Linklaters

Mai 2018

Cyber-Angriffe:

Krisenmanagement im Ernstfall

Spätestens seit „WannaCry“ und den dadurch verursachten Schäden sollte es jedem Unternehmen bewusst sein, wie wichtig es ist, Vorsorge gegen Cyber-Kriminalität zu treffen. Was zu tun ist, wenn es gleichwohl zu einem Cyber-Angriff kommt, ist ebenso Gegenstand dieses Newsletters wie die Frage, welche potentiellen Ansprüche dem betroffenen Unternehmen zustehen bzw. welchen typischen Ansprüchen Dritter sich ein betroffenes Unternehmen ausgesetzt sieht.

Inhalt

1 Warum ist das Thema Cyber-Kriminalität relevant?

Je weiter die Digitalisierung voranschreitet und je mehr computerbasierte Systeme im Einsatz sind, desto höhere Relevanz erlangen die rechtlichen Auswirkungen von Cyber-Kriminalität für betroffene Unternehmen. Schätzungsweise eine Million Infektionen mit Schadsoftware sind in Deutschland monatlich zu verzeichnen. Auch die Zahl von mit Schadsoftware belasteten E-Mails ist angestiegen. Insgesamt sind laut einer Studie des Bundeskriminalamts in den letzten Jahren 53% aller deutschen Unternehmen Opfer von Cyber-Kriminalität geworden, was Schäden in Höhe von 55 Mio. Euro verursacht hat.

Das bekannteste Beispiel jüngerer Zeit ist „WannaCry“. Bei diesem Hackerangriff wurden im Mai 2017 über 230.000 Computer in 150 Ländern infiziert und Lösegelder von den Betroffenen verlangt. Im Falle von „Equifax“ wurden persönliche Daten von 145 Millionen Menschen gestohlen, nachdem im Juli 2017 die amerikanische Kreditanstalt Equifax gehackt worden war. Ebenfalls weitreichende Konsequenzen hatte „NotPetya“, da ein Angriff, der zunächst auf ukrainische Unternehmen zielte, anschließend auf Unternehmen weltweit übergriff. So waren von „NotPetya“ letztlich u.a. FedEx in den USA, Rosneft in Russland sowie Maersk in Dänemark betroffen.

Vor diesem Hintergrund ist evident, dass der Schutz vor Cyber-Angriffen durch Prävention notwendiger Teil eines jeden Risikomanagements und Compliance-Systems ist. Daneben ist aber auch der richtige Umgang mit solchen Angriffen von größter Bedeutung. Auf letzterem Aspekt liegt der Fokus dieses Newsletters.

2 Was ist bei einem Cyber-Angriff zu tun?

Kommt es – trotz oder mangels Prävention – zu einem Cyber-Angriff, ist die zentrale Reaktion das schnellstmögliche Abstellen des unmittelbaren Angriffs durch technische Maßnahmen. Zusätzlich sind die folgenden Themen von der ersten Stunde an im Blick zu haben:

- **Feststellung des Ausmaßes des Angriffs:** Was ist betroffen und wo hat sich der Angriff ausgewirkt? Hierzu gehört auch, eine Kopie des betroffenen Systems für Beweiszwecke anzufertigen.
- **Ermittlung von Verantwortlichkeiten:** Dies umfasst die Ermittlung sowohl des Angreifers als auch der Verantwortlichen für fehler- oder lückenhafte Schutzmaßnahmen im Unternehmen, die den Angriff erst ermöglicht haben.
- **Meldepflichten gegenüber öffentlichen Stellen** wie der zuständigen Datenschutzbehörde (Art. 33 DS-GVO).
- **Information von betroffenen Personen** (Art. 34 DS-GVO).
- **Umgang mit Erpressungsforderungen**: Die Zahlung von Lösegeld kann im Einzelfall zu einer eigenen Strafbarkeit führen (z.B. Unterstützung krimineller Vereinigungen, Geldwäsche, Verstöße gegen das Außenwirtschaftsgesetz etc.).

Das betroffene Unternehmen sollte in jedem Fall davon absehen, „zurückzuhacken“, da sich sonst beteiligte Individuen ebenfalls strafbar machen könnten.

3 Was droht, auch wenn der unmittelbare Angriff beseitigt ist?

Ist der unmittelbare Angriff beseitigt und sind die erforderlichen Schutzmaßnahmen ergriffen, stellt sich in rechtlicher Hinsicht als nächstes die Frage nach etwaigen Haftungsansprüchen. Dabei stehen dem betroffenen Unternehmen Ansprüche zu, aber gleichzeitig kann es sich auch selbst Ansprüchen ausgesetzt sehen.

3.1 Ansprüche des betroffenen Unternehmens gegen Dritte

Die Schäden, die dem betroffenen Unternehmen entstehen können, sind vielfältig: In Betracht kommen etwa Reputationsschäden, Verzugsschäden (z.B. bei nicht rechtzeitig ausgeführten Finanztransaktionen), Produktionsausfälle, Kosten für die Abstellung des Angriffs und die Ermittlung der Verantwortlichen, Schäden durch den Diebstahl von Kundendaten etc. Dem betroffenen Unternehmen können dabei insbesondere Ansprüche gegen die folgenden Personen zustehen:

- Gegen den **Angreifer** bestehen zumeist deliktische Ansprüche wegen der Verletzung von Strafvorschriften (insbesondere §§ 202a, 202b, 202c, 202d, 303a, 303b, 263a, 269 StGB oder § 17 UWG).

