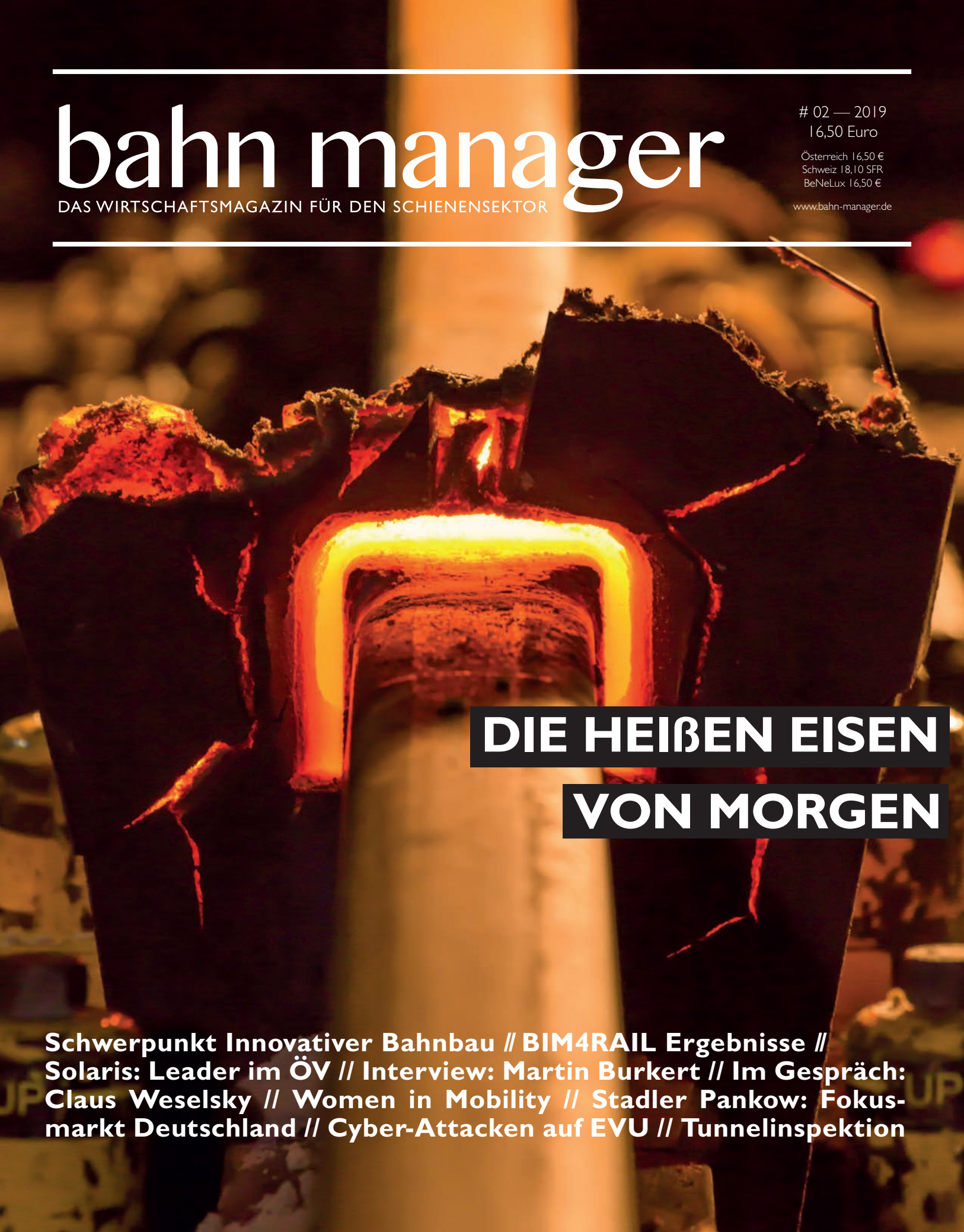
# bahn manager

DAS WIRTSCHAFTSMAGAZIN FÜR DEN SCHIENENSEKTOR

# 02 — 2019
16,50 Euro

Österreich 16,50 €
Schweiz 18,10 SFR
BeNeLux 16,50 €

www.bahn-manager.de



# DIE HEIßEN EISEN VON MORGEN

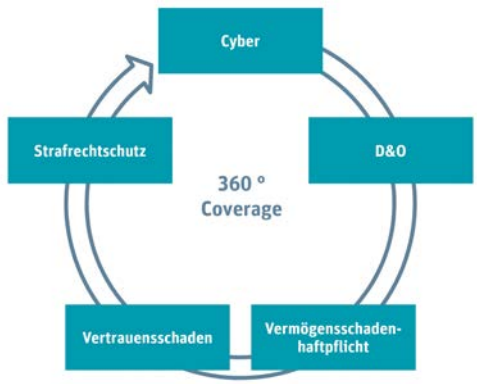
**Schwerpunkt Innovativer Bahnbau // BIM4RAIL Ergebnisse // Solaris: Leader im ÖV // Interview: Martin Burkert // Im Gespräch: Claus Weselsky // Women in Mobility // Stadler Pankow: Fokusmarkt Deutschland // Cyber-Attacken auf EVU // Tunnelinspektion**

# CYBER-ATTACKEN AUF EISENBAHNUNTERNEHMEN

WURDE IHR UNTERNEHMEN BEREITS ZIEL EINES ANGRIFFS? ZU DEN MITTLERWEILE ETABLIERTEN VERSICHERUNGEN FÜR DIE HAFTUNG VON UNTERNEHMEN UND DEREN LEITENDEN ANGESTELLTEN GEHÖREN INSBESONDERE DIE D&O-VERSICHERUNG, OFTMALS AUCH DIE STRAFRECHTS-SCHUTZVERSICHERUNG UND DIE VERTRAUENSSCHADENVERSICHERUNG.

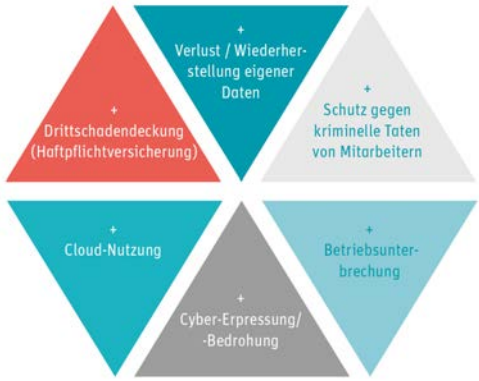
Einige Unternehmen haben zusätzlich eine sogenannte Vermögensschadenhaftpflichtversicherung abgeschlossen. Doch obwohl das Thema Cyber-Angriffe nahezu täglich in der Presse auftaucht, halten sich Unternehmen mit der Implementierung einer entsprechenden Versicherung noch zurück. „Dies liegt möglicherweise an den Erfahrungen der Vergangenheit, als Cyber-Versicherungskonzepte noch mit mehr Ausschlüssen als Einschlüssen auf dem Markt angeboten wurden“, erläutert Dr. Christian Heidersdorf, Geschäftsführer der DVA. „Mittlerweile