# Gemeinsam gegen die Gefahr

Verkehrsinfrastruktur ist nicht nur durch Verfall bedroht. Cybersicherheit ist daher unerlässlich.

**Von Lars Schnieder**

Unsere Wirtschaft kann ohne Infrastrukturen nicht erfolgreich sein. Im letzten Jahr haben Sabotageakte gezeigt, wie verwundbar insbesondere kritische Infrastrukturen der Energieversorgung und des Verkehrs sind. Der Schutz solcher Infrastrukturen hat daher für den gesamten Verkehrssektor höchste Priorität. Doch was ist zu tun, damit im Fall eines Cyberangriffs nicht alle Prozesse stillstehen?

### Rechtsrahmen

Betreiber kritischer Infrastrukturen (Kritis) müssen ein Bewusstsein für die rechtlichen Grundlagen entwickeln. Die Europäische Union (EU) gibt für den Schutz kritischer Verkehrsinfrastrukturen einen umfassenden Rechtsrahmen vor. Dazu gehört die Richtlinie zum Schutz von Netzwerk- und Informationssystemen („NIS-Richtlinie"), die Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Europäischen Union definiert. Die EU-Richtlinien werden von den Mitgliedstaaten innerhalb vorgegebener Fristen in nationales Recht umgesetzt. Demgegenüber stehen Verordnungen, die unmittelbar in den Nationalstaaten geltende rechtliche Vorgaben darstellen. Ein Beispiel ist die Verordnung zum Aufbau einer Europäischen Agentur für Cybersicherheit (ENISA). In diesen übergeordneten Kontext reihen sich die Vorgaben zum Schutz kritischer Verkehrsinfrastrukturen in Deutschland ein. Mit der Novellierung des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme wurde nationales Recht an die europäischen Vorgaben angepasst.

In dieser Rechtssystematik nehmen Normen eine wesentliche Rolle ein. Als nichtstaatliche Regelsetzung konkretisieren sie den Maßstab des rechtlich Gebotenen für den Schutz kritischer Verkehrsinfrastrukturen gegen unberechtigte Zugriffe Dritter. Die Umsetzung normativer Vorgaben leistet so einen wichtigen Beitrag zur Rechtssicherheit für Hersteller und Betreiber dieser Infrastrukturen. Unabhängige Konformitätsbewertungsstellen bewerten die Einhaltung der Vorgaben dieser außergesetzlichen technischen Regelwerke und schaffen hierdurch Vertrauen – nicht nur bei den Herstellern und Betreibern, sondern unter anderem auch bei den Nutzern der Verkehrsinfrastrukturen.

Geltendes Recht konstituiert auch einen institutionellen Rahmen zur Gewährleistung der Cybersicherheit in allen EU-Mitgliedstaaten. Dieser Rahmen ist gekennzeichnet durch das aufeinander abgestimmte Zusammenwirken von Institutionen auf nationaler und europäischer Ebene.

In Deutschland nehmen verschiedene Einrichtungen eine fachliche Aufsicht über kritische Verkehrsinfrastrukturen wahr. Hierbei tritt das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bezug auf die Belange der Sicherheit informationstechnischer Systeme der Betreiber kritischer Verkehrsinfrastrukturen neben die eigentliche verkehrsträgerspezifische Fachaufsicht des Bundes oder der Länder. Die Steuerung und Orchestrierung dieser verwaltungsübergreifenden Zusammenarbeit bedarf für einen reibungslosen Ablauf in der Praxis allerdings noch einer Feinjustierung.

### Umsetzung

Innerhalb des rechtlichen und institutionellen Rahmens müssen Betreiber kritischer Verkehrsinfrastrukturen basierend auf einem risikoorientierten Ansatz ein stringentes Managementsystem etablieren, das die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung des Schutzes kritischer Verkehrsinfrastrukturen abdeckt. Die Betreiber ermitteln hierzu zunächst die auf die Cybersicherheit bezogenen Risiken ihres Betriebs, entwickeln eine systematische und bedarfsgerechte Risikokontrolle und führen diese ein. Ausgangspunkt dieser Vorgehensweise ist eine Analyse von Schwachstellen des Systems und eine hierauf aufbauende Analyse der aus möglichen Bedrohungen resultierenden Risiken. Die getroffenen Vorkehrungen sind regelmäßig auf ihre Wirksamkeit zu überprüfen. Dies geschieht beispielsweise über regelmäßige Ernstfallübungen oder Eindringungstests („Penetrationstests"). Bestenfalls wird durch die Vorkehrungen und durch die Behebung aufgedeckter Schwachstellen Cyberangriffen wirksam vorgebeugt.

### Ernstfall

Ein tatsächlicher Cyberangriff ist eine besondere Krisensituation für Betreiber kritischer Verkehrsinfrastrukturen, da sie oft sämtliche Unternehmensbereiche und eventuell auch viele verschiedene Stakeholder – beispielsweise alle Unternehmen auf einem Terminal und ihre Kunden – gleichzeitig betrifft.

