Quelle:https://www.zevrail.de/artikel/ot-security-harmonisierter-bedrohungskatalog-am-beispiel-schienenfahrzeuge

2024 (Jahrgang 148) / Ausgabe 03 / Sprache: Deutsch

OT-Security – Harmonisierter Bedrohungskatalog am Beispiel Schienenfahrzeuge

Autoren: Dipl. Ing. Friedrich Feistle, Dipl. Ing. Martin Kursawe, Dr. Ing. Daniel Lüdicke, Dipl. Ing. Jürgen Sept

Zusammenfassung

Das Themengebiet „Cybersecurity“ gewinnt im Kontext der zunehmenden Digitalisierung im Eisenbahnsektor an immer größerer Bedeutung. Vor diesem Hintergrund sind alle Stakeholder in dieser Domäne daran interessiert eine Einschätzung über die IT- / OT- Security zu erhalten. Unterstützung liefern dabei die Industrienorm IEC 62443 [1] und die darauf aufbauende Richtlinie für Bahnen TS 50701 [2]. Bei beiden erfolgt der Nachweis der OT-Security bevorzugt über eine Risikoanalyse auf Basis der zu erwartenden Bedrohungen. Weder die IEC 62443 noch die TS 50701 liefert hierzu eine verbindliche Vorgabe in Form eines umfassenden Bedrohungskatalogs. Dadurch entsteht ein Interpretationsspielraum, der dazu führt, dass Risikoanalysen über mehrere Betrachtungsobjekte hinweg nur mühsam und aufwendig erfolgen können. Ein Vergleich von Schienenfahrzeugen unterschiedlicher Hersteller oder Baureihen ist damit nicht möglich. Die Autoren haben deshalb eine Methode entwickelt, um die bekannten Bedrohungslisten in einen anwendungsspezifisch konsolidierten Bedrohungskatalog zu überführen. Im folgenden Artikel wird dieser Katalog zusammen mit den bei der Erarbeitung gewonnenen Erkenntnissen vorgestellt.

1 Bedrohungen

Ausgangspunkt der Risikoanalyse für Cybersecurity sind die Bedrohungen (Threats), weshalb diese Analysen auch „Threat and Risk-Analysis“ genannt werden. Um eine möglichst vollständige, konsistente und für die Praxis geeignete Liste aller für ein Schienenfahrzeug relevanten Bedrohungen zu erhalten, wurden aktuelle Bedrohungslisten für OT-Systeme (OT=Operational Technology) detailliert analysiert.

1.1 Unterschiedliche Bedrohungslisten

Die einschlägigen Cybersecurity-Regelwerke für den Bahnbereich in Europa sind IEC 62443 [1] und TS 50701 [2]. Diese fordern als zentrales Element Risikoanalysen, allerdings fehlt dafür derzeit die Grundlage in Form konkreter Bedrohungslisten. TS 50701 verweist hierzu auf Bibliotheken wie dem ENISA Threat Landscape Yearly Report [3] oder der NIST 800-30 [4]. Für den Bahnsektor angepasste Bedrohungslisten stehen bislang nur vereinzelt zur Verfügung. Infolgedessen muss jeweils individuell für jeden Anwendungsfall eine Bedrohungsliste auf Basis sehr allgemeingültiger Vorgaben erstellt werden.
In den zuvor genannten Regelwerken findet man zwei unterschiedliche Formen von Bedrohungslisten:

1. Bedrohungslisten mit Bedrohungen aus Betreibersicht, welche die Abläufe auf IT-Ebene global beschreiben;
2. Bedrohungslisten, die detaillierte Bedrohungen mit gefährlichen Wirkmechanismen auf IT-Ebene enthalten (siehe MITRE ICS-Matrix [5] und CAPEC-Liste [6]).

Nachdem der Schwerpunkt dieser Arbeit auf der gemeinsamen Risiko-Ermittlung durch Stakeholder aller Fachbereiche abzielt, werden im Folgenden die IT-spezifischen Bedrohungslisten ausgeblendet und nur noch die Bedrohungslisten auf Betreiber-Ebene herangezogen.

