Fahrzeug-Cybersecurity – Erfahrungen bei der Implementierung in Bestandsfahrzeugen

Vehicle cybersecurity – Experience obtained from implementations on legacy rolling stock

Daniel Jaeggi | Raphael Santos Cavalcanti | Alex Cowan

Im Laufe der vergangenen Jahre hat das Bewusstsein für die Auswirkungen von Cyberbedrohungen auf das Schienennetz stark zugenommen. Dies hat zu vermehrten Regulierungsanstrengungen geführt, wonach Eigentümer und Betreiber von Schienenfahrzeugen dementsprechend die Cyberrisiken ihrer IT- und OT-Infrastruktur neu bewertet haben. Die Einführung von Abhilfemaßnahmen in Bestandsfahrzeuge bringt viele Herausforderungen mit sich. RazorSecure ist seit 2016 im Bereich der Cybersecurity für den Schienenverkehr tätig. In dem vorliegenden Beitrag stellen wir unsere Erfahrungen bzgl. der Implementierung von Cybersecurity-Lösungen in Bestandsfahrzeuge vor.

1 Einführung neuer Cybersecurity-Anforderungen

Eine der unmittelbaren Auswirkungen der aktuellen Entwicklungen besteht darin, dass Eigentümer / Betreiber bei neuen Anlagen- und Systemausschreibungen höhere Anforderungen an die Cybersecurity stellen und auch die Bestandsfahrzeuge einer eingehenden Untersuchung unterziehen. In der Vergangenheit wurden bei der Schienenfahrzeugbeschaffung keine ausdrücklichen Anforderungen an die Cybersecurity gestellt, oder wenn es doch solche Anforderungen gab, waren diese aus heutiger Sicht unzureichend. Unserer Erfahrung nach sind die technischen Sicherheitsvorkehrungen bei den Bestandsfahrzeugen im Allgemeinen nicht besonders ausgeprägt und variieren sehr stark. Ohne etablierte, erforderliche Sicherheitsanforderungen wurden Design und Implementierung von Bordnetzen und digitalen Systemen eher dem Zufall und der alleinigen Beurteilung des Fahrzeugherstellers überlassen. Hinzu kommt noch die Rolle des Fahrzeugherstellers als Systemintegrator, denn die Security-Konzepte der vielen Teilsysteme eines Zugs liegen in den Händen der Lieferanten der Teilsysteme, die oft nicht über das nötige Fachwissen in Sachen Cybersecurity verfügen und denen die notwendigen Anforderungen nicht auferlegt wurden.

Deshalb stehen heute Betreiber und Eigentümer vor folgenden Herausforderungen bei den Bestandsfahrzeugen:

- Cybersecurity-Schwachstellen entstanden bereits bei der Fahrzeugherstellung, da diesem Thema in der Vergangenheit nicht ausreichend Beachtung geschenkt wurde.
- Neue Schwachstellen werden bei der Wartung der Flotte eingeschleust, vor allem durch neue Konnektivitätssysteme zwischen dem Fahrzeug und der streckenseitigen Infrastruktur – und durch die Integration neuer digitaler Systeme.
- Bedrohungen im Bereich Cybersecurity sind dynamisch: Im Laufe der Zeit werden neue Schwachstellen erkannt, und die Bedrohungslage kann sich verändern.

In recent years, there has been increasing awareness of the potential for cyber threats to impact railway systems. This awareness has led to increased regulatory activity and has caused rolling stock owners and operators to reassess their cyber risks. Implementing mitigating strategies against these risks on legacy rolling stock brings with it many challenges. RazorSecure has been involved in rail cyber security since 2016. This article presents our experience of implementing cybersecurity solutions on these vehicles.

1 Introduction of new cybersecurity requirements

One direct impact of the increased awareness of cyber risks is that owners / operators have started incorporating more comprehensive cyber security requirements into their new rolling stock and system tenders and they have also started to look at their installed base fleets. In the past, rolling stock procurements did not have any explicit cyber security requirements or, if there were any, they were at a level that would be deemed insufficient today.

In our experience, the level of security engineering on installed base fleets is generally weak and highly variable. The lack of any established, mandatory security requirements means that the design and implementation of the on-board networks and digital systems has been left rather to chance and the judgement of the Original Equipment Manufacturer (OEM). This has been compounded by the role of the OEM as a system integrator, where the security of the many subsystems that comprise a train is left in the hands of the subsystem vendor, who may not have any cyber security expertise and may not have received all the requirements.