gibt es auf dem Markt aber sehr gute Wordings, die den Risiken der Branche zunehmend gerecht werden. Eine gute Empfehlung ist es, das Unternehmen ganzheitlich zu betrachten und den Versicherungsschutz schnittstellenübergreifend ineinander zu verzahnen, damit ein 360-Grad-Versicherungsschutz erreicht wird. Nur so kann ein umfassender Versicherungsschutz gewährleistet werden“.

*Financial Lines Risiken*




Michael Fabian, Eisenbahnjurist beim Verband Deutscher Verkehrsunternehmen e. V. (VDV), fügt hinzu, dass bei diesem verhältnismäßig jungen Thema bei den Mitgliedsunternehmen des VDV Beratungsbedarf besteht. „Deswegen haben wir die Experten der DVA und unsere Mitgliedsunternehmen an einen Tisch geholt, über die Risiken speziell im Bereich der Verkehrsunternehmen diskutiert und gemeinsam Lösungen entwickelt.“

- Zum Inhalt: Die Cyber-Versicherungskonzepte unterscheiden sich in vielen Einzelheiten, bieten aber in der Regel eine Kombination aus einer Drittschaden- (Haftpflicht-) und einer Eigenschadendeckung, die durch diverse Zusatzbausteine ergänzt werden kann. Gefahrenpotenziale resultieren etwa aus der zunehmenden Di-




gitalisierung der Arbeitswelt (z. B. mobiles Arbeiten), der immer schnelleren Veränderung der IT-Landschaft, der Globalisierung, der internationalen Vernetzung, dem Outsourcing, der Cloud-Nutzung und natürlich aus dem generellen Anstieg der Cyber-Kriminalität (z. B. Erpressung).

