Hogan Lovells

Cyber-Angriffe: Haftungsrisiken vermeiden

4. September 2020

Laut Bundesamt für Sicherheit in der Informationstechnik („BSI“) nutzen Cyber-Kriminelle verstärkt die aktuell anhaltende COVID-19-Pandemie zu ihren Gunsten. Viele weitere Quellen bestätigen dies. Cyber-Angriffe auf Unternehmen sind nicht nur subjektiv seit Jahresbeginn stark angestiegen, sondern werden immer mehr zur Realität. Verantwortliche in Unternehmen sollten deshalb Kapazitäten in Fachabteilungen nutzen, um ihre IT-Sicherheitsprozesse und insbesondere auch ihre Reaktionsprozesse und -pläne weiterzuentwickeln, praktisch zu üben sowie zu testen, um Haftungsrisiken vorzubeugen.

Laut dem Cybersicherheitsunternehmen McAfee nahmen externe Cyberangriffe auf Cloud-Dienste und -Tools in den vergangenen Monaten um 630% zu[1]. Dies zeigt, dass das Thema Cybersecurity insbesondere auch durch die COVID-19-Pandemie weiter an Bedeutung gewonnen hat. Aber auch davor sprachen die Zahlen für sich: Bereits 2018 gingen das Zentrum für Strategische und Internationale Studien (CSIS) und das Cybersicherheitsunternehmen McAfee von einem wirtschaftlichen Schaden durch Cyberkriminalität in Höhe von ca. USD 600 Mrd. weltweit aus – davon habe ein Viertel der Diebstahl geistigen Eigentums ausgemacht.[2]

Jedes Unternehmen potentiell betroffen

Daten bilden aktuell in praktisch jedem Unternehmen die Grundlage der Wertschöpfung – sei es als Programme, die Maschinen steuern, als Design- und Programmdaten für Produkte, als Personaldaten oder als Mittel der Kommunikation und Bezahlung. Ein Angriff auf dieses Gut kann daher jedes Unternehmen treffen. Sei es, dass Daten verschlüsselt und damit der Betrieb bis zur Zahlung einer Lösegeldsumme "lahmgelegt" wird, dass sensible Daten, wie personenbezo-gene Informationen oder Betriebsgeheimnisse gestohlen, verwendet oder verändert werden, oder direkt Geldmittel entwendet werden

Im Falle eines Angriffs drohen zudem behördliche Maßnahmen, wie z.B. nicht unerhebliche Bußgelder. Auch Kunden oder Geschäftspartner können mit teilweise erheblichen Schadenser-satzansprüchen an das Unternehmen herantreten, insbesondere wenn das betroffene Unter-nehmen Daten für andere Unternehmen oder für deren Kunden verarbeitet.

