RECHT UND STEUERN

Auf die Softwarepanne folgt die Klage

Ein schadhaftes Update von Crowdstrike hat auf der ganzen Welt Computer blockiert. Wer muss in solch einem Fall dafür geradestehen?

Von Christoph Süßenberger

Am 19. Juli verursachte ein Update der Sicherheitssoftware „Falcon“ des Herstellers Crowdstrike einen weltweiten Ausfall von Millionen Computern. Wer haftet für die Milliardenschäden? Die juristischen Herausforderungen sind vielschichtiger als auf den ersten Blick erkennbar.

Betroffen von dem Crowdstrike-Ausfall waren Organisationen, Behörden und Unternehmen verschiedener Branchen auf der ganzen Welt: An Flughäfen standen Check-in-Schalter und Gepäckabfertigungssysteme still, was zu massiven Verzögerungen und Flugausfällen führte. In Krankenhäusern war die Patientenversorgung gefährdet, Operationen mussten verschoben werden. Banken meldeten Ausfälle bei Zahlungssystemen und im Onlinebanking. Entgegen ersten Vermutungen handelte es sich nicht um einen Hackerangriff. Crowdstrike erklärte, dass ein interner Fehler in einem Routine-Update die Ursache des Ausfalls war, und konnte innerhalb weniger Stunden ein korrigiertes Update zur Verfügung stellen, um die betroffenen Systeme wieder in Betrieb zu nehmen.

Ein Glaubenssatz der Informationstechnologie lautet: „Fehlerfreie Software gibt es nicht.“ Doch Kunden, Hersteller und Juristen stehen vor der kritischen Frage: Muss der Kunde dieses Risiko hinnehmen, oder wer trägt die Verantwortung, wenn Software nicht fehlerfrei ist?

Die Antwort sieht nach deutschem Recht einfach aus: Der Kunde kann von dem Hersteller verlangen, dass die Software mangelfrei ist. Sie muss sich für die vorgesehene Verwendung eignen und ohne Unterbrechungen sicher funktionieren. Wenn die Software einen Mangel hat, muss der Hersteller ihn kostenlos beseitigen, indem er dem Kunden Updates zur Verfügung stellt oder ein fehlerfreies Release liefert. Kommt der Hersteller dem nicht nach, kann der Kunde von dem Vertrag zurücktreten und die Erstattung der Vergütung verlangen oder sie selbst reduzieren. Daneben hat der Kunde einen Anspruch auf Ersatz der ihm entstandenen Schäden, wenn der Hersteller den Mangel vorsätzlich oder fahrlässig verursacht hat. Dieser Anspruch fängt bei den Kosten des Kunden an und geht über die Kompensation von Produktionsausfällen bis hin zum Ersatz des entgangenen Gewinns. Wenn der Hersteller dem Kunden mit einem Service Level Agreement die Verfügbarkeit der Software und bestimmte Fristen zur Fehlerbeseitigung zugesichert hat, kann daneben noch eine Vertragsstrafe anfallen.

Schwierig wird es in der Praxis: Hersteller und Kunden stehen vor der Frage, ob die Software tatsächlich mangelhaft und der Hersteller zur Beseitigung verpflichtet ist. Falls der Hersteller selbst den Fehler einräumt und die passenden Updates zur Behebung verteilt, ist die Antwort schnell gefunden. Der Hersteller ist ebenfalls in der Verantwortung, wenn die Software zunächst mangelfrei funktioniert und erst ein fehlerhaftes Update zu Ausfällen führt, anstatt die Software routinemäßig zu aktualisieren. Unübersichtlich wird es, wenn sowohl Hardwaredefekte als auch Inkompatibilität oder Netzwerkprobleme die Ursache sein können. Der Kunde könnte den Ausfall selbst verursacht haben, indem er die Software falsch benutzt oder es versäumt, Updates zur Beseitigung von Fehlern und Sicherheitslücken aufzuspielen. Möglicherweise haben Hersteller und Kunde alles richtig gemacht, doch Malware oder Hacker haben den Ausfall provoziert. Der Hersteller ist also nicht immer verantwortlich, falls die Software nicht funktioniert.

Wenn feststeht, dass die Software selbst mangelhaft ist, muss der Kunde im Einzelfall entscheiden, wen er deswegen in Anspruch nehmen kann: Hat er die Software bei dem Hersteller direkt erworben, wird dieser auch für die Ansprüche des Kunden verantwortlich sein. Falls ein Händler die Software verkauft oder ein Dienstleister sie im IT-System des Kunden implementiert hat, kann der Kunde auch gegen diese Unternehmen vertragliche Ansprüche haben. Oder er hat nur gegen sie Ansprüche, weil er mit dem Softwarehersteller selbst keinen Vertrag geschlossen hat.

Wie weit geht dann die Verantwortung des Händlers, Dienstleisters oder Herstellers? Die Verpflichtung, den Mangel zu beheben, ist schnell bejaht, selbst wenn man akzeptieren würde, dass Software nicht fehlerfrei sein kann. Problematisch sind die weiteren Schäden, die durch Ausfälle unmittelbar und mittelbar verursacht werden. Ein Hersteller muss den Kunden für dessen eigene Kosten entschädigen. Aber haftet er auch für die Milliardenschäden von kritischen Infrastrukturen, wenn er die Software sorgfältig gemäß dem Branchenstandard entwickelt hat und sich trotzdem eine fehlerhafte Zeile Programmcode in einem kleinen Update einschleicht mit der Folge, dass weltweit Computer stillstehen? Kann ein Hersteller seine Haftung gegenüber dem Kunden vertraglich ausschließen, weil die beteiligten Juristen bis kurz vor Abschluss um eine passende Haftungsbeschränkung im Vertragstext gerungen haben?

Es ist ein Beleg für die Komplexität der Sach- und Rechtslage, dass es in Deutschland eine eher überschaubare Anzahl einschlägiger Gerichtsentscheidungen zu fehlerhafter Software und gescheiterten Projekten gibt, während Gerichte aller Instanzen die Verantwortung für Mängel am Bau oder bei Kraftfahrzeugen über Jahrzehnte sorgfältig ausgelotet haben. Richtern fehlen häufig die notwendige Sachkenntnis und Spezialisierung, und die Rechtsunsicherheit ist groß, wenn Sachverhalte wie der Crowdstrike-Ausfall in vielen Ländern mit unterschiedlicher Rechtslage zu beurteilen sind. Dann sind die Parteien motiviert, einen Kompromiss zu finden, anstatt einen langwierigen und kostenintensiven Prozess mit unberechenbarem Ausgang zu führen.

Nachdem die Computer wieder laufen und die IT-Abteilungen keine Überstunden mehr schieben müssen, wird der Crowdstrike-Ausfall die IT-Rechtler weltweit noch jahrelang beschäftigen.

Der Autor ist Partner der Kanzlei FPS. Er berät Unternehmen im IT-Recht und bei Gerichtsverfahren.