Dr. Dennis-Kenji Kipker

Lichter aus im Tunnel?

Neue rechtliche Wege und Umwege nach China

Düstere Prognosen bis hin zur flächendeckenden Abschaltung von VPN-Tunneln: Das neue "Cyber-Sicherheitsgesetz", das seit Juni 2017 in der Volksrepublik China gilt, hat während der vergangenen Monate in deutschsprachigen Medien und Blogs erneut für große Aufregung gesorgt.

Keine unabhängigen VPNs mehr für ausländische Firmen, Organisationen und Personen, dazu strenge Kontrollen von IT-Hardware - das chinesische Cyber-Sicherheitsgesetz (Cyber Security Law, CSL) schien es in sich zu haben. Von erheblichen wirtschaftlichen Konsequenzen für transnational operierende deutsche Unternehmen war teilweise die Rede, bis hin zur Entwertung kompletter Geschäftsmodelle, die zwingend auf abgesicherte Kommunikationsverbindungen angewiesen sind. In der Tat enthält das Gesetz vom Wortlaut her potenziell gravierende Neuregelungen für VPN-Verbindungen und die IT-Sicherheitszertifizierung - gleichwohl hat sich für Unternehmen und auch Privatpersonen bisher deutlich weniger verändert, als pessimistische Beobachter zunächst vermuteten.

"Blackbox" China

Dass die VR China in Sachen Gesetzgebung für viele Unternehmen eine Blackbox ist, kommt nicht von ungefähr: Unabhängig von politischen Fragen erschwert vor allem die Sprachbarriere den Zugang für Außenstehende. Doch das CSL ist auch für des Chinesischen mächtige Insider eine harte Nuss. Der Gesetzgeber hat es als

umfassende Regelung zur Verbesserung der landesweiten IT-Sicherheit konzipiert und mit zahlreichen Neuerungen ausgestattet. Damit einher gehen bisher ungekannte behördliche Befugnisse und einschneidende Maßnahmen für weltweit vernetzte Unternehmen.

Für Verstöße sieht das Gesetz bisweilen schwere Strafen vor, wie zum Beispiel die Verhängung lebenslanger Berufsverbote bei erheblichen IT-Sicherheitsverletzungen. Hinzu kommt, dass viele der im CSL benutzten Formulierungen und Begriffe zur Zeit noch nicht ausreichend konkretisiert sind. Deshalb haben einige Beobachter Beunruhigendes in sie hineingelesen - was insbesondere dann ein Problem darstellt, wenn man als Außenstehender keine umfassenden Kenntnisse der Rechtswirklichkeit und derzeitigen politischen Ziele der VR China hat.

VPN: Mehr Gerüchte als Fakten

Zunächst einmal enthält das CSL an keiner Stelle konkrete gesetzliche Ermächtigungsgrundlagen für strenge Maßnahmen gegen nicht-chinesische VPN-Netzwerke. Es beschreibt lediglich verschiedene generalklauselartig formulierte Tatbestände, in die man die Abschaltung von VPN-Tunneln hineinlesen könnte. Dazu gehören zum Beispiel die "Bekämpfung gesetzeswidrigen Cyberverhaltens" oder "zeitweilige Maßnahmen/Beschränkungen der Netzwerkkommunikation in bestimmten Regionen". Allein darauf eine belastbare Aussage zu treffen, ist jedoch fragwürdig. Letztlich müssten dann neben dem CSL auch die zahllosen gesetzlichen und untergesetzlichen Vorgaben aus dem älteren chinesischen IT-Recht anders als bisher verstanden werden. Die "Computer Information System Security Regulations" von 1994 etwa greifen in ihren Formulierungen zum

Teil ähnlich weit und hätten damit schon vor dem CSL Anlass zur Sorge vor restriktiven Maßnahmen geboten.

Befragt wurden im Zusammenhang mit der gesetzlichen Neuregelung aber auch verschiedene Unternehmen unterschiedlicher Größe, die VPN-Verbindungen nach China nutzen. Das Ergebnis war stets dasselbe: Niemand gab an, dass als unmittelbare und vermutete Folge der neuen chinesischen Vorschriften ein Tunnel abgeschaltet worden sei.