1.2 Bekannte Bedrohungslisten

Die meisten Bedrohungslisten auf Betreiber-Ebene beziehen sich generell auf industrielle Automatisierungstechnik. Nur die Bedrohungslisten der ENISA „RAILWAY CYBERSECURITY Good practices 2021“ [7] und der Shift2Rail X2Rail-1/WP8 [8] haben den Fokus auf den Eisenbahnsektor.
Die Bedrohungen lassen sich grob in zwei Kategorien unterteilen:

a) Intentional Threats (vorsätzliche Bedrohungen)
b) Unintentional Threats (unbeabsichtigte Bedrohungen)

Bild 1 zeigt die sehr unterschiedlichen Schwerpunkte der einzelnen Bedrohungslisten.
Während in der NIST 800-30 und der Bedrohungsliste der Shift2Rail X2Rail-1/WP8 die vorsätzlichen Bedrohungen deutlich überwiegen, ist in der ENISA RM Toolbox 2023 [9] genau das Gegenteil der Fall. Unterschiede zwischen ISO 27005 [10] und Shift2Rail X2Rail-1/WP8 ergeben sich hauptsächlich im IT-Bereich. Shift2Rail X2Rail-1/WP8 legt den Fokus auf die Bedrohungsschwerpunkte Malware, Denial of Service und Man in the Middle, während die unbeabsichtigten Bedrohungen nur in geringem Umfang enthalten sind.

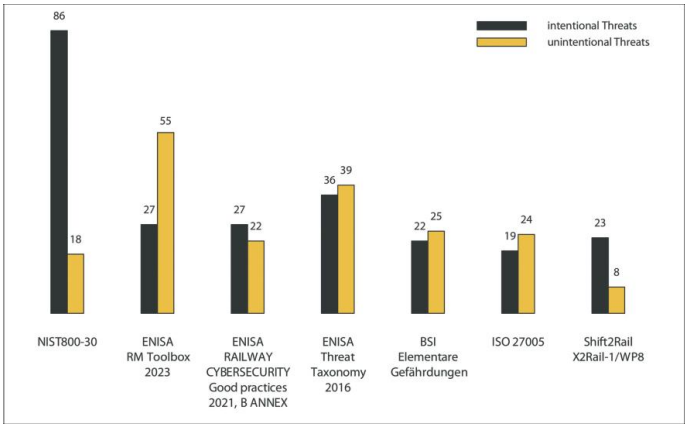

Bild 1: Aufteilung Bedrohungslisten in intentional / unintentional Threats

2 Entwicklung eines harmonisierten Bedrohungskataloges für Schienenfahrzeuge

Die heute existierenden Bedrohungslisten haben unterschiedliche Schwerpunkte und keiner deckt vollständig die gesamte Breite der bekannten Bedrohungen ab. Wird eine dieser Bedrohungslisten allein als Basis für eine Risikoanalyse verwendet, besteht die Gefahr, dass wesentliche Bedrohungen in der Analyse fehlen und damit die Risikoanalyse nicht vollständig ist.
Aus diesem Grund entstand der Wunsch, einen umfassenden Bedrohungskatalog zu entwickeln, der auch – durch Beschränkung auf das Notwendige – gut handhabbar ist. Aus Sicht der OT-Security stehen die vorsätzlichen Bedrohungen im Vordergrund. Die unbeabsichtigten Bedrohungen, die in o. g. Bedrohungslisten enthalten sind, werden bei der in diesem Artikel beschriebenen Arbeit nicht weiter betrachtet, da sie schon in diversen anderen Bereichen (z. B. Safety) umfassend behandelt werden.
Der harmonisierte Bedrohungskatalog wurde in fünf Schritten erarbeitet (Bild 2). Die gewählte Art der Sortierung nach Auswirkungen ist eine Alternative zu den aktuell gängigen Sortierverfahren nach Bedrohungstypen oder Angriffsphasen, die im Folgenden kurz erläutert werden.

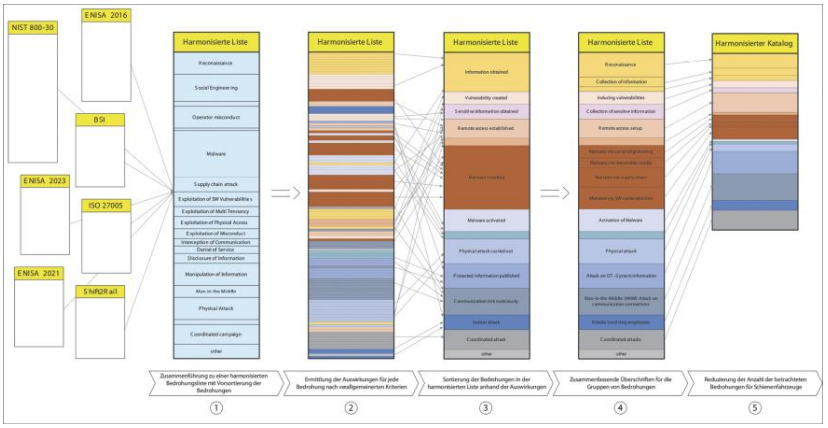

Bild 2: Entwicklung eines Bedrohungskataloges für Schienenfahrzeuge in 5 Schritten

2.1 Sortierverfahren

2.1.1 Sortierung nach Bedrohungstypen

Als Beispiel für eine Sortierung nach Bedrohungstypen ist die sogenannte „STRIDE“-Struktur von Microsoft bekannt. Dabei stehen die Buchstaben für folgende Bedrohungstypen:

