www.betriebs-berater.de

BB

Betriebs Berater

46 | 2019

Steuern ... GeschGehG ... Unternehmenssteuerreform ... IFRS ... Vertrauensarbeitszeit ...

11.11.2019 | 74. Jg.
Seiten 2689–2752

BB-Rechtsprechungsreport Gemeinnützigkeits- und Spendenrecht 2019

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Anne Baranowski, LL.M., RAin/FAinIT-Recht, Suntka von Halen, und Dr. Udo Kornmeier, RA

Reputationsschutz durch Kommunikation und Recht

Angesichts der wachsenden Zahl von Angriffen auf die Reputation von Unternehmen sind Kommunikation und Recht Schlüsselressourcen in der Krisenvorbereitung und in der akuten Krise. Synchronisiert eingesetzt, sind sie entscheidende Faktoren für eine erfolgreiche Krisenreaktion und den umfassenden Schutz der Reputation des Unternehmens.

I. Einleitung

„Business of business is business". Die berühmte *Friedman*-These aus den 70er-Jahren gilt nicht mehr uneingeschränkt. In der Unternehmensführung spielen Reputation und Positionierung eine zunehmend wichtige Rolle: Haltung und Kultur des Unternehmens sowie eine integrierte Kommunikation über alle relevanten Kanäle beeinflussen die Wahrnehmung durch sämtliche Stakeholder – Kunden, Mitarbeiter, Aktionäre und Gesellschafter, Aufsichtsbehörden, Öffentlichkeit. Sie beeinflussen deren Bindung und Loyalität und sind damit entscheidend für den unternehmerischen Erfolg.

Ein kritischer Moment für die Reputation eines Unternehmens ist die Bewältigung einer relevanten Krisensituation. Im Scheinwerferlicht der Öffentlichkeit werden Ursache, Lösung, Kommunikation und Serviceorientierung in Echtzeit verfolgt. Eine professionelle Lösung des Problems, die Erfüllung von Informations- und Schutzpflichten und eine umfassende, zielgruppenorientierte Kommunikation tragen dazu bei, die Reputation des Unternehmens zu stärken. Mangelnde Vorbereitung dagegen führt fast zwangsläufig zu unkoordinierten Prozessen, Verfahrensfehlern, inkonsistenter Kommunikation und in der Folge zu erheblichen Reputations- oder gar Haftungsschäden.

Zum Schutz der Reputation stehen Vorständen und Geschäftsleitungen im Rahmen der unternehmerischen Ressourcen die Bereiche Kommunikation und Recht zur Verfügung. Wie integriert und reibungslos diese zusammenarbeiten, entscheidet in der Praxis über Erfolg oder Misserfolg der Krisenbewältigung.

Im Folgenden geht der Beitrag auf Angriffe auf die Reputation (II.) ein, auf die Verantwortung der Unternehmensleitung (III.), rechtliche und kommunikative Maßnahmen zur Krisenvorbereitung (IV.) sowie Krisenmanagement (V.). Vorteile eines synchronisierten Vorgehens von Kommunikation und Recht bilden den Abschluss (VI.).

II. Angriffe auf die Reputation von Unternehmen

Es vergeht kaum ein Tag, an dem die Medien nicht von neuen Cyberangriffen, Datenschutzverletzungen oder sonstigen reputationsschädigenden Ereignissen für ein Unternehmen berichten. Im Zuge unternehmerischer Aktivitäten begangene Rechtsverstöße werden von der Presse und in der Öffentlichkeit ausführlich und prominent gehandelt. Wird die Reputation eines Unternehmens durch Äußerungen angegriffen, wird häufig auch von der Verletzung des „Unternehmenspersönlichkeitsrechts" gesprochen.[1]

Die praktische Bedeutung der Reputation als Vermögensgegenstand eines Unternehmens kann kaum überschätzt werden. Nach einer Studie schätzen Führungskräfte den Anteil der Unternehmensreputation am Wert des eigenen Unternehmens auf durchschnittlich 60 %.[2] Bei Cyberangriffen und Datenschutzverstößen entstehen den Unternehmen nicht nur Umsatzeinbußen, Kosten für Ursachenfeststellung und Wiederherstellung der Betriebssysteme. Darüber hinaus kann der Wert des Unternehmens an sich beeinträchtigt werden.[3] Der Angriff auf Yahoo, bei dem Millionen von Nutzerdaten entwendet wurden, hatte z. B. zur Folge, dass sich der Kaufpreis für Yahoo beim Verkauf an Verizon im Jahr 2016 um 350 Mio. US-Dollar reduzierte.

Nach einer Studie stellen Cyberangriffe neben der Verletzung von Datenschutzbestimmungen für Unternehmen das Risiko mit dem größten Bedrohungspotenzial dar.[4] Die Schäden durch Cyberangriffe in den Jahren 2016 bis 2018 werden vom Branchenverband Bitkom in Deutschland auf 43,4 Mrd. Euro geschätzt.[5] Im ersten Halbjahr 2017 wurden 1,9 Mrd. Datensätze verloren, gestohlen oder auf andere Art kompromittiert.[6] Das Onlinenetzwerk MySpace wurde gehackt, dabei konnten 427 Mio. Passwörter erbeutet werden.[7] Die Financial Times berichtete über (angebliche) Gesetzesverstöße von Mitarbeitern des Zahlungsdienstleisters Wirecard in Singapur und löste damit einen Sturz der Wirecard-Aktie aus. Gegen die Online-Bank N26 wurde von der Berliner Aufsichtsbehörde eine Geldbuße von 50 000 Euro wegen Verstößen gegen die Datenschutz-Grundverordnung verhängt. Die Hotelgruppe Marriott verlor bei einem Cyberangriff Datensätze von über 350 Mio. Hotelgästen und musste ein Bußgeld von über 100 Mio. Euro wegen Datenschutzverletzungen akzeptieren.

Nach dem aktuellen Jahresbericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) hat das BSI innerhalb eines Jahres rund 114 Mio. neue Schadprogramm-Varianten und bis zu 110 000 Bot-Infektionen täglich in deutschen Systemen registriert. Die Gesamtzahl der Schadprogramme ist innerhalb dieses Zeitraums auf mehr als 900 Mio. gestiegen. Insgesamt war im Jahr 2018 jeder dritte an der Cyber-Security-Umfrage des BSI teilnehmende Betrieb (33 %) von Cyber-Sicherheitsvorfällen betroffen. Rund 87 % der von Cyber-

1 Vgl. BGH, 3.2.2009 – VI ZR 36/07, NJW 2009, 1872.
2 Ergebnis der Studie „The Company behind the Brand: In Reputation we trust" der PR-Beratungsgesellschaft Weber Shandwick, 2012, 18, http://www.webershandwick.com/uploads/news/files/InRepWeTrust_ExecutiveSummary.pdf (Abruf: 21.10.2019).
3 S. hierzu auch *Seibt*, BB 2019, 2563, 2564; *Schmidt-Versteyl*, NJW 2019, 1637.
4 „Crisis Management" der Kanzlei Noerr und des Center for Corporate Compliance der EBS Law School, 2018, abrufbar unter http://www.ebs-compliance.de/index.php/center-COMP/aktuelle-nachrichten/aktuelles/articles/studie-crisis-management-2018.html (Abruf: 14.5.2019); *Klöhn/Schmolke*, NZG 2015, 689.
5 *Schmidt-Versteyl*, NJW 2019, 1637, Studie 2018 des Bitcom e. V.
6 *Heeg*, FAZ-ePaper vom 21.9.2017, Teure Datenlecks, Wirtschaft..
7 http://www.computerbild.de/artikel/cb-News-Internet-MySpace-Hacker-Angriff-15689389.html (Abruf: 15.6.2016).

