News 02 | 2022

IRM Versicherungsberatung GmbH

INHALT

Vorbeugende Schutzmaßnahmen für Serverräumlichkeiten

In Serverräumen und Rechenzentren entstehen insbesondere durch den Betrieb von Servern erhebliche Mengen Wärme, die abzuleiten sind, um die elektrischen Bauteile nicht zu überhitzen oder zu beschädigen. Daraus resultiert ein erhöhtes Brandrisiko. Im Rahmen einer ganzheitlichen Risikobetrachtung reicht dabei die Ausstattung mit Brandmeldetechnik und Löschanlagen allein nicht aus, um die Anlagen und die gespeicherten Daten wirksam zu schützen.

Gerade bei der Neubauplanung sollte die Wahl der Baumaterialien vor dem Hintergrund der Nicht-Brennbarkeit der Bausubstanz entsprechend berücksichtigt werden. Darüber hinaus ist für eine zusätzliche Feuerfestigkeit der Räumlichkeiten eine Brandabschottung sowohl von Wänden als auch Decken von essenzieller Bedeutung. Gerade die Durchführungen in Wänden und Decken für die Verkabelung können sich im Falle eines Brandes als weiterleitende Verbindungen zwischen den verschiedenen Räumlichkeiten herausstellen. Dadurch kann ein Feuer bzw. die Rauchausbreitung eine Verbindungsbrücke in andere Betriebsbereiche begünstigen.

Ein weiteres wichtiges Merkmal in der Absicherung bildet der Kühlungsprozess der Rechner, um eine Überhitzung zu vermeiden. Dabei ist die Gewährleistung einer permanenten Stromversorgung incl. Notstromversorgung zur Aufrechterhaltung des Kühlungssystem unabdingbar. Führt beispielsweise eine Unterbrechung der Stromversorgung zu einem Ausfall der Kühlung, so staut sich die von den Servern abgegebene Temperatur und steigt insgesamt rasch an. Dieser Umstand kann einerseits die Funktionsfähigkeit der Server mindern und andererseits auch einen Brand begünstigen. Gerade deshalb sind aus Serverräumen Brandlasten (z.B. Kartonagen, verpackte Ersatzteile) zwingend zu entfernen.

Auch sind Serverräume besonders vor Feuchtigkeit und Nässe zu schützen. Es empfiehlt sich regelmäßig zu prüfen, ob die Dichtigkeit von Gebäudeteilen (Dach, Decken, Wände) gegeben ist. Ferner sollten grundsätzlich keine Flüssigkeit führenden Leitungen (Wasserleitungen, Abflussleitungen, Kühlleitungen etc.) durch Serverräume führen. Insbesondere in betriebsfreien Zeiten kann sich z.B. ein zunächst räumlich geringer Leitungswasserschaden für Server und gespeicherte Daten zu einem Großschaden entwickeln. Der Einbau von Leckagedetektoren hilft dabei, einen solchen Vorfall rechtzeitig zu erkennen.

> > >

Bei Ausbruch eines Brandes in Serverräumlichkeiten hat ein rasches Löschen natürlich höchste Priorität. Wird der Brand frühzeitig erkannt, ist der Einsatz einer gasbasierten Löschanlage zu empfehlen. Derartige Anlagen können auch nachträglich noch in bestehende Räumlichkeiten zur Erreichung eines höheren Schutzgrades eingebaut werden.

Mit den vorgenannten Maßnahmen lassen sich Serverräumlichkeiten vorbeugend absichern. Zu einer gesamtheitlichen Betrachtung gehört allerdings auch die Dokumentation von Notfall- bzw. Business-Continuity-Plänen:

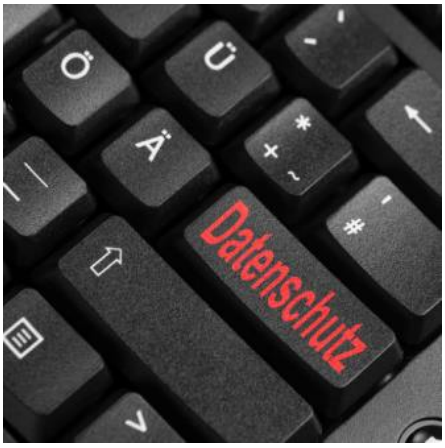
- Der Notfallplan beschreibt die Maßnahmen, wenn der Betrieb von einem Ausfall oder einer Abschaltung betroffen ist.
- Ein Business-Continuity-Plan beinhaltet einen Maßnahmenkatalog für die Aufrechterhaltung des Betriebs in Folge eines Schadenereignisses.

Ferner sollte auch sichergestellt sein, dass diese Pläne in regelmäßigen Abständen überprüft werden und der verantwortliche Personenkreis im Unternehmen die in den Plänen festgehaltenen Maßnahmen sensibilisiert haben und beherrschen.