- S=Spoofing Identity (vortäuschen einer anderen Identität)
- T=Tampering (böswillige Veränderung einer Information)
- R=Repudiation (Verhinderung der Rückverfolgbarkeit von Änderungen)
- I=Information Disclosure (Offenlegung vertraulicher Daten)
- D=Denial of Service (Überlastung eines Systems durch Überflutung mit Anfragen)
- E=Elevation of rights (sich Rechte verschaffen, die einem nicht zustehen)

Aufgrund der geringen Anzahl an Kategorien und eines gewissen Ungleichgewichts in der Anzahl der Einträge in den einzelnen Kategorien erscheint diese Strukturierung bezüglich der Übersichtlichkeit bei der späteren Abarbeitung nicht optimal.

2.1.2 Sortierung nach Angriffsphasen

Die NIST 800-30 sortiert nach Angriffsphasen und bildet eine sogenannte „Kill Chain“ nach, die einen möglichen Ablauf eines Cyber-Angriffs beginnend mit der ersten Informationssammlung bis hin zur finalen

Durchführung des Angriffs beschreibt.
Eine direkte Übernahme der NIST 800-30- Struktur birgt ebenfalls Nachteile bezüglich der Übersichtlichkeit, weil aufgrund der ablauforientierten Struktur einige Themen – wie z.B. Malware – auf mehrere Phasen verteilt sind.

2.1.3 Sortierung nach Auswirkungen

Um die Sortierung möglichst übersichtlich zu gestalten, entstand die Idee, die Bedrohungen anhand ihrer Auswirkungen zu sortieren. Diese Auswirkungen umschreiben teilweise Zwischenschritte im Verlauf eines Angriffs, die in vielen Fällen noch keinen von außen feststellbarem Schaden am OT-System verursachen.

2.2 Beschreibung der Arbeitsschritte zum harmonisierten Bedrohungskatalog im Einzelnen

2.2.1 Schritt 1: Zusammenführung zu einer harmonisierten Bedrohungs-liste mit Vorsortierung der Bedrohungen

Für die Zusammenführung mussten gleichartige Bedrohungen der einzelnen Listen erfasst, analysiert und harmonisiert werden. Dafür wurden die über 200 einzelnen Bedrohungen zunächst temporär in Kategorien unterteilt, um eine anschließende Zuordnung gleichartiger Bedrohungen zu erleichtern. Dies war notwendig, da die vorsätzlichen Bedrohungen in den meisten bekannten Listen – mit Ausnahme der NIST 800-30 – im Wesentlichen als monolithischer Block ohne weitere Unterteilung aufgelistet sind.
Die temporären Kategorien wurden so gewählt, dass ihnen jeweils eine ähnliche Anzahl von einzelnen Bedrohungen zugeordnet werden konnte.
Nachdem diese Kategorien feststanden, wurden die einzelnen Bedrohungen in diese Kategorien eingeordnet. Tabelle 1 zeigt in den rechten sieben Spalten, wie viele Bedrohungen jeweils den einzelnen Kategorien zugewiesen wurden. Die Spalte „harmonisiert“ zeigt die Anzahl der unabhängigen Bedrohungen aus den ursprünglichen Listen.
Danach wurden gleiche oder ähnliche Bedrohungen aus den einzelnen Listen zusammengefasst und ihnen jeweils eine harmonisierte Bezeichnung zugeordnet. Diese konsolidierten Bedrohungen wurden abschließend für die weitere Bearbeitung durchnummeriert um die Nachvollziehbarkeit / Traceability zu gewährleisten. Durch den Konsolidierungsschritt wurden die über 200 Bedrohungen auf nun 125 konsolidierte Bedrohungen reduziert.

Kapitel	harmonisiert	NIST 800-30	ENISA 2023	ENISA 2021	ENISA 2016	BSI	ISO 27005	Shift2 Rail
Reconaissance	9	6	3	2	2	3	3	3
Social Engineering	11	10	2	4	4	2	1	1
Elevating Authorisation	2	–	2	1	1	1	1	1
Operator misconduct	9	1	2	4	5	3	3	4
Brute force	1	1	-	1	1	–	–	–
Malware	19	18	1	1	2	1	–	1
Supply Chain Attack – Tampering of HW or SW	6	4	2	1	1	1	3	3
Exploitation of Software Vulnerabilities	7	6	–	–	1	–	–	–
Exploitation of Multi Tenancy or Cloud Environment	4	4	–	–	–	–	–	–
Exploitation by Physical Access	5	3	–	1	1	1	1	2
Exploitation of Misconfiguration	4	3	1	1	–	1	–	–
Interception of Communication	3	3	–	–	2	–	–	–
Denial of Service	3	3	1	1	1	1	–	1
Disclosure of information	3	1	2	1	1	–	2	2
Manipulation of information	6	5	2	2	3	2	1	2
Man in the middle	8	5	2	1	2	1	–	–
Physical Attack	9	4	2	2	4	3	–	–
Theft	2	1	2	1	1	1	2	1
Coordinated campaign	8	8	1	1	1	–	–	–
other	6	–	2	2	3	1	2	2
	125	86	27	27	36	22	19	23

