

|          |                                                                                       |           |
|----------|---------------------------------------------------------------------------------------|-----------|
| <b>1</b> | <b>Grundlegende Begriffe</b>                                                          | <b>1</b>  |
| 1.1      | Infrastrukturen                                                                       | 1         |
| 1.2      | Verkehrsinfrastrukturen                                                               | 1         |
| 1.2.1    | Städtische Verkehrsinfrastrukturen                                                    | 2         |
| 1.2.2    | Überregionale Verkehrsinfrastrukturen                                                 | 3         |
| 1.2.3    | Vernetzung der Verkehrsinfrastruktur mit<br>anderen Sektoren                          | 3         |
| 1.3      | Kritizität einer Verkehrsinfrastruktur                                                | 4         |
| 1.4      | Schutzziele Kritischer Verkehrsinfrastrukturen                                        | 5         |
| 1.5      | Technische Ressourcen Kritischer Verkehrsinfrastrukturen                              | 5         |
| 1.5.1    | Operational Technology (OT)                                                           | 6         |
| 1.5.2    | Informationstechnology (IT)                                                           | 6         |
| <b>2</b> | <b>Grundlegende Modellkonzepte</b>                                                    | <b>9</b>  |
| 2.1      | Barrierenmodell                                                                       | 9         |
| 2.2      | Angreifermodell                                                                       | 11        |
| 2.3      | Risikomodell                                                                          | 13        |
| <b>3</b> | <b>Rechtlicher und institutioneller Rahmen Kritischer<br/>Verkehrsinfrastrukturen</b> | <b>17</b> |
| 3.1      | Europäischer Rechtsrahmen                                                             | 17        |
| 3.2      | Nationaler Rechtsrahmen                                                               | 18        |
| 3.2.1    | Verankerung im legislativen Recht                                                     | 19        |
| 3.2.2    | Konkretisierung durch exekutives Recht                                                | 19        |
| 3.3      | Normen zur Konkretisierung des rechtlich Gebotenen                                    | 19        |
| 3.3.1    | Stand der Technik                                                                     | 21        |
| 3.3.2    | Harmonisierte Normen                                                                  | 21        |

|                  |                                                                                                  |           |
|------------------|--------------------------------------------------------------------------------------------------|-----------|
| 3.3.3            | Branchenspezifische Sicherheitsstandards (B3S) .....                                             | 22        |
| 3.4              | Institutioneller Rahmen .....                                                                    | 23        |
| 3.4.1            | Zusammenspiel europäischer und<br>nationaler Institutionen .....                                 | 24        |
| 3.4.2            | Behördliche Aufsicht auf nationaler Ebene .....                                                  | 25        |
| 3.4.3            | Konformitätsbewertungsstellen und ihre Anerkennung ....                                          | 26        |
| <b>4</b>         | <b>Haftungsvermeidung als Motivation zum Schutz Kritischer<br/>Verkehrsinfrastrukturen .....</b> | <b>29</b> |
| 4.1              | Haftung aus körperschaftsrechtlichen Sicherheitspflichten .....                                  | 29        |
| 4.2              | Haftung aus öffentlich-rechtlichen Sicherheitspflichten .....                                    | 30        |
| 4.3              | Haftung aus zivilrechtlichen Sicherheitspflichten .....                                          | 31        |
| 4.4              | Strafrechtliche Haftung .....                                                                    | 32        |
| <b>5</b>         | <b>Entwurf, Implementierung und Betrieb angriffsgeschützter<br/>Systeme .....</b>                | <b>35</b> |
| 5.1              | Bedrohungsanalyse .....                                                                          | 35        |
| 5.2              | Ableitung von Security-Anforderungen .....                                                       | 36        |
| 5.3              | Prüfung und Nachweis von Security-Anforderungen .....                                            | 38        |
| 5.4              | Zulassung .....                                                                                  | 42        |
| 5.5              | Betrieb .....                                                                                    | 43        |
| <b>6</b>         | <b>Angriffsschutz durch tief gestaffelte Verteidigung .....</b>                                  | <b>45</b> |
| 6.1              | Maßnahmen zur Härtung informationstechnischer Systeme .....                                      | 45        |
| 6.2              | Maßnahmen des physischen Zugriffsschutzes .....                                                  | 46        |
| 6.2.1            | Maßnahmen der Protektion/Prävention .....                                                        | 47        |
| 6.2.2            | Maßnahmen der Detektion .....                                                                    | 48        |
| 6.2.3            | Maßnahmen der Intervention .....                                                                 | 49        |
| 6.2.4            | Maßnahmen der Postvention (Beweissicherung) .....                                                | 50        |
| 6.3              | Organisatorische Maßnahmen .....                                                                 | 51        |
| 6.3.1            | Risikobasierter Ansatz .....                                                                     | 52        |
| 6.3.2            | Prozessorientierter Ansatz .....                                                                 | 53        |
| 6.3.3            | Führung (Leadership) .....                                                                       | 54        |
| 6.3.4            | Änderungskontrolle .....                                                                         | 54        |
| 6.3.5            | Einsatz qualifizierten Personals .....                                                           | 55        |
| 6.3.6            | Lenkung von Dokumenten und Aufzeichnungen .....                                                  | 56        |
| 6.3.7            | Kontinuierliche Verbesserung (PDCA-Zyklus) .....                                                 | 57        |
| <b>7</b>         | <b>Schlussfolgerung und Ausblick .....</b>                                                       | <b>59</b> |
| <b>Literatur</b> | <b>.....</b>                                                                                     | <b>63</b> |