Fazit

Digitale Daten bilden mittlerweile den Kern eines jeden gewerblichen und industriellen Unternehmens und sind für den täglichen Geschäftsbetrieb unverzichtbar. Deshalb hat vor allem eine umfangreiche Absicherung der Serverräume gegen die unterschiedlichsten Gefahren eine besondere Priorität erhalten. Maßnahmen zur Verhinderung bzw. Eingrenzung von Schadenfällen haben in der Versicherungswirtschaft vor dem Hintergrund steigender Schadenzahlungen einen nochmals größeren Stellenwert gewonnen. Derartigen Maßnahmen sollte in Serverräumen eine besondere Aufmerksamkeit geschenkt werden.

markus.alber@irm-vb.de



Versicherungsschutz für Datenschutzverletzungen und ihre Folgen

Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG - besser bekannt als Datenschutz-Grundverordnung (DSGVO) - ist seit dem Jahr 2018 innerhalb des Europäischen Wirtschaftsraums anzuwenden. Sie bildet den Rahmen für die Verarbeitung von personenbezogenen Daten. Viele Unternehmen haben die Einführung der DSGVO kritisch beäugt, da diese Sanktionen bei Nichteinhaltung der datenschutzrechtlichen Vorschriften von bis zu 20 Mio. € oder 4% des weltweiten Umsatzes vorsehen.

In jüngster Vergangenheit wurden immer wieder Fälle bekannt, bei denen Datenschutzbehörden Bußgelder gegen Unternehmen auf Grund sol-

cher Verstöße verhängt haben. So musste bspw. die AOK in Baden-Württemberg ein Bußgeld von über 1,2 Mio. € zahlen, da die vorhandenen technischen und organisatorischen Maßnahmen nicht geeignet waren, einen Datenschutzvorfall zu verhindern. In einem öffentlichen Fall aus der jüngeren Vergangenheit, dem Datenschutzvorfall der Scalable Capital, konnten Betroffene des Vorfalls nun vor Gericht einen Schadensersatzanspruch gegenüber Scalable Capital auf Grund eines Identitätsdiebstahl durchsetzen (Hinweis: Das LG München und das LG Köln sprachen zwei Klägern einen Schadensersatz von € 2.500 bzw. € 1.200 zu. Beide Urteile sind aber noch nicht rechtskräftig). Nach Art. 82 DSGVO müssen Verantwortliche oder Auftragsverarbeiter einen materiellen oder immateriellen Schaden ersetzen, sofern sie gegen die Verordnung verstoßen. Dabei sind jedoch verschiedene Faktoren wie Form, Verschulden und Dauer des Verstoßes zu berücksichtigen.

Es ist insgesamt festzustellen, dass auf der einen Seite vor allem Unternehmen die Anforderungen der DSGVO noch nicht vollständig umgesetzt haben, auf der anderen Seite einige Personen (und auch deren juristische Berater) für dieses Thema immer mehr sensibilisiert sind.

Daher wird es für Unternehmen im Zuge des aktiven Risikomanagements neben der Evaluierung und dem Ausbau der Prozesse und Maßnahmen hinsichtlich der Verarbeitung von personenbezogenen Daten immer wichtiger zu prüfen, welchen Versicherungsschutz Sie im Rahmen eines möglichen Datenschutzvorfalls haben.

Dabei kommen in aller Regel drei Arten von Versicherungen in Betracht:

1. Rechtschutz-Versicherung
2. Haftpflicht-Versicherung
3. Cyber-Versicherung

(Straf-) Rechtschutz-Versicherungen bieten Versicherungsschutz in der Form der Übernahme von Kosten gegenüber versicherten Personen (teilw. in einem eingeschränkten Umfang auch gegenüber dem versicherten Unternehmen), die für die rechtliche Beratung und Verteidigung in einem Verfahren anfallen. Der Versicherungsschutz von eventuellen Ansprüchen oder Sanktionen sehen Rechtschutz-Versicherungen nicht vor.

Daneben kann ein Datenschutzvorfall auch ein deckungsauslösendes Element einer Haftpflicht-Versicherung (bspw. einer Betriebs- oder Vermögensschaden-Haftpflicht-Versicherung) sein. Diese bietet Versicherungsschutz, sofern Ansprüche gegen versicherte Personen oder Unternehmen auf Grundlage gesetzlicher Ansprüche, wie es auch die DSGVO ist, erhoben wird. Der Versicherungsschutz umfasst die Prüfung des Anspruches und, sofern dieser versichert ist, die Abwehr unberechtigter sowie die Befriedigung berechtigter Ansprüche. Ein Ausschlussgrund einer Haftpflicht-Versicherung kann durch vorsätzliches Handeln, einen Wechsel des Risikoträgers (Stichwort Rückwärtsdeckung) oder einem speziellen Ausschluss (Stichwort Silent-Cyber) vorliegen. Nicht vom Versicherungsschutz von Haftpflicht-Versicherungen umfasst sind sämtliche Strafzahlungen oder Bußgelder sowie damit einhergehende Kosten.

