Gastbeitrag US-Wertpapierrecht

SEC weitet Zuständigkeit deutlich auf Cybersicherheit aus

Die US-Börsenaufsicht SEC schaut mit Blick auf interne Rechnungslegungskontrollbestimmungen intensiv auf das Thema Cybersicherheit. Das kann auch deutsche Unternehmen mit US-Listing treffen.

München/Dallas, 19. Juli 2024, 15:16 Uhr Katharina Humphrey, Sophie Rohnke

Die US-Börsenaufsicht SEC fordert Unternehmen in der Abwehr von Cybercrime mehr ab.
Foto: picture alliance / Sipa USA | SOPA Images

Die US-Börsenaufsicht SEC hat in ihrem Ende Juni abgeschlossenen Verfahren gegen das Unternehmen R.R. Donnelley & Sons Co. den Anwendungsbereich der internen Rechnungslegungskontrollbestimmungen des US-amerikanischen Wertpapierrechts signifikant in den Bereich Cybersicherheit hinein ausgeweitet. Damit erstreckt sich die Zuständigkeit der SEC von nun an auf die Cybersicherheitssysteme von Unternehmen, die an US-Börsen notiert sind. Und auch auf deutsche Unternehmen, die in den USA gelistet sind, kommt im Fall eines Cyberangriffs zusätzlich das Risiko zu, von der SEC im Falle eines unzureichenden Cybersicherheitssystem mit Geldbußen belegt zu werden.

Der Fall R.R. Donnelley

Wie aus der am 18. Juni 2024 veröffentlichten Pressemitteilung der SEC hervorgeht, kam die US-Börsenaufsicht in dem Verfahren gegen das im Verlagswesen tätige Unternehmen zu dem Schluss, dass R.R. Donnelley aufgrund seines unzureichenden Cybersicherheitssystems gegen die Rechnungslegungskontrollbestimmungen des US Securities Exchange Acts of 1934 („Exchange Act") verstoßen hat. Konkret wurde dem Unternehmen vorgeworfen, dass es zu spät auf einen gegen das Unternehmen gerichteten Cyberangriff reagiert hätte. R.R. Donnelley zahlte im Zuge des Verfahrens, das mit einem Vergleich endete, ein Bußgeld in Höhe von 2.125 Mill. US-Dollar. Bei der Bemessung des Bußgelds wurde die Kooperation des Unternehmens im Rahmen des SEC-Verfahrens berücksichtigt.

Verdachtsmeldungen nicht ernst genommen

R.R. Donnelley wurde Ende 2021 Opfer eines mehrwöchigen Ransomeware-Angriffs, im Zuge dessen die Angreifer Zugriff auf die Daten mehrerer Kunden erlangten. Bereits am ersten Tag des Cyberangriffs reagierte das interne Cybersicherheitssystem des Unternehmens und generierte eine IT-basierte Verdachtsmeldung. Weitere computergenerierte Verdachtsmeldungen folgten im Verlauf des Cyberangriffs.

Der Cybersicherheitsdienstleister, den das Unternehmen mit der Bearbeitung von Verdachtsmeldungen beauftragt hatte, leitete nur eine geringe Anzahl dieser Meldungen an das Unternehmen weiter, wies aber grundsätzlich auf das Risiko eines möglichen Angriffs hin. Das Unternehmen versäumte es, den Meldungen und Hinweisen des Dienstleisters nachzugehen und sie entsprechend zu eskalieren. Dies hatte zur Folge, dass das Unternehmen erst Wochen später aktiv wurde und erst dann Maßnahmen gegen den Angriff einleitete, als es von einem Geschäftspartner auf den Cyberangriff hingewiesen worden war.

Internes Kontrollsystem im Fokus

Die Börsenaufsicht sah in dem verspäteten Vorgehen gegen den Cyberangriff und den zugrundeliegenden Defiziten des Cybersicherheitssystems einen Verstoß gegen die Rechnungslegungskontrollbestimmungen des Exchange Acts. Diese erfordern, dass das interne Rechnungslegungskontrollsystem dergestalt konzipiert und implementiert ist, dass unberechtigte Zugriffe auf Unternehmensvermögenswerte mit hinreichender Sicherheit verhindert werden.

Die SEC argumentierte, dass auch die unternehmensinternen IT-Systeme und Netzwerke Unternehmensvermögenswerte im Sinne dieser Bestimmungen darstellen und insofern in deren Anwendungsbereich fallen. Besonders bemerkenswert hierbei ist, dass im vorliegenden Fall zwar Kundendaten Gegenstand des Cyberangriffs waren, die unternehmensinternen Finanz- und Rechnungslegungssysteme aber gar nicht betroffen waren.

Unzureichende Reaktion moniert

Die US-Börsenaufsicht legt bereits seit einigen Jahren einen starken Fokus auf die Nachverfolgung von Cybersicherheitsfällen. Bislang stellte sie dabei jedoch stets auf die verspätete Unterrichtung des Kapitalmarkts ab. So kam es beispielsweise im letzten Jahr zu einem Vergleich mit der SEC, in dem das Software-Unternehmen Blackbaud einem Bußgeld in Höhe von 3 Mill. Dollar für eine unvollständige Unterrichtung des Kapitalmarkts über den Umfang eines Cyberangriffs zustimmte.

