IT/OT-Verkehrsinfrastruktur gegen Cyberangriffe schützen

Artikel vom **14. Juni 2023**
IT

Der Aufbau eines effektiven SOCs ist ressourcen- und zeitaufwendig. Daher entscheiden sich zahlreiche Unternehmen dies als Dienstleistung an einen Anbieter von Managed Security Services zu vergeben (Bild: telent).

Betreiber kritischer Transport- und Verkehrsinfrastrukturen drohen Cyberangriffe auf Seiten der IT und der OT (Operational Technology). Greifen Hacker IT-Systeme an, um etwa Mobilitätsdienste oder Ticketverkäufe zu stören, kann das hohe wirtschaftliche Schäden verursachen. Noch erheblicher ist das Risikopotenzial, wenn sicherheitskritische Komponenten der OT ins Visier geraten. Ein Angriff auf die Betriebstechnologie könnte sich physisch auswirken bis hin zur Beeinträchtigung der Fahrgastsicherheit. Je digitaler der Personen- und Güternahverkehr wird, etwa durch digitale Stellwerke, desto unerlässlicher wird es, alle Systeme gegen Cyberrisiken bestmöglich zu schützen – wie es telent mit seinem »Security Operation Center« (SOC) als externe Dienstleistung anbietet.

Modulares SOC

Das SOC bündelt bewährte Prozesse, technische Tools und Cybersecurity-Know-how. Wie jedes modular aufgebaute SOC basiert es auf einem breiten Spektrum an Managed

Services, mit denen Bahnunternehmen auch die seit 1. Mai 2023 für KRITIS-Betreiber verschärften Anforderungen des IT-Sicherheitsgesetzes 2.0 erfüllen. Die Softwaremodule sind aber nur die Grundlage. Der Mehrwert für die Kunden entsteht durch das Spezialwissen des telent-Teams. Es besitzt ein tiefes Verständnis der OT-Infrastrukturen und ihrer Automatisierungs-, Prozess- und Netzleittechnik, über die telent durch die langjährige Betreuung von Kommunikations- und Datennetzen in KRITIS-Umgebungen, insbesondere im Transportsektor, verfügt. Dieses Wissen kombinieren Cybersecurity-Analysten zu einer ganzheitlichen Betrachtung, die ein professionelles Risikomanagement mit einem 360-Grad-Blick auf die komplette IT- und OT-Landschaft gewährleistet. Die Experten überwachen kontinuierlich die Netzwerke, suchen aktiv nach Bedrohungen, entfernen diese oder geben konkrete Handlungsempfehlungen. Der Vorteil des ganzheitlich ausgerichteten SOCs: Unternehmen schützen Angriffsflächen auf beiden Seiten – der IT und der OT.

Hersteller aus dieser Kategorie