02-2019

China insight

Wirtschaftsmagazin

Berufsausbildung: Aus den Klassenzimmern in die Werkstätten

Fußball-Training: An die „Graswurzel“ gehen

MAGAZIN AUS DEM DEUTSCH-CHINESISCHEN ÖKOPARK QINGDAO

Daniel Albrecht

Sicherheit im Netz

Ein Vergleich zwischen China, Europa und Deutschland

In den vergangenen Jahren wurden international die IT-Sicherheitsmaßnahmen erheblich verstärkt. In erster Linie geht es darum, den Herausforderungen von Angriffen auf IT-Systeme wirksam begegnen zu können. Insbesondere Deutschland, die EU und China haben weitreichende Gesetzesinitiativen angestoßen.

Deutschland, China und die EU verfolgen jedoch in ihren verabschiedeten Gesetzen unterschiedliche Ansätze.

Deutschlands IT-Sicherheitsgesetz

Das deutsche IT- Sicherheitsgesetz will in erster Linie Angriffen auf die sensible Infrastruktur wirksam begegnen. Gemäß dem bereits Mitte 2015 in Kraft getretenen deutschen IT-Sicherheitsgesetz gibt es diese kritischen Infrastrukturen in verschiedenen Branchen. Ob ein Unternehmen darunterfällt, hängt von seiner Größe ab. Ist dies der Fall, muss das Unternehmen regelmäßig nachweisen, für das Geschäft relevante Systeme und Prozesse besonders gesichert zu haben. Angriffe müssen kategorisiert und gemeldet werden.

Das Gesetz gilt auch für die öffentliche Hand, wohingegen die von der EU erlassenen Regelungen (NIS-RL) lediglich private Unternehmen betreffen. Zentrale Meldestelle für IT-Angriffe ist in Deutschland das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Zudem sind alle Betreiber von Telemedien und damit nahezu alle Anbieter von Webseiten in Deutschland entsprechend Telemediengesetz verpflichtet, dem „Stand der Technik angemessene IT-Sicherheitsmaßnahmen“ zu ergreifen. Technische Einrichtungen müssen außerdem gegen „Verletzungen des Schutzes personenbezogener Daten“ gesichert werden. Möglich sei dies durch Einsatz eines „als sicher anerkannten Verschlüsselungsverfahrens“, das den aktuellen technischen Richtlinien des BSI entspricht. Verstöße werden mit Bußgeld geahndet.

Europas Richtlinie

Eine ähnliche Richtung verfolgen die „Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union“ (NIS-RL), die am 8. August 2016 verabschiedet wurden. Sie sollen helfen, die Widerstandsfähigkeit der IT-Systeme zu verbessern, die Cyberkriminalität zu bekämpfen sowie die Cyberverteidigung der EU zu stärken.

Alle Mitgliedsstaaten sind verpflichtet, zentrale Anlaufstellen zu errichten, die für die Koordinierung der Sicherheit von Netz- und Informationssystemen zuständig sind. Eine enge Kooperation zwischen sogenannten Computer Security Incident Response Teams, zuständigen Behörden und den europäischen Kooperationszentren muss gewährleistet werden. Die Richtlinie sieht Sicherheitsanforderungen und Meldepflichten für die Betreiber wesentlicher Dienste vor und gilt auch für Anbieter digitaler Dienste wie Online-Suchmaschinen, Cloud-Computing-Dienste und Online-Marktplätze. Die Betreiber sind für die Gewährleistung der Sicherheit von Netz-und Informationssystemen in erheblichem Maße verantwortlich.

Die IT-Sicherheit in der EU ist stark durch die *Datenschutz-Grundverordnung* beeinflusst, die sich auf den Schutz personenbezogener Daten bezieht. Demnach müssen öffentliche Einrichtungen und Firmen Maßnahmen ergreifen, um die Sicherheit persönlicher Daten zu gewährleisten und dies auch nachweisen zu können.

Daniel Albrecht ist Rechtsanwalt und Managing Counsel der Beijing Starke Consulting Co. Ltd. law@beijing-starke.com

Fotos: 699pic.com (linke Seite) | Starke Consulting (rechte Seite)

Chinas IT-Sicherheitsrecht

Das chinesische IT-Sicherheitsgesetz, das seit Juni 2017 in Kraft ist, zielt darauf, die Interessen Chinas im weitesten Sinne zu schützen. Dies geschieht, indem einerseits der Regierung Zugriff auf alle in China gesammelten Daten gegeben und andererseits die Sicherheit der Daten erhöht wird. Um die Souveränität auf dem Gebiet der IT-Sicherheit zu behalten, werden zunehmend Gesetze verabschiedet, die den Umgang mit personenbezogenen und sensiblen Infrastruktur-Daten regeln.

