Cybersicherheit. Der Computerausfall könnte eine Prozesslawine nach sich ziehen – auch wenn die Aussichten auf Schadenersatz schwer einschätzbar sind. Vor allem aber steigen die möglichen Haftungsrisiken für die Zukunft.

Die Lehren aus dem Crowdstrike-Desaster

VON CHRISTINE KARY

Wien. Es war also doch nicht die seit Langem befürchtete, ultimative Cyberattacke. Sondern ein simpler Softwarefehler, der am 19. Juli Millionen Computer lahmgelegt hat.

Doch das macht es nicht besser. Im Gegenteil, es führt uns vor Augen, wie fragil die digitale Infrastruktur ist. Um sie global aus dem Tritt zu bringen, braucht es nicht einmal kriminelle Energie. „Softwarefehler passieren", sagt Cybersecurity-Experte Marc Nimmerrichter vom Wiener IT-Sicherheitsunternehmen Certitude zur „Presse". Die Crowdstrike-Panne habe erstmals gezeigt, „was passieren kann, wenn auch nur ein Dominostein fällt". Wobei es noch viel größere Steine gebe, die hätten fallen können. Mit noch verheerenderen Folgen.

Dabei war auch dieses Desaster schlimm genug. Spitäler mussten Operationen verschieben, Tausende Flüge fielen aus, auch Banken und zahlreiche andere Unternehmen waren betroffen. Das Ausmaß der finanziellen Schäden – und der Prozesslawine, die folgen könnte – lässt sich noch nicht einmal erahnen.

MGO

WIRTSCHAFTS RE©HT

diepresse.com/**wirtschaftsrecht**

Viele Haftungsfragen

Rechtsanwalt Philipp Zumbo, der bei Taylor Wessing CEE das Konfliktlösungs-Team leitet, nennt im Gespräch mit der „Presse" eine Reihe möglicher Haftungsbeziehungen und Rechtsansprüche, die für betroffene Firmen vor allem dann relevant werden können, wenn sie nicht hinreichend gegen Betriebsausfälle durch Cyberschäden versichert sind: gegenüber dem Softwareanbieter, sei es der Hersteller selbst oder ein IT-Provider, der die fehlerhafte Software verwendet hat. Gegenüber den Versicherern des jeweiligen Anbieters. Gegenüber den eigenen Leitungsorganen: Haben diese genug für die Cybersicherheit getan? Und nach dem Vorfall rasch genug reagiert? Selbst scheinbar Banales, wie die in Versicherungsbedingungen geforderte unverzügliche Schadensmeldung, könne da ein Thema sein. Umgekehrt können womöglich Forderungen von Kunden wegen entfallener Leistungen drohen.

Die Erfolgsaussichten bei alldem sind freilich schwer einschätzbar. Vieles hängt vom Einzelfall ab, zu etlichen Themen gibt es auch noch kaum Judikatur. So könnte sich die Frage stellen, inwieweit Unternehmen eine neue Software vor der breiten Anwendung hätten testen müssen. Dem einzelnen Anwender bzw. seinen Geschäftsleitern werde das Unterbleiben eines Tests wohl eher nicht vorwerfbar sein, wenn es um ein Update für Millionen von Computern geht, meint Zumbo. „Anders wäre es, wenn man z. B. keine Firewall hat, und es kommt zu einem Hackerangriff."

Aber auch die AGB von Softwareherstellern und -providern erschweren aktuell die Geltendmachung allfälliger Ansprüche. Diese enthalten üblicherweise umfangreiche Haftungsausschlüsse, in den AGB von Crowdstrike ist teilweise auch die Anwendbarkeit kalifornischen Rechts und die ausschließliche Zuständigkeit kalifornischer Gerichte festgeschrieben. Was jeweils gilt und inwieweit solche Klauseln rechtswirksam vereinbart sind, müsse im Einzelfall geprüft werden, sagt Zumbo.

AUF EINEN BLICK

Die Crowdstrike-Panne legte am 19. Juli weltweit rund 8,5 Millionen Windows-Computer lahm. Grund war ein fehlerhaftes Update für Sicherheitssoftware von Crowdstrike. Besonders gravierend waren die Folgen im Luftverkehr, aber z. B. auch Krankenhäuser, Banken, Supermärkte und Fernsehsender waren betroffen.

Wie schwer ist Verschulden?

