

Dennis-Kenji Kipker

VPN-Tunnelabschaltung und „Chinese Cybersecurity Law“

– wohl mehr Mythos als Realität

Bereits im November 2016 wurde in der Volksrepublik China das neue „Cyber-Sicherheitsgesetz“ verabschiedet. Infolgedessen wurde unter anderem eine flächendeckende „Abschaltung“ von VPN-Verbindungen zwischen Deutschland und China sowie ein damit einhergehender Verlust der internationalen Wettbewerbsfähigkeit prognostiziert. Der vorliegende Beitrag zeigt jedoch auf, dass es keinesfalls die Absicht des „Cyber-Sicherheitsgesetzes“ ist, die technische Entwicklung zu behindern, womit sich die zahlreich geäußerten Befürchtungen zumindest vorläufig als unbegründet erweisen dürften.

1 Bedenken zum Cybersecurity Law

Das nunmehr schon vor fast zwei Jahren, im November 2016, in der Volksrepublik China verabschiedete neue „Cyber-Sicherheitsgesetz“¹ schlägt auch hierzulande Wellen: So war in den vergangenen Monaten immer wieder von einer flächendeckenden „Abschaltung“ von VPN-Verbindungen zwischen Deutschland und China die Rede, mit der Folge, dass sensible Unternehmensdaten zukünftig nur noch abenteuerlich per „analoger Botenpost“ auf USB-Sticks zwischen den Ländern transferiert werden könnten. Erhebliche Einbußen in der internationalen Wettbewerbsfähigkeit wurden befürchtet, ebenso der Abfluss zentraler Unternehmensdaten im Sinne einer weit reichenden Industriespionage, bis hin zur Entwertung kompletter Geschäftsmodelle.

¹ Dazu ausführlich bereits Kipker, MMR-Aktuell 2015, 370972 (Entwurfassung des CSL) sowie Kipker, MMR 2017, S. 455 (verabschiedete Fassung des Gesetzes und Maßnahmenkatalog zum National Cybersecurity Review).



Dr. Dennis-Kenji Kipker

Geschäftsführender Gesellschafter der certavo compliance management; wissenschaftlicher Geschäftsführer des Instituts für Informations-, Gesundheits- und Medizinrecht (IGMR), Universität Bremen; Projektmanager beim Verband der

Elektrotechnik, Elektronik und Informationstechnik (VDE e.V.) – Abteilung CERT@VDE, Frankfurt am Main und Vorstandsmitglied der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID), Berlin.
E-Mail: kipker@uni-bremen.de

2 Bisherige Folgen des Chinese Cybersecurity Law

Doch was hat sich seither getan, was ist dran an der VPN-Tunnelabschaltung? Bisher – und das dürfte sicherlich viele erleichtern – überraschend wenig, gemessen an den Hiobsbotschaften der letzten Monate. Verschiedene, potenziell betroffene europäische Unternehmen wurden befragt – von mittelständisch bis hin zu Global Playern – stets mit dem gleichen Ergebnis: Denknwendigerweise sind VPN-Verbindungen nach China nicht immer so stabil wie zu manchen anderem westlichen Staat, aber derlei Probleme gab es auch schon vor dem Chinese Cybersecurity Law. Mehr noch: Kein Unternehmen gab an, als unmittelbare (vermutete) Folge der neuen Gesetzgebung aktuell eine Tunnelabschaltung erlitten zu haben.

3 Ermächtigung zur Abschaltung von VPN-Verbindungen nach China

Da die zurzeit diskutierte VPN-Tunnelabschaltung zudem auf das chinesische Cyber-Sicherheitsgesetz rückführbar sein soll, müssten sich hierin theoretisch auch entsprechende Ermächtigungsgrundlagen finden lassen. Fakt ist aber: Das Chinese Cybersecurity Law enthält keine expliziten gesetzlichen Vorgaben zur Abschaltung von VPN-Tunneln. Diese ließe sich höchstens über generalklauselartig formulierte Tatbestände in das Gesetz hineinlesen, so zum Beispiel über Art. 5 (staatliche Maßnahmen zum Umgang mit Netzwerksicherheitsrisiken im In- und Ausland; Bekämpfung gesetzeswidrigen Cyberverhaltens) sowie über Art. 58 (zeitweilige Maßnahmen/Beschränkungen der Netzwerkkommunikation in bestimmten Regionen aus wichtigen öffentlichen Interessen). Wollte man sich aber auf derlei Regelungen als ein konkretes Verdachtsmoment für die flächendeckende, dauerhafte und anlasslose VPN-Tunnelabschaltung stützen, dann dürf-



HILFE, unsere Kunden sind zufrieden!

