NIS-2 fordert mehr Cyber-Schutz für Verkehrsinfrastruktur

Artikel vom **18. April 2024**
Betriebs- und Verkehrsmanagement

Bei SOC-as-a-Service unterstützen externe Experten Unternehmen dabei, sich gegen Cyberangriffe zu schützen (Bild: Adobe Stock/telent).

NIS-2 stellt Betreiber von Transport- und Verkehrsinfrastrukturen vor neue Herausforderungen. Wenn die europäische Richtlinie ab Oktober 2024 in Deutschland nationales Recht wird, gilt jedes Unternehmen aus dem Verkehrssektor mit mehr als 50 Beschäftigten und einem Jahresumsatz von mehr als 10 Millionen Euro als »wesentlich« oder »wichtig«. Damit unterliegt es besonders hohen Cybersecurity-Anforderungen und Meldepflichten.

Security Operations Center von telent

Womit fangen ÖPNV-Betreiber nun am besten an, um widerstandsfähiger gegen Cyberangriffe zu werden? Dreh- und Angelpunkt ist die Sicherheit der vernetzten Systeme und Betriebsmittel. Wertvolle Unterstützung leistet dabei telent. Der Anbieter maßgeschneiderter Technologielösungen und Services, der seit Jahrzehnten Kommunikations- und Datennetzen in KRITIS-Umgebungen – insbesondere im Transportsektor – betreut, kennt die OT-Infrastrukturen und ihre Automatisierungs-, Prozess- und Netzleittechnik bis ins Detail. Hinzu kommt die Kompetenz des

Cybersecurity-Teams von telent, das sein Know-how mit technischen Tools und bewährten Prozessen in einem eigenen Security Operations Center (SOC) bündelt. Das SOC bietet ein breites Spektrum an Managed Services. Diese können Unternehmen individuell nach Bedarf auswählen, um die Sicherheit ihrer IT/OT-Infrastrukturen zu steigern oder einzelne NIS-2-Forderungen, etwa ein Schwachstellenmanagement oder den Einsatz von Verschlüsselungstechnologien, abzudecken. Als externe Dienstleistung überwacht das SOC-Team auch die kompletten Netzwerke seiner Kunden, sucht aktiv nach Bedrohungen, entfernt diese oder gibt konkrete Handlungsempfehlungen. Angesichts der Risikolage und der Summe der Maßnahmen, die im Rahmen der NIS-2-Umsetzung relevant werden, ist es keine Option, länger abzuwarten. Je eher Unternehmen handeln, desto sicherer erfüllen sie gesetzlichen Pflichten rechtzeitig und desto schneller schützen sie sich effektiv vor Cyber-Bedrohungen.

Anmerkung der Redaktion:

Die NIS-2-Richtlinie (The Network and Information Security (NIS) Directive) wurde am 27. Dezember 2022 im EU-Amtsblatt veröffentlicht und ist am 16. Januar 2023 in Kraft getreten. Sie regelt die Cyber- und Informationssicherheit von Unternehmen und Institutionen.

Hersteller aus dieser Kategorie