Wie bereits in dem Artikel unserer vorherigen Ausgabe 01/2022 der IRM News beschrieben, versuchen Versicherungsunternehmen Cyber-Risiken in ihren Versicherungsverträgen abzugrenzen. Dies kann bei Schadenfälle durch Datenschutzverstößen im Zusammenhang mit Cyber-Vorfällen dazu führen, dass ein möglicher Versicherungsschutz ausschließlich über spezielle Cyber-Versicherungen geboten wird. Cyber-Versicherungen beinhalten in aller Regel auch Komponenten aus klassischen Haftpflicht-Versicherungen und versichern explizit auch Datenschutzvorfälle. Cyber-Versicherungen bieten im Falle eines Datenschutzvorfalles aber nicht nur Versicherungsschutz für die Abwehr oder Befriedigung von Ansprüchen Dritter, es besteht auch für das Unternehmen als Versicherungsnehmer in abschließend genannten Kostenpositionen oft selbst Versicherungsschutz. Diese Kosten können in Form von rechtlicher Beratung, Krisenmanagement oder öffentlichkeitswirksamen Maßnahmen bestehen.

Einige Bedingungen für Cyber-Versicherungen am deutschen Versicherungsmarkt sehen auch die Möglichkeit vor, Bußgelder gegenüber Unternehmen zu versichern. Hierzu

behalten sich die Versicherungsunternehmen jedoch das Recht in den Versicherungsbedingungen vor, den Versicherungsschutz zu versagen, sofern die Versicherbarkeit von Bußgeldern in der jeweiligen Rechtsordnung eines Landes verboten ist. Eine explizite rechtliche Grundlage für ein Verbot zur Versicherbarkeit von Bußgeldern gibt es in Deutschland nicht, jedoch gab es bereits gerichtliche Entscheidungen durch die Versicherungsschutz von Bußgeldern versagt wurde. Auch die herrschende Meinung unter Juristen geht davon aus, dass es nach aktueller gesetzlicher Lage keine Grundlage für die Versicherbarkeit von Bußgeldern in Deutschland gibt. Vor dem Hintergrund dieser Diskussionen und der immer öfter aufkommenden gegenteiligen Meinung kann der Versicherungsschutz ohne eine höchstrichterliche Entscheidung oder eine Anpassung der gesetzlichen Rahmenbedingungen nicht abschließend beurteilt werden.

Sofern ein Unternehmen durch einen Datenschutzvorfall einen Schaden erlitten hat und dies auf ein zu vertretendes Handeln eines Organs zurückzuführen ist, kann über einen Regress beim Organ auch Versicherungsschutz über eine D&O-Versicherung bestehen. Hierbei ist jedoch ebenfalls zu beachten, dass derzeit keine rechtssichere Aussage über die Möglichkeit zum Versicherungsschutz von Regressen von Bußgeldern bei Organen von Unternehmen getroffen werden kann. Ein aktuelles Verfahren zu diesem Thema wurde nach derzeitiger Kenntnis durch einen Vergleich beendet. Zudem steht auch noch eine rechtlich kontroverse Diskussion im Raum, ob und in welcher Form Regresse eines Unternehmens-Bußgeld gegenüber einem Organ überhaupt zulässig sind.

Fazit:

Datenschutzvorfälle können für Unternehmen erhebliche Risiken darstellen. Dabei ist die Art der personenbezogenen Daten die gespeichert werden, der Umfang des Verstoßes bzw. des Mitverschuldens sowie die Anzahl der Daten zu berücksichtigen. Klassische Versicherungsprodukte wie Rechtschutz-, Haftpflicht- und Cyber-Versicherungen bieten für solche Fälle meist Deckung durch Übernahme von rechtlichen Kosten oder Ersatz von Ansprüchen. Strafzahlungen und Bußgelder sind nach derzeitiger Auffassung am deutschen Versicherungsmarkt nahezu nicht versicherbar.

christian.schuster@irm-vb.de

KONTAKT

IRM
Versicherungsberatung GmbH

Postfach 31 13 31, 70473 Stuttgart
Mittlerer Pfad 19, 70499 Stuttgart
Telefon: +49 711 820 508 0
Telefax: +49 711 820 508 11

Markus Alber
Telefon: +49 711 820 508 21
Mobil: +49 151 147 163 21
E-Mail:markus.alber@irm-vb.de

Thomas Hardt
Telefon: +49 711 820 508 24
Mobil: +49 151 147 163 24
E-Mail:thomas.hardt@irm-vb.de

www.irm-vb.de

Möchten Sie unsere IRM-News künftig
per E-Mail anstatt per Post erhalten?
Dann geben Sie uns bitte einen kurzen Hinweis an
E-Mail: info@irm-vb.de
oder per Telefon: +49 711 820 50 80