Das Cybersicherheits-gesetz der VR China

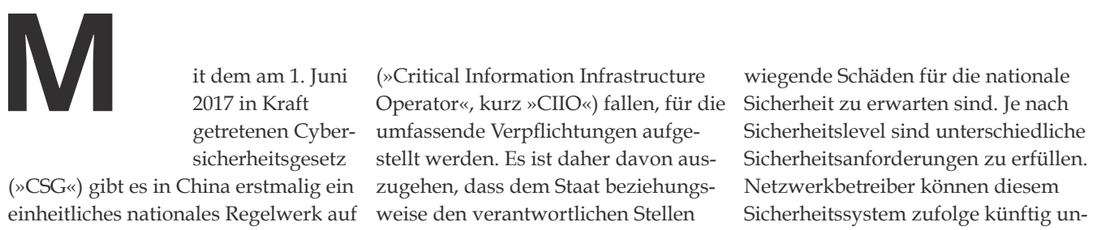
Mit dem am 1. Juni 2017 in Kraft getretenen Cybersicherheitsgesetz (»CSG«) gibt es in China erstmalig ein einheitliches nationales Regelwerk auf dem Gebiet der Cybersecurity. Nach der Intention des chinesischen Gesetzgebers soll durch das neue Gesetz Internetsicherheit gewährleistet werden, nationale Souveränität gesichert sowie die Rechte einzelner geschützt werden. Grundsätzlich ist der Vorstoß der chinesischen Regierung, sich dem Bereich Internetsicherheit auf nationaler Ebene anzunehmen, positiv zu bewerten. Das Gesetz wird jedoch aus deutscher Sicht nicht nur zu Verbesserungen führen, vielmehr ist es mit weitreichenden Verpflichtungen und Einschränkungen auch für deutsche Unternehmen verbunden, die in China geschäftlich aktiv sind. Ein Manko ist bereits die unpräzise Ausgestaltung des Gesetzes, die zu Rechtsunsicherheiten führt. Es mangelt an gesetzlichen Definitionen für wichtige Begrifflichkeiten, so ist zum Beispiel unklar, welche Unternehmen unter den Anwendungsbereich der Netzwerkbetreiber kritischer Infrastruktur (»Critical Information Infrastructure Operator«, kurz »CIIO«) fallen, für die umfassende Verpflichtungen aufgestellt werden. Es ist daher davon auszugehen, dass dem Staat beziehungsweise den verantwortlichen Stellen großer Beurteilungsspielraum und damit Einfluss bei der Gesetzesanwendung zusteht. Im Folgenden ein Überblick über einige Neuerungen, auf die sich die deutsche Wirtschaft einstellen muss.

Verpflichtungen für Netzwerkbetreiber

Nach dem CSG soll ein sogenanntes mehrschichtiges Sicherheitsnetz (»multi-level-protection-scheme«) zur Sicherstellung von Netzwerk- und Datensicherheit eingeführt werden. Im Juli diesen Jahres ist der Entwurf von Regelungen zu dessen Umsetzung erschienen. Die Einstufung erfolgt je nach Schwere der potenziellen Folgen, die bei einem Schaden des Netzwerksystems eintreten können. So sind Netzwerksysteme beispielsweise in die höchste Stufe, Stufe 5, einzuordnen, wenn schwerwiegende Schäden für die nationale Sicherheit zu erwarten sind. Je nach Sicherheitslevel sind unterschiedliche Sicherheitsanforderungen zu erfüllen. Netzwerkbetreiber können diesem Sicherheitssystem zufolge künftig unter anderem verpflichtet werden, einen Verantwortlichen für Internetsicherheit zu bestimmen und bestimmte technische Maßnahmen zur Gewährleistung interner Netzwerksicherheit zu ergreifen. Der Begriff »Netzwerkbetreiber« wird im CSG dabei nicht definiert. In Ansehung der bisherigen bestehenden Richtlinien ist von einem breiten Anwendungsbereich auszugehen; unter den Begriff könnten alle Betreiber fallen, die Datenverarbeitungssysteme in China betreiben oder nutzen.

Kritische Infrastruktur

Betreiber kritischer Infrastrukturen müssen weitergehende Verpflichtungen erfüllen. Im CSG werden als CIIO beispielhaft die Industriezweige Kommunikation, Energie, Transport, Wasserversorgung, Finanzen und öffentliche Dienstleistungen aufgezählt. Weiterhin werden unter dem Begriff der kritischen Infrastruktur diejenigen Bereiche erfasst, die die nationale Sicherheit, Wirtschaft oder öffentliche Interessen gefährden könnten. Es ist damit kaum eine klare Aussage zu treffen, welche Unternehmen genau unter den Anwendungsbereich fallen. Betreiber kritischer Infrastrukturen müssen unter anderem regelmäßige Trainings für ihre Mitarbeiter im Bereich Cybersecurity durchführen, Notfallpläne erstellen für Vorfälle im Bereich Datensicherheit sowie von wichtigen Systemen und Datenbeständen Backups erstellen.



