VDMA-Infoblatt

**Competence Center Industrial Security**

# Status Quo VPN & Datenaustausch in China

*Update mit Kenntnisstand März 2020*

## Hinweise

Mit diesem Faktenpapier werden Erfahrungen von VDMA und nicos AG zusammengeführt, um gemeinsam zum Verständnis über das Thema „VPN und China“ beizutragen. Dieses Papier ist ausschließlich zur Information an VDMA-Mitgliedsunternehmen bestimmt und stellt lediglich die Erfahrungen aus dem Betrieb von VPN-Zugängen sowie aus Gesprächen mit den chinesischen Carriern und Rechtsberatern der nicos AG zur Entwicklung der Cyber Security Regulierung in der Volksrepublik China dar.

## Zusammenfassung

Mit der im Jahr 2017 verabschiedeten Regulierung von Internetzugangsdiensten verschärfen chinesische Behörden die Regulierung verschlüsselter Datenübertragung von und nach China.[1] Die Umsetzung der Regulierungsmaßnahmen wurde auf Grund von wirtschafts-politischen Bedenken auf März 2019 verschoben. Unternehmen müssen seitdem Internetzugänge von zugelassenen Providern nutzen, soll die grenzüberschreitende verschlüsselte Datenübertragung auch weiterhin rechtskonform geschäftlich genutzt werden.

Der Regulierung entsprechend sind multinationalen Konzernen grenzüberschreitende VPN-Verbindungen dann erlaubt, wenn hierfür dedizierte direkte Zugänge angemietet werden[2]. Werden über Standard-Internetzugänge VPN-Verbindungen ins Ausland aufgebaut, wird die Datenübertragung zeitnah unterbunden – bis hin zur dauerhaften Blockade.

Der VDMA empfiehlt, eine dedizierte Leitung für den grenzüberschreitenden verschlüsselten Datenverkehr von Maschinendaten einzurichten. Der Datentransfer von Individuen und IT-Systemen ist, sofern möglich, zu trennen. Internetzugänge für Mitarbeiter sind auf betriebliche Zwecke zu reduzieren, insbesondere eigenmächtige VPN-Verbindungen sollten unterbunden werden. Die Business-Internetangebote von China Telecom und China Unicom haben sich für diesen Zweck als recht zuverlässig erwiesen. VPN-Verbindungen über MPLS-Leitungen sind sehr zuverlässig, aber auch sehr teuer.

Aktuell (Stand: März 2020) lässt sich keine Verschärfung der Regulierung von verschlüsselten Verbindungen erkennen. Der Fokus der Regulierung verschiebt sich vom Betrieb von VPNs hinzu der behördlichen Prüfung, welche Art von Daten übertragen werden (Stichwort “Important Data“). Hierbei geht es besonders um sensible, personenbezogene oder für die chinesische Wirtschaftskraft wichtige Daten.
Die Marktbereinigung der sogenannten „Gray Line Provider“ (Provider, die Individuen via VPN & Apps unerlaubt Zugang zum freien Internet verschafft haben) ist laut Informationen aus Gesprächen der nicos AG mit chinesischen Providern abgeschlossen.

[1] http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c5471946/content.html (Abrufdatum: 19.01.2018)
[2] Vgl. EU Chamber of Commerce in China: ICT Working Group Position Paper 2019, Kapitel “Internet Access”

VDMA e.V.
Lyoner Str. 18
60528 Frankfurt am Main, Germany
Telefon +49 69 6603-1360
E-Mail informatik@vdma.org
Internet industrialsecurity.vdma.org
Vereinsregister AG Frankfurt/Main, Nr. VR4278

**Informatik**
Abteilungsleiter:
Prof. Claus Oetter

Präsident:
Carl Martin Welcker
Hauptgeschäftsführer:
Thilo Brodtmann

## Rechtlicher Hinweis

Die Sachlage zum Thema Cyber Security ist in China alles andere als stabil. Zwar ist das Cyber Security Gesetz (Cyber Security Law) verabschiedet, aber die zur Umsetzung notwendigen Rechtsverordnungen befinden sich größtenteils noch in Abstimmung. Beachten Sie, dass sich die Rechtslage in China sehr schnell ändern kann und ein Handeln, das heute noch rechtmäßig ist, morgen unzulässig sein kann. Wir empfehlen daher eine regelmäßige Überprüfung der eigenen Vorgehensweise auf Gesetzeskonformität.
Die Abteilung Recht des VDMA benennt Ihnen hierzu gerne entsprechende Rechtsanwälte.