The challenge an operator or owner faces today is that for a given fleet:

- there are cyber vulnerabilities that were present from the factory gate, because insufficient regard has been given to cyber security historically
- system upgrades have introduced new vulnerabilities since the fleet came into service, primarily driven by the addition of wayside connectivity and the integration of different systems
- cyber risks are dynamic: new vulnerabilities are discovered over time and the threat environment may change

In other words, even if a cyber risk assessment were to have been performed on delivery of the fleet at some point in the past, the results of that assessment may no longer be valid. A

Anders gesagt, auch wenn bei Lieferung der Flotte eine Analyse der Cyberbedrohungen durchgeführt wurde, kann es sein, dass die Ergebnisse schnell nicht mehr der aktuellen Bedrohungslage entsprechen. Bei einer heute durchgeführten Bedrohungsanalyse werden mit Sicherheit neue Bedrohungen erkannt, die bei der Lieferung noch nicht ersichtlich waren oder neu hinzugekommen sind.
In der Vergangenheit haben wir uns hauptsächlich mit Bestandsfahrzeugen befasst, auch wenn die Arbeit mit Neufahrzeugen / -flotten immer wichtiger wird. Im Bereich der Implementierung von Cybersecurity-Lösungen für Bestandsfahrzeuge konnten wir einen breiten Erfahrungsschatz sammeln. Wir berücksichtigen hier aber nicht die organisatorischen und verfahrenstechnischen Auswirkungen der Cybersecurity, obwohl diese durchaus von Bedeutung sind, sondern konzentrieren uns auf die Maßnahmen zur Verbesserung der Cybersecurity für bereits existierende Schienenfahrzeuge.

2 Herausforderungen im Bereich der Bestandsfahrzeuge

Eine umfangreiche Risiko- und Bedrohungsanalyse, ggf. gekoppelt mit einem Penetrationstest, ist der erste wesentliche Schritt, um ein effektives Cybersecurity-Konzept für Bestandsfahrzeuge zu entwickeln [1]. Auf dieser Grundlage kann ein Prozess definiert, können Bedrohungen analysiert und Abhilfemaßnahmen entworfen, geplant und umgesetzt werden. In der Praxis allerdings tauchen etliche praktische Probleme auf, die es zu beachten gilt. Diese Probleme können ein beträchtliches Hindernis bei der Einführung eines verbesserten Security-Konzepts darstellen. Dazu zählen:

- Netzwerkarchitektur und -konfiguration
- Zugänglichkeit und Wartungsfreundlichkeit
- Veralterung / Obsolenz
- Informationsdefizite
- physikalische und systembedingte Einschränkungen
- Einbeziehung von Interessenvertretern („stakeholder“)

Wir werden diese Aspekte nachfolgend erläutern.

2.1 Netzwerkarchitektur und -konfiguration

Bei älteren Bestandsfahrzeugen sind die Netzwerke meist einfacher und flacher ausgelegt. Außerdem ist der Grad an logischer und physikalischer Trennung und Abgrenzung bei den alten Netzwerken nicht so hoch wie bei den neueren Netzwerkkonzepten. Firewalls sind in den älteren Netzwerken eher selten, und Switches verfügen über weniger Funktionen. Dies ist im Hinblick auf Security eine wahre Herausforderung. Ein Kernprinzip beim Netzwerkdesign ist das sogenannte Security Zoning [1], bei dem Systeme nach ihren jeweiligen Sicherheitsanforderungen gruppiert werden.
Wenn kein Security Zoning betrieben wird und es eine Tendenz gibt, System-Upgrades und Erweiterungen „huckepack“ in existierende Netzwerke zu übernehmen, um die Kosten und die komplexen Anforderungen für eine Neugestaltung des Netzwerks oder neue Switch-Hardware und zusätzliche Verkabelung zu umgehen, kann dies zu Netzwerken mit Schwachstellen führen, die schwer zu sichern sind.
Außerdem können neue oder aufgerüstete Systeme mit hohen Bandbreitenanforderungen (insbesondere durch Videoüberwachung) dazu führen, dass Netzwerke angreifbarer werden. Dieses Risiko entsteht, da es für Angreifer einfacher ist, Denial-of-Service-Angriffe gegen ein Netz mit geringerer Bandbreite zu richten.

risk assessment performed today will almost certainly throw up new risks that either weren't apparent on delivery or have emerged since.
The bulk of our work has historically been on existing fleets, although this is rapidly changing. As such, we have extensive experience of implementing cyber security solutions on existing fleets and the views expressed in this paper reflect this experience.
This paper does not consider the organisational and procedural implications of cyber security, which are important, but rather only focuses on the means of improving cyber security on existing vehicles.

2 The challenges facing existing rolling stock

A comprehensive risk and threat analysis, possibly coupled with a penetration test, is the first essential step in developing an effective cybersecurity concept for existing vehicles [1]. A process can be defined, threats analysed and remediation measures designed, planned and implemented on this basis. In practice, however, there are a number of issues that need to be considered and that cause not insignificant hurdles to the implementation of improved security. These are:

- the network architecture and configuration
- accessibility and maintainability
- obsolescence
- information deficits
- physical and system constraints
- stakeholder engagement

We will discuss these in turn.

