plenum.bluberries

veröffentlicht in
DER NAHVERKEHR

Informationssicherheit im Nahverkehr

7+8/2022

Informationssicherheit im Nahverkehr

Stand und aktuelle Entwicklungen

Achim Zeiner, Jan Albers; Frankfurt a. M.

Die Digitalisierung steigert die Bedeutung von Daten und Informationen für den Geschäftsbetrieb rasant. Immer mehr Daten werden digital übertragen, Entscheidungen zum Betrieb auf Basis von digitalen Informationen getroffen und Vorgänge von digitalen Systemen überwacht. Im Gleichschritt mit den auf der Hand liegenden Vorteilen steigen so aber auch die Risiken durch die zunehmende IT-Durchdringung der Geschäftsprozesse bei ausgeprägter Komplexität und vielen Abhängigkeiten.

Mehr und mehr IT-Anwendungen, -Infrastrukturen und Netzwerke gilt es auf Schwachstellen zu überwachen, welche durch zunehmend professionelle Angreifer ausgenutzt werden können. Darüber hinaus ist jede Technik, wie fortgeschritten sie auch sein mag, anfällig für Fehler und Defekte. Dies gilt auch und insbesondere für den ÖPNV.

Geltungsbereich aus Sicht der KRITIS

Um die Sektoren der kritischen Infrastruktur (KRITIS) zu schützen, hat der Gesetzgeber hier reagiert und Gesetze und Vorgaben entwickelt, wie zum Beispiel das IT-Sicherheitsgesetz. Dieses wurde 2015 verabschiedet und 2021 mit dem IT-Sicherheitsgesetz 2.0 neu aufgelegt. Über die bestehenden Pflichten für Betreiber kritischer Infrastrukturen hinaus enthält das IT-SiG 2.0 weitere Anforderungen wie zum Beispiel die unmittelbare Registrierung bei Erreichen der KRITIS-Schwellwerte sowie Systeme zur Angriffserkennung.

Der Gesetzgeber hat nach dem IT-Sicherheitsgesetz 2.0 im Jahr 2021 mit der BSI-Kritisverordnung 1.5 (teils BSI-Kritisverordnung 2.0 genannt) eine aktualisierte Verordnung beschlossen, die seit dem 1. Januar 2022 in Kraft ist. Die BSI-Kritisverordnung 1.5 enthält vor allem Änderungen zur Anpassung bisheriger Schwellenwerte von KRITIS-Anlagen in den bestehenden Sektoren sowie die Ergänzung und Anpassung, welche Anlagen als KRITIS-relevant gelten. Für ÖPNV-Betriebe ändert sich der Schwellenwert nicht. Diese zählen (bei Betrieb der entsprechenden Anlagenkategorien gemäß der BSI-KritisV) ab 125 Millionen unternehmensbezogenen Fahrgastfahrten pro Jahr zur kritischen Infrastruktur.

Gehört ein Unternehmen gemäß §8 der „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz" zur kritischen Infrastruktur im Sektor Transport und Verkehr, unterliegt es damit den Vorgaben des IT-Sicherheitsgesetzes.

Sie sind daher dazu verpflichtet, durch angemessene organisatorische und technische Vorkehrungen die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der relevanten Prozesse, Komponenten und Systeme der kritischen Infrastruktur zu gewährleisten.

Zur Erbringung dieser kritischen Dienstleistung im öffentlichen Personennahverkehr (ÖPNV) sind entsprechend der BSI KritisV folgende Anlagekategorien relevant:

- Schienennetz und Stellwerke des öffentlichen Straßenpersonenverkehrs (ÖSPV) – das schienengebundene Netz des ÖSPV einschließlich der zu diesen Strecken gehörenden Stellwerke und Beeinflussungsanlagen sowie der Fahrstromversorgung und Haltestellen,
- Leitzentrale des ÖSPV – eine Anlage oder ein System zur betreiberseitigen Überwachung und Steuerung des Verkehrs. Einschließlich der Systeme für die Fahrgastsicherheit und Fahrgastinformation, zur Personaldisposition und Fahrzeugdisposition, zur Fahrzeugbereitstellung, sowie der Flottentelematik, sofern eine Störung dieser Systeme das Potenzial aufweist, die kritische Dienstleistung zu beeinträchtigen, oder sie zur Evakuierung im Notfall kritisch sind.

