Und es nimmt kein Ende...

Wesentliche Veränderungen im Bereich von Haftung und Versicherungsschutz 2017 und 2018

Von Dipl. Betriebswirt (FH) Bernd Michael Schäfer

→ In den letzten beiden Jahren hat es eine Reihe von Veränderungen gegeben, die das Handeln von Sicherheitsdienstleistern erheblich beeinflussen. Im Folgenden eine kurze Übersicht mit den wesentlichen Punkten.

Arbeitnehmerüberlassungsgesetz (AÜG) per 01.04.2017

Einer der wesentlichen Punkte der Gesetzänderung besteht darin, dass es heute steuer- und sozialversicherungsrechtlich nicht mehr relevant ist, was Auftraggeber und Sicherheitsdienstleister vereinbaren. Vielmehr ist entscheidend, was ein Dritter – also zum Beispiel der Zoll – bei Prüfung eines gegebenen Sachverhaltes feststellt. Probleme entstehen zum Beispiel in gemischten Teams, in denen Mitarbeiter des Auftraggebers den Mitarbeitern des Dienstleisters Anweisungen geben oder wenn diese eigenständig untereinander Urlaubsvertretungen und Ähnliches regeln. Strukturelle Probleme können im Bereich der Bewachung militärischer Anlagen durch die Befehle der Wachvorgesetzten entstehen. Bei Werk- und Betriebsfeuerwehren kann dies der Fall sein, wenn der Truppführer vom Auftraggeber, die von ihm geführten Einsatzkräfte aber von dem Dienstleister stammen. Weil hier die steuerliche und sozialversicherungsrechtliche Stellung der Mitarbeiter des Dienstleisters unklar ist, droht in allen diesen Fällen der Vorwurf der Hinterziehung von Steuern und Sozialabgaben. Um sich adäquat gegen diesen gefährlichen strafrechtlichen Vorwurf zu schützen, ist eine Strafrechtsschutzversicherung sinnvoll.

In der Betriebshaftpflichtversicherung gilt marktüblich Versicherungsschutz für Arbeitnehmerüberlassung gemäß der §§ 1 und 2 AÜG. Diese Deckung ist an bestimmte Voraussetzungen geknüpft. Will man Arbeitnehmerüberlassung machen, stellen sich beide Vertragspartner darauf ein, diese Voraussetzungen zu erfüllen. Will man das jedoch nicht und bei einer nachfolgenden Prüfung wird festgestellt, dass es sich trotzdem um Arbeitnehmerüberlassung handelt, so fehlen die Voraussetzungen für den Versicherungsschutz in der Betriebshaftpflichtversicherung. Der Sicherheitsdienstleister hat dann rückwirkend keinen Versicherungsschutz für das Auswahlverschulden, wenn er also ungeeignete Mitarbeiter auswählt und diese dann bei dem Auftraggeber einsetzt.

Was wie ein überschaubares Problem aussieht, kann schnell ein großes werden: Kein Versicherungsschutz besteht dann nämlich auch für die Abwehr von unberechtigten Ansprüchen des Auftraggebers. Diese werden immer dann geltend gemacht, wenn zum Beispiel der „überlassene" Gabelstaplerfahrer einen Schaden an der Halle des Auftraggebers verursacht und der Auftraggeber den Schaden lieber vom Dienstleister ersetzt haben möchte als vom Mitarbeiter des Dienstleisters, für den dieser nicht haftet, wenn er beim Auftraggeber tätig ist. Das ist leider unverständlich: Die von dritter Seite festgelegte Arbeitnehmerüberlassung führt dazu, dass der so bewertete Dienstleister die Abwehr selbst übernehmen und alle Kosten selbst tragen muss. Die Anpassung der Betriebshaftpflichtversicherung an der richtigen Stelle ist die erforderliche Maßnahme, um dieses Problem zu vermeiden.

DIN 77200-1 per 01.11.2017

Zwar ist die neue DIN in dem Punkt Versicherungsschutz besser als die vorhergehende. Allerdings bleibt sie aus unverständlichen Gründen hinter dem Mindeststandard des BDSW zurück. Nach wie vor hat ein Großteil der Sicherheitsdienstleister in Deutschland keinen Versicherungsschutz für strafbare Handlungen seiner Mitarbeiter (Brandstiftung, Diebstähle sowie Telefon- und Internetmissbrauch), die Versicherungssumme für die Beschädigung und Vernichtung bewachter Sachen verharrt mit 250.000 Euro auf dem unzureichenden Niveau

BERND MICHAEL SCHÄFER
ist Geschäftsführender Gesellschafter der ATLAS Versicherungsmakler für Sicherheits- und Wertdienste GmbH.

