owc Verlag für Außenwirtschaft

6/2020 25€ 24. Jahrgang H49998 www.owc.de

ChinaContact

Das Außenwirtschaftsmagazin

NRW und China: Brücke in die Zukunft
Fünfjahresprogramm: Indirekte Kampfansage
RCEP: Ein großer Erfolg für China

Social Commerce: die Macht der KOLs

Ein Digital-TÜV für alle

Die KP Chinas und der chinesische Staat sehen vernetzte elektronische Systeme als Grundbedingung für Wohlstandsmehrung, gesellschaftliche Entwicklung und nationale Sicherheit und haben deshalb IT-Infrastrukturen und damit verbundene Risiken und Abhängigkeiten genau im Blick. Ausbau und Sicherheit dieser Systeme und damit ein „starkes digitales China“ stehen weit oben auf der Prioritätenliste der politischen Führung. Das zeigen auch die gerade veröffentlichten „Vorschläge für das 14. Fünfjahresprogramm (2021 bis 2025)“.

Foto: imago images / VCG

Seit Erlass des Cybersecurity-Gesetzes im Jahr 2016 folgen in hoher Taktzahl neue Gesetze, Verordnungen, politische Richtungsaussagen (意见) und nationale Standards, die einen immer dichteren Regelungsrahmen um den gesamten Internet- und IT-Bereich legen. Die „Sauberkeit" des Internets und die nachhaltige Sicherung der IT-Infrastruktur sind auch bei der Leistungsbewertung von Beamten von zunehmender Bedeutung.

Zentraler Baustein für eine sichere, nationale IT-Infrastruktur ist das sogenannte Stufensystem für den Schutz der Netzsicherheit, das oft als Multi Level Protection System for Network Security (kurz: MLPS) bezeichnet wird. Das MLPS soll eine flächendeckende Aufsicht über die IT-Sicherheit aller in China tätigen Unternehmen und Organisationen ermöglichen. Die rechtlichen Grundlagen gehen auf das Jahr 2007 zurück; das System wurde jedoch in der Vergangenheit außerhalb der Staatsunternehmen und der kritischen Infrastrukturen kaum angewandt. Falls die jüngsten Verlautbarungen nicht trügen, ist jedoch im nächsten Jahr mit einer konsequenteren Umsetzung zu rechnen.

Risikostufen

Adressaten des MLPS sind die Betreiber von Netzwerken. Jedes Unternehmen, in dem elektronische Daten über mehrere Endgeräte verarbeitet und über das Internet oder andere Netze ausgetauscht werden, ist ein Netzwerkbetreiber im Sinne des Gesetzes.

Das MLPS unterteilt Unternehmen beziehungsweise deren Netzwerke in fünf Risikoklassen – von Stufe 1 (Gefahr von Schäden für einzelne Personen oder Unternehmen, aber kein Risiko für die Allgemeinheit) bis zur höchsten Risikostufe 5 (äußerst schwerwiegende Schädigung der nationalen Sicherheit). Die Risiko- oder Schutzstufe bestimmt sich nach der Schadensgefahr, die von einer Störung oder von dem vollständigen Ausfall eines Computernetzwerks ausgeht. Je wichtiger das Schutzgut und je schwerer die drohende Beeinträchtigung, desto höher ist die Risikostufe.

Die Einstufung anhand der in der Tabelle genannten Kriterien – „schwerer Schaden" oder „öffentliches Interesse" usw. – wirft viele Fragen auf. Tatsächlich sind Abgrenzungen wie (einfacher) Schaden / schwerer Schaden kaum mit Gewissheit zu treffen. Die Auslegung vager Rechtsbegriffe wie „gesellschaftliche Ordnung" ist eine Wertungsfrage.

Am 1. November 2020 trat ein neuer nationaler Standard in Kraft, der diese Begriffe weiter aufgliedert und etwas konkretere Kriterien für die hier geforderte Risikofolgenabschätzung liefert.

