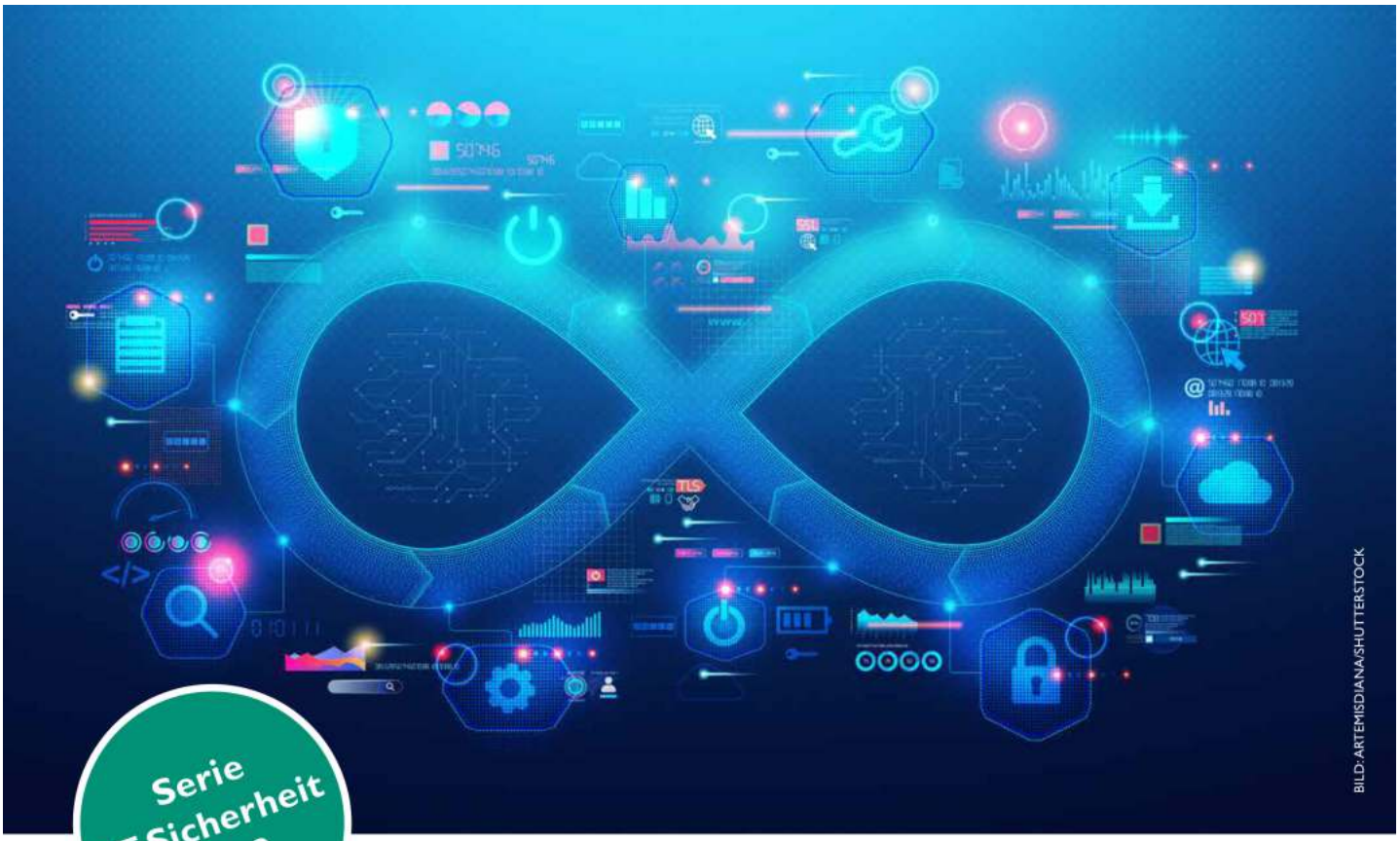

Serie IT-Sicherheit Teil 3

DevSecOps für die Schiene: Lebenslange IT-Sicherheit?

