vorgaben, wie das IT-Sicherheitsgesetz, die EU-NIS Directive (Security of network and information systems) oder die EU-Datenschutz-Grundverordnung.

Die Umsetzung dieser Regularien erfordert interne Ressourcen und Know-how. Des Weiteren haben professionelle Mobilkommunikation-Infrastrukturen im Vergleich zu Systemen für öffentliche oder Bürokommunikation eine längere Nutzungsdauer und müssen so immer wieder mit neuen Sicherheitsanforderungen kompatibel sein. „Security as a Function“ wird dabei abgelöst vom „Security by Design“-Prinzip, welches Sicherheit nicht mehr nur als Zusatzfunktion, sondern als explizite Anforderung von Beginn an in den Entwicklungsprozess integriert. Qualitative, automatisierte Sicherheitsmaßnahmen führen aber auch zu Kosten, die vor allem für kleine und mittlere Unternehmen und Organisationen ein Thema sind. Denn im Vergleich zu den verhältnismäßig geringen Herstellungskosten von Kommunikationsgeräten im Konsumentenbereich ist die Erfüllung von Sicherheitsanforderungen im professionellen Bereich aufwändig. Nicht zuletzt spielt Bedienerfreundlichkeit eine wichtige Rolle, denn die besten Schutzmaßnahmen nützen wenig, wenn sie niemand einsetzen kann

Sind Anforderungen wie diese erfüllt, dienen sichere Netzwerke und Infrastrukturen langfristig der Qualitätssicherung und Optimierung von Prozessen. Wer sich auf sichere Prozesse und zuverlässige Systeme stützt, kann diese kontinuierlich weiterentwickeln und verbessern. Dies ermöglicht es wiederum, die Kosten zu senken. Mit Maßnahmen zur Vorbeugung eines Schadensfalls



Ein gesamtheitliches Sicherheitskonzept muss Menschen, Prozesse und Technologie einbeziehen.

PMeV - Netzwerk sichere Kommunikation
Professioneller Mobilfunk e. V. • Schönhauser Allee 10-11 • 10119 Berlin
*Vorsitzender: e*Message Wireless Information Services Deutschland GmbH • Dr.-Ing. Klaus Hütten*
Redaktion: Jochen Müller • Kommunikation & Public Affairs • Hobsweg 78 • 53125 Bonn
www.pmev.de • mueller@pmev.de

vermeiden Unternehmen darüber hinaus eine Schädigung ihrer Reputation und stärken das Vertrauensverhältnis zu ihren Geschäftspartnern. Zuverlässige Services bilden wiederum die Grundlage für die betriebliche Optimierung. Nicht zuletzt ist das Zusammenspiel von Kommunikationsinfrastrukturen und Prozessen in einem sicheren Konzept essentiell. Dazu bedarf es nicht nur breiter Expertise über den Betriebsfunk, sondern eines übergreifenden Fachwissens. Spezialisten wie zum Beispiel telent und das Tochterunternehmen KORAMIS kombinieren das erforderliche Wissen aus einer Hand.

Strategische Entscheidung der Unternehmensführung

Wer Cybersecurity als Wettbewerbsvorteil einsetzen will, sollte immer ein ganzheitliches Konzept anstreben. Technologie ist nur ein Faktor. Man darf nicht aus den Augen verlieren, dass es Menschen sind, die sowohl die Prozesse definieren als auch die Technologie kontrollieren. Auf der einen Seite bedarf es also klarer Strukturen und Zuständigkeiten, um einen zuverlässigen Schutz zu gewährleisten. Auf der anderen Seite bietet Cybersecurity zahlreiche Optimierungsmöglichkeiten, die es zu identifizieren gilt.

So ist eine Security Policy gleichermaßen eine Frage des fachlichen Verständnisses und eine strategische Entscheidung auf Ebene der Unternehmensführung. Als Bestandteil der digitalen Transformation ist Cybersecurity ganz klar ein Business Enabler. Denn aus vertrauenswürdigen und gesamtheitlichen Sicherheitskonzepten schaffen Unternehmen nicht nur Prozessoptimierungen und Qualität – es eröffnen sich auch neue Optionen über die bislang erschlossenen Anwendungsmöglichkeiten hinaus. Essentiell sind dabei ein klares Bewusstsein der Verantwortlichen und die Sensibilisierung aller Beteiligten. Nur so lassen sich passgenaue Sicherheitslösungen finden und etablieren.

Der Autor:

Nico Werner ist Head of Cybersecurity der telent GmbH, einem Mitgliedsunternehmen des PMeV
nico.werner@telent.de