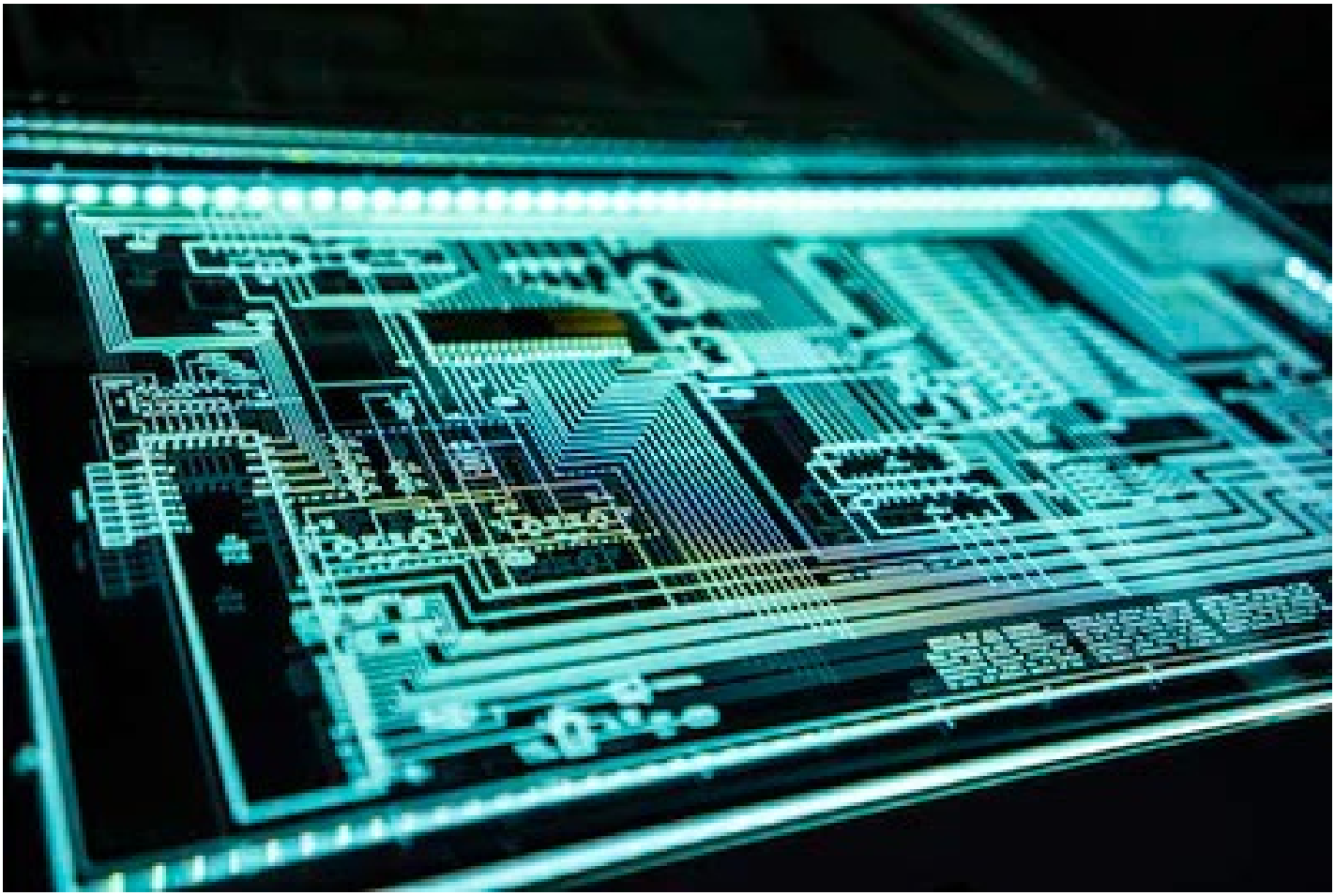

Methodik der Assekurata-Tarifanalyse

Cyber-Versicherung

(Gewerbe)

