Kommunikation & Recht

Betriebs-Berater für
● Medien ● Telekommunikation ● Multimedia

12
K&R

24. Jahrgang **Dezember 2021** Seiten 757 – 836

dfv Mediengruppe · Frankfurt am Main

jedoch kann an deren Stelle dispositives Gesetzesrecht treten.[45] Sie bestimmen nicht unmittelbar den Umfang der Vergütung von den Leistungen, die vom Anbieter auf rechtsgeschäftlicher Grundlage erbracht werden,[46] sondern wälzen lediglich Kosten oder Aufwendungen zur Erfüllung eigener gesetzlicher Verpflichtungen auf den Kunden ab.[47] Ob dies bei der weiteren Vergütung der Instandhaltung im Rahmen des Service der Fall ist, ist gerichtlich noch nicht geklärt. Dies kann hier auch dahinstehen, denn jedenfalls sind die Klauseln, wenn sie AGB darstellen, intransparent im Sinne des § 307 Abs. 1 S. 2 BGB und benachteiligen – auch unternehmerische – Vertragspartner in unangemessener Weise: § 307 Abs. 1 S. 2 BGB gebietet, AGB verständlich klar und übersichtlich zu gestalten.[48] Das gilt auch für den Preis. Der Kunde muss anhand der Klauseln nachvollziehen können, für welche Leistungen er welche Vergütung zahlt. Dieses Gebot der Preisklarheit wird unterlaufen, wenn im Rahmen der Servicegebühren eine „versteckte" weitere Vergütung für die Gebrauchserhaltungspflicht vorgesehen ist und sich diese daher aus zwei verschiedenen Vergütungen zusammensetzt. Dabei geht es weniger um die konkrete Höhe der Vergütung für die Gebrauchserhaltung, sondern darum, dass der Kunde davon ausgehen können soll, dass die gesamte Gebrauchserhaltung mit den Überlassungskosten vergütet wird. Den tatsächlichen Mietzins muss der Kunde sich also „zusammenbasteln".

Das Problem der Intransparenz lässt sich auch nicht durch die Abbedingung des § 535 Abs. 1 S. 2 BGB lösen. Obwohl die Gebrauchserhaltungspflicht des § 535 Abs. 1 S. 2 BGB grundsätzlich dispositiv ist,[49] wäre ein Ausschluss in AGB in diesen Fällen seinerseits gemäß § 307 Abs. 2 Nr. 1 und Nr. 2 BGB unwirksam. Zum einen wäre eine entsprechende Regelung mit wesentlichen Grundgedanken des Mietvertrags nicht vereinbar, da die Instandhaltungspflicht nur ausgeschlossen würde, damit der Softwareanbieter sich gegen ein Entgelt wieder dazu verpflichten lassen kann. Zum anderen kann die Instandhaltungspflicht nicht sinnvollerweise auf den Kunden abgewälzt werden, wenn dieser ohne den Quellcode der Software gar nicht in der Lage wäre, die Software zu bearbeiten. Die Software könnte also überhaupt nicht instandgehalten werden. Dadurch könnte ein Ausschluss wesentliche Rechte oder Pflichten, die sich aus der Natur des Mietvertrags ergeben, so einschränken, dass die Erreichung des Vertragszwecks – der ordnungsgemäßen Nutzung der Software – gefährdet wäre.

4. Lösungsvorschlag

Das Transparenzgebot des § 307 Abs. 1 S. 2 BGB setzt voraus, dass die Klausel so ausgestaltet ist, dass der Kunde klar erkennen kann, welche Leistung im Rahmen der Überlassung der Software und welche im Rahmen der Pflege (i. e. S.) der Software vergütet wird. Der Anbieter kommt also nicht umhin, die Leistungen, die der *Instandhaltung* der Software dienen, aus der Vergütungspflicht für die Pflegeleistung herauszunehmen. Dies kann er durch den Verweis auf eine detaillierte Leistungsbeschreibung tun, in der für die Serviceleistungen lediglich die Verbesserungsleistungen aufgeführt sind. Dafür muss sich der Anbieter zunächst selbst im Klaren darüber sein, welche Pflegeleistungen der Instandhaltung der Software dienen und welche sie lediglich verbessern sollen. Diese Frage hängt im Wesentlichen von dem Vertragszweck ab. So könnten auch neue Features der „vorbeugenden" Instandhaltung dienen, wenn die Software ansonsten veralten würde und nicht mehr dem Zweck entsprechend ordnungsgemäß genutzt werden könnte[50] (z. B. bei Anpassungen einer Steuersoftware an geänderte Steuergesetze). Serviceleistungen, die typischerweise unter die Gebrauchserhaltungspflicht fallen, sind beispielsweise: Patches, Bug Fixes, Beratungs- und Unterstützungsleistungen bei Systemausfällen, daraus notwendige Workarounds, Fehlersuche und Fehlerdiagnose.

