

}essentials{

Lars Schnieder

Schutz Kritischer Infrastrukturen im Verkehr

Security Engineering als
ganzheitlicher Ansatz

3. Auflage



Springer Vieweg

essentials

essentials liefern aktuelles Wissen in konzentrierter Form. Die Essenz dessen, worauf es als „State-of-the-Art“ in der gegenwärtigen Fachdiskussion oder in der Praxis ankommt. *essentials* informieren schnell, unkompliziert und verständlich

- als Einführung in ein aktuelles Thema aus Ihrem Fachgebiet
- als Einstieg in ein für Sie noch unbekanntes Themenfeld
- als Einblick, um zum Thema mitreden zu können

Die Bücher in elektronischer und gedruckter Form bringen das Fachwissen von Springerautor*innen kompakt zur Darstellung. Sie sind besonders für die Nutzung als eBook auf Tablet-PCs, eBook-Readern und Smartphones geeignet. *essentials* sind Wissensbausteine aus den Wirtschafts-, Sozial- und Geisteswissenschaften, aus Technik und Naturwissenschaften sowie aus Medizin, Psychologie und Gesundheitsberufen. Von renommierten Autor*innen aller Springer-Verlagsmarken.

Weitere Bände in der Reihe <http://www.springer.com/series/13088>

Lars Schnieder

Schutz Kritischer Infrastrukturen im Verkehr

Security Engineering als
ganzheitlicher Ansatz

3. Auflage

 Springer Vieweg

Lars Schnieder
ESE Engineering und Software-Entwicklung
GmbH, Braunschweig, Deutschland

ISSN 2197-6708

ISSN 2197-6716 (electronic)

essentials

ISBN 978-3-658-33650-9

ISBN 978-3-658-33651-6 (eBook)

<https://doi.org/10.1007/978-3-658-33651-6>

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2018, 2020, 2021

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jedermann benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des jeweiligen Zeicheninhabers sind zu beachten.

Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag, noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Planung/Lektorat: Alexander Grün

Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.

Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Was Sie in diesem *essential* finden können

- Definition von Begriffen und Schutzzielen Kritischer Verkehrsinfrastrukturen
- Darstellung grundlegender für das Verständnis des Angriffsschutzes relevanter Modelle
- Eine Darstellung des institutionellen Rahmens der Absicherung der IT-Sicherheit Kritischer Verkehrsinfrastrukturen
- Eine Motivation zum Schutz Kritischer Verkehrsinfrastrukturen aus dem Rechtsrahmen heraus
- Eine Darstellung technischer und organisatorischer Maßnahmen sowie Maßnahmen des physischen Zugriffsschutzes

Vorwort

Ein Leben ohne Smartphone und Tablet ist für viele von uns kaum noch vorstellbar.

„Always on“ – uneingeschränkte Konnektivität gehört mittlerweile zu den Grundbedürfnissen unserer Gesellschaft. Es gibt kaum noch einen Bereich unseres Lebens, der nicht von informationstechnischen Systemen abhängig ist. Dies gilt auch für städtische und großräumige Verkehrsinfrastrukturen. Technologietrends und neue Bedrohungsszenarien verstärken für Hersteller und Betreiber von Verkehrsinfrastrukturen die Notwendigkeit, sich den Herausforderungen des Schutzes gegen unberechtigten Zugriff Dritter systematisch zu widmen. Bedrohungen aus dem Internet dürfen die für die Lebensfähigkeit unserer Gesellschaft und Wirtschaft essenzielle Software in den Systemen der Verkehrssteuerung nicht manipulieren.

Sowohl auf europäischer Ebene als auch im nationalen Recht wurden in den letzten Jahren erweiterte Vorgaben für Kritische Verkehrsinfrastrukturen eingeführt. Der Gesetzgeber verpflichtet Betreiber Kritischer Verkehrsinfrastrukturen, angemessene technische, physische und organisatorische Vorkehrungen zur Absicherung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Verkehrsinfrastrukturen zu treffen. Erklärtes Ziel ist es hierbei, Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der in Verkehrssystemen eingesetzten informationstechnischen Systeme, Komponenten oder Prozesse zu vermeiden.

Dieses *essential* skizziert den Rechtsrahmen des Schutzes Kritischer Verkehrsinfrastrukturen und zeigt auf, welche Verkehrsanlagen einer besonderen Absicherung gegen Angriffe von außen bedürfen. Des Weiteren wird in diesem *essential* der umfassende nationale und europäische institutionelle Rahmen zur Absicherung der IT-Sicherheit dargestellt. Abschließend wird ein ganzheitlicher