50 JAHRE
50 YEARS

HOCHSCHULE FÜR
ÖFFENTLICHE VERWALTUNG UND FINANZEN
LUDWIGSBURG

UNIVERSITY OF APPLIED SCIENCES

Absicherung von Cyberrisiken in der öffentlichen Verwaltung

zur Erlangung des Grades eines

Bachelor of Laws (LL.B.)

Im Studiengang Rentenversicherung – Public Management

vorgelegt von

Valentino Grein

Studienjahr 2023/2024

Erstgutachter: Herr Prof. Dr. Martin Schulz

Zweitgutachterin: Frau Lea Feldmann

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abkürzung	Erläuterung
E-Government	Electronic Government
DRV BW	Deutsche Rentenversicherung Baden-Württemberg
KMU	Kleines oder mittleres Unternehmen
DSGVO (alt. in Kommentaren DS-GVO)	Datenschutz-Grundverordnung
BSI	Bundesamt für Sicherheit in der Informationstechnik
IBM	International Business Machines Corporation
GDV	Gesamtverband der Versicherer
AVB Cyber	Allgemeine Versicherungsbedingungen für die Cyberrisikoversicherung
CERT-DRV	Computer Emergency Response Team-Deutsche Rentenversicherung
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
VN	Versicherungsnehmer
Bpb	Bundeszentrale für politische Bildung
BVerfG	Bundesverfassungsgericht
ISMS	Informationssicherheitsmanagementsysteme
ILS	Insurance Linked Securities
Cat-Bond	Catastrophe-Bond

Abbildungsverzeichnis

Anhangsverzeichnis

Genderhinweis

Aus Gründen der leichteren Lesbarkeit wird in der vorliegenden Arbeit die gewohnte männliche Sprachform bei personenbezogenen Substantiven und Pronomen verwendet. Dies impliziert jedoch keine Benachteiligung des weiblichen Geschlechts, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral zu verstehen sein.

1 Einleitung

In so gut wie jedem Lebensbereich stellt der digitale Wandel und der Fortschritt von digitalen Anwendungsprodukten, Dienstleistungen und Kommunikations-möglichkeiten eine wichtige Rolle dar. Dementsprechend erwarten die Bürger von den Unternehmen, dass diese innovative Anwendungsprodukte und Kommunikationsmöglichkeiten umsetzen und dem Bürger zur Verfügung stellen. Zusätzlich zu dem, von außen eingehenden, Druck der Bevölkerung haben auch die Unternehmen des öffentlichen Sektors den Vorsatz ihre Organisation und Verwaltung dem Fortschritt der Digitalisierung anzupassen. Zusammengefasst strebt die öffentliche Verwaltung sowie auch viele andere Unternehmen den Ausbau von *Electronic Government (E-Government)* und der Verwaltungsmodernisierung an. So soll nicht nur der Informationsaustausch zwischen Staat und Bürger, sondern auch zwischen staatlichen Institutionen untereinander beschleunigt werden.[1] Die öffentliche Verwaltung muss sich somit verschiedensten Aufgaben stellen: Veraltete Systeme müssen erneuert oder gänzlich ausgetauscht und durch neue ersetzt werden, neue Technologien müssen sowohl in der eigenen Organisationsstruktur, als auch bei öffentlich zugänglichen Systemen Anwendung finden und die IT muss mit dem wachsenden Datenstrom mithalten und die vorhandenen Daten sorgfältig aufbewahren, auswerten und schützen. Leider bieten diese digitalen Anwendungsmöglichkeiten und der Ausbau des Cyberraumes, sowie das Wachstum der Datenmengen „[…] auch neue Angriffsflächen für hochintelligente und hochprofessionelle Kriminelle weltweit“.[2] Im Falle eines erfolgreichen Angriffs bieten Cyberversicherungen die nötige Unterstützung, um die Gefahrenlage zu entschärfen und den entstandenen Schaden zu übernehmen. Cyberversicherungen stellen zwar noch eine sehr junge Versicherungssparte dar, doch durch die ansteigende Menge an Daten und dem daraus resultierenden Anstieg der möglichen Risiken, gewinnen Cyberversicherungen immer mehr an Wichtigkeit. Besonders in der öffentlichen Verwaltung könnten solche Versicherungen interessant werden, da gerade im öffentlichen Sektor eine enorme Anzahl an höchstpersönlichen und

[1] Vgl. Hill/Schliesky: Herausforderung e-Government, S.197.
[2] Vgl. Steimer, Michael: Einführung in die Cyberversicherung – Praktischer Einstieg für Vermittler von Klein-KMU, S. IX.

empfindlichen Daten verarbeitet wird. Folglich stellt der Verlust soeben genannter Daten nicht nur ein Verstoß gegen verschiedene Datenschutzrechte, sondern auch ein Vertrauensrisiko gegenüber dem Bürger dar. Auch die Deutsche Rentenversicherung Baden-Württemberg (DRV BW) muss sich als Institution der öffentlichen Verwaltung dieser Herausforderung stellen. Mithilfe eines ausgebauten digitalen Verarbeitungssystems können die Mitarbeiter der DRV BW zukünftig eingehende Anträge, Anfragen oder sonstige Anliegen effizienter und schneller bearbeiten. Die hierbei verarbeiteten Daten sind grds. höchstpersönliche Daten der Versicherten, wie beispielsweise das Jahreseinkommen, Daten bezüglich der Familie oder Krankenakten.[3]

1.1 Problemstellung

Im vergangenen Jahr wurde ein drastischer Anstieg der Bedrohungen im Cyberraum festgestellt; dies bestätigt ein Bericht der Cybersicherheitsbehörde des Bundes.[4] Besonders interessant sind hierbei Cyberangriffe in Form von *Ransomware, Malware* und *Phishing*, welche auch für die DRV BW eine ernstzunehmende Bedrohung darstellen könnten. „Nicht mehr nur große, zahlungskräftige Unternehmen stehen im Mittelpunkt, sondern zunehmend auch kleine und mittlere Organisationen sowie staatliche Institutionen und Kommunen“.[5] Kurz gesagt: In einer Welt, die sich immer mehr dem digitalen Fortschritt fügt, passen sich auch Kleinkriminelle sowie kriminelle Organisationen diesem Fortschritt an und entwickeln sich weiter. Somit stehen nunmehr auch staatliche Institutionen wie die DRV BW im Fadenkreuz solcher Cyberattacken. Ein erfolgreicher Cyberangriff könnte schwerwiegende Folgen für das Unternehmen und deren Kunden bzw. Versicherten haben. Neben Ausfällen von Dienstleistungen besteht auch die Möglichkeit, dass sich Dritte Zugang zu personenbezogenen Daten der Versicherten beschaffen. Demnach besteht ein enormes Schutzbedürfnis sowohl für Unternehmen, als auch für die Kunden bzw. Versicherten.

[3] Vgl. Anhang 1: Erfasste Daten.
[4] Vgl. Bundesamt für Sicherheit in der Informationstechnik, o. J.: Die Lage der IT-Sicherheit in Deutschland 2023 (Internet).
[5] Bundesamt für Sicherheit in der Informationstechnik, o. J.: Die Lage der IT-Sicherheit in Deutschland 2023 (Internet).

1.2 Zielsetzung und Forschungsfrage

Cyberversicherungen stellen eine sehr junge Versicherungssparte dar, haben aber aufgrund der im Kapitel 1.1 genannten Probleme des Cyberraumes großes Potenzial und Aufstiegschancen in der Versicherungsbranche. Verschiedene Datenschutzrichtlinien, sowie Gesetzesvorschriften, wie das *Grundgesetz* können sogar für eine dringliche Notwendigkeit einer Cyberversicherung sprechen. Jedoch haben Cyberversicherungen noch keine feste Stellung im Versicherungsmarkt.[6] Besonders Institutionen der öffentlichen Verwaltung tragen eine große Verantwortung gegenüber dem Bürger. Verpflichtende Leistungen wie beispielsweise Kranken- oder Rentenversicherungsbeiträge, die den Bürger an die jeweiligen Institutionen gesetzlich bindet, sprechen ebenfalls für größere Schutzmaßnahmen. Die DRV BW sollte demnach großen Wert auf die eigenen IT-Sicherheitsvorkehrungen legen. Die ansteigende Anzahl von erfolgreichen Cyberangriffen zeigt allerdings, dass auch ein stabiles digitales Verwaltungssystem nicht vor jedem Cyberangriff Schutz gewährt und das Risiko zunehmend steigt. So soll folgende Forschungsfrage in dieser Bachelorarbeit erarbeitet werden: Ist der Abschluss einer Cyberversicherung für die Deutsche Rentenversicherung Baden-Württemberg sinnvoll?

1.3 Methodisches Vorgehen

Zunächst soll innerhalb dieser Bachelorarbeit der aktuelle Forschungsstand relevanter Themenbereiche für Cyberversicherungen untersucht werden. Die für die Untersuchung genutzten Quellen bestehen neben Lehrbüchern und Kommentaren größtenteils aus verschiedensten Internetquellen, da die Cyberversicherung ein noch relativ junges Konzept auf dem deutschen Versicherungsmarkt darstellt und somit der Literaturbestand sehr dürftig ausgefallen ist. Zudem stehen einige Formen der Literatur, wie Versicherungsfachzeitschriften, auch online zur Verfügung. Bei der Benennung von versicherten Personen oder Versicherten handelt es sich um Personen, die bei der DRV BW versichert sind. Die Benennung als Versicherungsnehmer ist ausschließlich der DRV BW gewidmet. Zu Beginn wird

[6] Vgl. Steimer, Michael: Einführung in die Cyberversicherung – Praktischer Einstieg für Vermittler von Klein-KMU, S. 6.

die Digitalisierung der DRV BW analysiert, um die Relevanz einer Cyberversicherung für das Unternehmen darzustellen. Anschließend wird die Anwendbarkeit von Cyberversicherungen durch die Übertragung der Regelungen der Musterbedingungen des *Gesamtverbands der deutschen Versicherungswirtschaft* (GDV), den *Allgemeinen Versicherungsbedingungen für die Cyberrisikoversicherung*, oder kurz AVB Cyber, auf die öffentliche Verwaltung bzw. die DRV BW herausgearbeitet. Anhand der hieraus resultierenden Ergebnisse wird ein Konzept für mögliche Versicherungsbedingungen einer Cyberversicherung konstruiert, welche auf die öffentliche Verwaltung oder konkreter auf die DRV BW Anwendung finden können. Neben der Anwendbarkeit einer Cyberversicherung auf die DRV BW wird zudem deren Notwendigkeit und deren Lage auf dem Versicherungsmarkt erarbeitet. Die aufgezeigten Erkenntnisse der Untersuchung des aktuellen Forschungsstandes werden abschließend in einem Resümee zusammengefasst. Im Anschluss wird mithilfe der Trendforschung Aussagen über zukünftige Entwicklungen im Bereich Cyber getroffen, die der weiterführenden Bewertung der aktuellen Marktlage von Cyberversicherungen dienen. Die hierfür genutzten Statistiken wurden dem Bestand der Online-Plattform „Statista“ entnommen. Eine konkrete Aufschlüsselung, um welche Unternehmen oder Personen es sich bei den Befragungen handelt, wird von der Online-Plattform Statista nicht gestellt. Es bedarf jedoch keiner konkreten Benennung und Aufzählung der befragten Unternehmen und Personen, da lediglich die Tendenzen der untersuchten Trends relevant sind. Letztlich wird die Gesamtheit aller Ergebnisse und Erkenntnisse in einer Schlussfolgerung und Prognose zusammengeführt, um die Forschungsfrage zu beantworten und einen Blick auf mögliche Entwicklungen in der Zukunft zu gewähren.

2 Aktueller Forschungsstand

2.1 Digitalisierung in der DRV BW

Die DRV BW steht vor der schwierigen Aufgabe die Bedürfnisse der Bürger in der Form zu befriedigen, wie es diese auch aus der Privatwirtschaft gewohnt sind. „[…] Servicequalität, Schnelligkeit und jederzeitige Erreichbarkeit […]“[7] definieren

[7] Asghari, Reza: E-Government in der Praxis – Leitfaden für Politik und Verwaltung, S. 40.

unter anderem die Erwartungen der Bürger an eine Behörde.[8] Die Nutzung moderner Technologien könnte nicht nur diese Erwartungen erfüllen, sondern auch die Verwaltung modernisieren und für einen Bürokratieabbau sorgen.[9] Im Zuge des Ausbaus der digitalen Infrastruktur fällt auch der Begriff E-Government, der nach der Speyerer Definition „die Abwicklung geschäftlicher Prozesse des Regierens und Verwaltens (Government) mit Hilfe von Informations- und Kommunikationstechniken über elektronische Medien“[10] beschreibt. Die DRV BW hat verschiedene Leistungen im Leistungsfall, beispielsweise Renten oder Leistungen zur Prävention und Rehabilitation, an den Versicherten zu zahlen bzw. zu leisten.[11] Bezüglich dieser Leistungen besteht für die Versicherten in der Regel ein Anspruch, was bspw. an den gesetzlichen Vorschriften der Altersrente aus § 35 ff. SGB VI ersichtlich ist. Um die Leistungen ordnungsgemäß erbringen zu können, prüfen die Mitarbeiter der DRV BW, ob die versicherte Person die versicherungsrechtlichen Voraussetzungen der jeweiligen Leistung erfüllt. Die hierfür relevanten Daten werden in einem Versicherungskonto gespeichert.[12] Die Speicherung der Daten erfolgt in der Regel elektronisch in Form von elektronischen Versicherungskonten oder elektronischen Akten.[13] Aufgrund der grds. bestehenden Versicherungspflicht in der gesetzlichen Rentenversicherung gem. § 1 ff. SGB VI kann davon ausgegangen werden, dass ein Großteil der Bevölkerung unter die Versicherungspflicht der genannten Vorschriften fällt und eine dementsprechend große Menge an Daten gespeichert wird. Interessant ist hierbei, dass die DRV BW auf die Daten zugreifen und diese, wenn notwendig, auch an Dritte weitergeben darf.[14] Aus diesem Verwaltungsverfahren geht hervor, dass die DRV BW „[…] Zugriff auf bereits von der Verwaltung erhobene Datenbestände […]“[15] hat und diese Datenbestände, sollten diese auch weiterhin vorliegen, nicht erneut erheben muss. Das hierbei angewandte Verfahren der digitalen Verwaltung wird auch *Once-*

[8] Vgl. Asghari, Reza: E-Government in der Praxis – Leitfaden für Politik und Verwaltung, S. 40.
[9] Vgl. Seckelmann, Margrit: Digitalisierte Verwaltung Vernetztes E-Government, S. 55.
[10] Vgl. Seckelmann, Margrit: Digitalisierte Verwaltung Vernetztes E-Government, S. 55.
[11] Vgl. DRV BW, o. J.: Unsere wichtigsten Aufgaben (Internet).
[12] Vgl. DRV BW, o. J.: Unsere wichtigsten Aufgaben (Internet).
[13] Vgl. Anhang 2: Speicherung der Daten.
[14] Vgl. Anhang 3: Zugriff und Weitergabe der Daten.
[15] Seckelmann, Margrit: Digitalisierte Verwaltung Vernetztes E-Government, S. 73.

Only-Prinzip genannt.[16] Damit die Daten nach Zusage des jeweiligen Leistungsanspruches vor weiteren Zugriffen geschützt sind, ist prinzipiell die Löschung dieser Datenbestände naheliegend.[17] Von einer Löschung des Gesamtbestandes der Daten eines Versicherungskontos ist zumindest zu Lebzeiten der versicherten Person an keiner Stelle die Rede. Zur Prüfung der versicherungsrechtlichen Voraussetzung einer Hinterbliebenenrente gem. § 46 ff. SGB VI sind außerdem die Versicherungszeiten des verstorbenen Versicherten von Nöten. Im Zusammenhang mit Art. 5 Abs. 1 e) DSGVO, der besagt, dass die Speicherung personenbezogener Daten so lange ermöglicht wird, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, kann davon ausgegangen werden, dass das Versicherungskonto und die darin enthaltenen Daten einer versicherten Person grds. über den Tod hinaus gespeichert bleiben. Die langfristige Speicherung dieser personenbezogenen Daten birgt allerdings auch große Gefahren. Die Vernetzung durch digitale Strukturen ermöglicht es auch unerwünschten Nutzern Zugriff auf diese Daten zu erhalten. Problematisch ist hierbei, dass diese Daten auch ohne Spuren kopiert werden und an Dritte gelangen können und dies zum Teil auch unbemerkt bleibt. Folglich spricht man von einer Cyberattacke, bei der die Schwachstellen eines Systems, Programmes oder einer Software ausgenutzt wird, um in das Netzwerk der Behörde zu gelangen.[18] Dies allein beschreibt allerdings nur einen Teil der Gesamtheit aller Angriffe. „Cyberangriffe sind vorsätzliche Versuche, Daten, Anwendungen oder andere Assets durch unbefugten Zugriff auf ein Netzwerk, ein Computersystem oder ein digitales Gerät zu stehlen, offenzulegen, zu verändern, zu deaktivieren oder zu zerstören.“[19] Aus dieser Definition des IBM kann abgeleitet werden, dass die Art eines Cyberangriffes und die genutzten Mittel und Möglichkeiten variieren. In welcher Form ein Cyberangriff vorliegen kann, wird in Kapitel 2.3 aufgegriffen.

[16] Vgl. Seckelmann, Margrit: Digitalisierte Verwaltung Vernetztes E-Government, S. 73.
[17] Vgl. Detken/Eren: Handbuch Datensicherheit, S. 289.
[18] Vgl. Detken/Eren: Handbuch Datensicherheit, S. 50-51.
[19] IBM, o. J.: Was ist ein Cyberangriff? (Internet).

2.2 Die Cyberversicherung

Durch den Abschluss einer Cyberversicherung können die finanziellen Folgen und Schäden eines Cyberangriffes begrenzt und angebotene Service-Leistungen für das Krisenmanagement genutzt werden.[20] Da zunächst fraglich ist, ob eine Cyberversicherung für die DRV BW Anwendung finden kann, muss das Versicherungsprodukt, der historische Hintergrund dieser Versicherungen, sowie auch deren Stellung auf dem Versicherungsmarkt betrachtet werden. Das Versicherungsprodukt „[…] kennzeichnet den angebotenen Versicherungsschutz.“[21] Der angebotene Versicherungsschutz einer Cyberversicherung erstreckt sich über mehrere Bereiche. Unter anderem werden Leistungsfälle in den Bereichen Haftpflicht-, Sach-, Eigenschaden- und Lösegeldversicherungen gedeckt, was eine konkrete Einordnung im Versicherungsmarkt erschwert. Die Cyberversicherung stellt somit eine *Kombi-Versicherung* vieler verschiedener Versicherungssparten dar.[22] Das Produkt konnte sich erst im Jahre 2011 durch das britische Unternehmen *Hiscox Insurance* auf dem deutschen Markt einfinden. Seitdem gab es viel Bewegung in der Branche und durch den rasanten Anstieg an Ransomware-Angriffen wuchs auch das Interesse bezüglich solcher Versicherungspolicen.[23] Im Jahr 2017 hat der *Gesamtverband der deutschen Versicherungswirtschaft (GDV)* erstmals Musterbedingungen für eine Cyberversicherung aufgestellt, die *Allgemeinen Versicherungsbedingungen für die Cyberrisikoversicherung* oder kurz *AVB Cyber*. Teil A dieser Bedingungen gibt zu erkennen, dass der Versicherungsgegenstand grds. in vier verschiedene Bausteine aufgegliedert ist: Der Basis-Baustein, der Service- und Kosten-Baustein, der Drittschaden-Baustein und der Eigenschaden-Baustein. Zwar gibt der GDV somit eine Grundstruktur einer Cyberversicherung vor, jedoch sind die AVB Cyber unverbindlich und lassen sogar abweichende Regelungen in der Erstellung eigener Versicherungsbedingungen zu. Ein einheitliches Konstrukt von Cyberversicherungen liegt somit nicht vor und ermöglicht den Versicherern eigene

[20] Vgl. Gesamtverband der deutschen Versicherungswirtschaft, 2018: Das leistet eine Cyberversicherung (Internet).
[21] Vgl. Hartung, Thomas, Gabler Banklexikon, 2020: Versicherungsprodukt (Internet).
[22] Vgl. Fortmann, r + s, 2019, S. 430.
[23] Vgl. Steimer, Michael: Einführung in die Cyberversicherung, S. 5.

Versicherungsbedingungen aufzustellen und unterschiedliche Tarife anzubieten.[24] Diese Varietät von Versicherungsprodukten stellt allerdings kein Problem für die öffentliche Verwaltung dar. Vielmehr bietet dieser Umstand eine gewisse Flexibilität, die es den Behörden ermöglicht eine risikoorientierte Tarifierung zu wählen, um genau die Risiken abzusichern, die den Bedürfnissen der Behörden gerecht werden.[25] Zudem wurden die Musterbedingungen seit ihrer Veröffentlichung dem sich wandelnden Versicherungsmarkt und der Digitalisierung angepasst.[26] Das Ziel dieser Musterbedingungen ist die kleinen und mittleren Unternehmen mit einem umfassenden Versicherungspaket zu versorgen.[27] Der öffentliche Sektor fällt jedoch nicht unter diese Begrifflichkeiten. Demnach gilt es die Anwendbarkeit der AVB Cyber auf die Unternehmen im öffentlichen Sektor genauer zu untersuchen.

2.2.1 Die Bausteine der AVB Cyber

Die *Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)* empfiehlt eine umsichtige Tarifierung durch Aufteilung des Versicherungsproduktes in die Bausteine Eigenschäden, Drittschäden und Service und Kosten, um die unsicheren Schadensfälle effektiv decken zu können.[28] Wie bereits in Kapitel 2.2 angemerkt, hat auch der GDV, zusammen mit dem Basisbaustein, diese in seinen Musterbedingungen aufgenommen. Zwar wurden diese Musterbedingungen auf kleine und mittelständische Unternehmen ausgelegt, die aufgrund erfolgreicher Cyberangriffe den Verlust, Diebstahl oder gar die Manipulation sensibler Daten von Kunden oder Kooperationsdaten zu befürchten haben.[29] Dennoch scheint die Übertragung dieser Musterbedingungen auf die Unternehmen der öffentlichen Verwaltung sinnvoll, da die Erhebung sensibler Daten nicht nur Teil der hoheitlichen Aufgabe der Behörde, sondern auch für die Gewährleistung einer funktionierenden Verwaltung und der Leistung rechtlicher Ansprüche notwendig

[24] Vgl. Fortmann, r + s, 2019, S. 430.
[25] Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht, 2022: Cyberversicherung (Internet).
[26] Vgl. Versicherungsmagazin, 2024: GDV hat seine Musterbedingungen überarbeitet (Internet).
[27] Vgl. AssCompact, 2024: GDV legt neue Musterbedingungen für Cyberversicherung vor (Internet).
[28] Vgl. Ganz, Robert, Bundesanstalt für Finanzdienstleistungsaufsicht, 2024: Cyberversicherungen – hohe Nachfrage – und hohe Risiken? (Internet).
[29] Vgl. Bundesamt für Sicherheit und Informationstechnik, o. J.: Kleine und mittlere Unternehmen (Internet).

ist.[30] Besonders die DRV BW bedarf einer Vielzahl an sensibler Daten, um die Leistungserbringung zu ermöglichen, wie unter anderem Identifizierungs- und Kontaktdaten, berufliche, soziale und familiäre Informationen, Finanz- und Zahlungsdaten und Gesundheitsdaten. Zudem werden diese Daten grds. in elektronischer Form gespeichert.[31] So lässt sich die Anwendung der Musterbedingungen der GDV auf die Unternehmen der öffentlichen Verwaltung zumindest nicht ausschließen.