45 BGH, 8. 10. 1998 – III ZR 278/97, NJW-RR 1999, 125, 126.
46 BGH, 23. 8. 2018 – III ZR 192/17, K&R 2018, 711 ff. = NJW 2019, 47 ff., Rn. 15.
47 BGH, 23. 8. 2018 – III ZR 192/17, K&R 2018, 711 ff. = NJW 2019, 47 ff., Rn. 15.
48 *Wurmnest*, in: Säcker/Rixecker/Oetker/Limperg (Fn. 9), § 307 Rn. 57.
49 *Häublein*, in: Säcker/Rixecker/Oetker/Limperg (Fn. 9), § 535 Rn. 127; *Schmidt*, in: Gsell/Krüger/Lorenz/Reymann (Fn. 19), § 535 Rn. 319.
50 *Roth-Neuschild*, in: Auer-Reinsdorff/Conrad (Fn. 39), § 13 Rn. 74.

RA Stefan Hessel, LL.M., RAin Karin Potel und Lizandra Beerwald*

Supply Chain Cybersecurity

Rechtliche Vorgaben für Cybersicherheit in der Lieferkette und Maßnahmen zur Abwehr von Cyberangriffen

Kurz und Knapp

Eine Supply Chain ist nur so stark wie ihr schwächstes Glied. Die gravierenden Auswirkungen von Cyberangriffen auf Unternehmen haben in den letzten Jahren immer wieder für Schlagzeilen gesorgt und treffen vermehrt ganze Unternehmensnetzwerke. Dieser Beitrag zeigt, welche gesetzlichen Vorgaben für Cybersicherheit in der Lieferkette gelten und erläutert, wie präventive Maßnahmen für die Abwehr von Cyberangriffen rechtlich sichergestellt werden können.

I. Einführung und Relevanz der Problemstellung

Supply-Chain-Management (kurz SCM) beschreibt das Lieferkettenmanagement und die damit zusammenhängenden Prozesse. Während bisher die einzelnen Bereiche weitgehend losgelöst voneinander standen, werden im SCM die Verbesserungspotenziale an den Schnittstellen aufgedeckt. SCM ist grundsätzlich kein neues Themengebiet der Betriebswirtschaft, sondern vielmehr eine führungsorientierte Sichtweise der Logistik in unternehmensübergrei-

* Mehr über die Autoren erfahren Sie auf S. XII. Alle zitierten Internetquellen wurden zuletzt abgerufen am 29. 10. 2021.

fenden Wertschöpfungsbeziehungen, die zunehmend an Bedeutung gewinnt.[1]

1. SCM und Digitalisierung

Die zunehmende Digitalisierung der Industrie hat auch auf Lieferketten Auswirkungen. Die Digitalisierung im SCM geht mit einer Steigerung der Effizienz immer komplexer werdender Lieferketten einher. Dabei beschreibt der Überbegriff Digitalisierung das Umwandeln analoger Werte in digitale Formate und ihre Verarbeitung oder Speicherung in einem digitaltechnischen System.[2] Die Digitalisierung ist Teil von Industrie 4.0 bzw. SCM 4.0 und wird in diesem Zusammenhang genutzt, um Prozesse wie die Beschaffung und Lieferantenauswahl zu automatisieren, transparenter zu gestalten und wettbewerbsfähig zu bleiben. Ziel ist zudem die Vernetzung sämtlicher Schritte der Wertschöpfungskette und damit die gesamte digitale Verknüpfung des Lebenszyklus eines Produkts, vom Auftrag über Entwicklung, Fertigung und Auslieferung zum Endkunden bis schließlich zum Recycling. Die Vernetzung globaler Märkte bringt jedoch auch Risiken im Bereich der Cybersicherheit, d. h. der Sicherheit von Information Technology (IT) und Operation Technology (OT).[3]