Die Erkenntnisse und Empfehlungen in diesem Faktenpapier wurden auf Basis von nicht-amtlichen Übersetzungen aktuell verfügbarer Entwürfe und verabschiedeter Gesetze formuliert und dienen ausschließlich der Information. Keinesfalls lässt sich ein Anspruch auf Vollständigkeit und Richtigkeit ableiten. Das vorliegende Dokument ist also in keiner Form als rechtliche Beratung zu verstehen. Es wird ausdrücklich darauf hingewiesen zur abschließenden Einschätzung des konkreten Sachverhalts Rechtsanwälte mit entsprechender Expertise zu konsultieren.

## Internet vs. China Internet

Mit der permanenten Anbindung von China an das Internet im Jahr 1994 haben frühzeitig regulatorische Anordnungen Einzug gehalten. In der ersten Anordnung aus dem Jahr 1994 ("*Regulations of the People's Republic of China for Safety Protection of Computer Information Systems*") wird bereits auf die Nutzung des Internet im Einklang mit staatlichen Interessen hingewiesen.[3]

Ebenfalls in den späten 90er Jahren wurden die technischen Weichen für eine weitreichende Zensur der Internetzugänge in China gestellt. Die so genannte „*Great Firewall of China*" (GFW oder GFC) wird seitdem vom "*National Computer Network Emergency Response Technical Team Coordination Center of China*" (CNCERT/CC) unter dem Dach des "*Ministry of Industry and Information Technology (MIIT)*" betrieben. Die Vorgaben, welche Webseiten und Schlüsselwörter geblockt oder gefiltert werden sollen, kommen direkt von der chinesischen Regierung. Übergeordnetes Ziel ist die nationale Sicherheit („*National Security*"), womit insbesondere der Schutz und Erhalt der Gesellschaftsstruktur Chinas gemeint ist. Es wird propagiert, dass sowohl Staat und Bürger vor negativen, äußeren Einflüssen geschützt werden sollen. Inoffizielles Ziel der neuen Regulierung ist es, alle anonymen VPN Dienste massiv einzuschränken und insbesondere Individuen an einem unkontrollierten Weg in das „freie Internet" zu hindern.

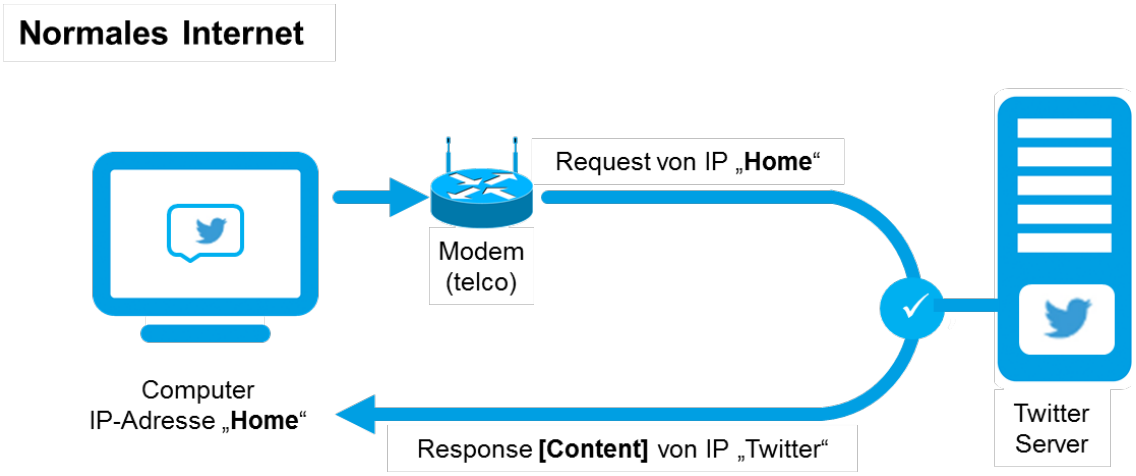


*Abbildung 1: Webseiten wie Twitter.com werden geladen, wenn der Computer an den Server eine Anfrage sendet. Zusammen mit den angefragten Daten wird die eigene IP-Adresse des Servers zurückgesendet. Die Seite ist erreichbar. (Quelle: nicos AG)*

