Luther.

# Rechtliche Implikationen des Crowdstrike-Vorfalls: Ein Weckruf für IT-Sicherheit

## Einleitung

Am vergangenen Freitag, dem 19. Juli, erschütterte ein schwerwiegender IT-Sicherheitsvorfall die digitale Welt. Ein fehlerhaftes Update der renommierten Sicherheitsfirma Crowdstrike für ihre Falcon-Software führte zu massiven Computerausfällen bei Unternehmen und Organisationen weltweit. Die Auswirkungen waren dramatisch: Flugzeuge blieben am Boden, Krankenhäuser mussten Operationen absagen, und zahlreiche Unternehmen sahen sich mit erheblichen Betriebsstörungen konfrontiert. Besonders betroffen waren Organisationen in den USA, Deutschland, Indien und Australien, was die globale Dimension dieses Vorfalls unterstreicht.

Dieser Beitrag beleuchtet nicht nur die Fakten des Vorfalls, sondern gibt Ihnen auch wertvolle Einblicke in die rechtlichen Implikationen. Zudem stellen wir konkrete Handlungsempfehlungen dar, die Unternehmen und Organisationen einen Leitfaden an die Hand geben sollen, wenn sie von einem Cybervorfall betroffen sind. Aus diesem Grund sind die Handlungsempfehlungen allgemein formuliert. In Zeiten zunehmender digitaler Vernetzung und Abhängigkeit von IT-Systemen zeigt dieser Vorfall einmal mehr, wie wichtig es ist, grundsätzlich auf solche Szenarien vorbereitet zu sein – sowohl technisch als auch rechtlich. Als Rechtsexperten wollen wir Sie über die möglichen rechtlichen Konsequenzen und Handlungsoptionen in Folge eines Cybervorfalls informieren.

## Was ist passiert?

Das am 19. Juli veröffentlichte Update der Crowdstrike Falcon-Sicherheitssoftware sollte ursprünglich die Schutzfunktionen der Software verbessern. Stattdessen führte es zu weitreichenden Systemausfällen bei den Kunden des Unternehmens. Da auch viele IT-Dienstleister diese Sicherheitssoftware einsetzen, kam es zu einer Kettenreaktion, weil die Systeme der IT-Dienstleister ausgefallen sind.

Crowdstrike Falcon, ein führendes Produkt für Enterprise Detection and Response (EDR), bietet umfassenden Schutz für Endgeräte in Unternehmensnetzwerken. Um seine Effektivität zu gewährleisten, nutzt Crowdstrike ein System kontinuierlicher Aktualisierungen. Diese Updates werden über sogenannte Channel-Dateien verteilt, die es ermöglichen, dynamische Verbesserungen und neue Detektionsregeln nahtlos an die installierten Falcon Sensoren zu übermitteln. Diese Falcon Sensoren sind auf Servern und Endgeräten installiert. Ein fehlerhaftes Update führte auf Windows-Systemen zu Abstürzen und dem sog. „Blue Screen of Death“.

Tausende von Organisationen weltweit meldeten Störungen, wobei Schätzungen von mehreren zehntausend betroffenen Systemen ausgehen. Crowdstrike reagierte innerhalb weniger Stunden mit einem Workaround. Dabei handelt es sich jedoch nicht um einen Notfall-Patch, der automatisiert in die betroffenen Systeme übernommen werden kann, sondern um eine Arbeitsanleitung für die IT-Verantwortlichen, wie die betroffenen Systeme zurückgesetzt werden können. Die IT-Verantwortlichen mussten dies dann für die betroffenen Systeme manuell umsetzen, was erhebliche Ressourcen in den betroffenen Unternehmen bindet.

Es wird vermutet, dass Crowdstrike das fehlerhafte Update nicht hinreichend getestet hat, bevor es veröffentlicht wurde und so die Fehlerursache übersehen hat. Auch wenn es sich bei dem Vorfall nicht um einen gezielten Cyberangriff handelte, zeigen die globalen Auswirkungen doch, wie fragil die IT-Welt sein kann. Besonders pikant ist, dass die Ursache durch eine Sicherheitssoftware ausgelöst wurde, die derartige Vorfälle eigentlich vermeiden sollte. Allerdings liegt darin wohl auch eine Ursache für die massiven Auswirkungen, denn Sicherheitssoftware hat in IT-Systemen häufig sehr weitgehende Rechte und Privilegien, damit reguläre Software überwacht und Bedrohungen eingedämmt und beseitigt werden können.