2. Cyberangriffe auf die Lieferkette

Für Cyberangriffe auf Lieferketten existiert bisher keine einheitliche Definition. Es kann jedoch grundlegend zwischen zwei Angriffsszenarien unterschieden werden. Bei Cyberangriffen auf die Lieferkette im weiteren Sinne wird ein Zulieferer Opfer eines Cyberangriffs, z. B. eines Verschlüsselungstrojaners (Ransomware). Dies kann einen Stillstand der Produktion des Zulieferers zur Folge haben oder auch auf anderen Ebenen der Zuliefererpyramide zu Störungen oder Ausfällen in der Produktion führen. Von derartigen Angriffen, die eher zufällig Auswirkungen auf die Lieferkette haben, sind die zielgerichteten Angriffe auf die Lieferkette abzugrenzen.[4] Sie zeichnen sich durch eine Kombination von mindestens zwei Angriffen auf unterschiedliche Akteure einer Lieferkette aus.[5] Befeuert werden diese Angriffe insbesondere dadurch, dass Original Equipment Manufacturer (OEM) und Zulieferer auf höheren Ebenen in zunehmendem Maße über ausgereifte Cybersicherheitsmaßnahmen verfügen, die unmittelbare Angriffe erschweren.[6] Die Besonderheit dieser Angriffsszenarien liegt darin, dass sich der Angriff in der Regel zunächst unmittelbar gegen einen Lieferanten des eigentlich anvisierten Unternehmens, z. B. einen OEM, richtet.[7] Durch dieses Vorgehen stehen den Angreifern neue Angriffsflächen zur Verfügung. Lieferanten, die in Bezug auf ihre Cybersicherheitsstandard unzureichend aufgestellt sind, können den Angreifern so alternative Zugangsmöglichkeiten zu Unternehmen mit ausgereiften Abwehrmechanismen eröffnen.[8] Technische Maßnahmen gegen Angriffe auf Lieferanten stellen für Hersteller oder höherrangige Zulieferer eine Herausforderung dar, denn einerseits muss eine Vielzahl von digitalen Schnittstellen in den Lieferketten abgesichert werden (u. a. Ressourcen (Hardware und Software), Speicher (Cloud oder lokal), Verteilungsmechanismen (Webanwendungen, Online-Shops) und Verwaltungssoftware),[9] andererseits bestehen in der Regel nur eingeschränkte Möglichkeiten zur technischen Einflussnahme auf Zulieferer bzw. deren Systeme. Cyberangriffe auf Lieferketten gehen mit vielseitigen Folgen einher. Diese reichen von Systemausfällen und Reputationsverlusten bis hin zu erheblichen finanziellen Einbußen.[10]

3. Bekannte Vorfälle in der Vergangenheit

Basierend auf den Analyseergebnissen der ENISA gab es im Zeitraum vom Januar 2020 bis Juli 2021 bereits 24 Supply-Chain-Angriffe. Die Hälfte der Angriffe wurde bekannten APT-Gruppen[11] zugeschrieben. Rund 62 % der Angriffe auf Kunden nutzten dabei das Vertrauen des Kunden in ihre Lieferanten aus. Darüber hinaus prognostiziert die ENISA für das Jahr 2021 eine Vervierfachung der Supply-Chain-Angriffe im Vergleich zum Vorjahr.

Der Angriff auf die Software des IT-Dienstleisters Kaseya verdeutlicht ebenfalls die Problematik. Er veranschaulicht den Domino-Effekt, der mit einem Angriff auf eine Lieferkette verbunden sein und mehrere Firmen lahmlegen kann. Trotz grundsätzlich ausreichender Maßnahmen zur Cybersicherheit konnten Unternehmensdaten aufgrund einer Schwachstelle in der Software des IT-Dienstleisters erlangt werden. Diese Vorfälle erinnern zudem an den Hacker-Angriff auf den IT-Anbieter SolarWinds.[12] Aufgrund der Breite der betroffenen Einrichtungen, darunter zahlreiche Regierungsorganisationen und große Unternehmen, gilt er als einer der größten bekannten Supply-Chain-Angriffe der letzten Jahre. Die Angreifer konnten sich Zugriff auf die IT-Verwaltungssoftware des Herstellers SolarWinds verschaffen und dadurch über einen Updateserver Schadsoftware an 18 000 Kunden ausliefern.[13] Ein weiteres Beispiel stellen die von der Sicherheitsfirma JSOF detektierten Sicherheitslücken im TCP/IP-Stack des Softwareunternehmens Treck, die unter der Bezeichnung „Ripple20“ zusammengefasst werden, dar.[14] Durch diese Sicherheitslücken könnten Hunderte von Millionen Geräte von Smart-Homes bis zu medizinischen Geräten, Industrieanlagen und sogar Flugzeuge betroffen sein.

Diese skizzierten Vorfälle unterstreichen die Notwendigkeit für politische Entscheidungsträger und für die Forschung und Entwicklung, im Bereich der Cybersicherheit neue Schutzmaßnahmen zu entwickeln und einzuführen, um potenzielle Angriffe auf Lieferketten in der Zukunft effektiv bekämpfen zu können und deren Auswirkungen zu

1 *Schulze*, Informationstechnologieeinsatz im Supply Chain Management, 2009, S. 1.
2 Vgl. *Bendel*, in: Gabler Wirtschaftslexikon, Stichwort: Digitalisierung, abrufbar unter: https://wirtschaftslexikon.gabler.de/definition/digitalisierung-54195.
3 ENISA, ENISA Threat Landscape for Supply Chain Attacks, July 2021, S. 27, abrufbar unter: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.
4 Hier lässt sich auch von Cyberangriffen auf die Lieferkette im engeren Sinne sprechen.
5 ENISA (Fn. 3), S. 6.
6 ENISA (Fn. 3), S. 30.
7 ENISA (Fn. 3), S. 6.
8 New Zealand Government – GCSB, Guide to Supply Chain Cyber Security, S. 6 ff., abrufbar unter: https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Supply-Chain-Cyber-Security.pdf.
9 ENISA (Fn. 3), S. 6.
10 ENISA (Fn. 3), S. 3.
11 Organisationen, die Angriffe auf die Informationsressourcen eines Landes von nationaler Sicherheit oder strategischer wirtschaftlicher Bedeutung entweder durch Cyberspionage oder Cybersabotage führen.
12 *Benrath*, Massiver Cyberangriff gefährdet deutsche Behörden, abrufbar unter: https://www.faz.net/aktuell/wirtschaft/digitec/solarwinds-hack-massiver-cyberangriff-gefaehrdet-deutsche-behoerden-17134477.html.
13 ENISA (Fn. 3), S. 15.
14 *Schmidt*, Ripple20 erschüttert das Internet der Dinge, abrufbar unter: https://www.heise.de/security/meldung/Ripple20-erschuettert-das-Internet-der-Dinge-4786249.html.

