- Lange Lebensdauer – Eisenbahnsysteme können über 25 Jahre lang verwendet werden. So muss sichergestellt sein, dass die im System eingesetzten Sicherheitstechniken noch in 25 Jahren funktionieren. Es ist unmöglich vorherzusagen, wie die Cybersicherheit in ferner Zukunft aussehen wird, aber der Lösungsansatz muss beweglich bleiben.
- Sicherheitsauswirkungen – Cybersicherheitslösungen erfordern häufig aktive Eingriffe in das Netzwerk, um auftauchende Bedrohungen zu bekämpfen. Ein solcher Eingriff kann sich auf bestehende Sicherheitsmechanismen auswirken und sollte im Rahmen der Sicherheitsbetrachtungen bewertet werden.
- Bahnkompatibilität – Wirksame Sicherheitslösungen im Bahnbereich sollten die „Eisenbahnersprache" verstehen und die Möglichkeit bieten, diese vor Bedrohungen zu schützen. Lösungen aus dem IT-Bereich oder anderen Branchen können mit Eisenbahnprotokollen und -systemen inkompatibel und deshalb nur von begrenztem Wert sein. Daher muss der Schutzumfang der Bahntechnologien genau verstanden werden.

3 CylusOne für Signalsysteme

Cylus hat seine Sicherheitslösung CylusOne auf die besonderen Bedürfnisse der Bahnbranche abgestimmt. CylusOne überwacht die Sicherheitsrisiken eines Netzwerks und schützt durch Sichtbarkeit der wichtigsten Cybersicherheitselemente des Systems vor Bedrohungen.

3.1 Sichtbarkeit des Eisenbahnsystems

CylusOne bietet in Echtzeit eine vollständige Sicht auf das gesamte Netzwerk mit alle Ebenen abdeckenden Detailinformationen – von der Netzwerktopologie bis hin zu den einzelnen Anlagenschichten, einschließlich streckenseitiger Anlagen, Stellwerke, Management-Arbeitsstationen usw. Durch diesen Detaileinblick in das Netzwerk werden blinde Stellen eliminiert, Verbindungen zwischen Anlagen aufgedeckt und redundante Verbindungen klassifiziert.
CylusOne ermittelt den Cybersicherheitsstatus von Netzwerken in Echtzeit, indem passiv erfasste Daten ohne vorherige Informationen über das Netzwerk mit der Deep Packet Inspection analysiert werden.

3.2 Bedrohungserkennung

Um Cyberangriffen vorzubeugen, analysiert CylusOne das Netzwerk als Ganzes und deckt Fälle auf, in denen die Sicherheit verletzt und die Verfügbarkeit von Diensten beeinträchtigt wird. Durch die laufende Sicherheitsüberwachung aller Signalsysteme, einschließlich ERTMS (European Rail Traffic Management System), CBTC (Communication-Based Train Control), proprietärer und alter Systeme sowie der Betriebsleitsysteme können unsere proprietären Algorithmen Netzwerkanomalien sofort erkennen.
CylusOne wird durch Feeds ergänzt, die die neuesten Erkenntnisse des Cylus-Forschungsteams im Bereich Eisenbahncybersicherheit repräsentieren. Dadurch kann CylusOne neu entdeckte Sicherheitslücken und Bedrohungen im Bereich der Signaltechnik erkennen und Cyberangriffe schnell und genau identifizieren.

3.3 Reaktion auf Cybersicherheitsvorfälle

Echtzeitalarme für sicherheitsrelevante Ereignisse werden durch kontextbezogene detaillierte Ereignisinformationen ergänzt, z. B. durch die Grundursache und die betroffenen Anlagen. Die Ereigniswarnungen mit Einblick in das System erlauben eine schnelle Analyse und ermöglichen rechtzeitige Reaktionen auf Bedrohungen, um Risiken zu verringern oder Angriffe zu isolieren. Die Anweisungen zur Schadensbegrenzung können vollständig mit den gültigen Eisenbahnrichtlinien harmonisiert werden. ■

3.2 Threat detection

To proactively detect cyber-attacks, CylusOne views the network as a whole, uncovering cases where safety is breached, and service availability is affected. The ongoing security monitoring of all signaling systems, including ERTMS, CBTC, proprietary and legacy systems, as well as Traffic Management Systems (TMS), enables Cylus' proprietary algorithms to immediately detect anomalies on the network.
CylusOne is augmented with feeds displaying the latest discoveries by Cylus' rail cybersecurity research team. As a result, it can detect newly found rail signaling vulnerabilities and threats, providing accurate and up-to-date identification of cyber-attacks.

3.3 Incident response

Real-time alerts for security events are supplemented with contextual, detailed information about the incident, such as the root cause and affected assets. These actionable insights, attached to the event alerts lead to swift analysis of events, enabling a timely response to the threat in order to remediate the risk or contain the attack. The mitigation instructions can also be fully customized to meet existing railway policies. ■

AUTOR | AUTHOR

Miki Shifman
Cief Technical Officer
Cylus
Anschrift / *Address*: 23 Yehuda HaLevi St., IL-Tel Aviv
E-Mail: miki@cylus.com