Sicherheitsvorfällen Betroffenen gaben an, dass es in der Folge zu Betriebsstörungen oder -ausfällen kam.[8]

Die Reputation eines Unternehmers kann von außen angegriffen oder durch interne Verstöße von Mitarbeitern geschädigt werden. Externe Angriffe richten sich gegen das Unternehmen an sich, dessen Geschäftsleitung und/oder dessen Produkte. In der Regel sind dabei vor allem IT-Systeme, die Verfügbarkeit, Vertraulichkeit und Integrität von Daten, Geschäftsgeheimnisse und Know-how, geistiges Eigentum, wie z. B. Software, Datenbanken, urheberrechtlich geschützte Werke, Marken, Persönlichkeitsrechte, und der Ruf des Unternehmens an sich betroffen.

Bei internen Verstößen handelt es sich in der Regel um Compliance-Verstöße, z. B. irreführende oder diskriminierende Werbung, Fehlinformationen des Kapitalmarktes, Datenschutzpannen, Mängel der IT-Sicherheit und um eine mangelhafte Organisationsstruktur zum Unternehmensschutz. In manchen Fällen erfolgen interne Verstöße mit Vorsatz: Mitarbeiter, die vor der Entlassung stehen oder mit unternehmerischen Entscheidungen nicht einverstanden sind, stellen sich nicht selten als Urheber von Verstößen heraus. Diese Fälle haben aufgrund des Zugangs zu detaillierten Informationen oft erhebliche Reputationsschäden zur Folge.

Reputationsschäden können durch Krisen in allen Unternehmensbereichen und auf allen Ebenen entstehen.

Mit dem Schadensausmaß einer Krise wächst auch das Risiko für die Unternehmensreputation, denn signifikante Schäden entstehen überwiegend aus mangelnder Umsicht oder durch die Unfähigkeit eines Unternehmens, seine Vermögenswerte zu schützen. Reputationsschäden können in der Folge erhebliche Auswirkungen auf das Management eines Unternehmens haben. In vielen Fällen müssen im Zusammenhang von relevanten Krisenereignissen Top-Führungskräfte die Verantwortung übernehmen und zurücktreten. Gründe hierfür sind oft gleichermaßen die Verantwortung dafür, dass die Krise überhaupt aufgetreten ist, wie auch ein mangelhaftes Krisenmanagement. Prominentes Beispiel ist Equifax, die infolge eines massiven Datenlecks CEO, CIO und CSO verloren. In Unternehmen, deren Geschäftsmodelle auf hoher Vertraulichkeit basieren wie Kanzleien, Beratungen oder auch medizinischen Institutionen, ist eine Exponierung der Daten von Mandanten ein besonders gravierendes Reputationsrisiko.

Über potenzielle Vermögensschäden und organisatorische Auswirkungen hinaus ist die wichtigste Dimension von Reputation wohl ihre Auswirkung auf die Zukunft. Die Reputation eines Unternehmens beeinflusst die Kaufentscheidung von Kunden, den Zugang zu Kooperationspartnern und politischen Entscheidern, die Bindung von Leistungsträgern und den Kampf um Talente.

Wie die Öffentlichkeit als eine der verschiedenen Zielgruppen auf das Unternehmen schaut, schlägt insbesondere bei B2C-Unternehmen direkt auf die Geschäftsentwicklung durch. Im Durchschnitt dauert es bis zu zwölf Monate, bis sich ein Unternehmen von einem relevanten Imageschaden erholt hat. In dieser Zeit belasten verminderte Umsätze, erhöhte Marketingaufwendungen und weitere Opportunitätskosten Ressourcen und Ergebnis.

An dieser Stelle soll noch einmal die hohe Bedeutung des Umgangs mit einer Krise für die Unternehmensreputation unterstrichen werden. Laut PR-Trendmonitor sind 63 % der Befragten der Überzeugung, dass der Versuch, Probleme zu vertuschen, am häufigsten der Auslöser von Unternehmenskrisen ist.[9]

III. Schutz der Reputation ist Chefsache

In dem Umfang, in dem die Reputation Haftungs- und Ergebnisrisiken birgt und Auswirkungen auf die Perspektive der Geschäftsentwicklung hat, liegt ihr Schutz in der Verantwortung der Unternehmensleitung.[10]

Es ist die originäre Aufgabe und Verantwortung der Unternehmensleitung, die von ihr verantworteten unternehmerischen Aktivitäten in einer Art und Weise zu organisieren und zu überwachen, dass Dritte nicht in ihren Rechten verletzt werden, dass gesetzliche Vorschriften eingehalten werden und Dritte das Unternehmen nicht in seinen Rechten beeinträchtigen können. Die rechtliche Grundlage der Compliance-Pflichten liegt in den Bestimmungen des Ordnungswidrigkeitsrechts zur Haftung des Aufsichtspflichtigen und zur Haftung des Unternehmens selbst im Fall eines zurechenbaren Fehlverhaltens seiner Aufsichtspflichtigen (§§ 130, 9, 30 OWiG). Die Ordnungswidrigkeit der Aufsichtspflichtigen kann mit einer Geldbuße bis zu einer Millionen Euro geahndet werden (§ 130 Abs. 3 OWiG). Die maximale Höhe einer Geldbuße des Unternehmens beträgt im Fall einer vorsätzlichen zurechenbaren Pflichtverletzung zehn Millionen Euro (§ 30 OWiG).

Neben der bußgeldrechtlichen Haftung droht den Mitgliedern der Unternehmensleitung auch eine zivilrechtliche Inanspruchnahme, sofern in Folge eines Verstoßes gegen die ihnen obliegende Aufsichtspflicht ein Vermögensschaden beim Unternehmen eingetreten ist. Ausreichend ist insoweit bereits ein leicht fahrlässig begangener Pflichtverstoß (§ 93 Abs. 2 AktG, § 43 Abs. 2 GmbHG).

Neben der allgemeinen Sorgfaltspflicht ergibt sich der Pflichtenmaßstab für die Geschäftsführung teilweise aus Spezialnormen, z. B. die Verpflichtung im Datenschutz und der IT-Sicherheit zu angemessenen technischen und organisatorischen Maßnahmen (Art. 32 DSGVO, § 8a BSIG), und im Bankensektor zu einem angemessenes Notfallkonzept für IT-Systeme (§ 25a Abs. 1 Nr. 5 KWG, BAIT, MaRisk II). Soweit dem Leitungsorgan ein Verstoß des Unternehmens gegen diese Spezialnormen aufgrund von Organisations- oder Delegationsverschulden zuzurechnen ist, stellt dies ohne Weiteres eine Pflichtverletzung dar.

Es ist die Pflicht der Unternehmensleitung, die für die Tätigkeit des Unternehmens erforderlichen Maßnahmen festzulegen. Auf Grundlage der Rechtsprechung hat sich ein Mindeststandard mit drei Kardinalpflichten entwickelt.[11]

- Prävention/Organisationspflicht: Vornahme geeigneter organisatorischer Maßnahmen in der Prävention zur Verhinderung von Fehlverhalten.
- Kontrollpflicht: Regelmäßige Kontrollen, um den Mitarbeitern vor Augen zu führen, dass die Aufsicht von der Unternehmensleistung ernst genommen wird.
- Untersuchungspflicht: Nachverfolgung von substantiierten Hinweisen auf Fehlverhalten.

