Das IT-Sicherheitsgesetz 2.0 und seine Auswirkungen auf die Cyber-Versicherung

Dr. Herbert Palmberger,
Rechtsanwalt,
Heuking Kühn Lüer Wojtek PartGmbB

Ausgangslage

Unmittelbar vor den Weihnachtsferien hat das Bundeskabinett am 16. Dezember 2020 den Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme („IT-Sicherheitsgesetz 2.0") beschlossen und dem Bundestag zur Billigung vorgelegt. Nach der parlamentarischen Befassung ist somit im Laufe des Jahres 2021 mit dem Inkrafttreten zu rechnen.

Das IT-Sicherheitsgesetz 2.0 baut auf dem bestehenden IT-Sicherheitsgesetz vom 17. Juli 2015 auf und erweitert den dort geschaffenen Ordnungsrahmen ganz erheblich. Insbesondere werden die Rolle und die Befugnisse des Bundesamts für Sicherheit in der Informationstechnik (BSI) ebenso ausgeweitet wie die Anwendbarkeit des neuen Gesetzes auf Industriezweige außerhalb der Telekommunikation und Telemedien oder die Etablierung des Verbraucherschutzes als zusätzliche Aufgabe des BSI.

Anwendungsbereich

Das ursprüngliche IT-Sicherheitsgesetz geht im Kern davon aus, Mindeststandards für die Stellen des Bundes zu setzen. Zukünftig sollen dieselben Standards auch für IT-Dienstleister gelten, die Dienstleistungen für die Kommunikationstechnik des Bundes erbringen. Weiterhin soll eine Anordnungsbefugnis des BSI gegenüber Telekommunikations- und Telemediendienstanbietern zur Abwehr spezifischer Gefahren für die Informationssicherheit geschaffen werden.

Hinzu kommt allerdings, dass die bereits nach dem ersten IT-Sicherheitsgesetz bestehenden Meldepflichten und verpflichtenden Mindeststandards für Betreiber der sogenannten Kritischen Infrastruktur (KRITIS) auf weitere Teile der Wirtschaft ausgeweitet werden, insbesondere auf Unternehmen von besonderem öffentlichen Interesse. Durch eine Rechtsverordnung soll weiterhin konkretisiert werden, welche Unternehmen eine besondere volkswirtschaftliche Bedeutung haben, die dann ebenfalls in den Kreis der Verpflichteten einbezogen werden sollen.