## Rechtliche Implikationen

Dieser Vorfall wirft eine Reihe komplexer rechtlicher Fragen auf. Ganz konkret geht es aktuell um die Frage der Verantwortung und Haftung von Crowdstrike für den massiven IT-Ausfall. Zwar sind noch keine genauen Zahlen bekannt, aber die Presse berichtet vom größten IT-Vorfall der Geschichte. IBM schätzt die Kosten eines Datenlecks in 2023 auf 4,3 Mio EUR (https://de.newsroom.ibm.com/2023-07-11_IBM-Bericht-Ein-Datenleck-kostet-deutsche-Unternehmen-durchschnittlich-4,3-Millionen-Euro). Zwar handelt es sich bei dem Crowdstrike-Vorfall nicht um ein Datenleck (soweit man aktuell weiß), aber die Dimension zeigt, welche finanzielle Dimension Cybervorfälle haben.

Crowdstrike könnte für Fahrlässigkeit bei der Entwicklung und Testung des Updates haftbar gemacht werden, wobei die Sorgfaltspflicht bei der Bereitstellung von Sicherheitssoftware besonders hoch ist. Auch IT-Dienstleister und sonstige Akteure könnten je nach Vertragslage für Schäden haftbar sein, die durch die nicht rechtzeitige Erkennung oder Behebung des Problems entstanden sind. Hier hängt es von den noch zu klärenden Detailfragen ab, ob nicht sogar grobe Fahrlässigkeit angenommen werden muss. Dies hätte u.a. auch Auswirkung auf das Eingreifen etwaiger Haftungsbeschränkungen. Zunächst muss geklärt werden, ob Regelungen in den Allgemeinen Geschäftsbedingungen mit Blick auf Rechtswahl und Gerichtsstand überhaupt wirksam sind. Haben Unternehmen individuelle Vereinbarungen getroffen, hängt es vom Einzelfall ab.

Soweit bekannt, ist es durch den Vorfall nicht zu einem Datenleck gekommen. Meldepflichten nach der DSGVO dürften danach nicht eingreifen. Dennoch kann das Datenschutzrecht regelmäßig auch Ansatzpunkt sein, um Ansprüche gegen einen IT-Dienstleister zu begründen. Wurde mit einem IT-Dienstleister ein Vertrag zur Auftragsverarbeitung geschlossen, kann dieser helfen, weitere Informationen über den Vorfall zu sammeln. Denn regelmäßig sehen diese Verträge Kontroll- und Auditmöglichkeiten vor. Ferner ist daran zu denken, dass das Ausspielen des fehlerhaften Updates einen Verstoß gegen die technischen und organisatorischen Maßnahmen darstellt. Denn datenschutzrechtlich ergeben sich mögliche Verletzungen der DSGVO-Vorgaben zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 DSGVO). Damit könnte eine Haftung auf Grundlage des Auftragsverarbeitungsvertrags begründet werden.

Aber auch betroffene Unternehmen könnten sich haftbar gemacht haben. Vertraglich könnte es zu Verletzungen von Service Level Agreements (SLAs) mit Kunden und Geschäftspartnern kommen, ebenso wie zu möglichen Verletzungen von Lieferverträgen oder anderen geschäftlichen Vereinbarungen aufgrund von Betriebsunterbrechungen. Betroffene Unternehmen könnten zudem haftbar sein, wenn sie keine angemessenen Notfallpläne hatten. Selbst wenn man scheinbar Opfer des Vorfalls war, stellt sich damit die Frage, ob man gegenüber den eigenen Kunden und Geschäftspartner nicht für Fehler haftet, die die eigenen IT-Sicherheitsmaßnahmen betreffen. Denn der Gesetzgeber in Deutschland und der Europäischen Union setzt die rechtlichen Anforderungen mit zahlreichen gesetzlichen Regelungen ständig höher. Zu nennen sind hier etwa die NIS2-Richtlinie, DORA oder etwas branchenspezifische Regelungen aus dem Digitalgesetz, die die IT-Sicherheitsanforderungen an Krankenhäuser und Arztpraxen erhöhen.

Für Unternehmen und Organisationen, die von einem Cybervorfall betroffen sind, ist es wichtig, Dauer und Ausmaß der Störungen sowie alle getroffenen Maßnahmen zur Problembehebung zu dokumentieren. Mit Blick auf spätere Schadenersatzforderungen sollten auch entstandene Schäden und Verluste quantifiziert werden. Dies gilt auch für die Arbeitszeit und konkret ausgeübten Tätigkeiten von Mitarbeitern, die nun in die Beseitigung des Schadens eingebunden sind.

Bei einem Cybervorfall sind zudem Melde- und Transparenzpflichten zu prüfen und zu beachten. Regelmäßig müssen zunächst die internen Meldewege absolviert werden und alle relevanten Funktionen (etwas IT-Sicherheit, Datenschutz, Rechtsabteilung, Kommunikation, HR) informiert werden. Zudem ist zu prüfen, ob und inwieweit Meldepflichten gegenüber Behörden bestehen, z.B. dem BSI oder den Datenschutzaufsichtsbehörden. Zudem sollte geklärt werden, ob und inwieweit Melde- und Informationspflichten gegenüber Kunden und anderen Geschäftspartner bestehen.