Normale Internetverbindungen werden auf Seiten der Telekommunikationsanbieter gemäß dem Grundsatz der Netzneutralität nicht gefiltert. Der Deutsche Bundesrat sieht solche einen diskriminierungsfreien Zugang zum Internet als notwendig an, um „*eine gleichberechtigte und uneingeschränkte Teilhabe der Bürgerinnen und Bürger am offenen Internet als einem zentralen Medium unserer Informationsgesellschaft zu gewährleisten*"[4]. Ein Webseitenaufruf wird grundsätzlich weder blockiert noch gefiltert (Abbildung 1).

[3] Vgl. (Chen & Yang, 2018), S. 50.
[4] http://www.computerundrecht.de/0689_13_B.pdf

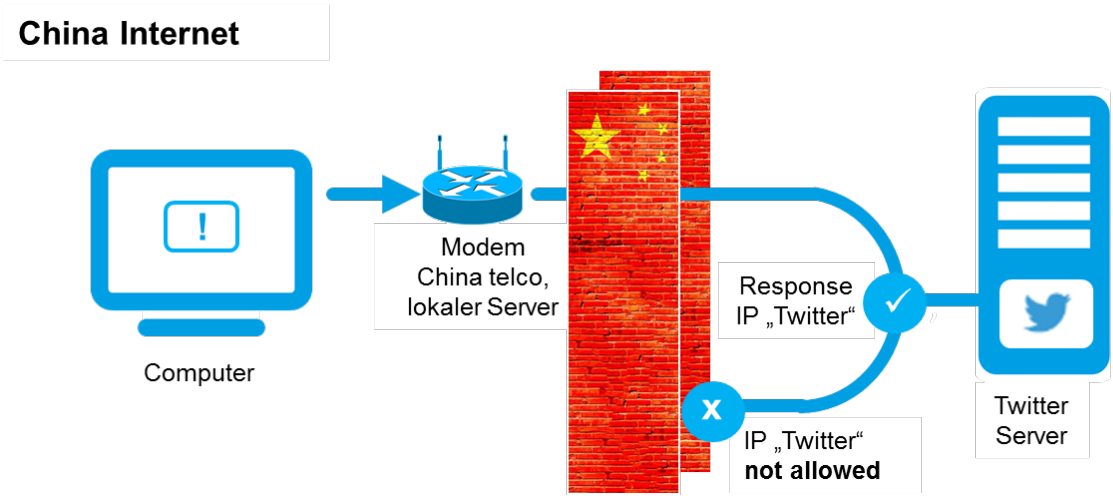


*Abbildung 2: Die „Great Firewall China“ filtert und blockiert „verbotene“ Inhalte, die zwischen den lokalen Servern (China Mainland) und Übersee-Servern fließen. Antworten von IP-Adressen bestimmter Dienste werden nicht zugelassen und erreichen damit den lokalen Computer nicht. (Quelle: nicos AG)*

Der Zugang zu Diensten und Webseiten aus China heraus wird durch die chinesische Firewall eingeschränkt. Dabei sind technisch gesehen alle Anfragen möglich, aber der Datentransfer von bekannten und in der Firewall eingepflegten Internetadressen (IP-Adressen) wird blockiert (Abbildung 2). Da das System auf einer „Blacklist“ von Internetadressen basiert, muss dieses System seitens der Behörden mit einem hohen Pflegeaufwand aktuell gehalten werden. Solch einer Blockade Ihrer Quell-IP-Adresse außerhalb China Mainland unterliegen jährlich mehrere VDMA-Mitglieder, ohne dass für diese Unternehmen eine Möglichkeit zur Aufhebung der Sperre besteht. Jegliche Sperren von IP-Adressen in der chinesischen Firewall sind nachhaltig. Diese Blockaden wirken sich daher in Besonderem auf feste IP-Adressen und statische Verbindungen aus.