8 Die Lage der IT-Sicherheit in Deutschland 2019, BSI, 10/19, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf?__blob=publicationFile&v=6 (Abruf: 24.10.2019).

9 Quelle: PR-Trendmonitor von news aktuell und Faktenkontor, Befragung von 510 Fach- und Führungskräften der PR im März 2019.

10 Zum Rechtsrahmen für Geschäftsleiterhandeln im Rahmen des Krisenmanagements ausführlich *Seibt*, BB 2019, 2563 ff.

11 *Moosmayer*, Compliance, 3. Aufl. 2015, A. Einleitung, Rn. 2 f.

Die auch dem Reputationsschutz dienende Compliance-Organisation wird jedoch nur dann erfolgreich sein, wenn die Unternehmensleitung Compliance als eigene Verantwortung annimmt, sie zur „Chefsache" erklärt, dies im Unternehmen entsprechend kommuniziert[12] und hierbei Kommunikation und Recht bei der Vorbereitung und Krisenbewältigung zusammenwirken.

Neben den rechtlichen Pflichten zum Schutz der Reputation muss sich die Unternehmensleitung grundsätzlich darüber im Klaren sein, wie sehr ihre Kommunikation den Erfolg des Unternehmens im Krisenfall beeinflusst. Bei der Entscheidung, zu welchem Zeitpunkt die Unternehmensleitung an die Öffentlichkeit tritt, spielt die Erwartungshaltung der Unternehmenszielgruppen eine wichtige Rolle.

In B2C-Unternehmen wird die Erwartungshaltung von Kunden und Öffentlichkeit oft unterschätzt. Diese sind an Echtzeit- und Multichannel-Kommunikation gewöhnt. Darüber hinaus hat die allgegenwärtige Markeninszenierung von B2C-Unternehmen auch den Anspruch von Kunden an Präsenz und Dialogbereitschaft in einer Krisenphase verändert.

In B2B-Unternehmen liegt die Parallele in der Anspruchshaltung der Key Stakeholder, die dem Management mit steigenden Anforderungen an Service- und Management-Attention gegenübertreten.

Der vermeintlich weiche Faktor von öffentlichen bzw. Key Stakeholder-Erwartungen an die Kommunikation der Unternehmensleitung muss im Rahmen einer Krisenreaktion mit Blick auf Reputationsschutz in jedem Fall angemessen berücksichtigt werden.

Aus rechtlichen wie kommunikativen Gründen muss die Unternehmensleitung den Reputationsschutz also zur Chefsache erklären.

IV. Vorbereitung auf den Krisenfall

Im Folgenden werden die kommunikativen und rechtlichen Maßnahmen zur Vorbereitung auf Krisenfälle dargestellt und anhand von Beispielen erläutert. Naturgemäß gibt es in jedem Unternehmen eine Vielzahl spezifischer Risiken. Die Krisenvorbereitung bildet die Basis der Krisenreaktion; jeder akute Krisenfall erfordert aber darüber hinaus die Flexibilität der Beteiligten, um die Situation im jeweiligen Kontext bestmöglich zu lösen.

1. Vorbereitung Krisenkommunikation

Mit integrierter Kommunikation relevanter Themen für Unternehmens- und Produktmarken über klassische Kanäle sowie online und soziale Medien transportiert ein Unternehmen seine Geschichten, Haltung und Kultur und erschafft sich über einen längeren Zeitraum einen Reputational Track Record, eine Reputationsbilanz. Auch herausragende Persönlichkeiten prägen diesen Track Record. Kluge Positionierung der Köpfe und gutes Storytelling formen und untermauern die Reputation, und sie unterstützen die Glaubwürdigkeit in einer Krise.

Darüber hinaus sind eine gute Vorbereitung und kontinuierliches Training der Krisenkommunikationsprozesse die Grundlage für erfolgreiche Krisenkommunikation. Je näher die Vorbereitung dem tatsächlichen Krisenfall kommt, umso wirksamer ist sie. Daher müssen am Krisenkommunikationstraining diejenigen Funktionen im Unternehmen beteiligt sein, die auch im Fall einer Krise zusammenarbeiten.

Die Erfahrung zeigt, dass Teams, die auf diese Weise gemeinsam trainieren, im Krisenfall strukturiert und zügig in den Aktionsmodus umschalten. Bei unvorbereiteten Teams geht in den ersten 24 Stunden oft viel Zeit mit der Klärung von Zuständigkeiten und Kommunikationsinfrastruktur verloren. Außerdem passieren in dieser Phase häufig zwei Fehler, die die Reputation nachhaltig schädigen: Die initiale Kommunikation kommt zu spät, und es werden Informationen veröffentlicht, die im Nachhinein korrigiert werden müssen, weil genauere Untersuchungen neue Erkenntnisse bringen.

a) Integration der Unternehmenskommunikation in unternehmensweite Krisenreaktionspläne

Die Erfahrung aus der Krisenvorbereitung zeigt, dass viele Unternehmen zwar ihre Business Continuity-Pläne an wachsende und veränderte Risikoszenarien anpassen, aber die Ressource Kommunikation oft nicht mitberücksichtigt wird.

Dabei löst beispielsweise eine Cyberattacke einen anderen Kommunikationsprozess aus als ein Brand in einem Werk (räumlich begrenzt) oder ein produktbezogener Zwischenfall. In der Krisenvorbereitung müssen Kommunikationsprozesse fester Bestandteil des übergreifenden Krisenreaktionsplans des Unternehmens sein. Nur so kann die Kommunikationsstrategie rechtzeitig festgelegt und das Medien- und Social Media-Monitoring eingerichtet werden, damit das Unternehmen nicht „blind" durch die Krise steuert. Auch erste Stellungnahmen (Holding Statements) und Argumentationslinien für externe und interne Kommunikation müssen rechtzeitig aufgestellt und die Unternehmensleitung auf ihre eventuelle Sprecherrolle vorbereitet werden. Die Unternehmenskommunikation ist eine der Ressourcen, die an vorderster Stelle dazu beiträgt, Reputationsschäden für das Unternehmen zu vermeiden und das Vertrauen der Zielgruppen zu bewahren.

b) Grundlage der Krisenvorbereitung: Der Kommunikationsprozess

Ziel der Krisenvorbereitung ist es, einen Krisenkommunikationsprozess aufzusetzen und zu trainieren, der im Krisenfall die Reaktion des Unternehmens steuert. Üblicherweise sind folgende drei Phasen der Krisenreaktion von Unternehmen vorzubereiten: Zu Beginn steht die Einschätzung des Krisenlevels. In der zweiten Phase des Kommunikationsprozesses wird die Krisenkommunikation vorbereitet, in Phase 3 umgesetzt.

Bei der Neuentwicklung oder Überarbeitung eines Kommunikationsprozesses ist vorab das Risikoassessment kritisch, das Unternehmensrisiken hinsichtlich der jeweiligen Reputationsauswirkung untersucht. Aufbauend auf diesem Assessment werden u. a. Eskalationskriterien festgelegt, die darüber entscheiden, welche Teams und Funktionen intern und extern benötigt und alarmiert werden. Eine zu frühe Eskalation bindet unnötig unternehmensweite Ressourcen, eine zu späte Eskalation ist ein erhebliches Reputationsrisiko.