2.2.1.1 Basis-Baustein

Der Versicherungsgegenstand des Basis-Bausteins sind nach Ziffer A1-1 AVB Cyber Vermögensschäden, die durch eine Informationssicherheitsverletzung verursacht wurden. Fraglich hierbei ist, ob die gespeicherten und verarbeiteten Daten der DRV BW, sowie deren verwendeten Software und Programme ebenfalls in diesen Schutzbereich aufgenommen werden können und ein Schaden an diesen Daten kein Sachschaden begründet, welcher gem. Ziffer A 1 – 3 Abs. 1 AVB Cyber vom versicherten Gegenstand ausgeschlossen wäre.[32] Ein wesentlicher Bestandteil der Cyberversicherung ist die persönliche Reichweite des gebotenen Versicherungsschutzes. Der Schutz umfasst nach Ziffer A 1-7 Abs. 1 AVB Cyber den Versicherungsnehmer selbst, also beispielsweise die DRV BW, und alle im Versicherungsschein genannten mitversicherten Unternehmen. Es empfiehlt sich demnach, jede Außenstelle der DRV BW im Versicherungsschein ausdrücklich zu nennen. Im Sinne der Ziffer A 1-7 Abs. 2 AVB Cyber werden die Mitarbeitenden der DRV BW automatisch in die Mitversicherung aufgenommen. Die Mitversicherung von Beschäftigten und Unternehmen stellt eine Fremdversicherung dar.[33] Dies ist insofern relevant, als „wenn etwa von den informationsverarbeitenden Systemen oder Daten des VN die Rede ist, […] auch die Systeme oder Daten der Mitversicherten gemeint [sind].“[34] So können nach den AVB Cyber alle Außenstellen, sowie deren Mitarbeiter in den Umfang des

[30] Vgl. Mobilitätsmagazin, 2024: Datenschutz in Behörden – Strenge Auflagen für öffentliche Stellen (Internet).
[31] Vgl. Anhang 1: Erfasste Daten, Vgl. Anhang 2: Speicherung der Daten.
[32] Vgl. Fortmann, r + s 2019, S. 430 – 431.
[33] Vgl. Prölss/Martin/Klimke, AVB Cyber Abs. A1_7 A1-7, Rn. 1-3.
[34] Vgl. Prölss/Martin/Klimke, AVB Cyber Abs. A1_8 A1-8, Rn. 1.

Versicherungsschutzes aufgenommen werden. Die Versagung einer Versicherungsleistung aufgrund einer fehlenden, im Versicherungsschein aufgenommenen, Versicherteneigenschaft der beteiligten Akteure scheint eher unwahrscheinlich und begrenzt die Prüfung der Leistung im Versicherungsfall auf den eingetretenen Schaden. Aus Ziffer A 1-3 Abs. 1 AVB Cyber geht hervor, dass Vermögensschäden solche Schäden sind, die weder Personenschäden (Tötung, Verletzung des Körpers oder Schädigung der Gesundheit von Menschen), noch Sachschäden (Beschädigung, Verderben, Vernichtung oder Abhandenkommen von Sachen) sind, noch sich unmittelbar aus solchen Schäden herleiten. Ziffer A 1-3 Abs. 2 S. 1 AVB Cyber stellt klar, dass elektronische Daten keine Sachen im Sinne dieser Bedingungen sind. Sollte die DRV BW durch einen Cyberangriff Daten verlieren, diese lediglich eingeschränkt nutzen können oder aufgrund von Manipulation der Daten diese zunächst nicht verarbeiten können, stellt dies somit ein Vermögensschaden i.S.d. Ziffer A 1-1 AVB Cyber dar. Außerdem ist zu beachten, dass aufgrund der Gleichstellung in Ziffer A1-2.3 AVB Cyber auch Software und Programme unter den Begriff „elektronische Daten“ fallen.[35] Die von der DRV BW angebotenen Online-Dienste wie beispielsweise einen Online-Antrag zu stellen oder Versicherungsdaten anzufordern, werden über den Webbrowser abgewickelt und elektronisch an den zuständigen Rentenversicherungsträger übersandt.[36] Sollte hierbei durch eine Sicherheitslücke eine Schadsoftware die Systeme der DRV BW befallen und jede weitere Benutzung der Systeme einschränken, könnte auch dieser Schaden in den Schutzbereich aufgenommen werden. Zudem bleibe der Verlust von elektronischen Daten gem. Ziffer A 1-3 Abs. 2 S. 2 AVB Cyber als Folge des Abhandenkommens von Sachen als Vermögensschaden versichert; sog. Vermögensfolgeschäden. Zu beachten ist hierbei allerdings, dass der Verlust von elektronischen Daten infolge der Zerstörung einer Sache nicht als Vermögensschaden, sondern als Sachschaden gilt und somit nicht zu dem Versicherungsgegenstand gehört.[37] Weiterhin stellt sich die Frage was unter dem Begriff der Informationssicherheitsverletzung verstanden wird. Ziffer A 1-2.1 AVB Cyber stellt klar, dass eine Informationssicherheitsverletzung

[35] Vgl. Rüffer/Halbach/Schimikowski/Pawig-Sander, AVB Cyber A.1-3, Rn. 2.
[36] Vgl. Anhang 4: Online-Dienste der DRV.
[37] Vgl. Fortmann, r + s 2019, S. 431.

eine Beeinträchtigung der Verfügbarkeit, Integrität und Vertraulichkeit von elektronischen Daten oder von informationsverarbeitenden Systemen darstellt. Der Begriff der informationsverarbeitenden Systeme umfasst nach dem Schutzzweck der AVB Cyber die gesamte IT-Infrastruktur und ist weit auszulegen. Dies stellt sicher, dass Server und Computer der DRV BW, sogar private Geräte der Mitarbeiter, wie private Laptops oder private Computer geschützt sind, soweit sie zu beruflichen oder betrieblichen Zwecken genutzt werden.[38] Nach dem Wortlaut der Ziffer A 1-2.1 AVB Cyber und dem allgemeinen Verständnis informationsverarbeitender Systeme, sind zudem auch Systeme, die alleinig der Datenspeicherung dienen nicht ausgeschlossen.[39]

2.2.1.2 Service- und Kosten-Baustein

Im Service- und Kosten-Baustein (Ziffer A 2 AVB Cyber) werden diejenigen Kosten genannt, welche vor und nach dem Versicherungsfall vom Versicherer übernommen werden. Nach Ziffer A 2-1 bis A 2-3 AVB Cyber sind das Forensik- und Schadenfeststellungskosten, versicherte Kosten im Versicherungsfall und Aufwendungen vor Eintritt des Versicherungsfalls. Der Versicherungsschutz in Bezug auf die übernommenen Kosten im Versicherungsfall wirkt allerdings sehr dünn, da lediglich die Übernahme der Forensik- und Schadensfeststellungskosten zusammen mit den in Ziffer A 2-2.1 AVB Cyber genannten Benachrichtigungskosten als verpflichtende Leistung gilt. Zumal Aufwendungen vor Eintritt des Versicherungsfalls (Ziffer A 2-3 AVB Cyber) eher weniger in der Praxis Anwendung finden, da der Versicherungsnehmer in der Regel keine Kenntnis bezüglich einer unmittelbar bevorstehenden Informationssicherheitsverletzung erlangt.[40] Demnach liegt der Fokus dieses Bausteins lediglich auf der Übernahme von Forensik- und Schadensfeststellungskosten und den Benachrichtigungskosten. Bei den Benachrichtigungskosten handelt es sich hauptsächlich um Kosten für die Prüfung und Erfüllung gesetzlicher und behördlicher Informationspflichten, sowie um die Ersatzpflicht aufgrund der Verletzung datenschutzrechtlicher Vorschriften. Eine behördliche Informationspflicht ergibt sich aus den Art. 33 und 34 DSGVO.

[38] Vgl. Prölss/Martin/Klimke AVB Cyber Abs. A1_2 A1-2, Rn. 8, 9.
[39] Vgl. Prölss/Martin/Klimke, AVB Cyber Abs. A1_2 A1-2, Rn. 8, 9.
[40] Vgl. Fortmann, r + s 2019, S. 431.

Ein möglicher Anwendungsfall bezüglich der DRV BW wäre, dass durch einen Cyberangriff Daten einer bei der DRV BW versicherten Person abhandenkommen und die betroffene Person von diesem Vorfall unterrichtet werden muss.[41] Für die DRV BW könnte der Versicherungsschutz in Bezug auf die Benachrichtigungskosten jedoch überflüssig sein. Die DRV BW ist als öffentliche Behörde selbstverständlich mit den Anforderungen der *Datenschutz-Grundverordnung (DSGVO)* vertraut und verarbeitet ihre Daten auch nach deren Vorschriften. Die gebotene Transparenz bezüglich der Datenschutzbeauftragten und Datenschutzbehörden eines jeden Rentenversicherungsträgers zeigt, dass nicht nur die DRV BW, sondern auch die übrigen Rentenversicherungsträger auf mögliche Komplikationen rund um das Thema Datenschutz vorbereitet sind und den gebotenen Vorschriften der DSGVO auch gewissenhaft nachgehen.[42] Die Problematik der Prüfung und Erfüllung gesetzlicher und behördlicher Informationspflichten liegt hingegen nicht in der Aufgabe selbst. Werden durch einen Cyberangriff eine beträchtliche Menge an Versichertendaten gefährdet, steigt allerdings das Ausmaß der behördlichen Informationspflicht auf ein beinahe untragbares Maß. Dahingehend scheint die Übernahme von Benachrichtigungskosten aufgrund eintretender Datenschutzverletzungen eine äußerst umfassende Unterstützung für Unternehmen der öffentlichen Verwaltung zu bieten. Letztlich kann die Übernahme von Kosten verschiedener Forensik-Leistungen ebenfalls eine überaus nützliche Versicherungsleistung darstellen. Der Versicherer gewährt diese Leistungen zwar nicht selbst, benennt aber einen Dienstleister der im Versicherungsfall die Forensik-Leistungen gewährt. Der Versicherungsnehmer kann den Dienstleister im Notfall über eine Hotline erreichen, der bereits telefonisch Soforthilfe leisten kann.[43] Man spricht bei dieser Art Leistungen auch von *Assistance Leistungen*.[44] Die sofortige Unterstützung im Krisenfall kann für viele Versicherungsnehmer ein besonders entscheidendes Merkmal für den Abschluss einer Cyberversicherung darstellen. Auch die DRV BW könnte ein großes Interesse daran haben im Krisenfall sofortige Unterstützung

[41] Vgl. Prölss/Martin/Klimke, AVB Cyber Abs. A2_2 A2-2, Rn. 3.
[42] Vgl. Anhang 5: Datenverarbeitung.
[43] Vgl. Rüffer/Halbach/Schimikowski/Erichsen, AVB Cyber A.2-1, Rn. 1.
[44] Vgl. Wagner, Fred, Gabler Wirtschaftslexikon, 2018: Assistance (Internet).

einzufordern, um die ausgehende Gefahr auf die Daten derer Versicherten oder auch auf betriebsinterne Daten umgehend beseitigen zu können. Die Ursachenerkennung und Abschätzung des Schadensumfangs allein reichen jedoch nicht aus, um den Schaden schnell zu regulieren. Der externe Sachverständiger sollte zusätzlich noch Vorschläge bringen, welche Maßnahmen zur Behebung der Informationssicherheitsverletzung erforderlich seien.[45] So könnte die hauseigene IT-Abteilung der DRV BW im Schadensfall schneller reagieren und mithilfe der externen Sachverständiger den Schaden begrenzen. Auch wenn der Service- und Kosten-Baustein der GDV Musterbedingungen nicht besonders viele, für die DRV BW geeignete oder praktikable, Versicherungsleistungen enthält, ist gerade die unterstützende Wirkung der *Assistance Leistungen* ein wesentliches Argument für die Tauglichkeit des Service- und Kosten-Bausteins. Die DRV BW kann immerhin bei einer akuten Bedrohung durch einen Cyberangriff von einer schnellen Unterstützung durch einen externen Fachexperten mehr profitieren, als von einem gezahlten Geldbetrag des Versicherers.[46] Die Begrenzung der Versicherungsleistungen auf die Übernahme der Forensik- und Schadensfeststellungskosten und die Benachrichtigungskosten hat zudem zur Folge, dass der Beitrag, den die DRV BW für eine Cyberversicherung an das jeweilige Versicherungsunternehmen zu zahlen hat, geringer ausfällt.[47]

2.2.1.3 Drittschaden-Baustein

Der Versicherungsgegenstand des Drittschaden-Bausteins ist nach Ziffer A 3-1 AVB Cyber Versicherungsschutz im Rahmen des versicherten Risikos für den Fall, dass der Versicherungsnehmer wegen einer Informationssicherheitsverletzung gemäß Ziffer A 1-2 AVB Cyber, die einen Vermögensschaden zur Folge hat, aufgrund gesetzlicher Haftpflichtbestimmungen privatrechtlichen Inhalts von einem Dritten auf Schadensersatz in Anspruch genommen wird. Sollten also, beispielsweise durch einen Cyberangriff, Daten von Versicherten der DRV BW gestohlen und missbraucht werden, wodurch diese einen Schaden erleiden, könnte

[45] Vgl. Rüffer/Halbach/Schimikowski/Erichsen, AVB Cyber A.2-1, Rn. 2.
[46] Vgl. Fortmann, r + s 2019, S. 440.
[47] Vgl. Klein, René, Für Gründer, o. J.: Cyberversicherung – Ist Ihr Unternehmen in Gefahr? (Internet).

die DRV BW haftbar gemacht werden. Im Grunde wird diese Haftbarmachung an die allgemeinen Haftpflichtbedingungen angelehnt. Durch die Voraussetzung einer Informationssicherheitsverletzung als Auslöser des Schadensersatzanspruches, liegt eine Differenzierung zwischen der Regelung aus Ziffer A 3-1 AVB Cyber und den allgemeinen Haftpflichtversicherungen vor.[48] Auch wenn die DRV BW im Besitz einer Haftpflichtversicherungspolice und eine Abtrennung beider Versicherungsbedingungen im Zweifelsfall nicht unkompliziert wäre, stellt die Regelung aus Ziffer A 1-12 AVB Cyber klar, dass die Cyberrisikoversicherung vorgeht, sollte Versicherungsschutz nach den Bedingungen der Cyberversicherung auch in einem anderen Versicherungsvertrag bestehen. Als datenschutzrechtliche Anspruchsgrundlage dieser Schadensersatzansprüche kann Art. 82 DSGVO herangezogen werden.[49] Gemäß der eben genannten Vorschrift hat eine Person, der wegen eines Verstoßes gegen die DSGVO ein Schaden entstanden ist, einen Anspruch auf Schadensersatz. Anspruchsberechtigte Personen sind somit alle von der Datenverarbeitung nach den Vorschriften der DSGVO betroffenen Personen. Ein Verschulden wird hier allerdings nicht vorausgesetzt, weshalb das Verschulden des Verantwortlichen zunächst angenommen wird.[50] Von dieser Ausgangsvermutung kann sich der Verantwortliche zwar gem. Art. 82 Abs. 3 DSGVO entlasten, indem er nachweist, dass er für den Umstand, der zu dem Schaden geführt hat, nicht verantwortlich ist. Dennoch können Datenschutzverletzungen trotz des Nichtverschuldens aufgrund der Fremdeinwirkung durch eine Cyberattacke nicht ausgeschlossen werden. Sollten sich Dritte durch bereits bekannte oder erkennbare Angriffswege Zugang zu den Daten beschaffen, könnte sich die DRV BW nicht auf eine Nichtverantwortlichkeit berufen und eine Befreiung nach Art. 82 Abs. 3 DSGVO wäre nicht möglich.[51] Bei solch einer Auslegung und Ahndung von Datenschutzverletzungen liegt die Vermutung nahe, dass die DRV BW und auch andere Behörden der öffentlichen Verwaltung mit dem Wandel der digitalen Welt zukünftig vermehrt mit einer Vielzahl von Schadensersatzansprüchen aufgrund einer Datenschutzverletzung

[48] Vgl. Rüffer/Halbach/Schimikowski/Erichsen, AVB Cyber A.3-1, Rn. 1-3.
[49] Vgl. Prölss/Martin/Klimke, AVB Cyber Abs. A3_1 A3-1, Rn. 2.
[50] Vgl. Paal/Pauly/Frenzel, DS-GVO Art. 82, Rn. 6.
[51] Vgl. Paal/Pauly/Frenzel, DS-GVO Art. 82, Rn. 15.

konfrontiert werden würden und eine Cyberversicherung allein dieses Ausmaß an Schadensersatzansprüchen nicht stemmen könnte. Die Begrenzung der Leistungen aus Ziffer A 3-6 AVB Cyber könnte im Umkehrschluss ebenfalls ein Hinweis darauf sein, dass sich die innerhalb des Drittschaden-Bausteins aufgenommenen Schäden beträchtlich summieren können und sich der Versicherer durch diese Regelungen vor zu hohen Zahlungsversprechen schützen will. Die Rechtsprechung wirkt einer Überflutung von durchsetzbaren Schadensersatzforderungen allerdings entgegen, indem sich diese nicht allein mit dem Verstoß der Verordnung aus Art. 82 DSGVO begnügt, sondern auch einen eingetretenen Schaden verlangt und der Verstoß auch kausal für den eingetretenen Schaden sein muss.[52] In Verbindung mit der Befreiungsmöglichkeit aus Art. 82 Abs. 3 DSGVO kann durch die starke Einschränkung der Geltendmachung solcher Schadensersatzansprüche davon ausgegangen werden, dass die Übernahme von Drittkosten durch die Cyberversicherung im Falle einer Geltendmachung von Schadensersatzansprüchen durch Dritte grds. eine angemessene finanzielle Unterstützung für die DRV BW ermöglicht. Sollten die entstanden Kosten dennoch die Deckungsfähigkeit des Versicherers übersteigen, führt Kapitel 2.5 eine Möglichkeit auf, enorme Schadenssummen decken zu können.

2.2.1.4 Eigenschaden-Baustein

Der Eigenschaden-Baustein sollte wohl für die DRV BW und allgemein dem öffentlichen Sektor der interessanteste Baustein für den Abschluss einer Cyberversicherung sein. Anhaltspunkte für diese Annahme lassen sich den Versicherungsgegenständen aus den Ziffern A 4-1 und 4-2 AVB Cyber entnehmen. Hierbei handelt es sich um den Betriebsunterbrechungs- bzw. Unterbrechungsschaden aus Ziffer A 4-1 und die Wiederherstellung von Daten nach Ziffer A 4-2 AVB Cyber. Eine Betriebsunterbrechung liegt nach Ziffer A 4-1.1.1 AVB Cyber dann vor, wenn infolge einer Informationssicherheitsverletzung elektronische Daten oder informationsverarbeitende Systeme des Versicherungsnehmers nicht zur Verfügung stehen oder nicht die übliche Leistung erbringen und daraus ein Unterbrechungsschaden entsteht. Die nachfolgende

[52] Vgl. Paal/Pauly/Frenzel, DS-GVO Art. 82, Rn. 10-11.

Ziffer A 4-1.1.2 definiert einen Unterbrechungsschaden folgendermaßen: Unterbrechungsschaden sind der Betriebsgewinn und die fortlaufenden Kosten, die im Zeitraum der Betriebsunterbrechung, längstens jedoch der Haftzeit durch den Versicherungsnehmer nicht erwirtschaftet werden können. Nach dieser Definition stellt sich allerdings die Frage, ob der Betriebsgewinn und die fortlaufenden Kosten der DRV BW durch eine Betriebsunterbrechung überhaupt in Versäumnis geraten können und falls ja, ob das Ausbleiben des Betriebsgewinns bzw. das Versäumnis der fortlaufenden Kosten Auswirkungen auf die Bestandskraft oder auf die Aufgabenerfüllung der DRV BW hat. Der Betriebsgewinn beschreibt die Differenz zwischen Betriebsertrag, also die Summe der Erlöse, und den Betriebskosten.[53] Die öffentliche Verwaltung wirtschaftet jedoch grds. nicht gewinnorientiert, sondern mit dem Ziel die jeweiligen Sachziele zu erfüllen.[54] Auch die DRV BW wirtschaftet nicht gewinnorientiert und zielt auf die Deckung der Ausgaben durch die Einnahmen ab, was anhand des Umlageverfahrens aus § 153 Abs. 1 SGB VI erkennbar ist. Selbst wenn man bei dem Begriff „Betriebsgewinne“ auf die Einnahmen der DRV BW abstellt, geht aus § 153 Abs. 2 SGB VI hervor, dass die Einnahmen der DRV BW aus den Beiträgen der Versicherten und den Zuschüssen des Bundes zusammengesetzt sind. Die Beitragszahlung ist nach den §§ 173 ff. SGB VI i.V.m. §§ 168 ff. SGB VI gesetzlich verankert, ebenso die Zuschüsse des Bundes gem. §§ 213 ff. SGB VI und erfolgen somit unabhängig von den innerhalb der DRV BW einschlägigen Aufgaben und Prozessen. Die laufenden Zahlungen zur Leistungserbringung stellen die laufenden Kosten der DRV BW dar. Diese Geldleistungen werden grds. durch die Deutsche Post AG ausgezahlt (§ 119 Abs. 1 SGB VI) und sind ebenfalls unabhängig von der örtlichen Behörde der DRV BW. Bei der DRV BW eingegangene Anträge, die während einer Betriebsunterbrechung nicht bearbeitet werden können, führen nicht direkt zu einem Schaden, da mit dem Antrag lediglich ein Verwaltungsakt aus § 31 SGB X eingeleitet wurde und die Entscheidung über den Antrag noch aussteht. Das Verfahren könnte also durch eine Betriebsunterbrechung über einen längeren Zeitraum andauern, ein Unterbrechungsschaden liegt aber mithin noch nicht vor.

[53] Vgl. Deutsche-Versicherungsboerse, o. J.: Betriebsgewinn-Definition (Internet).
[54] Vgl. Libbe, Jens, Bundeszentrale für politische Bildung, 2021: Öffentliche Unternehmen (Internet).

Auch wenn dadurch das Verfahren über die Erfüllung der Anspruchsvoraussetzungen hinaus andauern würde, läge kein Schaden vor, da die fällige Geldleistung aus § 118 Abs. 1 SGB VI auch nachgezahlt werden kann und sogar eine Verzinsung des Anspruchs einer Geldleistung nach § 44 SGB I in Betracht kommt. Eine Entschädigung, also die Zahlung eines im Versicherungsschein genannten Tagessatzes, wird nach Ziffer A 4-1.3.1 AVB Cyber nur so lange geleistet, wie ein Unterbrechungsschaden vorliegt und so Betriebsgewinn und laufende Kosten nicht weiter beeinflusst werden.[55] Ohne einen vorliegenden Unterbrechungsschaden könnte die öffentliche Verwaltung und so auch die DRV BW keine Entschädigungsleistung des Cyberversicherers in Anspruch nehmen.

Hinsichtlich der drohenden Gefahr durch eine Informationssicherheitsverletzung sensible Daten von Versicherten, Bürgern oder der Behörde selbst zu verlieren, scheint die Wiederherstellung der Daten aus Ziffer A 4-2 AVB Cyber für die öffentliche Verwaltung viel applikabler. Versicherungsgegenstand ist nach Ziffer A 4-2.1 AVB Cyber der Versicherungsschutz für notwendige Aufwendungen zur Wiederherstellung der von der Informationssicherheitsverletzung (Ziffer A 1-2 AVB Cyber) betroffenen Daten, sowie für die Entfernung der Schadsoftware. Schutzwürdig sind nur solche Daten, zu deren Nutzung der Versicherungsnehmer berechtigt ist.[56] Bereits die §§ 67a und 67b SGB X lassen lediglich eine rechtmäßige Erhebung und Verarbeitung von Sozialdaten durch die DRV BW zu und im Zusammenhang mit der Anforderung des Art. 6 DSGVO sind dies die optimalen Voraussetzungen, um die größtmögliche Menge an Daten in den Umfang des Versicherungsschutzes aus Ziffer A 4-2 AVB Cyber aufzunehmen. Dennoch ist hier anzumerken, dass einzig die Wiederherstellung und nicht etwa Kosten für das Beseitigen einer Sicherheitslücke oder die Einbringung einer verbesserten Software übernommen werden.[57] Dies lässt sich ebenfalls aus der charakteristischen

[55] Vgl. Prölss/Martin/Klimke, AVB Cyber Abs. A4_1 A4-1, Rn. 21-22.
[56] Vgl. Rüffer/Halbach/Schimikowski/Sander, AVB Cyber A.4-2, Rn. 3.
[57] Vgl. Prölss/Martin/Klimke, AVB Cyber Abs. A4_2 A4-2, Rn. 8.