- Gegen **Hilfspersonen des Angreifers**, also Personen, die der Angreifer einsetzt, um den Angriff auszuführen und seine eigene Identität zu schützen, bestehen über § 830 BGB die gleichen deliktischen Ansprüche, wie gegen den Angreifer.
- Zu prüfen ist, ob die Schäden des Angriffs von bestehenden Versicherungspolicen des Unternehmens abgedeckt sind, also gegenüber **Versicherungen** geltend gemacht werden können. Zu denken ist hierbei vor allem an D&O- und Cyber-Versicherungen, die nebeneinanderstehen können.
- Bei Ansprüchen gegen **Mitarbeiter** sind die üblichen Grundsätze der arbeitsvertraglichen Haftungsverteilung bei der Prüfung von Ansprüchen zu berücksichtigen; im Rahmen von deliktischen Ansprüchen ist zu beachten, dass bei mittelbaren Verletzungshandlungen ein spezieller Pflichtenverstoß vorliegen muss, um zu einer Haftung eines Mitarbeiters zu kommen.
- **Organe** können für die Verletzung von Überwachungs- und Risikovorsorgepflichten haften. Dazu zählt auch die Einführung und regelmäßige Überwachung eines IT-Sicherheitssystems. Für Unternehmen der Versicherungs- und Bankenbranche hat die BaFin diese Pflichten erst jüngst konkretisiert („Versicherungsaufsichtliche Anforderungen an die IT“ – VAIT und „Bankenaufsichtliche Anforderungen an die IT“ – BAIT).
- Gegen **externe IT-Dienstleister**, die für die Wartung des unternehmensinternen IT-Systems verantwortlich sind, bestehen in der Regel Schadensersatzansprüche, sofern diese ihre Pflichten nicht sorgfältig wahrgenommen und dadurch einen Angriff ermöglicht haben.
- Gegen den **Hersteller** einer fehlerhaften Software bestehen vor allem Ansprüche aus Produzentenhaftung.

3.2 Ansprüche gegen das angegriffene Unternehmen

Neben eigenen Ansprüchen ist zu beachten, dass das betroffene Unternehmen in Folge des Cyber-Angriffs auch selbst Ansprüchen ausgesetzt sein kann. Vor allem die folgenden Gruppen können anspruchsberechtigt sein:

- In Betracht kommen bei **Mitarbeitern, Kunden und Dritten**, deren Daten aufgrund des Angriffs missbraucht oder entwendet wurden, vor allem vertragliche Schadensersatzansprüche, sofern das Unternehmen seine Pflichten im Hinblick auf IT-Sicherheit verletzt hat. War ein Angriff nach dem aktuellen Stand der Technik hingegen unvermeidbar, dürfte eine Haftung regelmäßig ausscheiden. Eine Haftung des Unternehmens gegenüber seinen Kunden kommt im Übrigen aber auch dann in Betracht, wenn den von einem Datendieb-

stahl betroffenen Kunden ein Schaden entsteht, weil das Unternehmen nicht seinen Informationspflichten nach Art. 34 DS-GVO nachgekommen ist. Hieran zeigt sich, wie wichtig es ist, Meldepflichten unverzüglich nachzukommen anstatt – etwa aus Sorge um einen Reputationsverlust – abzuwarten. Zudem sind deliktische Ansprüche der Kunden denkbar (insbesondere § 44 Abs. 1 TKG sowie Art. 82 DS-GVO).

- In Bezug auf **Vertragspartner** sind schuldrechtliche Ansprüche (wegen Verzugs oder gar Unmöglichkeit) gegen das betroffene Unternehmen denkbar, etwa wenn die Produktion stillliegt und daher bestehende Verpflichtungen nicht erfüllt werden können. Entscheidend ist insoweit stets die Frage nach dem Vertretenmüssen durch das Unternehmen.
- **Sonstigen Dritten** können im Einzelfall deliktische Ansprüche gegen das betroffene Unternehmen zustehen (etwa auf Grundlage von § 44 Abs. 1 TKG, Art. 82 DS-GVO sowie § 823 Abs. 1 BGB i.V.m. Art. 1 und 2 GG sowie i.V.m. DS-GVO).

4 Fazit

Cyber-Kriminalität ist ein hochaktuelles Thema, das angesichts fortschreitender Digitalisierung und Vernetzung zunehmend an Bedeutung gewinnt. Jedes Unternehmen muss sich darüber im Klaren sein, dass Cyber-Vorfälle im Ernstfall existenzbedrohend sind. Daher wird es sich auch kein Unternehmen leisten können, bei der Vorsorge gegen Cyber-Kriminalität oder beim Krisenmanagement im Ernstfall nachlässig zu sein.

Linklaters

Ansprechpartner

Für weitere Informationen kontaktieren Sie bitte:

Dr. Christian Schmitt
Partner
Dispute Resolution
(+49) 69 71003 261
christian.schmitt@linklaters.com

Dr. Daniel Pauly
Partner
Head of Technology Media & Telecommunication Germany
(+49) 69 71003 570
daniel.pauly@linklaters.com

Dr. Kerstin Wilhelm
Managing Associate
Dispute Resolution
(+49) 89 41808 506
kerstin.wilhelm@linklaters.com

Autoren: Mirjam Erb, Jacqueline Kusserow, Dr. Daniel Pauly, Dr. Christian Schmitt, Dr. Kerstin Wilhelm