2.1 Network architecture and configuration

Network designs on older rolling stock are typically simpler and flatter and older networks lack the degree of logical or physical separation and segregation found in newer designs. Firewalls are not common and switches have lower levels of functionality. This presents a challenge from a security perspective. A core principle in network design is security zoning [1], where systems are grouped according to their security requirements.
The lack of zoning, coupled with a tendency for system upgrades and additions to piggyback onto existing networks to avoid the cost and complexity of re-engineering the network or adding new switch hardware and cabling, can result in a vulnerable network that is hard to secure.
Furthermore, the addition of new or upgraded systems with high bandwidth demands (video surveillance being a particular case in point) can itself cause the network to be more exploitable by making it easier for an attacker to perform Denial of Service attacks against networks with smaller bandwidth margins.
Finally, the addition of wayside connectivity, and applications leveraging this connectivity, expands the network perimeter without a corresponding re-assessment of the risks being performed.

2.2 Accessibility and maintainability

A significant source of the cyber threat (whether malicious or non-malicious) to existing rolling stock comes from maintenance practices and, specifically, the degree of trust and the corresponding lower level of access controls placed on technicians connecting to on-board networks and systems in or-

Schließlich wird die Netzwerkumgebung eines Fahrzeugs oft mit Konnektivitätssystemen für die Kommunikation zwischen dem Fahrzeug und der streckenseitigen Infrastruktur ausgerüstet, ohne die dadurch entstehenden, potenziellen neuen Risiken in Betracht zu ziehen.

2.2 Zugänglichkeit und Wartungsfreundlichkeit

Eine wesentliche Quelle für Cyberbedrohungen – bösartig oder nicht – bei den Bestandsfahrzeugen liegt in der Wartung – und hier insbesondere in dem Vertrauen, das den Technikern beim Verbinden mit den Bordnetzwerken und den Systemen entgegengebracht wird, wenn sie Updates und Wartungsaufgaben durchführen. Wir haben eine allgemeine Tendenz beobachtet, dem Zugang Vorrang vor der Security einzuräumen: Der Netzwerkzugang wird in der Regel nur durch eine Einschränkung des physischen Zugangs verhindert (z. B. durch Anbringen der Netzwerkanschlüsse in abgeschlossenen Schaltschränken oder in der Fahrerkabine). Diese Maßnahme hilft nur gegen zufällige Anwender von außen, aber nicht gegen Insider oder entschlossene Hacker. Ältere Systeme verfügen oftmals nur über eine schwache oder keine Passwortkontrolle, und veraltete Wartungssoftware läuft oft auf „ungepatchten" Service-Laptops. Diese Schwachstellen sind nicht einfach zu beheben, da sie in einigen Fällen umfangreiche Anpassungen der Wartungsverfahren erfordern. Dies kann sehr komplex und kostenintensiv sein.

2.3 Veralterung / Obsolenz

Unserer Ansicht nach ist veraltete Software ein sehr wichtiges Thema, das von der Industrie bislang nicht angemessen berücksichtigt und angegangen wurde. Software unterscheidet sich von Hardware insofern, dass während der gesamten Lebensdauer der Software immer wieder Änderungen erforderlich sind. Dies ist durch die Komplexität und die Wahrscheinlichkeit bedingt, dass Schwachstellen oder Fehler vorhanden sind, die Auswirkungen auf die Funktionsfähigkeit haben und erst nach einiger Zeit entdeckt werden. Wenn für eine Software kein Update durchgeführt werden kann, gilt sie als veraltet. Veraltete Software ist wiederum eine Quelle für mögliche Cyberbedrohungen.

Was sind die Ursachen der Veralterung? Aus unserer Erfahrung sind diese meist eine veraltete Hardware an sich, die Einstellung des Anbieter-Supports, der Marktaustritt des Anbieters, die mangelnde Software- und Dokumentationsintegrität, und ein Know-how-Verlust durch „Wissensabwanderung".

Die Veralterung stellt eine Herausforderung in Sachen Cybersecurity dar, da Schwachstellen nicht mehr direkt an der Quelle behoben werden können. Falls möglich, sind in einem solchen Fall weitere Schutzmaßnahmen vorzusehen, und / oder es muss ein Erkennungssystem implementiert werden, das vor möglichen Bedrohungen warnt. Man muss allerdings bereit sein zu akzeptieren, dass nicht alle Schwachstellen behoben werden können. Im Hinblick auf Bestandsfahrzeuge geht es darum zu lernen, mit Schwachstellen im System zu leben.

2.4 Informationsdefizite

Die Eigentümer / Betreiber können sich beim Bewerten von Cyberbedrohungen oder beim Entwickeln von Strategien zur Risikominimierung einer ganzen Reihe von Herausforderungen gegenübersehen, die als Informationsdefizite eingeordnet werden können. Diese Informationsdefizite können verhindern, dass eine bestimmte Schwachstelle und deren Auswirkungen richtig eingeschätzt werden, und dazu beitragen, dass die Kosten und die Komplexität der Risikoanalyse steigen. Außerdem können die

der to perform updates and maintenance tasks. We have observed a general tendency to prioritise accessibility over security: network access may typically only be controlled by restricting physical access (e.g. placing network ports in locked cabinets or in the driver's cab), which is effective only at preventing a casual outsider, but has no impact against an insider or a determined outsider. Similarly, older systems may have weaker or no password controls or have obsolete maintenance software running on un-patched service laptops. These vulnerabilities are not easy to fix, because they sometimes require significant changes to maintenance practices, which can be both complex and costly.