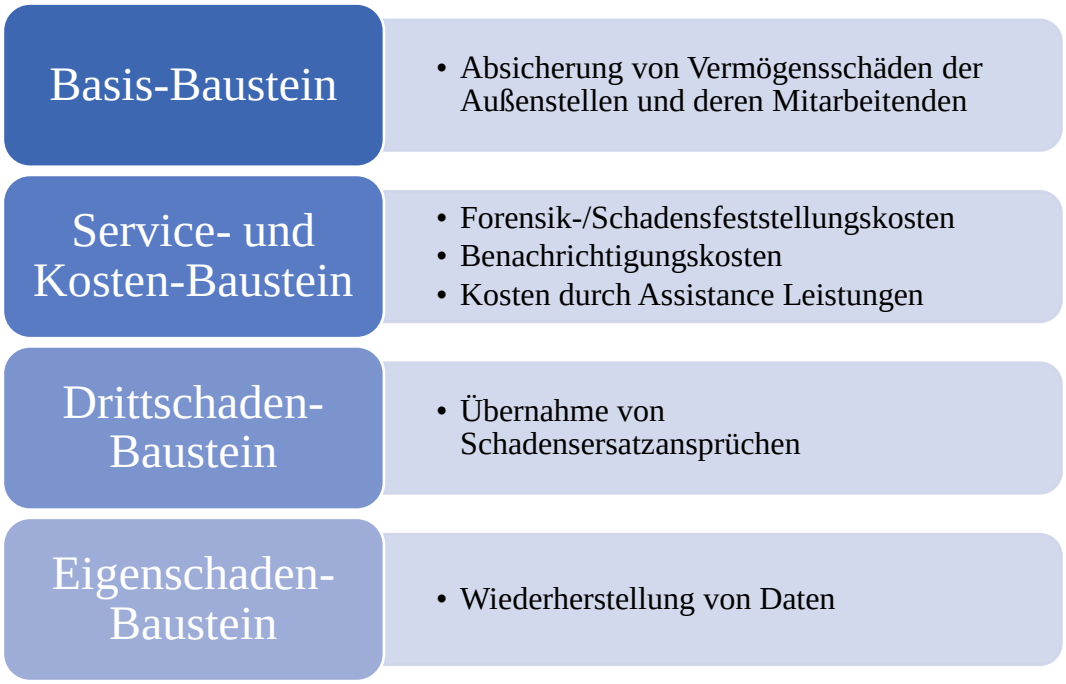
Schutzunktion einer Cyberversicherung ableiten, die im Schadensfall und nicht präventiv Schutz und Unterstützung gewähren soll.[58]

2.2.2 Zwischenfazit

Die Bausteine der GDV Musterbedingungen zeigen wie komplex und vielfältig der Versicherungsschutz einer Cyberversicherung ist. Die Trennung der Versicherungsgegenstände in einzelne Bausteine hat zum Vorteil, dass jeder Versicherungsgegenstand klar definiert und diskutiert werden kann. Auch wenn die Bausteine einige Versicherungsleistungen beinhalten, welche weniger Anwendung für die öffentliche Verwaltung, und damit auch für die DRV BW finden, könnten die Behörden von einigen Versicherungsleistungen stark profitieren. Ein Beispiel sind die in Kapitel 2.2.1.2 genannten *Assistance-Leistungen*, welche nicht eine einfache Geldleistung, sondern schnelle und unkomplizierte Unterstützung im Krisenfall anbieten.[59] Man bedenke, dass die GDV Musterbedingungen, wie der Name bereits verrät, lediglich Musterbedingungen und nicht verbindlich sind. Da die Versicherer die Möglichkeit haben eigene Versicherungsbedingungen aufzustellen und noch kein einheitlicher Markt bezüglich Cyberversicherungen existiert, könnte die DRV BW mithilfe einer umfassenden Beratung ein Versicherungsangebot wählen, dass genau auf die Bedürfnisse des Unternehmens und die priorisierten Versicherungsleistungen zugeschnitten ist.[60] Nach Untersuchung der einzelnen Bausteine hat sich folgendes Bild zu den einzelnen Versicherungsleistungen ergeben:

[58] Vgl. Eggen, Jonathan: Die Cyberversicherung, S. 14.
[59] Vgl. Fortmann, r + s 2019, S. 440.
[60] Vgl. Sieverding, Ole, AssCompact, 2024: Cyber-Bedingungswirrwarr – Herausforderungen für Vermittlung (Internet).

Abb. 1: Darstellung eines Konzepts für Versicherungsbedingungen einer Cyberversicherung



Quelle: Eigene Darstellung.

Die Konkretisierung auf diese Leistungen ist nur durch die ursprüngliche Betrachtung und Analyse der GDV Musterbedingungen möglich und zeigt, dass die GDV Musterbedingungen eine brauchbare Grundlage für ein individuelles Konzept von Versicherungsbedingungen einer Cyberversicherung mit Blick auf die öffentliche Verwaltung darstellen. Die oben abgebildete Grafik (Abb. 1) beschreibt demnach ebenso das Fundament einer möglichen Tarifierung einer Cyberversicherung, das für die DRV BW Anwendung finden kann. Solch ein Konzept allein reicht allerdings nicht aus, um eine zuverlässige Aussage über die Bestandskraft und Notwendigkeit von Cyberversicherungen in der öffentlichen Verwaltung zu treffen. Neben den Versicherungsbedingungen sind auch die Wirkungen von verschiedenen Außeneinflüssen auf den Versicherungsmarkt und die gesetzlichen Schutzpflichten des Staates zu untersuchen.

2.3 Cyberangriffe

Eine Informationssicherheitsverletzung nach Ziffer A 1-2 AVB Cyber kann auf verschiedene Art und Weisen umgesetzt werden. Die bekanntesten und häufigsten Methoden lauten wie folgt: Schadsoftware/Malware, Ransomware, Spam- und Phishing-Mails, Botnetze, DDoS-Angriffe, Schwachstellen in Soft- und Hardware,

Advanced Persistent Threats (APTs) und Social Engineering.[61] Eine große Gefahr geht bereits von den rechtmäßigen Benutzern eines Computersystems aus, also bspw. von den Mitarbeitern der DRV BW, indem ein System durch unachtsame Benutzung, wie die Wahl eines leicht zu entzifferndes Kennworts, gefährdet wird. Dadurch dringen sogenannte Viren, Würmer, Trojaner usw. in das System ein und können große Schäden verursachen, indem sie Daten verändern oder zerstören.[62] Nach der Definition einer Informationssicherheitsverletzung aus Ziffer A 1-2 AVB Cyber sollte eine Cyberversicherung grundsätzlich Versicherungsschutz gegen diese Form von Cyberangriffen bieten. Andererseits könnten unberechtigte Dritte, wie bspw. Hacker, nicht nur aus der Ferne mithilfe solcher Schadprogramme angreifen, sondern auch selbst in ein Netzwerk eindringen, um sich Daten zu verschaffen, die sie an andere Dritte verkaufen oder mithilfe derer sie für die Wiedererlangung besagter Daten ein Lösegeld von dem betroffenen Unternehmen verlangen.[63] Eine konkrete Schadsoftware zielt explizit auf die Verschlüsselung von Daten ab, woraufhin im Anschluss ein Lösegeld für die Freigabe der Daten verlangt wird. Schadprogramme dieser Art werden als *Ransomware* betitelt.[64] Die Anzahl von Cyberangriffen durch Ransomware insbesondere auf öffentliche Einrichtungen ist in den letzten Jahren stark angestiegen und stellen ein großes Problem für den öffentlichen Sektor dar.[65] Es stellt sich die Frage, ob eine Cyberversicherung auch gegen diese Art von Cyberangriffen schützen kann.

Nach den GDV Musterbedingungen wird laut Ziffer A 1-17.6 AVB Cyber die Zahlung von Löse- und Erpressungsgelder, sowie die Erfüllung von Erpressungsforderungen vom Versicherungsschutz ausgeschlossen. Entgegen dieser Vorschrift hat der Versicherer gezahlte Lösegelder dann zu ersetzen, wenn diese Rettungskosten nach § 83 Abs. 1 S. 1 VVG darstellen. Dies kann bei Löse- und Erpressungsgeldern angenommen werden, da der Versicherungsnehmer weiteren Schaden, wie im Beispiel der DRV BW die unberechtigte

[61] Vgl. Myra Security, o. J.: Was ist ein Cyberangriff? (Internet).
[62] Vgl. Detken/Eren: Handbuch Datensicherheit, S. 103.
[63] Vgl. Detken/Eren: Handbuch Datensicherheit, S. 104.
[64] Vgl. Bundesamt für Sicherheit in der Informationstechnik, o. J.: Ransomware – Vorsicht vor Erpressersoftware (Internet).
[65] Vgl. Kretschmer, Christian, tagesschau, 2023: Cyberangriffe: Ein Weckruf für Kommunen (Internet).

Weiterverbreitung sensibler Versicherungsdaten, verhindern will und damit der Pflicht aus § 82 Abs. 1 VVG, weiteren Schaden abzuwenden oder zu mindern, nachkommt.[66] Gesetze sind laut Duden „vom Staat festgesetzte, rechtlich bindende Vorschrift[en].“[67] Damit gehen diese Vorschriften den unverbindlichen Musterbedingungen der GDV vor und könnten sogar den Anspruch des Versicherungsnehmers auf Ersatz von Löse- und Erpressungsgeldern als Pflichtleistung des Versicherers begründen. Dennoch „[…] dürfte jede Lösegeldzahlung zur Existenzsicherung der Hacker beitragen und sie zu weiteren Angriffen motivieren.“[68] Insofern liegt die Vermutung nahe, dass die Zusage eines Versicherers Lösegeldzahlungen zu ersetzen, auch mittelbar ein Verstoß gegen die guten Sitten gem. § 138 Abs. 1 BGB darstellen könnte. Der Unterschied vom § 138 Abs. 1 BGB und Verbotsnormen ist der Bewertungsrahmen. Etwas sittlich Verwerfliches ist nicht nach einer strengen Gesetzesnorm geregelt, sondern wird von der sich ständig wandelnden gesellschaftlichen Haltung gesteuert und bedarf einer abwägenden Entscheidung, bei der alle Gesichtspunkte und Umstände herangezogen werden.[69] Die DRV BW könnte ebenso Opfer eines Ransomware-Angriffs und einer daraus resultierenden Lösegeldforderung werden. Der Zugriff auf die Daten der versicherten Personen könnte eingeschränkt oder gar unmöglich sein und es bestehe die Gefahr, dass diese Daten von den Verantwortlichen gestohlen und missbraucht werden. Einerseits geht das *Bundesamt für Sicherheit in der Informationstechnik (BSI)* recht in der Annahme, eine Zahlung der Lösegeldforderungen erhöhe die Wahrscheinlichkeit weiterer Ransomware-Angriffe, da man sich so dem Willen der Täter beugt und diesen einen Beweggrund gibt, weitere Angriffe einzuleiten und potenziell nicht nur der DRV BW, sondern auch der restlichen Bevölkerung zu schaden. Andererseits bestehe bei einer präventiven Nichtzahlung der Forderung durch die DRV BW die Gefahr, dass die Versicherten zwangsweise in eine Situation geraten, in der deren Eigentum, existenzielle Freiheit oder sogar das Leben bedroht wäre.[70] Beide Alternativen wirken negativ auf die gesellschaftliche Ordnung ein, sind aber unterschiedlich

[66] Vgl. Die Versicherungspraxis: Die neuen Musterbedingungen für die Cyberversicherung, S.31.
[67] Duden, o. J.: Gesetz (Internet).
[68] Vgl. Eggen, Jonathan: Die Cyberversicherung, S. 115.
[69] Vgl. Eggen, Jonathan: Die Cyberversicherung, S. 116-117.
[70] Vgl. Eggen, Jonathan: Die Cyberversicherung, S. 117-118.

risikobehaftet. Der Staat hat nach Auffassung des *Bundesverfassungsgerichts (BVerfG)* unter grundrechtlicher Betrachtung eine Schutzpflicht vor Angriffen auf elektronische Kommunikation und informationstechnische Systeme, auch wenn ein solcher Angriff von Privaten und nicht vom Staat ausgehe.[71] Für die DRV BW als Behörde der öffentlichen Verwaltung gelten somit dieselben Schutzpflichten. Auch wenn die Möglichkeit einer erneuten Bedrohung entgegenzustehen besteht, überwiegt doch das Wohl der Bürger und die drohende Gefahr, die sich aus der Nichtbeachtung von Lösegeldforderungen ergeben könnte. Ein Verstoß gegen die guten Sitten nach § 138 Abs. 1 BGB kann anhand der vorliegenden Abwägung der Umstände zunächst verneint werden. Der ständige Wandel gesellschaftlicher Haltungen lässt jedoch vermuten, dass dieses Problemfeld zukünftig weiteren Diskussionsbedarf fordert und von den jeweiligen, zu der maßgebenden Zeit, herrschenden Moralvorstellungen der Gesellschaft abhängig sind. Eine endgültige Abwägungsentscheidung hinsichtlich des Ersatzes von Lösegeldzahlungen durch Cyberversicherungen liegt mithin nicht vor. Es wäre nach dem aktuellen Stand jedoch durchaus möglich den Ersatz von Lösegeldzahlungen in die Tarifierung des Versicherungsvertrages mitaufzunehmen.

"Die Stärkung der Unternehmensresilienz gegenüber Cyberrisiken ist ein kontinuierlicher Prozess[…]."[72] Aufgrund dieser ständigen technischen Entwicklungen verändern sich auch mit der Zeit die auftretenden Cyberangriffe. Das BSI verfolgt beispielsweise mit der Veröffentlichung des IT-Grundschutzhandbuchs das Ziel das bestehende Sicherheitsrisiko von Unternehmen und Kommunen zu mindern und den wachsenden technologischen Risiken entgegenzuwirken.[73] Neben der Absicherung von Schäden, die infolge eines Cyberangriffes zustande gekommen sind, stehen daher auch präventive Maßnahmen für Cyberangriffe im Vordergrund. Je widerstandsfähiger ein Unternehmen gegen Cyberangriffe aufgestellt ist, desto eher kann die Schadenseintrittswahrscheinlichkeit minimiert werden. Selbst im Falle eines erfolgreichen Cyberangriffes wäre das Unternehmen durch präventive Maßnahmen

[71] Vgl. Taeger/Pole/Deusch/Eggendorfer, Computerrechts-Handbuch, Rn. 390.
[72] Griese, Michael, Versicherungswirtschaft heute, 2023: Unsichtbare Bedrohung – Wie eine effektive Vorsorge gegen Cyberangriffe aussehen kann (Internet).
[73] Vgl. Detken/Eren: Handbuch Datensicherheit, S. 103.

auf solche Angriffe vorbereitet und könnte diesen möglichst schnell entgegenwirken.[74] Neben ständiger Anpassung der Sicherheitsmaßnahmen und Schließung verschiedener Sicherheitslücken, durch Nutzung verstärkter Passwörter oder Aktualisierung verwendeter Software, sollten auch die Mitarbeitenden des Unternehmens stets sensibilisiert werden. Die Verbreitung aktueller Warnungen bezüglich Betrugsmaschen oder anderen Gefahren unter den Mitarbeitenden und Schulungen zum Thema Cybersicherheit, wie der Umgang mit fragwürdigen E-Mails oder Phishing, sind unter anderem mögliche Präventionsmaßnahmen, um die Mitarbeitenden vor Cyberangriffen durch eigenes Fehlverhalten zu bewahren.[75] Ferner können mithilfe sog. *Informationssicherheitsmanagementsysteme (ISMS)* durch eine laufende Überprüfung des Standes der Informationssicherheit neuen Bedrohungen und Risiken entgegengewirkt werden. Hierbei werden Risikoanalysen entwickelt und implementiert, die nach Durchführung und Überwachung stetig verbessert werden.[76] Der Bundesvorstand der Deutschen Rentenversicherung Bund hat zum 14. Mai 2020 für alle Träger der Deutschen Rentenversicherung die Anwendung des *branchenspezifischen Sicherheitsstandards* verbindlich beschlossen.[77] Aus diesen geht hervor, dass die DRV BW ihre IT-Systeme eigenständig und ohne Abhängigkeiten gegenüber Dritten verwaltet und eine interne Zuständigkeitsverteilung der IT-Systeme pflegt um eine aussagekräftige Risikoanalyse zu gewähren. Neben einer organisierten Risikoanalyse berücksichtigt die DRV BW die aktuelle Gefahrenlage und gibt die aktuell relevanten Informationen durch das CERT-DRV (Computer Emergency Response Team-Deutsche Rentenversicherung) weiter.[78] Die Informationssicherheitsstrategie der DRV BW wird in Abbildung 2 zusammengefasst:

[74] Vgl. Griese, Michael, Versicherungswirtschaft heute, 2023: Unsichtbare Bedrohung – Wie eine effektive Vorsorge gegen Cyberangriffe aussehen kann (Internet).
[75] Vgl. Griese, Michael, Versicherungswirtschaft heute, 2023: Unsichtbare Bedrohung – Wie eine effektive Vorsorge gegen Cyberangriffe aussehen kann (Internet).
[76] Vgl. Detken/Eren: Handbuch Datensicherheit, S. 89.
[77] Vgl. Anhang 6: Branchenspezifischer Sicherheitsstandard.
[78] Vgl. Anhang 7: Risikoanalyse und Gefährdungslage.

Abb. 2: Informationssicherheitsstrategie der DRV

Quelle: Ausschnitt aus Anhang 8: Sicherheitskonzeption der DRV aus: Deutsche Rentenversicherung – Branchenspezifischer Sicherheitsstandard, S. 21-23.

Weiterhin führt die DRV BW, wie in Abbildung 2 erkennbar, selbst ein ISMS, um die hausinterne Informationssicherheit zu kontrollieren und zu fördern. Die geschaffene Sicherheitskonzeption hat die DRV BW in fünf Ebenen unterteilt. Diese Ebenen differenzieren zwischen den Zielen der Sicherheitsstrategien, den geltenden Richtlinien, den Konzepten der Informationssicherheit und den Handlungsanweisungen für den Umgang mit den IT-Systemen und IT-Services.[79] Die DRV BW weist durch diese Informationsstrategie ein strukturiertes Vorgehen vor, durch das das Unternehmen die Informationssicherheit stets im Blick behält und weitgehend anpasst und optimiert.

In den branchenspezifischen Sicherheitsstandards wird außerdem konkret auf die personelle Sicherheit eingegangen. Aufgeführt werden notwendige Maßnahmen, um unbewusste oder bewusste Manipulationen von Daten durch das Personal zu verhindern. Mitunter soll auf allen Ebenen die Wichtigkeit der IT-Sicherheit

[79] Vgl. Anhang 8: Sicherheitskonzeption der DRV.

vermittelt werden. Die Zuverlässigkeit des Personals wird durch Sicherheitsmechanismen, wie die Anforderung zur Vorlage eines Führungszeugnisses, geprüft und gesichert. Die Mitarbeitenden sollen zudem durch Schulungen Fachkenntnisse im Umgang mit IT-Systemen erlangen und es werden unterschiedliche Kompetenzen und Verantwortungen festgelegt.[80] Überdies hat die DRV BW physische Sicherheitsmaßnahmen zu treffen, die vor Schäden aufgrund von Manipulation, Diebstahl und Zerstörung relevanter Systeme vor Ort schützen soll. Darunter zählen unter anderem die Absicherung von Fenstern und Türen, die Notwendigkeit von Zutrittskontrollanlagen und Videoüberwachung, sowie die Einrichtung einer Notstromversorgung und Klimatisierung der IT-Systeme. Damit ein Vorfall innerhalb der IT-Systeme erkannt und bearbeitet wird, wird fachlich spezialisiertes Personal eingesetzt, das spezielle Werkzeuge nutzt, um gegen eine Sicherheitsverletzung vorzugehen. Die jeweiligen Sicherheitsmaßnahmen werden ständig an den Stand der technischen Entwicklung angepasst und aufgrund der Veränderung der Bedrohungslage auch optimiert, sodass auch Schwachstellen ausfindig und unschädlich gemacht werden können.[81] Aus dem branchenspezifischen Sicherheitsstandard geht hervor, dass die DRV BW für den Fall einer Informationssicherheitsverletzung an eine ausgiebige und effektive Präventionsstruktur gebunden ist. Bereits die Nutzung eines ISMS und die damit eingeführte IT-Sicherheitskonzeption spricht für eine organisierte Sicherungsstruktur innerhalb des Unternehmens. Die DRV BW gibt somit zum Ausdruck sich den aktuellen Gefahren bewusst zu sein und dem daraus resultierenden Handlungsbedarf nachzugehen.

Auch für den Abschluss einer Cyberversicherung profitiert die DRV BW von den verpflichtenden Anforderungen des branchenspezifischen Sicherheitsstandards. Bereits in den AVB Cyber werden unter der Ziffer A 1-16 AVB Cyber Obliegenheiten aufgeführt, die der Versicherungsnehmer vor Eintritt des Versicherungsfalles einzuhalten hat. Dabei handelt es sich insbesondere um verschiedene Maßnahmen zum Schutz der informationsverarbeitenden Systeme. Für Cyberversicherungen sind die Schadensrisiken schwer einschätzbar und ohne

[80] Vgl. Anhang 9: Personelle Sicherheit, Vorfallerkennung/-bearbeitung.
[81] Vgl. Anhang 9: Personelle Sicherheit, Vorfallerkennung/-bearbeitung.

Entgegenkommen der Unternehmen teilweise untragbar. Durch die Einrichtung präventiver Schutzmaßnahmen und der Risikoeinschätzung der DRV BW kann ein Cyberversicherer das Schadensrisiko besser abschätzen. Die zu vereinbarende Versicherungssumme kann sich überdies, aufgrund verminderter Vorfälle und dementsprechend geringerer Kosten infolge von Schäden durch Cyberangriffen, in geringerem Umfang ausgestalten.[82]

2.4 Gesetzlicher Hintergrund

„Die Deutsche Rentenversicherung Baden-Württemberg ist eine Körperschaft des öffentlichen Rechts mit demokratischer Selbstverwaltung, also keine unmittelbare staatliche Behörde.“[83] Als Körperschaft des öffentlichen Rechts übernimmt sie spezielle Aufgaben des Staates.[84] Durch die Übernahme der staatlichen Aufgaben vertritt die DRV BW den Staat in seinem Handeln. Entsprechendes kann von den Bundeszuschüssen i.S.d. § 153 Abs. 2 SGB VI abgeleitet werden. Demnach sollte die DRV in ihrem Handeln auch die Ziele des Staates verfolgen.