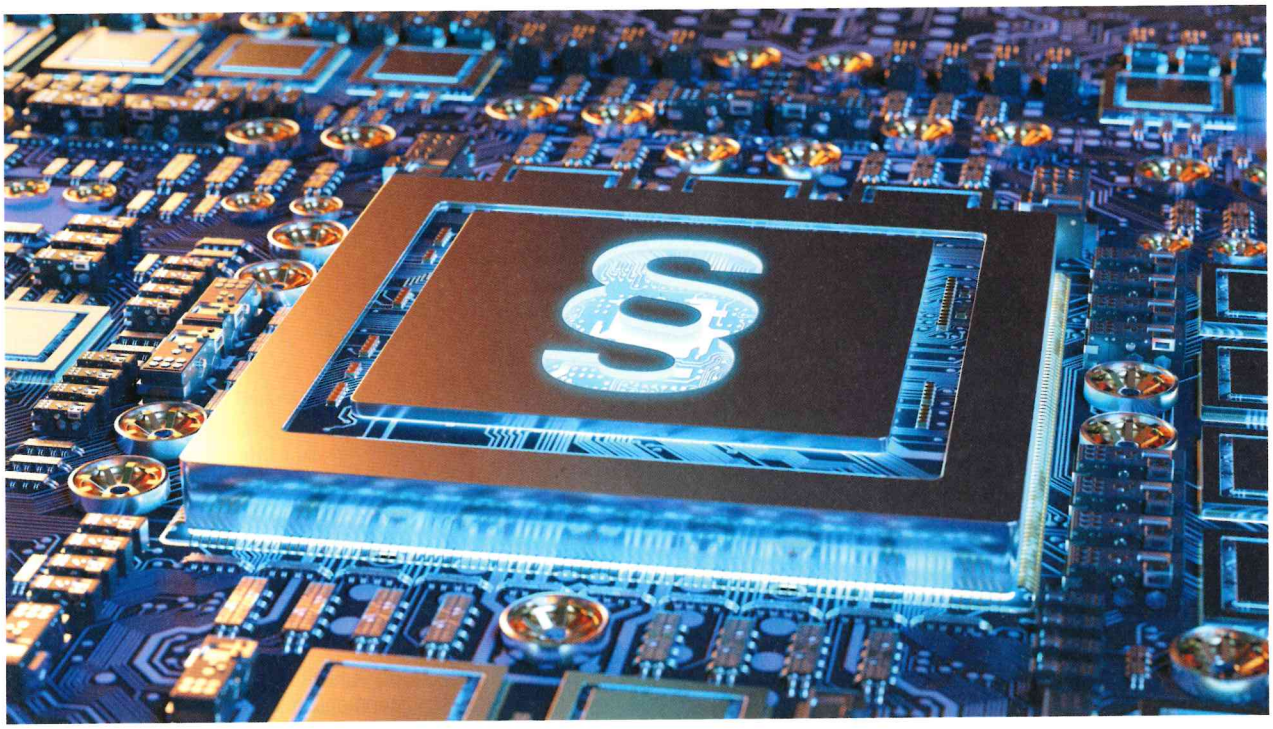
Hier kommt also einiges auf die versicherungsnehmende Wirtschaft zu. Neben beispielsweise Rüstungsunternehmen oder Herstellern von IT-Produkten für die Verarbeitung staatlicher Verschlusssachen, Unternehmen der Siedlungsabfallwirtschaft, der Energie- und Wasserversorgung denkt der Gesetzgeber bei dem Kriterium des besonderen öffentlichen Interesses auch an die besondere volkswirtschaftliche Bedeutung sowie an die hohe Wertschöpfung, die zahlreiche weitere Unternehmenszweige erzielen. Die Berechnungsmethodik soll sich an den Gutachten der Monopolkommission gemäß § 44 Abs. 1 GWB orientieren, in denen alle zwei Jahre die 100 größten Unternehmen Deutschlands nach inländischer Wertschöpfung ermittelt werden. Die Unternehmen sollen nach der amtlichen Gesetzesbegründung dann selbst ermitteln, ob sie von den Regelungen des IT-Sicherheitsgesetzes 2.0 betroffen sind, wobei die Berechnungsmethodik und ein Schwellenwert in der zukünftigen Rechtsverordnung aufgrund des Gesetzes noch spezifiziert werden sollen.

Auswirkungen

Die Wirkung der Regelungen des IT-Sicherheitsgesetzes 2.0 für die betroffenen Unternehmen hängen eng mit den Befugnissen des BSI zusammen. Letztere werden stark ausgeweitet. Die Unternehmen müssen teils erheblichen Aufwand betreiben, um den Anforderungen gerecht zu werden, und Verstöße werden durch ebenfalls ausgeweitete Bußgeldregelungen sanktioniert. Bisher ging der Strafrahmen bis EUR 100.000,00 je Verstoß. In Angleichung an die EU-DSGVO sind nun Geldbußen von bis zu EUR 20 Mio. oder bis zu 4 % des gesamten weltweit erzielten Unternehmensumsatzes des vorangegangenen Geschäftsjahres vorgesehen, je nach dem, welcher der Beträge höher ist. Auf die leichte Schulter ist so etwas nicht zu nehmen.

Das BSI hat auf der einen Seite die Möglichkeit, Meldepflichten durchzusetzen, aber es soll auch weitgehende Anordnungsbefugnisse erhalten, und zwar insbesondere gegenüber Telekommunikations- und Telemediendienstanbietern. Damit sollen spezifische Gefahren für die Informationssicherheit umfassend abgewehrt werden. Das kann so weit gehen, dass der Einsatz von Komponenten, bei denen Störungen zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktion oder Integrität der sogenannten Kritischen Infrastrukturen führen können, durch das BSI untersagt wird. Gleichzeitig können die Hersteller von kritischen Komponenten zu umfassenden Garantieerklärungen verpflichtet werden.