Im Bereich von Cyberangriffen zeigt die Erfahrung, dass zu oft zu viel Zeit verloren geht, weil ein Angriff allein in der IT bearbeitet wird. Eine Cyberattacke ist nicht „ein IT-Problem". Wie oben beschrieben, ist sie wie fast jede relevante Krise des Unternehmens Beleg dafür, dass sensible Daten, Produktionsprozesse oder Vermögenswerte nicht ausreichend geschützt wurden. Daher muss abgewogen werden, ob und zu welchem Zeitpunkt ein Vorfall eskaliert wird, zu-

12 *Moosmayer*, Compliance, 3. Aufl. 2015, A. Einleitung, Rn. 6.

sätzliche Ressourcen hinzugerufen werden und unter Umständen das Engagement der Unternehmensleitung in der Kommunikation geboten ist.
Bei dieser Abwägung unterstützt das Risikoassessment, denn es bildet die Grundlage für die Kategorisierung von Vorfällen, die anschließend in den Krisenkommunikationsprozess einfließt.

aa) Phase 1: Wann ist eine Krise eine Krise? Zuordnung von Vorfällen zu Krisenleveln

Die verschiedenen Risiken eines Unternehmens werden in einem Levelsystem kategorisiert, denen je nach Krisenausmaß entsprechende Kommunikationsprozesse zuordnet werden. Üblicherweise werden die Level nach Umfang der Auswirkung auf Kunden, nach wirtschaftlichem Schaden und nach den unternehmensweit zur Lösung benötigten Ressourcen unterschieden.
Cybervorfälle beispielsweise können in den seltensten Fällen lokal isoliert gelöst werden.
Durch die digitale Vernetzung und länderübergreifende Kommunikation der Systemlandschaft eines Unternehmens wird üblicherweise ein länderübergreifendes Krisenteam mit internationaler Koordination aktiv, so dass diese Art von Vorfällen in den meisten Fällen auf mittlerem Krisenlevel eingeordnet wird.
Ist bei einem Vorfall die Sicherheit von Mitarbeitern und Öffentlichkeit betroffen, gehört der Vorfall automatisch in das höchste Krisenlevel.

bb) Phase 2: Die Umsetzungsplanung

Das Krisenteam
In effizienten Krisenteams sind alle relevanten Unternehmensfunktionen und -hierarchien vertreten, z. B. Vertreter der Geschäftsbereiche, IT, Recht, Kommunikation, HR, Compliance, Security, Top-Management. Sie sorgen dafür, dass alle unternehmensweit relevanten Parameter in der Krisenreaktion berücksichtigt werden und organisieren den Informationsfluss und die notwendige Unterstützung aus den Bereichen.
Das Krisenteam trifft Entscheidungen mit unter Umständen weitreichenden strategischen und operativen Konsequenzen; denn alles Handeln hat neben den Auswirkungen auf das Geschäft auch Auswirkungen auf die Kommunikation und Reputation des Unternehmens.
Im Krisenteam erfolgt u. a. die enge Abstimmung von Kommunikationsstrategie und Kernaussagen mit der Rechtsabteilung. Eine gute Zusammenarbeit stellt sicher, dass die Kommunikation des Unternehmens rechtlich zutreffend ist und nicht mit unzutreffenden Aussagen zusätzliche Problemfelder schafft. Gleichzeitig werden die rechtlichen Rahmenbedingungen und Maßnahmen für die Zielgruppen des Unternehmens nachvollziehbar erklärt.
Dieser Punkt ist nicht zu unterschätzen. Die rechtlichen Maßnahmen zur Bewältigung einer Krisensituation stützen sich naturgemäß auf eine umfangreiche Rechtsprechung, und Folgeprozesse beanspruchen in den meisten Fällen einen längeren Zeitraum bis zur letztendlichen Entscheidung über Haftung des Unternehmens oder Ansprüche gegen Dritte. Die Kommunikation dagegen muss in kurzer Zeit in für die Zielgruppen nachvollziehbaren Worten einen aggregierten Überblick über die jeweilige Situation und die Maßnahmen des Unternehmens geben. Die Erfahrung zeigt, dass die Unternehmenskommunikation in Krisensituationen eine wichtige Rolle als Erklärer, in der Zusammenarbeit mit einer kritischen Öffentlichkeit manchmal schon als Mediator zwischen Unternehmen und Zielgruppen wahrnehmen muss. Um diese Rolle im Sinne des Unternehmens bestmöglich erfüllen zu können, ist eine schnelle und flexible Abstimmung zwischen Rechtsabteilung und Kommunikation entscheidend.

Unternehmensleitung: Gesicht des Unternehmens in der Krise
Zur Krisenvorbereitung gehört wie oben beschrieben, auch die Entscheidung, ab wann die Unternehmensleitung persönlich auftritt. In der Krisenkategorisierung ist definiert, in welchen Situationen auf die höchste Ebene eskaliert wird, dennoch können veränderte Rahmenfaktoren jederzeit erfordern, dass das Topmanagement das Unternehmen nach außen vertritt. In einem solchen Moment entscheidet die Sichtbarkeit des CEO's oder vergleichbarer Unternehmensvertreter mit darüber, wie erfolgreich der Reputationsschaden begrenzt werden kann.
Teil der Krisenvorbereitung ist das Training dafür. Interview- und Kameratraining, aber auch der Umgang mit persönlichen Angriffen oder schwierigen Situationen sind Voraussetzungen für erfolgreiche Krisenkommunikation. Nicht jeder reagiert automatisch so gelassen auf Tomatenwürfe wie *Angela Merkel* bei einem Wahlkampfauftritt in Heidelberg im Jahre 2017.[13]

cc) Phase 3: Die Implementierung

Projektmanagement Krisenkommunikation
Die Vorbereitung von Kriseninfrastruktur und Kommunikationsmaterialien sind zentrale Bestandteile der Krisenvorbereitung. Zur Infrastruktur gehören beispielsweise Kommunikationsroutinen für Updates, Kommunikationsprotokolle für digitale Kommunikation wie E-Mail- oder Messengerverkehr, Vertraulichkeitsstufen, Kontaktlisten und Datenräume. Ebenso sind Sprecherregelungen wichtig, dazugehörige Vertretungen, Rotationen und Standby. Bei internationalen Krisenteams werden diese nach Zeitzonen festgelegt.

Kanäle
Im B2C-Bereich erwarten Kunden von Unternehmen eine über alle Kommunikationskanäle integrierte und dialogorientierte Kommunikation. Dementsprechend muss die Krisenkommunikation über Print-, digitale und persönliche Formate koordiniert werden. Wichtig ist, dass sämtliche Kontaktpunkte des Unternehmens im Krisenfall informiert werden und eine erste Stellungnahme und gegebenenfalls Argumentationslinien bekommen. Insbesondere auf die Social Media-Teams, Key Account-Manager sowie Call Center und Empfangsmitarbeiter kommt es dabei an, denn dort treffen externe Anfragen oder auch unangemeldete Journalisten – unter Umständen direkt mit Kamerabegleitung – als erstes ein. Im Bereich Social Media ist in der internen Kommunikation der Hinweis auf Social Media-Guidelines des Unternehmens ein ebenso wichtiger wie sensibler Punkt.