2.3 Obsolescence

We view software obsolescence as a key issue that has not been adequately addressed in the industry. Software differs from hardware in that there is an implicit need for change over the lifetime of that software. This is due to complexity and the likelihood that there are vulnerabilities or bugs affecting function that are only discovered some way into its lifetime. If the software cannot be updated, then it is deemed obsolete. Obsolete software is a potential source of cyber vulnerabilities.

What are the causes of obsolescence? In our experience, they include hardware obsolescence, the withdrawal of support by the vendor, the vendor going out of business, a loss of software and documentation integrity and a loss of knowledge.

Obsolescence presents a challenge for cyber security in that vulnerabilities then cannot be fixed at the source. Additional protective measures must then be deployed, if possible, or detection must be implemented to provide a warning of any potential threats. The fact that it may not be possible to fix every vulnerability has to be accepted; the "game" for existing fleets is learning to live with vulnerabilities.

2.4 Information deficits

An owner / operator may be faced with a range of challenges that can be classed as information deficits when assessing cyber risks or designing risk mitigation strategies. These information deficits may prevent the correct identification assessment of a given vulnerability and its impact, add to the cost and complexity of analysing the risk or lead to suboptimal mitigation solutions being designed and implemented.

We have observed an occasional lack of openness and information sharing regarding security-relevant information (e.g. architectural design, protocol details, detailed risk assessments); this information is said to be proprietary and is withheld on these grounds. Alternately, information disclosure is sometimes ruled out on the basis of it constituting a security risk. This argument is, in effect, an appeal to the principle of Security by Obscurity, which is generally not recommended.

Furthermore, the documentation may be incomplete or incorrect and this further hinders the identification of risks. Incompletely documented information may only be regained at significant cost and operating impact, if at all. Incorrect information may only be discovered following the direct testing of the system in the network in question and a comprehensive verification testing strategy may be costly and time consuming to complete.

A final information deficit relates to asset inventory and configuration management. In some instances, we find that a comprehensive and up to date asset inventory is not available

Defizite dazu führen, dass die Lösungen, die zur Risikominimierung entwickelt und implementiert werden, unzureichend sind.
Wir konnten beobachten, dass sicherheitsrelevante Informationen gelegentlich nicht offen kommuniziert und weitergeleitet wurden (z. B. Architekturentwurf, Einzelheiten zu Protokollen, detaillierte Risikobewertungen); diese Informationen sind angeblich firmeneigen und werden daher zurückgehalten. Es kann auch vorkommen, dass die Offenlegung von Informationen mit der Begründung verhindert wird, sie stelle ein Sicherheitsrisiko dar. Dieser Ansatz entspricht tatsächlich dem Prinzip der „Security by Obscurity" (etwa: Sicherheit durch absichtliches Im-Unklaren-Lassen) und ist im Allgemeinen nicht empfehlenswert.
Zusätzlich ist es möglich, dass die Dokumentation unzureichend oder gar fehlerhaft ist, wodurch die Erkennung von Bedrohungen noch weiter behindert wird. Unzureichend dokumentierte Informationen können, wenn überhaupt, nur zu beträchtlichen Kosten und mit betrieblichen Auswirkungen zurückgewonnen werden. Falsche Informationen können nur durch einen direkten Test des Systems in dem betreffenden Netzwerk ermittelt werden, und eine umfassende Prüfstrategie zur Verifizierung kann sehr kosten- und zeitaufwendig sein.
Die letzte Art von Informationsdefizit bezieht sich auf die Bestandsaufnahme von Anlagen und auf das Konfigurationsmanagement. Wir stellen immer wieder fest, dass in manchen Fällen keine vollständige und aktuelle Bestandsliste verfügbar ist und genaue Informationen zur Softwarekonfiguration digitaler Bestände fehlen. Dadurch wird die Schwachstellenerkennung bedeutend erschwert.

2.5 Physikalische und systembedingte Einschränkungen

Wenn Schwachstellen nicht behoben werden können (z. B. aufgrund veralteter Software oder Hardware) oder zusätzliche Sicherheitsmaßnahmen ergriffen werden müssen, um Bedrohungen aus dem Weg zu räumen (z. B. durch Anwendung des Prinzips der mehrschichtigen Verteidigung), dann ist es sehr wahrscheinlich, dass für Bestandsfahrzeuge erhebliche und umfangreiche zusätzliche Sicherheitsmaßnahmen erforderlich sind. Bei einer solchen Maßnahme kann es sich um eine Änderung der Software handeln (vorausgesetzt, es handelt sich nicht um ein veraltetes System) oder aber um das Hinzufügen einer Software- und Hardwarelösung. Beide Ansätze bringen in der Praxis einige Herausforderungen mit sich.
Viele Bestandsfahrzeuge haben physikalische Einschränkungen. Vor allem aus Platzgründen kann es schwierig sein, neue Hardware hinzuzufügen. Die neue Hardware erfordert eine Netzwerkanbindung, und die vorhandenen Netzwerk-Switches sind möglicherweise bereits ausgelastet und können nicht oder nur zu sehr hohen Kosten aufgerüstet werden.
Sicherheitssoftware (z. B. Angriffserkennungssysteme oder ein „Intrusion Detection System" – IDS) kann zum Kernsystem und zur Netzwerkausrüstung hinzugefügt werden, wobei an dieser Stelle die Einschränkungen der Ressourcen ins Spiel kommen. Ältere Systeme verfügen unter Umständen nur über eingeschränkte Ressourcen und können die zusätzliche Verarbeitungskapazität und die Anforderungen an Arbeitsspeicher und Langzeitspeicherung der zusätzlichen Software nicht unterstützen.
Für diese Probleme gibt es nicht die eine einfache Lösung schlechthin, sondern nur eine flexible Bandbreite an Lösungen, die, je nach der betreffenden Flotte, für verschiedene Szenarien eingesetzt und angepasst werden können. Softwarelösungen profitieren davon, dass sie leicht zu handhaben sind. Wir haben unsere IDS-Software erfolgreich auf eine 32-Bit-PowerPC-Ar-