mindern.[15] Zur Vermeidung und Vorbeugung solcher Ereignisse werden im Folgenden technische Gegenmaßnahmen dargestellt. Anschließend sollen die Vollständigkeit und Effektivität der gesetzlichen Regelungen bewertet werden, um die Notwendigkeit und den Inhalt vertraglicher Lösungen zu erörtern.

II. Technische Gegenmaßnahmen

Geeignete Maßnahmen zur Cyberabwehr bedürfen zunächst eines grundlegenden Verständnisses bezüglich potenzieller Angriffe auf die Supply Chain. Die ENISA hat in diesem Zusammenhang einen systematischen Ansatz vorgestellt. In einem ersten Schritt differenziert die Behörde zwischen gegen Lieferanten gerichtete und gegen Kunden gerichtete Angriffstechniken.[16] Im Anschluss daran soll die konkrete Vorgehensweise analysiert werden, z. B., ob ein Brute-Force-Angriff vorliegt oder Passwörter über Social Engineering erlangt wurden.[17] Die Analyse der ENISA hebt hervor, dass 16 % der Angriffsmethoden durch das Ausschöpfen von Softwareschwachstellen wie bei SolarWinds und Kaseya entstanden sind.[18] Der größte Teil der Angriffsmethoden (66 %), Cyberattacken auf Lieferanten, wurde noch nicht aufgeklärt oder wurde von den Unternehmen nicht transparent gemacht.[19] Darüber hinaus haben 9 % der betroffenen Kunden keine Kenntnis darüber, wie sich der Angriff ereignet hat.[20]

1. Automatisierte Schwachstellenscans und Pentests

Bei automatisierten Schwachstellenscans und Penetrationstests werden durch eine Überprüfung auf bekannte Sicherheitslücken bzw. eine realitätsnahe Simulierung von Angriffen Schwachstellen ausfindig gemacht. Aus Pentests gewonnene Erkenntnisse können zur Lösung grundlegender Probleme, wie falsch konfigurierte Sicherheitseinstellungen, mangelhafte Zugriffskontrollmechanismen und sonstige Logikfehler, beitragen.[21] Der Sinn und Zweck eines Pentests ist die Inaugenscheinnahme bestehender Sicherheitsmaßnahmen sowie das Bestreben, diese erfolgreich zu umgehen.[22] Im Anschluss entwickelte Sicherheitsmaßnahmen werden sodann erneut auf die Probe gestellt. Ziel ist eine kontinuierliche Reduktion potenzieller Angriffsmöglichkeiten.[23] Insbesondere durch automatisierte Pentests können Hersteller auch zusätzliche Überwachungsmöglichkeiten hinsichtlich getroffener Sicherheitsmaßnahmen durch ihre Lieferanten erhalten.

2. Vendor-Assessment und Fragebogen

Im Rahmen des Vendor-Assessments werden regelmäßig Sicherheitsinformationen durch Risikobewertungsumfragen und Vor-Ort-Inspektionen (OSI – On-Site-Inspections) gesammelt. Diese werden gespeichert und ausgewertet, um schwerwiegende Cyberbedrohungen ausfindig zu machen.[24] Folglich kann dem Unternehmen geholfen werden, die Risiken zu analysieren, die mit der Verwendung des Produkts oder der Dienstleistung eines Lieferanten verbunden sind, oder Due-Diligence-Prozesse zu identifizieren, die für diesen bestimmten Drittanbieter am besten geeignet sind.[25] Das Risk-Assessment-Framework der Deutschen Cyber-Sicherheitsorganisation (DSCO) beispielsweise misst das Sicherheitsniveau im Rahmen der Zusammenarbeit mit externen Dienstleistern durch die Unterstützung der Risikobewertung bei (Cloud-)Sourcing-Vorhaben.[26] Die Optimierungsmöglichkeiten reichen von den Bereichen Sicherheitsmanagement über Datenschutz bis hin zur Sicherheitsarchitektur.

3. Abwehrmaßnahmen und Empfehlungen von der ENISA

Vor diesem Hintergrund fordert die ENISA weitere technische Maßnahmen, denn bei der Auswahl und Überprüfung der Lieferanten sowie beim Risikomanagement, das sich aus diesen Beziehungen ergibt, sollten Unternehmen erhöhte Sorgfalt walten lassen.[27] Insbesondere im Einklang mit den technischen Normen ISO 27002, ISO 9001 und ISO 31000 lassen sich entsprechende Maßnahmen etablieren und Strategien entwickeln.