Hier gilt es, auch in Bezug auf die konkrete Reaktion auf die Krise vorzusorgen, etwa durch die Kommunikation diverser Unternehmen miteinander. Wenn für den Umgang mit solchen Angriffen keine geeignete Vorgehensweise vorgegeben ist, hat dies schwerwiegende Folgen. In Eile und unter Stress können falsche Entscheidungen getroffen werden. Diese können dazu führen, dass die Öffentlichkeit falsch informiert wird, was wiederum massive Auswirkungen auf die Reputation der jeweiligen Organisation hat. Auch können Dritte durch kompromittierte sicherheitsrelevante Systeme und falsche Entscheidungen geschädigt werden und in späteren Rechtsverfahren Schadenersatz fordern.

Wird außerdem nach einem Cyberangriff nicht nach zuvor klaren und definierten Vorgaben gehandelt, kann dies dazu führen, dass wichtige Beweisspuren für die Aufklärung oder die spätere juristische Verfolgung unbeabsichtigt zerstört werden.

Cyberangriffe sind ein sich dynamisch veränderndes Kriminalitätsphänomen. Die Täter passen sich flexibel an technische und gesellschaftliche Entwicklungen an, agieren global und greifen dort an, wo es sich aus ihrer Sicht am meisten lohnt. Straftaten im digitalen Raum sind daher schnell zu analysieren, wirkungsvoll zu bekämpfen und die Täter aufzuspüren und zur Verantwortung zu ziehen. Dies stellt innerhalb der multilateralen Struktur der Europäischen Union sowie der föderalen Struktur der Bundesrepublik Deutschland eine Herausforderung dar.

Als Zentralstelle der deutschen Polizei übernimmt das Bundeskriminalamt im Bereich der Cybercrime-Bekämpfung unter anderem diverse koordinierende Aufgaben im Rahmen der nationalen Zusammenarbeit aller Beteiligten.

### Ausblick

Die Digitalisierung erhöht die Möglichkeit unberechtigter Zugriffe auf Datensysteme und damit auch die Verwundbarkeit kritischer Infrastrukturen. Um dem entgegenzutreten, rücken künftig der Wissensaufbau und der Erfahrungstransfer im Verkehrssektor in den Vordergrund. Hierbei sind mit Herstellern, Betreibern, Behörden und der Wissenschaft alle Beteiligten gefordert, sich auszutauschen und ihren Beitrag zu leisten. *(zp/fh)*

Nachgefragt

## *Systematisches Engineering als Schlüssel*

**Lars Schnieder** ist Geschäftsführer der ESE Engineering und Software-Entwicklung GmbH in Braunschweig, lehrt an zwei Hochschulen und ist Sachverständiger für Zugsicherung. Er kennt sich aus mit kritischen Infrastrukturen, besonders im Bahnbereich.

**DVZ: Herr Schnieder, welche sind die größten Risiken für den Schienenverkehr?**
**Lars Schnieder:** Die Bahn ist physisch am verwundbarsten etwa durch Kupferkabelklau aufgrund ihrer flächenmäßig weit verteilten und darum schwer zu schützenden Infrastruktur. Die Möglichkeiten, IT-Systeme anzugreifen, sind ebenfalls erheblich, schon durch die hohe Zahl der Mitarbeitenden etwa bei der DB AG. Bei der Anfälligkeit für Cyber Crime ist der Mensch das erste schwache Glied der Kette.

**Wie lässt sich die Gefährdung eindämmen?**
Durch systematisches Engineering. Da die Sanierung des Netzes sowieso bis 2040 geplant ist, bietet sich eine gute Möglichkeit, im Zuge der ´Digitalen Schiene´ von Beginn an resiliente Systeme zu implementieren. Zudem ist eine konsequente Vorsorge in der Organisation auf Basis von Schulungen und Weiterbildungen sowie der Kontrolle, dass alle Regeln konsequent umgesetzt werden, erforderlich. Hier ist die Bahn schon deutlich weiter als noch vor fünf Jahren.

**Ihr Unternehmen digitalisiert und automatisiert mit IT-Systemen unter anderem den Bahnsektor und den öffentlichen Verkehr. Wie machen Sie ihre Programme widerstandsfähig gegen Angriffe?**
Einerseits schützen wir unsere Entwicklungsumgebung, andererseits identifizieren wir mit unseren Kunden gemeinsam mögliche Bedrohungen und prüfen unsere Produkte entsprechend auch mit Penetration-Tests. Das größte Risiko für ESE als Unternehmen sind Ransomware-Attacken, die klassische Büroarbeiten betreffen.

**Wie gehen Sie selbst mit Risiken um?**
Ich bin überzeugter Bahnnutzer, fahre Fahrrad mit Helm und besitze ein Auto mit diversen Assistenzsystemen – ich vermeide also Risiken. Beruflich wie privat bin ich überzeugt, dass Technik hilft, Gefährdungen zu vermeiden. Als Geschäftsführer der ESE bin ich getrieben von der Vision Zero: Niemand soll durch einen Verkehrsunfall ums Leben kommen. Ein Schlüssel hierzu ist der zielgerichtete Einsatz von Technik. Ich bin dankbar, mich jeden Tag mit großer persönlicher Begeisterung für die Projekte unserer Kunden engagieren zu dürfen, die immer auch etwas mit Risikominimierung zu tun haben. *(zp/fh)*

R·SIKO