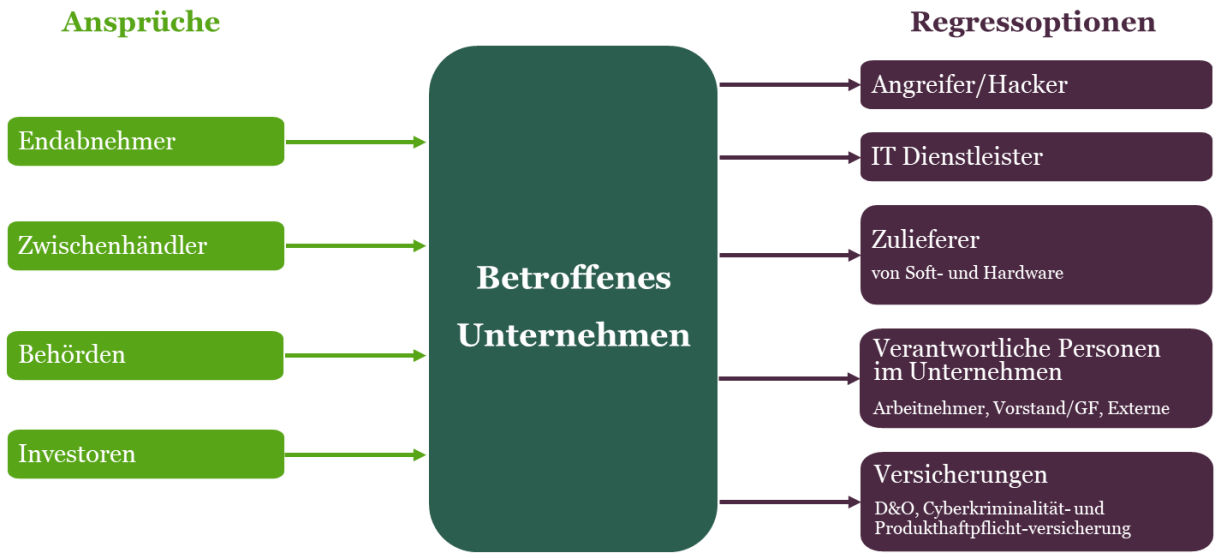
---

1 Bundeskriminalamt (BKA) Lagebilder Cybercrime, abrufbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2018.html;jsessionid=CEC4827CF18931E016550A5381747668.live0611?nn=28110, veröffentlicht 2018.

2 Economic Impact of Cybercrime, abrufbar unter: https://www.csis.org/analysis/economic-impact-cybercrime, veröffentlicht am 21.02.2018.

Daneben hat das Unternehmen zu untersuchen und entscheiden, ob Regressansprüche gegen Verantwortliche in Betracht kommen: Hat der IT-Service-Provider seine Pflicht zur Sicherung des Netzwerks nicht erfüllt, der Hersteller von IT-Sicherheitssoftware eine fehlerhafte Software geliefert, ein Anbieter eines angeschlossenen Geräts unzureichende Sicherheitsmaßnahmen implementiert, ein Mitarbeiter ein Datenleck verursacht oder aber die Manager Aufsichts- und Compliance-Plichten verletzt? Der Versuch, sich direkt an den Hacker oder Dritte zu wenden, die vorsätzlich oder fahrlässig das Durchsickern der Daten verursacht haben, führt demgegen-über regelmäßig ins Leere.

Mögliche Anspruchssteller und Regressoptionen sind im folgenden Schaubild zusammenge-fasst:



Schadensbilder sind mannigfaltig – von Betriebsausfallschäden bis Bußgelder der Datenschutzbehörden

Als mögliche Haftungsgrundlagen bei Cyberattacken kommen Verträge, direkt die DS-GVO, die gesetzliche Haftung von Geschäftsführern sowie eine deliktische Haftung und nicht zuletzt auch (datenschutzrechtliche) Bußgeldvorschriften in Betracht.

Neben der direkten, gesetzlichen Haftung sind für das Unternehmen auch Schäden, wie zum Beispiel dem sogenannten "Blacklisting" öffentlicher Aufträge oder der Verlust des Kundenvertrauens hervorgerufen durch Reputationsschäden, zu berücksichtigen. Diese können wiederum zu einer Haftung von Verantwortlichen im Unternehmen oder Dritten (wie z.B. Dienstleistern) führen.

Der Verlust personenbezogener Daten (z. B. Geburtsdatum, Bankkonto- und Kreditkartennummern sowie weitere personenbezogene Daten) ist grundsätzlich durch die DS-GVO und die BDSG geschützt. Der Diebstahl dieser Daten verursacht im Regelfall keinen unmittelbar erkenn-baren finanziellen Schaden. Wenn aber – wie häufig – Daten einer großer Anzahl von Betroffe-nen von einem Cyberangriff erfasst sind, können sich selbst an sich kleine Schadenspositionen schnell zu erheblichen Schäden summieren, wie z.B. Kosten für den Ersatz von Kreditkarten, Kommunikationskosten und Rechtsverfolgungskosten zur Abwehr von Ansprüchen.

Professionelle Kläger und staatliche Bestrebungen hin zu effektiveren Massenklagen senken die Schwelle auch für Verbraucher

Professionelle Kläger, die eine Vielzahl von kleinen Ansprüchen bündeln, die Möglichkeit von Verbandsklagen oder auch die von der Europäischen Union geplante Europäische Verbandsklage[3] führen dazu, dass es sich auch bei kleinen monetären Schäden immer häufiger lohnt, diese trotzdem geltend zu machen.