In der behördlichen Praxis herrscht allerdings die Auffassung vor, dass es praktisch in jedem Unternehmen zum Ernstfall kommen könne – zum Beispiel durch Diebstahl „sensitiver" Mitarbeiterdaten – und deswegen die Einstufung in die Risikoklasse 2 der Regelfall sei. Viele Beamte argumentieren zudem, dass nur die Überprüfung durch eine qualifizierte Einrichtung Gewissheit verschaffen könne, dass die (Selbst-)

Schwere des Eingriffs / Schutzgut	Einfacher Schaden	Schwerer Schaden	Äußerst schwerer Schaden
Rechte und Interessen von Einzelpersonen, Unternehmen, Organisationen	**Stufe 1**	**Stufe 2**	**Stufe 3**
Gesellschaftliche Ordnung Öffentliches Interesse	**Stufe 2**	**Stufe 3**	**Stufe 4**
Nationale Sicherheit	**Stufe 3**	**Stufe 4**	**Stufe 5**

Quelle: Entwurf einer „Verordnung über das mehrstufige Netzwerksicherheits-Schutzsystem" vom 27.06.2018

Einstufung richtig ist und das Unternehmen die gesetzlichen Pflichten erfüllt. Die Eingangsstufe 1 bliebe damit nur ganz kleinen Unternehmen vorbehalten.

Pflichtenprogramm

Unternehmen sind ausnahmslos verpflichtet, für die Sicherheit ihrer Netzwerke zu sorgen. Dies gilt nicht nur für die Betreiber kritischer Infrastrukturen wie Versorgungsunternehmen – so wie es in Deutschland vorgeschrieben ist –, sondern für alle. Ab Stufe 2 muss der Betreiber nachweisen, dass

Wer IT-Netzwerke betreibt, muss in China für deren Sicherheit sorgen.(Foto: Darstellung eines Servicenetzwerks in einer Niederlassung von Chongqing City Construction Investment).

er sich der Prüfung durch eine staatlich anerkannte Prüfungseinrichtung (eine Art Netzwerk-TÜV) unterzogen hat. Diese Stelle übersendet den Prüfbericht direkt an die Abteilung für Netzsicherheit der zuständigen Polizeibehörde, in der Regel auf Stadt- oder Bezirksebene. Ohne diese Anmeldung ist der Betrieb des Netzwerks rechtswidrig.

Je höher die Schutzstufe, desto umfangreicher und strenger gestalten sich die dem Betreiber auferlegten Pflichten. Netzwerkbetreiber müssen in technischer, organisatorischer und personeller Hinsicht die für ihre Gefahrenstufe angemessenen Vorkehrungen treffen, um Gefahren für die Funktionsfähigkeit ihrer Systeme und die Sicherheit der von ihnen verwalteten Daten abzuwenden. Das Pflichtenprogramm ähnelt den Anforderungen für die Zertifizierung von Informationssicherheitssystemen nach international gebräuchlichen Standards (zum Beispiel der ISO/IEC 27000-Reihe) mit chinaspezifischen Elementen.

Die Kernpflichten aus dem MLPS-Kanon sind:

- klare Zuordnung von Verantwortlichkeiten und Bestellung eines IT-Sicherheitsbeauftragten; ab Stufe 3 Einrichtung einer entsprechenden Abteilung
- Identitäts- und Zugangskontrolle
- technische und organisatorische Vorkehrungen zur Abwehr von Angriffen durch Schadprogramme und Hacker
- Schutz persönlicher Daten, „wichtiger Daten“ und von Staatsgeheimnissen (auch mit Blick auf das Verbot oder die Restriktionen beim Datenexport)
- Sicherung von Datenbeständen und ein Notfallkonzept, um im Angriffsfall schnell reagieren zu können
- Meldung von Störungen binnen 24 Stunden an die zuständige Behörde
- Speicherung der Logdateien für mindestens sechs Monate
- physische Sicherung der Systeme (Serverraum usw.)

Anders als in den meisten westlichen Staaten hat der Betreiber auch die Pflicht, angemessene Vorkehrungen zu treffen, um den Austausch und das Verbreiten rechtswidriger Inhalte durch Mitarbeiter oder externe Nutzer zu unterbinden. Eine Verletzung dieser Pflicht kann angesichts der weiten Begriffsdefinition unangenehme Folgen haben.

Unternehmen können Aufbau, Wartung und Verwaltung ihrer Netzwerke auf spezialisierte Dienstleister auslagern, müssen aber in diesem Fall die Qualifikation des Dienstleisters prüfen. Ab der Stufe 3 gelten verschärfte Anforderungen hinsichtlich der Beschaffung von Produkten und Leistungen. Die externe Systemwartung etwa darf nur an inländische Dienstleister vergeben werden.