ASSEKURATA
Assekuranz Rating-Agentur GmbH

September 2020

Grundlagen und Vorgehensweise

In Zeiten einer voranschreitenden Digitalisierung werden Unternehmen zunehmend mit den Auswirkungen von Cyber-Kriminalität konfrontiert. Der Umgang mit potenziellen Cyber-Angriffen gehört mittlerweile zu den größten betriebswirtschaftlichen Herausforderungen. Cyber-Kriminalität kann dabei ganz unterschiedliche Formen und Motive aufweisen. Sie kann beispielsweise darauf ausgerichtet sein, Know-how von einem Unternehmen abzuschöpfen oder dieses durch Erpressungstrojaner zur Auszahlung von hohen Geldsummen zu bewegen. IT-Sicherheitsvorfälle treten aber auch in anderer Form auf, sei es Datenverlust, Datendiebstahl oder die Nichtverfügbarkeit von Daten und Systemen. Oft geschieht dies durch Hackerangriffe und Malware, kann aber auch eine Folge von Nachlässigkeit oder internen Datenschutzverletzungen sein. Unternehmen sind nach der Datenschutzgrundverordnung (DSGVO) dazu verpflichtet, technische und organisatorische Maßnahmen zum Datenschutz zu ergreifen. Zugleich dienen diese Maßnahmen einigen Hackern zuweilen als Ansporn, die Sicherheitskonzepte der Unternehmen zu attackieren, was erhebliche finanzielle und reputative Schäden nach sich ziehen kann.

Ein professionelles Management von Cyber-Risiken ist daher zwingend erforderlich. Absicherungslösungen in Form von Cyber-Versicherungen sind darin ein wichtiger Baustein. Neben der monetären Entlastung für auftretende Eigenschäden decken Cyber-Versicherungen auch Haftungsansprüche gegenüber Dritten ab. Ein weiterer typischer Tarifbestandteil sind Assistance-Leistungen, die insbesondere auf die Bereitstellung von Expertise im Schadenfall abzielen. Im digitalen Ernstfall stellt der Versicherer einem betroffenen Unternehmen dann ein Expertenteam zu Seite, welches das Schadenausmaß begrenzen und den Betrieb schnellstmöglich zum Normalzustand zurückbringen soll.

Anders als in den USA sind Cyber-Versicherungen in Deutschland noch ein junges Geschäftsfeld. Ein Marktstandard für geeigneten Versicherungsschutz hat sich noch nicht herauskristallisiert, was nicht zuletzt auf die geringen Schadenerfahrungen der Versicherer zurückzuführen ist.

In der Konsequenz sind die Tarifstrukturen und Versicherungsbedingungen am Markt sehr unterschiedlich. Hinzu kommt, dass in den Prospekt- und Angebotsunterlagen häufig Cyber-typische Schlagwörter wie „Fake President“ bzw. „CEO-Fraud“ zu finden sind, die einen vermeintlich umfangreichen Versicherungsschutz suggerieren, die aber einer Überprüfung der zugrunde liegenden Versicherungsbedingungen häufig nicht Stand halten können. Für Kunden und Vermittler ist es somit schwierig, den Leistungsumfang und die Qualität eines Cyber-Versicherungstarifes sachgerecht einzuschätzen.

Aufgrund der großen Heterogenität der Bedingungen und der Intransparenz des tatsächlichen Deckungsumfangs hat Assekurata eine spezielle Tarifanalyse für Cyber-Angebote in der Gewerbeversicherung entwickelt. Hierbei wird jeder Tarif systematisch anhand seiner versicherungstechnischen Leistungsmerkmale untersucht. Die Bewertungsanforderungen orientieren sich an der Praxis und wurden anhand von Marktanalysen zu tatsächlichen Bedrohungspotenzialen und Schadenfällen abgeleitet.

Aufgrund des hohen Absicherungsbedarfs von kleinen und mittleren Unternehmen (KMU) bei gleichzeitig wachendem Angebot an Cyber-Tarifen für diese Zielgruppe werden die Deckungskonzepte hinsichtlich ihrer Eignung für KMU analysiert und bewertet. Nach der Definition der Europäischen Kommission zählt ein Unternehmen zu den KMU, wenn es nicht mehr als 249 Mitarbeiter beschäftigt, einen Jahresumsatz von maximal 50 Millionen € erwirtschaftet oder eine Bilanzsumme von maximal 43 Millionen € aufweist.

Die Bewertungsskala des Verfahrens ist auf intuitive Verständlichkeit ausgelegt. Aus Kundensicht hat sich dabei das Schulnotensystem etabliert, da die Kombination aus Ziffer und Wort bei den Benotungen von beispielsweise 1,0 (sehr gut) und 1,4 (sehr gut) auch Unterschiede im Detail sichtbar machen.

Die genaue Zuordnung von Punkten und Noten wird anhand folgender Tabelle deutlich.