and accurate information relating to the software configuration on digital assets is missing. This makes the assessment of vulnerabilities extremely difficult.

2.5 Physical and system constraints

As has been discussed, if a vulnerability cannot be fixed (e.g. due to obsolescence) or if additional security measures are required to mitigate any identified risks (e.g. by the application of the Defence in Depth principle), it is likely that an existing fleet will require a security countermeasure, either in the form of a software change (assuming this can be done on a non-obsolete system) or the addition of a hardware and software solution. Both approaches present some challenges in practice.
Many existing fleets are subject to physical constraints. It can be challenging to add a new piece of hardware, primarily for reasons of space. New hardware will require network connectivity and existing network switches may be at capacity and unable to be upgraded or it may be costly to do so.
Security software (e.g. Intrusion Detection Systems – IDS) can be added to core systems and networking equipment but resource constraints frequently come into play here. Older systems may be resource limited and unable to support the additional processing, memory or storage requirements of the additional software.
There are no easy solutions to these problems, other than to have a flexible range of solutions that are able to be deployed and to be adapted to multiple scenarios, depending on the fleet in question. Software solutions in particular benefit from being lightweight – we have successfully ported our IDS software to a 32-bit PowerPC architecture as the most extreme example of a CPU and RAM constrained system.

2.6 Stakeholder engagement

A train can be considered to constitute a system of systems and there are many parties who may be, directly or indirectly, involved in the design, operation or maintenance of the vehicle. Without clear cyber requirements having been set and, critically, contractual obligations and processes governing cyber security related activities having been put in place, it can become challenging to align the different stakeholders and effect changes. Security is only as good as its weakest link; effective security requires coordination and cooperation between different stakeholders.

3 Three effective approaches for existing fleets

We present three general approaches that we have found effective in addressing cyber risks on existing fleets. These approaches are the result of our experience analysing onboard networks, developing rolling stock-specific cybersecurity solutions and deploying them to secure multi-OEM estates.

3.1 Adding detection to vantage points

Adding network-based IDS to monitor key network traffic and host-based IDS to high-risk systems (e.g. communications gateways) caters particularly well to scenarios where minimally invasive solutions are required due to hardware or resource limitations. This very approach has been deployed across more than 1600 rail vehicles across Europe and North America and has demonstrated its ability to detect events that would have otherwise gone unseen (fig. 1).

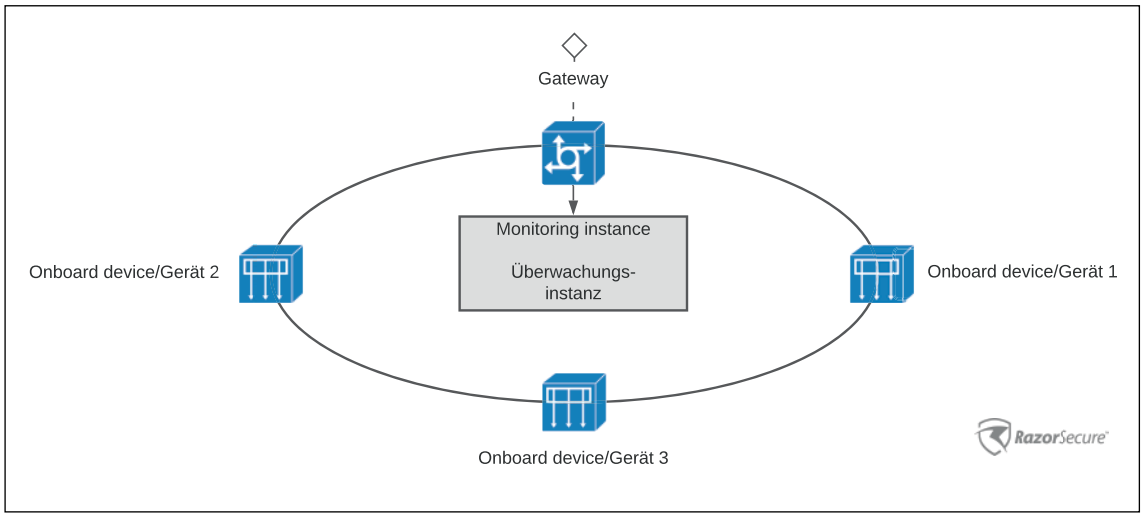

Bild 1: Beispiel Netzwerkarchitektur mit Monitoring- / Überwachungs-instanz als Komponente eines IDS
Fig. 1: An example network architecture with an Intrusion Detection System

chitektur portiert, das extremste Beispiel für ein System mit begrenzter CPU- und RAM-Leistung.