Barbara Feldmann

Die IT-Szene ist seit jeher großzügig mit Schlagwörtern, Trends und innovativen Verheißungen – manche verpuffen, manche bewähren sich dauerhaft. Ein hoch gehandelter Begriff der vergangenen Jahre ist das Prinzip DevSecOps – Development, Security, Operations. Hinter diesem Ansatz verbirgt sich die enge Verzahnung von Softwareentwicklung, Sicherheit und dem Betrieb von Systemen und Anwendungen über ihren kompletten Lebenszyklus hinweg. Ein kollaborativer und zugleich agiler Ansatz, der zunehmend auch Einzug in komplexe, operationale und industrielle Umgebungen hält. Der dritte Teil unserer Serie zur IT-Sicherheit im Bahnsektor geht dem Potenzial der DevSecOps-Philosophie für die Schiene auf den Grund.

„Organisationen mit einer gelebten DevSecOps-Kultur haben kürzere Go-to-Market-Zeiten, geringere Fehlerraten und eine neunmal höhere Wahrscheinlichkeit, schwere Sicherheitsprobleme zu vermeiden" – eine klare Einschätzung, abgeliefert vom US-amerikanischen IT-Sicherheitskonzern Palo Alto Networks im „The State of Cloud Native Security Report 2022". Doch was genau verbirgt sich hinter DevSecOps? In seiner ursprünglichen und damit sehr engen Bedeutung bezieht sich der Ansatz auf die Arbeit in einem Entwicklerteam. Als logische Weiterführung von DevOps zielt die Methode auf die nahtlose Integration, Ausführung und Optimierung von Sicherheitsroutinen sowohl in der Entwicklung als auch in der Einführung und im Betrieb. Für komplexe Umgebungen wie die Bahnbranche muss der Begriff eines integrativen, Lebenszyklus überspannenden Sicherheitsverständnisses sehr weit gefasst werden. Schließlich geht es hier nicht um reine Informationstechnologie, sondern um ein großflächiges Netzwerk aus physikalischen Größen und operativen Prozessbausteinen.

ARTIKELSERIE IT-SICHERHEIT TEIL III — ENTWICKLUNG, SICHERHEIT, BETRIEB

Ein übertragbares Prinzip?

Wenn es um die digitale Transformation geht, ist kaum eine Landschaft so komplex wie die Schiene. Deshalb ist die Anwendung übergreifender, flexibler Denkweisen wie DevSecOps in einem festen Entwicklerteam mit einer fest definierten Aufgabe und eindeutig vereinbarten Service Levels Agreements (SLAs) sicherlich deutlich einfacher umzusetzen als im heterogenen Ökosystem Bahn. Und doch lassen sich einige Kernelemente dieser Herangehensweise ableiten und auf die komplexe Bahnbranche anwenden: Kollaboration, Agilität, kontinuierliche Integrationsprozesse, eine fortlaufende Softwarebereitstellung, die systematische Arbeit entlang definierter Roadmaps, ein konsequentes System-Monitoring und – wo immer möglich und sinnvoll – Automatisierung sowohl in der Entwicklung als auch im laufenden Betrieb. Stefan Katzenbeisser, Professor für Technische Informatik an der Universität Passau, schätzt die Verbreitung einer entsprechenden Philosophie im Bereich Schiene als „noch sehr früh" ein. „Ich beobachte, dass man zumindest infrastrukturseitig damit beginnt sich Gedanken über die Sicherheit der eingesetzten Komponenten zu machen." Die Prozesse dahinter seien aber noch ein ganz anderes Thema. Schließlich müsse bei jedem Modul, das einmal ins Feld gebracht wurde, garantiert werden, dass es nicht nur am Anfang sicher ist, sondern auch nach der Integration noch sicher bleibt – und das über den gesamten Lebenszyklus des Produkts und eines Systems hinweg. Katzenbeisser erläutert weiter: „Hier liegen die eigentlichen Herausforderungen: Im Patch-Management, im Schwachstellen-Management und in der Frage, wie ich Angriffe erkennen, darauf reagieren und mein System entsprechend optimieren kann." Katzenbeissers Einschätzungen zufolge ist die Branche „noch weit von einer finalen Lösung entfernt".