NOTENSKALA									
sehr gut		gut		befriedigend		ausreichend		nicht ausreichend	
ab Punkte	Note	ab Punkte	Note	ab Punkte	Note	ab Punkte	Note	ab	Note
921	1,0	810	1,6	650	2,6	490	3,6	330	4,6
890	1,1	794	1,7	634	2,7	474	3,7	314	4,7
874	1,2	778	1,8	618	2,8	458	3,8	298	4,8
858	1,3	762	1,9	602	2,9	442	3,9	282	4,9
842	1,4	746	2,0	586	3,0	426	4,0	266	5,0
826	1,5	730	2,1	570	3,1	410	4,1	250	5,1
		714	2,2	554	3,2	394	4,2	234	5,2
		698	2,3	538	3,3	378	4,3	218	5,3
		682	2,4	522	3,4	362	4,4	202	5,4
		666	2,5	506	3,5	346	4,5	186	5,5

In der Tarifanalyse Cyber beurteilt Assekurata die spezifischen Leistungen in der jeweiligen Cyber-Versicherung (Cyber-Police). Hiermit erhalten

- **Unternehmen** die Möglichkeit, die Qualität ihrer Produkte nachzuweisen,
- **Vermittler** Sicherheit für den Beratungsprozess und
- **Kunden** eine Orientierung bei der Entscheidung.

Eine ausführliche Dokumentation versetzt die Unternehmen zudem in die Lage, die Bewertung im Detail nachzuvollziehen und somit auch gezielte Ansatzpunkte für eine Tarifverbesserung zu nutzen.

Die Assekurata-Tarifanalyse ist gemäß EU-Verordnung 1060/2009 über Ratingagenturen eine Nebendienstleistung der *ASSEKURATA* Assekuranz Rating-Agentur GmbH.

Bewertungsverfahren

Assekurata untersucht die Cyber-Policen im Hinblick auf die Tarifbedingungen, den Leistungsumfang und die Transparenz. Hierfür wurde ein detailliertes Prüf- und Bewertungsschema definiert. Jeder Cyber-Tarif wird anhand von zehn Hauptprüfpunkten mit über 60 Detailkriterien analysiert. Die einzelnen Kriterien fließen mit unterschiedlichen Gewichten in die Bewertung ein.

Die Gewichtung orientiert sich an der Wichtigkeit der jeweiligen Leistung aus Kundensicht. Damit ist sichergestellt, dass die Leistungen im Hinblick auf ihre Relevanz für die Kunden im Verfahren adäquat berücksichtigt werden. Die Kriterien wurden anhand der Überprüfbarkeit und des Vergleichs der Tarife untereinander validiert und führen somit zu einem eindeutigen und klaren Ergebnis.

Im Fokus der Bewertung steht jeweils ausschließlich der angebotene Cyber-Tarif. Um Überlagerungseffekte zu vermeiden, bleiben anderweitige Versicherungen, deren Deckungsumfang sich ausschnittsweise mit Cyber-Policen überschneiden können (z. B. Sach- und Ertragsausfallversicherung, Betriebshaftpflichtversicherung, Vertrauensschadenversicherung), bei der Betrachtung außen vor.

Um im Sinne der Zielgruppe nur verbindliche Produkteigenschaften zu berücksichtigen, wird bei der Bewertung der Cyber-Policen auf die allgemeinen Versicherungsbedingungen (AVB) zurückgegriffen, die den Tarifen rechtsverbindlich zugrunde liegen. Unberücksichtigt bleiben sonstige Erklärungen oder Auslegungen der Versicherer, welche Bestandteile von individuellen Vereinbarungen sein können. Ebenso bleibt die Höhe der Versicherungsprämie bei der Einstufung der Tarife unberücksichtigt.

Im Folgenden werden die Bewertungsbereiche (Hauptkriterien) einzeln dargestellt und mit Beispielen erläutert.

Allgemeine Bestimmungen

(z. B. Definition des Versicherungsfalls, Begriffstransparenz, Repräsentanten, Rückwärtsversicherung, Nachhaftung)

Es wird untersucht, ob der Versicherungsfall offen und zukunftssicher definiert ist oder durch Aufzählung bestimmter Ereignisse oder Methoden (z. B. Phishing, Trojaner, Viren) eingeschränkt wird. Dem Grunde nach wird hierbei abstrakt die schadenstiftende Wirkung der Auslöser des Versicherungsfalls betrachtet, da die konkrete Bewertung innerhalb der zuzuordnenden Hauptkriterien (z. B. Eigenschaden, Fremdschaden) erfolgt.