Tabelle 1: Anzahl der Bedrohungen in den einzelnen Kategorien in der harmonisierten Liste und den bekannten Bedrohungslisten

2.2.2 Schritt 2: Ermittlung der Auswirkungen für jede Bedrohung nach verallgemeinerten Kriterien

Für die weitere Sortierung wurde zunächst für die zusammengefassten 125 Bedrohungen die Auswirkung jeder Bedrohung in einer verallgemeinerten Form ermittelt.

- Information obtained (Information beschafft)
- Vulnerability created (Schwachstelle geschaffen)
- Sensitive Information obtained (kritische Informationen beschafft)
- Remote access established (Fernzugriff eingerichtet)
- Physical access established (Physischer Zugang zum OT-System hergestellt)
- Access to communication link established (Kommunikationsverbindung gekapert)
- Malware installed (Schadsoftware installiert)
- Malware activated (Schadsoftware aktiviert)
- OT component unavailable respectively its function disrupted (Unverfügbarkeit der Komponente oder einer Funktion erlangt)
- Physical attack carried out (physischer Angriff auf Komponenten des OT-Systems ausgeführt)
- Protected information published (geschützte Information veröffentlicht)
- Communication link maliciously manipulated (Kommunikationsverbindung böswillig manipuliert)
- Insider attack (Angriff durch einen OT-System-Mitarbeiter erfolgt)
- Coordinated attack (mehrstufiger Angriff an verschiedenen Stellen ausgeführt)
- other (noch nicht abschließend zuordenbare Bedrohungen)

2.2.3 Schritt 3: Sortierung der Bedrohungen in der harmonisierten Liste anhand der Auswirkungen

Im nächsten Schritt wurden die 125 Bedrohungen anhand der zugeordneten Auswirkungen neu angeordnet. Gemäß der im Schritt 2 definierten 15 verallgemeinerten Auswirkungen ergaben sich dabei 15 Gruppen mit unterschiedlicher Anzahl an Bedrohungen.

2.2.4 Schritt 4: Zusammenfassende Überschriften für die Gruppen von Bedrohungen

In diesem Schritt erhielten die 15 Gruppen Überschriften, die die in der jeweiligen Gruppe enthaltenen Bedrohungen geeignet zusammenfassen. In den Gruppen mit den Auswirkungen „Information obtained“, „Vulnerability created“ und „Malware installed“ war dabei aufgrund der Vielzahl der Einträge eine zusätzliche Untergliederung notwendig, so dass die Gesamtzahl der Gruppen auf 19 stieg.
Zur weiteren Strukturierung sind diese Gruppen in vier Kapiteln zusammengefasst, die den zentralen Phasen eines Angriffs entsprechen (Tabelle 2).
Die Anzahl der in den einzelnen Gruppen enthaltenen Bedrohungen ist jeweils in der zweiten Spalte angegeben.

Gruppen von Bedrohungen	Anzahl gesamt	es geht um folgende Bedrohung	Verallgemeinerte Auswirkung
Gathering information		**Informationsbeschaffung durch**	
Reconaissance	10	Aufklärung im Umfeld	Information obtained
Collection of information in a in Multi-tenancy environment (e.g. Cloud or Virtual Machine)	4	Ausnutzen von Schwachstellen in virtuellen Maschinen oder einer Cloud	Information obtained
Collection of information from OT-System portable devices	2	Zugriff auf portable Speichermedien von OT-Mitarbeitern	Information obtained
Gaining access		**Zugang schaffen durch**	
Inducing Vulnerabilities	5	Erzeugen von Schwachstellen	Vulnerability created
Collection of information from employees (Social Engineering)	6	Beeinflussung von OT-Mitarbeitern	sensitive information obtained
Remote Access setup	8	Einrichtung eines Remote Zugangs	remote access established
physical Intrusion into OT-System premises	3	körperliches Eindringen in die Systemumgebung	physical access established
Installing malicious capabilities via		**Installation bösartiger Funktionen über**	
Social Engineering	5	Einflussnahme auf OT-Mitarbeiter	Malware installed
Removable media	4	austauschbare Speichermedien	Malware installed
Supply chain	8	die Lieferkette	Malware installed
SW Vulnerabilities	9	Ausnutzen von SW Schwachstellen	Malware installed
Causing damage		**Schaden verursachen durch**	
Activation of Malware	9	Aktivierung von Schad-SW	Malware activated
Denial of Service Attack	3	Überflutung einer OT-Komponente mit Anfragen	OT component unavailable respectively its function disrupted
Physical attack	10	Körperlicher Angriff auf Komponenten des OT-Systems	physical attack carried out
Attack on OT-System information	10	Angriff auf vertrauliche Informationen	protected information published
Man-in-the-Middle (MitM) Attack on communication connections	11	Angriff durch Zwischenschalten in bestehende Kommunikations-verbindungen	communication link maliciously manipulated
Attacks involving employees	6	Angriffe unter Einbeziehung von OT -Mitarbeitern	Insider attack
Coordinated Attacks	8	mehrstufige Angriffe	Coordinated attack
other	4	noch nicht abschließend zuordenbare Bedrohungen	other
	125		