End-to-End-Sicherheit im IoRT

Laut der internationalen PwC-Befragung „Global Digital Trust Insights 2023" erwartet „jedes vierte deutsche Unternehmen (26 Prozent) einen signifikanten Anstieg der Attacken auf Infrastrukturen im Zusammenhang mit Industrial-Internet-of-Things (IIoT) und Betriebstechnologien (Operational Technology, OT)." Das System Schiene repräsentiert mit seinem Internet-of-Railway-Things (IoRT) eine ganz spezifische Ausprägung des IIoT. Eine großflächige Systemlandschaft, die Unmengen an Datenquellen und Prozessen vorhält: Von der reinen Informationsverarbeitung im Vertrieb und der Fahrgastinformation bis hin zu Echtzeitdaten etwa aus Signalanlagen, Stellwerken oder Zugsteuerungssystemen. Um in operativen Umgebungen sowohl land- als auch fahrzeugseitig durchgängige Überwachungsprozesse im Sinne maximaler Sicherheit herzustellen, müssen alle Systeme eine Sprache sprechen – und mit adäquaten Mechanismen, Protokollen und Anwendungen ausgestattet sein. Denn Sicherheit im Sinne einer übergeordneten DevSecOps-Strategie ist nur dann nahtlos gewährleistet, wenn Interoperabilität unter den Systemen herrscht. Für OEMs und Betreiber bedeutet das: Sie müssen sich auf Standards einigen, diese einhalten und die Schnittstellen zwischen Hardware- und Softwareumgebungen sicher integrieren. Damit tut sich eine besondere Herausforderung im Bereich Schiene auf, wenn es um digitale Sicherheit entlang des kompletten Lebenszyklus geht. Nicht nur die unterschiedlichen Systemwelten Informationstechnologie und operationale Technologie bringen deutlichen Harmonisierungsbedarf mit, die massive Heterogenität der Systeme, Module und damit auch Stakeholder ist ohne strukturierte Abstimmungsprozesse nicht möglich.

„Organisationen mit einer gelebten DevSecOps-Kultur haben (…) eine neunmal höhere Wahrscheinlichkeit, schwere Sicherheitsprobleme zu vermeiden."

Palo Alto Networks, „The State of Cloud Native Security Report 2022"

Altsysteme ohne Security-Nachweis

Gottfried Greschner, Gründer und Vorstandsvorsitzender von INIT, verfolgt die Entwicklung der Digitalisierung im Mobilitätssektor seit über 40 Jahren. Der IT-Konzern entwickelt, produziert, installiert und wartet Hardware- und Softwarelösungen für Verkehrsunternehmen – insbesondere auch für die lokale und regionale Schiene. „Da ist Cyber Security momentan ein Riesenthema", sagt Greschner.

BILD: INIT | KERSTIN GROH

OEM und IT-Zulieferer müssen mittlerweile strenge Cyber Security-Auflagen erfüllen – das betrifft sowohl Software als auch physische Netzwerkelemente

Große Fahrzeughersteller wie etwa Alstom oder Siemens forderten inzwischen einen Cybersecurity-Nachweis. Dabei spielten immer mehr Produktbereiche eine Rolle. „Für die Leit- und Steuerzentralen war die Sicherheit der IT-Umgebung seit jeher von großer Bedeutung. Nun ziehen die operativen Systeme auf Geräteebene nach." Greschners Einschätzung zufolge besteht inzwischen ein durchaus scharfes Bewusstsein dafür, dass Sicherheit bereits bei der Entwicklung eines Produktes geplant werden muss (security by design) und nicht als solitäre Lösung nachgerüstet werden sollte. „Man darf jedoch nicht vergessen, dass wir uns gerade in einer Übergangszeit befinden", so der Softwareexperte. „Es sind noch zahlreiche Altsysteme im Einsatz, die eben diese sicherheitsrelevanten Prozesse nicht abbilden." Durch die zunehmende Vernetzung der Altsysteme wird der Zwang für neue, gegen Attacken geschützte Systeme immer größer. Neben INIT-Chef Greschner sieht auch Stefan Katzenbeisser eine Aufgabe in der sicheren Integration sogenannter Legacy-Systeme. „Es ist klar, dass wir nicht alles, was da draußen im Feld steht, neu bauen oder neu konzipieren können", so Katzenbeisser. Für den Bestand müsse man Konzepte entwickeln, um das Sicherheitsniveau so weit wie möglich anzuheben. „Das wird nicht durchgängig möglich sein, aber man kann zum Beispiel Maßnahmen ergreifen wie einen erhöhten Zugangsschutz oder die Etablierung von Prüfroutinen zur Erkennung von Anomalien."