Hierdurch liegt ein großer Fokus auf der digitalen Leittechnik im ÖPNV. Je nach Ausprägung des Verkehrsunternehmens können eine Vielzahl an Informationen in der Leitzentrale zusammenfließen, wie zum Beispiel Daten von Zugzielanzeigern, Lautsprechern, Notrufsäulen und von Kameras sämtlicher Haltestellen und Fahrzeuge, aber auch Daten von Rolltreppen, Aufzügen, Fahrausweisautomaten und auch die Beleuchtung in ein durchgängig vernetztes, multifunktionales Betriebsleitsystem. Neben der Überwachung und Lenkung des Zugverkehrs ermöglicht das Leitsystem so der Betriebsleitstelle auch die Kontrolle und Steuerung der technischen Anlagen auf den Haltestellen.

Aus der komplexen digitalen Vernetzung ergibt sich jedoch auch eine hohe Abhängigkeit hinsichtlich des Betriebes und der Sicherheit der eingesetzten Technik. Die Erkennung, Vorbeugung und Abwehr von Bedrohungen der Informationssicherheit wird damit zum vitalen Faktor für die ÖPNV-Betreiber.

Um diese Bereiche zu schützen, muss ein Informationssicherheitsmanagementsystem (ISMS), zum Beispiel nach den Vorgaben der ISO 27001 für das Unternehmen eingeführt werden. Dabei können die Branchenanforderungen an ein ISMS im Bereich des ÖPNV aus der VDV-Schrift 440 und der VDV-Mitteilung 4400 als Prüfungsgrundlage herangezogen werden.

Informationssicherheitsmanagementsystem

Die richtige Gestaltung eines ISMS ist kritisch, um das Unternehmen angemessen schützen zu können. Das ISMS ist ein Managementsystem mit verschiedenen Rollen und Aufgaben, welches auf einem kontinuierlichen Verbesserungsprozess basiert.

Homepageveröffentlichung unbefristet genehmigt für www.plenum.de. Rechte für einzelne Downloads und Ausdrucke für Besucher der Seiten genehmigt von DVV Media Group.

Das Ziel des ISMS ist die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität aller relevanten Informationen des Unternehmens zu schützen. Dazu werden Regeln, Verfahren und Methoden definiert (Leitlinie und Richtlinien) und risikoadäquate Schutzmaßnahmen festgelegt, um die Informationssicherheit im Unternehmen zu gewährleisten, zu steuern und zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Um eine erfolgreiche Umsetzung der Sicherheitsmaßnahmen aus dem ISMS sicherzustellen, ist eine Unterstützung durch die Fachbereiche und IT zu gewährleisten.

Die Vorteile eines erfolgreich umgesetzten ISMS erstrecken sich weit über die Erfüllung der Regulatorik hinaus. So können Risiken durch eine systematische Erfassung und Bewertung nachhaltig minimiert werden. Zudem können zukünftige Schadenkosten durch die erfolgreiche, zielgerichtete Behandlung von Risiken erheblich reduziert werden. Darüber hinaus wird durch diese Maßnahmen das Sicherheitsniveau des Unternehmens gestärkt, indem zum Beispiel Notfallpläne und BackUp-Tests vorgehalten und durchgeführt werden und so die Krisenfestigkeit erhöht wird. Durch die externe Überprüfung und Auditierung wird die Sicherheit und Verhältnismäßigkeit des ISMS garantiert. Darüber hinaus erhöht eine Zertifizierung das Vertrauen der Kunden in die Zuverlässigkeit der kritischen Dienstleistung.

Nutzung über ursprünglich angedachte Einsatzgebiete hinaus sinnvoll

Die meisten Betreiber der kritischen Infrastruktur haben ein ISMS für die kritischen Bereiche bereits umgesetzt, oder sind aktuell dabei. Doch auch außerhalb kritischer Infrastrukturen können schwere Risiko-Expositionen entstehen. So sind zahlreiche Unternehmen auch außerhalb der Sektoren teilweise existenziellen Risiken ausgesetzt, beispielsweise über die Infiltrierung von Ransomware.

Bei der Frage nach der weiteren Entwicklung und nach Systemen zum Schutz der Informationssicherheit ergeben sich folgerichtig zwei wesentliche Stoßrichtungen:

– die Ausweitung der bewährten Methoden des ISMS auf Risikogebiete außerhalb der typischen kritischen Infrastruktur, zum Beispiel im Bereich der Logistik- und Finanzsysteme und deren IT-Infrastrukturen,

Zum Autor

Achim Zeiner ist Senior Manager – Lead Consultant CIO-Advisory – bei der plenum AG Management Consulting in Frankfurt am Main. Er ist zudem zertifizierter ISMS-Manager/Lead Auditor nach ISO/IEC 27001. Zuvor war er mit diversen Aufgabenstellungen als Logistiker, IT-Leiter und CIO in diversen Branchen betraut.