Ein weiterer Aspekt sind die versicherten Systeme und Daten. Da die Anbieter weitgehend frei in ihrer Formulierung sind und die Rechtsprechung bisher keine ausreichende Grundlage zur Klarstellung von Begrifflichkeiten gelegt hat, ist es im Sinne des Kunden, durch Nennung von Beispielen und/oder konkreter Aufzählung der versicherten Systeme die Definitionen in den Bedingungstexten entsprechend zu verbriefen.

Ein Augenmerk wird auch auf die Nennung der Repräsentanten gelegt. Versicherungsrechtlich wird dem Versicherungsnehmer das Verhalten der Repräsentanten zugerechnet, wobei die genaue Abgrenzung nicht gesetzlich geregelt ist. Für Versicherungsnehmer ist daher eine klar formulierte Festlegung der Repräsentanten von Bedeutung. Dabei ist es von Vorteil, einen möglichst kleinen Personenkreis als Repräsentanten in den Bedingungen zu definieren, um sich im Schadenfall das Verhalten möglichst weniger Mitarbeiter bzw. Entscheidungsträger leistungsmindernd zurechnen lassen zu müssen.

Unterschätzt werden sollte nicht, dass eine Cyber-Versicherung auch für Schäden aufkommen kann, die bereits vor Abschluss des Vertrages eingetreten sind, aber bis dahin noch nicht festgestellt wurden. Mitunter können Schadprogramme so konzipiert sein, dass sie für Monate oder Jahre in den IT-Systemen schlummern. Hierfür sollte der Vertrag eine möglichst lange Zeit der Rückwärtsversicherung enthalten. Auf der anderen Seite sollte ein versierter Versicherer auch noch nach Ablauf des Vertrages für Schäden haften, die während der Laufzeit des Vertrages eingetreten sind, sich aber noch nicht manifestiert haben.

Gegenstand der Versicherung

(Definition von Vermögens- und Sachschäden)

Vermögensschäden sind in den verschiedenen Versicherungsbedingungen nicht einheitlich definiert. Zuvorderst sollten sie die Wiederherstellung der betroffenen Daten und die Entfernung der Schadsoftware abdecken. Im Detail prüft Assekurata hier zunächst, was unter Vermögensschäden zu subsumieren ist. Dem Grunde nach sind dies solche Schäden, 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.

Sachschäden können grundsätzlich nur an körperlichen Gegenständen auftreten. Sinnvoll ist es, wenn diese in den Versicherungstarifen eindeutig deklariert werden (Substanzdeckung). Dabei wird auch analysiert, ob der Versicherer die Reparatur oder den Austausch der versicherten Sachen vorsieht. In Abgrenzung hierzu sind elektronische Daten keine Sachen. Der Verlust oder die Beschädigung von elektronischen Daten als Folge des Abhandenkommens von Gerätschaften kann aber als Vermögensschaden versichert sein.

Eigenschäden (Überblick)

Die Palette der möglichen Eigenschäden ist breit. Viele Risiken betreffen zunächst den Versicherungsnehmer, in der Folge aber eventuell auch weitere Geschädigte. Zu klären ist daher, wer in den Versicherungsschutz aufgenommen wurde (mitversicherte Person bzw. mitversicherte Unternehmen). In der Prüfung kommt es dann darauf an, ob und wie eine Ermittlung des Schadens und die entsprechende Rechtshilfe zur Verfügung stehen. Die Eigenschäden werden subsumiert in die Hauptkriterien

- *Schutz von Identität und Reputation*,
- *Zahlungsmittelkonten und Kreditkarten*,
- *Schutz von Sachen und Daten* und
- *Betriebsunterbrechung*.

Schutz von Identität und Reputation

(z. B. Ermittlung, Rechtshilfe, Erpressungsgelder und Belohnungen)

Ein Identitätsdiebstahl liegt vor, wenn Identitätsdaten versicherter Personen durch Dritte, die zur Nutzung dieser personenbezogenen Daten weder selbst berechtigt, noch vom Versicherungsnehmer oder einer mitversicherten Person beauftragt oder

bevollmächtigt worden sind, für eigene Zwecke des Dritten genutzt werden.

Beispielsweise kommt es mit Hilfe von Verschlüsselungs-Schadprogrammen (Ransomware) immer häufiger zu kriminell motivierten Angriffen auf die informationstechnische Infrastruktur, wobei die Angriffe typischerweise die Erlangung von Lösegeldern zum Ziel haben.