Unternehmen sollten im Rahmen des Risikomanagements Arten von Lieferanten und Dienstleistern identifizieren und dokumentieren, um Risikokriterien zu bestimmen, wie wichtige Lieferantenabhängigkeiten, kritische Software-Abhängigkeiten und „Single Points of Failure". Zudem sollen laut der ENISA auch eigene Risiken der Lieferkette anhand von Folgenabschätzungen und Anforderungen zur Geschäftsfortführung im Krisenfall bewertet werden, um im selben Zuge auf bewährten Praktiken („Good Practices") basierende Maßnahmen zur Risikobehandlung zu bestimmen.[28] Auf der Grundlage der Ergebnisse aus der Leistungsprüfung und Bewertung der Lieferanten sowie interner und externer Informationsquellen zur Cybersicherheit sollten regelmäßig Risiken und Bedrohungen überwacht werden. Ferner können bereits existierende Notfallpläne[29] überarbeitet und angepasst werden. Auch unternehmensseitig sollten hinreichende Maßnahmen über den Produktlebenszyklus hinweg getroffen werden. Der Fokus liegt dabei auf den IT-Assets und Informationen, die mit den Lieferanten geteilt werden oder für diese verfügbar sind. Für eine geregelte Handhabung und einen kontrollierten Zugang zu den IT-Assets sollten geeignete Prozesse bestimmt werden. Es sind Verpflichtungen für Lieferanten zum Schutze des Informationsaustausches vonnöten sowie für Auditrechte, für die Geschäftsfortführung im Krisenfall, für das Personalscreening und den Umgang mit Vorfällen in Bezug auf Verantwortlichkeiten, Meldepflichten und weiteren Verfahren.[30] Ferner sollten Sicherheitsanforderungen an die erworbenen Produkte und Dienstleistungen gestellt werden. Sinnvoll sind in diesem Zusammenhang Rückmeldungen der Lieferanten hinsichtlich versteckter Features oder Hintertüren.

15 ENISA (Fn. 3), S. 4.
16 ENISA (Fn. 3), S. 6.
17 ENISA (Fn. 3), S. 45.
18 ENISA (Fn. 3), S. 23.
19 ENISA (Fn. 3), S. 25.
20 ENISA (Fn. 3), S. 25.
21 *Deusch/Eggendorfer*, K&R 2018, 223, 226.
22 BSI, IS-Penetrationstest und IS-Webcheck, abrufbar unter: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Sicherheitspruefungen/Pen_Test_und_IS_Webcheck/pent-tests-und-is-webcheck_node.html.
23 *Demand*, DSB 2014, 261, 261.
24 *Kelly/Gardener*, in: Real-Time Vendor Scanning Is Not Optional, CyberSecurity Magazine (Februar 2021), abrufbar unter: https://cybersecuritymagazine.com/real-time-vendor-scanning-is-not-optional/.
25 PwC, Viewpoint on Third Party Risk Management, 2013, S. 7, abrufbar unter: https://www.pwc.com/us/en/risk-assurance-services/assets/pwc-viewpoint-vendor-risk-management.pdf.
26 DCSO, Vendor Assessment, abrufbar unter: https://www.dcso.de/service/vendor-assessment/.
27 ENISA (Fn. 3), S. 27.
28 ENISA (Fn. 3), S. 28.
29 *Voigt*, IT-Sicherheitsrecht, 2018, Rn. 276.
30 ENISA (Fn. 3), S. 27.

Außerdem sollten die Anforderungen an die Lieferanten detailliert bestimmt sein. Für die regelmäßige Anpassung der Systeme und Infrastrukturen können hier Normen wie z. B. die IEC 62443 herangezogen werden, die speziell für den Cybersecurity-Bereich der Industrie-Infrastrukturen gedacht sind. Auch speziellere Standards, wie die CSA-Cloud-Controls-Matrix (CCM) für Cloud-Services können angewendet werden.

III. Regulatorische Rahmenbedingungen für SCM

Technische Maßnahmen sind in ihren Möglichkeiten zur Abwehr von Supply-Chain-Angriffen limitiert, sodass ergänzend auch rechtliche Maßnahmen zum Schutz heranzuziehen sind. Anforderungen an die Unternehmen im Bereich der Cybersicherheit ergeben sich insbesondere aus dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) und der Datenschutz-Grundverordnung (DSGVO). Zudem bestehen weitere branchenspezifische Regelungen, z. B. für das Finanz- und Bankwesen (Kreditwesengesetz, Wertpapierhandelsgesetz, Börsengesetz), Betreiber von Energieversorgungsnetzen (Energiewirtschaftsgesetz) oder Versicherungsunternehmen (Gesetz über die Beaufsichtigung der Versicherungsunternehmen). Darüber hinaus bestehen branchenübergreifende Anforderungen, wie unternehmerische Sorgfaltspflichten (Aktiengesetz, Gesetz betreffend die Gesellschaften mit beschränkter Haftung) und Pflichten zu Lageberichten und Abschlussprüfungen im Handelsgesetzbuch (HGB).[31]