Tabelle 2: Finale Struktur der harmonisierten Bedrohungsliste

2.2.5 Schritt 5: Reduzierung der Anzahl der betrachteten Bedrohungen für Schienenfahrzeuge

Um eine effektive Durchführung der Risikoanalysen zu ermöglichen, wurden die 125 Einzelbedrohungen nun auf ihre Relevanz für die OT-Security von Schienenfahrzeugen geprüft.

Dabei wurde festgestellt, dass auf die Berücksichtigung einzelner Bedrohungen verzichtet werden kann, wenn man alle Bedrohungen gemäß nachfolgenden Kriterien bewertet:

„relevant“
Die Bedrohung ist für die finale Bedrohungsliste relevant

„nicht relevant“
Die Bedrohung ist für ein Schienenfahrzeug nicht relevant (z. B., weil dort keine personenbezogenen Daten verarbeitet werden)

„Spezialfall“
Die Bedrohung beschreibt einen Spezialfall, der in einer anderen – allgemeiner formulierten – Bedrohung bereits enthalten ist und bei dem diese Unterscheidung für ein Schienenfahrzeug nicht relevant ist (z. B. bei einer spezifischen Art von Malware)

„nicht OT Security“
Die Bedrohung beschreibt gehört nicht zum Bereich OT Security (z. B. Blockierung einer Funkdatenübertragung durch Störsender)

Bei diesem Prozess konnten 53 Positionen der 125 Bedrohungen aussortiert werden (Tabelle 3). Somit ist von der ursprünglichen umfangreichen Sammlung von über 200 Bedrohungen ein handhabbarer harmonisierter Katalog von 72 relevanten Bedrohungen entstanden.
Die Grafiken im folgenden Abschnitt geben einen Überblick über die in den vier Hauptkategorien erfassten Bedrohungen.

Gruppen von Bedrohungen	Anzahl gesamt	Anzahl reduziert	Begründung		
			nicht relevant	Spezialfall	nicht IT Security
Gathering information					
Reconaissance	10	6	–	1	3
"Collection of information in a in Multi-tenancy environment (e.g., Cloud or Virtual Machine)"	4	3	–	1	–
Collection of information from OT-System portable devices	2	2	–	–	–
Gaining access					
Inducing Vulnerabilities	5	3	2	–	–
Collection of information from employees (Social Engineering)	6	2	–	4	–
Remote Access setup	8	8	–	–	–
physical Intrusion into OT-System premises	3	1	–	2	–
Installing malicious capabilities					
Social Engineering	5	3	–	2	–
Removable media	4	1	–	3	–
Supply chain	8	1	1	6	–
SW Vulnerabilities	9	5	–	4	–
Causing damage					
Activation of Malware	9	1	–	8	–
Denial of Service Attack	3	1	–	2	–
Physical attack	10	3	–	7	–
Attack on OT-System information	10	9	1	–	–
Man-in-the-Middle (MitM) Attack on communication connections	11	11	–	–	–
Attacks involving employees	6	4	–	–	2
Coordinated Attacks	8	8	–	–	–
other	4	0	3	–	1
	125	72	7	40	6

Tabelle 3: Reduktion der harmonisierten Bedrohungsliste von 125 auf 72 Bedrohungen

3 Übersicht über den harmonisierten Bedrohungskatalog

In den vorhergehenden Kapiteln standen die Zusammenfassung und Sortierung der Bedrohungen im Vordergrund. In diesem Abschnitt wird ein komprimierter Überblick über die Art der einzelnen Bedrohungen aus dem harmonisierten Bedrohungskatalog gegeben.