von § 6 BewachV. Lediglich den Punkt der Diebstähle regelt die neue DIN analog zu dem Mindeststandard; alles andere bleibt unfertig liegen und wartet auf die nächste Überarbeitung. Jeder Sicherheitsdienstleister ist für sich selbst und für alle von ihm eingesetzten Subunternehmer gut beraten, wenn er sich von seinem und von den Versicherern seiner Subunternehmer das Vorhandensein des Versicherungsschutzes nach BDSW-Mindeststandard auf dem Standardformular bestätigen lässt. Dieses kann hier heruntergeladen und mit dem eigenen Firmenlogo versehen werden: Nutzen Sie dazu den QR-Code oder **www.bdj.de/fileadmin/fotos/ATLAS/BHV_Mindeststandard_Bewachung.pdf**

Datenschutzgrundverordnung vom 25.05.2018

Dieses Ungetüm, welches für Facebook und Co. gedacht war, betrifft leider auch Wachdienst XY mit zehn Mitarbeitern. Die Lage ist derzeit unübersichtlich und mangels Rechtsprechung schwierig bewertbar. Fakt ist jedoch, dass jedes Unternehmen hier angreifbar ist. Die Folgen können schwerwiegend sein: 4 Prozent des Jahresumsatzes oder bis zu 20 Mio. Euro als Bußgeld gegen das Unternehmen, 50.000 Euro Bußgeld und/oder je nach Schwere des Verstoßes zwei bis drei Jahre Freiheitsentzug für die handelnde Person. Als „handelnde Person" gilt jeder, nicht nur der Datenschutzbeauftragte und die Geschäftsführung. Gerade bei kleineren Sicherheitsdienstleistern kann die Existenz gefährdet werden. Eine so hohe Strafe gegen den Halter der Gewerbeerlaubnis nach § 34a GewO kann den Verlust der Erlaubnis nach sich ziehen.

Jedes Unternehmen muss einen Datenschutzbeauftragten haben, sobald zehn Personen und mehr in der automatisierten Verarbeitung personenbezogener Daten dauerhaft beschäftigt sind (§ 38 BDSG vom 30.06.2017). Damit ist auch klargestellt, dass nicht jedes Sicherheitsunternehmen mit mehr als insgesamt zehn Mitarbeitern einen Datenschutzbeauftragten benötigt. Der Datenschutzbeauftragte kann intern bestellt oder extern beauftragt sein. Grundsätzlich ist bei kleineren und mittleren Unternehmen die Beauftragung eines externen Datenschutzbeauftragten vorzuziehen. Dieser ist auf diese Tätigkeit spezialisiert und immer tagaktuell am Thema. Insbesondere haftet er für Fälle, in denen er falsch berät. Um sich dagegen abzusichern, ist es erforderlich, dass er eine Vermögensschadenhaftpflichtversicherung eindeckt und dies gegenüber seinem Auftraggeber nachweist. Hier gibt es im Moment noch viel Wildwuchs, da viele Dienstleister nicht den erforderlichen Nachweis liefern. An dieser Stelle der ganz klare Hinweis, dass die Unternehmen als Auftraggeber von externen Datenschutzbeauftragten immer den Nachweis für eine Vermögensschadenhaftpflichtversicherung einfordern sollten. Dies ist nicht gleichzusetzen mit einer Betriebshaftpflichtversicherung, was oft verwechselt wird.

Wird ein interner Datenschutzbeauftragter bestellt, so kann dessen Haftungsrisiko für von ihm verursachte Schäden für das Unternehmen durch eine separate Vermögensschadenhaftpflichtversicherung abgedeckt werden. Außerdem sollte er in die bestehende D&O-Versicherung als mitversicherte Person mit aufgenommen werden.

Cyberattacken

Die Bedrohungslage, der alle Unternehmen ausgesetzt sind, wächst. Mittlerweile gibt es auch Attacken auf Sicherheitsunternehmen. Bei einem Unternehmen wurden die virtuellen Server der Notrufserviceleitstelle für die Kameras „gehackt" und gesperrt. Mehrere Tage dauerte die Wiederherstellung, in dieser Zeit war eine große Anzahl von Objekten nicht kameraüberwacht. In einem anderen Fall wurden vier virtuelle Server mit allen Unternehmens- und Kundendaten übernommen und gegen Zahlung eines Lösegeldes nach fast zwei Wochen wieder freigeschaltet.

Die finanziellen Auswirkungen eines Schadens aus diesem Bereich können mittlerweile allerdings durch brauchbare Versicherungsprodukte gepuffert werden.

Grundsätzlich gibt es Möglichkeiten für sogenannte Annex-Lösungen, also Cyberdeckungen, die an andere Verträge angehängt werden (zum Beispiel an Sach-Inhaltsversicherung oder Betriebshaftpflicht). Vorteilhaft dabei ist, dass dies problemlos geht und man auch keinen aufwändigen Fragebogen benötigt. Nachteilig ist jedoch, dass es sich nur um Ausschnittsdeckungen handelt, die zum Beispiel regelmäßig den Baustein „Erpressungsgeld" nicht abdecken.

Eigenständige Cyberdeckungen bieten heute – anders als noch vor fünf Jahren – zwar regelmäßig ausreichenden und bezahlbaren Versicherungsschutz. Allerdings setzen viele Versicherer einen von IT-Experten entwickelten Fragebogen voraus. Dieser wird oft nicht ausgefüllt und deshalb kommt es auf diesem Weg derzeit selten zum Abschluss. Allerdings gibt es praktikable Lösungen für Unternehmen bis zu 10.000.000 Euro Jahresumsatz.