Aus Art. 20 Abs. 1 GG ergibt sich die staatliche Schutzpflicht gegenüber dem Bürger. Diese Schutzpflicht verpflichtet den Staat in erster Linie den wirtschaftlich Schwachen „[…] Freiheit von Not, ein menschenwürdiges Dasein und eine angemessene Beteiligung am allgemeinen Wohlstand zu gewähren.“[85] Anhand dieser weiten Auslegung der Schutzpflicht und der Tatsache, dass die Erfüllung dieser Schutzpflicht im Interesse der Allgemeinheit steht, kann auch von einer staatlichen *Daseinsvorsorge* die Rede sein.[86] Der Begriff der Daseinsvorsorge muss unter Berücksichtigung der sich wandelnden technischen Entwicklungen und den sich verändernden Bedürfnissen der Bevölkerung gedeutet werden. Ein Anwendungsbeispiel ist die Anschaffung von Breitband-Internet-Anschlüssen im ländlichen Raum, aufgrund der neuen eingeführten Systeme im Identitätsmanagement, bspw. des E-Personalausweises.[87] Im Hinblick auf den technologischen Fortschritt lässt die Daseinsvorsorge des Staates darauf schließen,

[82] Vgl. Stanczyk, Michael, Versicherungswirtschaft heute, 2024: Gefangen im System (Internet).
[83] DRV BW, o. J.: Selbstverwaltung (Internet).
[84] Vgl. Bundeszentrale für politische Bildung, 2016: Körperschaft des öffentlichen Rechts (Internet).
[85] Vgl. Hömig/Wolff/Antoni, GG Art. 20, Rn. 4.
[86] Vgl. Radtke, MüKoStGB § 11, Rn. 58.
[87] Vgl. Hill/Schliesky: Herausforderung e-Government, S. 305-306.

dass der Staat auch der öffentlichen Verwaltung die nötigen und zeitgemäßen Ressourcen für die Einrichtung neuer Technologien, also eine sog. *digitale Grundversorgung*, garantiert.[88] Im Zusammenhang mit dem Sozialstaatsprinzip und der daraus verstandenen Daseinsvorsorge kann auch eine Schutzpflicht aus Art. 2 Abs. 1 GG dem allg. Persönlichkeitsrecht verstanden werden. Dem Grundsatz nach schützt der Art. 2 Abs. 1 GG i.S.d. allg. Persönlichkeitsrecht die Elemente der Persönlichkeit, also die Persönlichkeitssphäre und deren Erhalt, insbesondere vor Gefährdungen der Persönlichkeitsentfaltung.[89] Hierbei ist das Persönlichkeitsrecht nicht auf den privaten Raum beschränkt, sondern schützt auch die Darstellung der Person gegenüber Dritten in der Öffentlichkeit. Die betroffene Person hat also die Möglichkeit selbst zu entscheiden, „[…] inwieweit Dritte seine Persönlichkeit zum Gegenstand öffentl. Erörterungen machen dürfen […].“[90] Dieses Persönlichkeitsrecht wird zusammen mit der allg. Handlungsfreiheit, welche sich ebenfalls aus Art. 2 Abs. 1 GG ergibt, durch die Versicherungspflicht in der allg. Rentenversicherung aus den §§ 1 ff. SGB VI eingeschränkt. Von der Versicherungspflicht können sich die Versicherten, bei Vorhandensein der gesetzlichen Voraussetzungen, grds. nicht befreien und es liegt eine Versicherung kraft Gesetzes vor. Bei dieser Betrachtung wird konkret auf die versicherungspflichtig Beschäftigten abgestellt, da diese den größten Teil der Pflichtversicherten in der gesetzlichen Rentenversicherung umfassen.[91] Damit liegt auch ein Eingriff in das allg. Persönlichkeitsrecht aus Art. 2 Abs. 1 GG vor. Dieser Eingriff ist dann gerechtfertigt, wenn die Prüfung des Verhältnismäßigkeitsprinzips zu dem Ergebnis führt, dass die vorliegende Beeinträchtigung durch den § 1 SGB VI einen legitimen Zweck verfolgt und hierfür auch geeignet, erforderlich und angemessen ist.[92] Legitim und geeignet ist ein Zweck, wenn der Grundrechtseingriff dem Allgemeininteresse dient und der Eingriff dieses Ziel zumindest fördert.[93] Ziel der Norm aus § 1 SGB VI ist die abhängig Beschäftigten im Falle der Minderung oder des Wegfalls der Erwerbsfähigkeit oder im Falle des

[88] Vgl. Hill/Schliesky: Herausforderung e-Government, S. 306.
[89] Vgl. Jarass/Pieroth/Jarass, GG Art. 2, Rn. 38.
[90] ErfK/Schmidt, GG Art. 2, Rn. 38.
[91] Vgl. Kreikebohm/Roßbach/Segebrecht, SGB VI § 1, Rn. 2.
[92] Vgl. ErfK/Schmidt, GG Art. 2, Rn. 15.
[93] Vgl. BeckOK/Ruffert, GG Art. 12, Rn. 89-90.

Todes eines Familienmitgliedes zu schützen und abzusichern. Durch den gesetzlichen Zwang werden die Beschäftigten i.S.d. § 1 SGB VI Teil einer Versicherungsgemeinschaft und müssen zur Finanzierung der aktuellen Ausgaben für die Versicherungsgemeinschaft beitragen, um bei Erfüllung der versicherungsrechtlichen Voraussetzungen selbst einen Anspruch auf den Schutz durch die Versicherungsgemeinschaft zu haben.[94] Der aufgeführte Zweck des § 1 SGB VI dient demzufolge dem allgemeinen Interesse der Bevölkerung und das Gesetz fördert auch die o.g. soziale Absicherung. Weiterhin muss die Beeinträchtigung durch Gesetz auch erforderlich und angemessen sein. Die Erforderlichkeit ist dann gegeben, wenn kein milderes, gleich effektives Mittel zur Erreichung des genannten Zwecks vorliegt. Unter der Abwägung von dem Verhältnis zwischen dem Eingriff und dem verfolgten Zweck wird letztendlich über die Angemessenheit entschieden.[95] Abgesehen von einer gesetzlichen Zwangsbindung kommen private Vorsorgesysteme in Betracht, die dem Bürger zwar die freie Wahl über die Art und Form der Vorsorge überlassen, allerdings keine so starke Solidargemeinschaft und dementsprechend keine vergleichbare Absicherung, wie die gesetzliche Rentenversicherung bieten.[96] Die Erforderlichkeit des Gesetzes ist aufgrund dieser Betrachtung zu bejahen. Bei Abwägung zwischen dem verfolgten Zweck und der hierfür eintretenden Beeinträchtigung ist anzumerken, dass die Versicherten zwar durch die Versicherungspflicht keine andere Wahl haben, als ihre Daten den zuständigen Behörden zu überlassen. Dies ist für einen funktionierenden Staat jedoch notwendig. Mithilfe der gesetzlichen Zwangsbindung an die gesetzliche Rentenversicherung schafft der Gesetzgeber ein so großes und gesetzlich geschütztes Kollektiv, dass dem Einzelnen im Leistungsfall auch eine Versicherungsleistung garantiert werden kann. Alle Pflichtversicherten werden hierbei gleichermaßen zur Finanzierung der Altersvorsorge herangezogen und erhalten Ihre Leistung nach den für alle gleich geltenden Normen. Das Bestimmungsrecht über die Herausgabe von Daten kann für das Interesse der Solidargemeinschaft und des gesetzlich fixierten Kollektivs

[94] Vgl. Knickrehm/Roßbach/Waltermann/Berchtold, SGB VI § 1, Rn. 2.
[95] Vgl. BeckOK/Ruffert, GG Art. 12, Rn. 91-92.
[96] Vgl. Bundesministerium für Arbeit und Soziales, 2017: Gesetzliche Rentenversicherung (Internet).

durchaus für gesetzliche Zwecke eingeschränkt werden.[97] Das BVerfG hat allerdings das allg. Persönlichkeitsrecht in der Form konkretisiert, dass für die Gewährung vertraulicher informationstechnischer Systeme ein eigenes grundrechtliches Verständnis geschaffen wurde. Unter den Begriff dieser Systeme fallen solche, die personenbezogene Daten beinhalten und durch Zugriff auf solche Systeme Informationen über das Leben einer individuellen Person preisgegeben werden, also bspw. PCs, Laptops sogar konkreter die E-Mail. Überdies ist die Schaffung entsprechender Schutzvorkehrungen erforderlich.[98] Diese Regelungen wurden zwar vordergründig für den privaten Raum geschaffen, können aber analog auf öffentliche Behörden angewendet werden, da auch in dieser Sphäre informationstechnische Systeme zum Einsatz kommen, die personenbezogene Daten speichern oder verarbeiten. Die DRV BW hat mit dem hausinternen Risikomanagement und unter Anwendung des branchenspezifischen Sicherheitsstandards zwar bereits einige wirksame Sicherheitsvorkehrungen getroffen, doch scheinen diese Maßnahmen dem Schutzbedürfnis des allg. Persönlichkeitsrecht und konkreter der persönlichen Daten nicht voll und ganz zu genügen. Die Intimsphäre einer Person, also der Bereich der persönlichen Lebensgestaltung und -entfaltung, ist unantastbar.[99] In diesen Bereich wird durch die Versicherungspflicht nicht direkt eingegriffen. Personenbezogenen Daten wie bspw. Krankenkassendaten können dennoch Aufschluss über bestimmte Lebensumstände und der persönlichen Lebensgestaltung gewähren. Aus diesem Kontext wird die Empfindlichkeit dieser Daten, sowie die Dringlichkeit verstärkter Sicherheitsvorkehrungen ersichtlich. An dieser Stelle ist die Cyberversicherung in ihrer Funktion als erweiterndes und ergänzendes Versicherungsprodukt zu nennen. Besonders im Zusammenhang mit dem bereits o.g. Sozialstaatsprinzip aus Art. 20 Abs. 1 GG und der sich hierdurch ergebenden Daseinsvorsorge des Staates kann hinsichtlich des technologischen Fortschritts sogar an eine Förderpflicht des Staates bezüglich erweiterter Schutzmaßnahmen wie eine Cyberversicherung appelliert werden. Cyberversicherungen können den zu erwartenden Schaden nicht unerheblich begrenzen und durch schnelle Serviceleistungen gleichermaßen schnell

[97] Vgl. ErfK/Schmidt, GG Art. 2, Rn. 60.
[98] Vgl. ErfK/Schmidt, GG Art. 2, Rn. 43.
[99] Vgl. ErfK/Schmidt, GG Art. 2, Rn. 56.

auf die einwirkende Bedrohung reagieren. Welche Auswirkungen der technologische Fortschritt auf die Kehrseite desselben Fortschritts, also die Nutzung verschiedenster technologischen Systeme für kriminelle Zwecke, hat kann nur schwer vorhergesagt werden. Nichtsdestotrotz darf sich der Staat nicht von der technologischen Entwicklung abwenden, sondern müsste sich dieser Entwicklung anschließen. So wie die Privatwirtschaft mit neuen Technologien wächst und dem Bürger neue Anwendungsmöglichkeiten in den verschiedensten Bereichen verschafft, so hat auch der Staat dem Bürger entsprechende Anwendungsmöglichkeiten zu bieten.[100] Gleichermaßen sollte der Staat im Sinne dieser Auslegung auch stetig verbesserte und angepasste Schutzmechanismen für diese Technologien implementieren, um den Bürger auch vor neuen Bedrohungen zu schützen.

2.5 Kapazität auf dem Versicherungsmarkt

Die im Kapitel 2.4 genannten Präventionsmaßnahmen der Unternehmen kommen zwar den Cyberversicherern entgegen, allerdings bleibt die Situation aufgrund des steigenden Risikos und der hohen Schäden ernst. Im Jahre 2021 mussten die Cyberversicherer sogar erstmals negative Zahlen einbüßen und viele Versicherer haben sich aus dem Cybergeschäft zurückgezogen.[101] Zusätzlich zu den knappen Kapazitäten haben die übrigen Cyberversicherer verschärfte Anforderungen gefordert, was die Risikoprüfung des Unternehmens betrifft.[102] Die Kapazitäten sind gesunken und der Abschluss einer Cyberversicherung wird zusätzlich erschwert, kurz gesagt: Die aktuelle Lage auf dem Versicherungsmarkt birgt demnach große Spannungen und die Versicherer haben es nicht leicht. Eine mögliche Lösung den knappen Kapazitäten entgegenzuwirken und die Versicherer zu entlasten, ist das Konzept des Alternativen Risikotransfers. Durch den alternativen Risikotransfers kann der Versicherer das Versicherungsrisiko auf den Kapitalmarkt auslagern, wodurch die Risikotragfähigkeit erhöht wird. Die Risikoträger sind hierbei sog. Investoren, die auf hohe Risiko-Renditen hoffen,

[100] Vgl. Asghari, Reza: E-Government in der Praxis – Leitfaden für Politik und Verwaltung, S. 17.
[101] Vgl. Unternehmen Cybersicherheit, 2023: Cyberversicherungen immer schwerer zu bekommen – Interview zu den Entwicklungen am Versicherungsmarkt (Internet)
[102] Vgl. Unternehmen Cybersicherheit, 2023: Cyberversicherungen immer schwerer zu bekommen – Interview zu den Entwicklungen am Versicherungsmarkt. (Internet).

während Erst- und Rückversicherer das Risiko an das jeweilige Rückversicherungsunternehmen abgeben.[103] Diese Form des Risikotransfers stellt eine abgewandelte Form der allg. Rückversicherung dar. Bei einer traditionellen Rückversicherung übernimmt der Rückversicherer das Versicherungsrisiko von einem Erst- oder Rückversicherer selbst. Mithilfe der *Verbriefung* kann der Rückversicherer im Zuge des Alternativen Risikotransfers das Risiko in wertpapiermäßiger Form in den Kapitalmarkt transferieren.[104] Herausforderung dieses alternativen Risikotransfers ist allerdings der gerechte Interessenausgleich zwischen Investoren und Erst- und Rückversicherern. Einerseits verlangen Investoren eine möglichst ausgedehnte Transparenz, aufgrund möglicher hoher Verluste und der Tatsache, dass die Investoren im Gegensatz zu den Versicherern über weniger Informationen bezüglich der alternativen Risikotransfer-Transaktionen verfügen, was wiederum zu einer negativen Risikoauslese führen kann. Andererseits verfolgen Erst- und Rückversicherer das Ziel, das Basisrisiko zu verringern. Das Basisrisiko ist das Risiko, dass der tatsächlich eingetretene Schaden höher als die vorgegebene Deckungshöhe des Rückversicherers ist, und so den Erst- und Rückversicherern keine vollständige Absicherung geboten wird. All die genannten Faktoren sind insbesondere von den gewählten *Triggern* abhängig, die allerdings stark variieren können.[105] Die Trigger sind hierbei die definierten Auslöser eines Risikos, die den Rückversicherer zur Einstandspflicht verpflichten.[106] Die Zukunft des alternativen Risikotransfers hängt somit nicht nur von der gebotenen Transparenz versicherungsrechtlicher Informationen und der umfassenden Risikobewertung für ein minimales Basisrisiko ab, sondern auch von der Wahl und konkreten Definition der Trigger.

Auch wenn das allgemeine Konzept des alternativen Risikotransfers, oder auch *Insurance Linked Securities (ILS)*, noch vor einer großen Herausforderung steht, war es doch dieses Konzept, das den Risikotransfer von Cyberrisiken in den

[103] Vgl. Lale, Önder, BaFin, 2013: Alternativer Risikotransfer – Vorteile und Risiken des Transfers versicherungstechnischer Risiken auf die Kapitalmärkte (Internet).
[104] Vgl. Langheid/Wandt/Sasserath-Alberti/Vogelgesang, MüKo VVG, Rn. 493-494.
[105] Vgl. Lale, Önder, BaFin, 2013: Alternativer Risikotransfer: Vorteile und Risiken des Transfers versicherungstechnischer Risiken auf die Kapitalmärkte (Internet).
[106] Vgl. Brand/Baroch Castellvi/Goltz, VAG § 168, Rn. 11-12.

Kapitalmarkt ermöglichte.[107] Und dies scheint angesichts der aktuellen Lage von Cyberbedrohungen nicht ganz unwichtig. Cyberrisiken können als *Kumulrisiken* ein unvorhersehbares Risikopotenzial hervorbringen, da die Reichweite dieser Risiken weit über den lokalen oder nationalen Bereich hinausgehen. Dadurch ist die Erkennung und Bewertung des Kumulrisikos und des zu erwartenden Schadens erschwert.[108] Dieser *Kumulschaden* kann durch die hohe Risikoreichweite und der Abhängigkeit in Bezug auf zufällig eintretende Ereignisse die Deckungskapazität von Versicherern weit übersteigen.[109] Für solche *Katastrophenrisiken* bestehen *Catastrophe Bonds (Cat-Bonds)* also Katastrophenanleihen, mit derer Hilfe die explizite Verbriefung von Katastrophenrisiken möglich wird.[110] 2023 wurde von dem britischen Unternehmen *Beazley* auch bereits der erste *Cyber-Cat-Bond* als nicht-proportionales Deckungsmittel mit einer Kapazität von 65 Mio. US-Dollar eingeführt, der sogar Schutz vor Schäden über 300 Mio. US-Dollar gewährt. Die Einführung solcher und weiterer Deckungsformen sei von äußerster Wichtigkeit, um die Entwicklung des Cyber-Marktes voranzutreiben und mehr Kapazitäten für Cyberrisiken zu schaffen.[111] Der Cyber-Versicherungsmarkt war zwar anfangs mit Skepsis verbunden und Versicherer haben sich teilweise aus dem Versicherungsmarkt für Cyber zurückgezogen, jedoch nimmt die Anzahl der Versicherer auf dem Markt wieder zu. Gründe dafür sind beispielsweise die ansteigende Professionalität der Versicherer im Cyber-Versicherungsmarkt oder die zunehmende Awareness der Cyberrisiken und des Handlungsbedarfs der Unternehmen, was zu einem Wachstum der Nachfrage von verschiedenen Instrumenten zur Bekämpfung von Cyberrisiken, wie auch Cyberversicherungen, zur Folge hat.[112] Es besteht durchaus großes Potenzial für die Entwicklung weiterer Deckungsstranchen im Bereich Cyber, allerdings liegen diese bisher nur bedingt vor und die o.g. Herausforderungen des alternativen Risikotransfers sind aufgrund

[107] Vgl. Surminski, Marc, Zeitschrift für Versicherungswesen: Neue Kapazitätskonzepte in Cyber, S. 525.
[108] Vgl. Eggen, Jonathan: Die Cyberversicherung, S. 16.
[109] Vgl. Wagner, Fred, Gabler Wirtschaftslexikon, 2018: Kumulrisiko (Internet).
[110] Vgl. Lale, Önder, BaFin, 2013: Alternativer Risikotransfer: Vorteile und Risiken des Transfers versicherungstechnischer Risiken auf die Kapitalmärkte (Internet).
[111] Vgl. Surminski, Marc, Zeitschrift für Versicherungswesen: Neue Kapazitätskonzepte in Cyber, S. 525.
[112] Vgl. AssCompact, 2023: Cyberversicherungen – Markt stabilisiert sich, Wachstum hält an, 2023 (Internet).

der zufällig eintretenden Ereignisse im Cyberrisiko umso schwerer zu bewältigen. Nichtsdestotrotz sollte es möglich sein zuversichtlich auf die Zukunft des Cyber-Versicherungsmarktes zu blicken. Immerhin liegt die Grundlage für neue Kapazitätsmöglichkeiten bereits vor und hat, infolge der oben erwähnten ansteigenden Cyber-Bedrohungen und dem hiermit verbundenen ansteigenden Bedarf an Sicherheit, die Möglichkeit auch weiter zu wachsen.

2.6 Resümee des Forschungsstandes

Aus dem aktuellen Forschungsstand geht zunächst die Dringlichkeit der Prävention und Bekämpfung von Cyberrisiken hervor. Der voranschreitende technologische Fortschritt ermöglicht die Gründung und Herstellung neuer Anwendungen, Leistungen und Produkten. Durch diese neuen Möglichkeiten haben Kriminelle selbstverständlich auch Zugang zu neuen Technologien und können ihr kriminelles Vorhaben anpassen und verbessern. Daher kann vermutet werden, dass sich Cyberangriffe, durch z.B. Ransomware, ebenfalls weiterentwickeln und sich auch neuartige Bedrohungen entwickeln werden. Diese Vermutung wird zusätzlich durch den Anstieg von Cyberangriffen in den letzten Jahren gestützt. Besonders die öffentliche Verwaltung ist von diesen Angriffen bedroht. Durch die Verarbeitung sensibler personenbezogener Daten haben öffentliche Behörden ein ausgesprochen großes Schutzbedürfnis und sollten Cyberangriffe möglichst präventiv unterbinden, damit eine Massengefährdung von den Daten der Bürger, jedoch auch die Gefährdung der Daten eines einzelnen Individuums gemindert oder gar gänzlich vermieden werden kann. Mithin kann die Relevanz von Cybersicherheit insbesondere in der öffentlichen Verwaltung deutlich unterstrichen werden. Aus dem Sozialstaatsprinzip nach Art. 20 Abs. 1 GG lässt sich sogar eine gewisse Daseinsvorsorge ableiten, die im Wandel der Informationstechnik den Staat zum Handeln verpflichten könnte. Aus Art. 2 Abs. 1 GG, dem allg. Persönlichkeitsrecht, geht immerhin die Wichtigkeit der Intimsphäre und der persönlichen Entwicklung eines jeden Bürgers hervor. Jeder Bürger hat unter Betrachtung dieses Grundrechts ein Anrecht auf besonderen Schutz der eigenen Gestaltung des persönlichen Lebensbereiches. Durch die gesetzliche Versicherungspflicht aus § 1 SGB VI sind die Bürger dazu verpflichtet ihre persönlichen Daten an die vorgegebenen zuständigen Behörden weitergeben zu lassen. Eine dieser Behörden ist Die DRV

BW. Diese hat hinsichtlich des E-Governments bereits einige Schritte in Richtung Digitalisierung unternommen und bearbeitet die Versicherungsdaten der Versicherten grds. digital. Im Zuge der Digitalisierung und der einhergehenden Umstrukturierung verschiedener Arbeitsprozesse hat sich nicht nur die IT-Abteilung der DRV BW, sondern ebenso alle anderen Unternehmensbereiche auf die Gefahrenlage im Cyberraum einzustellen und den Schutz gegen Cyberrisiken anzupassen und zu verbessern. Hierbei bietet der branchenspezifische Sicherheitsstandard, welcher für alle Träger der Deutschen Rentenversicherung verpflichtend gilt, eine effektive und effiziente Lösung zur Bekämpfung von Cyberrisiken. Dieser beschreibt die IT-Sicherheitsstrategie und erörtert die Struktur des hausinternen ISMS, durch welches die Informationssicherheit überprüft und verbessert wird. Dennoch können solche präventiven Maßnahmen keinen hundertprozentigen Schutz gegen Cyberangriffe bieten. Informationsverarbeitende Systeme können bspw. verschiedene Sicherheitslücken vorweisen, die für eine gewisse Zeit auch unbemerkt bleiben können. Cyberversicherungen bieten in diesem Kontext mithilfe eines individuell angepassten Versicherungsangebots zusätzlichen Schutz, falls ein Cyberangriff, trotz präventiv getroffener Schutzmaßnahmen, Erfolg haben sollte. Im Zusammenhang mit dem aufgeführten Sozialstaatsprinzip, dem Schutzbedürfnis der Bürger und der Darstellung einer Daseinsvorsorge des Staates, sollte die öffentliche Verwaltung ein großes Interesse daran haben, sich nicht nur durch ein Risikomanagement und gleichartigen Maßnahmen vor Cyberangriffen zu schützen, sondern auch Schutz gegen die schädlichen Folgen eines Cyberangriffes zu gewähren. Ohne ein einheitliches Konzept für die Erstellung von Versicherungsbedingungen lassen sich schwer Aussagen über ein mögliches Versicherungsangebot für die öffentliche Verwaltung oder genauer für die DRV BW treffen. Der GDV hat zwar Musterbedingungen veröffentlicht, die von den Versicherern angewendet werden können, dennoch sollen diese Musterbedingungen lediglich für den Versicherungsschutz von kleinen und mittelständischen Unternehmen ausgelegt sein. Nach der Untersuchung der in den AVB Cyber genannten Vorschriften und Regelungen konnte letztendlich ein für die DRV BW individuell angepasstes Konzept für mögliche Rahmenbedingungen eines Cyberversicherungsvertrages konstruiert werden. Auch wenn die

Musterbedingungen der GDV Regelungen enthalten, die auf die öffentliche Verwaltung eher weniger Anwendung finden, brachten die Musterbedingungen Vorschriften hervor, die für eine Anwendbarkeit von Cyberversicherungen auf die öffentliche Verwaltung sprechen. Das Nichtvorhandensein eines einheitlichen Konzeptes für Versicherungsbedingungen in der Versicherungssparte Cyber ist zudem ein begünstigender Umstand, da dieser noch individuellere Vereinbarungen für die DRV BW ermöglicht und somit den Bedürfnissen des Unternehmens entgegenkommen kann. Die aktuelle Lage auf dem Versicherungsmarkt scheint sich ebenfalls stetig zu verbessern. Vermehrt stoßen neue Versicherer dem Cyber-Versicherungsmarkt hinzu und die Schaffung neuer Kapazitätsmodelle, die dem alternativen Risikotransfer zugrunde liegen, wie etwa die Cyber-Cat-Bonds schaffen positive Zukunftsaussichten für die Entwicklung des Cyber-Versicherungsmarktes. Es stellt sich allerdings die Frage, ob sich die eben angedeutete Annahme einer positiven Entwicklung auf dem Versicherungsmarkt auch wirklich bewahrheiten kann und Cyberrisiken, wie auch Cyberversicherungen auch in der Zukunft eine große Rolle spielen und demnach der DRV BW auch das Abschließen einer Cyberversicherung zu empfehlen wäre. Um diesem Phänomen nachzugehen werden im nachfolgenden Kapitel 3 verschiedene Trends im Bereich Cyber untersucht und analysiert. Mit deren Hilfe kann dieses Fazit um eine Prognose zukünftiger Ereignisse ergänzt werden.