Krisenhandbuch
Alle diese Themen sollten mit dazugehörigen Action Lists, detaillierter Beschreibung der notwendigen Schritte und Verantwortlichkeiten im Krisenhandbuch Kommunikation eines jeden Unternehmens vorab definiert und festgelegt sein. Das Krisenhandbuch sollte für alle Mitarbeiter zugänglich sein, in Print, im Intranet oder – falls vorhanden – unternehmensinternen Krisen-Apps.

13 https://www.faz.net/aktuell/politik/bundestagswahl/angela-merkel-bei-wahlkampfauftritt-mit-tomaten-beworfen-15185352.html (Abruf: 24.10.2019).

c) Awareness und kontinuierliches Training

Jede Krisenvorbereitung ist wenig wirksam ohne Awareness und kontinuierliches Training. Insbesondere wenn das Unternehmen eine längere Phase ohne relevante Krisen durchlebt hat, ist die Versuchung groß, sich zurückzulehnen. „Permanent alert", d.h. regelmäßiges Awareness- und Krisentraining, ist daher wichtig. Im Bereich Awareness setzen erfolgreiche Unternehmen auf Kreativität und halten Risiken mit spielerischen Kampagnen, Videos und Spielen im Bewusstsein der Mitarbeiter.

2. Krisenvorbereitung aus rechtlicher Sicht

Angesichts der mannigfachen Angriffsmöglichkeiten auf ein Unternehmen, muss die Geschäftsleitung in Abhängigkeit von Art, Größe und Organisation des Unternehmens, eine auf Schadensprävention und Risikokontrolle angelegte Compliance-Organisation einrichten,[14] insbesondere auch um eine persönliche Haftung oder eine Haftung des Unternehmers nach §§ 130, 9, 30 OWiG zu vermeiden.

Zunächst bedarf es einer Analyse der zu schützenden Unternehmensgegenstände und deren Bedrohungen. Im Fall der IT-Sicherheit ist z.B. zu klären, wo die Daten des Unternehmens und seiner Vertragspartner sind, wer Zugang dazu hat, welcher Sicherheitsstandard als „Stand der Technik" gilt, welche Daten verarbeitet werden und wie lange. Sodann ist ein Maßnahmenkatalog aufzustellen, der das individuelle Unternehmensrisiko, Opfer eines Cyberangriffs zu werden, minimiert. Dieser Maßnahmenkatalog umfasst z.B. Schulungen, Virenschutz, Kontrollmechanismen und einen Notfallplan.

Als Standard des präventiven Risikomanagements gehört das Aufsetzen eines Handlungsplans mit Anweisungen zur Informationskette, der eindeutigen Zuordnung von Verantwortlichkeiten und Entscheidungsbefugnissen, eines Prozesses zur Beweissicherung, Einbindung von Behörden (z.B. Staatsanwaltschaft oder Landesmedienaufsicht) sowie der Sicherung der Vermögenswerte.

Darüber hinaus hat die Geschäftsleitung geeignete Maßnahmen für ein Monitoring-System zu ergreifen, um die Umsetzung und Einhaltung der eingeleiteten Maßnahmen zur Risikoanalyse zu kontrollieren (§ 91 Abs. 2 AktG). Die Nichterfüllung dieser Anforderung kann zur Anfechtung der Entlastungsbeschlüsse gegenüber den Organen des Unternehmens führen.[15] So sind z.B. Maßnahmen zum Schutz des Know-hows, der Verfügbarkeit der IT-Systeme und Sicherstellung der Business Continuity erforderlich. Des Weiteren soll eine Vertrauenskultur im Unternehmen geschaffen werden, die es Mitarbeitern ermöglicht, auf Missstände, Fehler, Angriffe und Risiken hinzuweisen.[16]

Zudem sind Analyse- und Überwachungsmaßnahmen umfassend zu dokumentieren. Nach einer Entscheidung des Landgerichts München I stellt eine fehlende Dokumentation des Risikomanagements einen wesentlichen Gesetzesverstoß dar.[17]

Bei der Einschätzung der erforderlichen Maßnahmen ist insbesondere die Gefährdungslage des Unternehmens zu berücksichtigen. Je abhängiger ein Unternehmen z.B. von seinen IT-Systemen ist, desto größer ist die Gefährdungslage.[18] Die bloße Einrichtung von IT-Schutzmechanismen alleine genügt nicht. Vielmehr zählt auch die regelmäßige Überprüfung der Gefährdungslage und der zur Wahrung der IT-Sicherheit erforderlichen Maßnahmen zum Pflichtenkreis der Geschäftsleiter.[19] Eine Pflichtverletzung liegt regelmäßig nahe, wenn elementare Sicherheitsstandards nicht befolgt werden, die nach dem Stand der Technik und der gängigen Unternehmenspraxis zu erwarten gewesen wären. Hierzu gehören Maßnahmen zur Datensicherung, Archivierung, Virenschutz und Notfallvorsorge.[20]

Präventiv für den Fall einer Verletzung, z.B. des Datenschutzes oder von IT-Sicherheitsanforderungen, ist auch ein Prozess für gesetzliche Informationspflichten (z.B. Art. 33 DSGVO, § 23 WpHG, § 131 Abs. 3 AktG) vorzusehen. Dafür sind Mitarbeiter durch Schulungen hinsichtlich solcher Verstöße zu sensibilisieren. Zudem sind verbindlich Ansprechpartner, Verantwortliche, Entscheidungsbefugnisse und die Informationskette festzulegen. Dieser Prozess muss klar und eingeübt sein, um beispielsweise die 72-stündige Meldefrist gegenüber der Datenschutzaufsichtsbehörde einhalten zu können (vgl. Art. 33 DSGVO). Neben den gesetzlichen Informationspflichten sind auch vertragliche Informationspflichten zu beachten. Diese können sich z.B. aus Vertraulichkeitsvereinbarungen, Joint-Venture-, Lizenz- und Projektverträgen ergeben.

Aus rechtlicher Sicht empfehlen sich somit folgende präventive Maßnahmen:

- Entwicklung eines Schutzkonzepts,
- Einführung eines Organisationshandbuchs,
- Richtlinien zu Compliance, IT-Sicherheit und Datenschutzmanagement,
- Schutzkonzept für Geschäftsgeheimnisse und Know-how,
- Anordnung interner Kontrollen,
- Einrichtung eines Notfallplans,
- Prozess zur Beweissicherung,
- Einbindung von Behörden,
- Einrichtung von technischen Schutzvorkehrungen sowie

die Sensibilisierung der Mitarbeiter hinsichtlich der Risiken, z.B. durch regelmäßige Schulungen, Anweisung zur Informationskette und eindeutige Zuordnung von Verantwortlichkeiten und Entscheidungsbefugnissen.

Rechtliche Maßnahmen, wie z.B. das Compliance Programm, sollten in operative Geschäftsprozesse integriert werden. Für eine effektive Umsetzung reicht es nicht, dass die Unternehmensleitung die Compliance-Maßnahmen den Mitarbeitern bekannt gibt. Es bedarf also einer kommunikativen Maßnahme, um diese rechtlichen Vorgaben umsetzen, im Unternehmen bekannt zu machen und einzuüben, sodass im Ernstfall ein informiertes und strukturiertes Agieren „auf Knopfdruck" der Mitarbeiter und der Unternehmensleitung möglich ist.

V. Maßnahmen im Krisenfall

Im akuten Krisenfall stehen dem Unternehmen die folgenden rechtlichen und kommunikativen Maßnahmen zum Schutz der Reputation zur Verfügung.

