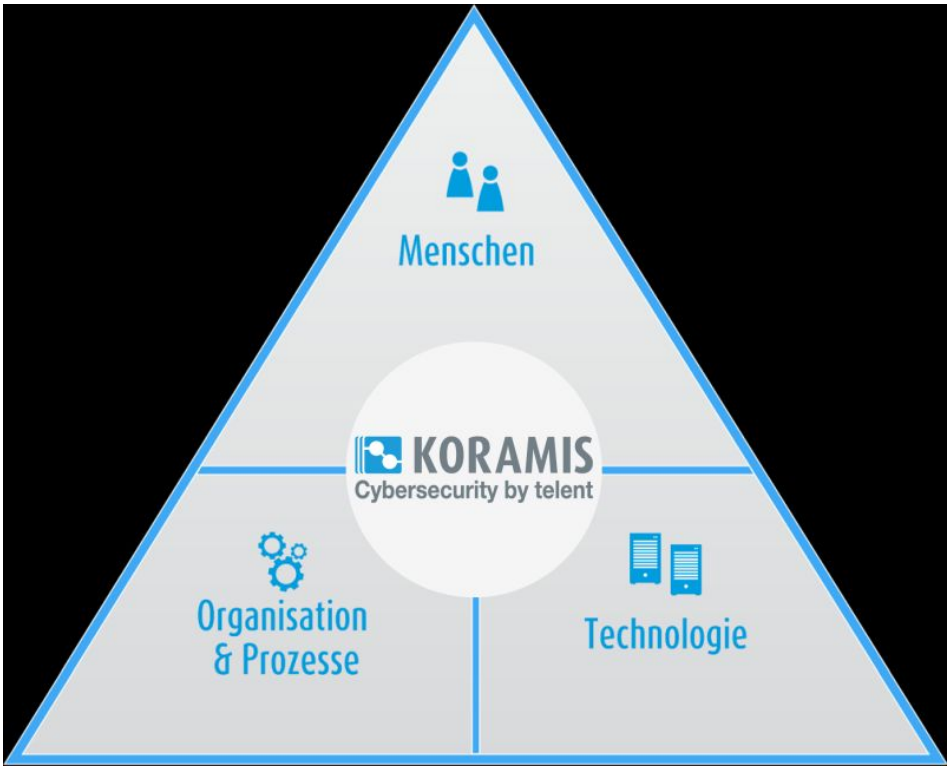
Cyber-Angriffe auf intelligente Transportsysteme abwehren

Artikel vom **14. April 2021**
Wissenstransfer

Intelligente Transportsysteme (ITS) und autonom fahrende Autos werden in Zukunft Teil unseres Alltags sein. Schon heute stehen sie im Fokus des öffentlichen Interesses und der politisch Handelnden – insbesondere der ÖPNV und bei den Bahnunternehmen. Da sie in die Kategorie der Kritischen Infrastrukturen (KRITIS) gehören, müssen sie besonders gegen Cyberangriffe geschützt werden. Ransomware-Angriffe, Datendiebstahl, Übernahme der Systeme und DDoS-Attacken sind bereits Realität.



Effiziente Strategie gegen Cyber-Angriffe für intelligente Transportsysteme (Bild: telent).

Neben diesen Cyber-Bedrohungen gehört es auch zur Lebenswirklichkeit, dass elektronische Verkehrssignale kompromittiert und missbraucht werden, um fragwürdige Botschaften zu verbreiten oder Videoüberwachungskameras und Anzeigesysteme mit Ransomware zu infizieren. Die Gefahren, die von den Attacken ausgehen, sind hoch und reichen von Personenschäden über Unfälle und Staus bis hin zu wirtschaftlichen Verlusten privater und öffentlicher Verkehrsbetriebe. Das Sicherheitsgesetz 2.0 trägt diesem Risiko Rechnung und verpflichtet auch Verkehrsbetriebe mit gezielten gesetzlichen Anforderungen, dieses Risiko zu minimieren. Um die damit einhergehenden Herausforderungen zu meistern, brauchen gerade mittelständische Unternehmen einen kompetenten strategischen Cybersecurity-Partner wie den Systemintegrator telent. Dessen Sicherheitsspezialisten bieten eine kostengünstige und zukunftsorientierte Strategie. Der große Vorteil: Der Dienstleister kümmert sich um IT-Services wie Netzwerkdienste, Monitoring oder Security und entlastet Kunden, die dafür oft nicht über die notwendigen Ressourcen und Spezialisten verfügen. Die Experten von telent, die unter der Marke »KORAMIS - Cybersecurity by telent« Sicherheitsaktivitäten bündeln, decken von der Schwachstellenanalyse über die Netzwerkplanung bis hin zur Umsetzung von Managed-Security-Konzepten alle Aspekte ab. Managed Security Support Services schützen traditionelle IT- und Betriebsbereiche. Schulungen und Sensibilisierungskampagnen ergänzen die Maßnahmen, die sich an die organisatorische Sicherheit und die Betriebsprozesse richten.

Hersteller aus dieser Kategorie