- Drittschadendeckung (Haftpflicht): Versicherungsschutz für ein Unternehmen besteht, wenn es aufgrund eines Cyber-Vorfalls von Dritten wegen eines Vermögensschadens erstmals auf Schadenersatz in Anspruch genommen wird. Diese Schäden können aus der Beschädigung der IT-Systeme entstehen, oder es kann sich um Datenschutzvorfälle handeln.
- Eigenschadendeckung: Versicherungsschutz für ein Unternehmen besteht bei nachteiliger Veränderung, Nichtverfügbarkeit oder Verlust von versicherten Daten und Programmen durch Cyber-Angriffe oder Datendiebstahl. Ebenfalls kann eine Betriebsunterbrechung in Folge eines Cyber-Vorfalls mitversichert werden.
- Zusätzliche Dienstleister: Bei der Risiko-Ermittlung und insbesondere im Schadenfall bieten die Versicherer den Zugriff auf hochspezialisierte Dienstleister, die den Kunden unterstützen. Dies betrifft alle Bereiche des Managements eines Cyber-Vorfalls von der Beendigung des Angriffs über die Aufarbeitung der Ursachen bis zur Abwicklung der Schadenfälle. Ergänzt werden die IT-Dienstleistungen durch Rechts- und PR-Beratung.

Darüber hinaus kann die Deckung durch Bausteine erweitert werden.

Betroffen sind nicht nur große internationale Unternehmen, sondern in hohem Maße auch kleine und mittelständische Unternehmen. Denn diese erweisen sich im Vergleich zu Großunternehmen mit entsprechend üppigem IT-Sicherheitsbudget als die leichter angreifbaren Ziele (auch Einbrecher wählen bevorzugt weniger gesicherte Gebäude).

Weitere Brisanz erhält die Thematik durch das Inkrafttreten der EU-Datenschutz-Grundverordnung (DSGVO) im Mai 2018. Diese auferlegt den Unternehmen neben einer Vielzahl von Sicherheitsstandards und Maßnahmen auch Informationspflichten und sanktioniert Verstöße scharf mit hohen Bußgelddrohungen.

Zusammenfassend lässt sich festhalten, dass jede Unternehmensleitung gut beraten ist, sich intensiv mit dem Thema Cyber-Sicherheit auseinanderzusetzen.

„Neben der Verbesserung der eigenen IT-Infrastruktur können unvermeidbare Restrisiken einschließlich der spezifischen, im Ereignis- bzw. Schadenfall erforderlichen IT-Dienstleistungen (professionelle Eliminierung von Schadsoftware und Datenrettung) kurzfristig mit einer Versicherungslösung abgedeckt werden“. ═

## Schadenbeispiele

**Veröffentlichung von Kundendaten mit Schadenersatzpflichten**
- z. B. nach DSGVO

**Betriebsunterbrechung durch Systemausfall z. B.**
- Leitstelle
- Stromversorgung
- Disposition

**Erpressungsszenario**
- "Wanna Cry" --> Fahrgastinformation
- Datenverlust --> Kundendaten
  --> Wartungssoftware (z. B. Schienenfahrzeuge)
  --> Datensätze ECM

**DR. JUR. CHRISTIAN HEIDERSDORF**

Seit 2011 Mitglied der Geschäftsführung der DVA und seit 2014 deren Sprecher. Zuvor war der promovierte Jurist als Rechtsanwalt sowie in unterschiedlichen Leitungsfunktionen im DB-Konzern tätig.

**MICHAEL FABIAN**

Er ist Fachbereichsleiter Eisenbahnrecht beim VDV. Er war zuvor für den ehemaligen BDE Bundesverband Deutscher Eisenbahnen, Kraftverkehre und Seilbahnen e. V. tätig.

FOTOS / GRAFIKEN: DVA / VDV