3 Trendforschung

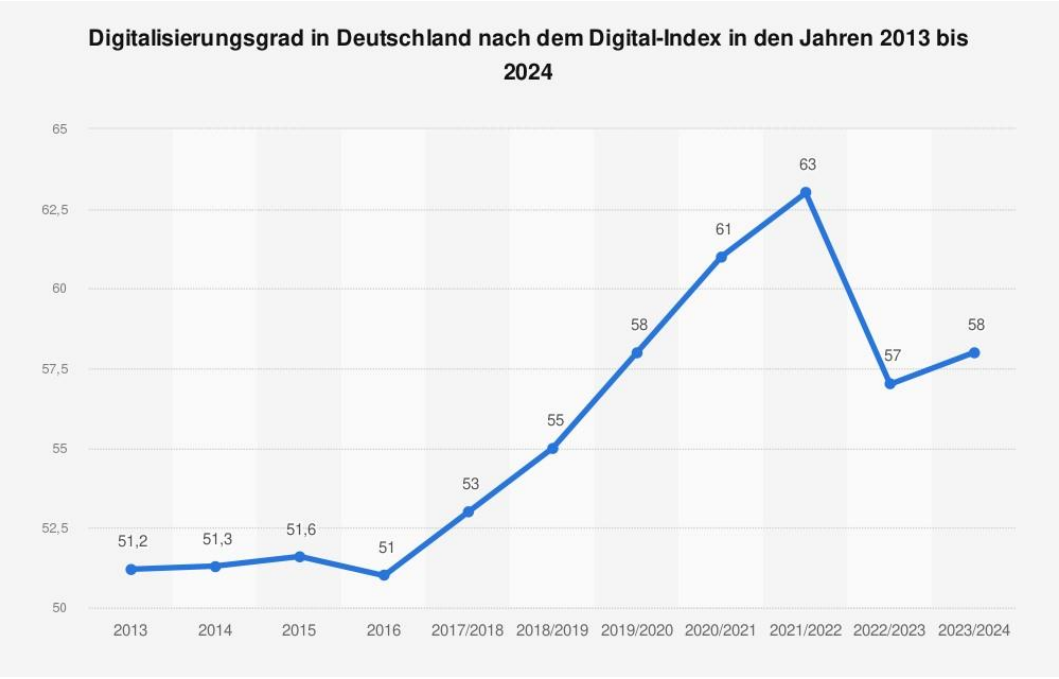
In Kapitel 2 wurden anhand des aktuellen Forschungsstands verschiedene Themen untersucht, die einen Einblick in die Möglichkeit des Abschlusses einer Cyberversicherung für die DRV BW gewähren. Für einige dieser Themenbereiche geben verschiedenen Statistiken Auskunft über die bisherige Entwicklung und lassen im Zusammenhang mit den Erkenntnissen des untersuchten Forschungsstands die Ausarbeitung einer Prognose zukünftiger Ereignisse und Entwicklungen zu. Im Folgenden werden verschiedene Statistiken analysiert, um

eine langfristige Entwicklungsrichtung bestimmter relevanter Größen, sog. *Trends*, zu untersuchen.[113]

3.1 Darstellung des Megatrends

Die zu erforschenden Trends werden unter Betrachtung eines *Megatrends* analysiert. Bei einem Megatrend handelt es sich um weitaus langwierigere und grundlegend verändernde Entwicklungen, die nicht nur nationale, sondern auch globale Ausmaße annehmen können. Diese Megatrends entstehen zwar durch das Zusammenführen mehrerer Subtrends, können allerdings so auch rückwirkend Aussagen über die einzelnen Subtrends preisgeben.[114] Der im Zuge dieser Untersuchung betrachtete Megatrend ist die *Digitalisierung der deutschen Gesellschaft*. Die nachfolgende Statistik (Abbildung 3) stellt den Digitalisierungsgrad der deutschen Gesellschaft von 2013 bis 2024 dar:

Abb. 3: Digitalisierungsgrad in Deutschland nach dem Digital-Index in den Jahren 2013 bis 2024



Quelle: Initiative D21, Statista, 2024: Digitalisierungsgrad in Deutschland nach dem Digital-Index in den Jahren 2013 bis 2024 (Internet).

[113] Vgl. Pfadenhauer, Michaela: Gegenwärtige Zukünfte – Interpretative Beiträge zur sozialwissenschaftlichen Diagnose und Prognose, S. 135.
[114] Vgl. Freundl, Maximilian, Bundesakademie für Sicherheitspolitik, 2023: Methoden zur strategischen Vorausschau – Megatrends (Internet).

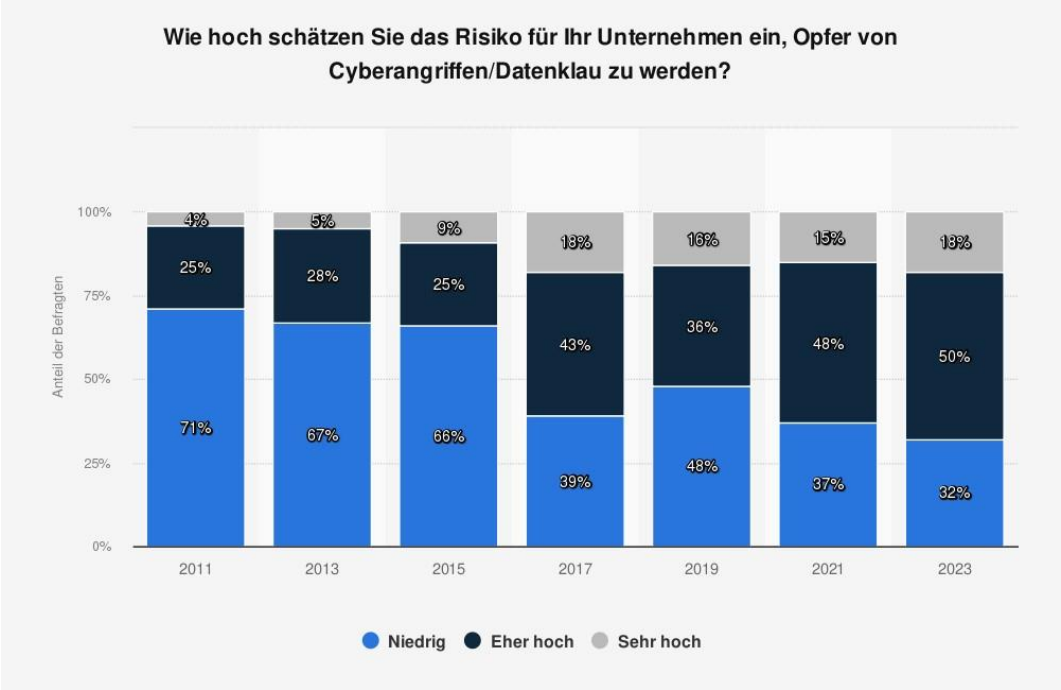
Die Bestimmung des Digitalisierungsgrads erfolgt hier nach dem Digital-Index, welcher von der Initiative D21 jährlich veröffentlicht wird, und kann zwischen 0 und 100 Punkten erreichen. Je höher die Punktzahl des Digital-Indexes ist, desto höher ist auch der Digitalisierungsgrad. Der Digital-Index setzt sich aus den Kriterien Zugang zur Digitalisierung, Nutzungsverhalten, digitale Kompetenz und Offenheit gegenüber Digitalisierung zusammen. Zu beachten ist die unterschiedliche Bewertung dieser Kriterien, wobei die digitale Kompetenz am stärksten und das Nutzungsverhalten am schwächsten gewertet wird. Von 2016 bis 2019 ist ein linearer Anstieg des Digital-Indexes erkennbar. Den höchsten Wert erreichte der Digital-Index in den Jahren 2020 bis 2022, was auf die Corona-Pandemie zurückzuführen ist.[115] Da in den nachfolgenden Jahren 2022/2023 eine starke Abnahme des Digital-Indexes von 63 Punkten auf 57 Punkten erkennbar ist, können die Auswirkungen der Corona-Pandemie auf den Digitalisierungsgrad als Anomalie oder Unregelmäßigkeit eingestuft werden, sodass sich der Digital-Index folglich nach Abklingen der Auswirkungen der Corona-Pandemie wieder in einem Normalwert einpendelt. Zu Beginn der Befragung im Jahre 2013 betrug der Wert noch 51,2 und weist zum Ende der Befragung in den Jahren 2023/2024 einen Wert von 58 vor. Mithin ist innerhalb der letzten zehn bis elf Jahre, unter Berücksichtigung der zeitweisen Schwankung während der Corona-Pandemie, ein tendenzielles Wachstum des Digitalisierungsgrades in der deutschen Gesellschaft erkennbar. Auch wenn die Corona-Pandemie lediglich eine Schwankung in dieser Statistik hervorbringt, kann aus dieser Schwankung geschlossen werden, dass die Möglichkeiten und der Bedarf digitaler Anwendungsprodukte und neuer Technologien zur Kenntnis genommen wurden und auch in Zukunft eine große Rolle spielen könnten. Durch die verallgemeinerte Betrachtung der Digitalisierung und des Verzichts auf die Konkretisierung der Digitalisierung in Bezug auf Unternehmen oder der öffentlichen Verwaltung vermeidet man eine beschränkte Betrachtung der digitalen Entwicklung und integriert zusätzlich die Bevölkerung in die Analyse des Megatrends, welche eine genauso große Rolle spielen. Die aus der Statistik erkennbare Mentalität in Bezug auf die Entwicklung der Digitalisierung lässt nämlich vermuten, dass sich das Konsumverhalten und die Bedürfnisse der

[115] Vgl. Initiative D21, Statista, 2024: Digitalisierungsgrad in Deutschland bis 2024. (Internet).

deutschen Gesellschaft weiterentwickeln und demnach ebenso Einfluss auf die Wirtschaft, Politik und dem Versicherungsmarkt haben.

3.2 Untersuchung der Cyber-Trends

Abb. 4: Risiko für Unternehmen, Opfer von Cyberangriffen/Datenklau zu werden

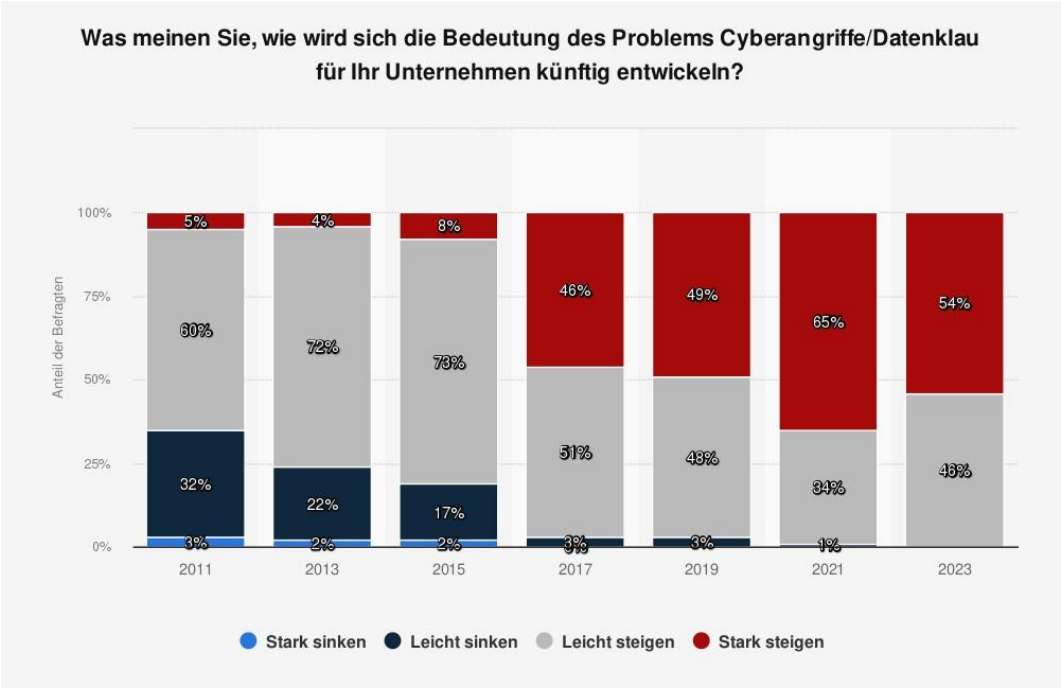


Quelle: EY, Statista, 2023: Wie hoch schätzen Sie das Risiko für Ihr Unternehmen ein, Opfer von Cyberangriffen/Datenklau zu werden? (Internet).

Abb. 4 zeigt die Risikoeinschätzung verschiedener Führungskräfte deutscher Unternehmen, Opfer von Cyberangriffen bzw. Datenklau zu werden. Hier lässt sich bereits beobachten, dass die Mehrheit der befragten Unternehmen, also 71%, im Jahre 2011 das Risiko solcher Cyberangriffe als niedrig einstufen und lediglich 25% ein eher hohes Risiko und 4% ein sehr hohes Risiko in solchen Cyberangriffen sehen. Mit dem Wandel der Digitalisierung und der damit verbundenen voranschreitenden Entwicklung hat sich auch das Meinungsbild der befragten Unternehmen gewandelt, was mit der Zeit zu stark veränderten Ergebnissen führt. Im Jahre 2023 sind inzwischen nur noch 32% der befragten Unternehmen der Meinung, dass das Risiko eines Cyberangriffs niedrig ist und bereits 50% sehen darin ein eher großes Risiko. Außerdem sind in 2023 sogar 18% der Unternehmen der Meinung im Hinblick auf Cyberangriffen einem sehr großen Risiko entgegenzutreten, was mehr als das Vierfache der ursprünglichen 4% aus dem Jahr

2011 entspricht. Dementsprechend lässt sich bei deutschen Unternehmen ein immer bedachteres Risikobewusstsein erkennen. Mit der Zeit erkennen deutsche Unternehmen also vermehrt die möglichen Gefahren verschiedener Cyberangriffe und passen ihre Risikoeinschätzung den sich wandelnden Entwicklungen der Digitalisierung an. In der nachfolgenden Abbildung 5 wird zudem erkennbar, dass sich diese Prägung des Risikobewusstseins auch in Bezug auf die Einschätzung zukünftiger Begebenheiten ausgewirkt hat:

Abb. 5: Künftige Entwicklung von Cyberangriffen/Datenklau

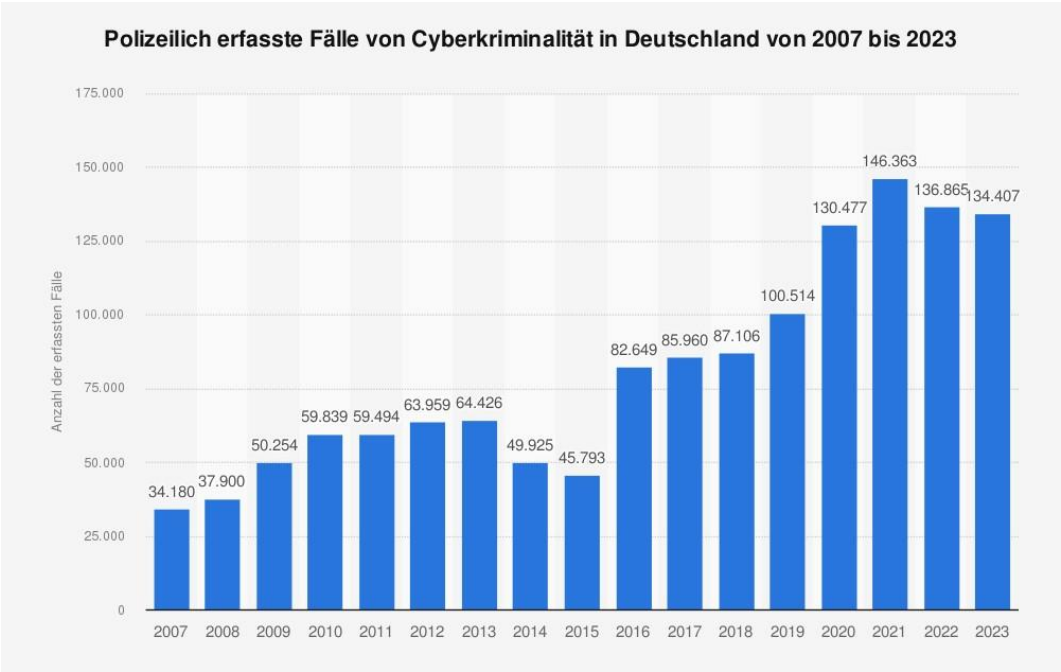


Quelle: EY, Statista, 2023: Was meinen Sie, wie wird sich die Bedeutung des Problems Cyberangriffe/Datenklau für Ihr Unternehmen künftig entwickeln?.

Hierbei wurden dieselben Unternehmen wie aus der Statistik der vorigen Abbildung 4 befragt, wie sich die Problematik von Cyberangriffen bzw. Datenklau in Zukunft entwickeln wird. Während die Mehrheit der befragten Unternehmen in den Jahren 2011, 2013 und 2015 noch meinte, einen leichten Anstieg von Cyberangriffen zu erwarten, sind in den Jahren 2019, 2021 und 2023 die Mehrheit der befragten Unternehmen inzwischen der Meinung einen starken Anstieg von Cyberangriffen zu erwarten. Besonders interessant ist der Prozentsatz an Unternehmen, die sogar der Meinung waren, dass in Zukunft die Problematik der Cyberangriffe leicht sinken oder stark sinken wird. Im Jahre 2023 vertritt kein

Unternehmen mehr diese Meinung. Die genannten Auswertungen der Statistiken sind Indizien für ein wachsendes Bedrohungspotenzial von Cyberangriffen. Die Unternehmen erwarten ein Wachstum der Bedrohungen durch Cyberangriffe und schätzen diese gefährlicher ein, als in den Jahren zuvor.

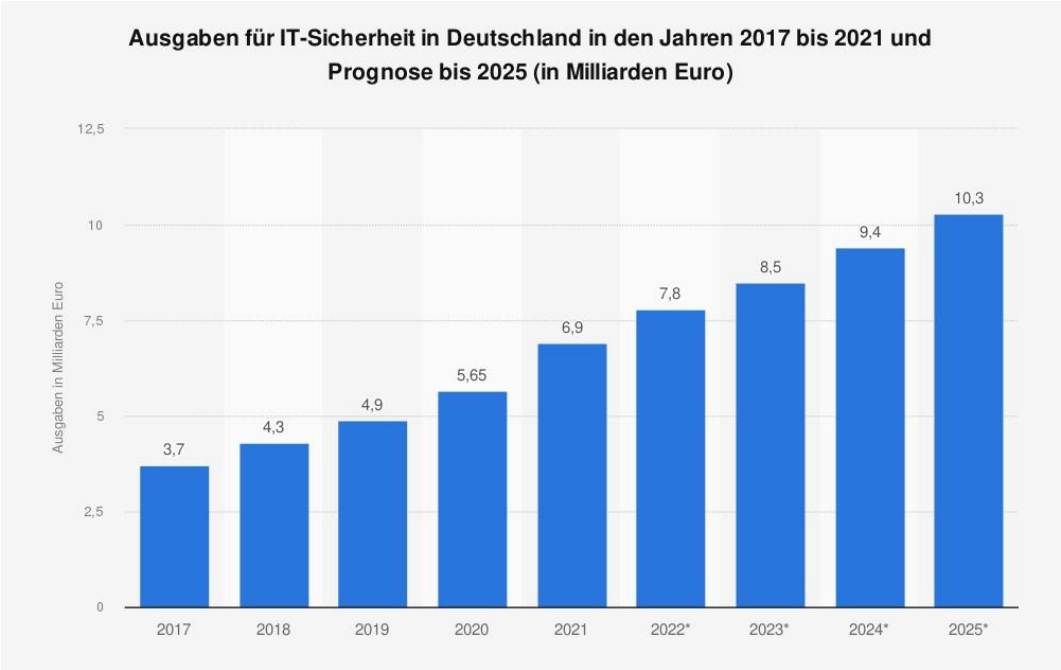
Abb. 6: Polizeilich erfasste Fälle von Cyberkriminalität in Deutschland von 2007 bis 2023



Quelle: Bundeskriminalamt, Statista, 2024: Polizeilich erfasste Fälle von Cyberkriminalität in Deutschland von 2007 bis 2023 (Internet).

Die vom Bundeskriminalamt erfassten Fälle von Cyberkriminalität in Deutschland bis 2023 bestätigen diese Vermutung. Aus der abgebildeten Statistik (Abbildung 6) ist ein tendenzielles Wachstum von Cyberkriminalität in Deutschland erkennbar. Berücksichtigt man die Entwicklung der Digitalisierung in der deutschen Gesellschaft und die Erfahrungen bzw. Meinungen der deutschen Unternehmen hinsichtlich der ausgehenden Bedrohung von Cyberangriffen, kann man von einem weiteren tendenziellen Wachstum von Cyberkriminalität und -angriffen in der Zukunft ausgehen. Dieser Trend der steigenden Cyberkriminalität in Deutschland kann nach dieser Auffassung als Kehrseite oder Schattenseite der Entwicklung der Digitalisierung bezeichnet werden und ist unweigerlich an diese gekoppelt. Da ein Anstieg der Cyberkriminalität sehr wahrscheinlich ist, liegt es im Interesse der Unternehmen sich vor den möglichen Gefahren abzusichern.

Abb. 7: Ausgaben für IT-Sicherheit in Deutschland

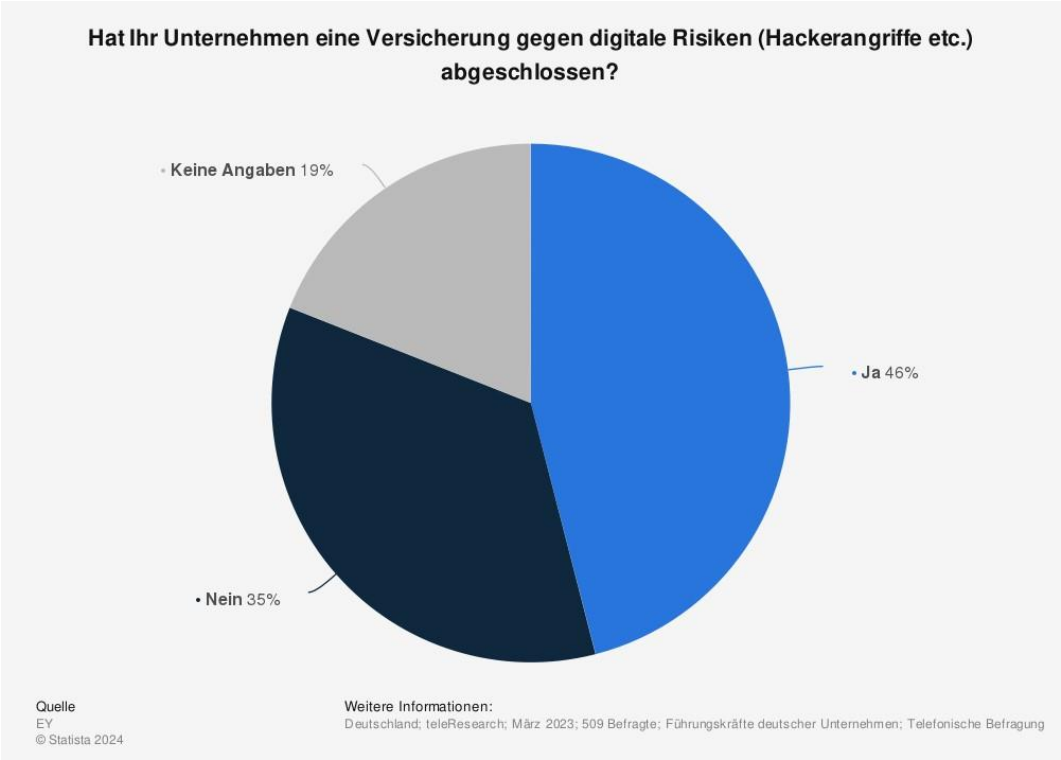


Quelle: Bitkom, Statista, 2022: Ausgaben für IT-Sicherheit in Deutschland in den Jahren 2017 bis 2021 und Prognose bis 2025 (in Milliarden Euro) (Internet).