1. Rechtliche Maßnahmen

Sowohl bei externen Angriffen auf das Unternehmen sowie bei internen Verstößen durch Mitarbeiter sind rechtliche Maßnahmen zum

14 Vgl. LG München I, 10.12.2013 – 5 HKO 1387/10, BB 2014, 850 Ls, NZG 2014, 345; *Schmidt-Versteyl*, NJW 2019, 1637.
15 *Schmidt-Versteyl*, NJW 2019, 1637.
16 *Auf der Heide/Fischer*, CCZ 2017, 319.
17 LG München I, 5.4.2007 – 5 HKO 15964/06, NZG 2008, 319.
18 *v. Holleben/Menz*, CR 2010, 63, 66.
19 *Bensinger/Kozok*, CB 2015, 376, 378.
20 *Mehrbrey/Schreibauer*, MMR 2016, 75.

Schutz des Unternehmens erforderlich. Bei externen Angriffen kommt eine Reihe von Abwehransprüchen in Betracht, von denen einige nachfolgend kurz dargestellt werden. Anschließend werden mögliche rechtliche Reaktionen auf interne Verstöße skizziert.

a) Äußerungen gegen das Unternehmen

Das Recht gibt Unternehmen eine Reihe von Instrumenten an die Hand, um sich gegen Äußerungen zur Wehr zu setzen. Dem Unternehmen stehen deliktische Ansprüche gegen geschäftsschädigende Kritik zu. Soweit die falsche Tatsache geeignet ist, den Kredit des Unternehmens zu gefährden oder sonstige Nachteile für dessen Erwerb und Fortkommen herbeizuführen, kann das Unternehmen Schadensersatz nach § 824 BGB geltend machen. § 824 BGB schützt das Interesse des Unternehmens, durch Falschmeldungen in den wirtschaftlichen Beziehungen zu seinen Geschäftspartnern belastet zu werden.[21] Darüber hinaus können bei herabwürdigender Kritik Schadensersatzansprüche aus unlauterem Wettbewerb (§§ 3, 4 Nr. 1, 9 UWG), bei Eingriff in den Gewerbebetrieb (§ 823 BGB) oder bei Schädigungsabsicht (§ 826 BGB) bestehen.

Soweit die Kritik inhaltlich jedoch der Wahrheit entspricht, muss das Unternehmen diese erstmal hinnehmen.[22] Mit dieser Prämisse darf die Presse auch den Unternehmer beim Namen nennen, sofern damit keine unangemessene „Prangerwirkung" verbunden ist.[23] Ein weites Verständnis der Meinungswirkung gilt zum Beispiel auch dann, wenn mit den betreffenden Äußerungen im Interesse der übrigen Marktteilnehmer ein tatsächliches Informationsinteresse verfolgt wird, das auch eine die Verbraucher wesentlich berührende Frage betrifft.[24] Der weitreichende Schutz der Meinungsäußerung findet jedoch seine Grenze bei bewusst oder nachweislich unwahren Tatsachenbehauptungen.[25]

Meinungsäußerungen sind grundsätzlich zulässig, auch wenn sie polemisch, unrichtig, unvernünftig, grundlos, schädlich oder verletzend sind. Die Grenze ist meist nur die Schmähkritik. Häufig sind Meinungsäußerungen schon aufgrund ihrer Pauschalität zu substanzarm und daher nicht justiziabel. Die Äußerung des Verdachts „unsauberer Geschäfte" in einem von Mutmaßungen geprägten Fernseh-Interview mit dem Sprecher eines Aktionärsverbandes über die Gründe für den Rücktritt des Vorstandsvorsitzenden eines Großunternehmens blieb sanktionslos.[26]

Ein weiteres Hemmnis gegen geschäftsschädigende Kritik ist gerade im Online-Bereich, dass der Verfasser häufig unbekannt ist, unter Pseudonymen agiert und falsche Daten angibt.[27] Auf vielen Plattformen besteht keine Klarnamenpflicht mit Adressangabe, sodass Kritiker sich verstecken können. In einem solchem Fall kann eine Strafanzeige bei der Staatsanwaltschaft gegen Unbekannt und ein Hinweis bei der Landesmedienaufsicht gemacht werden. Die Feststellung der Identität, auch mittels der IP-Adresse, gelingt jedoch häufig nicht. Dies hat zur Folge, dass keine zustellungsfähige Adresse bekannt ist, um rechtliche Ansprüche, z. B. Auskunft oder Unterlassung, geltend zu machen. Daher ist es häufig schwierig, Ansprüche gegen diskreditierende Äußerungen im Internet durchzusetzen. Eine Methode könnte sein, gegen den Webseitenbetreiber mit Unterlassungsansprüchen vorzugehen und eine einstweilige Verfügung durchzusetzen. Diese einstweilige Verfügung kann zum einen beunruhigten Geschäftspartnern vorgelegt, zum anderen bei Suchmaschinen eingereicht werden, die dann in der Regel die Verlinkung zu der Seite bei einer Suche nach dem Unternehmen löschen.[28]

b) Netzdurchsetzungsgesetz gegen Falschnachrichten?

Unternehmen werden häufig Opfer von Fake News. Um „Fake News" handelt es sich, wenn falsche Nachrichten über das Internet und insbesondere soziale Netzwerke bewusst verbreitet werden (Desinformation).[29] „Fake News" sind folglich bewusst unwahre Tatsachenbehauptungen. Es stehen je nach den Umständen des Einzelfalls eine Reihe von zivil- und strafrechtlichen Ansprüchen zur Verfügung, die gegen Falschnachrichten auch in sozialen Netzwerken zum Schutz Dritter oder der Allgemeinheit Schutz bieten können, z. B. Anspruch auf Widerruf und auf Richtigstellung §§ 1004, 823 BGB und Beleidigung (§§ 186–188 StGB) etc.

Darüber hinaus soll das Netzdurchsetzungsgesetz (NetzDG) helfen, Falschnachrichten zu bekämpfen. Die sozialen Netzwerke sollen die Einhaltung des Notice-and-Take Down-Verfahrens selbst überwachen, dafür effektive Konkretisierungen entwickeln und darüber Bericht erstatten. Kern des NetzDG ist, dass die Netzbetreiber rechtswidrige Inhalte innerhalb einer bestimmten Frist löschen müssen. Rechtswidrige Inhalte sind solche, die die in § 1 Abs. 3 NetzDG aufgeführten 22 Straftatbestände (z. B. Volksverhetzung, Gewaltdarstellung, Beleidigung, Nötigung) erfüllen und nicht gerechtfertigt sind. Von diesen Straftatbeständen richten sich aber nur wenige potenziell gegen die Verbreitung von Falschnachrichten. Insgesamt hilft das NetzDG daher wenig gegen Falschnachrichten.[30]

c) Verletzung von geistigem Eigentum

Zum Schutz der Reputation eines Unternehmens gegen Angriffe auf dessen geistiges Eigentum, wie z. B. Software, Datenbanken, Marken oder urheberrechtlich geschützte Werke, ergeben sich aus einer Reihe von spezialgesetzlichen Unterlassungs- und Schadensersatzansprüchen (§§ 8 UWG, 14 MarkenG, 97 UrhG).

d) Rechtswidrige Offenlegung von Geschäftsgeheimnissen

Gegen die unbefugte Offenlegung von Geschäftsgeheimnissen/ Know-how bietet das seit 26.4.2019 in Kraft getretene Geschäftsgeheimnisgesetz (GeschGehG) einen umfassenderen Schutz.[31] Wer ein Geschäftsgeheimnis rechtwidrig erlangt, nutzt oder offenlegt, ist unter anderem zur Unterlassung, Beseitigung, Herausgabe, Auskunft und zu Schadensersatz verpflichtet.

e) Angriff auf IT-Sicherheit und auf Daten

Bei Angriffen auf die IT-Sicherheit, z. B. durch Phishing, Hackern und Viren, und auf Daten, z. B. Daten-/Passwortdiebstahl, stehen dem Unternehmen deliktische Abwehr- und Schadensersatzansprüche zur Verfügung (z. B. §§ 1004, 823 f. BGB) sowie strafrechtliche Sanktionen (§§ 202a, 202b, 202d, 204 StGB). Allerdings wird es auch hier häufig nicht möglich sein, die Identität des Angreifers festzustellen und rechtliche Ansprüche gegen ihn geltend zu machen.