Im Strafrecht schützt eine Reihe von Tatbeständen die Vertraulichkeit von Daten in IT-Systemen. Der Schutz der §§ 202a bis 202d Strafgesetzbuch (StGB) bezieht sich auf gespeicherte oder sich in der Übermittlung befindliche Daten, unabhängig von ihrem Inhalt, vor dem Zugriff Dritter.[32] Darüber hinaus werden Privatgeheimnisse sowie der höchstpersönliche Lebensbereich durch die §§ 201 bis 204 StGB geschützt. Aufgrund der Anonymität des Internets gestaltet sich eine strafrechtliche Verfolgung der Angreifer in der Praxis jedoch oftmals schwierig.[33]

Das Zivilrecht ist für eine vertrags- und haftungsrechtliche Durchsetzung des IT-Sicherheitsrechts insbesondere im Verhältnis zwischen Endkunden und Herstellern sowie Händlern, aber auch gegenüber Dritten grundsätzlich geeignet. Speziell im Gewährleistungsrecht können Sicherheitslücken einen Mangel im Einzelfall begründen.[34] Dies spiegelt sich auch in der Umsetzung der Digitalen-Inhalte-Richtlinie[35] sowie der Warenkauf-Richtlinie[36] im Bürgerlichen Gesetzbuch (BGB) wider. Aufgrund der von Sicherheitslücken ausgehenden abstrakten Risiken wird in der Praxis nur ein geringer Teil der materiellrechtlichen Ansprüche geltend gemacht.[37]

1. IT-Sicherheitsgesetz 2.0

Mit Blick auf die zunehmende Digitalisierung aller Lebensbereiche und die daraus folgende zunehmende Bedeutung der Cyber- und Informationssicherheit für Staat, Wirtschaft und Gesellschaft wurde das IT-Sicherheitsgesetz 2.0 beschlossen, das in überwiegenden Teilen ab dem 28. 5. 2021 in Kraft getreten ist und eine weitreichende Novellierung des BSIG vorsieht. Das BSIG findet auf Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber) Anwendung und erstreckt sich durch die Novellierung auch auf Unternehmen im besonderen öffentlichen Interesse (UNBÖFI).

Die neue Fassung des BSIG sieht im Rahmen der §§ 9a, 9b BSIG[38] die Pflicht vor, die gesamte Lieferkette abzusichern und adressiert nun auch Hersteller kritischer Komponenten. Gemäß § 2 Abs. 13 BSIG sind kritische Komponenten IT-Produkte, die in Kritischen Infrastrukturen eingesetzt werden, bei denen Störungen zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit Kritischer Infrastrukturen oder zu Gefährdungen für die öffentliche Sicherheit führen können oder die aufgrund eines Gesetzes als solche bestimmt werden bzw. eine als kritisch bestimmte Funktion realisieren. Gemäß § 9b Abs. 4 BSIG dürfen KRITIS-Betreiber kritische Komponenten ausschließlich von vertrauenswürdigen Herstellern beziehen. Die Verwendung ist gemäß § 9b Abs. 1 BSIG anzeigepflichtig. Erweist sich der Hersteller als nicht vertrauenswürdig, kann der weitere Einsatz der kritischen Komponente gemäß § 9b Abs. 3 BSIG untersagt werden. Der Hersteller von IT-Produkten für KRITIS-Sektoren steht nach § 9b Abs. 5 Nr. 3, 4 BSIG in der Pflicht, selbst an Sicherheitsüberprüfungen, wie z. B. Penetrationsanalysen, mitzuwirken und unterliegt einer Meldepflichtpflicht bei eingetretenen oder befürchteten Sicherheitsvorfällen.

Außerdem ist der Anzeige des KRITIS-Betreibers eine Herstellererklärung beizufügen. Der Hersteller ist nach § 9b Abs. 3 BSIG verpflichtet, gegenüber dem KRITIS-Betreiber eine Erklärung über seine Vertrauenswürdigkeit (Garantieerklärung) abzugeben, die sich über die gesamte Lieferkette erstreckt. Daraus soll hervorgehen, wie der Hersteller sicherstellt, dass die kritische Komponente nicht über technische Eigenschaften verfügt, die spezifisch geeignet sind, missbräuchlich, insbesondere zum Zwecke von Sabotage, Spionage oder Terrorismus auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können.

