

Inhalt

Vorwort.....	4
1 Hintergründe.....	8
1.2 Rechtlicher Rahmen zur Risikominimierung	11
1.3 Technischer Rahmen zur Risikominimierung	12
1.4 Organisatorischer Rahmen zur Risikominimierung	13
1.5 Haftung bei Drittschäden – Schadenpotenziale und rechtliche Grundlagen	15
1.6 Interne Interessenskonflikte.....	16
2 Bedrohungspotenziale	18
2.1 Hackerangriff und Cyberwar	19
2.2 Darstellung des Cyber-Risikos anhand von Schadenbeispielen	24
2.3 Durchschnittliche Gesamtschäden und durch- schnittliche Ermittlungs- und Folgekosten	26
2.4 Eigenschäden im eigenen Unternehmen	27
3 Risikoermittlung, Risikobewertung, Risikoprävention.....	30
3.1 Internes Risikomanagement	31
3.2 IT-Risikomanagement	32
3.3 IT-Forensik	35
3.4 Fragebögen, Workshops, Interviews	35
3.5 Unterstützung durch Dienstleister	37
4 Versicherungslösungen im Überblick.....	38
4.1 Kurzüberblick über den Versicherungsschutz im eigenen Unternehmen im Rahmen der „Klassischen Versicherungen“	38
4.2 Versicherungsschutz für Cyber-Risiken.....	40
4.3 Bedingungen	43

4.4	Die Deckungsangebote der Versicherungswirtschaft..	44
4.5	Anbieter von Cyber-Versicherungen	46
4.6	Überblick Deckungskonzepte in tabellarischer Form...	54
4.7	Struktur der Policen als vergleichende Betrachtung.....	56
5	Versicherungsbedarf	62
6	Preisgestaltung.....	65
7	Zahlen, Daten, Fakten.....	66
8	Gesetzliche Rahmenbedingungen und Zertifizierungsmöglichkeiten.....	68
9	Fazit	72
10	Literatur.....	74
11	ANHANG: Überblick Deckungskonzepte in tabellarischer Form.....	78
11.2	Ausschlüsse (nicht abschließend)	82
11.3	Notwendige und vom Anbieter geforderte und nachzuweisende Voraussetzungen für die Gewährung von Versicherungsschutz.....	87
11.4	Subsidiaritätsklausel – Formulierungen	89
11.6	Geltungsbereich	100
11.7	Sanktionsklausel.....	104
11.8	Obliegenheiten zur Risikominderung – Schadenverhütung.....	105
11.9	Versicherungsfalldefinition – Formulierungen.....	106
11.11	Kapazitätsbandbreiten	146
12	Ergebnisse einer DVS-Cyber-Umfrage im März 2016.....	148