## Umgehung von Zugangsbeschränkungen mittels VPN Lösungen

Sowohl Privatleute als auch Unternehmen nutzen weltweit VPN-Anwendungen, um eine vertrauliche Kommunikation mit Diensten und Unternehmen sicherzustellen. Der Schutz von personenbezogenen Daten, von vertraulichen Informationen und Unternehmens-Know-how steht hierbei im Mittelpunkt. Chinesische Bürger, Expats und Dienstreisende haben zu diesem Zweck in der Vergangenheit immer wieder Mittel und Wege gesucht, ihre Verbindungen abzusichern. In der Regel werden hierzu VPN-Dienste genutzt, mit denen sowohl die Vertraulichkeit von Daten sichergestellt wird als auch die Blockade von Diensten in der chinesischen Firewall umgangen werden kann. Dies ist, sofern hierfür keine lizensierten VPN-Verbindungen genutzt werden, nach chinesischem Recht illegal und wird entsprechend sanktioniert. So unterbinden chinesische Behörden solche unlizenzierten Verbindungen, insbesondere bei Verdacht auf gesetzeswidrige Nutzung, bereits nach kurzer Zeit.

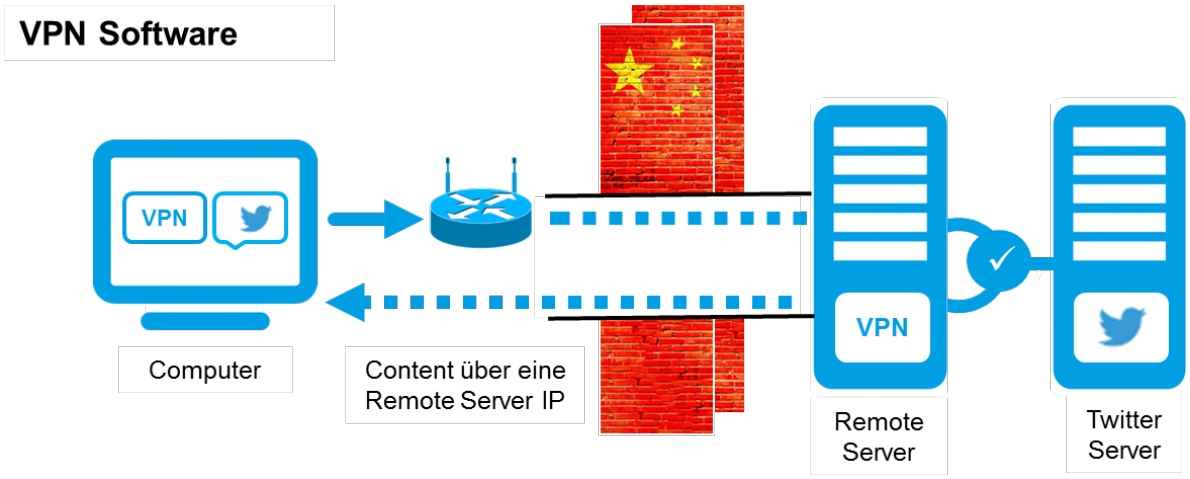


*Abbildung 3: Die VPN-Software wird auf einem lokalen Computer in China und einem entfernten Server außerhalb Chinas installiert und baut zwischen diesen einen verschlüsselten Tunnel auf. Für den Verbindungsaufbau zu Twitter werden die Daten vom lokalen Computer durch den versschlüsselten VPN-Tunnel zu dem entfernten VPN-Server gesendet. Dieser stellt die eigentliche Verbindung zum Twitter-Server her. Die zurückgesandten verschlüsselten Daten werden nicht von der Firewall als Twitter-Daten erkannt und daher nicht blockiert.*
*(Quelle: nicos AG)*

Die Technologien, sowohl zur Umgehung der chinesischen Firewall als auch die Blockade von verschlüsselten Verbindungen, liefern sich seit Jahren ein wahres Katz-und-Maus-Spiel.