Stärkere Vernetzung von Safety und Security

Laut Katzenbeisser gibt es zwischen der klassischen funktionalen Sicherheit und IT-Security markante Unterschiede im Sicherheitsverständnis: „Die funktionalen Safety-Ingenieure gehen in der Regel davon aus, dass einmalig bewiesene Sicherheit für immer gültig ist." Im Bereich der IT-Security gäbe es dieses Denken nicht: „Selbst wenn ein Produkt einmal sicher ist, heißt das nicht, dass es am nächsten Tag oder in der Woche darauf immer noch als sicher angesehen werden kann." Hier wird von unterschiedlichen Prämissen ausgegangen, die gerade in komplexen Industrieumgebungen wie der Schiene im Sinne eines zukunftssicheren Safety- und Security-Verständnisses abgeglichen und kooperativer betrachtet werden müssen. So prognostiziert die bereits zitierte PwC-Befragung nicht nur eine steigende Cyber-Vulnerabilität operationaler Technologien, sie verweist zugleich auf die fundamentale Bedeutung einer Systemwelten übergreifenden Zusammenarbeit: Neben dem wachsenden Risiko von Angriffen auf IIoT und OT „erhöhen fehlende Synergien zwischen den IT- und OT-Teams das Risiko, da Angreifer:innen auf diese Weise viele blinde Flecken ausnutzen können." 38 Prozent der 242 befragten deutschen Unternehmen gaben laut PwC an, „dass unklare Verantwortlichkeiten zwischen beiden Fachbereichen zu den größten Herausforderungen gehören, um die Sicherheit an der IT-OT-Schnittstelle zu verbessern." Ein Lichtblick, gerade vor dem Hintergrund des eklatanten Fachkräftemangels: 64 Prozent der deutschen Führungskräfte gaben an, dass sie die Zusammenarbeit in ihren Teams von Mitte 2021 bis Mitte 2022 – dem Zeitpunkt der Befragung – verstärken konnten. Eine Entwicklung, die für die ausgesprochen heterogene Bahnbranche mit ihren zahlreichen Stakeholdern und Playern zwar eine

„(…) erhöhen fehlende Synergien zwischen IT- und OT-Teams das Risiko, da Angreifer:innen auf diese Weise viele blinde Flecken ausnutzen können."

PwC „Global Digital Trusts Insights 2023"

Herausforderung darstellt, die deshalb jedoch nicht weniger wichtig ist.

CENELEC: Neue europäische Cyber-Norm

Mit der CENELEC (CLS/TS) 50701 wurde im April 2023 eine neue Norm veröffentlicht, die Bahnbetreibern, Systemintegratoren und Produktlieferanten in Europa Leitlinien und Spezifikationen für das Management der Cyber-Sicherheit bietet – und damit in ihren Grundzügen das DevSecOps-Prinzip widerspiegelt. „Die Kernaussage der 50701 ist, dass man IT-Sicherheit in jeder Phase des Lebenszyklus eines Produkts sicherstellen muss", erläutert der Informatikwissenschaftler Katzenbeisser. „Das gilt von der Systemdefinition und der Spezifikation über das Ausrollen bis hin zum Betrieb. Daran wird man nicht mehr vorbeikommen." Die Ausgestaltung der neuen Leitlinie orientiert sich an den Maßgaben des in der EN 50126 definierten RAMS-Prozesses. Hinter RAMS verbergen sich die Spezifikation und der Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit von Bahnanwendungen. Das CENELEC-Papier fokussiert die Umsetzung dieser Maßgaben auf der Ebene digitaler Systeme. Katzenbeisser bringt die zentrale Botschaft der Cyber-Norm auf den Punkt: „Es geht nicht darum, nur punktuell Sicherheitsmaßnahmen zu ergreifen. Vielmehr muss Cyber-Sicherheit ein durchgängiger Prozess sein, der sich entlang des gesamten Design-Zyklus wiederfindet." Im Interesse eines Sicherheitsdenkens, das dem DevSecOps-Ansatz entsprechend sowohl technische als auch organisatorische Welten verbindet, hat CENELEC 50701 gute Karten, der Goldstandard für Cyber-Sicherheit in der Bahnbranche zu werden. ═