WZR China Update zum chinesischen Cybersecurity Gesetz

+

Worum geht es im Cybersecurity Gesetz?

Datenschutz
Datendiebstahl und -handel sind massive Probleme in China. Das neue Gesetz schafft erstmals einheitliche Regelungen zum Umgang mit personenbezogenen und wichtigen Daten.

IT-Sicherheit
Das Gesetz regelt, was Unternehmen tun sollen, um die Sicherheit ihrer Daten zu wahren. Interne Maßnahmen sind Thema, genau wie technischer Schutz oder der Einkauf sicherer Netzwerkprodukte.

Tens of thousands of Chinese firms, institutes affected in WannaCry global cyberattack

PUBLISHED : Monday, 15 May, 2017, 2:36pm
UPDATED : Monday, 12 June, 2017, 12:53pm

COMMENTS: 12

Verhalten im Internet
Welche Inhalte darf man im chinesischen Internet verbreiten? Das Gesetz dient mit Regelungen zur Veröffentlichung von Inhalten auch zur Wahrung der öffentlichen Ordnung in China.

+

Wer muss das Gesetz einhalten?

Das Gesetz findet Anwendung auf alle Unternehmen, die

- Personenbezogene Daten von chinesischen Staatsbürgern verarbeiten, also z.B. Namen und Anschrift von Mitarbeitern, oder
- „wichtige“ Daten, z.B. aus E-Commerce-Transaktionen, in China verarbeiten, oder
- in irgendeiner Weise Inhalte für chinesische Nutzer im Internet anbieten, z.B. auf Webseiten oder in Social Media-Kanälen.

Das Cybersecurity Gesetz unterscheidet bei den Verpflichteten zwischen den Gruppen

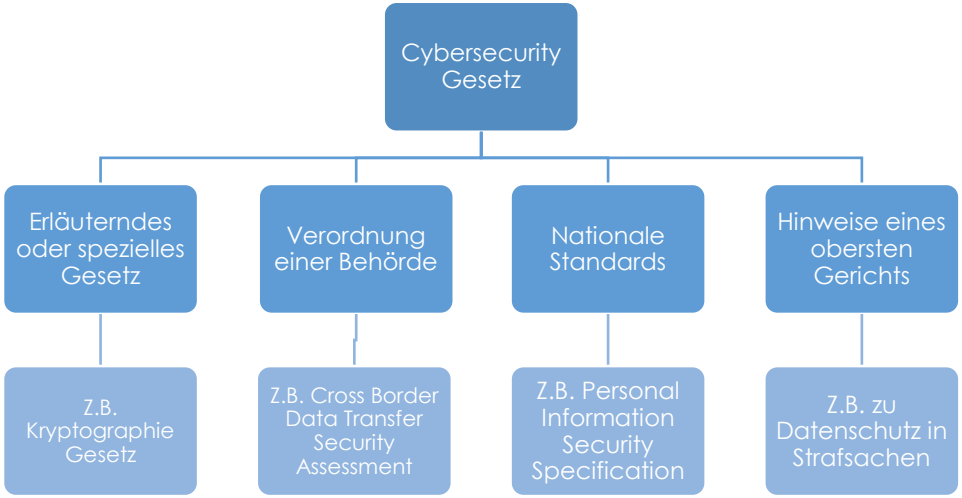
- allgemeine Nutzer,
- Anbieter von Netzwerkprodukten,
- Netzwerkbetreiber und
- Betreiber von Schlüsselinfrastruktur / Kritische Infrastruktur.

Für jede einzelne Gruppe gelten verschiedene Pflichten, wobei Unternehmen je nach Tätigkeit auch in verschiedenen Gruppen gleichzeitig betroffen sind.

Achtung: Der Anwendungsbereich des Gesetzes ist extrem schnell eröffnet. Es genügt, dass ein Datensatz über einen Mitarbeiter, z.B. Name, Anschrift und Kontodaten erhoben und gespeichert wird. Es stellt sich dann lediglich die Frage nach dem Umfang der Verpflichtungen im Einzelnen.