Um hier hinreichenden Versicherungsschutz sicherzustellen, sollte die Police die notwendigen Kosten für das Schadenmanagement durch die spezialisierten Fachleute übernehmen. Wichtig ist hierbei, dass auch kurzfristig auf die Expertise des IT-Dienstleisters zurückgegriffen werden kann.

Neben dem versicherten Kreis (Personen und Unternehmen) ist auch zu prüfen, bis zu welcher Höhe der Versicherungsschutz besteht bzw. wie oft ein Sublimit zur Verfügung steht. Darüber hinaus bedarf es einer hohen Diskretion im Schadenmanagement, insbesondere dann, wenn beispielsweise Verhandlungen mit dem Erpresser um die Lösegeldzahlung anstehen.

Des Weiteren ist zu prüfen, ob Belohnungen bzw. weitere Honorare oder Auslagen mitversichert sind. Denn infolge eines Cyber-Angriffs müssen Unternehmen oft auf externe Hilfe zurückgreifen, beispielsweise für eine gute Krisenkommunikation und professionelle Öffentlichkeitsarbeit, um die Reputation wieder herzustellen.

Zahlungsmittelkonten und Kreditkarten

(Kredit-/Überwachungsdienstleistungen, Sublimits)

Der Missbrauch kompromittierter Kreditkarten-, Bankkarten- oder Geldkartendaten liegt vor, wenn durch nicht autorisierte Dritte für die Karteninhaber nachteilige Verfügungen getroffen werden.

Neben den häufig vorkommenden Phishing-Versuchen, bringen Angreifer zunehmend auch legitime Webseiten mit korrekten Zertifikaten unter ihre Kontrolle.

Daher sollte auch hierfür ein ausreichender Versicherungsschutz bestehen.

Schutz von Sachen und Daten

(Angabe der versicherten Gefahren und Leistungen)

Im Hinblick auf den Schutz von Sachen und Daten ist zunächst eine konkrete Abgrenzung von versicherten und nicht versicherten Sachen und Daten vonnöten, damit klargestellt wird, was in den Versicherungsschutz fällt und was nicht. Je eindeutiger hier die Formulierung ist, umso verständlicher ist der Vertrag für den Versicherungsnehmer. Die Skizzierung von Beispielen geben dem Kunden zusätzliche Orientierung.

Der Diebstahl bzw. Verlust von IT-Systemen (i. S. v. technischen Problemen) ist ein hohes unternehmerisches Risiko. Insofern ist zu beachten, dass der Tarif auch für die Wiederherstellung von Daten infolge eines Datenverlusts, welcher unmittelbar auf einen Diebstahl oder Verlust (Untergang, physische Zerstörung) zurückzuführen ist, leistet – und zwar auch in den Fällen, in denen der Schaden nicht auf eine unbefugte Nutzung der IT-Systeme zurückzuführen ist.

Betriebsunterbrechung

(z. B. versichertes Risiko, versicherte Gefahren, Haftzeit und Selbstbeteiligung, Beendigung der Leistung)

Wenn ein Unternehmen die Produktion aufgrund einer Cyber-Attacke einstellen bzw. für einen längeren Zeitraum unterbrechen muss, bedeutet dies eine große finanzielle Belastung, die schnell zu existenziellen Problemen führen kann. Daneben sind auch indirekte Kosten von Betriebsunterbrechungen zu berücksichtigen, etwa die Kundenabwanderung bei Nichtverfügbarkeit von kritischen Prozessen und Anwendungen oder die Strafen bei Beeinträchtigung vertraglich zugesicherter Service-Level und -Verfügbarkeiten.

Demnach ist es wichtig, dass die wirtschaftlichen Auswirkungen einer Betriebsunterbrechung infolge einer unbefugten Nutzung von IT-Systemen (einschließlich der Überschreitung der jeweiligen Zugriffsberechtigung und Bedienfehler von Mitarbeitern) sowie von Datenschutzvorfällen professionell identifiziert, zusammengetragen und abgesichert sind.

Die Kernleistung einer Betriebsunterbrechungsdeckung besteht darin, den Ertragsausfall aufgrund eines Angriffs abzusichern. Wichtig ist hierbei, dass der Auslöser zur Leistungspflicht klar definiert ist. Eine entscheidende Rolle für die Bemessung der Versicherungsleistung stellen auch die Dauer der Betriebsunterbrechung, die maximale

Haftzeit und die zeitliche Selbstbeteiligung/Wartefrist dar.