Deswegen suchen wir, ein führendes Beratungsunternehmen im Datenschutz und in der Informationssicherheit, einen

Datenschutzberater (m/w)

Interesse? Weitere Informationen unter jobs.uimc.de

Wir suchen Verstärkung!

te man auch nicht die zahllosen anderen gesetzlichen und untergesetzlichen Vorschriften des chinesischen IT-Rechts außer Acht lassen, die in den letzten Jahren erlassen wurden und die teils ebenso weit gefasst sind und damit in vielerlei Hinsicht Anknüpfungspunkte bieten. Eine wirklich belastbare Aussage für eine über das bisherige Maß hinausgehende und weitreichende Abschaltung speziell von VPN-Tunneln lässt sich ausgehend vom chinesischen Cyber-Sicherheitsgesetz somit nicht treffen.

4 Auslegung des Cybersecurity Law

Soweit es die Auslegung des Chinese Cybersecurity Laws anbelangt, kann aus verlässlicher Quelle ferner die Information gegeben werden, dass das Gesetz die technische Entwicklung nicht behindern soll und auch nicht behindern wird. Das bedeutet konkret, dass bestehende VPN-Verbindungen wie bisher auch grundsätzlich aufrechtzuerhalten sind. Von einer möglichen Unterbrechung sollen lediglich solche Anbieter bzw. Verbindungen betroffen sein, die rechtswidrig sind – was aber auch schon nach „altem“ Recht der Fall gewesen sein kann und nicht mit einer flächendeckenden und anlasslosen VPN-Abschaltung zu tun hat. Daraus wiederum lässt sich folgern, dass solche VPN-Tunnel, die bisher auch schon ohne grundsätzliche Konflikte bestanden, mit großer Wahrscheinlichkeit selbst unter dem Regelungsregime des chinesischen Cyber-Sicherheitsgesetzes ebenso weiterhin ohne zu erwartende Konflikte betrieben werden können. Ein hierzu ebenfalls bekanntes chinesisches Unternehmen traf in diesem Zusammenhang die Feststellung, dass die Abschaltung von VPN-Tunneln ein deutsches und europäisches Gerücht sei. Das scheint sich bei nüchterner Betrachtung der einzelnen Puzzlesteine zumindest zum jetzigen Zeitpunkt auch zu bestätigen – VPN-Abschaltung, wohl mehr Mythos denn Realität.

5 Stand der Cyber-Sicherheitsgesetzgebung in China

Wie geht es aber weiter? Die Cyber-Sicherheitsgesetzgebung in China ist noch lange nicht abgeschlossen. So steht zwar in Aussicht, dass das chinesische Ministerium für Industrie und Informationstechnik (MIIT) zukünftig konkrete und branchenspezifische Managementregelungen für VPN erarbeitet, die vielleicht ein wenig mehr Licht ins Dunkel des regulatorischen Kosmos bringen. Doch VPN-Tunnel, so breit sie in letzter Zeit hierzu auch diskutiert wurden, sind nicht das einzige Thema der Volksrepublik China in Sachen Cyber-Sicherheit: Die Zertifizierung und Produktzulassung für kritische Netzwerkprodukte ist (wirtschaftlich) mindestens genauso bedeutsam – und hier tut sich nicht nur einiges auf rechtlicher Ebene, sondern ebenso in der bereichsspezifischen Normung und Standardisierung, sowohl national als auch international.

6 Fazit

Festzustellen bleibt, dass sich deutsche und EU-Unternehmen zumindest beim Thema „VPN und China“ etwas entspannen können, gleichwohl aber trotzdem noch genügend zu tun ist, will man Produkte und Leistungen auf dem chinesischen Markt platzieren. Freilich bedeutet dies nicht, dass sich die zukünftige Situation in Sachen VPN nicht doch noch ändern könnte – aber hundertprozentige Garantien gab es schon bisher nicht. Dies betrifft insbesondere die Diskussion um die Nutzung staatlich lizenzierter VPNs. Zudem stellt sich auch für die Volksrepublik China auch die Frage, ob eine flächendeckende Abschaltung von VPN-Tunneln nicht langfristig doch mehr wirtschaftliche Nachteile als Vorteile bringt. Und nicht zuletzt sitzen wir außerdem irgendwo alle im selben Boot: Das, was für die Europäer das Chinese Cybersecurity Law ist, ist für die Chinesen die Europäische Datenschutz-Grundverordnung – und so ist es doch auch gut, auf diese Weise wieder einmal mehr die Gelegenheit zu finden, die transnationalen Beziehungen zu intensivieren.