Anders als der europäische und nordamerikanische war der chinesische Datenraum hinsichtlich IT-Sicherheit und Datenmanagement lange Zeit kaum reguliert. Der Internetzugang wurde durch die „Great Firewall“ kontrolliert, ehe ab Juli 2015 mit verschiedenen Gesetzen begonnen wurde, ihn zu überwachen und der Regierung Zugang zu privaten Daten zu verschaffen.

Das Cyber-Security-Law zielt vor allem auf Inhaber von Netzwerkeinrichtungen, auf Netzbetreiber und Online-Dienstleistungsanbieter. Sie haben strenge Sicherheitspflichten für „kritische Informationsstrukturen“. Laut Gesetz sind dies traditionell sensible Sektoren, wie öffentliche Telekommunikation und Informationsdienste, Energie,

Transport, Finanzierung, Stadtwerke und e-Government. Allerdings können „auch andere Bereiche, die die nationale Sicherheit, Wirtschaft und öffentliche Interessen beeinträchtigen könnten", als solche verstanden werden. Netzbetreiber müssen sensible Daten, die in China erhoben werden, auf nationalen Servern speichern und dürfen diese nicht ohne Genehmigung ins Ausland weiterleiten.

- Als *Netzbetreiber* definiert das Gesetz Netzeigentümer, -manager und -anbieter. Nicht nur Betreiber von Telekommunikationsnetzen und Internetfirmen sind umfasst, sondern auch Wirtschaftsinstitutionen, die persönliche Daten von Bürgern erfassen und Online-Dienste anbieten.

  Netzbetreiber sollen Maßnahmen zur Sicherung der Netzbetriebe ergreifen und in der Lage sein, effektiv auf Störungen der IT-Sicherheit zu reagieren, sowie Internetkriminalität zu verhindern. Sie müssen mit den zuständigen Behörden kooperieren, ihnen uneingeschränkt Zugang zu Daten gewähren und die technische Unterstützung bei Problemen anbieten. Außerdem müssen Ausrüstungen für sensible Bereiche getestet und zertifiziert werden. Die zuständige Administration für den Datenraum entwickelt entsprechende technische Standards und konsultiert dabei nationale und internationale IT-Verkäufer.
- Bei der *kritischen Informationsinfrastruktur* wird zwischen Webseiten, Plattformen und Produktionsunternehmen unterschieden. Aufgrund der weiten Auslegungsmöglichkeit des Gesetzes sollte auf den „Network Security Check Practice Guide" zurückgegriffen werden, der von der Central Cyberspace Affairs Commission (CAC) bereits vor der Verabschiedung des Gesetzes erlassen wurde. Betreiber müssen mindestens einmal jährlich ihre IT-Sicherheitssysteme testen und über mögliche Risiken berichten. Gleichzeitig sind sie verpflichtet, sich einer Überprüfung zur Gewährleistung der nationalen Sicherheit zu unterziehen. Wie sich diese von anderen Inspektionen unterscheiden, ist noch unklar. Einfluss auf multinationale Konzerne in China werden sie aber haben.
- Laut Gesetz sind Netzbetreiber für die *Gewährleistung der Netzwerksicherheit* verantwortlich. Sie sollen verschiedene Technologien zum Schutz gegen Cyber-Angriffe einsetzen und erforschen, um

Netzwerkrisiken zu reduzieren. Vor allem sollen zur Optimierung des Datenschutzes Administrationssystem effektiv gesichert und technische Lösungen entwickelt werden.

Derzeit hat China zwei Netzwerksicherheitsprogramme, die sich überschneiden. Sie unterscheiden zwischen fünf Sicherheitsstufen eines Computerinformationssystems oder Telekommunikationsnetzes, je nach der Bedeutung, die das System für die nationale Sicherheit, die wirtschaftliche Entwicklung und das gesellschaftliche Leben hat. Unklar ist, ob diese dem vom Cyber Security Law vorgeschriebenen System genügen.