Was ist der Stand der Gesetzgebung?

Das Cybersecurity Gesetz ist ein Rahmengesetz, das für sich genommen die gesetzlichen Pflichten nur sehr vage beschreibt. Es wird daher durch eine Vielzahl von Umsetzungsvorschriften konkretisiert.



Der Stand der Gesetzgebung ist in den einzelnen Themenbereichen sehr unterschiedlich.

- Im Bereich Datenschutz liegen Vorschriften teils final, teils als Entwurf vor. Hier fehlt jedoch insbesondere der finale Entwurf der Regelungen zur Übertragung von Daten ins Ausland.
- Im Bereich IT-Sicherheit liegen zahlreiche Entwürfe, jedoch kaum finale Vorschriften vor.
- Im Bereich Verhalten im Internet sind die meisten der erwarteten Umsetzungsvorschriften bereits in Kraft.

Info: nationale Standards

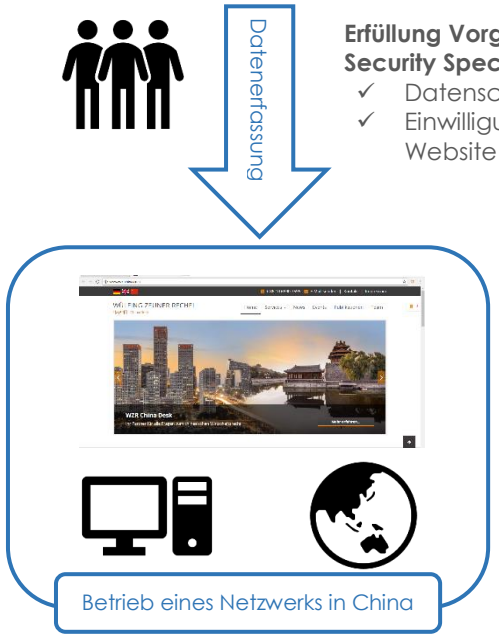
Ein Großteil der konkretisierenden Umsetzungsvorschriften zum Cybersecurity Gesetz ergeht als nationaler Standard. Nationale Standards stehen nicht im Rang eines Gesetzes, sondern darunter. Rein rechtlich sind sie daher nicht zwingend. Trotzdem wenden viele Behörden nationale Standards wie ein Gesetz an. Vereinzelt werden nationale Standards durch Verweise in anderen Gesetzen auch auf „Quasi-Gesetzesrang“ gehoben. Wer die rechtlichen Pflichten sicher erfüllen möchte, sollte deshalb die Regelungen der nationalen Standards eher genau anwenden.

Im Einzelnen: Datenschutz

Bereits vorliegende Regelungen
Für den Bereich der Verarbeitung von personenbezogenen Daten werden die datenschutzrechtlichen Pflichten des Cybersecurity Gesetzes umfassend konkretisiert in der kürzlich erlassenen „**Personal Information Security Specification**“, die am 01. Mai 2018 in Kraft tritt. Diese stellt insbesondere klar:

- Management-Personal und gesetzliche Vertreter tragen umfassende Verantwortung für die Einhaltung des Gesetzes.
- Genaue Definition von personenbezogenen Daten und/oder sensitive personenbezogene Daten in zwei Beispiellisten.
- Es gibt ein umfassendes Erfordernis, Einwilligungen einzuholen. Zentrale Ausnahme für ausländische Unternehmen ist die Erforderlichkeit der Daten zur Erfüllung eines Vertrags.
- Unternehmen müssen interne Richtlinien zum Umgang mit personenbezogenen Daten formulieren. Die Prozesse sind von Erhebung bis Löschung der Daten genau aufzuzeichnen.
- Datenschutzerklärungen müssen exakt formuliert sein. In den Vorschriften selbst ist eine Vielzahl von Musterklauseln enthalten.