Betreiber sind verpflichtet, ihr IT-Sicherheitskonzept mindestens einmal pro Jahr zu überprüfen. Bis Stufe 2 handelt es sich um eine Selbstprüfung. Ab Stufe 3 muss dies extern geschehen.

Kritische Infrastrukturen

In vielen Bereichen gelten besonders hohe Anforderungen für die Informationssicherheit. Dies sind die kritischen Infrastrukturen, deren Funktionsfähigkeit und Unversehrtheit von besonderer Bedeutung für das Gemeinwesen sind. Zu dem nicht abschließenden Katalog gehören: Telekommunikation/Internet, Energie, Wasser, Gesundheit, Finanzinstitute, Lebensmittel, Chemieindustrie und Rüstung. Die IT-Netzwerke in diesen Bereichen gehören in der Regel in die MLPS-Stufen 3 bis 5.

Ein besonderes Augenmerk liegt auf dem Ausschluss von Risiken durch die Verwendung ausländischer Hardware, Software und Clouddienste. Betreiber kritischer Infrastrukturen und von Netzwerken ab Risikostufe 3 sollen bei der Bekämpfung von Cyberangriffen mit den zuständigen Aufsichtsbehörden zusammenwirken.

Fazit

Das IT-Sicherheitsmanagement ist eine Compliance-Aufgabe und gehört in die Zuständigkeit der Geschäftsführung. In China kommt hinzu, dass es sich bei der Wahrung der Netzwerksicherheit auch um eine öffentlich-rechtliche Pflicht handelt. Verstöße können zu Bußgeldern und weiteren Sanktionen führen, selbst wenn kein Schaden entstanden ist oder das Unternehmen selbst auch Opfer ist, etwa im Zuge eines Ransomware-Angriffs.

Viele ausländisch investierte Unternehmen stehen dem MLPS noch abwartend gegenüber. Das ist angesichts der Kosten und der Unsicherheit ob der Einstufung in Schutzstufe 1 oder 2 verständlich. Das System verschafft aber auch ein Stück Entlastung. Wenn die IT-Sicherheit gemäß MLPS geprüft und zertifiziert wurde, kann das Management sicher sein, dass zumindest die grundlegenden Pflichten erfüllt sind.

Philip Lazare
ist Rechtsanwalt und Partner bei Luther Law Offices in Shanghai.

Zhang Yuhua
ist Associate bei Luther Law Offices in Shanghai.

www.luther-lawfirm.com

Impressum

Herausgeber und Geschäftsführender Gesellschafter:
Ulf Schneider (v. i. S. d. P.)

Leitende Redakteurin: Petra Reichardt

Art Director: Jonas Grossmann

OWC-Verlag für Außenwirtschaft GmbH
Ritterstraße 2 B, 10969 Berlin
Telefon: +49 30 615089-0 / Fax: +49 30 615089-29
E-Mail: info@owc.de

Anzeigen: OWC-Verlag für Außenwirtschaft GmbH
Ritterstraße 2 B, 10969 Berlin
Telefon: +49 30 615089-0 / Fax: +49 30 615089-29
E-Mail: anzeigen@owc.de

Sachar Jaschaev: +49 30 615089-18 / sj@owc.de
Büro Moskau: +7 495 956 55 57

Abonnement: Jahresabonnement 120 €, Inland: zzgl. 7 % MwSt.
EU-Ausland: zzgl. 28 € Porto / Non-EU: zzgl. 48 € Porto
Einzelheft: 25 €

Leserservice: Telefon +49 6123 9238257 / Fax: +49 6123 9238244
E-Mail: leserservice-owc@vuservice.de

Gerichtsstand: Berlin, Amtsgericht Charlottenburg,
HRB 170362 B / ISSN 1869-3539

Druck: Bösmann Medien und Druck GmbH & Co. KG,
32758 Detmold

Titel: Eigene Darstellung

Hinweis: Namentlich gekennzeichnete Beiträge geben nicht in jedem Fall die Meinung der ChinaContact-Redaktion wieder.

Redaktionsschluss: 17. Dezember 2020

ChinaContact

Chinaaktuell

Der Newsletter für Außenwirtschaft

Aktuelle Meldungen zur Wirtschaftsentwicklung in China, zu Akteuren und Investments. In unserem neuen China-Nachrichten-Portal und wie gewohnt alle 14 Tage als Newsletter.

owc.de/ca