3.1 Informationsbeschaffung (gathering information)

Für die gezielte Vorbereitung eines Angriffs wird ein Angreifer sich zunächst umfangreiche Informationen über das anzugreifende Objekt und sein Umfeld beschaffen. Ziel ist dabei die grundsätzliche Funktionsweise des Systems, Schnittstellen, Datenflüsse, organisatorische Abläufe und Schwachstellen in Erfahrung zu bringen (Bild 3).
Kennzeichnend für diese Vorarbeiten ist, dass sie vorwiegend ohne Eingriff in das OT-System erfolgen und somit nur wenige Spuren hinterlassen.
Zur Informationsbeschaffung gehört neben der Datensammlung von öffentlich verfügbaren Quellen (z. B. technischen Informationen aus dem Internet) vor allem das Mitlesen und die Analyse des Datenverkehrs an den Schnittstellen oder innerhalb des OT-Systems.
Eine weitere wertvolle Fundgrube zur Informationsbeschaffung ist die Auswertung von beschafften mobilen Datenträgern.
In modernen IT-Umgebungen mit virtuellen Maschinen oder bei Lösungen unter Einbeziehung von Cloudsystemen kommt außerdem der Beobachtung von benachbarten Prozessen unter Ausnutzung von

deren Schwachstellen eine wachsende Bedeutung zu.
Schließlich kann auch eine physische Beobachtung typischer Abläufe dem Angreifer wichtige Informationen über organisatorische Abläufe liefern.

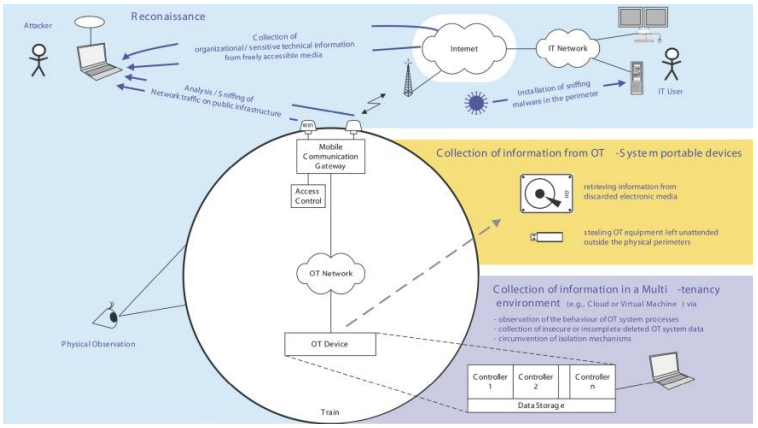

Bild 3: Typische Maßnahmen zur Informationsbeschaffung

3.2 Zugang verschaffen (Gaining access)

Sobald die notwendigen Informationen beschafft sind, versucht der Angreifer auf Basis des gewonnenen Wissens nun Wege zum Eindringen in das OT-System zu finden (Bild 4). Dabei geht er schrittweise vor und dringt immer tiefer in das System ein.
Im Mittelpunkt dieses Abschnitts steht ein Angreifer, der auf verschiedenen Wegen versucht, sich Zugang zu dem OT-System zu verschaffen.
Durch die Beeinflussung von OT-Mitarbeitern, die der Angreifer im ersten Abschnitt durch „Social Engineering“ ausgeforscht hat, versucht er an Passwörter, Zugangscodes etc. zu gelangen. Eine weitere Methode ist, die Zugangsdaten über verschiedene Methoden wie Bruteforce o. ä. zu erraten.
Erkannte Schwächen im OT-System wie Sicherheitslücken oder sogenannte Backdoors versucht der Angreifer auszunutzen.
Eine weitere Methode, die von Angreifern oft genutzt wird, ist die direkte oder indirekte Beeinflussung von OT-Mitarbeitern mit dem Ziel, gezielt Schwachstellen in dem OT-System zu erzeugen, beispielsweise durch Installation nicht zugelassener Software oder durch Ausnutzung von Informationen über Schwachstellen, die sie gezielt – durch Missbrauch von Analysewerkzeugen – herausgefunden haben.
Darüber hinaus wird der Angreifer selbst aktiv und erschleicht sich einen physischen Zugang zum OT-

System, um dort böswillige Veränderungen vorzunehmen.