Eine dementsprechende Reaktion auf den Anstieg der Cyberkriminalität ist mithin in der aufgezeigten Abbildung 7 ersichtlich. Mit dem tendenziellen Wachstum der Cyberkriminalität ist ein ebenso tendenzielles Wachstum von Ausgaben für IT-Sicherheit in Deutschland erkennbar. Ein weiterer wichtiger Faktor dieser Statistik sind die vorhandenen Prognosedaten für die Jahre 2024 und 2025, die einen relativ gleichmäßigen Anstieg an zukünftigen Ausgaben für IT-Sicherheit prognostizieren. Die Unternehmen weisen hier nicht nur erneut das Vorhandensein eines konkreten Risikobewusstseins auf. Vielmehr geben die Unternehmen zusätzlich zu erkennen, dass eine gewisse Bereitschaft, in die IT-Sicherheit und Maßnehmen zum Schutze gegen Cyberangriffe zu investieren, vorhanden ist und sich diese mit dem Wandel der verschiedenen Trends weiterentwickelt, was wiederum in sich einen weiteren Trend begründet. Der Fokus dieser Bachelorarbeit liegt in der Untersuchung der Cyberversicherung als mögliches Versicherungsprodukt für die DRV BW und demnach als konkrete Maßnahme gegen die ausgehende Bedrohung von Cyberangriffen. Aufgrund der in Kapitel 2.2 genannten Problematik eines nicht-einheitlichen Angebots von Cyberversicherungen, kann bei der statistischen Betrachtung auf die allgemeine Bereitschaft ein Versicherungsangebot zu wählen

abgestellt werden. So kann die Bereitschaft bezüglich der Investition in IT-Sicherheitsschutzmaßnahmen auf den Abschluss eines Versicherungsangebots konkretisiert werden, auch wenn unter dieses Versicherungsangebot nicht nur Cyberversicherungen, sondern eben auch solche Versicherungen gefasst werden können, die einen entsprechenden Schutz bieten.

Abb. 8: Versicherung gegen digitale Risiken bei deutschen Unternehmen



Quelle: EY, Statista, 2023: Hat Ihr Unternehmen eine Versicherung gegen digitale Risiken (Hackerangriffe etc.) abgeschlossen? (Internet).

Aus Abb. 8 geht hervor, dass im Jahre 2023 die Mehrheit der Unternehmen, die Angaben zu dem Abschluss einer Versicherung gegen digitale Risiken gemacht haben, auch bereits eine solche Versicherung abgeschlossen haben: 46% der befragten Unternehmen haben bereits eine Versicherung gegen digitale Risiken abgeschlossen, während 35% eine solche Versicherung noch nicht abgeschlossen haben und 19% der Unternehmen keine Angaben gemacht haben. Dies untermauert die Erkenntnis über die erhöhte Bereitschaft zur Absicherung gegen Cyberangriffe und derartige Bedrohungen. Der dennoch relativ große Anteil an Unternehmen, welcher noch keine Versicherung gegen Cyberrisiken abgeschlossen hat, könnte bspw. auf den mangelnden Bedarf aufgrund eines niedrig bewerteten Risikos

zurückzuführen sein. Ist die Gefahrenlage von Cyberangriffen für das jeweilige Unternehmen eher gering, dürfte der Abschluss einer Versicherung gegen Cyberrisiken als überflüssig eingeschätzt werden und das Unternehmen könnte sich mit den eigenen internen Risikomaßnahmen zufriedengeben. Der hier erforschte Trend bezüglich des Abschlusses einer Versicherung gegen Cyberrisiken ist an die vorangehend untersuchten Trends und den Megatrend gekoppelt. Man könnte auch von einer Kausalkette sprechen. Je digitalisierter die deutsche Gesellschaft wird, desto höher ist das Risiko von Cyberangriffen einzuschätzen. Die Unternehmen reagieren auf den Anstieg der Cyberrisiken und entwickeln ein zunehmendes Risikobewusstsein. Insoweit sind Unternehmen bereit höhere Ausgaben für den Erhalt und die Verbesserung der IT-Sicherheit zu kalkulieren. Dazu gehören ebenfalls Ausgaben, die im Zuge des Abschlusses einer Versicherung gegen Cyberrisiken entstehen.

Im Zuge der Trendforschung lassen sich die herausgearbeiteten Ergebnisse auf die Anwendbarkeit von Cyberversicherungen übertragen. Mithilfe der untersuchten Trends können die Ergebnisse des untersuchten Forschungsstandes ergänzt werden und in einer Prognose über die aktuelle aber auch zukünftige Zweckmäßigkeit von Cyberversicherungen zusammengefasst werden.

4 Prognose und Schlussfolgerung

Aus der Analyse der verschiedenen Trends können verschiedene Aussagen über den Cyberversicherungsmarkt und die Relevanz von Cyberversicherungen für die DRV BW abgeleitet werden:

Grds. ist die Digitalisierung nicht nur für die öffentliche Verwaltung, sondern auch für die Gesellschaft in Deutschland als „Wegbegleiter in die Zukunft“ zu klassifizieren. Der digitale Fortschritt weist ein immer stärker werdendes Wachstum auf und findet so immer neue Wege sich in der Gesellschaft zu etablieren. Eine solch einflussreiche Entwicklung lässt sich somit zurecht nur als Megatrend beschreiben und die tendenzielle Entwicklung zu einer zunehmend digitalisierten Gesellschaft dürfte nicht nur viele Jahre, sondern sogar viele Jahrzehnte andauern. Somit kann davon ausgegangen werden, dass die Gesellschaft sich vermehrt mit dem Thema Digitalisierung auseinandersetzen und sich nicht nur mit den neu

geschaffenen Möglichkeiten und Chancen der Digitalisierung, sondern auch mit den einhergehenden Cyberrisiken vertraut machen und dementsprechend jeweilige Schutzmaßnahmen anpassen und verbessern wird. Dennoch scheinen die Fälle von Cyberkriminalität weiter zu steigen und aus Abbildung 6 kann zudem auch ein weiterer Anstieg in den kommenden Jahren vermutete werden. Hacker und anderweitige Kriminelle weisen demnach ein adaptives Verhalten auf, passen sich den verändernden Umständen und neuen Schutzmaßnahmen an und entwickeln sich ebenfalls weiter. Die ausgehende Gefahr von Cyberrisiken darf mithin nicht unterschätzt werden und könnte in den nachfolgenden Jahren ein großes, wenn nicht sogar immer größer werdendes, Problem darstellen. Aus Abbildung 4 geht hervor, dass das deutsche Unternehmen zunehmend genauso sehen und sich die Wahrnehmung in Bezug auf Cyberrisiken fortlaufend wandelt. Cyberversicherungen spielen mithin ebenfalls eine wichtige Rolle für die zukünftige Entwicklung verschiedenster Unternehmen, darunter auch der DRV BW. Vor allem öffentliche Behörden sehen sich durch die steigende Anzahl an Ransomware- und ähnlichen Cyberangriffen bedroht und müssen dem steigenden Risiko durch die Weiterentwicklung der Digitalisierung entgegenwirken. Selbstverständlich sind Sicherheitsmaßnahmen wie ein Risikomanagement, den Erhalt der IT-Sicherheit, Schulungen der Mitarbeiter und die Schaffung eines gewissen Risikobewusstseins unerlässlich für die Gewährung eines angemessenen Maßes an Schutz gegen Cyberangriffen. Die DRV BW ist in dieser Hinsicht hervorragend ausgestattet, was der angewendete branchenspezifische Sicherheitsstandard, die gebotene Transparenz rund um das Thema Datenverarbeitung und das Bestreben, die IT-Sicherheit einer kontinuierlichen Überprüfung und Verbesserung zu unterziehen, zeigen. Dennoch zeigt bereits Abbildung 6, dass kein vollumfänglicher Schutz gegen Cyberrisiken gewährt werden kann. Sollten Kriminelle mit ihrem, durch einen Cyberangriff ausgeführtem, Vorhaben Erfolg haben, könnte das fatale Folgen für die Behörden der öffentlichen Verwaltung und so auch für die DRV BW mit sich ziehen. Unberechtigte Dritte könnten sich bspw. Zugang zu verschiedensten Daten von Bürgern verschaffen und diese Daten manipulieren, löschen oder weiterverkaufen, sodass dem Bürger ein Schaden entstehen kann. Die DRV BW hat als öffentliche

Behörde und damit als Vertreter des Staates ein großes Interesse den Bürger vor der Gefährdung seiner Daten zu schützen, was auch aus dem Sozialstaatsprinzip aus Art. 20 Abs. 1 GG hervorgeht. Da die DRV BW als öffentliche Behörde und im gesetzlichen Rahmen der verschiedenen Sozialgesetzbücher unzählige Versichertendaten verarbeitet, kann allerdings das Ausmaß eines erfolgreichen Cyberangriffs nur schwer eingeschätzt werden. Es gilt zukünftige Entwicklungen der Digitalisierung und der Cyberkriminalität zu untersuchen und die Gefahren stets neu einzuschätzen. Die Versicherer müssen das gebotene Risiko angemessen tragen können, ohne sich selbst übermäßig zu belasten. Die DRV BW kann hierbei mit einem jeweiligen Versicherer Vertragsverhandlungen durchführen, aus denen eine individuelle Risikoeinschätzung erfolgt und evtl. eigene Präventionsmaßnahmen wie die Struktur eines ISMS oder das Risikomanagement an verschärfte Bedingungen gebunden ist, um den Versicherer ebenfalls zu entlasten. Kumulrisiken stellen hierbei dennoch ein großes Problem dar. Die enorme Reichweite eben besagter Kumulrisiken kann unvorstellbare Größenordnungen annehmen und den Deckungsrahmen der Versicherer, trotz korrekter Risikoeinschätzung und verschärfter Präventionsmaßnahmen von Seiten der DRV BW, sprengen. Verschiedene Formen des alternativen Risikotransfers wie bspw. Cat-Bonds können dieses scheinbar untragbare Risiko auf den Kapitalmarkt verlagern und ermöglichen die Deckung von enormen Schadenssummen. Diese Deckungstranchen sind auf dem Versicherungsmarkt für Cyber zwar noch relativ neu, bieten allerdings zuversichtliche Aussichten auf die zukünftige Entwicklung von Cyberversicherungen. Das Risiko Opfer eines Cyberangriffes zu werden steigt und wird mit der fortlaufenden Digitalisierung wohl auch nicht sinken. Aus diesem Umstand lässt sich bereits die wachsende Nachfrage nach Absicherung von Cyberrisiken erkennen und kann Versicherer zu einem Ausbau des Cyberversicherungsschutzes anregen, indem diese das Risiko verbriefen und auf den Kapitalmarkt transferieren. Durch die Schaffung dieser Deckungstranchen könnten somit nicht nur bestehende Versicherer ihr Versicherungsangebot ausbauen, sondern auch neue Versicherer auf dem Versicherungsmarkt auftreten. Mit einem ausgebauten Versicherungsangebot und einer größeren Auswahl an Versicherern, die mehr Sicherheiten versprechen können, wächst vermutlich auch

das Interesse der Versicherungsnehmer den Abschluss einer Cyberversicherung in Betracht zu ziehen. Cyberversicherungen haben mithin ein gewisses Grundgerüst, welches viel Potenzial für weiteres Wachstum in Aussicht stellt. Das erarbeitete Konzept für Rahmenbedingungen eines Versicherungsvertrages aus Kapitel 2.2.2 kann für die DRV BW Anwendung finden und einen angemessenen Versicherungsschutz gewähren. Nach Untersuchung der verschiedenen Trends im Bereich Cyber und der Gefahrenlage von Cyberrisiken scheint eine solche zusätzliche Absicherung auch dringend nötig. Die DRV BW wird sich dem digitalen Wandel, wie auch andere Behörden der öffentlichen Verwaltung, fügen und die hausinterne Digitalisierung ausbauen. Die Gesellschaft in Deutschland gibt zu erkennen, dass der Ausbau der Digitalisierung durchaus gefragt ist und so haben auch die öffentlichen Behörden, wie die DRV BW, die Pflicht i.S.d. der Daseinsfürsorge und dem Sozialstaatsprinzip die Interessen der Bürger innerhalb der Privatwirtschaft auf die öffentliche Verwaltung zu übertragen und einen Mindeststandard an Digitalisierung zu erfüllen. Diese Erkenntnis lässt die Vermutung zu, dass Kriminelle mehr Schwachstellen in verschiedensten IT-Systemen der DRV BW lokalisieren können und das Risiko eines schädigenden Ereignisses, bspw. eines Cyberangriffs, steigt. Folglich erscheint die zusätzliche Absicherung gegen Cyberrisiken in Form einer Cyberversicherung für die DRV BW mehr als sinnvoll. Auch wenn die Untersuchung der einzelnen Bausteine der AVB Cyber in Kapitel 2.2.1 einzelne Leistungen für die Anwendung der AVB Cyber auf die öffentliche Verwaltung und konkret die DRV BW ausschließt, sichern die in das konstruierte Konzept nach Abbildung 1 aufgenommenen Leistungen der einzelnen Bausteine Unterstützung und Sicherheit im Falle eines Versicherungsfalles, also bspw. eines Hackerangriffes, zu. Konkrete Vereinbarungen für die Ausfertigung eines jeweiligen Versicherungsvertrages sind abhängig von den jeweiligen Bedürfnissen der DRV BW und den Anforderungen, die der gewählte Versicherer fordert.

5 Ausblick und Fazit

Cyberversicherungen begründen eine noch relativ junge Versicherungssparte und müssen sich dementsprechend erst auf dem Versicherungsmarkt etablieren. Mit dem Anstieg des Digitalisierungsgrades der Bevölkerung in Deutschland haben Cyberversicherungen großes Potenzial auch in Zukunft an Relevanz zu gewinnen und mehr Aufmerksamkeit auf sich zu ziehen. Besonders die Behörden der öffentlichen Verwaltung geraten vermehrt in das Visier von Cyber-Kriminellen und können vom Versicherungsschutz einer Cyberversicherung stark profitieren. Diese Gegebenheiten können im Zusammenhang mit den geschaffenen Deckungstranchen dazu führen, dass mit der Zeit ein einheitliches Konzept von Versicherungsbedingungen für Cyberversicherungen realisiert wird. Sobald Cyberversicherungen auf dem Versicherungsmarkt adäquat Fuß gefasst haben, kann sogar über eine gesetzlich verankerte Pflicht von Unternehmen, insbesondere öffentlicher Behörden, bezüglich des Abschlusses einer Cyberversicherung diskutiert werden. Angesichts der Tatsache, dass sich die Gesellschaft nach und nach dem Fortschritt der Digitalisierung fügt und Cyberrisiken somit immer relevanter werden, insbesondere in Bezug auf die innerhalb öffentlicher Behörden gespeicherten und verarbeiteten Daten der Bürger, ist der Gedanke einer gesetzlichen Verpflichtung nicht abwegig. Immerhin geht es um die Daten der Bürger und das Wohl der Bürger sollte für den Staat an erster Stelle stehen. Die Entwicklungen auf dem Versicherungsmarkt können nicht hundertprozentig vorhergesagt werden. Unabhängig hiervon werden Cyberversicherungen im Zuge der voranschreitenden Digitalisierung stets ein relevantes Gesprächsthema darstellen, und das nicht nur für die DRV BW oder die öffentliche Verwaltung, sondern auch für die Bürger im privaten Sektor.

6 Anhang

Anhang 1: Erfasste Daten

Welche Daten werden erfasst und warum

Wenn Ihr Versicherungsleben vollständig erfasst ist, können wir sachgerecht über Ihren Antrag entscheiden. Dazu benötigen wir alle relevanten Informationen und Unterlagen, die für die Leistungserbringung wichtig sind.

Wir erheben grundsätzlich folgende Daten:
- → Identifizierungs- und Kontaktdaten,
- → berufliche Informationen,
- → soziale Informationen,
- → familiäre Informationen,
- → Finanz- und Zahlungsdaten und
- → Gesundheitsdaten.

Dank Ihrer Mithilfe können Ihre Angelegenheiten durch unsere Mitarbeiter rasch erledigt werden.

Die Speicherung Ihrer Daten erfolgt in der Regel elektronisch in Form von digitalen Akten.

Bitte bedenken Sie, dass wir Ihnen, falls uns nicht alle relevanten Daten vorliegen, eine

4

Quelle aus: *Datenschutz: Ihre Daten – Ihre Rechte*, S. 4, Download verfügbar unter: https://www.deutsche-rentenversicherung.de/SharedDocs/Downloads/DE/Broschueren/national/datenschutz_ihre_daten_und_ihre_rechte.html.

Anhang 2: Speicherung der Daten

Was mit Ihren Daten geschieht

Daten, die Sie uns mitteilen, sind in der Regel auch nur für uns gedacht. Manchmal benötigen aber auch andere Stellen oder Personen diese Daten.

Wo Ihre Daten gespeichert werden

Wir führen für Sie ein elektronisches Versicherungskonto sowie elektronische Akten. Hier werden alle wichtigen Daten zu Ihrer Person gespeichert. Als Ordnungsmerkmal dient dabei Ihre Versicherungsnummer. Die individuelle Versicherungsnummer ist eine Kennziffer, die jeder Versicherte zur Zuordnung seiner Daten erhält. Sie enthält unter anderem Ihr Geburtsdatum und den Anfangsbuchstaben Ihres Geburtsnamens.

Die Versicherungsnummer ist mit der Kontonummer einer Bank vergleichbar und macht Sie in der Rentenversicherung unverwechselbar. Sie müssen sie bei Ihrem Arbeitgeber oder, wenn Sie arbeitslos werden, bei der Agentur für Arbeit oder dem Jobcenter angeben.

14

Quelle aus: *Datenschutz: Ihre Daten – Ihre Rechte*, S. 14, Download verfügbar unter: https://www.deutsche-rentenversicherung.de/SharedDocs/Downloads/DE/Broschueren/national/datenschutz_ihre_daten_und_ihre_rechte.html.

Anhang 3: Zugriff und Weitergabe der Daten

Wer Ihre Daten lesen darf

Ein umfassender Einblick in sämtliche Daten aller Versicherten und Rentner ist für die Mitarbeiter der Rentenversicherung grundsätzlich nicht möglich.

Wir dürfen nur dann auf Ihre Sozialdaten zugreifen, wenn und soweit dies notwendig ist, um Ihre Ansprüche zu erfüllen und den sonstigen Aufgaben nach dem Sozialgesetzbuch nachzukommen. Das wird durch geeignete organisatorische und technische Maßnahmen sichergestellt.

Wann wir Ihre Daten weitergeben

Grundsätzlich dürfen Ihre Daten Dritten nicht zur Kenntnis gelangen. Das ist nur in Ausnahmefällen zulässig, wenn eine Vorschrift aus dem Sozialgesetzbuch eine Datenübermittlung ausdrücklich vorsieht oder wenn Sie ausdrücklich eingewilligt haben.

An wen wir Ihre Daten weitergeben dürfen

Mit Ihrer Einwilligung dürfen wir Sozialdaten an alle Stellen oder Personen übermitteln. Ohne Ihre Einwilligung ist eine Übermittlung Ihrer Sozialdaten nur zulässig an

- → Sozialleistungsträger (hierzu gehören insbesondere andere Rentenversicherungsträger, Arbeitsagenturen, gesetzliche Krankenkassen, Versorgungsämter, Berufsgenossenschaften, Kindergeldstellen, Wohnungsämter, Sozialämter, Jugendämter und Grundsicherungsämter),
- → Polizeibehörden, Staatsanwaltschaften, Gerichte, Behörden der Gefahrenabwehr und Justizvollzugsanstalten,
- → Behörden, gegenüber denen besondere gesetzliche Pflichten und Mitteilungs-

15

befugnisse bestehen, zum Beispiel bei Strafverfolgungsbehörden, Gesundheitsämtern, im Besteuerungsverfahren bei Finanzämtern, der Zentralen Zulagenstelle für Altersvermögen (Riester-Rente), bei den zur Bekämpfung von Schwarzarbeit zuständigen Behörden oder beim Statistischen Bundesamt,

- → die Behörden für Verfassungsschutz, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und das Bundeskriminalamt,
- → Privatpersonen in Unterhaltsanspruchs- oder Versorgungsausgleichsangelegenheiten (dies aber nur, wenn Sie Ihren eigenen Mitteilungspflichten gegenüber diesen Personen nicht nachkommen),
- → öffentliche Stellen, soweit diese öffentlich-rechtliche Ansprüche geltend machen,
- → Gerichtsvollzieher zur Durchführung eines Vollstreckungsverfahrens,
- → die Finanzverwaltung im Rahmen des sogenannten Rentenbezugsmitteilungsverfahrens (unabhängig von Ihrer eventuellen Pflicht, eine Steuererklärung abzugeben) und im Falle eines Anspruchs auf Grundrentenzuschlag und
- → den Rentenservice der Deutschen Post AG (zur Auszahlung Ihrer Rente).

16

Bitte beachten Sie:
Wir geben Ihre Daten nur dann an Dritte weiter, wenn die besonderen gesetzlichen Voraussetzungen dafür erfüllt sind oder wenn Sie darin eingewilligt haben.

Zur Erfüllung unserer gesetzlichen Aufgaben können wir erforderliche Daten auch an andere Dienstleister übermitteln (zum Beispiel externe Rehabilitationseinrichtungen, medizinische Labore, Übersetzungsbüros). Die Verpflichtung zum Schutz Ihrer Sozialdaten wird dabei auf den Dienstleister übertragen.

Wann wir Ihre Daten ins Ausland übermitteln dürfen
Grundsätzlich dürfen wir nur bei einem Auslandsbezug Ihre Daten ins Ausland übermitteln, beispielsweise wenn Sie einen Wohnort außerhalb Deutschlands oder im Ausland gearbeitet haben.

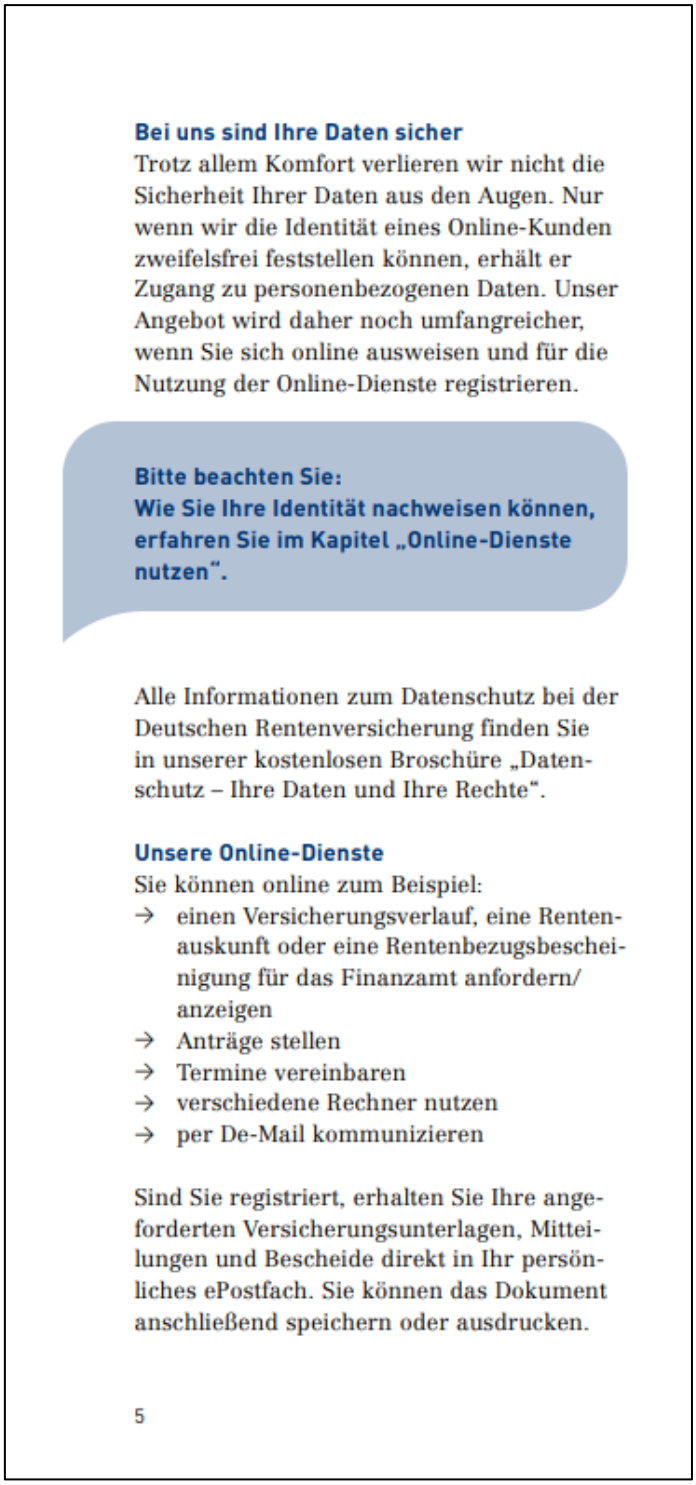
An ausländische Versicherungsträger innerhalb der Europäischen Union dürfen wir Ihre Daten übermitteln, wenn diese Versicherungsträger diese Daten für ihre Aufgabenerfüllung benötigen oder Sie der Übermittlung zugestimmt haben.