Zum Autor

Jan Albers ist Senior Consultant bei der plenum AG Management Consulting in Frankfurt am Main. Er ist zertifizierter Information Security Officer nach ISO 27001. Er hat in seiner Funktion als Berater diverse Unternehmen im KRITIS-Umfeld und darüber hinaus bei der Einführung eines ISMS unterstützt.

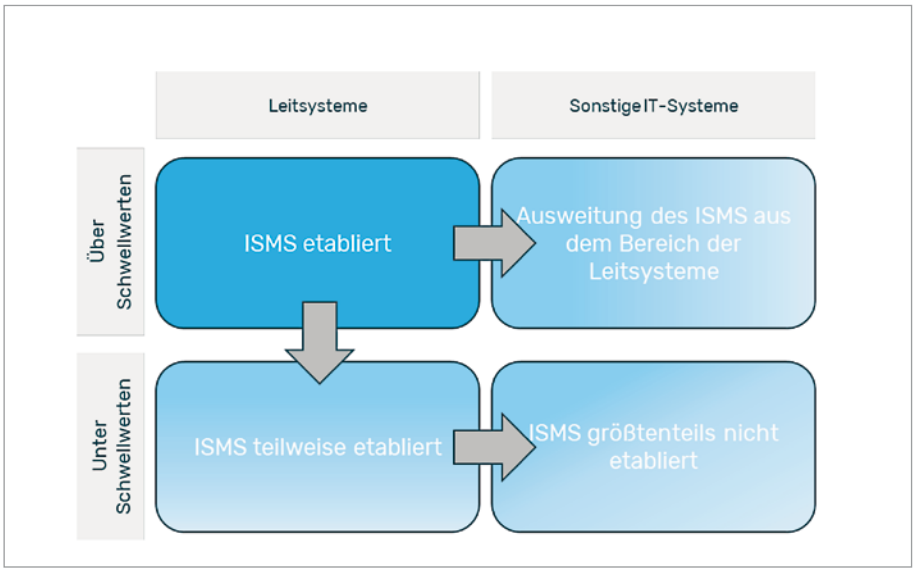

Abb. 1: Entwicklungspfade Einsatz ISMS.

Grafiken: plenum AG

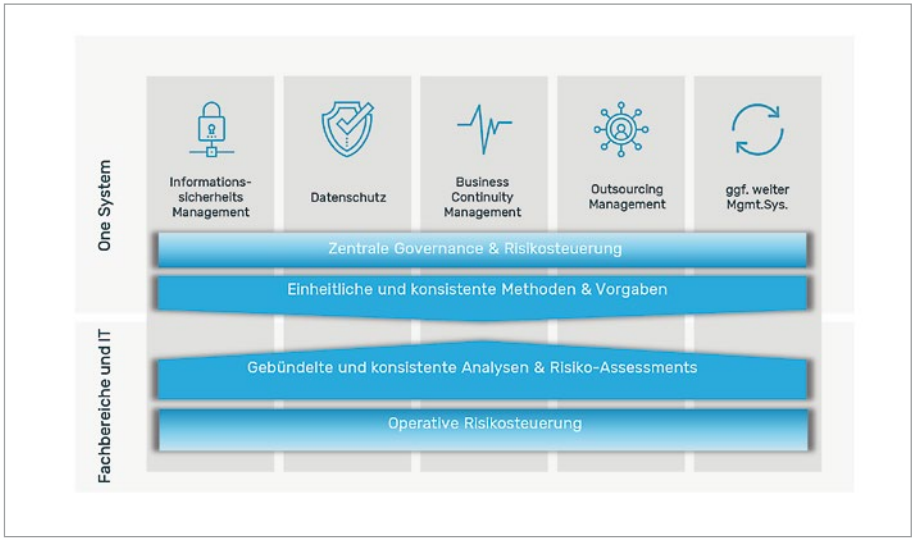

Abb. 2: „One System“.

Homepageveröffentlichung unbefristet genehmigt für www.plenum.de. Rechte für einzelne Downloads und Ausdrucke für Besucher der Seiten genehmigt von DVV Media Group.

– die Einführung und Nutzung praktikabler, an den Standardmethoden angelehnten schlanken Mechanismen „Lean ISMS“ bei „unterschwelligen“ Verkehrsunternehmen; das heißt Unternehmen unter den Schwellenwerten (125 Millionen Fahrgastfahrten pro Jahr). Auch hier ist eine ganzheitliche Sichtweise auf die Leitsysteme wie auch auf die sonstige IT sinnvoll.