- Die Definition für *persönliche Daten* umfasst alle Merkmale, die eine Person identifizieren: Name, Geburtstag, Telefonnummer, Adresse. Das Gesetz schreibt vor, in China durch kritische Infrastruktur erfassten persönlichen und andere wichtigen geschäftlichen Daten im Land zu speichern. Sollten die Daten aus geschäftlichen Gründen außerhalb Chinas benötigt werden, müssen Netzbetreiber die Zustimmung der Personen einholen, die Daten gegenüber Dritten zu nutzen.
- Zuständig für die Durchsetzung des Gesetzes ist die Central Cyberspace Affairs Commission. Sie verhängt auch *Sanktionen* bei Verstößen. Typischerweise werden Betreiber zunächst gewarnt und aufgefordert, den Verstoß zu beheben. Gemäß Gesetz illegale Einnahmen können einbezogen oder Bußgelder verhängt werden. In besonders schwerwiegenden Fällen kann die Stilllegung von Webseiten oder Betrieben bei gleichzeitiger Entziehung von Lizenzen angeordnet werden. Bußgelder für den unautorisierten Export von Daten können bis zu 500.000 Yuan betragen, mehr als 65.000 Euro.
- Ausländischen Firmen fürchten eine vermehrte Datenkontrolle sowie ein *größeres Risiko des Diebstahls geistigen Eigentums*. Aufgrund der vagen Definitionen und fehlender offizieller Anleitung zum Cyber Security Law herrscht nach wie vor große Ungewissheit. Die Überprüfung von Daten durch Behörden birgt das Risiko, dass Information verloren geht, an lokale Wettbewerber weitergegeben oder durch die Behörden selbst verwendet wird. Zur Daten-Lokalisierung müssen ausländische Firmen entweder in neue Datenserver in China investieren, die von der Regierung überprüft werden können, oder einen lokalen Serverbetreiber in Anspruch nehmen, Huawei etwa, Tencent oder Alibaba.

  Viele ausländische Firmen in China transferieren Daten an die Muttergesellschaften. Aufgrund der Bedenken um den Schutz geistigen Eigentums haben viele Firmen interne Regelungen für Informationstechnik, Datenmanagement und Geheimhaltung. Während größere Unternehmen in der Lage sind, die Kosten zur Einhaltung der Sicherheitsvorkehrungen zu tragen, könnte dies bei mittelständigen und kleineren Unternehmen nicht der Fall sein.

  Des Weiteren wird die Kooperation zwischen kritischen Systemen und ausländischen Partnern beeinflusst. Chinesische Partner könnten nicht mehr bereit sein, Daten auszutauschen. Auch chinesische Unternehmen sind im täglichen Betrieb auf internationalen Datentransfer angewiesen. Dies könnte letztlich Druck auf die Regierung ausüben, und zu einer flexiblen Interpretation des IT-Sicherheitsgesetzes führen. So könnte Raum für Zugeständnisse geschaffen werden.

Fazit

Sowohl die europäischen Datenschutz-Verordnungen als auch Chinas IT-Sicherheitsgesetz zielen auf eine Verzahnung zwischen Industrie und Kontrolle. Besonders im IT-Sicherheitsbereich hängt der Erfolg dieses Ziels von der Kooperation zwischen öffentlicher Hand und privaten Unternehmen ab.

Beide Sicherheitsregime zeigen Parallelen. Grundsätzlich geht es hier wie dort um Verlässlichkeit, Transparenz und Rechtmäßigkeit, Information zu Rechtsverletzungen, die Frage, wie Daten gespeichert und genutzt, aber auch gelöscht werden. Beide erzeugen bei betroffenen Unternehmen Angst vor hohen Bußgeldern. In der EU kommt die Angst vor Rufschädigung hinzu.

Der größte Unterschied zwischen beiden Herangehensweisen ist, dass China nicht nur „den rechtlichen Schutz der Interessen der Massen im Cyberspace“ verfolgt, sondern auch „die Wahrung der nationalen Souveränität“. Die heimische Produktion anzuregen, kann intern als positives Nebenprodukt des Gesetzes gesehen werden, könnte jedoch dazu führen, dass ausländische Firmen, die ihr geistiges Eigentum nicht länger halten können, abwandern, was letztendlich der chinesischen Wirtschaft schaden würde.