Des Weiteren ist im Hinblick auf § 9b BSIG zu berücksichtigen, dass kritische Komponenten nicht direkt vom Hersteller an die Betreiber verkauft werden, sondern im Rahmen einer Wertschöpfungskette, an Reseller, Systemhäuser und andere Unternehmen veräußert werden, die diese an Kritische Infrastrukturen weitergeben.[39] Eine Meldepflicht nach § 9b Abs. 5 BSIG erscheint vor diesem Hintergrund nicht effizient, da Lieferanten teilweise keine Kenntnis darüber haben, in welchen Infrastrukturen ihre Produkte eingesetzt werden. Folglich fehlt es bereits im KRITIS-Sektor an einer abschließenden Regelung, die Lieferketten vollständig berücksichtigt.

---

31 *Voigt* (Fn. 29), Rn. 35.
32 *Singelnstein/Zech*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 2021, § 20 Schutz der IT-Sicherheit durch das Strafrecht, Rn. 37.
33 *Voigt* (Fn. 29), Rn. 271 f.
34 *Rockstroh/Peschel*, NJW 2020, 3345, 3347.
35 Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. 5. 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen.
36 Richtlinie (EU) 2019/771 des Europäischen Parlaments und des Rates vom 20. 5. 2019 über bestimmte vertragsrechtliche Aspekte des Warenkaufs, zur Änderung der Verordnung (EU) 2017/2394 und der RL 2009/22/EG sowie zur Aufhebung der RL 1999/44/EG.
37 *Riehm/Meier*, MMR 2020, 571, 574.
38 Im Folgenden wird auf die Normen des BSIG nach Änderung durch das IT-SiG 2.0 Bezug genommen.
39 AG KRITS, Notbremse für den Entwurf! – Stellungnahme der AG KRITIS zum 3. Entwurfs des IT-SiG 2.0, S. 11 f., abrufbar unter: https://ag.kritis.info/2020/12/03/notbremse-fuer-den-entwurf-stellungnahme-der-ag-kritis-zum-3-entwurfs-des-it-sig-2-0/.

Vor dem Hintergrund der skizzierten gesetzlichen Regelungen kann daher davon ausgegangen werden, dass diese in ihrem Regelungsumfang den wünschenswerten Anforderungen entsprechen, sodass ergänzend einzelvertragliche Vereinbarungen zwischen den Vertragsparteien innerhalb der Lieferkette heranzuziehen sind.

2. Datenschutzrecht – „TOM" und Auftragsverarbeitung

Art. 32 DSGVO stellt Anforderungen an eine sichere Verarbeitung personenbezogener Daten. Nach Art. 32 Abs. 1 DSGVO treffen sowohl der Verantwortliche als auch der Auftragsverarbeiter im Rahmen ihrer Gewährleistungspflichten[40] geeignete technische und organisatorische Maßnahmen (kurz: „TOM"), um ein dem Risiko angemessenes Schutzniveau unter Berücksichtigung des Stands der Technik zu gewährleisten. Die TOM sollen die Schutzziele der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste garantieren.

Personenbezogene Daten sind jedoch in der Regel nicht Gegenstand von Supply-Chain-Angriffen. Dennoch können sich auch im Zusammenhang mit dem SCM datenschutzrechtliche Fragestellungen ergeben. Dies gilt z. B. im Zusammenhang mit virtuellen Werksbesichtigungen oder Schnittstellen in der Logistik, bei denen mit personenbezogenen Daten auf Servern und Systemen zur Distributions- und Transportplanung agiert wird. Darüber hinaus kann sich auch durch die Datenübermittlung in Drittstaaten außerhalb der Europäischen Union (EU) ein höheres Risiko für die Einhaltung eines hinreichenden Schutzniveaus ergeben, sodass sich für Hersteller und Lieferanten die Frage nach der Zulässigkeit von Drittlandsübermittlungen stellt.