Begleitet werden diese Pflichten und Maßnahmen von umfassenden Meldepflichten gegenüber dem BSI. Weiterhin müssen insbesondere Anbieter von Telekommunikationsdiensten mit mehr als 100.000 Kunden im ständigen tagesaktuellen Prozess auf Anordnung des BSI Malware-Domänen sperren, um infizierte Nutzersysteme zu schützen. Die Unternehmen können auf Anordnung durch das BSI sogar dazu gezwungen werden, den Datenverkehr auf vom BSI genannte Adressen umzuleiten. Alle Betreiber



Kritischer Infrastrukturen müssen zudem Systeme zur Angriffserkennung einsetzen und entsprechende Daten für mindestens vier Jahre speichern. Während bisher gegenüber dem BSI nur eine Kontaktstelle benannt werden musste, soll nun eine Registrierung als Betreiber Kritischer Infrastrukturen erfolgen. Wiederum im Bereich Telekommunikationsnetze und -dienste dürfen kritische Komponenten nur eingesetzt werden, wenn sie ein Zertifizierungsverfahren durchlaufen haben. Das Zertifizierungsverfahren wiederum muss eng durch die Hersteller der kritischen Komponenten begleitet werden.

Hinzukommt, dass der Verbraucherschutz neu in den Zuständigkeitskatalog des BSI aufgenommen wird. Das wiederum hat weitere Auswirkungen auf Meldepflichten, vorbeugende Maßnahmen und den operativen Teil der Unternehmensaktivitäten im IT-Bereich. Zwischen BSI, Herstellern und Diensteanbietern soll ein kontinuierlicher Verbraucherschutzdialog etabliert werden. Zum Schutz der Verbraucher soll ein IT-Sicherheitskennzeichen für verbrauchernahe Produkte und Dienste eingeführt werden. Dessen Verwendung ist zwar freiwillig, aber schon aus Konkurrenzgründen wird kein Unternehmen darauf verzichten können. Den damit verbundenen Aufwand trägt das Unternehmen ebenso wie die Verantwortung für die damit verbundenen Aussagen.

Gravierend erscheint in diesem Zusammenhang die gesetzlich vorgesehene Unterstützung von Abmahnungen und Klagen bei verbraucherrechtswidrigen Praktiken – welche das auch immer sind – durch das BSI. Dabei setzt das BSI seine fachliche Expertise im Bereich der IT-Sicherheit ein, aber es hat darüber hinaus auch die Befugnis, informationstechnische Produkte zu untersuchen und die hieraus gewonnenen Erkenntnisse für Abmahn- und Klagezwecke weiterzugeben sowie in Fragen der Sicherheit der Informationstechnik zu beraten und bei der Durchsetzung von Ansprüchen zu unterstützen.

Schließlich, aber keineswegs letztlich ist auf die für die Betreiber Kritischer Infrastrukturen ausdrücklich eingeführte Pflicht hinzuweisen, spätestens innerhalb eines Jahres nach Inkrafttreten des neuen Gesetzes Systeme zur Angriffserkennung einzurichten und zu unterhalten.

Versicherungsaspekte

Das IT-Sicherheitsgesetz 2.0 bringt für Unternehmen erhebliche Verpflichtungen mit sich, deren Nichteinhaltung zu gravierenden Schäden führen kann. Ansprüche im Haftpflichtbereich gegen betroffene Unternehmen sind in diesem Zusammenhang vielfältiger Natur, insbesondere dann, wenn Dritten durch die Nicht- oder Schlechterfüllung der normierten Pflichten ein Schaden entsteht. Gefahrenpotential entsteht dabei neu durch den im Gesetz ausdrücklich festgeschriebenen Verbraucherschutz. Weiterhin können Maßnahmen des BSI zu Betriebsunterbrechungen führen, die für das betroffene Unternehmen selbst ebenso wie für Dritte erhebliches Schadenpotential in sich bergen.

Für die Cyberversicherung heißt das, dass die einzelnen Haftungs- und Schadensszenarien erfasst und je nach Deckung in die Bedingungen einzuarbeiten sind. Teilweise sind die neuen Risiken auch über die Betriebshaftpflichtversicherung zu decken, ebenso über die Betriebsunterbrechungsversicherung. Zudem wird – wieder einmal – die D&O-Versicherung in Betracht zu ziehen sein, denn gerade auf die Unternehmensleiter kommen zahlreiche neue und umfängliche Pflichten zu, die zu ihrer persönlichen Inanspruchnahme führen können, wenn diese Pflichten mangelhaft erfüllt werden.

Versicherungsunternehmen und Vermittler sind in besonderem Maße gefordert, die Versicherungsbedingungen an die neue Rechtslage anzupassen. Wie oben ausgeführt, betrifft dies nicht nur die – wie auch immer ausgestaltete – Cyberversicherung, sondern ebenfalls die Haftpflicht- und Sachversicherungen außerhalb von speziellen Cyber-Deckungskonzepten. ■