TaylorWessing

Nichts ging mehr:

Weltweiter Computerstillstand wirft viele rechtliche Fragen auf

Antworten für betroffene Unternehmen

Freitag, 19. Juli 2024 wird wohl in die Geschichte eingehen: Auf Grund eines fehlerhaften Codes in einem CrowdStrike Update standen weltweit Millionen Computer still. Betroffen waren unter anderem Flughäfen, Banken, Telekommunikationsunternehmern, Krankenhäuser und Rundfunksender. Die Konsequenzen des Vorfalls dauern zum Teil immer noch an.
Der bisher wohl größte Cyber-Vorfall bringt ein immenses juristisches Nachspiel mit sich und wirft zahlreiche Fragen auf. Die Experten der Disputes & Investigations und IT-Teams der internationalen Sozietät Taylor Wessing, Philipp Zumbo, Ivo Deskovic und Andreas Schütz, setzen sich mit der Thematik auseinander und haben Antworten.

1. Wer haftet den betroffenen Unternehmen für Umsatzausfälle?

In jenen Fällen, in denen CrowdStrike der direkte Vertragspartner der betroffenen Unternehmen ist und keine (hinreichende) Versicherungsdeckung für nicht böswillige Cyber-Angriffe besteht, müssten die Unternehmen versuchen, direkt gegen CrowdStrike bzw. deren Versicherer vorzugehen.

Philipp Zumbo, CEE Head of Disputes & Investigations bei Taylor Wessing, weiß: „Das ist für österreichische Unternehmen vor allem deswegen schwierig, weil sich in den AGB von CrowdStrike nicht nur umfangreiche Haftungsausschlüsse finden. In einem Teil der AGB von CrowdStrike wird auch die Anwendbarkeit Kalifornischen Rechts und die ausschließliche Zuständigkeit Kalifornischer Gerichte vereinbart. Das gilt aber nicht unbedingt. Welche AGB zwischen CrowdStrike und den betroffenen Unternehmen gelten, und ob diese wirksam vereinbart wurden, ist in jedem Einzelfall gesondert zu prüfen“.

Ist der Vertragspartner hingegen ein anderes (EU-)Unternehmen, das die CrowdStrike-Software – etwa als Plug-In – für seine eigene Sicherheitssoftware einsetzt, wären Ersatzansprüche primär gegenüber diesem Unternehmen zu prüfen. Auch in diesen Fällen sind vorab das anwendbare Recht, die Gerichtszuständigkeit und allfällige Haftungsbeschränkungen zu klären.

2. Müssen betroffene Unternehmen ihren Kunden in jedem Fall Schadenersatz leisten?

Nein. Bei Flugausfällen etwa stellt sich die Rechtslage als komplex dar, weil nach der Fluggastrechteverordnung zwar in der Regel ein Anspruch auf einen Ersatztransport besteht, andererseits aber eine Ausgleichszahlung entfällt, wenn die Annullierung des Fluges aufgrund „außergewöhnlicher Umstände“ erfolgt. Technische Probleme sind zwar in der Regel keine außergewöhnlichen Umstände. Wenn aber der Flugausfall auf ein technisches Problem des Flughafens zurückzuführen ist, dann entfällt die Haftung der Fluglinie im Regelfall.
Überdies enthalten zahlreiche AGB von betroffenen Unternehmen Haftungsausschlüsse für (leicht) fahrlässig verursachte (Folge-)Schäden und unabwendbare Ereignisse. „Ob ein solcher Fall tatsächlich vorliegt, ist für jedes Vertragsverhältnis gesondert zu prüfen. Die genannten Haftungsbeschränkungen sind zumindest im B2B-Bereich regelmäßig weitgehend wirksam. Im B2C-Bereich stellt sich dies eher umgekehrt dar“, so Ivo Deskovic, Partner im Taylor Wessing Disputes & Investigations Team.

3. Wie sieht es mit indirekt betroffenen Unternehmen aus (Kunden/Lieferanten von direkt betroffenen Unternehmen)?

Indirekt betroffene Unternehmen stehen vor dem Problem, dass sie die erforderlichen Vorleistungen von den direkt Betroffenen nicht erhalten, aber ihrerseits gegenüber den eigenen Kunden eine Leistungspflicht erfüllen müssen. Während sich die Endkunden, vor allem wenn sie Verbraucher sind, bei den indirekt betroffenen Unternehmen regelmäßig weitgehend schadlos halten können, müssen diese gegen ihre oft im Ausland befindlichen Vertragspartner – oder direkt gegen CrowdStrike bzw. deren Versicherer – vorgehen.

4. Gibt es Tipps für direkt/indirekt betroffene Unternehmen?

Zunächst sollten die bestehenden Vereinbarungen mit den betroffenen Vertragspartnern geprüft werden. An bestehende Versicherungen sollten Deckungsanfragen gestellt werden. Dabei ist Eile geboten: Viele Versicherungsverträge sehen die Leistungsfreiheit des Versicherers vor, wenn die Versicherungsmeldung nicht unverzüglich erfolgt; man spricht in einem solchen Fall von einer Obliegenheitsverletzung.

5. Die Wahrscheinlichkeit, dass sich solche Vorfälle wiederholen werden, ist groß. Gibt es Tipps, um als Unternehmen künftig für solche Vorfälle gewappnet zu sein?

IT Partner Andreas Schütz rät: „Unternehmen sollten für zukünftige Vorfälle Fallback-Lösungen entwickeln oder bereits bestehende Systeme, die das Risiko einer Kompromittierung oder eines vollständigen Ausfalls der operativen Tätigkeit möglichst reduzieren, ausbauen. Darüber hinaus ist es empfehlenswert, neben der Etablierung paralleler Systeme zur Risikostreuung den Abschluss einer Cyberversicherung zu prüfen und bestehende Versicherungsdeckungen allenfalls zu erhöhen. Dabei sollte auch beachtet werden, dass je nach Polizze gegebenenfalls Wartefristen für Betriebsunterbrechungen von einigen Stunden bestehen."

Für Rückfragen zuständig:
***Mag. Ivo Deskovic**, i.deskovic@taylorwessing.com*
***Dr. Philipp Zumbo**, p.zumbo@taylorwessing.com*