Ihre Daten dürfen wir nur dann außerhalb der Europäischen Union übermitteln, wenn es zwischenstaatliche Abkommen auf dem Gebiet der sozialen Sicherung gibt und die Daten zur Aufgabenerfüllung benötigt werden oder Sie der Übermittlung zugestimmt haben.

17

Quelle aus: *Datenschutz: Ihre Daten – Ihre Rechte*, S. 15-17, Download verfügbar unter: https://www.deutsche-rentenversicherung.de/SharedDocs/Downloads/DE/Broschueren/national/datenschutz_ihre_daten_und_ihre_rechte.html.

Anhang 4: Online-Dienste der DRV



Bei uns sind Ihre Daten sicher
Trotz allem Komfort verlieren wir nicht die Sicherheit Ihrer Daten aus den Augen. Nur wenn wir die Identität eines Online-Kunden zweifelsfrei feststellen können, erhält er Zugang zu personenbezogenen Daten. Unser Angebot wird daher noch umfangreicher, wenn Sie sich online ausweisen und für die Nutzung der Online-Dienste registrieren.

Bitte beachten Sie:
Wie Sie Ihre Identität nachweisen können, erfahren Sie im Kapitel „Online-Dienste nutzen".

Alle Informationen zum Datenschutz bei der Deutschen Rentenversicherung finden Sie in unserer kostenlosen Broschüre „Datenschutz – Ihre Daten und Ihre Rechte".

Unsere Online-Dienste
Sie können online zum Beispiel:
- → einen Versicherungsverlauf, eine Rentenauskunft oder eine Rentenbezugsbescheinigung für das Finanzamt anfordern/anzeigen
- → Anträge stellen
- → Termine vereinbaren
- → verschiedene Rechner nutzen
- → per De-Mail kommunizieren

Sind Sie registriert, erhalten Sie Ihre angeforderten Versicherungsunterlagen, Mitteilungen und Bescheide direkt in Ihr persönliches ePostfach. Sie können das Dokument anschließend speichern oder ausdrucken.

5

Quelle aus: *Nur einen Klick entfernt: Ihre Rentenversicherung*, S. 5, Download verfügbar unter: https://www.deutsche-rentenversicherung.de/SharedDocs/Downloads/DE/Broschueren/national/nur_ein_klick_entfernt.html.

Anhang 5: Datenverarbeitung

An wen Sie sich wenden können

Wenn Sie Fragen zum Datenschutz haben oder Ihre Rechte geltend machen wollen: Wir sind der richtige Ansprechpartner.

Verantwortlich für die Datenverarbeitung ist Ihr Rentenversicherungsträger. Er verarbeitet Ihre personenbezogenen Daten auf der Grundlage der europaweit geltenden Datenschutz-Grundverordnung (DSGVO) und der datenschutzrechtlichen Bestimmungen der Sozialgesetzbücher.

Unser Tipp:

Die wichtigsten Regelungen finden Sie in § 35 SGB I – Sozialgeheimnis – und im zweiten Kapitel SGB X – Schutz der Sozialdaten – ausführlich kommentiert im Internet unter rvrecht.deutsche-rentenversicherung.de.

Fühlen Sie sich in Ihren Rechten verletzt, weil Sie vermuten, dass Ihre personenbezogenen Daten nicht korrekt verwendet

26

werden, oder haben Sie Fragen zum Datenschutz, dann können Sie sich direkt an den Datenschutzbeauftragten Ihres Rentenversicherers wenden. Für Ihre Fragen per E-Mail haben wir auf der nächsten Seite die entsprechenden Adressen zusammengestellt. Natürlich sind wir auch schriftlich oder telefonisch erreichbar. Im Kapitel „Nur einen Schritt entfernt: Ihre Rentenversicherung" ab Seite 31 finden Sie alle notwendigen Informationen.

Auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sowie die Landesbeauftragten für den Datenschutz sind mögliche Anlaufstellen für Sie.

Kontaktdaten der Datenschutzbeauftragten und der Datenschutzaufsichtsbehörden

Deutsche Rentenversicherung ...	Datenschutzbeauftragter	Datenschutzaufsichtsbehörden
Baden-Württemberg post@drv-bw.de	datenschutz beauftragter@ drv-bw.de De-Mail: datenschutz@ drv-bw.de-mail.de	Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg Lautenschlagerstraße 20 70173 Stuttgart Telefon: 0711 615541-0 Telefax: 0711 615541-15 poststelle@lfdi.bwl.de
Bayern Süd service@drv-bayernsued.de	datenschutz@ drv-bayernsued.de	Der Bayerische Landesbeauftragte für den Datenschutz Postfach 22 12 19, 80502 München (Wagmüllerstr. 18, 80538 München) Telefon: 089 212672-0 Telefax: 089 212672-50 poststelle@datenschutz-bayern.de

Deutsche Rentenver-sicherung ...	Datenschutz-beauftragter	Datenschutz-aufsichtsbehörden
Berlin-Brandenburg post@drv-berlin-brandenburg.de	datenschutz@drv-berlin-brandenburg.de De-Mail: datenschutz@drv-berlin-brandenburg.de-mail.de	Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Stahnsdorfer Damm 77 14532 Kleinmachnow Telefon: 033203 356-0 Telefax: 033203 356-49 poststelle@lda.brandenburg.de
Braun-schweig-Hannover info@drv-bsh.de	datenschutz@drv-bsh.de	Die Landesbeauftragte für den Datenschutz Niedersachsen Prinzenstraße 5 30159 Hannover Telefon: 0511 120-4500 Telefax: 0511 120-4599 poststelle@lfd.niedersachsen.de
Hessen post@drv-hessen.de	datenschutz@drv-hessen.de	Der Hessische Datenschutz-beauftragte Postfach 31 63 65021 Wiesbaden Telefon: 0611 1408-0 poststelle@datenschutz.hessen.de
Mittel-deutschland service@drv-md.de	datenschutz@drv-md.de	Die Sächsische Datenschutz- und Transparenzbeauftragte Postfach 11 01 32 01330 Dresden Telefon: 0351 85471-101 Telefax: 0351 85471-109 post@sdtb.sachsen.de
Nord info@drv-nord.de	datenschutz@drv-nord.de	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Holstenstr. 98 24103 Kiel Telefon: 0431 988-1200 Telefax: 0431 988-1223 mail@datenschutzzentrum.de

28

Deutsche Rentenver-sicherung ...	Datenschutz-beauftragter	Datenschutz-aufsichtsbehörden
Nordbayern info@drv-nordbayern.de	datenschutz-sicherheit@drv-nordbayern.de	Der Bayerische Landesbeauftragte für den Datenschutz Postfach 22 12 19 80502 München (Wagmüllerstr. 18, 80538 München) Telefon: 089 212672-0 Telefax: 089 212672-50 poststelle@datenschutz-bayern.de
Oldenburg-Bremen info@drv-oldenburg-bremen.de	datenschutz@drv-oldenburg-bremen.de	Die Landesbeauftragte für den Datenschutz Niedersachsen Prinzenstraße 5 30159 Hannover Telefon: 0511 120-4500 Telefax: 0511 120-4599 poststelle@lfd.niedersachsen.de
Rheinland post@drv-rheinland.de	datenschutz beauftragter@drv-rheinland.de	Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen Postfach 20 04 44 40102 Düsseldorf Telefon: 0211 38424-0 Telefax: 0211 38424-10 poststelle@ldi.nrw.de
Rheinland-Pfalz service@drv-rlp.de	datenschutz@drv-rlp.de	Der Landesbeauftragte für den Datenschutz und die Informations-freiheit Rheinland-Pfalz Postfach 30 40 55020 Mainz Telefon: 06131 208-2449 Telefax: 06131 208-2497 poststelle@datenschutz.rlp.de
Saarland service@drv-saarland.de	datenschutz@drv-saarland.de	Unabhängiges Datenschutz-zentrum Saarland Fritz-Dobisch-Straße 12 66111 Saarbrücken Telefon: 0681 94781-0 Telefax: 0681 94781-29 poststelle@datenschutz.saarland.de

29

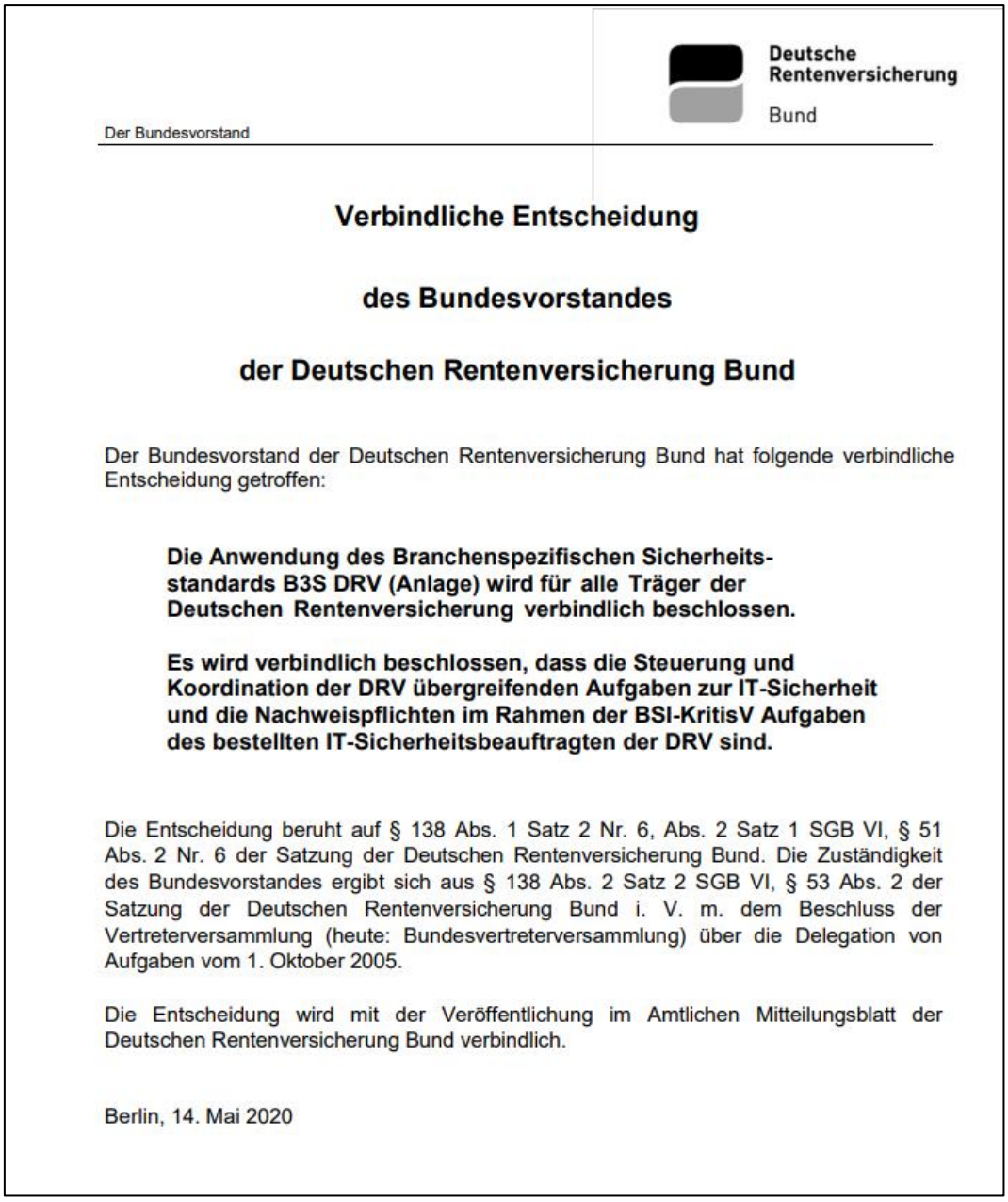
Deutsche Rentenver-sicherung ...	Datenschutz-beauftragter	Datenschutz-aufsichtsbehörden
Schwaben info@drv-schwaben.de	datenschutz@drv-schwaben.de	Der Bayerische Landesbeauftragte für den Datenschutz Postfach 22 12 19 80502 München (Wagmüllerstr. 18, 80538 München) Telefon: 089 212672-0 Telefax: 089 212672-50 poststelle@datenschutz-bayern.de
Westfalen kontakt@drv-westfalen.de	datenschutz@drv-westfalen.de	Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen Postfach 20 04 44 40102 Düsseldorf Telefon: 0211 38424-0 Telefax: 0211 38424-999 poststelle@ldi.nrw.de
Bund drv@drv-bund.de	datenschutz-drv-bund@drv-bund.de De-Mail: datenschutz-drv-bund@drv-bund.de-mail.de	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Graurheindorfer Str. 153 53117 Bonn Telefon: 0228 9977990-0 poststelle@bfdi.bund.de
Knappschaft-Bahn-See rentenversicherung@kbs.de	datenschutz@kbs.de	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Graurheindorfer Str. 153 53117 Bonn Telefon: 0228 9977990-0 poststelle@bfdi.bund.de

Bitte achten Sie darauf, dass Ihre E-Mail an uns keine vertraulichen Informationen enthält. Warum das wichtig ist, lesen Sie im Abschnitt „Datenaustausch per E-Mail" auf Seite 22.

30

Quelle aus: *Datenschutz: Ihre Daten – Ihre Rechte*, S. 26-30, Download verfügbar unter: https://www.deutsche-rentenversicherung.de/SharedDocs/Downloads/DE/Broschueren/national/nur_einen_klick_entfernt.html.

Anhang 6: Branchenspezifischer Sicherheitsstandard



Deutsche Rentenversicherung Bund

Der Bundesvorstand

Verbindliche Entscheidung

des Bundesvorstandes

der Deutschen Rentenversicherung Bund

Der Bundesvorstand der Deutschen Rentenversicherung Bund hat folgende verbindliche Entscheidung getroffen:

Die Anwendung des Branchenspezifischen Sicherheitsstandards B3S DRV (Anlage) wird für alle Träger der Deutschen Rentenversicherung verbindlich beschlossen.

Es wird verbindlich beschlossen, dass die Steuerung und Koordination der DRV übergreifenden Aufgaben zur IT-Sicherheit und die Nachweispflichten im Rahmen der BSI-KritisV Aufgaben des bestellten IT-Sicherheitsbeauftragten der DRV sind.

Die Entscheidung beruht auf § 138 Abs. 1 Satz 2 Nr. 6, Abs. 2 Satz 1 SGB VI, § 51 Abs. 2 Nr. 6 der Satzung der Deutschen Rentenversicherung Bund. Die Zuständigkeit des Bundesvorstandes ergibt sich aus § 138 Abs. 2 Satz 2 SGB VI, § 53 Abs. 2 der Satzung der Deutschen Rentenversicherung Bund i. V. m. dem Beschluss der Vertreterversammlung (heute: Bundesvertreterversammlung) über die Delegation von Aufgaben vom 1. Oktober 2005.

Die Entscheidung wird mit der Veröffentlichung im Amtlichen Mitteilungsblatt der Deutschen Rentenversicherung Bund verbindlich.

Berlin, 14. Mai 2020

Quelle aus: *Deutsche Rentenversicherung – Branchenspezifischer Sicherheitsstandard*, Download verfügbar unter: https://www.deutsche-rentenversicherung.de/SharedDocs/Downloads/DE/Selbstverwaltung/20200810_branchenspezif_sicherheitsstandard_pdf.html.

Anhang 7: Risikoanalyse und Gefährdungslage

3.4.3 Berücksichtigung von Abhängigkeiten bei der Risikoanalyse

Da die IT-Systeme vollständig durch die DRV selbst sowie die eigenen IT-Dienstleister der DRV (Gesellschafter der IT-Dienstleister sind ausschließlich RVTR der DRV) betrieben werden, existieren keine Abhängigkeiten zu IT-Systemen Dritter.

Innerhalb der DRV sind übergreifend die Zuständigkeiten aller relevanten dezentralen und zentralen Verfahren, IT-Systeme und Infrastrukturen festzulegen, um eine vollständige Bewertung im Rahmen der Risikoanalysen zu gewährleisten.

Es muss dabei sichergestellt werden, dass die verfahrensspezifischen Risikoanalysen der RVTR sowohl auf die Risikoanalysen der relevanten Infrastrukturen als auch auf die Risikoanalysen der zentralen Verfahren (z.B. rvDialog) referenzieren.

Die externen Anbieter von Dienstleistungen sowie der externe Betreiber des DRV-WAN müssen die Mindestanforderungen der DRV über vertragliche Regelungen erfüllen.

3.4.4 Berücksichtigung der allgemeinen Gefährdungslage

Die allgemeine Gefährdungslage für die kDL-relevanten Systeme muss laufend überprüft werden. Dazu sind u.a. die Hinweise des BSI auf aktuelle Gefahrenlagen und weitere verfügbare Warnungen zu beachten.

Dabei müssen insbesondere berücksichtigt werden:

- allgemeine Bedrohungen und geänderte Gefährdungslage, z.B.
    - neu hinzugekommene Typen von Angreifern und Angriffen,
    - intensivere Aktivität oder verbesserte Expertise / Ressourcen von Angreifern,
    - Neuausrichtung von Angreifern,
- bekannt gewordene neue Schwachstellen,
- Änderungen der Gefährdungslage durch Veränderungen an der Systemarchitektur.

Die Berücksichtigung der allgemeinen Gefährdungslage erfolgt aufgrund der technischen und verfahrensbezogen Vernetzung und Zusammenarbeit in der DRV federführend durch das CERT-DRV (Computer Emergency Response Team), welches die relevanten Informationen intern weitergibt und die internen Prozesse koordiniert.

Quelle aus: *Deutsche Rentenversicherung – Branchenspezifischer Sicherheitsstandard*, S. 19, Download verfügbar unter: https://www.deutsche-rentenversicherung.de/SharedDocs/Downloads/DE/Selbstverwaltung/20200810_branchenspezif_sicherheitsstandard_pdf.html.

Anhang 8: Sicherheitskonzeption der DRV

4 Teil 2: Sicherheitsanforderungen nach Stand der Technik und Vorgehensweisen

4.1 Informationssicherheitsmanagementsystem (ISMS)

Ein ISMS nach IT-Grundschutz ist in der DRV zur nachhaltigen und angemessenen Planung, Steuerung, Kontrolle und Verbesserung der Informationssicherheit unabdingbar. Als wesentliche Bestandteile sind insbesondere der Aufbau einer Sicherheitsorganisation sowie die IT-Sicherheitskonzeption der DRV anzusehen.

Abbildung 2 Sicherheitskonzeption

Aufgrund der heterogenen Struktur und Arbeitsteilung der DRV und zur Sicherstellung einer DRV-weit einheitlichen Umsetzung müssen grundsätzliche Vorgaben zu den Prozessen und zur Organisation der Informationssicherheit übergreifend für alle RVTR, die DSRV sowie IT-Dienstleister der DRV verbindlich festgelegt werden. Die DRV hat dazu eine Sicherheitskonzeption entwickelt und mit der DRV-weit verbindlichen Informationssicherheits-Policy (ISP) einen Rahmen und ein Regelwerk erstellt, in dem die Vorgaben hierarchisch über fünf Ebenen festgelegt sind:

- Ebene 1: Leitlinie zur Informationssicherheit:
  Die Leitlinie beschreibt die Sicherheitsstrategie sowie allgemeine Zielfestlegungen, welche

durch eine verbindliche Entscheidung des Bundesvorstandes der DRV Bund in Kraft gesetzt sind.

- Ebene 2: Grundzüge der Informationssicherheit (GdIS):
  Die GdIS beschreibt unter anderem grundlegende Festlegungen für die Dokumente der ISP, langlebige Sicherheitsziele und -grundsätze für die DRV, die Umsetzung der Informationssicherheitsstrategie, Rahmenbedingungen und Aufgaben der IT-Sicherheitsbeauftragten (ITSIBE) sowie der Informations-Sicherheitsmanagement-Teams (ISMT) zur Unterstützung der ITSIBE.

– Die GdIS ist ebenfalls durch eine verbindliche Entscheidung des Bundesvorstandes der DRV Bund in Kraft gesetzt. Die in der GdIS beschriebenen Maßgaben und Zielsetzungen gelten unmittelbar und uneingeschränkt für alle Formen der Datenverarbeitung. Sie sind für alle RVTR und deren Beschäftigten verbindlich.

- Ebene 3: Richtlinien zu Teilbereichen der Informationssicherheit:
  In den Richtlinien werden die in der GdIS vorgegebenen Sicherheitsanforderungen für abgegrenzte Themengebiete konkretisiert. Es wird unterschieden zwischen
  - für die gesamte DRV verbindliche Richtlinien und
  - regional- bzw. trägerspezifische Richtlinien.

– Anmerkung: Im Rahmen der Erstellung und Überarbeitung einer Richtlinie kann diese auch vorübergehend durch ein Dokument „AGIS-Mindestanforderungen“ für den entsprechenden Themenbereich ersetzt werden.

- Ebene 4: Konzepte zu Teilbereichen der Informationssicherheit:
  In den Konzepten wird themenspezifisch dargestellt und festgelegt,
  - welche Daten in welcher Art und Weise und von welchen Stellen zu erheben und zu verarbeiten sind,
  - welche Rechtsgrundlagen dabei einzuhalten sind,
  - welche Technologien zum Einsatz kommen sollen und
  - welche Richtlinien dabei zu berücksichtigen sind.

– Analog zu Ebene 3 wird auch auf Ebene 4 unterschieden zwischen
  - für die gesamte DRV verbindlichen Konzepten und
  - regional- bzw. trägerspezifischen Konzepten.

- Ebene 5: Handlungsanweisungen:
  Die Handlungsanweisungen beschreiben konkret und zielgruppengerecht den Umgang mit IT-Systemen, IT-Verfahren, IT-Services etc.

Die Regelungen der GdIS und der für verbindlich erklärten Richtlinien zur Informationssicherheit bilden Mindeststandards für die gesamte DRV, deren Sicherheitsniveau nicht unterschritten werden darf.

In der Richtlinie „Organisation der Informationssicherheit" sind alle Richtlinien, Konzepte und Handlungsanweisungen aufgeführt, die DRV-weit verbindlich sind.

4.2 Erstellung von IT-Sicherheitskonzepten

4.2.1 Basis-IT-Sicherheitskonzepte

In der GdIS, Kap 4.3.2 sind wesentliche Standards geregelt. In der Sicherheitskonzeption der DRV wird der Umfang der Basis-IT-Sicherheitskonzepte geregelt. Für jede organisatorisch eigenständige Institution der DRV ist jeweils ein Basis-IT-Sicherheitskonzept zu erstellen. Ein weiteres Basis-IT-Sicherheitskonzept thematisiert das WAN der DRV.

Ziel ist es, einen angemessenen Schutz für alle Informationen einer Institution nach IT-Grundschutz zu erreichen.

Alle physischen Objekte sind im Basis-IT-Sicherheitskonzept zu betrachten.

4.2.2 IT-Verfahrenssicherheitskonzepte

Für alle IT-Verfahren hat der jeweilige Verfahrensverantwortliche auf Grundlage des Verfahrenszwecks in einem IT-Verfahrenssicherheitskonzept darzustellen, welche technischen und organisatorischen Maßnahmen unter Berücksichtigung der tatsächlichen örtlichen und personellen Gegebenheiten getroffen wurden, um die Anforderungen des Verfahrens an die Informationssicherheit auf Grundlage der IT-Grundschutzkataloge zu erfüllen.