2.6 Einbeziehung von Interessenvertretern („stakeholder")

Schienenfahrzeuge bestehen aus vielen Untersystemen, und es sind direkt oder indirekt viele Parteien an der Konzeption, dem Betrieb und der Wartung der Fahrzeuge beteiligt. Ohne eine eindeutige Definition der Cyber-Anforderungen und vor allem vertragliche Verpflichtungen zu den Aktivitäten im Bereich Cybersecurity kann es schwierig werden, verschiedene Interessen unter einen Hut zu bringen und Änderungen zu bewirken. Ein wirkungsvolles Security-Konzept erfordert die Koordinierung und Zusammenarbeit verschiedener Interessenvertreter.

3 Drei wirkungsvolle Herangehensweisen für Bestandsfahrzeuge

Wir stellen im Folgenden drei allgemeine Herangehensweisen vor, die sich bei der Bekämpfung von Cyberbedrohungen bei Bestandsfahrzeugen als wirkungsvoll erwiesen haben. Diese Ansätze sind das Ergebnis unserer Erfahrungen bei der Analyse von Bordnetzwerken, der Entwicklung von flottenspezifischen Cybersecurity-Lösungen und deren Einsatz zur Sicherung von Flotten mit Fahrzeugen von mehreren Fahrzeugherstellern.

3.1 Bedrohungserkennung an Schlüsselpunkten hinzufügen

Das Hinzufügen netzbasierter IDS zum Überwachen des zentralen Netzwerkverkehrs und hostbasierter IDS zu Hochrisikosystemen (z. B. Kommunikationsschnittstellen) erweist sich als besonders wirkungsvoll, wenn aufgrund von Hardware- oder Ressourceneinschränkungen minimalinvasive Lösungen gefragt sind. Dieser Ansatz wurde bereits bei mehr als 1600 Schienenfahrzeugen in Europa und Nordamerika realisiert. Es hat sich herausgestellt, dass Ereignisse erkannt wurden, die sonst unentdeckt geblieben wären (Bild 1).
Unsere Erfahrung zeigt, dass für Schienenfahrzeuge mit eingeschränkten digitalen Möglichkeiten der „minimalinvasive" IDS-Ansatz im Hinblick auf die technische Komplexität, die Netzwerkabdeckung und die Kosten die ausgewogenste Lösung ist. Dies gilt insbesondere für Bestandsfahrzeuge, die über Systeme mit Schwachstellen und veraltete Systeme verfügen, bei denen aber ein Austausch / Upgrade zu kostspielig oder komplex (oder beides) wäre oder bei denen die Sicherheitsmaßnahmen als zu

Our experience has shown us that "minimally invasive" IDS deployments are able to provide the most balanced solution in terms of technical complexity, network coverage and cost for older trains with limited digital capabilities. This is especially true on rolling stock where vulnerable and obsolete systems are present, but where it would be too costly or complex to upgrade/replace them (or both), or where security controls have been judged to be weak, while improving them was neither technically feasible nor financially attractive. Likewise, this approach is also favoured in cases where the cost of the comprehensive re-engineering of the network architecture and system design would have been unjustifiable.

3.2 Improving network architecture and zoning

In contrast to the pure detection approach described in the previous section, implementing an improved network design by upgrading the switches, changing the network configuration and adding firewalls aims to fix network-level vulnerabilities at the source by improving the zoning and permitting a finer-grained network segmentation, as well as adding network monitoring at the same time. The ideal deployment strategy varies greatly and is a function of the required monitoring and protection capabilities, any physical or technical constraints and the lifetime cost of the implemented solution (fig. 2).
What we have observed through our deployments is that owners / operators prefer this approach for newer, more digitised rolling stock, and combine it with enhanced detection capabilities. This approach can deliver significant security benefits; vehicle homologation does need to be considered, though in practice this can be navigated with the support of the OEM. A secondary benefit of an improved network architecture is the ease of applying future system upgrades without incurring additional network engineering costs in the future.