Worum sich chinesische Tochterunternehmen jetzt kümmern sollten:



Erfüllung Vorgaben Personal Information Security Specification (in Kraft ab 01. Mai!):

- ✓ Datenschutzerklärung anpassen
- ✓ Einwilligungserfordernis klären und Website entsprechend anpassen

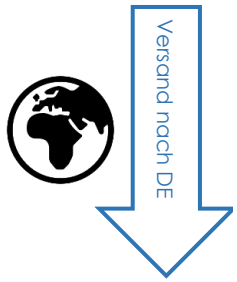
Internes Management:

- ✓ Verantwortlichkeit klären für Datenschutz
- ✓ Datenverarbeitungsprozesse aufzeichnen von Erfassung bis Löschung der Daten
- ✓ Interne Richtlinien zum Umgang mit Daten im Unternehmen, z.B. Zugriffs-rechte und Freigabeprozesse

Noch zu erwartende Regelungsbereiche
Im Bereich Datenschutz werden insbesondere noch in folgenden Bereichen Vorschriften erwartet:

- Regelungen zu **Speicherpflicht für personenbezogene und wichtige Daten in China** und Datentransfer ins Ausland. Verweisnormen in der „Personal Information Security Specification“ deuten darauf hin, dass es mindestens beim Erfordernis einer **intern durchzuführenden Sicherheitsüberprüfung** vor Versand von Daten ins Ausland bleiben wird. Mit Blick auf die Speicherpflicht sind die finalen Vorschriften abzuwarten.
- Wichtige Daten: der bislang vorliegende **Katalog von „wichtigen Daten“** soll gekürzt werden. Insbesondere ist abzuwarten, ob Überschneidungen zu personenbezogenen Daten, z.B. bei Rechnungsdaten oder im Bereich E-Commerce aufgehoben werden.
- **Nutzung von pseudonymisierten und anonymisierten Daten**: es wird grundsätzlich möglich sein, pseudonymisierte bzw. anonymisierte Daten umfangreich zu nutzen, z.B. für Marketingzwecke. Konkrete Anforderungen an die Pseudonymisierung bzw. Anonymisierung sollen noch festgelegt werden.

Weitere zu erwartende Themen:
- ✓ Konkretisierung des Begriffs der wichtigen Daten und der Pflichten zum Umgang mit diesen Daten im Unternehmen
- ✓ Klärung der Pflicht zur Speicherung von wichtigen und personenbezogenen Daten in China
- ✓ Anforderungen an interne Regelungen zur Nutzung pseudonymisierter bzw. anonymisierter Daten



Weitere zu erwartende Themen:
- ✓ Erforderlichkeit zur Durchführung einer (internen) Sicherheitsüberprüfung bei Versand von wichtigen und personenbezogenen Daten außerhalb Chinas

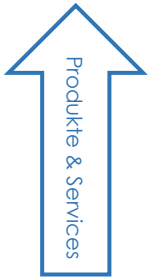
+

Im Einzelnen: IT-Sicherheit

Auch im Bereich IT-Sicherheit macht das Cybersecurity Gesetz grundsätzliche Vorgaben. Gemäß Artikel 21 ist eine **verantwortliche Person zu benennen**, die sich um die Einführung eines internen Sicherheitsmanagementsystems einschließlich technischer und organisatorischer Maßnahmen und deren Implementierung kümmert.

Im Bereich IT-Sicherheit werden insbesondere noch in folgenden Bereichen finale Umsetzungsvorschriften erwartet:
- Konkretisierung des **Begriffs der Schlüsselinfrastruktur** bzw. Kritischen Infrastruktur und der durch diese zu erfüllenden Sicherheitsanforderungen.
- Definition von **Standards zum Aufbau und zur Prüfung von internen Sicherheitsmanagementsystemen**. In vorliegenden Entwürfen werden ausführliche Regelungen zur Bewertung von Gefahrpotentialen und hierfür geltenden Sicherheitsmaßnahmen getroffen.
- Standards für die **Bewertung des Sicherheitsniveaus von Netzwerkprodukten und Netzwerkservices**.