IV. Notwendigkeit von vertraglichen Regelungen

Trotz der Vielzahl an gesetzlichen Regelungen und technischen Normen besteht das Bedürfnis einer vertraglichen Ausgestaltung der Cybersicherheit insbesondere im SCM, da bestehende gesetzliche Regelungen die Sicherheitsanforderungen innerhalb der Lieferkette bislang nur unzureichend abbilden können.[41] Dies gilt auch in Bezug auf datenschutzrechtliche Pflichten. Zwar regelt Art. 32 DSGVO branchenübergreifend die Verarbeitung personenbezogener Daten, jedoch werden reine Unternehmens- und maschinengenerierte Daten ohne Personenbezug, wie sie im Zusammenhang mit Lieferketten in der Regel vorliegen, nicht vom Anwendungsbereich erfasst.[42] Ferner enthält Art. 32 DSGVO keine generischen Anforderungen an die IT-Sicherheit, sondern legt Verantwortlichen und Auftragsverarbeitern auf, in Abhängigkeit des jeweils bestehenden Risikos für Rechte und Freiheiten der betroffenen Personen differenzierte Schutzmechanismen zu implementieren. Demnach lässt sich ein allgemeinverbindliches Anforderungsprofil im Kontext eines Cyberangriffs nur schwer ermitteln. Es bedarf daher eines einheitlichen und allgemeinverbindlichen Anforderungsprofils,[43] besonders in Bezug auf Lieferketten. Bei der Inanspruchnahme von IT-Diensten bietet es sich daher an, vertraglich strenge Vorgaben für Cybersicherheit vorzusehen. Dabei können zum einen gesetzliche regulatorische Anforderungen nach unten „durchgereicht" und Nachweisregelungen eingeführt werden. Der „Durchreichende" lässt sich dabei garantieren, dass die Verarbeitung bestimmten gesetzlichen Vorgaben zur Sicherheit entspricht. Eine Absicherung des Konstrukts kann durch vertragliche Haftungs- und Freistellungsregelungen erfolgen.[44] Daneben besteht die Möglichkeit, soweit die bestehenden regulatorischen Vorgaben nicht für ein Cybersicherheitsniveau ausreichen, den Vertragspartner originär durch den Vertrag zur Einhaltung bestimmter Maßnahmen zu verpflichten. Derartige vertragliche Vereinbarungen können auch Regelungen zur Kontrolle wie z. B. automatisierte Pentests enthalten. Zur Konkretisierung von Outsourcingverträgen werden in der Praxis oft technische Normen und Praxisleitfäden herangezogen. So kann sich ein Zulieferer z. B. gegenüber dem Unternehmen verpflichten, die Mindeststandards ISO/IEC 27001 bzw. die IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in ihrer jeweils geltenden Fassung einzuhalten oder eine entsprechende Zertifizierung durchzuführen.[45] Es bietet sich zudem eine vorgeschaltete Risikoanalyse an, bei der eine Risikoverteilung von regulatorischen und haftungsrechtlichen Pflichten sowie der Beweislage stattfindet.[46]

V. Fazit

Angesichts der aktuellen Bedrohungslage durch Cyberangriffe, die sich vermehrt gegen die Lieferkette richten, reicht es nicht mehr aus, sich hinsichtlich erforderlicher Cybersicherheitsmaßnahmen auf das eigene Unternehmen zu konzentrieren. Durch den steigenden einzelunternehmerischen Cybersicherheitsschutz findet eine Verlagerung der Angriffe auf die Lieferanten statt.[47] Dabei geht es auf technischer Ebene nicht nur um den reaktiven Schutz vor Angriffen, sondern er wird im Rahmen der „Industrie 4.0" um die Angriffserkennung erweitert. Ziel ist die Identifikation der Angreifer sowie die Analyse der zur Kompromittierung angewendeten Methoden und eingesetzten Tools. Diese sogenannte „Cyberintelligence" gewinnt daher neben klassischen IT-Sicherheitsmaßnahmen, wie der Verschlüsselung und dem Schutz vor „Malware", immer mehr an Bedeutung.[48] Cybersicherheitsanforderungen für Lieferketten werden gesetzlich nicht abschließend oder nur unzureichend geregelt und damit der steigenden Bedrohungslage nicht gerecht. Daher obliegt es Unternehmen, eigenständig ausreichende Sicherheitsmaßnahmen zu implementieren. Dabei ist es unerlässlich, vertragliche Regelungen zur Cybersicherheit innerhalb der Lieferkette zu vereinbaren. Zur Gewährleistung eines angemessenen Sicherheitsniveaus bedarf es darüber hinaus einer kontinuierlichen Anpassung und Weiterentwicklung der Schutzmechanismen und Abwehrstrategien.

40 *Martini*, in: Paal/Pauly, DSGVO BDSG, 3. Aufl. 2021, Art. 32 DSGVO, Rn. 1a.
41 *Rafsendjani/Bomhard*, in: Hornung/Schallbruch (Fn. 32), § 9 IT-Sicherheit im Zivilrecht und in der Vertragsgestaltung, Rn. 52.
42 *Rafsendjani/Bomhard*, in: Hornung/Schallbruch (Fn. 32), § 9 IT-Sicherheit im Zivilrecht und in der Vertragsgestaltung, Rn. 53.
43 *Rafsendjani/Bomhard*, in: Hornung/Schallbruch (Fn. 32), § 9 IT-Sicherheit im Zivilrecht und in der Vertragsgestaltung, Rn. 53.
44 *Rafsendjani/Bomhard*, in: Hornung/Schallbruch (Fn. 32), § 9 IT-Sicherheit im Zivilrecht und in der Vertragsgestaltung, Rn. 58 ff.
45 *Rafsendjani/Bomhard*, in: Hornung/Schallbruch (Fn. 32), § 9 IT-Sicherheit im Zivilrecht und in der Vertragsgestaltung, Rn. 53.
46 *Rafsendjani/Bomhard*, in: Hornung/Schallbruch (Fn. 32), § 9 IT-Sicherheit im Zivilrecht und in der Vertragsgestaltung, Rn. 120.
47 ENISA (Fn. 3), S. 6.
48 *Bensinger*, in: Schulz (Hrsg.) Compliance Management im Unternehmen, 2. Aufl. 2021, 13. Kap. Cybersecurity, IT-Sicherheit und Krisenmanagement, Rn. 17 ff.