3.3 Implement access controls

The third effective approach relates to the lack of controls and authentication with regard to internal staff and maintenance teams when accessing onboard digital networks and systems.
Our experience has shown that network access controls, which greatly reduce the attack surface, are relatively inexpensive and quick to implement. Additionally, it must be

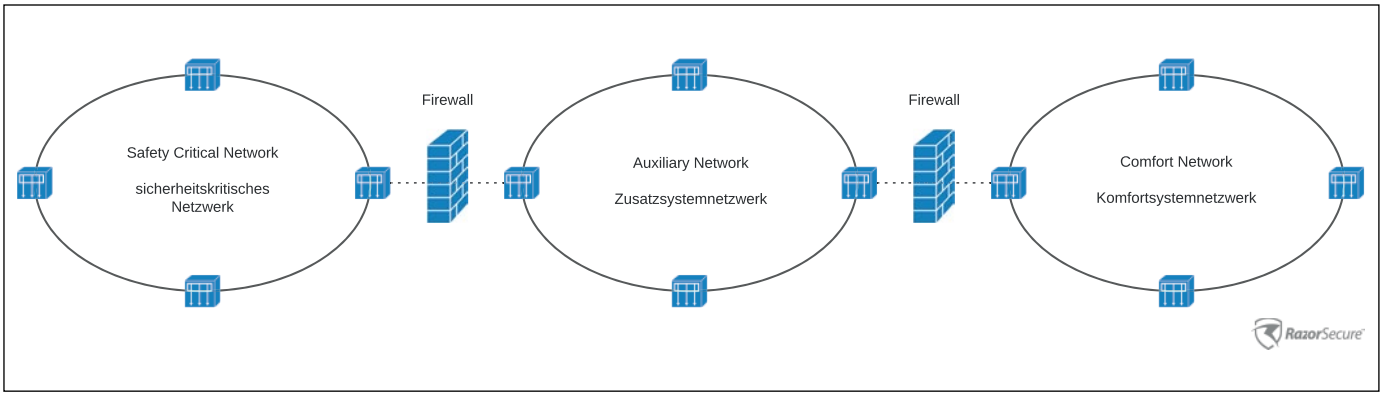

Bild 2: Beispiel Netzwerkarchitektur mit verbessertem Netzwerkdesign durch Firewall-Trennung
Fig. 2: An example network architecture with improved security zoning and firewalling

schwach beurteilt wurden, eine Aufrüstung aber technisch nicht machbar oder finanziell uninteressant war. Dieser Ansatz wurde auch bevorzugt, wenn die Kosten einer umfassenden Neugestaltung der Netzwerkarchitektur und des Systemdesigns nicht zu rechtfertigen gewesen wären.

3.2 Optimierung von Netzwerkarchitektur und Zoning

Im Gegensatz zu dem Ansatz reiner Bedrohungserkennung zielt das Implementieren eines optimierten Netzwerkdesigns durch eine Aufrüstung der Switches, eine Änderung der Netzwerkkonfiguration oder das Hinzufügen von Firewalls darauf ab, die Schwachstellen im Netzwerk an der Quelle zu beheben. Dies erfolgt durch eine Optimierung des Zoning und ermöglicht eine feinere Netzwerksegmentierung bei gleichzeitigem Hinzufügen einer Lösung zur Netzwerküberwachung. Die ideale Implementierungsstrategie unterschied sich von Fall zu Fall sehr und hing von den erforderlichen Überwachungs- und Schutzfunktionen, den physikalischen und technischen Einschränkungen sowie von den Lebenszykluskosten der jeweiligen Lösung ab (Bild 2).
Wir haben im Rahmen der von uns durchgeführten Bereitstellungen erkannt, dass Eigentümer / Betreiber diesen Ansatz bei neueren, digitalisierten Bestandsfahrzeugen bevorzugten und ihn mit optimierten Lösungen zur Bedrohungserkennung kombinierten. Dieser Ansatz kann bedeutende Verbesserungen in puncto Security bieten; allerdings muss die Zulassung der Schienenfahrzeuge berücksichtigt werden. Dabei kann normalerweise der Fahrzeughersteller behilflich sein. Der zweite Vorteil einer optimierten Netzwerkarchitektur besteht darin, dass künftige Systemaufrüstungen einfach durchgeführt werden können, ohne dass zusätzliche Kosten für die Netzwerktechnik anfallen.

3.3 Implementieren von Zugangskontrollen

Der dritte effektive Ansatz bezieht sich auf die mangelnde Kontrolle und Authentifizierung der unternehmensinternen Mitarbeiter und der Wartungsteams beim Zugriff auf die digitalen Bordnetzwerke und Systeme (Bild 3) .
Wir haben die Erfahrung gemacht, dass die Einführung von Netzwerkzugangskontrollen, mit denen sich die Angriffsfläche deutlich reduzieren lässt, recht kostengünstig und einfach umzusetzen ist. Außerdem sollte an dieser Stelle angemerkt werden, dass in den meisten Bereichen, in denen Mitarbeiter Zugang zu kritischen Systemen benötigen oder erhalten können, stressed that in most areas where staff require or can obtain access to critical systems, a cultural change with regard to safe and secure practices needs to accompany any procedural and technological change (fig. 3).

