LEGAL REVOLUTIONary
Recht in der digitalen Wirtschaft

Gefahr durch Cyber-Angriffe

Absicherungsmöglichkeiten und Haftungsfragen beim Thema IT-Sicherheit

Marco Degginger | Associate | Oppenhoff

Sebastian Gutmann | Associate | Oppenhoff

28. Dezember 2020

LR 2020, Seiten 337 bis 342 (insgesamt 6 Seiten)

Um Betriebsausfälle und eine persönliche Haftung zu vermeiden, sollten Geschäftsführer ihre Unternehmen vor Cyberattacken ausreichend schützen. Hilfestellung bieten insbesondere anerkannte IT-Sicherheitsstandards und Versicherungslösungen.

Die Digitalisierung der deutschen Wirtschaft schreitet mit großen Schritten voran. Nicht erst die Coronapandemie fordert den Auf- und Ausbau digitaler Infrastrukturen (Stichwort Home-Office). Stand 2018 arbeitete bereits jede vierte Maschine in deutschen Fabriken vernetzt, Tendenz steigend. 2

Gleichzeitig erlitten in den Jahren 2018/2019 laut einer Umfrage des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien in Deutschland 75 % der befragten Unternehmen eine Cyberattacke. Derartige Angriffe sind vielfältig: Sie reichen von der Ausspähung von Daten über die Beeinträchtigung der Erreichbarkeit von Webservern bis hin zur Infizierung ganzer unternehmensinterner IT-Systeme mit Schadsoftware. Ein besonders beliebtes Angriffsziel stellen dabei mittelständische als GmbH fungierende Unternehmen in der Größe 100-499 Mitarbeiter dar. Der vorliegende Artikel beleuchtet zum einen die rechtlichen Rahmenbedingungen der IT-Sicherheit in Unternehmen. Zum anderen soll er mittelständischen Unternehmen als Praxishilfe zur Umsetzung von Präventivmaßnahmen sowie zur Sicherstellung möglichst effizienten Schadensersatzes nach einer Cyberattacke dienen.

I. Gesetzliche Pflichten zur Gewährleistung einer angemessenen IT-Sicherheit?

Weder das europäische noch das deutsche Gesetz regeln für Unternehmen zusammenhängend Pflichten hinsichtlich des Aufbaus IT-sicherheitstechnischer Mindeststandards. Relevante Vorschriften finden sich vielmehr verstreut in mehreren Sondergesetzen. Ein solches Gesetz, das in der Praxis nahezu jedes Unternehmen betrifft, ist die Europäische Datenschutz-Grundverordnung (DSGVO). Bei Verarbeitung personenbezogener Daten sind hier insbesondere Art. 25 und Art. 32 DSGVO zu beachten, 3

die die Umsetzung von „geeigneten technischen und organisatorischen Maßnahmen" zur Erreichung eines „angemessenen Schutzniveaus" vorschreiben. Unternehmen, die eine „kritische Infrastruktur" betreiben (insbes. Unternehmen aus den Sektoren Energie, Telekommunikation und Gesundheit; Einzelheiten ergeben sich aus der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (KritisVO)), müssen gem. § 8a Abs. 1 BSI-Gesetz angemessene Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse treffen. Für Betreiber von Kommunikationsnetzen gilt zusätzlich § 109 TKG, der spezifische Pflichten zu IT-sicherheitstechnischen Vorkehrungen enthält.

II. Möglichkeiten zur Installation eines adäquaten IT-Sicherheitskonzepts

Neben der Verarbeitung personenbezogener Daten und den dargelegten Sonderregelungen gibt es keine allgemeine Pflicht zu Aufbau und Absicherung einer IT-Infrastruktur. Dieser Mangel an Pflichten schützt jedoch selbstverständlich nicht vor Ertragsausfall oder Schadensersatzansprüchen, die sich aus Cyberangriffen ergeben (z.B. Produktionsstillstand durch Serverabstürze etc.). Als praktisch nutzbare Anleitung dazu, wie Unternehmen eine sinnvolle, risikogerechte IT-Infrastruktur aufbauen können, dienen daher vor allem die anerkannten technischen Standards und Vorgaben von Fachbehörden und Branchenverbänden. 4