In dem Verfahren gegen R.R. Donnelley weicht die SEC von diesem Vorgehen ab. Sie bezieht sich auf die unzureichende Reaktion des Unternehmens auf den Cyberangriff sowie auf die Defizite des unternehmensinternen Cybersicherheitssystems. Damit weitet die SEC die Rechnungslegungskontrollbestimmungen des US-amerikanischen Exchange Acts auf unternehmensinterne IT-Systeme sowie Cybersicherheitssysteme aus.

Hieraus folgt, dass sich auch die Zuständigkeit der SEC in diese Bereiche im Zusammenhang mit Cyberangriffen erstreckt, und zwar auch dann, wenn die Finanz- und Rechnungslegungssysteme nicht betroffen sind. Für an US-Börsen gelistete Unternehmen hat dies im schlimmsten Fall zur Folge, dass sie sich nicht nur einem Cyberangriff ausgesetzt sehen, sondern auch noch den rechtlichen Risiken im Zusammenhang mit einem SEC-Verfahren.

Ausweitung der Kontrollbestimmungen

Die Anwendung und signifikante Ausweitung der Rechnungslegungskontrollbestimmungen in dem R.R. Donnelley-Verfahren waren innerhalb der SEC stark umstritten. Zwei der fünf SEC-Kommissare veröffentlichten im Zusammenhang mit dem Verfahren eine abweichende Meinung, in der von einer „Ausweitung des Rechts“ und einer „Verzerrung“ der Rechnungslegungskontrollbestimmungen die Rede ist.

Vermengung von Kontrollen

Die Auslegung, dass auch die unternehmensinternen IT-Systeme Unternehmensvermögenswerte darstellen, geht in den Augen der beiden SEC-Kommissare zu weit und führt zu einer Vermengung von dezidierten Rechnungslegungskontrollen, die Gegenstand des Exchange Acts sind, mit den allgemeinen Kontrollen des internen Kontrollsystems eines Unternehmens.

Dieselben SEC-Kommissare hatten bereits im Zusammenhang mit einem früheren Verfahren, in dem es zu einer Ausweitung der Rechnungslegungskontrollbestimmungen seitens der SEC kam, angemahnt, dass es der SEC nicht zustünde, Unternehmen zu sagen, wie sie sich zu organisieren haben („how to run themselves“).

Die SEC führt im Vergleich mit R.R. Donnelley nicht aus, welche Elemente ein Cybersicherheitssystem beinhalten muss, um im Sinne der Rechnungslegungskontrollvorschriften angemessen zu sein. Anhand der Schwachstellen, die die Behörde im Zusammenhang mit dem Cybersicherheitssystem von R.R. Donnelley moniert, lassen sich jedoch einige Rückschlüsse ziehen.

Unklare Verantwortlichkeiten

Die Behörde bemängelt zum einen, dass die IT-generierten Verdachtsmeldungen nicht in adäquater Weise ausgewertet und eskaliert wurden. Hierin sah die SEC eine Schwachstelle, da nicht sichergestellt ist, dass die Unternehmensleitung zeitgerecht über alle erforderlichen Informationen verfügt, um bestehenden Verpflichtungen zur Unterrichtung des Kapitalmarkts nachzukommen.

Ein weiteres Defizit sah die SEC in der Überwachung des von R.R. Donnelley beauftragten Dienstleisters, der es ebenfalls versäumte, die Verdachtsmeldungen ordnungsgemäß nachzuverfolgen. Letztlich bemängelte die Börsenaufsicht diverse grundsätzliche Schwachstellen im Cybersicherheitsprotokoll des Unternehmens. Dies betraf zum einen die unklare Ausgestaltung von Verantwortlichkeiten sowie unzureichende Ressourcen, aber auch die inadäquate Priorisierung und Eskalierung möglicher Cybervorfälle.

Rechtliche Risiken

Für deutsche Unternehmen, die an einer US-Börse gelistet sind und insofern in den Zuständigkeitsbereich der US-Börsenaufsicht SEC fallen, führt die Entscheidung letztlich zu weiteren rechtlichen Risiken. Einschlägige Unternehmen müssen damit

rechnen, dass die SEC im Falle eines Cyberangriffs nicht nur die kapitalmarktrechtliche Kommunikation des Unternehmens, sondern auch die Reaktion auf den Cyberangriff selbst sowie das interne Cybersicherheitssystem des Unternehmens genau unter die Lupe nimmt.

Empfindliche Bußgelder drohen

Welchen Erfordernissen ein solches adäquates Cybersicherheitssystem entsprechen sollte, beantwortet die SEC in dem vorliegenden Verfahren nicht. Es lässt sich jedoch ableiten, dass eine klare Festlegung von Verantwortlichkeiten sowie eine angemessene Berichterstattung und Eskalation von Verdachtsmeldungen zentrale Elemente sein müssen. In den USA gelistete Unternehmen sind insofern gut beraten, ihre internen Cybersicherheitssysteme sowie ihr Notfallprotokoll für Cyberangriffe zu überprüfen und etwaige Defizite zu adressieren, damit im Falle eines Cyberangriffs nicht noch das Risiko eines empfindlichen Bußgelds im Zusammenhang mit einem Verfahren der US-amerikanischen Börsenaufsicht besteht.

Katharina Humphrey ist Partnerin im Münchner Büro von Gibson, Dunn & Crutcher. Sophie C. Rohnke ist Of Counsel im Büro der Kanzlei in Dallas.