## Blockade von VPN durch chinesische Diensteanbieter

Die chinesischen Behörden haben erkannt, dass die Bemühungen zur technischen Unterbindung von verschlüsselten Verbindungen nicht generell greifen. Daher wurde nun mit der neuen Regulierung von Internetzugangsdiensten die Provider verpflichtet, bei Kenntnis einer illegalen Nutzung von Leitungen oder VPN-Verbindungen die entsprechenden VPN-Dienste zu blockieren bzw. Internetzugänge komplett abzuschalten.

## Betroffenheit von VDMA-Mitgliedsunternehmen

Da deutsche, aber auch andere international tätige Unternehmen mit ihren Niederlassungen in China i.d.R. über verschlüsselte Verbindungen (VPN) Daten austauschen, können auch diese Verbindungen grundsätzlich „reguliert“ bzw. abgestellt werden.

In der Vergangenheit wurden VDMA-Mitglieder mehrfach Opfer von dauerhaften Abschaltungen oder Blockaden in der chinesischen Firewall:

- Blockade der deutschen IP-Adresse(n), diese sind aus China heraus nicht mehr erreichbar
- Verlangsamung von verschlüsselten Verbindungen, so dass Dienste (z.B. ERP-Anbindung) unbenutzbar werden
- Abschaltung des Internetzugangs in der chinesischen Niederlassung durch den chinesischen Anbieter
- Abschaltung oder Blockade des mobilen Internetzugangs
- Blockade von verschlüsselten Verbindungen (VPN) zu Diensten außerhalb Chinas

Abschaltungen bzw. Blockaden sind dauerhaft und erfolgten in der Vergangenheit regelmäßig aus einem dieser zwei Gründe:

- Mitarbeiter des Unternehmens nutzten verschlüsselte Verbindungen, um auf in China nicht zugelassene Internetdienste oder Portale zuzugreifen (z.B. Twitter, Facebook);
- Das Unternehmen betrieb einen nicht zugelassenen VPN-Dienst, z.B. SSL-VPN, um die Datenübertragung zur Zentrale im Ausland (Deutschland) kostengünstig zu verschlüsseln.

Dabei ist festzuhalten, dass mehrere Mitgliedsunternehmen teilweise über einen sehr langen Zeitraum unbehelligt auch nicht zugelassene VPN-Verbindungen aufbauen und nutzen konnten. Näherten sich jedoch aus Sicht der chinesischen Regierung wichtige Termine, Veranstaltungen oder Jahrestage, so fand eine gezielte Bereinigung der bis dahin geduldeten VPN-Nutzung statt. Beispiele für solche kritischen Termine sind:

- Tagungen des Nationalen Volkskongresses im März (zuletzt 5. März 2019)
- Jahrestag der Proteste chinesischer Studenten im Juni (Tiananmen, 4. Juni 1989)
- Proteste in Hongkong (September 2019)

## Rechtliche Anforderungen aus dem Cyber Security Law

Um die technische Umsetzung eines zuverlässigen Datenaustausches zwischen Deutschland und China sicherzustellen, müssen Maschinen- und Anlagenbauer die Einbettung der technischen Maßnahmen in notwendige organisatorische Maßnahmen sicherstellen.
Insbesondere die Beachtung von Anforderungen, die sich aus dem im Jahr 2017 verabschiedeten Cyber Security Law ergeben, schränken die Möglichkeiten einer sicheren, grenzüberschreitenden Vernetzung ein.
Das Cyber Security Law (CSL) legt den Fokus auf Nationale Sicherheit, den Schutz chinesischer IT-Infrastrukturen, auf Datenschutz und auf nationale Souveränität. Es formuliert

- Importbeschränkungen von Security-Produkten,
- Anforderungen an den sicheren Betrieb von IT-Netzwerken
- Einschränkungen für Datenexport
- Bestimmungen zum Datenschutz

Der VDMA hat zum Cyber Security Law ein Infoblatt veröffentlicht.[5]

Aus der Pflicht zur lokalen Datenspeicherung ergibt sich zum Beispiel, dass ein Export von Daten ausschließlich nach bestandener Sicherheitsüberprüfung erlaubt ist. Dabei muss gegenüber einer Kommission aus Experten glaubhaft dargelegt werden, warum dieser Export für die Geschäftsaktivitäten notwendig sein sollte. Die Sicherheitsüberprüfung wird im Auftrag eines „*Büros für Sicherheitsüberprüfung*“ unter der durch die China Cyberspace Administration (CAC) etablierten „*Kommission zur Sicherheitsüberprüfung*“ durch Tests und Inspektionen vor Ort ausgeführt. Die Überprüfung basiert auf den Kriterien Rechtmäßigkeit, Notwendigkeit und Legitimität sowie der Einschätzung der Risikofaktoren, die durch den Datentransfer entstehen. Die Ergebnisse der Prüfung werden einem Expertenkomitee zur Entscheidung vorgelegt.

