Zehn. Minuten

Nr. 05 | 2026

ZIRP. Zukunftsinitiative Rheinland-Pfalz

Unsere Infrastruktur – sicher in die Zukunft

Cyberangriffe, marode Straßen- und Schienennetze, geopolitische Abhängigkeiten von großen Digitalkonzernen aus Übersee: Die Frage, wie krisenfest Deutschlands Infrastruktur wirklich ist, war selten so dringlich wie heute. Unter dem Titel „Unsere Infrastruktur – sicher in die Zukunft" lud die ZIRP gemeinsam mit der BBT-Gruppe am 25. Juni 2026 in den Albertus-Magnus-Saal des Krankenhauses der Barmherzigen Brüder in Trier ein. Moderiert von Lena Reuter diskutierten Experten aus Gesundheitswesen, Mobilität, Zivilgesellschaft und Finanzwirtschaft, wie sich kritische Infrastrukturen gegen Cyberrisiken, Systemausfälle und digitale Abhängigkeiten wappnen lassen und warum digitale Souveränität am Ende oft doch günstiger ist als die Bequemlichkeit, Infrastruktur großer Techkonzerne aus den USA oder China zu nutzen.

Verantwortung lässt sich delegieren, Haftung nicht

Dr. Frank Zils, Geschäftsführung Personal, christliche Unternehmenskultur und Unternehmenskommunikation der BBT-Gruppe, eröffnete in seinem Grußwort den fachlichen Teil mit einem Blick auf die besondere Verantwortung des Gesundheitswesens. Anschließend setzte Guido Jost, Leiter des Geschäftsfelds HealthSec Advisory und Informationssicherheitsbeauftragter des privaten Trägers, den Ton für seinen Vortrag: „Verantwortung kann man delegieren. Haftung nicht." Anhand von Beispielen wie vernetzten Wearables und robotergestützter Chirurgie zeigte Jost, wie eng KI-Einsatz, Cybersicherheit und Produkthaftung im Gesundheitswesen mittlerweile verzahnt sind. Ein wachsender Flickenteppich aus Regulatorik, wie dem AI Act, der neuen Medizinprodukteverordnung, der neuen EU-Richtlinie NIS-2, dem KRITIS-Dachgesetz und dem Data Act, zwinge Unternehmen zu komplexen integrierten Sicherheits- und KI-Managementsystemen. Sein Befund: Das eigentliche Risiko liege selten in der Technologie selbst, sondern in mangelnder Governance: KI-Projekte entstünden isoliert, Cybersecurity werde separat gedacht, Regulatorik erst nachträglich ergänzt.

„Das Problem ist nicht mangelnde Technologie. Das Problem ist mangelnde Integration."

Guido Jost
Leiter des Geschäftsfelds HealthSec Advisory und Informationssicherheitsbeauftragter

Verwundbare Infrastruktur im Verkehrssektor

Henrik Behrens, Geschäftsführer und Leiter Strategische Projekte & Partnerschaften sowie Hochschulbeauftragter des Future Mobility Labs bei der Transdev Verkehr GmbH, rückte anschließend die Abhängigkeit kritischer Mobilitätsleistungen von funktionierender IT, Energieversorgung und Telekommunikation in den Fokus. Mit Verweis auf den DB-InfraGO-Netzzustandsbericht 2025 verdeutlichte er, dass 106 Milliarden Euro investiert werden müssten, um Schienenanlagen zu erneuern. Rheinland-Pfalz liegt hier beim Netzzustand bundesweit nur auf Platz 14 von 16. Die Summe der erneuerungsbedürftigen Anlagen ist beachtlich: mehr als 2.000 Stellwerke sind in Stand zu setzen. Hier steht der Bund in der Verantwortung.

An technischen Defiziten erklären sich die meisten Störfälle jedoch nicht: 68 Prozent der erfolgreichen Cyberangriffe gingen auf den Faktor Mensch zurück, die durchschnittliche Zeit bis zur Erkennung eines Vorfalls im Transportsektor liegt bei 241 Tagen. Als warnendes Beispiel nannte Behrens chinesische Yutong-Elektrobusse, die in Norwegen im öffentlichen Personennahverkehr eingesetzt werden. Dabei wies die örtliche Verkehrsbehörde aktive Fernzugriffsmöglichkeiten durch den Hersteller nach, die Busse könnten also jederzeit per Knopfdruck aus der Ferne funktionsunfähig gemacht werden. Sicherheit sei kein rein technisches, sondern vor allem ein organisatorisches Thema aus Prozessen, Entscheidungen und klaren Verantwortlichkeiten, so Behrens.