4 Conclusions

Existing fleets should be assessed for vulnerabilities and cyber risks. The goal of such an assessment is to understand

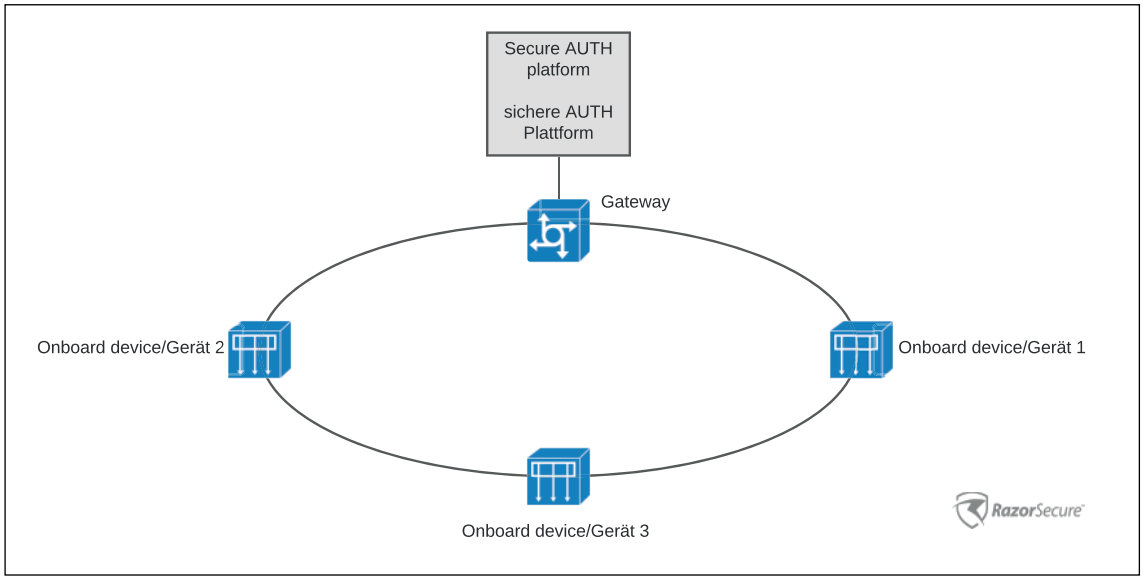

Bild 3: Beispiel Netzwerkarchitektur mit Zugangskontrollen durch sichere Authentifizierungs-Plattform
Fig. 3: An example network architecture with network access control

ein kultureller Wandel im Hinblick auf sichere Praktiken unternommen werden sollte.

4 Schlussfolgerungen

Bestandsfahrzeuge sollten auf Schwachstellen und Cyberrisiken untersucht werden. Ziel einer solchen Bewertung ist es, zu verstehen, welchen Bedrohungen eine Fahrzeugflotte ausgesetzt ist und welche Auswirkungen mögliche Bedrohungen haben können. Im Anschluss an die Bewertung können die Risiken nach Priorität gestaffelt werden.
Bestandsfahrzeuge stellen eine Herausforderung dar, was die Machbarkeit der Einführung von Abhilfemaßnahmen für die ermittelten Risiken angeht. Schwachstellen können unter Umständen nicht an der Quelle behoben werden; es bleibt uns nur der Einsatz von Ausgleichskontrollen in Form von Schutzmaßnahmen für das Netzwerk / System sowie die Überwachung von Netzwerken und Systemen. Technische Zwänge und Einschränkungen können aber den möglichen Umfang der Schutz- und Erkennungsmaßnahmen einschränken.
Drei wirkungsvolle Strategien für die Einführung von Abhilfemaßnahmen bei Bestandsfahrzeugen wurden vorgestellt:

- Maßnahmen zur Erkennung von Bedrohungen hinzufügen
- Zusätzliche Netzwerksegmentierung und -trennung hinzufügen
- Kontrolle des Wartungszugangs zu Netzwerken und Systemen. ■

how a fleet might be compromised and the impacts of such a compromise. This then leads to the prioritisation of risks.
Existing fleets present challenges in the feasibility of mitigating the identified risks. Vulnerabilities may not be able to be fixed at the source; we are left with deploying compensating controls in the form of additional network / system protection and network / system monitoring. Engineering challenges and constraints may limit the scope of the feasible protection and detection measures that can be deployed.
We have presented three feasible strategies for mitigating the risks on existing fleets:

- adding detection
- adding additional network segmentation and segregation
- controlling maintenance access to networks and systems. ■

LITERATUR | LITERATURE
[1] Railway applications – Cybersecurity CLC/TS 50701:2021 https://www.dke.de/de/normen-standards/dokument?id=7152279&type=dke%7Cdokument 28. Januar 2022 um 11:00 CET

AUTOREN | AUTHORS

Daniel Jaeggi
Head of Business Development
Razorsecure Limited
Anschrift / *Address*: Belvedere House, Suite LG8, Basing View, UK-RG21 4HG Basingstoke
E-Mail: danielj@razorsecure.com

Raphael Santos Cavalcanti
DACH Business Development Lead
Razorsecure Limited
Anschrift / *Address*: Lessingstraße 4, D-90443 Nürnberg
E-Mail: raphael@razorsecure.com

Alex Cowan
CEO
Razorsecure Limited
Anschrift / *Address*: Belvedere House, Suite LG8, Basing View, UK-RG21 4HG Basingstoke
E-Mail: alex@razorsecure.com