Mit der Sicherheitsüberprüfung einher gehen technische Anforderungen an die Übertragungstechnik. So dürfen nur in China zugelassene Produkte verwendet werden, deren kryptographische Verfahren zur Datenübertragung durch die OSCCA[6] freigegeben sind.

All dies hat Auswirkungen auf die technische legale Umsetzung und Nutzung der VPN-Verbindung.

[5] https://www.vdma.org/v2viewer/-/v2article/render/22344784 (Abrufdatum: 11.05.2018)
[6] OSCCA: Office of the State Commercial Cryptography Administration

## Umsetzungsempfehlungen VPN

Nachfolgend finden Sie aus Sicht des VDMA zusammengefasst die rechtlichen und technischen Empfehlungen, die Ihnen einen zuverlässigen Betrieb eines länderübergreifenden Datenaustausches ermöglichen sollen.

### Betriebliche Empfehlungen

- Machen Sie das Thema zu einem Geschäftsführungsthema! Es gehört nicht in die IT.
- Benennen Sie einen IT-Security-Beauftragten, der die organisatorische und technische Umsetzung steuert und überwacht. Diese Person kann durchaus in Deutschland sitzen.
- Nutzen Sie Unternehmen vor Ort, die Ihnen bei der technischen Umsetzung helfen. Dies kann auch ein deutsches Systemhaus sein, welches über Erfahrungen im Umgang mit der Einrichtung von Verbindungen verfügt.
- Prüfen Sie, ob eine Datenübertragung für den Betriebsprozess wirklich notwendig ist.
- Finden Sie heraus, welche Daten als „wichtig“ oder „sensibel“ anzusehen sind und damit der lokalen Datenspeicherpflicht unterliegen könnten.

### Technische Empfehlungen

- Nutzen Sie zwei technisch separate Leitungen für Internet und VPN, um die Datenübertragungen der Mitarbeiter von denen der IT-Systeme zu trennen.
- Unterbinden Sie mit Hilfe von Webfiltern die private Nutzung des Internets, um Sperrungen Ihres Anschlusses vorzubeugen.
- Nutzen Sie für die wichtigen IT-Systeme oder grenzüberschreitenden Datenaustausch eine lizensierte Leitung mit erhöhter Verfügbarkeit für Business-Kunden.
- Nutzen Sie bei der „Business-Leitung“ je nach Verfügbarkeitsanforderung für VPN-Verbindungen zulässige Angebote für Industrial Internet von
    - China Unicom (AS9929, bisher keine Einschränkungen) oder
    - China Telekom Global Internet Service (AS4809, kleine Einschränkungen) oder
    - Dedizierte MPLS-Leitungen (höchste Verfügbarkeit, teuer).
- Klären Sie gemeinsam mit Ihrem Dienstleister oder Technologieanbieter, inwieweit eine Zulassung von Software oder Hardware zur verschlüsselten Datenübertragung notwendig ist und diese eingereicht bzw. erteilt wurde.

### Datenspezifische Empfehlungen

- Speichern Sie chinesische Daten in China, wenn Sie keine entsprechende Freigabe oder Zulassung zur Datenübertragung bzw. -speicherung im Ausland beantragt haben.
- Nutzen Sie für Cloud-Dienstleistungen weltweit anerkannte Partner mit einem Endpunkt in „Mainland China“ (nicht Hongkong). Dann muss der Partner für die notwendigen Zulassungen sorgen.