Unabhängig von einer rechtlichen Verpflichtung ist in jedem Fall zu klären, was und wie Mitarbeiter und Geschäftspartner informiert werden. Denn wird ein Unternehmen durch einen Cybervorfall lahm gelegt, dauert dies häufig mehrere Tage oder gar Wochen. Reagiert niemand auf E-Mails oder sind die Telefone nicht erreichbar, führt dies schnell zu Spekulationen. Soweit Sie eine Cyber-Versicherungspolice abgeschlossen haben, müssen Sie auch darin auf etwaige Informationspflichten achten. Schließlich ist – abhängig von der Art des Vorfalls – zu klären, ob Polizei und Sicherheitsbehörden informiert und eingebunden werden sollten. Dabei ist zu beachten, dass diese Unternehmen häufig auch umfangreiche Hilfestellung bieten.

Um sich besser vor ähnlichen Vorfällen in der Zukunft zu schützen, empfehlen wir die Implementierung eines mehrstufigen Sicherheitskonzepts, das nicht von einer einzelnen Lösung abhängig ist, sowie die Etablierung eines strukturierten Prozesses für Software-Updates, einschließlich Tests in einer isolierten Umgebung vor der breiten Ausrollung, soweit dies aufgrund der technischen Abhängigkeiten der Softwarelösung möglich ist. Entwickeln Sie detaillierte Notfallpläne für verschiedene Szenarien und implementieren Sie ein robustes Backup-System mit regelmäßigen Tests zur Wiederherstellung.

## Auswirkungen

Der Crowdstrike-Vorfall könnte weitreichende Auswirkungen auf die IT-Sicherheitsbranche und das regulatorische Umfeld haben. Es ist mit einer Verschärfung der Auflagen für Sicherheitssoftware-Anbieter zu rechnen, insbesondere in Bezug auf Testverfahren und Qualitätssicherung. Zudem könnte es zu einer Zunahme von Gerichtsverfahren zur Klärung von Haftungsfragen bei IT-Sicherheitsvorfällen kommen, die möglicherweise Präzedenzfälle zur Produkthaftung bei Sicherheitssoftware schaffen werden. Es ist auch zu erwarten, dass Betrüger und Cyberkriminelle den Vorfall nutzen, um Geld zu

erlangen. Insoweit sollten entsprechende Anfragen kritisch gewertet werden.

Zudem stellen sich Fragen zur Abhängigkeit von Big-Tech Unternehmen. Lina Kahn, die Chefin der amerikanischen FTC, setzt sich sehr für eine Aufspaltung der marktmächtigen Big Tech Unternehmen ein. Im Zuge des Crowdstrike-Vorfalls hat sie sich auf der Plattform X entsprechend positioniert.

Als Experten für IT-Recht und Datenschutz stehen wir Ihnen bei der Bewältigung der rechtlichen Herausforderungen im Zusammenhang mit dem Crowdstrike-Vorfall und ähnlichen IT-Sicherheitsproblemen zur Seite. Unser Leistungsangebot umfasst die rechtliche Analyse und Bewertung Ihrer individuellen Situation, Unterstützung bei der Kommunikation mit Behörden, Geschäftspartnern und Kunden, Beratung zur Optimierung Ihrer Verträge und AGBs sowie die Vertretung Ihrer Interessen in Verhandlungen und vor Gericht. Gemeinsam können wir die restlichen Herausforderungen im dynamischen Umfeld der IT-Sicherheit meistern, Ihr Unternehmen bestmöglich schützen und Ihre Ansprüche bestmöglich geltend machen.

Zögern Sie nicht, uns zu kontaktieren, wenn Sie Fragen haben oder Unterstützung benötigen. Gemeinsam können wir die rechtlichen Herausforderungen im dynamischen Umfeld der IT-Sicherheit meistern und Ihr Unternehmen bestmöglich schützen.

## Ihre Ansprechpartner:


**Christian Kuss, LL.M.**
Rechtsanwalt, Partner
Köln
T +49 221 9937 25686
christian.kuss@luther-lawfirm.com

**Dr. Richard Happ**
Rechtsanwalt, Partner
Hamburg
T +49 40 18067 12766
richard.happ@luther-lawfirm.com

**Katharina Klenk-Wernitzki, Dipl. Reg.-Wiss**
Rechtsanwältin, Partnerin
Berlin
T +49 30 52133 25741
katharina.klenk@luther-lawfirm.com

**Dr. Michael Rath**
Rechtsanwalt, Partner
Köln
T +49 221 9937 25795
michael.rath@luther-lawfirm.com

**Tim Rauschning**
Rechtsanwalt, Partner
Hamburg
T +49 40 18067 15999
tim.rauschning@luther-lawfirm.com

**Franziska Neugebauer**
Rechtsanwältin, Senior Associate
Köln
T +49 221 9937 25790
franziska.neugebauer@luther-lawfirm.com