Für die Wirksamkeit eines Haftungsausschlusses kommt es zudem auf die Qualität des Verschuldens an. Gegenüber Verbrauchern kann die Haftung für grobe Fahrlässigkeit nicht ausgeschlossen werden, während zwischen Unternehmen mitunter auch noch zwischen „einfacher" und „krasser" grober Fahrlässigkeit differenziert wird. Für Letztere lässt sich auch im B2B-Bereich die Haftung keinesfalls ausschließen. Aber wie werden Gerichte hier die Grenze ziehen? Auch da erscheinen Prognosen schwierig. Zahlt sich also eine Prozessführung überhaupt aus – oder ist der Ausgang zu ungewiss? Diese Frage werden sich Entscheidungsträger stellen müssen. Wichtig sei es dann auch, zu dokumentieren, wie man zu seiner Entscheidung gekommen ist, sagt Zumbo. Denkbar seien auch alternative Lösungsansätze – etwa dahingehend, dass man sich mit dem Provider auf einen Nachlass für die restliche Vertragslaufzeit einigt und die Vergangenheit ruhen lässt.

Das führt zu den Weichenstellungen für die Zukunft: Wie lassen sich ähnliche Vorfälle verhindern und Haftungsrisiken reduzieren? Nach diesem Vorfall seien die Anforderungen jedenfalls strenger zu sehen, sagt Zumbo.

Auf der technischen Seite gibt es laut Nimmerrichter zwei Stellschrauben: die Erhöhung der Softwarequalität und den Umgang mit Fehlern. „Da muss man robuster reagieren, um den Dominoeffekt zu verhindern." Vor allem in sensiblen Bereichen brauche es meist ein zweites, redundantes System. Wobei aber als Back-up nicht immer nur eine IT-Lösung infrage kommt. „Für manche Dinge sollte es als Plan B auch einen analogen Prozess geben", sagt Nimmerrichter. Zumindest bei Lebensnotwendigem sollte ein Mensch einspringen können. Auf der anderen Seite mag es Anwendungen geben, bei denen ein kurzzeitiger Ausfall verkraftbar ist und sich ein teures Back-up schlicht nicht lohnt.

Vorhandene Versicherungspolizzen seien jetzt ebenfalls zu prüfen, sagt Ivo Deskovic, Partner bei Taylor Wessing: Was ist gedeckt, wo sollte man nachverhandeln, wie teuer wäre eine Erweiterung des Schutzes, und zahlt sich das aus? Genauso sind Abläufe bei Vertragsabschlüssen zu hinterfragen: „AGB werden oft gar nicht gelesen und mit einem Klick akzeptiert", nennt Deskovic ein Beispiel. Auch da wird man künftig genauer hinschauen und zumindest versuchen müssen, etwa bei zu weitreichenden Haftungsausschlüssen nachzuverhandeln.

„Gurtpflicht für Cyberraum"

Aber auch EU-Regularien werden künftig eine größere Rolle spielen. Etwa die NIS2-Richtlinie, die bis 17. Oktober umgesetzt werden muss: Wäre sie früher gekommen, hätte sie das Desaster womöglich verhindert, meint Nimmerrichter. Unternehmen kritischer Sektoren sind demnach künftig verpflichtet, sich zu schützen – das liegt dann nicht mehr in deren freiem Ermessen. „NIS2 ist so etwas wie eine Gurtpflicht für den Cyberraum", sagt Nimmerrichter. Direkt betroffen seien in Österreich 3000 bis 5000 Unternehmen, ebenso die öffentliche Verwaltung. Da die kritischen Sektoren weit gefasst sind und direkt Betroffene auch ihre Lieferanten in die Pflicht nehmen müssen, berührt NIS2 einen großen Teil der Wirtschaft.

Eine weitere EU-Verordnung soll künftig Software- und Hardware-Hersteller stärker in die Pflicht nehmen (Cyber Resilience Act, CRA). Hersteller werden verpflichtet, Schwachstellen zu beheben und zu melden und ein Qualitätssicherungssystem für die Konzeption, Entwicklung, Endabnahme und Prüfung digitaler Produkte zu etablieren, erläutert Nimmerrichter. Bei Verstößen drohen empfindliche Strafen. Auch Importeure und Händler sind betroffen. Daher werden Produkte von US-Herstellern wie Crowdstrike, die in Europa vertrieben werden, ebenfalls erfasst sein. Auch Microsoft selbst werde sich um eine widerstandsfähigere Architektur des eigenen Betriebssystems Gedanken machen müssen, ist man bei Certitude überzeugt. Wann CRA in Kraft tritt, ist indes noch offen. Das EU-Parlament hat bereits zugestimmt, das Placet des Rats steht noch aus.