## Erfahrungen der nicos AG

*„Die nicos AG als Managed Service Dienstleister in den Bereichen (WAN und Security) verfügt über langjährige Erfahrung in Bezug auf die Vernetzung internationaler Standorte ihrer Kunden. Performance-Probleme und das Blockieren von Verbindungen von und nach China gehören nach unserer Erfahrung seit vielen Jahren zur Normalität. Wenn eine Verbindung geblockt wird, ist dieses nicht steuer-/regelbar, so dass wir in diesen Fällen individuelle Alternativlösungen mit lizensierten Providern für unsere Kunden erarbeiten, um die Verbindung der Standorte schnellst möglich wiederherzustellen. Hierzu pflegen wir sehr enge Beziehungen zu den Carriern und unseren Rechtsberatern. Wir stehen in ständigem Austausch um schnell auf neue Entwicklungen reagieren und Kundenschaden abwenden zu können.*
*Nach unseren bisherigen Erkenntnissen haben sich mit dem Abschluss der Regulierungsmaßnahmen bzw. seit dem 01.04.2018 keine Änderungen in Bezug auf Blocking-Aktivitäten ergeben. Dies stützt unsere Vermutung, dass sich die Regulierungsmaßnahmen in erster Linie auf von „Gray Line Providern“ angebotene VPN-Dienste beziehen, die von Individuen genutzt werden und Netzwerke für die grenzüberschreitende Unternehmenskommunikation nicht im Fokus stehen. Nach neusten Erkenntnissen aus den im Dezember 2019 geführten Gesprächen lässt sich eine Verschiebung des Fokus auf den Inhalt und die Notwendigkeit der übertragenen Daten erkennen. (Stichwort: Datenschutz, Data Privacy)*
*Auf Grund unserer Erfahrung, lässt sich das Risiko eines Verbindungsausfalls durch den Einsatz von MPLS Leitungen minimieren. Da es sich hierbei jedoch, im Vergleich zu internetbasierten VPN Verbindungen, um eine hochpreisige Lösung handelt, empfiehlt es sich die Technologie vorrangig für (zeit-)kritische Datenkommunikationen einzusetzen.*
*Eine weitere Reduktion des Ausfallrisikos kann durch die Implementierung von Redundanzen in Bezug auf die Leitung und deren Anbieter erzielt werden.*
*Grundsätzlich wird Unternehmen in China empfohlen, dass der Zugriff auf „verbotene Inhalte“ für die Mitarbeiter der lokalen Gesellschaften unterbunden werden sollte („[…] It is when users are "going" to these "unapproved" sites, that the Chinese government blocks all the traffic”[7]).*
*In Bezug auf die Erfordernis von behördlichen Genehmigungen für den Einsatz und die Nutzung von Kryptografie Produkten in China empfehlen wir Ihnen, mit Rechtsanwälten vor Ort in Kontakt zu treten, um Rechtssicherheit zu erhalten.*
*Gerne stehen wir den VDMA Mitgliedern als die Spezialisten der nicos AG für den Aufbau und Betrieb von chinesischen und natürlich auch weltweiten verschlüsselten Datenanbindung zur Verfügung.“*

[7] Nathalie Elizeon (Globalinternet; Partner der nicos AG), per E-Mail vom 20.03.2018.

## Ansprechpartner VDMA in China

Claudia Barkowsky
VDMA-Verbindungsbüro China (Beijing)
+86 10 87730212-808
claudia.barkowsky@chinavdma.org

## Ansprechpartner der nicos AG

Axel Metzger,
Vorstand
+49 251 98633 5102
ametzger@nicos-ag.com

Jost Bertels
Carrier Manager Access Solution Center
+49 251 986 33 5509
jbertels@nicos-ag.com

China VPN Faktenpapier VDMA-nicos v6.docx
01.04.2020

## Ansprechpartner im VDMA (Frankfurt)

Oliver Wack
Abteilung Außenwirtschaft
+49 69 6603-1444
oliver.wack@vdma.org

Hermann Wegner
Abteilung Technik, Umwelt und Nachhaltigkeit
+49 69 6603-1899
hermann.wegner@vdma.org

Daniel van Geerenstein
Abteilung Recht
+49 69 6603-1359
daniel.vangeerenstein@vdma.org

Steffen Zimmermann
Competence Center Industrial Security
+49 69 6603-1978
steffen.zimmermann@vdma.org