Rail Server

Studiengang: MAS Cyber Security

Die Cyberangriffe auf Industriesysteme nehmen stetig zu. Die SBB möchten ihre Fahrzeugsysteme besser schützen. Eine virtuelle Firewall, auf einer modernen Server Plattform, sorgt für die sichere Bahn von morgen.

Ausgangslage

Die Medien berichten vermehrt über Cyber- und Ransomware Angriffe. Industriesysteme von kritischen Infrastrukturen bilden da keine Ausnahme. Die zunehmende Vernetzung von Systemen lässt die Angriffsfläche wachsen und die Transparenz im eigenen Netz wird eine immer grössere Herausforderung.
Im Zug verbaute Hardware muss Aspekte der Norm EN 50155 erfüllen, damit sie als bahntauglich gilt. Beispielsweise werden die Geräte nachweislich auf extreme Betriebstemperaturbereiche oder elektromagnetische Verträglichkeit (EMV) geprüft.
Diese Voraussetzungen schränken den Markt für Lieferanten ein.
Die Schweizerischen Bundesbahnen (SBB) investieren daher in die IT-Sicherheit. Die als bahntauglich geltenden Firewalls erfüllen aber die Anforderungen an eine moderne Firewall nicht.
Durch die Möglichkeit, Systeme zu virtualisieren, werden Ablösungen von Altsystemen vereinfacht und der Zugang für Systemlieferanten anderer Branchen ermöglicht. Zukünftig bildet eine marktführende und virtuelle Firewall das Herzstück der IT-Sicherheit in den Zügen der SBB.

Zielsetzung

Mit der Master-Thesis wird die aktuelle Lage der IT-Sicherheit untersucht und dient als Grundlage für eine Risikobeurteilung. Die momentane Situation weist Schwachstellen und potenzielle Angriffspunkte auf.
Mitarbeitende müssen auch mit den zukünftigen Sicherheitsvorkehrungen ihre Arbeiten am System ausführen können. Daher ist es wichtig, die dafür unterschiedlichen Rollen zu kennen, damit ihnen die nötigen Berechtigungen gewährt werden.
Diese Informationen helfen, das Netzwerk sinnvoll und bedarfsgerecht zu segmentieren.
Ein weiteres Ziel der SBB ist, Fahrzeugsysteme in das Security Operation Center (SOC) einzugliedern. Mögliche Angriffsszenarien sind in Anwendungsfällen erfasst und werden anschliessend im SOC abgebildet. Das Erstellen der technischen Datenverbindung zwischen dem Zug und dem SOC ermöglichte die erste Umsetzung eines Anwendungsfalls.

Lösungsansatz

Die SBB beschaffen eine Server Plattform, welche die Anforderungen an die Bahntauglichkeit erfüllt.
Ein Linux System bildet die Basis und ermöglicht den Betrieb von virtuellen Maschinen oder Containern.
Die Server Plattform verfügt über neuste Mobilfunktechnologie. Fahrzeugsysteme können so über die Firewall eine Verbindung in das Internet oder Firmennetz herstellen.

Schlussbetrachtung

Der Rail Server ermöglicht den Einsatz modernster Technologien. Neue Applikationen können dank Container-Lösungen zukünftig rascher und günstiger auf den Zug gebracht werden. Bis anhin musste dedizierte Hardware für den Betrieb einer Applikation verbaut werden.
Der Vernetzung von Systemen im Zug sowie zwischen den Zügen und der Landseite kann mit gutem Gewissen vorangetrieben werden, um den heutigen und zukünftigen Anforderungen gerecht zu werden.
Dank einer modernen Firewall müssen die SBB dabei keinen Kompromiss bei der IT-Sicherheit eingehen.

Sascha Berger