IT- Verfahrenssicherheitskonzepte setzen auf den Basis-IT-Sicherheitskonzepten auf.

Quelle aus: *Deutsche Rentenversicherung – Branchenspezifischer Sicherheitsstandard*, S. 21-23, Download verfügbar unter: https://www.deutsche-rentenversicherung.de/SharedDocs/Downloads/DE/Selbstverwaltung/20200810_branchenspezif_sicherheitsstandard_pdf.html.

Anhang 9: Personelle Sicherheit, Vorfallerkennung/-bearbeitung

4.9 Personelle und organisatorische Sicherheit

Zur Vermeidung von Schäden an den kDL-relevanten Systemen oder bewusster oder unbewusster Manipulation der Daten sind geeignete personelle und organisatorische Maßnahmen zu treffen, die mindestens folgende Aspekte berücksichtigen:

- Sicherstellung der Fachkunde durch den Einsatz von geschultem Personal.
- Sicherstellung der Zuverlässigkeit durch geeignete Mechanismen (wo erforderlich z.B. durch Sicherheitsüberprüfungen oder Vorlage von Führungszeugnissen).
- Schaffung der Awareness für IT-Sicherheit auf allen Ebenen.
- Definition aller notwendigen Vorgaben für die Beschäftigten inkl. der Sanktionen bei Nichtbeachtung.
- Umsetzung eines Rollenkonzepts inkl. Ausschlussmatrix und Festlegung des Zwei-Personen-Prinzips, wo erforderlich.
- Umsetzung eines Identitäts- und Berechtigungsmanagements.
- Festlegung notwendiger Kompetenzen und Verantwortlichkeiten.
- Sicherstellung ausreichender Personalressourcen.

4.10 Bauliche und physische Sicherheit

Zur Vermeidung von Schäden an den zentralen kDL-relevanten Systemen durch Naturgefahren, Manipulation, Diebstahl, Zerstörung oder infrastrukturelle Mängel sind angemessene bauliche und physische Sicherheitsmaßnahmen in den Rechenzentren zu treffen, die folgende Aspekte (vgl. auch BCM, Kap. 4.5) berücksichtigen:

- Umfeldrisikoanalyse: Bewertung der Gefährdungspotentiale in der Umgebung.
- Bauliche Gegebenheiten: Bauliche Sicherheit bezüglich Fenstern, Türen, Brandabschnitten, Trassenverläufen.

- Brandmelde- und Löschtechnik: Brandmeldeanlage mit Aufschaltung auf die Feuerwehr, Etablierung von Abschaltfunktionen und Schadensbegrenzungsmaßnahmen.
- Sicherheitssysteme: Zutrittskontrollanlagen, Videoüberwachung, Einbruchmeldeanlagen inkl. Aufschaltung auf ständig besetzte Sicherheitszentrale oder Polizei.
- Energieversorgung: Nach einschlägigen Normen erbrachte Installationen mit Überspannungsschutz und entsprechender unterbrechungsfreier Notstromversorgung.
- Raumlufttechnische Anlagen: Klimatisierung der IT-Systeme und der Infrastrukturkomponenten.
- Organisation: Sicherstellung der regelmäßigen Prüfung und Wartung der Sicherheitseinrichtungen durch entsprechende Pläne und Verträge.

Die bauliche und physische Sicherheit ist in den Basis-IT-Sicherheitskonzepten der RVTR und der IT-Dienstleister zu betrachten. Des Weiteren sind in der übergreifend verbindlichen Richtlinie „Zutrittsschutz" grundlegende Vorgaben und Maßnahmen zur Gebäudehärtung und zu den erlaubten Methoden zur Zutrittssicherung aufgeführt, die DRV-weit berücksichtigt werden müssen.

4.11 Vorfallserkennung und –bearbeitung

Zur Erkennung und Bearbeitung von Vorfällen an den kDL-relevanten Systemen sind geeignete Maßnahmen zu treffen.

Vorfälle können sowohl Störungen sein, welche z.B. durch systematische Log-Auswertungen erkannt werden können, als auch Angriffe, welche z.B. durch Intrusion Detection Systeme (IDS) oder ein Security Information and Event Management System (SIEM) erkannt werden können.

Die zur Erkennung und Bearbeitung erforderlichen Tools und Prozesse sind durch fachkundiges Personal der operativen IT-Sicherheit zu betreiben. Bei den Betreibern der Rechenzentren der DRV sind dafür eigeständige Bereiche (Security Operation Center, SOC) zu betreiben, die jeweils vom Bereich des IT-Betriebs unabhängig sind.

Das CERT-DRV übernimmt die Funktion einer „Gemeinsamen übergeordnete Ansprechstelle" (GÜAS) gegenüber dem BSI (§8b BSIG) und koordiniert das Vorgehen bei DRV-weiten Sicherheitsvorfällen.

In der übergreifend verbindlichen Richtlinie „Behandlung von Sicherheitsvorfällen“ sind Grundsatzvorgaben zu Meldewegen, Reaktionsprozessen und der Nachbereitung von Sicherheitsvorfällen aufgeführt, die DRV-weit berücksichtigt werden müssen.

4.12 Überprüfung

Um die Funktionsfähigkeit der eingesetzten Sicherungsmaßnahmen zu überprüfen und Schwachstellen zu identifizieren, sind regelmäßige (mind. alle zwei Jahre) Überprüfungen durchzuführen. Darüber hinaus müssen anlassbezogene Prüfungen durchgeführt werden, z. B. aufgrund von

- Änderungen in der Bedrohungs- oder Gefährdungslage,
- Änderungen an den IT- oder Kommunikationssystemen,
- nicht zuverlässig erklärbaren Beeinträchtigungen der kDL oder der zugehörigen IT-Systeme,
- erfolgreichen oder möglicherweise erfolgreichen Angriffen

Sowohl bei den regelmäßigen als auch anlassbezogenen Überprüfungen muss sichergestellt sein, dass alle Bereiche berücksichtigt werden:

- interne Überprüfungen bei den Institutionen der DRV müssen die jeweiligen IT-Sicherheitsbeauftragten koordinieren,
- übergreifende Überprüfungen zentraler bzw. trägerübergreifender Verfahren, Services und Dienste müssen durch den/die IT-Sicherheitsbeauftragte(n) der DRV und den ihm/ihr zugeordneten Organisationseinheiten koordiniert werden.

4.13 Externe Informationsversorgung und Unterstützung

Zur Aufrechterhaltung und stetigen Verbesserung des Sicherheitsniveaus sind regelmäßig und anlassbezogen Informationen über aktuelle Entwicklungen der IT-Sicherheitslage zu beschaffen. Neben den einschlägigen Informationsquellen im Internet ist insbesondere das BSI als Betreiber des CERT-Bund und der zentralen Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen nach §§ 8a bis 8c BSIG als Informationsquelle und zur Unterstützung einzubeziehen.

Die externe Informationsversorgung wird DRV-weit durch das CERT-DRV koordiniert, welches die relevanten Informationen intern an die beteiligten Rechenzentren, SOCs und RVTR weitergibt.

In der übergreifend verbindlichen Richtlinie „Behandlung von Sicherheitsvorfällen“ sind die Anforderungen an das CERT-DRV aufgeführt, die DRV-weit berücksichtigt werden müssen.

Quelle aus: *Deutsche Rentenversicherung – Branchenspezifischer Sicherheitsstandard*, S. 26-28, Download verfügbar unter: https://www.deutsche-rentenversicherung.de/SharedDocs/Downloads/DE/Selbstverwaltung/20200810_branchenspezif_sicherheitsstandard_pdf.html.

7 Literaturverzeichnis

Asghari, Reza (Hrsg.): *E-Government in der Praxis*: *Leitfaden für Politik und Verwaltung*, Software & Support Verlag GmbH, Frankfurt, 2005.

AssCompact, 06.10.2023: *Cyberversicherungen: Markt stabilisiert sich, Wachstum hält an*, verfügbar unter: https://www.asscompact.de/nachrichten/cyberversicherungen-markt-stabilisiert-sich-wachstum-h%C3%A4lt?page=komp, zuletzt aufgerufen am 25.04.2024.

AssCompact, 19.02.2024: *GDV legt neue Musterbedingungen für Cyberversicherung vor*, verfügbar unter: https://www.asscompact.de/nachrichten/gdv-legt-neue-musterbedingungen-f%C3%BCr-cyberversicherung-vor, zuletzt aufgerufen am 23.04.2024.

Bitkom, Statista, 2022: *Ausgaben für IT-Sicherheit in Deutschland in den Jahren 2017 bis 2021 und Prognose bis 2025 (in Milliarden Euro)*, verfügar unter: https://de.statista.com/statistik/daten/studie/1041736/umfrage/ausgaben-fuer-it-security-in-deutschland/, zuletzt aufgerufen am 26.04.2024.

Brand, Oliver/Baroch Castellvi, Manuel (Hrsg.): *Versicherungsaufsichtsgesetz*, Nomos Verlagsgesellschaft mbH & Co. KG, Baden-Baden, 2. Auflage, 2024.

Bundesamt für Sicherheit in der Informationstechnik, o. J.: *Die Lage der IT-Sicherheit in Deutschland 2023*, verfügbar unter: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html, zuletzt aufgerufen am 25.11.2023.

Bundesamt für Sicherheit in der Informationstechnik, o. J.: *Kleine- und Mittlere Unternehmen*, verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/KMU/KMU_node.html, zuletzt aufgerufen am 23.04.2024.

Bundesamt für Sicherheit in der Informationstechnik, o. J.: *Ransomware – Vorsicht vor Erpressersoftware*, verfügbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Schadprogramme/Ransomware/ransomware_node.html, zuletzt aufgerufen am 24.04.2024.

Bundesanstalt für Finanzdienstleistungsaufsicht, 06.05.2022: *Cyberversicherung*, verfügbar unter: https://www.bafin.de/DE/Verbraucher/Versicherung/Produkte/Cyber/cyberversicherung_node.html, zuletzt aufgerufen am 23.04.2024.

Bundeskriminalamt, Statista, 2024: *Polizeilich erfasste Fälle von Cyberkriminalität in Deutschland von 2007 bis 2023*, verfügbar unter: https://de.statista.com/statistik/daten/studie/295265/umfrage/polizeilich-erfasste-faelle-von-cyberkriminalitaet-im-engeren-sinne-in-deutschland/, zuletzt aufgerufen am 26.04.2024.

Bundesministerium für Arbeit und Soziales, 06.04.2017: *Gesetzliche Rentenversicherung*, verfügbar unter: https://www.bmas.de/DE/Soziales/Rente-und-Altersvorsorge/Gesetzliche-Rentenversicherung/gesetzliche-rentenversicherung-art.html, zuletzt aufgerufen am 24.04.2024.

Bundeszentrale für politische Bildung, 2016: *Körperschaft des öffentlichen Rechts*, verfügbar unter: https://www.bpb.de/kurz-knapp/lexika/lexikon-der-wirtschaft/19896/koerperschaft-des-oeffentlichen-rechts/, zuletzt aufgerufen am 24.04.2024.

Detken, Oliver/Eren, Evren: *Handbuch Datensicherheit*, Kommunal- und Schul-Verlag GmbH & Co. KG, Wiesbaden, 2020.

Deutsche Rentenversicherung Baden-Württemberg, o. J.: *Unsere wichtigsten Aufgaben*, verfügbar unter: https://www.deutsche-rentenversicherung.de/BadenWuerttemberg/LS/Aufgaben/aufgaben_node.html, zuletzt aufgerufen am 23.04.2024.

Deutsche Rentenversicherung, 01.12.2023: *Datenschutz: Ihre Daten – und Ihre Rechte*, Download verfügbar unter: https://www.deutsche-rentenversicherung.de/SharedDocs/Downloads/DE/Broschueren/national/datenschutz_ihre_daten_und_ihre_rechte.html, zuletzt aufgerufen am 23.04.2024.

Deutsche Rentenversicherung, o. J.: *Deutsche Rentenversicherung – Branchenspezifischer Sicherheitsstandard*, Download verfügbar unter: https://www.deutsche-rentenversicherung.de/SharedDocs/Downloads/DE/Selbstverwaltung/20200810_branchenspezif_sicherheitsstandard_pdf.html, zuletzt aufgerufen am 24.04.2024.

Deutsche Rentenversicherung, o. J.: *Selbstverwaltung*, verfügbar unter: https://www.deutsche-rentenversicherung.de/BadenWuerttemberg/DE/Ueber-uns/Selbstverwaltung/selbstverwaltung_node.html, zuletzt aufgerufen am 24.04.2024.

Deutsche-Versicherungsboerse, o. J.: *Betriebsgewinn-Definition*, verfügbar unter: https://www.deutsche-versicherungsboerse.de/verswiki/index_dvb.php?title=Betriebsgewinn_-_Definition, zuletzt aufgerufen am 23.04.2024.

Die Versicherungspraxis: *Die neuen Musterbedingungen für die Cyberversicherung*, Heft 3, 2024, S. 28-32, Download verfügbar unter: https://www.wiso-net.de/document/DVP__6704c7c9da76f65b7846614352bf33036e470771, zuletzt aufgerufen am 27.04.2024.

Duden, o. J.: *Gesetz*, verfügbar unter: https://www.duden.de/rechtschreibung/Gesetz#bedeutungen, zuletzt aufgerufen am 24.04.2024.

Eggen, Jonathan: *Die Cyberversicherung Zur Versicherbarkeit von Lösegeldern bei Ransomware und Bußgeldern im Zusammenhang mit Datenschutzverstößen* (E-Book), Verlag Versicherungswirtschaft GmbH & Co. KG, Band 28, Karlsruhe, 2023.

Epping, Volker/Hillgruber, Christian (Hrsg.): *Beck'scher Online-Kommentar Grundgesetz*, C.H. Beck, München, 57. Edition, 2024.

Erb, Volker/Schäfer, Jürgen (Hrsg.): *Münchener Kommentar zum StGB*, Verlag C.H. Beck, München, Band 1, 4. Auflage, 2020.

EY, Statista, 2023: *Hat Ihr Unternehmen eine Versicherung gegen digitale Risiken (Hackerangriffe etc.) abgeschlossen?*, verfügbar unter: https://de.statista.com/statistik/daten/studie/760310/umfrage/versicherungen-gegen-digitale-risiken-in-deutschen-unternehmen/, zuletzt aufgerufen am 26.04.2024.

EY, Statista, 2023: *Was meinen Sie, wie wird sich die Bedeutung des Problems Cyberangriffe/Datenklau für Ihr Unternehmen künftig entwickeln?*, verfügbar unter: https://de.statista.com/statistik/daten/studie/760039/umfrage/zukuenftige-bedeutung-von-cyberkriminalitaet-fuer-deutsche-unternehmen/, zuletzt aufgerufen am 26.04.2024.

EY, Statista, 2023: *Wie hoch schätzen Sie das Risiko für Ihr Unternehmen ein, Opfer von Cyberangriffen/Datenklau zu werden?*, verfügbar unter: https://de.statista.com/statistik/daten/studie/760006/umfrage/wahrgenommenes-risiko-von-cyberangriffen-unter-unternehmen-in-deutschland/, zuletzt aufgerufen am 26.04.2024.

Fortmann, Michael: *Cyberversicherung: ein gutes Produkt mit noch einigen offenen Fragen*, in: r + s recht und schaden, 2019, Heft 8, S. 429-444.

Freundl, Maximilian, Bundesakademie für Sicherheitspolitik, 19. April 2023: *Methoden zur Strategischen Vorausschau: Megatrends*, verfügbar unter: https://www.baks.bund.de/de/aktuelles/methoden-zur-strategischen-vorausschau-megatrends, zuletzt aufgerufen am 27.04.2024.

Ganz, Robert, Bundesanstalt für Finanzdienstleistungsaufsicht, 07.02.2024: *Cyberversicherungen: hohe Nachfrage – und hohe Risiken?* Verfügbar unter: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2024/fa_bj_2402_Cyberversicherung.html, zuletzt aufgerufen am 23.04.2024.

Gesamtverband der Versicherer, 01.03.2018: *Das leistet eine Cyberversicherung*, verfügbar unter: https://www.gdv.de/gdv/themen/digitalisierung/das-leistet-eine-cyberversicherung-31152, zuletzt aufgerufen am 23.04.2024.

Griese, Michael, Versicherungswirtschaft heute, 2023: *Unsichtbare Bedrohung: Wie eine effektive Vorsorge gegen Cyberangriffe aussehen kann*, verfügbar unter: https://www.juris.de/perma?d=jzs-VersW-2023-9-013-28, zuletzt aufgerufen am 24.04.2024

Hartung, Thomas, Gabler Banklexikon, 26.03.2020: *Versicherungsprodukt*, verfügbar unter: https://www.gabler-banklexikon.de/definition/versicherungsprodukt-62323/version-375816, zuletzt aufgerufen am 23.04.2024.

Hill, Hermann/Schliesky, Utz (Hrsg.): *Herausforderung e-Government*, Nomos Verlagsgesellschaft, Baden-Baden, Band 11, 1. Auflage, 2009.

Hitzler, Ronald/Pfadenhauer, Michaela (Hrsg.): *Gegenwärtige Zukünfte: Interpretative Beiträge zur sozialwissenschaftlichen Diagnose und Prognose*, VS Verlag für Sozialwissenschaften, Wiesbaden, 2005.

Hömig, Dieter/Wolff, Amadeus/u. a.: *Grundgesetz für die Bundesrepublik Deutschland,* Nomos, Baden-Baden, 13. Auflage, 2022.

IBM, o. J.: *Was ist ein Cyberangriff?*, verfügbar unter: https://www.ibm.com/de-de/topics/cyber-attack, zuletzt aufgerufen am 23.04.2024

Initiative D21, Statista, 2024: *Digitalisierungsgrad in Deutschland nach dem Digital-Index in den Jahren 2013 bis 2024*, verfügbar unter: https://de.statista.com/statistik/daten/studie/1451432/umfrage/entwicklung-digitalisierungsgrad-in-deutschland/, zuletzt aufgerufen am 26.04.2024.

Jarass, Hans/Pieroth, Bodo/Kment, Martin: *Grundgesetz für die Bundesrepublik Deutschland*, C.H. Beck, München, 18.Auflage, 2024.

Klein, René, Für Gründer, o. J.: *Cyberversicherung: Ist Ihr Unternehmen in Gefahr?*, verfügbar auf: https://www.fuer-gruender.de/wissen/unternehmen-gruenden/versicherung/cyber-versicherung/#c49116, zuletzt aufgerufen am 23.04.2024.

Knickrehm, Sabine/Roßbach, Gundula/Waltermann, Raimund (Hrsg.): *Kommentar zum Sozialrecht*, C.H. Beck, München, 8. Auflage, 2023.

Kreikebohm, Ralf/Roßbach, Gundula (Hrsg.): *Sozialgesetzbuch gesetzliche Rentenversicherung SGB VI*, C.H. Beck, 6. Auflage, 2021.

Kretschmer, Christian, tagesschau, 19.04.2023: *Cyberangriffe: Ein Weckruf für die Kommunen*, verfügbar unter: https://www.tagesschau.de/inland/gesellschaft/cyberangriffe-verwaltung-101.html, zuletzt aufgerufen am 24.04.2024.

Lale, Önder, Bundesanstalt für Finanzdienstleistungsansicht, 06.06.2013: *Alternativer Risikotransfer: Vorteile und Risiken des Transfers versicherungstechnischer Risiken auf die Kapitalmärkte*, 2013, verfügbar unter: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2013/fa_bj_2013_06_alternativer_risikotransfer.html, zuletzt aufgerufen am 25.04.2024.

Langheid, Theo/Wandt, Manfred (Hrsg.): *Münchener Kommentar zum Versicherungsvertragsgesetz*, C.H. Beck, München, 2. Auflage, Band 3, 2017.

Libbe, Jens, Bundeszentrale für politische Bildung, 2021: *Öffentliche Unternehmen*, verfügbar unter: https://www.bpb.de/kurz-knapp/lexika/handwoerterbuch-politisches-system/202081/oeffentliche-unternehmen/, zuletzt aufgerufen am 24.04.2024.

Mobilitätsmagazin, 27.02.2024: *Datenschutz in Behörden: Strenge Auflagen für öffentliche Stellen*, verfügbar unter: https://www.bussgeldkatalog.org/datenschutz-behoerden/, zuletzt aufgerufen am 23.04.2024.

Myra Security, o. J.: *Was ist ein Cyberangriff?*, verfügbar unter: https://www.myrasecurity.com/de/knowledge-hub/cyberangriff/, zuletzt aufgerufen am 24.04.2024.

Paal, Boris/Pauly, Daniel (Hrsg.): *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz*, C.H. Beck, München, 3. Auflage, 2021.

Prölss, Jürgen/Martin, Anton/u. a.: *Versicherungsvertragsgesetz*, C.H. Beck, München, 31. Auflage, 2021.

Rüffer, Wilfried/Halbach, Dirk/Schimikowski, Peter (Hrsg.) u. a.: *Versicherungsvertragsgesetz*, Nomos, 4. Auflage, 2020.

Schmidt, Ingrid/Gallner, Inken/u. a. (Hrsg.): *Erfurter Kommentar zum Arbeitsrecht*, C.H. Beck, München, 24. Auflage, 2024.

Seckelmann, Margrit (Hrsg.): *Digitalisierte Verwaltung Vernetztes E-Government*, Erich Schmidt Verlag GmbH & Co. KG, Berlin, 2. Auflage, 2019.

Sieverding, Ole, AssCompact, 21.03.2024: *Cyber-Bedingungswirrwarr: Herausforderungen für Vermittlung*, verfügbar unter: https://www.asscompact.de/nachrichten/cyber-bedingungswirrwarr-herausforderungen-f%C3%BCr-vermittlung, letzter Zugriff am 24.04.2024.

Stanczyk, Michael, Versicherungswirtschaft heute, 2024: *Gefangen im System*, verfügbar unter: https://www.juris.de/perma?d=jzs-VersW-2024-1-009-10, zuletzt aufgerufen am 24.04.2024.

Steimer, Michael: *Einführung in die Cyberversicherung, Praktischer Einstieg für Vermittler von Klein-KMU* (E-Book), Versicherungswirtschaft GmbH & Co. KG, Karlsruhe, 1. Auflage, 2023.

Surminski, Marc: *Neue Kapazitätskonzepte in Cyber*, in: Zeitschrift für Versicherungswesen, Ausgabe 19, 2023, S. 525.

Taeger, Jürgen/Pohle, Jan (Hrsg.): *Computerrechts-Handbuch*, C.H. Beck, München, 38. Ergänzungslieferung, 2023.

Unternehmen Cybersicherheit, 20.06.2023: *Cyberversicherungen immer schwerer zu bekommen: Interview zu den Entwicklungen auf dem Versicherungsmarkt*, verfügbar unter: https://unternehmen-cybersicherheit.de/cyberversicherungen-immer-schwerer-zu-bekommen-interview-zu-den-entwicklungen-am-versicherungsmarkt/, zuletzt aufgerufen am 24.04.2024

Versicherungsmagazin, 21.02.2024: *GDV hat seine Musterbedingungen überarbeitet*, verfügbar unter: https://www.versicherungsmagazin.de/rubriken/branche/gdv-hat-seine-musterbedingungen-ueberarbeitet-3432762.html, zuletzt aufgerufen am 27.04.2024.

Wagner, Fred, Gabler Wirtschaftslexikon, 19.02.2018: *Assistance*, verfügbar unter: https://wirtschaftslexikon.gabler.de/definition/assistance-31423/version-254980, zuletzt aufgerufen am 23.04.2024.

Wagner, Fred, Gabler Wirtschaftslexikon, 19.02.2023: *Kumulrisiko*, verfügbar unter: https://wirtschaftslexikon.gabler.de/definition/kumulrisiko-37785/version-261216, zuletzt aufgerufen am 25.04.2024.

8 Eidesstattliche Versicherung

Erklärung

„Ich versichere, dass ich diese Bachelorarbeit selbständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe. Die aus anderen Quellen direkt oder indirekt übernommenen Daten und Konzepte sind unter Angabe der Quelle gekennzeichnet. Mir ist bekannt, dass meine Abschlussarbeit von Seiten der Hochschule mit einer Plagiatssoftware überprüft werden kann.“

Datum, Unterschrift