> *„Nur durch Kollaboration wird es gelingen, nach vorne zu kommen."*
>
> **Henrik Behrens**
> Geschäftsführer und Leiter Strategische Projekte & Partnerschaften sowie Hochschulbeauftragter des Future Mobility Labs bei der Transdev Verkehr GmbH

Schritte in die digitale Unabhängigkeit

Björn Staschen, Mitgründer von Save Social – Networks For Democracy und Mitinitiator des Digital Independence Day, plädierte eindringlich für digitale Souveränität als Voraussetzung für den Fortbestand der Demokratie. Zum Einstieg illustrierte Staschen, wie Zivilistinnen und Zivilisten im Gaza-Konflikt, die Social-Media-Plattformen nutzten, durch gezielte Ortung und Datenauswertung zum leichten Ziel für Drohnenabschüsse geworden seien. Die Konzentration von Infrastruktur, Daten und Ortungsmöglichkeiten in den Händen weniger Tech-Konzerne berge hohe gesellschaftliche und geopolitische Risiken. Als präventive und „gesellschaftsschonende" Maßnahme stellte Staschen den Digital Independence Day vor, der seit Februar 2025 mehr als 200 Organisationen und Veranstaltungen mobilisiert hat: An jedem ersten Sonntag im Monat soll mit einfachen „Wechselrezepten" mit einem Dienst auf die „gute Seite" gewechselt werden, z.B. von X zu Mastodon, von Google Maps zu OpenStreetMap, von WhatsApp zu Signal.

> *„So viel Geld wie die Hyperscaler kann allein niemand aufbringen – deshalb müssen wir zusammenarbeiten."*
>
> **Björn Staschen**
> Mitgründer von Save Social – Networks For Democracy und Mitinitiator des Digital Independence Day

Dabei kann der Wechsel einfach sein. Mit der +1-Strategie soll der Umstieg durch parallele Nutzung alternativer Plattformen erleichtert werden, bis eine kritische Masse den Wechsel trägt. Seine Kriterien für gute Alternativen: mehr Datenschutz, mehr Wahlfreiheit, weniger Lock-in-Effekte, die Nutzende auf der eigenen Plattform halten sollen. Als positives Beispiel nannte er unter anderem Schleswig-Holstein, das als erstes Bundesland

konsequent auf die datenschutzfreundlichere Alternative Nextcloud mit Hauptsitz in Stuttgart statt auf US-Cloud-Anbieter umgestellt hat.

Digitale Souveränität im Zahlungsverkehr

Alexander Schaubeck, stellvertretender Verbandsgeschäftsführer und Leiter Geschäftsbereich Strategie und Gremien, Sparkassenverband Rheinland-Pfalz, schlug die Brücke zur Finanzinfrastruktur. Die Aufrechterhaltung des Zahlungsverkehrs sowie der Bargeldversorgung sei in einer Krise sehr wichtig, damit Wirtschaft und Handel weiter funktionieren. Eine stabile Infrastruktur schafft darüber hinaus Sicherheit.

Auch wenn inzwischen mehr als die Hälfte aller Handelstransaktionen bargeldlos ablaufen, bleibt Bargeld gerade im Krisenfall unverzichtbar, weil es auch bei technischen Störungen oder bei Stromausfällen funktioniert. Das bestätigt auch eine Bevölkerungsbefragung der Deutschen Bundesbank: 95 % der Befragten unterstreichen die Wichtigkeit des Bargelds im Krisenfall. Sparkassen sorgen regional mit eigenen Notfallplanungen und einem Business-Continuity-Management vor, um die Bargeldversorgung auch im Krisenfall sicherzustellen – in engem Austausch mit anderen Unternehmen der kritischen Infrastruktur, wie beispielsweise den örtlichen Energieversorgern oder Geld- und Wertdienstleistern.