Aktuelle ToDos:
- ✓ Verantwortlichkeit klären für IT-Sicherheit
- ✓ Status Quo im chinesischen Tochterunternehmen klären: welche Sicherheitsmaßnahmen bestehen? Welche internen Richtlinien gibt es?
- ✓ Ggf. Identifizierung bestehender Sicherheitslücken durch Auditierung



Weitere zu erwartende Themen:
- ✓ Konkretisierung der Anforderungen an IT-Sicherheits-management im Unternehmen
- ✓ Konkretisierung der Anforderungen für das Anbieten und den Einkauf von Netzwerkprodukten und Netzwerkservices

Im Einzelnen: Verhalten im Internet

Der Bereich Verhalten im Internet ist mit Blick auf den Stand der Gesetzgebung am weitesten fortgeschritten. Viele der Regelungen sind jedoch für ausländische Unternehmen nicht relevant, da sie Bereiche betreffen, die für ausländisch investierte Unternehmen nicht zugänglich sind. Hierzu gehören z.B. Online-Nachrichtenservices.

Ausländische Unternehmen sollten jedoch aktuelle Themen rund um das Thema im Blick behalten. Hierzu gehören beispielsweise

- Klarnamenspflicht für Kommentare im Internet,
- Sperrung von Webseiten wegen der Verwendung von Landkarten, auf denen Taiwan nicht eindeutig als Teil Chinas gekennzeichnet ist bzw. die Taiwan als eigenständig bezeichnen,
- Sperrung von Online-Kanälen, die nicht „sozialistischen Werten“ entsprechen und „Gossip“ verbreiten.

Aktuelle ToDos für Ihr Tochterunternehmen in China

- Auf Management-Ebene: Benennung zuständige Personen für Koordinierung im Unternehmen
- IT-Abteilung: Benennung zuständige Person für IT-Sicherheit und Datenschutz
- In allen Abteilungen des chinesischen Tochterunternehmes: Feststellung des Status Quo
  - Welche Daten werden vom Unternehmen erfasst und wie werden diese verarbeitet? Insbesondere welche Daten von Mitarbeitern, Kunden und Kooperationspartnern werden erfasst?
  - Welche internen Richtlinien und Maßnahmen zu Datenschutz und IT-Sicherheit und Verhalten im Internet liegen vor?
- Feststellung der individuellen Betroffenheit und Abgleich des Status Quo mit gesetzlichen Anforderungen, z.B. durch externe Auditierung
- Für Unternehmen mit Online-Angeboten für den chinesischen Markt: Formulierung bzw. Anpassung von Datenschutzerklärungen
- Laufendes Monitoring der weiteren Gesetzgebung und Anpassung interner und externer Prozesse, insbesondere zu den Themen
  - Speicherpflicht für personenbezogene Daten in China
  - Sicherheitsüberprüfung bei Versand von Daten ins Ausland
  - IT-Sicherheitsmaßnahmen

Cybersecurity-Gesetz: Leistungen von WZR China

- Feststellung der individuellen Pflichten ihres chinesischen Tochterunternehmens nach dem Cybersecurity Gesetz
- Beratung zur Umsetzung des Gesetzes im Unternehmen: unter anderem Updates von Arbeitsverträgen, Mitarbeiterhandbüchern und Erstellung von internen Richtlinien
- Prüfung und Formulierung von Verträgen mit IT-Dienstleistern und Kunden
- Formulierung von Datenschutzerklärungen für Ihre Website
- Laufende Informationen zu aktuellen Entwicklungen rund um das Cybersecurity Gesetz

Cybersecurity-Gesetz: Ansprechpartner

Jost Blöchl
Senior Associate WZR Beijing
Hauptansprechpartner Cybersecurity Gesetz

T. + 86 10 6590 7595
jost.bloechl@wzr-china.com

Dr. Florian Kessler
Managing Partner WZR Beijing
Hauptansprechpartner Cybersecurity Gesetz

T. + 86 10 6590 7595
Florian.kessler@wzr-legal.com

Dieses Update ist eine unverbindliche Information von:

WZR Ltd., Beijing
Landmark Tower II, Unit 0406
8 North Dongsanhuan Road
Beijing 100004, P.R. China
Stand: 08. März 2018