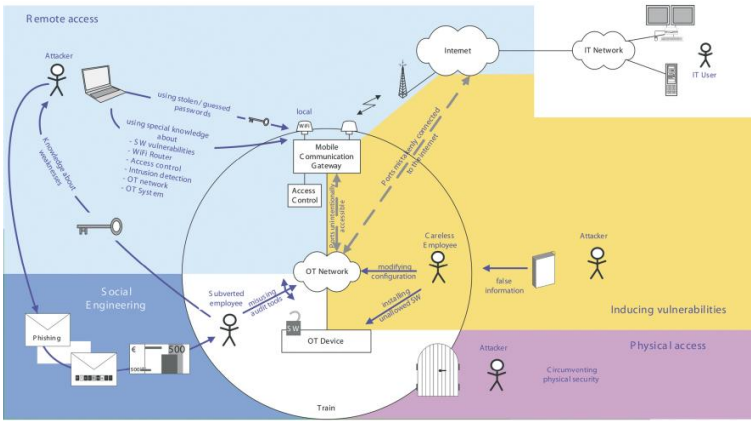

Bild 4: Wege zur Schaffung von Zugängen in das OT-System

3.3 Einbringen von Malware (installing malicious capabilities)

Der Angreifer versucht in diesem Schritt auf verschiedenen Wegen Malware in das OT-System einzubringen.
Im Mittelpunkt dieses Abschnitts steht der Versuch des Angreifers, einen dauerhaften Zugang einzurichten und die Malware so zu positionieren, dass sie später die gewünschten Schäden verursachen kann (Bild 5).
Ein typischer Weg ist dabei die Installation entsprechender mit Malware bestückter Speichermedien durch beeinflusste Personen mit Zugang zum OT-System oder durch den Angreifer selbst über einen physischen Zugang.
Eine wichtige Rolle spielt auch die Installation von Malware in HW- und SW-Komponenten der diversen Zulieferer des OT-System ebenso wie die Einschleusung über Service-Laptops oder Rechner der IT, die neben der Verbindung zum OT-System auch einen Anschluss zum Internet haben.
Die eingeschleuste Malware kann im finalen Schritt einerseits autark schädliche Funktionen ausführen oder auch über eine Schnittstelle verfügen, über die diese ferngesteuert aktiviert werden kann.

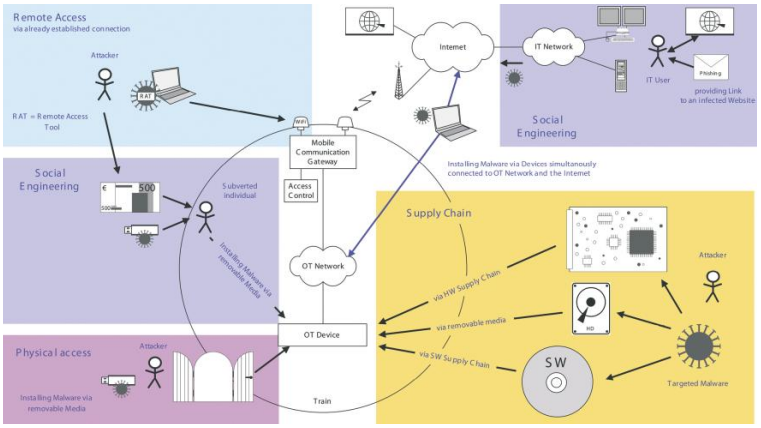

Bild 5: Optionen zur Einschleusung von Malware in das OT-System

3.4 Schaden verursachen (causing damage)

In diesem Abschnitt wird – nach der Vorbereitung in den vorhergehenden Schritten – der eigentliche Angriff durchgeführt und ein Schaden verursacht.
In dieser Phase des Angriffs ist es das Ziel des Angreifers, die erarbeiteten Möglichkeiten zu nutzen und einen möglichst großen Schaden herbeizuführen (Bild 6).
Bei einer Man-in-the-Middle-Attacke werden Schwächen in bestehenden Kommunikationsverbindungen ausgenutzt, um in diese einzudringen, sie abzuhören, die Kontrolle über sie zu übernehmen und die Daten zu verfälschen mit dem Ziel, Funktionseinschränkungen im Zielsystem zu erreichen. Eine weitere gängige Angriffsmethode ist ein sogenannter DOS-Angriff (Denial of Service) auf das OT-Netzwerk, der das Ziel hat, das Netzwerk mit so vielen Anfragen zu überfluten, dass das OT-System seine Aufgaben nicht mehr bewältigen kann.Angriffe unter Einbeziehung von Mitarbeitern umfassen ein weites Spektrum, das auch diverse – nicht zerstörende – Manipulationen beinhaltet. Physische Attacken durch Angreifer zielen dagegen auf eine starke Beeinträchtigung oder gar die Zerstörung von Teilen oder des gesamten OT-Systems.
Angreifer benutzen oft Malware, die geschützte interne Informationen des OT-Systems gezielt beeinflusst. Mittels solcher Schadprogramme können die Datenspeicher ausgelesen und ggf. verändert oder auch die ausgelesenen Daten an den Angreifer weitergeleitet werden. Weiteres Ziel einer aktivierten Malware sind schädliche Eingriffe in die Funktion des OT-Systems bzw. die Einrichtung eines dauerhaften Zugriffs durch den Angreifer.
Der bei den Attacken verursachte Schaden kann neben den genannten unmittelbaren Schäden auch in

mittelbar dadurch hervorgerufenen Folgeschäden bestehen. Das können Verletzungen der Vertraulichkeit ebenso wie die Einschränkung der Verfügbarkeit oder gar der Verlust der Integrität des OT-Systems sein, was im schlimmsten Fall zu Unfällen durch Störung von Sicherheitsfunktionen führen kann.