Haftungsvermeidung und -begrenzung durch IT-Sicherheit und gelebte und geprobte Reaktionskonzepte (Incident Response Plan)

Erstes Ziel zur Haftungsvermeidung sollte eine möglichst gute und professionelle IT-Sicherheit sein. Neben der richtigen Technik ist hier insbesondere die Schulung aller Mitarbeiter relevant. Zur Vermeidung von Bußgeldern und datenschutzrechtlichen Schadensersatzansprüchen ist ein gut funktionierendes DS-GVO Compliance Konzept unerlässlich. Um Schäden möglichst klein zu halten, Ansprüche abzuwehren und wo möglich Regressansprüche geltend zu machen, sind jedoch insbesondere auch gut dokumentierte "Data Breach Response Pläne" – auch "Incident Response Plan" oder "Business Continuity Plan" genannt – von zentraler Bedeutung:

- Sie dienen der schnellen Bewertung einer Bedrohungslage und ermöglichen eine schnelle und sachgerechte Reaktion.
- Sie dienen zur Vermeidung und Verminderung von Folgeschäden wie Bußgeldern, insbesondere der schnellen Sicherstellung eines Notbetriebs oder von anderen Sicherungsmaßnahmen insb. für die Produktion.
- Sie ermöglichen eine gründliche und zugleich schnelle Ermittlung der Ursache eines Cyberangriffs. Diese ist für die Durchsetzung von oder Verteidigung gegen potenzielle Schadensersatzansprüche von entscheidender Bedeutung, da hier insbesondere auch der richtige Umgang mit eventuell betroffenen Daten und die richtige Reaktion dargelegt werden muss.

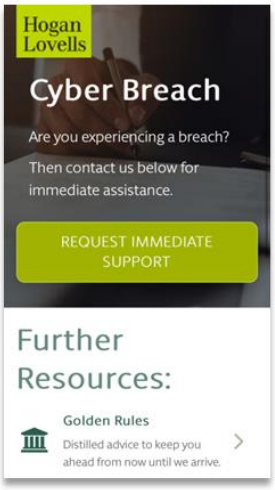
Beim Entwurf eines maßgeschneiderten Incident Response Plans sind neben technischen Implikationen insbesondere auch zahlreiche rechtliche Implikationen zu bedenken: die Einhaltung von Meldepflichten, die Datenschutz-Compliance der Reaktions-Maßnahmen aber auch Fragen rund um das Thema Legal Privilege.

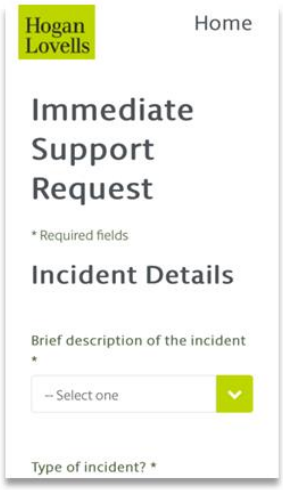
Einer der wichtigsten, aber häufig unterschätzten Aspekte des Incident Response Plans ist die regelmäßige Übung der Reaktion auf einen Cyberangriff mit allen Beteiligten bis hin zum Top-Management. Nur so kann sichergestellt werden, dass im Ernstfall schnell und effizient gehandelt wird und alle Beteiligten wissen, was zu tun ist.

---

[3] Vorschlag für eine RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher und zur Aufhebung der Richtlinie 2009/22/EG *https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52018PC0184&from=DE*

Hogan Lovells – Cyber Breach App





JETZT BEI Google Play

Laden im App Store

Kontakt

Nicole Böck
Produkthaftung
Counsel, München
T +49 89 290 12 0
nicole.boeck@hoganlovells.com

Dr. Martin Strauch, LL.M. (Edinburgh)
Prozessführung und Schiedsgerichtsbarkeit
Associate, München
T +49 89 290 12 0
martin.strauch@hoganlovells.com

David Bamberg
Datenschutz
Senior Associate, München
T +49 89 290 12 0
david.bamberg@hoganlovells.com

Jakob Theurer, LL.M. (Amsterdam)
Produkthaftung
Senior Associate, Berlin
T + 49 30 80 09 30 000
jakob.theurer@hoganlovells.com

www.hoganlovells.com