21 BGH, 10.12.1991 – VI ZR 53/91, NJW 1992, 1312.
22 BGH, 16.12.2014 – VI ZR 39/14, K&R 2015, 196, NJW 2015, 775, Rn. 21; BGH, 22.2.2011 – VI ZR 120/10, BB 2011, 1169 m. BB-Komm. *Dahlke*, NJW 2011, 2204.
23 BGH, 12.7.1994 – VI ZR 1/94,GRUR 1994, 913, 914.
24 *Bamberger u. a.*, in: BeckOK BGB, 51.Edition, Stand: 1.8.2019, § 823, Rn. 224.
25 BVerfG, 13.4.1994 – 1 BvR 23/94, NJW 1994, 1779.
26 BGH, 22.9.2009 – VI ZR 19/08, WRP 2009, 1540, NJW 2009, 3580, Rn. 14.
27 *Ziegelmayer*, GRUR 2012, 761.
28 *Höch*, FAZ-ePaper vom 16.10.2019, Angriff auf die Ehre des Unternehmens, Wirtschaft.
29 *Holznagel*, MMR 2018, 18.
30 *Holznagel*, MMR 2018, 18.
31 Allgemein zum GeschGehG s. *Burghardt-Richter/Bode*, BB 2019, 2697 (in diesem Heft).

f) Interne Verstöße

Datenschutzverstöße und IT-Sicherheitsmängel beruhen häufig auf Mängeln der Organisation. Sobald ein Mitarbeiter einen solchen Verstoß meldet oder der Verstoß auf andere Weise bekannt wird, ist zunächst der Sachverhalt genau festzustellen. Sobald der Sachverhalt bekannt ist, ist rechtlich zu prüfen, ob tatsächlich ein Verstoß gegen rechtliche Vorschriften oder sonstige Vorgaben vorliegt. Dabei sind sämtliche Vorgänge zu dokumentieren, auch zu Beweiszwecken. Wurde ein solcher Verstoß festgestellt, sind die rechtlichen Maßnahmen zu erwägen. Im Datenschutz und bei IT-Sicherheitsmängeln ist z. B. zunächst zu prüfen, ob eine Informationspflicht z. B. an die Datenschutzaufsichtsbehörde besteht (Art. 33 DSGVO) und vielleicht auch an die Betroffenen selbst (Art. 34 DSGVO). Im nächsten Schritt ist der Verstoß zu beheben und rechtliche Compliance herzustellen. Dann ist zu prüfen, ob und inwieweit Dritte von dem internen Verstoß in ihren Rechten verletzt sein könnten und was für Ansprüche auf das Unternehmen zukommen könnten.

Die beim Verstoß aufgetretenen Defizite sind auch in der Compliance-Struktur nachzuverfolgen. Der Verstoß kann arbeitsrechtliche Maßnahmen gegen Mitarbeiter erforderlich machen. Es können auch fachliche Defizite auffallen, die von der Fachabteilung nachzubessern sind. Dies zeigt, dass eine effektive Compliance-Organisation nicht nur eine Risikoanalyse sowie das Einführen einer Compliance-Struktur erfordern, sondern stets auch Prüfungen, Kontrollen, Monitoring der Effektivität der Compliance-Maßnahmen sowie die fortlaufende Verbesserung.

Soweit z. B. datenschutzrechtliche Vorschriften bei der Verarbeitung von personenbezogenen Daten von Mitarbeitern, Kunden und Geschäftspartnern verletzt werden, kann dies nicht nur zu einer empfindlichen Geldbuße für das Unternehmen führen, sondern auch zum Verlust des Vertrauens in das Unternehmen. Zudem können neben den Bußgeldern der Aufsichtsbehörden auch Schadensersatzansprüche der Betroffenen geltend gemacht werden. Darüber hinaus kann die unbefugte Verarbeitung von personenbezogenen Daten bei gewerblichem Handeln oder bei Bereicherungs-/Schädigungsabsicht einen Straftatbestand erfüllen (§ 42 BDSG).

2. Kommunikative Maßnahmen

In der Krise offenbart sich die Haltung des Unternehmens. Eine detaillierte Krisenvorbereitung, regelmäßige Awareness-Kampagnen und kontinuierliches Training sind die Grundlagen für die erfolgreiche Krisenreaktion eines Unternehmens. Auch ein guter Reputational Track Record wirkt sich unterstützend aus, sofern das Unternehmen einen solchen in der Vergangenheit aufgebaut hat.

Darüber hinaus hat jede Krise ihre eigenen Parameter und muss mit einer individuellen Krisenreaktion beantwortet werden. in der Praxis sind dabei diejenigen Unternehmen erfolgreich aus Krisen hervorgegangen, die mit einer zügigen, rechtlich abgesicherten, professionellen Kommunikation und einer den Zielgruppen zugewandten und insbesondere kundenorientierten Haltung agiert haben. Folgende wichtige Kommunikationsgrundsätzen haben sich in der Krise bewährt:

1. Konsistenz: Auch unter hohem Druck müssen Informationsfluss und Abstimmung zwischen den relevanten Teams aufrechterhalten werden, und das Unternehmen muss nach innen und außen mit konsistenten Informationen kommunizieren.
2. Schnelligkeit und Genauigkeit: Rechtzeitige und angemessen kontinuierliche Informationen gehören zu den Grundprinzipien für jede Reaktion. Schnelligkeit ist hierbei eine Ableitung der Vorbereitung.
3. Rechtlich geprüft: Alle öffentlichen Erklärungen und Hintergrundinformationen müssen vorab mit der Rechtsabteilung geklärt werden. Dies ist besonders wichtig, wenn der Vorfall Gegenstand von Rechtsstreitigkeiten, polizeilichen Untersuchungen oder regulatorischen Verpflichtungen ist.
4. Keine Vergleiche: Ein Vergleich mit Wettbewerbern erleichtert zwar unter Umständen eine Einordnung oder Rechtfertigung im ersten Schritt, ist aber sehr oft rechtlich angreifbar und damit ein Reputationsrisiko.
5. Interne Kommunikation: Sie wird häufig vernachlässigt, dabei gehören die Mitarbeiter des Unternehmens zu den wichtigsten Zielgruppen. Zudem sind sie Multiplikatoren und beeinflussen die Unternehmensreputation in ihrem Umfeld maßgeblich. Informationen per Email, Intranet und Teammeetings gehören zur initialen Kommunikation.
6. Kommunikation als Hilfestellung verstehen: Auch wenn der erste Impuls ist, in einer unübersichtlichen Krisenlage erst einmal gar nicht zu kommunizieren, sollte sich das Unternehmen seinen Zielgruppen gegenüber so hilfreich und transparent wie möglich verhalten. Informationen zu geben und einen effektiven Dialog aufrecht zu erhalten, ist in Krisenfällen von wesentlicher Bedeutung.
7. Perspektiven geben: Was lernt das Unternehmen aus der Krise? Welche Verbesserungen werden angestoßen, um das Unternehmen und seine Kunden, Mitarbeiter und weiteren Zielgruppen zukünftig besser gegen Krisen zu schützen? Dies zu kommunizieren, ist essentiell, um das Unternehmen aus der Krise herauszuführen.