Zur Stärkung der digitalen Souveränität im Zahlungsverkehr treiben Sparkassen gemeinsam mit vielen weiteren europäischen Banken und Finanzdienstleistern im Rahmen der European Payments Initiative (EPI) den digitalen Zahlungsdienst WERO voran. Mit dieser europäischen Alternative zu weit verbreiteten US-amerikanischen Zahlungsdienstleistern sollen Zahlungen in Echtzeit sowohl zwischen Privatpersonen als auch im Handel und bei Kommunen einfach und nach europäischen Datenschutzstandards sicher möglich sein. Bereits über 8,4 Millionen Registrierungen in Deutschland und mehr als 55 Millionen in Europa zeigen das wachsende Interesse der Menschen an europäischen Zahlungslösungen. Auch das bestätigt eine Bundesbank-Befragung: Fast zwei Drittel der Befragten halten mehr Autonomie im europäischen Zahlungsverkehr für notwendig.

> *„Wachsende geopolitische Risiken machen eine resiliente, stabile Finanzinfrastruktur wichtiger denn je. Digitale Souveränität und die Kommunikation und Vernetzung aller Partner der kritischen Infrastruktur sind deshalb entscheidende Zukunftsfaktoren."*
>
> **Alexander Schaubeck**
> Stellvertretender Verbandsgeschäftsführer und Leiter Geschäftsbereich Strategie und Gremien, Sparkassenverband Rheinland-Pfalz

Nur durch Kooperation kann es vorangehen

Die abschließende Gesprächsrunde drehte sich im Wesentlichen um eine zentrale Frage: Welcher Weg ist langfristig kostspieliger, eine souveräne, initial teurere Lösung oder der Zustand der Abhängigkeit von US-amerikanischen oder chinesischen Tech-Konzernen? Einigkeit bestand darin, dass sich die Kosten für Sicherheit und Resilienz kaum von einzelnen Unternehmen allein stemmen lassen. Als Lösungsmöglichkeit wurden dabei verschiedene Modelle und Anwendungsszenarien diskutiert: von

eigenen, souveränen anwendungsspezifischen KI-Lösungen und dezentral betriebenen Rechenzentren bis hin zur Frage, wie Unternehmen sich gegenseitig absichern können, ohne in vollständige Abhängigkeit von Big-Tech aus Übersee zu geraten. Als Beispiel für Resilienz diente die Gegenüberstellung von Batteriespeicher und Diesel-Notstromaggregat. Beide Technologiegenerationen ergänzen sich eher, als dass eine die andere vollständig ersetzt, gerade wenn es zum Krisenfall durch Naturkatastrophen, Cyberangriffe oder menschliches Versagen kommen sollte.

Für mehr digitale Souveränität und Resilienz sollte man bereits bei der jungen Generation ansetzen und in den Bildungsanstalten mehr digitale Aufklärung betreiben, so die Diskussion. Anstatt Heranwachsende der Sogkraft der Algorithmen von Big-Tech-Konzernen auszusetzen, könne man eigene dezentral agierende Systeme etablieren. Beispielsweise ein eigens von Lehrkräften und Schülerinnen und Schülern programmiertes internes Netzwerk, ähnlich wie TikTok, in dem in einem sicheren Umfeld digitale Kompetenzen geschult werden können. Dezentrale Systeme passten eigentlich hervorragend zum föderalen System Deutschlands, man müsse diese Stärke nur konsequenter nutzen.

Der Dialog der unterschiedlichen gesellschaftlichen und wirtschaftlichen Institutionen zeigte sehr deutlich, dass Resilienz in der Diversität aller gesellschaftlichen Kräfte liegt und in deren Fähigkeit zur Zusammenarbeit. Thematisch sind sektorübergreifende Kooperationen also nicht als Kür, sondern als Voraussetzung für eine resiliente Infrastruktur der Zukunft zu begreifen. Diese Kooperationsfelder sichtbar zu machen ist Wesenskern der ZIRP und wird auch eine wichtige Rolle in zukünftigen Veranstaltungen spielen.

Impressum

Zukunftsinitiative
Rheinland-Pfalz
(ZIRP) e.V.
Auf der Bastei 3
55131 Mainz
Tel.: 0 61 31 – 16 56 87
Fax: 0 61 31 – 16 25 54
E-Mail: mail@zirp.de
www.zirp.de

Verantwortlich:
Dr. Christiane Liesenfeld,
Geschäftsführerin
Vorsitzende:
Dr. Katja Scharpwinkel
Stv. Vorsitzender:
Ministerpräsident
Gordon Schnieder

Redaktion:
Max Helmes
Layout & Satz:
Claudia Kut

Bildnachweise:
© ZIRP
© Adobe Stock
© Florian Biege