1. Grundschutz des Bundesamts für Informationstechnik und der internationale Standard ISO/IEC 27001

Ein solcher Standard, der sog. IT-Grundschutz, wird durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben. Das internationale Äquivalent hierzu sind die Standards der ISO/IEC-27000-Reihe, insbesondere der Standard ISO/IEC 27001. Letztere werden von der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC) herausgegeben, bei denen es sich jeweils um in der Schweiz ansässige Vereinigungen nationaler Normungsorganisationen handelt (Mitglied der ISO ist bspw. das Deutsche Institut für Normung e.V. (DIN)). 5

a) Methodik des IT-Grundschutzes des BSI

Für deutsche Unternehmen ist der IT-Grundschutz des BSI zentral. Es handelt sich um eine ganzheitlich konzipierte Methodik, deren Ziel es ist, die Informationssicherheit in Behörden und Unternehmen zu erhöhen. Ganzheitlich ist die Methodik deshalb, weil sie sich nicht nur auf rein technische Aspekte stützt, sondern insbesondere auch dazu dient, die personellen und organisatorischen Voraussetzungen für eine zyklische Überprüfung der IT-Sicherheit zu schaffen. Der IT-Grundschutz des BSI besteht im Wesentlichen aus verschiedenen 6

Dokumenten, die jeweils Anleitungen zu Aufbau und Fortentwicklung der IT-Infrastruktur in Unternehmen und Behörden enthalten.

Welches Dokument für welche Institution zu empfehlen ist, richtet sich nach dem Bedarf und Entwicklungsstand des jeweiligen Unternehmens. Den Einstieg bietet der Leitfaden zur Basis-Absicherung, der auch kleineren Unternehmen, die sich noch nicht intensiv mit dem Thema befasst haben, einen verständlichen Einstieg bietet. Der BSI-Standard 200-1, der mit dem international anerkannten Standard ISO 27001 kompatibel ist, enthält allgemeine Anforderungen an ein Managementsystem für Informationssicherheit (ISMS), während der BSI-Standard 200-2 die Basis zum Aufbau eines weiter fortgeschrittenen ISMS bietet. Der Standard 200-2 wird durch das jeweils aktuelle „IT-Grundschutz-Kompendium" ergänzt, das für derzeit insgesamt 94 sicherheitsrelevante „Bausteine" (z.B. Ausspähen von Informationen, Schadprogramme, Kryptokonzept und Informationsaustausch) konkrete, dem Stand der Technik entsprechende Handlungsempfehlungen enthält und jährlich aktualisiert wird. Für fortgeschrittene Institutionen, die bereits mit der BSI-Grundschutzmethodik arbeiten, bietet der BSI-Standard 200-3 gebündelt risikobezogene Arbeitsschritte zur Erkennung und Behebung eventuell noch bestehender Defizite. 7

Unabdingbar für die Schaffung und den Erhalt eines angemessenen Niveaus der Informationssicherheit ist insbesondere die Errichtung einer effizienten Binnenstruktur im Unternehmen selbst. Denn die dauerhafte Umsetzung gleich welcher Sicherheitsstandards ist kein einmaliges Geschehen, sondern erfordert einen kontinuierlichen Fortentwicklungs- und Überprüfungsprozess. Das Thema IT-Sicherheit sollte von der obersten Leitungsebene des Unternehmens – bei einer GmbH also durch die Geschäftsführer – initiiert, gesteuert und kontrolliert werden. Die Umsetzung der notwendigen Schritte in die Praxis kann dabei regelmäßig an einen zentralen Mitarbeiter, den Informationssicherheitsbeauftragten (ISB), delegiert werden. Die Koordination und Kommunikation zwischen dem ISB und der Leitungsebene bildet einen integralen Teil der BSI-Grundschutz-Methodik.

b) Möglichkeit der Zertifizierung

Möchte sich ein Unternehmen die Qualität seiner praktizierten Informationssicherheit bescheinigen lassen, ermöglicht das BSI u.a. die Ausstellung eines Testats nach der Basis-Absicherung und – weitergehend – die Zertifizierung der Einhaltung des internationalen Standards ISO-27001 auf der Basis des IT-Grundschutzes. Voraussetzung für die Ausstellung des Testats/die Zertifizierung ist jeweils die Überprüfung des jeweiligen ISMS durch einen vom BSI zertifizierten Auditor. Zertifizierte Unternehmen und der Gegenstand der jeweiligen Zertifizierung werden auf der Webseite des BSI veröffentlicht. Global Player, wie z.B. die Deutsche Post AG oder Vodafone, aber auch viele Mittelständler haben von der Möglichkeit eines solchen Zertifizierungsverfahrens bereits Gebrauch gemacht. 8

