

**Dimitri Tsiganovski**

## Cyberkriminalität in der Schifffahrt

Operative und wirtschaftliche Auswirkungen eines  
Cyberangriffs auf eine mittelständische Reederei

Projektarbeit

# BEI GRIN MACHT SICH IHR WISSEN BEZAHLT



- Wir veröffentlichen Ihre Hausarbeit, Bachelor- und Masterarbeit
- Ihr eigenes eBook und Buch - weltweit in allen wichtigen Shops
- Verdienen Sie an jedem Verkauf

Jetzt bei [www.GRIN.com](http://www.GRIN.com) hochladen  
und kostenlos publizieren



## **Bibliografische Information der Deutschen Nationalbibliothek:**

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

Dieses Werk sowie alle darin enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsschutz zugelassen ist, bedarf der vorherigen Zustimmung des Verlanges. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen, Auswertungen durch Datenbanken und für die Einspeicherung und Verarbeitung in elektronische Systeme. Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

## **Impressum:**

Copyright © 2018 GRIN Verlag  
ISBN: 9783346024664

## **Dieses Buch bei GRIN:**

<https://www.grin.com/document/497916>

**Dimitri Tsiganovski**

## **Cyberkriminalität in der Schifffahrt**

**Operative und wirtschaftliche Auswirkungen eines Cyberangriffs auf eine mittelständische Reederei**

## **GRIN - Your knowledge has value**

Der GRIN Verlag publiziert seit 1998 wissenschaftliche Arbeiten von Studenten, Hochschullehrern und anderen Akademikern als eBook und gedrucktes Buch. Die Verlagswebsite [www.grin.com](http://www.grin.com) ist die ideale Plattform zur Veröffentlichung von Hausarbeiten, Abschlussarbeiten, wissenschaftlichen Aufsätzen, Dissertationen und Fachbüchern.

### **Besuchen Sie uns im Internet:**

<http://www.grin.com/>

<http://www.facebook.com/grincom>

[http://www.twitter.com/grin\\_com](http://www.twitter.com/grin_com)

Cyberkriminalität in der Schifffahrt – operative und wirtschaftliche Auswirkungen auf eine mittelständische Reederei

**Dimitri Tsiganovski**

## Inhaltsverzeichnis

|   |    |
|---|----|
| II. Abbildungsverzeichnis .....   | 3  |
| III. Abkürzungen und Erläuterungen .....  | 4  |
| Einleitung .....  | 9  |
| 2. Vorstellung der Reederei F. A. Vinnen & Co. ....                                   | 10 |
| 2.1 Geschichte .....  | 10 |
| 2.2 Tätigkeitsbereich .....   | 11 |
| 3. Operative Aufgaben eines Reeders in der Position eines I Zeitverfrachters .....    | 12 |
| 3.1 Unterschied eines Verfrachters und Befrachters bei einem Zeitchartervertrag ..... | 12 |
| 3.2 Schiff .....  | 13 |
| 3.2.1 Navigation .....  | 13 |
| 3.2.2 Ausrüstung/Provisionierung .....  | 15 |
| 3.2.3 Besatzung .....   | 16 |
| 3.3 Bedeutung von Internet für operatives Arbeiten .....                              | 18 |
| 4. Bedeutung .....  | 20 |
| 4.1 Cyberkriminalität – ein globales Problem .....                                    | 20 |
| 4.2 Motive und Gefahren der Cyberkriminalität .....                                   | 22 |
| 4.3 Aktuelle Entwicklungen von Cyberangriffen .....                                   | 24 |
| 4.4 Zunehmende Relevanz in der Schifffahrt .....                                      | 27 |
| 4.5 Autonome Schifffahrt .....  | 30 |
| 5. Konsequenzen einer Cyberattacke auf eine mittelständische I I Reederei .....       | 33 |
| 5.1 Operative Auswirkungen .....  | 33 |
| 5.2 Wirtschaftliche Auswirkungen .....  | 35 |
| 6. Chancen/Vorgaben der Abwehr eines Reeders gegen Cyberangriffe .....                | 36 |
| 6.1 Richtlinien zur Cybersicherheit von (Schifffahrts-)Institutionen .....            | 36 |
| 6.1.1 Cyber Risk Management .....   | 37 |
| 6.1.2 Erweiterung des Safety Management Systems .....                                 | 39 |
| 6.1.3 Einführung von IDS/IPS-Systemen .....   | 40 |
| 6.1.4 Schutzmechanismen für E-Mail und Web Browser .....                              | 43 |
| 6.1.5 Awareness-Programm für die Schiffsbesatzung .....                               | 44 |
| 6.2 Haftung und mögliche Haftungsausschlüsse eines Reeders .....                      | 46 |
| 6.3 Versicherungen .....  | 47 |
| 7. Zusammenfassende Analyse .....   | 49 |
| 7.1 Operative Betrachtung .....   | 49 |
| 7.2 wirtschaftliche Betrachtung .....   | 50 |
| 7.3 Fazit .....   | 51 |
| IV. Anhang .....  | 53 |
| V. Quellen .....  | 54 |