Datentransfer

Der Datentransfer ins Ausland wird durch das CSG stark eingeschränkt. Künftig müssen alle personenbezogenen Daten in China gespeichert werden, ein Transfer ins Ausland ist nicht ohne weiteres möglich. Unternehmen, die während des Betriebs von Critical Information Infrastructure Daten sammeln, müssen diese ebenfalls in China speichern. Wichtige Daten können nur ins Ausland transferiert werden, wenn dies aus geschäftlichem Anlass notwendig ist und eine Sicherheitsüberprüfung durchgeführt wird. Der Datentransfer kann verweigert werden, wenn aus Sicht der zuständigen Behörde Schäden für die Sicherheit, Wirtschaft oder andere Interessen zu befürchten sind. Es ist aus dem Gesetz jedoch nicht ersichtlich, welche Daten unter den Begriff »wichtige Daten« fallen werden.

Netzwerkprodukte und Netzwerkdienstleistungen

Auswirkungen ergeben sich auch für Anbieter von Netzwerkprodukten, die beim Verkauf ihrer Produkte nach China die Anforderungen nationaler Standards erfüllen müssen. Netzwerkprodukte und -dienstleistungen, die für den Bereich kritischer Infrastrukturen genutzt werden, müssen zuerst einer offiziellen behördlichen Sicherheitsprüfung standhalten. Wie genau diese Sicherheitsprüfung ausgestaltet sein soll, ist im Gesetz nicht geregelt. Es ist zu befürchten, dass chinesische Standards erwartet werden, und nicht internationale. Weiterhin sollen Anbieter von Netzwerkdienstleistungen ihre Sicherheitsprodukte fortlaufend warten und ihre Kunden über potenzielle Gefahrenquellen aufklären.

Abschaltung von VPN-Tunneln

Neben den Neuerungen durch das CSG ist das Bestreben der chinesischen Regierung, nun auch die sogenannte Virtual Private Networks, VPN-Verbindungen, mehr und mehr unter staatliche Kontrolle zu bringen, kritisch zu sehen. VPN-Lösungen sind für ausländische Unternehmen in China essenziell. VPN werden eingesetzt für die Umgehung der chinesischen Firewall, die schon seit geraumer Zeit Internetseiten wie Google, Facebook, WhatsApp & Co. blockt. VPN-Lösungen sind für die interne Firmenkommunikation, die sichere Übertragung sensibler Daten sowie zum Beispiel für Fernwartungen von Maschinen und Anlagen von großer Bedeutung. Ist eine Anlage, die ein deutscher Anlagenbauer nach China verkauft hat, defekt und muss gewartet werden, kann sich das deutsche Unternehmen über einen VPN-client auf die Anlage schalten und so Probleme lösen oder Änderungen vornehmen. Die chinesische Regierung hat in den letzten Jahren ihre »Souveränität im Internet« immer weiter ausgebaut. Für Februar diesen Jahres war von der chinesischen Regierung angekündigt, dass nur noch solche VPN-Tunnel erlaubt sein würden, die staatlich lizenziert und zugelassen worden sind. Dies ist bislang nicht der Fall, jedoch bleibt abzuwarten wie sich das Thema rund um die VPN-Verbindungen weiter entwickelt.

Fazit

Das Cybersicherheitsgesetz bringt weitreichende Änderungen mit sich. Auf deutsche Unternehmen kommen teilweise größere finanzielle Belastungen zu, um die Compliance-Anforderungen zu erfüllen. Sollten VPN-Tunnel in Zukunft nicht mehr genutzt werden können, sind alternative Lösungen ebenfalls mit teilweise hohen Kosten verbunden. Die Restriktionen und Vorschriften erschweren zudem den Geschäftsverkehr mit der wichtigen Wirtschaftsmacht China. Es ist deutschen Unternehmen zu raten, sich bestmöglich zu informieren, unter welchen Anwendungsbereich sie fallen und welche Verpflichtungen erfüllt werden müssen, da sonst mit empfindlichen Strafen gerechnet werden muss.

AUTOR
Dr. Björn Etgen gehört mit über 20 Jahren Erfahrung zu den Pionieren in der Rechtsberatung deutscher Unternehmen in China. Zu den Schwerpunkten seiner Tätigkeit zählen die Beratung von Direktinvestitionen sowie M&A-Transaktionen in und aus China. Daneben ist Herr Dr. Etgen als Schiedsrichter bei verschiedenen chinesischen und internationalen Schiedsinstitutionen zugelassen. Herr Dr. Etgen hat den Beitrag zusammen mit Marie-Therese Schnappauf verfasst, die jüngst eine Praktikumsstation im Büro von GVW Shanghai absolviert hat.