OT Security mit Schwerpunkt auf Forensik im Bahnumfeld

Studiengang: MAS Cyber Security

Die SBB AG (Schweizerische Bundesbahn) hat in ihren Divisionen (z.B. Infrastruktur) unterschiedliche operative Technologien (Operational Technology) im Einsatz. Nun wird, nicht zuletzt auch durch die Cyberkriminalität, der Bereich OT-Security für die SBB AG zunehmend wichtiger, da sich die Cyberbedrohungen erhöht haben. Zudem ist es auch eine Strategie von der SBB Konzernsicherheit, OT-Security und OT-Forensik anzugehen und Prozesse zu etablieren.

Ausgangslage / Problemstellung

Die Betreiberorganisationen der SBB AG haben im Bereich OT und in Bezug auf «Safety & Security sowie Verfügbarkeit» entsprechende Herausforderungen (z.B. forensische Analyse bei einem Vorfall) zu bewerkstelligen. Insbesondere wird die OT-Forensik unterschiedlich wahrgenommen, da IT-Forensik nicht gleich OT-Forensik bedeuten muss. Ein Punkt ist, dass je nach OT-Umgebung diverse Logs und Protokolle existieren, welche unterschiedlichen Informationsgehalt für die IT-Forensik liefern könnten. Es sind zudem keine Prozesse für Datenerhebungen seitens IT-Forensik in Bezug auf OT-Systeme vorhanden. Ob das IT-Forensik Framework in Bezug auf Sammlung, Untersuchung, Analyse und Berichterstattung angewendet werden kann, ist unklar. Auch die Zusammenarbeit zwischen IT-Forensik und den OT-Abteilungen ist nur beschränkt oder kaum vorhanden und muss aufgebaut werden.

Ziele / Motivation

Basierend auf der Ausgangslage wurden unterschiedliche Ziele und Anforderungen abgeleitet, welche in Business Value und Business Outcome definiert sind. Zudem besteht ein grosses Interesse seitens Themensponsor, dass ein OT-Forensik Konzept und Prozess aufgebaut wird. Die Ziele der Business Values sind, die Sicherheit und Resilienz zu erhöhen, die bestehenden Ressourcen zu optimieren sowie Compliance und Regulierung in Bezug auf OT-Forensik zu dokumentieren. Auch die Business Outcomes, wie die Entwicklung eines OT-Forensik Konzepts, eine verbesserte Zusammenarbeit und Kommunikation zwischen den OT relevanten Stakeholdern sowie die Durchführung eines Proof of Concepts (PoC), um die Anwendbarkeit und Effektivität des entwickelten OT-Forensik Prozesses zu verifizieren, sind abgeleitete Ziele.

Vorgehen / Konzept

Die Vorgehensweise und Datenerhebung basieren einerseits auf Interviews von unterschiedlichen OT-Fachpersonen sowie auf Internet- und Literaturrecherchen, um das Thema zu vertiefen und um wertvolles Wissen für das Konzept zu erhalten. Die Bahnsteuerung musste in Zusammenhang mit ETCS (European Train Control System) und dem System Iltis (Integrales Leit- und Informationssystem für die Bahn) verstanden werden. Eine Recherche über die Bedrohungslage zu OT/ICS in Bezug auf Bahninfrastruktur wurde ebenfalls durchgeführt. Als weitere Quellen wurden Vorgaben und Standards z.B. vom BAV (Bundesamt für Verkehr) oder NIST (National Institute of Standards and Technology) konsultiert. Die Standards bzw. Normen wie IEC 62443 (OT/ICS) und CLC/TS 50701 (Cybersecurity für Railway Application) sind essenzielle Bestandteile für OT. Nicht zuletzt wurde auch die Anwendbarkeit von der IT-Forensik auf OT-Forensik dokumentiert. Basierend auf diesem Vorgehen wurde ein Konzept und ein PoC erarbeitet, in welchen die Rollen definiert, ein OT-Forensik Prozess modelliert sowie Anforderungen an OT-Forensik dokumentiert wurden.

Rajeevan Rabeendran

Ergebnisse

Durch den PoC wurden alle Anforderungen und Ziele erfolgreich verifiziert. Insbesondere der OT-Forensik Prozess und das OT-Forensik Vorgehensmodell wurden geprüft und bieten für die IT-Forensik eine sehr gute Basis. Auch für die unterschiedlichen OT-Betreiberorganisationen bietet es ein Konzept, um die Zusammenarbeit zwischen OT-Forensik und den OT-Fachexperten sicherzustellen.

Ausblick

Das Ziel der Master Thesis, dass ein OT-Forensik Konzept erstellt wird, wurde intern in der SBB kommuniziert. Dies hat intern „Früchte“ getragen und soll in den verschiedenen OT-Bereichen eingesetzt werden. Die Reise mit OT-Forensik geht somit weiter und fördert nun die Zusammenarbeit der unterschiedlichen Stellen gewaltig.