2. Handreichungen zur IT-Sicherheit von Branchenverbänden

Neben den IT-Grundschutz des BSI und den Standard ISO/IEC 27001 treten Handreichungen diverser Branchenverbände (z.B. die Handreichung zum Stand der Technik in der IT-Sicherheit des Bundesverbands IT-Sicherheit e.V.), denen eine ergänzende Funktion zukommt. Verbände der Betreiber Kritischer Infrastruktur im Sinne der KritisVO geben auf der Grundlage von § 8a Abs. 2 BSIG branchenspezifische Sicherheitsstandards heraus. Diese werden durch das BSI genehmigt und enthalten teilweise speziellere Vorgaben als die genannten BSI-Standards. Beispiele hierfür sind die Sicherheitsstandards der Deutschen Krankenhausgesellschaft e.V. und des Bundesverbands der Energie- und Wasserwirtschaft e.V. 9

III. Schadensersatz bei Cyberangriffen

Wird ein Unternehmen trotz aller ergriffener Sicherheitsvorkehrungen Opfer eines Cyberangriffs, stellt sich die Frage, wie erlittene Schäden ersetzt werden können. In Betracht kommt die persönliche Inanspruchnahme der Angreifer oder gar eigener Mitarbeiter (Angestellte oder Leitungsgremien), sofern diese den Angriff (mit-)verschuldet haben. Zusätzlich kann der Abschluss einer Cyber- und/oder D&O-Versicherung sinnvoll sein. 10

Es sollte beachtet werden, dass das Schadenspotenzial von Cyberangriffen enorm ist: Die Wiederherstellung gravierender Beschädigungen an unternehmensinterner IT erfordert nicht selten das Spezialwissen von externen Fachdienstleistern. Möglich sind ebenso ersatzpflichtige Schäden bei Vertragspartnern des betroffenen Unternehmens oder kommerzielle Einbußen, die durch die Ausspähung von Betriebs– und Geschäftsgeheimnissen entstehen. Schließlich können – insbesondere nach den Regeln der DSGVO – behördliche Bußgelder drohen, etwa wenn das betroffene Unternehmen die Preisgabe personenbezogener Daten durch eigene Versäumnisse im Bereich der IT-Sicherheit erst ermöglicht hat. 11

1. Ohne Versicherung meist keine greifbaren/solventen Arbeitgeber

Bei Angriffen von außen gelingt es in der Praxis nur selten, der Angreifer habhaft zu werden. Eigene Mitarbeiter, die durch fahrlässiges Verhalten unfreiwillig zum Erfolg von Cyberangriffen beitragen, haften für Schäden nur bei erhöhter Fahrlässigkeit. Sollte dies einmal der Fall sein, deckelte die Rechtsprechung bisher zusätzlich die zu begleichende Schadenssumme häufig auf das jeweilige Jahreseinkommen. 12

Einzig "greifbarer" Anspruchsgegner bleibt daher oft nur der eigene Geschäftsführer. Dessen Inanspruchnahme ist jedenfalls dann denkbar, wenn er eine angemessene

informationstechnische Absicherung des Unternehmens fahrlässig nicht vorgenommen hat. Denn gem. § 43 Abs. 1, 2 GmbHG haften Geschäftsführer einer GmbH für Schäden, die daraus resultieren, dass sie in den Angelegenheiten der Gesellschaft nicht die erforderliche Sorgfalt angewendet haben. Dies wird häufig der Fall sein, wenn der jeweilige Geschäftsführer nicht (unter Orientierung an den oben genannten Standards) dafür Sorge trägt, dass ein angemessenes IT-Sicherheitsniveau im Unternehmen hergestellt wird. Die anerkannten BSI Standards könnten somit in Zukunft nicht nur technische Hilfestellung sein, sondern im Einzelfall auch über Haftungsfragen entscheiden.

2. D&O Versicherung nicht immer ein Rettungsanker

Eng verbunden mit dem Thema Haftung des Geschäftsführers bei Cyberattacken ist eine mögliche Inanspruchnahme der D&O-Versicherung, also einer Versicherung, die das Unternehmen zur Abdeckung von Haftungsrisiken ihrer Leitungsorgane abschließt.