VI. „USP" von Kommunikation & Recht

In der Krise gilt es, rasch auf den Angriff oder den internen Verstoß zu reagieren, mit synchronisierten kommunikativen und rechtlichen Maßnahmen nach außen wie auch nach innen. Eine synchronisierte Krisenvorbereitung von Kommunikation und Recht entscheidet über den erfolgreichen Reputationsschutz in einer Krise.

Eine synchronisierte Vorbereitung auf den Krisenfall bedeutet:

– Prüfung der rechtlichen Zulässigkeit der kommunikativen Maßnahmen;
– kommunikative Unterstützung der rechtlichen Maßnahmen;
– Erkennen von Defiziten in bestehenden rechtlichen und kommunikativen Abläufen und Verbesserung dieser Prozesse;
– angemessene Sensibilisierung und Awareness der Mitarbeiter hinsichtlich der Unternehmensrisiken und potenziellen Reputationsschäden;
– definierte und abgestimmte Zuständigkeiten und Entscheidungsbefugnisse;
– Implementierung von Compliance- und Kommunikationsrichtlinien und entsprechenden unternehmensweiten Trainings;
– Aufbau und Dokumentation eines integrierten Krisenreaktionsprozesses, der „auf Knopfdruck" gestartet werden kann.

Die Verankerung der rechtlichen und kommunikativen Krisenvorbereitungsmaßnahmen im Unternehmen erfolgt über ein synchronisiertes Konzept, das gleichermaßen die Kommunikation nach innen, als auch die Kommunikation nach außen, etwa zu Kunden, Geschäftspartnern und der Öffentlichkeit, berücksichtigt.

Im Ergebnis ist festzuhalten, dass Kommunikation und Recht Schlüsselressourcen und Erfolgsfaktoren im Krisenfall sind. Werden sie synchronisiert eingesetzt, unterstützen sie eine erfolgreiche Krisenbewältigung und stärken damit die Reputation des Unternehmens.

Suntka von Halen ist Director bei der strategischen Kommunikationsberatung Brunswick Group. Sie berät globale Unternehmen u. a. in den Bereichen Krisenvorbereitung und Krisenkommunikation, Restrukturierung und Change.

Anne Baranowski, LL.M., RAin und FAin im IT-, Urheber- und Medienrecht bei Schalast Rechtsanwälte Notare in Frankfurt a. M. Sie betreut Mandanten insbesondere im IT-, Datenschutz- und Urheberrecht mit einem Schwerpunkt auf der Technologie- und Medienbranche.

Dr. Udo Kornmeier, RA, ist Partner bei Schalast Rechtsanwälte Notare und betreut Mandanten insbesondere im Urheber- und Medienrecht sowie im Bereich International Litigation.

Ingrid Burghardt-Richter, RAin/FAinHaGesR, und Dr. Johannes Bode, RA

Geschäftsgeheimnisschutzgesetz: Überblick und Leitfaden für Unternehmen zur Wahrung ihrer Geschäftsgeheimnisse

Am 26.4.2019 trat das Gesetz zum Schutz von Geschäftsgeheimnissen (Geschäftsgeheimnisschutzgesetz, „GeschGehG") in Kraft. Das Gesetz dient der Umsetzung der „Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung" („Know-how Richtlinie") (EU) 2016/943. Mit Hilfe des neuen Gesetzes können Unternehmen den Schutz ihrer Geschäftsgeheimnisse effektiver durchsetzen. Um allerdings in den von diesem Gesetz gewährten Schutz vor rechtswidriger Erlangung, Nutzung und Offenlegung von Geschäftsgeheimnissen zu gelangen, enthält das Gesetz einige Neuerungen, die Unternehmen dringend berücksichtigen sollten.

I. Einleitung

Zu den wichtigsten Neuerungen durch das Geschäftsgeheimnisschutzgesetz zählt die in § 2 Nr. 1 GeschGehG enthaltene Legaldefinition des „Geschäftsgeheimnisses", worunter auch das in der Praxis bedeutende technische Wissen (Know-how) fällt. Der Rückgriff auf das bisherige naturgemäß lückenhafte Richterrecht wird hierdurch abgelöst. Das hat seinen Preis: Denn die zentrale Neuerung in der Definition des Geschäftsgeheimnisses liegt darin, dass nunmehr die zu schützende Information Gegenstand von „*angemessenen Geheimhaltungsmaßnahmen*" sein muss. Der Inhaber des Geschäftsgeheimnisses ist hierfür im Streitfall beweisbelastet. Dadurch werden die Anforderungen an den Geheimnisschutz im Vergleich zur früheren Rechtslage deutlich verschärft.

Positiv hervorzuheben ist die Vereinheitlichung der Regelungen zur Durchsetzung von Ansprüchen bei Rechtsverletzungen (rechtswidrige Erlangung, Nutzung oder Offenlegung von Geschäftsgeheimnissen).[1] Diese sind im zweiten Abschnitt in den §§ 6 bis 14 GeschGehG ähnlich der Verletzung gewerblicher Schutzrechte wie Unionsmarken und europäischer Patente geregelt. Danach können dem betroffenen Unternehmen weitreichende Ansprüche zustehen, wie Beseitigungs- und Unterlassungsansprüche oder Auskunfts- und Schadensersatzansprüche. Beachtenswert ist ferner, dass die betroffenen Unternehmen nunmehr auch Ansprüche auf Vernichtung, Herausgabe, Rückruf, Entfernung und Rücknahme der rechtsverletzenden Produkte vom Markt haben.

Schließlich birgt das Geschäftsgeheimnisschutzgesetz in Umsetzung des Art. 9 der Know-how-Richtlinie auch einige verfahrensrechtliche Neuerungen. Bestand zuvor das Risiko, Geschäftsgeheimnisse während eines Prozesses preisgeben zu müssen, wird dem nunmehr durch das neue Verfahren in Geschäftsgeheimnisstreitsachen des dritten Abschnitts in den §§ 15 bis 22 GeschGehG Rechnung getragen. Dabei kann das Gericht nach § 16 GeschGehG geheimhaltungsbedürftige Informationen auch als solche einstufen. In diesem Fall sind derartige Informationen während und auch nach dem Gerichtsverfahren von allen Beteiligten vertraulich zu behandeln.

II. Wesentliche Neuerungen durch das Geschäftsgeheimnisschutzgesetz

Der zuvor bloß mosaikartige Schutz der Geschäftsgeheimnisse wird durch das Geschäftsgeheimnisschutzgesetz grundlegend reformiert und umfassend in einem eigenen Spezialgesetz geregelt.

1 Vgl. *Lamy/Vollprecht*, IR 2019, 201, 204.