Bei größeren Unternehmen sollte eine Risikoanalyse durch einen externen Berater erfolgen. Zum einen erhält das Unternehmen durch diese externe Expertise wichtige Hinweise, wie es sich schützen kann. Die neutrale Meinung eines Beraters, der nicht betriebsblind ist und – anders als der IT-Verantwortliche des Unternehmens – kein Interesse daran hat, Schwachstellen zu kaschieren, zeigt möglicherweise ungeahnte Schwachstellen auf. Zum anderen ist ein Teilergebnis dieser Analyse ein perfekt ausgefüllter Fragebogen, auf dessen Basis dann der geeignete Versicherungsschutz ermittelt und hergestellt werden kann. ←

Checkliste Versicherungsschutz 2017/2018

DATUM	VORSCHRIFT	PROBLEM	LÖSUNG
01.04.2017	**Arbeitnehmer-überlassungs-gesetz (AÜG)**	Versicherungsschutz besteht nur bei Arbeitnehmerüberlassung gemäß der §§ 1 und 2 AÜG.	Die Deckung der Betriebshaftpflichtversicherung muss darauf angepasst werden. Auch im Falle des Nichteinhaltens der gesetzlichen Vorgaben, wenn also ANÜ nicht gewünscht ist, aber nachträglich von Dritten (z. B. Zoll) festgestellt wird, muss Deckung bestehen. Gegen die aus der Verteidigung gegen den Vorwurf der Hinterziehung von Steuern und Sozialabgaben resultierenden Aufwendungen (Strafverteidiger, Gerichtskosten, Gutachterkosten) hilft die Eindeckung einer Strafrechtsschutzversicherung.
01.11.2017	**DIN 77200-1**	**Problem 1** Die DIN unterschreitet den Mindest-standard des BDSW und sorgt dadurch für Verwirrung. **Problem 2** Sehr viele Unternehmen haben keinen Versicherungsschutz für strafbare Handlungen ihrer Mitarbeiter, insbesondere nicht für Diebstähle gemäß Ziffer 4.3 DIN 77200-1.	**Zu Problem 1** Versicherungsschutz sollte ausnahmslos nur mit Versicherungsbestätigungen nach BDSW-Mindest-standard nachgewiesen werden, auf denen sich der Zusatz „Erfüllt die Vorgaben der DIN 77200-1 in der aktuellen Fassung." befindet. **Zu Problem 2** Im Versicherungsvertrag sollte explizit nachlesbar geregelt sein, dass Versicherungsschutz für straf-bare Handlungen der Sicherheitsmitarbeiter besteht, insbesondere für Fälle von Brandstiftung, Diebstahl sowie Telefon- und Internetmissbrauch.
25.05.2018	**Datenschutz-grundverord-nung (DSGVO)**	**Problem 1** Die Vielzahl von möglichen Verstößen macht eine Vermeidung schwierig. Die hohen Strafen gegen Unternehmen (Art. 83 DSGVO: bis zu 4 Prozent des Jahresumsatzes oder bis zu 20 Mio. Euro, je nachdem, welcher Betrag höher ist), aber auch gegen die handelnden Personen (bis zu 50.000 Euro nach § 43 (2) BDSG) und dazu die Bedrohung mit Frei-heitsstrafen bis zu 3 Jahren (BDSG § 42 (1) und (2)) machen eine Verteidigungsstrategie erforderlich. **Problem 2** Durch Fehler in den AGB und insbesondere auf der Website drohen Abmahnungen. **Problem 3** Externe wie interne Datenschutzbeauftragte können Schäden verursachen.	Auslagerung des Risikos durch die Beauftragung eines externen Datenschutzbeauftragten, der für Falschberatung haftet und versichert ist. Hier ist der Nachweis der Vermögensschadenhaftpflichtversiche-rung wichtig. Bei internen Datenschutzbeauftragten Eindeckung einer speziellen Vermögensschadenhaft-pflichtversicherung. Zur Verteidigung gegen Vorwürfe in einem Straf-verfahren Eindeckung einer Strafrechtsschutzver-sicherung. Um sich gegen Abmahnungen zu wehren Eindeckung einer Firmenrechtsschutzversicherung entweder generell oder speziell für Schäden aus dem Bereich der DSGVO. Zum Schutz des Managements gegen Schadenersatz-ansprüchen aus Pflichtverletzungen Eindeckung einer D&O-Versicherung. In dieser muss der interne Daten-schutzbeauftragte als mitversicherte Person aufge-führt sein.
Laufend		Cyberangriffe » Betriebsunterbrechung » Hackerangriffe » Erpressungsgelder » Hardwareschäden » Datenverluste » Krisenreaktion » Haftpflichtschäden	Eindeckung einer Cyberversicherung bestehend aus » Cyberhaftpflicht, » Eigenschaden-Deckung und » Betriebsunterbrechungs-Versicherungsschutz