D&O-Versicherungen sind jedoch häufig nicht das Allheilmittel bei Verschulden des Geschäftsführers: Zum einen sind solche Versicherungen gerade in Unternehmen "cyberattackenbeliebter" Größenordnungen nicht besonders verbreitet, sofern keine Konzernpolice besteht. Doch auch dort, wo eine D&O-Versicherung vorliegt, schützt diese oft nicht vor allen Eventualitäten. Zwar finden sich in den einschlägigen Policen i.d.R. keine Ausschlüsse für Cyberattacken. Allerdings enthalten D&O-Versicherungen teils beträchtliche Selbstbehalte. Auch wird keine Deckung für Vorsatz übernommen. Gerade bei Unternehmen aus Branchen mit typischerweise risikobehafteten Datenbeständen (Automobilzulieferer, Medikamentenentwicklung etc.) wird sich die Versicherung bei Inanspruchnahme eher auf den Standpunkt stellen, der Geschäftsführer habe leichtfertig eine ordnungsgemäße IT-Sicherung unterlassen und so eine Auszahlung der Versicherungssumme verweigern. 13

3. Absicherung durch Cyberversicherung

Die standardmäßig abgeschlossenen Sachversicherungen, also Feuer, Elektronik- oder Maschinenversicherungen, greifen wiederum in aller Regel nur bei Sachschäden. Ein Cyber-Vorfall und die damit verbundenen Kosten lösen jedoch normalerweise keine Eingriffe in die Sachsubstanz aus. Unter den Sachversicherungen besteht daher in aller Regel kein Versicherungsschutz. 14

Schützen können sich Unternehmen hier mit sog. Cyberversicherungen, die bisher vergleichsweise wenig verbreitet sind. Vorteilhaft sind Cyberversicherungen vor allem deshalb, weil sie nicht nur Betriebsgewinn und fortlaufenden Kosten ersetzen, sondern teilweise sogar Expertenteams zur Ermittlung von Schadenquellen und Wiederherstellung

des IT-Systems zur Verfügung stellen bzw. finanzieren (sog. Assistance-Leistungen). Letzteres kann im Einzelfall wesentlich hilfreicher sein als die bloße Zahlung von Geld.

Gleichwohl gilt es auch hier, einige Besonderheiten zu beachten: So ist zum Beispiel nach den AVB-Cyber unklar, ob Schäden aus Datenverlusten durch Beschädigung oder Zerstörung einer Sache einen Deckungsfall darstellen. Auch fallen bei vielen Cyberversicherungen "kriegsähnliche" Handlungen unter den Ausschlusstatbestand. Nicht geklärt ist bisher, ob durch Organisationen oder gar Staaten in feindseliger Absicht flächendeckend eingesetzte Malware darunterfällt. Insofern sollte vor Vertragsabschluss geprüft werden, ob die entsprechende Police auf die Bedürfnisse des jeweiligen Unternehmens zugeschnitten ist.

IV. Fazit

In Deutschland existieren für die überwiegende Zahl der Unternehmen keine konkreten rechtlichen Vorgaben dazu, welche Maßnahmen zur Herstellung eines ausreichenden IT-Sicherheitsniveaus ergriffen werden müssen. Wegen des erheblichen Schadenspotenzials sind jedoch auch (oder vor allem) mittlere und kleine Unternehmen gut beraten, sich intensiv mit dem Thema IT-Sicherheit zu befassen. Denn eine mangelhafte informationstechnische Absicherung führt nicht nur zu erheblichen Risiken der Außenhaftung. Durch Cyberangriffe erlittene Schäden können regelmäßig nicht oder nicht vollständig durch eine Inanspruchnahme der Angreifer oder eigener Mitarbeiter ersetzt werden. Brauchbare Orientierungshilfen zum Aufbau eines angemessenen und risikogerechten Managementsystems für IT-Sicherheit bieten national und international anerkannte Sicherheitsstandards, wobei für deutsche Unternehmen eine Orientierung am IT-Grundschutz des BSI sinnvoll erscheint. Unternehmen, denen alleine die Prävention von Schadensfällen nicht genügt, können zusätzlich eine Cyber- und/oder D&O-Versicherung abschließen, wobei die jeweiligen Policen stets genau analysiert werden müssen. 15