Verlässliche Quellen von chinesischer Seite sehen die Situation ähnlich. Von ihnen hieß es, dass die technische Entwicklung durch das CSL nicht behindert werden solle. Alles in allem ist die bevorstehende Abschaltung von VPN-Tunneln nach China in großem Stil daher zur Zeit mehr Gerücht als Fakt. Auch ausländische und einheimische Privatpersonen lässt das CSL in der VR China prinzipiell weiterhin auf gängige VPN-Verbindungen zugreifen, solange solche Personen nicht gegen andere Gesetze verstoßen.

Strenge Regeln für IT-Importe

Nicht nur Daten fließen von und nach China, sondern auch IT-Erzeugnisse werden dorthin eingeführt. Laut CSL müssen zukünftig eine oder mehrere Behörden "kritische Netzwerkausrüstung" und "spezifische Cybersicherheitsprodukte" überprüfen und zertifizieren, bevor sie auf dem chinesischen Markt vertrieben oder innerhalb Chinas eingesetzt werden dürfen.

Welche Ausrüstung und Produkte gemeint sind, spezifizierten die Cyberspace Administration of China (CAC), das Ministry of Industry and Information Technology (MIIT), das Ministry of Public Security (MPS) sowie die Certification

and Accreditation Administration of China (CNCA) 2017 in einem Produktkatalog. Er enthält unter anderem Router, Switches, Server, Firewalls und Anti-Spam-Produkte, die ab einer festgelegten Leistungsgrenze geprüft werden. Die Standards, nach denen die Zertifizierung stattfindet, erarbeitet das chinesische nationale technische Normungskomitee für Informationssicherheit (TC 260), das unmittelbar der CAC untersteht. Das Komitee wird teilweise und in abgewandelter Form auch internationale Standards berücksichtigen. Dazu finden regelmäßige Konsultationen mit Behörden und Organisationen anderer Länder statt, darunter auch dem Bundeswirtschaftsministerium - und nach dem bisherigem Verlauf der Gespräche ist nicht mit bösen Überraschungen zu rechnen.

Für die betroffenen deutschen Unternehmen werden die neuen Bestimmungen konkret bedeuten, dass sie ab deren Inkrafttreten bei einer akkreditierten und für die IT-Sicherheitszertifizierung zuständigen Stelle einen Zertifizierungsantrag einreichen müssen. Welche Stelle das im Einzelnen ist, hängt vom Produkt ab. Die Überprüfung selbst führen behördlich bestimmte chinesische Labore durch, die im Auftrag der akkreditierten Stelle handeln. Sie stellen die Testergebnisse anschließend auch der CNCA zur Verfügung.

Aufmerksamkeit statt Panik

Trotz der vorläufigen Entwarnung wird der Weg nach China für einige deutsche Firmen durch das CSL voraussichtlich schwieriger. Daher sollten betroffene Unternehmen die Lage aufmerksam beobachten. Zu vermuten ist beispielsweise, dass das momentan noch im Entwurfsstadium befindliche neue chinesische Kryptografiegesetz erhebliche Auswirkungen auf den transnationalen Datentransfer haben wird. Auf längere Sicht

steht ferner die Frage im Raum, wie sich die Nutzung chinesisch-staatlich lizensierter VPNs durch ausländische Unternehmen entwickelt. In diesem Zusammenhang will das MIIT die nationalen Anbieter von Telekommunikationsdiensten dazu verpflichten, dass keine ungenehmigten VPNs in ihren Netzwerken genutzt werden. Doch auch in diesem Fall sind noch keine Details bekannt. Daher gehen Insider davon aus, dass zumindest bis Ende 2018 keine überraschenden Maßnahmen zu erwarten sind.

Dr. Dennis-Kenji Kipker ist Jurist und Projektmanager beim VDE – Abteilung CERT@VDE – in Frankfurt a.M.