Drittschäden

(z. B. versichertes Risiko, versicherte Gefahren, Abwehrkosten, Straf-Rechtsschutz, Erstattung von Bußgeldern wegen Datenschutzverletzungen)

Ein zentraler Deckungsbaustein von Cyber-Versicherungen sind auch Drittschäden. Dabei hat die Drittschäden-Absicherung innerhalb von Cyber-Versicherungen einen signifikanten Haftpflichtcharakter. Es sollte demnach Versicherungsschutz für durch einen Dritten gegen den Versicherungsnehmer, die mitversicherten Unternehmen oder die versicherten Personen geltend gemachten Haftpflichtanspruch für Cyber-Schäden bestehen.

Auch im Hinblick auf die unberechtigte Veröffentlichung von digitalen Medien und den daraus resultierenden Verstößen gegen das Wettbewerbsrecht ist besondere Sorgfalt bei der Auswahl des angemessenen Versicherungsschutzes zu wahren. Dabei kommt es auch darauf an, ob der Versicherer im Sinne des Versicherten die Verteidigung bei öffentlich-rechtlichen Verfahren durch Datenschutzverletzungen übernimmt. Einige Tarife bieten in diesem Zusammenhang einen Straf-Rechtsschutz an oder erstatten Bußgelder, die aufgrund von Datenschutzverletzungen verhängt wurden.

Schadenmanagement

(z. B. Unterversicherungsverzicht, Regressverzicht, Kostenanrechnung, Kostenübernahme für psychologische Unterstützung)

Beim Abschluss des Versicherungsschutzes stellt der gemeldete Vorjahresumsatz eine Prämien-Bemessungsgröße für die Betriebsunterbrechungsabsicherung dar. Jedoch hat die Auswirkung einer festgestellten Unterversicherung Auswirkungen auf sämtliche Deckungselemente. Sollte also der gemeldete Vorjahresumsatz niedriger sein als der tatsächliche Vorjahresumsatz, wird die Entschädigungsleistung verhältnismäßig gekürzt. Wünschenswert wäre hier die Darstellung von Korrelation und Kausalität des Vorjahresumsatzes eines Unternehmens zur Prämienberechnung außerhalb der Betriebsunterbrechungsabsicherung. Werden im Rahmen des Versicherungsschutzes Schäden auch dann versichert, wenn diese von Mitarbeitern des Versicherungsnehmers oder von anderen mitversicherten Unternehmen vorsätzlich herbeigeführt wurden, stellt sich die Frage, ob der Versicherer darauf verzichtet, nicht vorsätzlich handelnde Mitarbeiter in Regress zu nehmen.

Im Rahmen der kostenfreien Assistance-Dienstleistungen wird einem betroffenen Unternehmen neben 24/7-Hotline(s) auch ein Krisenplan zur Verfügung gestellt. Bei Unternehmen, die einen größeren Wirkungsradius haben, ist hinsichtlich der Hotlines zu prüfen, ob diese auch in der jeweiligen Landessprache zu erreichen ist. Gleiches gilt für den Krisenplan.

Sollte der Druck auf das Personal bzw. die versicherten Personen bei der Kompromittierung persönlicher Daten oder auch bei auftretenden Schuldzuweisungen oder Existenzängsten der Betroffenen nur noch professionell zu lösen sein, ist die Kostenübernahme von psychologischer Betreuung ein sinnvoller Leistungsbaustein, dessen Vorhandensein und Umfang in der Bewertung ebenfalls berücksichtigt wird.

Transparenz

(z. B. Definition von Legalbegriffen, Beispiele, Dienstleister)

Im Hauptkriterium Transparenz wird die Übersichtlichkeit und nachvollziehbare Ausgestaltung der Versicherungsbedingungen als Ganzes untersucht. Der Kunde sollte möglichst übersichtlich, verständlich und sachlogisch durch die vielfältigen Begrifflichkeiten und Definitionen geführt werden. Hierbei hilft beispielsweise die Verwendung eines Glossars, die Nennung von Fallbeispielen oder die plastische Erklärung von Sachverhalten.

Darüber hinaus wird auch die transparente Darstellung der kooperierenden Dienstleister im Rahmen der Assistance-Leistungen gewürdigt. Wenngleich sich die praktische Kompetenz und Serviceverfügbarkeit der Dienstleister über eine Bedingungsbetrachtung naturgemäß nicht einschätzen lässt, wird die bedingungsmäßige Zusicherung von Dienstleistern mit anerkannter Zertifizierung (z. B. BSI-Zertifizierung) positiv berücksichtigt.