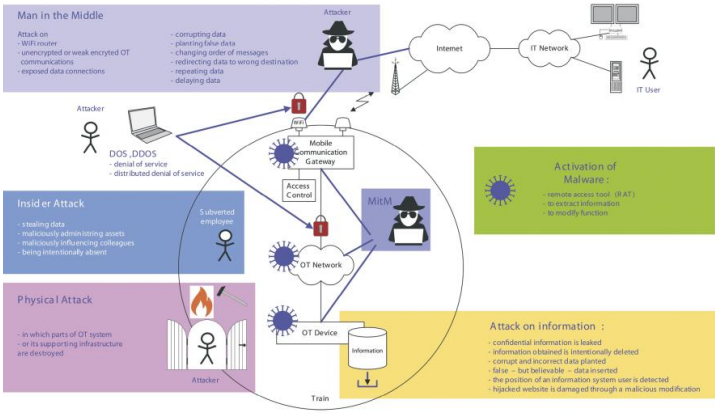

Bild 6: Typische Angriffsszenarien

4 Schlussbetrachtung

Im vorliegenden Artikel wird ein Verfahren vorgestellt, wie aus den unterschiedlichen Bedrohungslisten für OT-Systeme ein harmonisierter Bedrohungskatalog abgeleitet werden kann. Mit diesem Verfahren wird ein harmonisierter und optimierter Bedrohungskatalog für Schienenfahrzeuge erarbeitet, der als Diskussionsgrundlage für eine Abstimmung zwischen Herstellern, Betreibern und Behörden dienen kann. Mit diesem Artikel möchten die Autoren eine breite Diskussion mit allen Stakeholdern anstoßen, um einen abgestimmten Bedrohungskatalog für den Bahnbereich zu entwickeln.

https://doi.org/10.62682/VFTN3956

Literatur

[1] IEC 62443-3-2:2020-06:2020-06. Security for industrial automation and control systems Part 3-2: Security risk assessment for system design. VDE Verlag GmbH, Berlin, Juni 2020.

[2] TS 50701:2021-01 Railway applications – Cybersecurity. VDE Verlag GmbH, Berlin, Januar 2021, https://www.dke.de/de/normen-standards/dokument?id=7160007&type=dke 7Cdokument, abgerufen am 15.01.2024.

[3] ENISA THREAT LANDSCAPE 2023, DOI: 10.2824/782573, Oktober 2023, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023, abgerufen am 16.01.2024.

[4] NIST SP 800-30 Guide of Conducting Risk Assessments, Rev. 1, DOI: 10.6028/NIST.SP.800-30r1, September 2012, https://doi.org/10.6028/NIST.SP.800-30r1 , abgerufen am 03.01.2024.

[5] MITRE ATT&CK® Matrix for ICS, 2023. https://attack.mitre.org/matrices/ics/, abgerufen am: 04.12.2023.

[6] MITRE: CAPEC- Common Attack Pattern Enumeration and Classification. A Community Resource for Identifying and Understanding Attacks, 2023. https://capec.mitre.org/, abgerufen am 04.12.2023.

[7] ENISA RAILWAY CYBERSECURITY. Good practices in cyber risk management, DOI: 10.2824/92259, November 2021, https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management, abgerufen am 15.01.2024.

[8] Shift2Rail X2Rail-1 Appendix to D8.2 Security Assessment: A mapping of threat landscapes, Rev. 1.0, November 2018, https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-1, dann klick auf „Results and Publications“ und „Deliverable D8.2 Security Assessment“, abgerufen am 15.01.2024.

[9] ENISA Interoperable EU Risk Management Toolbox, DOI: 10.2824/68948, Februar 2023, https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox, abgerufen am 15.01.2024.

[10] ISO/IEC 27005:2022-10. Information security, cybersecurity and privacy protection – Guidance on managing information security risks, Oktober 2022, International Organization for Standardization, Genf, Schweiz, https://www.iso.org/standard/80585.html, abgerufen am 15.01.2024.

[11] ENISA Threat Taxonomy. Latest version of ENISA‘s Threat Taxonomy, European Union Agency for Cybersecurity, September 2016, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view, abgerufen am 15.01.2024.

[12] BSI IT-Grundschutz-Kompendium – Werkzeug für Informationssicherheit. Elementare Gefährdungen, Bundesamt für Sicherheit in der Informationstechnik, Dezember 2020, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Elementare_Gefaehrdungen.html?nn=128562, abgerufen am 15.01.2024.