Harmonisierung des ISMS mit Managementsystemen notwendig

Zur Steigerung der Effizienz sollte das ISMS zudem, im Sinne eines One System, mit weiteren Disziplinen, zum Beispiel BCM, synchronisiert werden. Es gilt, in den betroffenen Unternehmen dafür zu sorgen, dass diverse Managementsysteme im Bereich der Compliance miteinander integriert werden und synergetisch ihre jeweilige Wirkung entfalten. Die Breite der Vorgaben wird dabei von einer engen Taktung der Änderungen und Erweiterungen begleitet. Den Verantwortlichen für Disziplinen wie zum Beispiel Informationssicherheitsmanagement, Business Continuity Management und Datenschutz ist dabei bewusst, dass sie ähnliche Vorgaben und miteinander verbundene Ziele haben.

In einer Vielzahl der betroffenen Unternehmen finden sich in Ermangelung einer zentralen Instanz beziehungsweise einer übergreifenden Systematik („One System“) unterschiedliche Methoden und voneinander isolierte Vorgehensweisen. In der Konsequenz entsteht ein unbefriedigender Zustand von Redundanzen und Inkonsistenzen im Gesamtsystem mit unnötiger administrativer Belastung in der Steuerung der jeweiligen Compliance-Disziplin und auch in den Fachbereichen.

So werden beispielsweise geschäftliche Risiken sowohl im ISMS in der Methode der Schutzbedarfsfeststellung als auch im BCM in der Business-Impact-Analyse beurteilt. Oft erfolgt dies in unterschiedlichen Skalierungen und Bewertungsmaßstäben.

Über Zusammenhänge im Gesamtsystem wird so in der Regel keine Transparenz geschaffen. Die Fachbereiche werden von mehreren Seiten in die Pflicht genommen. Sie erleben unabgestimmte mehrfache Abfragen zu ähnlichen Sachverhalten. Dieser redundante Aufwand belastet die knappen Ressourcen und mindert die Akzeptanz für das Risikomanagement.

Zusammenfassung / Summary

Informationssicherheit im Nahverkehr

Vor dem Hintergrund einer sich weiter verschärfenden Sicherheitslage durch zunehmende Abhängigkeiten von digitalen Technologien und zusätzlich getrieben durch die aktuellen Ereignisse auf internationaler Ebene, ist die Weiterentwicklung der Informationssicherheit wichtiger denn je. Einerseits ist diese Weiterentwicklung geprägt von der Ausweitung der bewährten Methoden des ISMS auf Risikogebiete außerhalb der typischen kritischen Infrastruktur, zum Beispiel im Bereich der Logistik- und Finanzsysteme und deren IT-Infrastrukturen. Andererseits ist sie bei „unterschwelligen“ Verkehrsunternehmen geprägt durch die Einführung und Nutzung praktikabler und schlanker, an den Standardmethoden angelehnter Mechanismen wie „Lean ISMS“. Gleichzeitig bietet die Harmonisierung des ISMS mit weiteren Compliance-relevanten Managementsystemen im Sinne eines „One System“ vielfältige Potenziale und Synergien.

Information Security in Public Transport

In light of increasing exposure due to the growing dependency on digital technologies and current international events, the advancement of information security is more important than ever. On the one hand, this development is being driven by the expansion of proven methods of the Information Security Management System (ISMS) to risk areas beyond the scope of conventional critical infrastructure, for example to logistics and financial systems and their respective IT infrastructures. On the other hand, in the case of sub-threshold transport companies, it is characterised by the introduction and use of practicable and streamlined mechanisms based on standardised methods, such as “Lean ISMS”. At the same time, consolidating the ISMS and other compliance-relevant management systems into a single structure offers diverse potentials and synergies.

ANZEIGE

Jetzt noch an die **Messe-Ausgabe** denken …

Ausgabe 9/2022

zur InnoTrans + IAA TRANSPORTATION

ET: 08.09.22 • AS: 11.08.22

Buchen Sie jetzt Ihre Anzeige.

Kontakt: Andrea Kött • Tel. +49 (0)211 505-26536
andrea.koett@dvvmedia.com

Homepageveröffentlichung unbefristet genehmigt für www.plenum.de. Rechte für einzelne Downloads und Ausdrucke für Besucher der Seiten genehmigt von DVV Media Group.