merics
Mercator Institute
for China Studies

China Monitor

Nummer 22 | 18. Februar 2015

Cyber Security in China (III): Standortfaktor Internetsicherheit: Herausforderung für westliche Unternehmen

Cyber-Souveränität. Verschärfte Internetzensur. IT-Schattenwirtschaft.

von Hauke Johannes Gierow

ZENTRALE BEFUNDE UND SCHLUSSFOLGERUNGEN

- China fördert bewusst den Aufbau einer eigenen IT-Industrie und schottet sich zunehmend von internationaler IT-Technologie ab. Durch die Kontrolle der großen Staatsunternehmen behält China gleichzeitig die Souveränität im IT-Bereich.

- Die Regierung unterstützt relevante Firmen im IT-Bereich – die sogenannten nationalen Champions – bei der internationalen Expansion und bei ihren Verkaufsbemühungen. Diese Verzahnung von Politik und Wirtschaft löst bei westlichen Kunden häufig Sicherheitsbedenken aus.

- China entwickelt Parallelstandards im Bereich Soft- und Hardware. Zudem sollen alternative Verschlüsselungsstandards, Betriebssysteme und konkurrierende App-Stores Chinas Unabhängigkeit im IT-Bereich stärken. Unzureichende Qualitätsvorgaben bedrohen jedoch die IT-Sicherheit.

- Zensur und gedrosselte Internetverbindungen wirken sich zunehmend negativ auf den Standort China aus. Aus Sorge vor IT-Spionage und Diebstahl von Geschäftsgeheimnissen verlagern internationale Unternehmen Personal und ganze Abteilungen ins asiatische Ausland.

- Eine IT-Schattenwirtschaft bedroht chinesische Internetnutzer. Denn auf Computern sind oft illegale Programme installiert, die nicht mit Sicherheitsupdates versorgt werden. Hacker können diese ungeschützten Rechner übernehmen und damit weltweit Systeme angreifen.

- Statt auf eine grundlegende Änderung der chinesischen Internetpolitik zu drängen, sollte die Bundesregierung konkrete Verbesserungen für deutsche Unternehmen aushandeln, etwa im Bereich Marktzugang oder beim Schutz von Urheberrechten.

1 Keine Internetsicherheit ohne eigene Technologie

Anfang 2014 haben 15 private chinesische IT-Hersteller im Beijinger Stadtteil Zhongguancun (中关村) – dem Silicon Valley Chinas – eine Allianz gegründet. Damit verstärken sie bestehende Bemühungen zur Entwicklung eines chinesischen Betriebssystems auf Linux-Basis, das künftig auf Regierungscomputern und auf Rechnern sicherheitsrelevanter Unternehmen und Banken laufen soll: **Mit diesem Schritt möchte sich Beijing gegen Spionage aus den USA absichern und die Innovationskraft der chinesischen IT-Wirtschaft demonstrieren.**[1]

China ist trotz des rasanten Wachstums der IT-Industrie noch abhängig von ausländischer Technologie. 2012 stammten nach Angaben der staatlichen Nachrichtenagentur Xinhua 90 Prozent der Mikrochips und 65 Prozent der Firewall-Produkte aus dem Ausland, vor allem aus den USA.[2]

Doch die Regierung betrachtet die ausländische Technologie als potenzielle Bedrohung der nationalen Sicherheit, etwa durch heimlich eingebaute Hintertüren, die die Möglichkeit zur Ausforschung von Computern und Netzwerken bieten. In sicherheitskritischen Bereichen ist die Verwendung ausländischer IT-Produkte deswegen bereits streng reguliert.

Die Abschottung des Marktes soll gleichzeitig die industrie- und innovationspolitische Entwicklung in China vorantreiben:[3] Die Regierung in Beijing will die heimischen IT-Unternehmen wettbewerbsfähiger machen (siehe MERICS China Monitor Nr. 20).

2 Cyber Security: Chancen und Kosten für die chinesische IT-Wirtschaft

2.1 Gezielte staatliche Förderung

Der chinesischen Regierung ist es gelungen, eine dynamische IT-Industrie mit starken Privatunternehmen zu fördern und gleichzeitig die Kontrolle über den Bereich zu behalten. Die staatseigenen Telekommunikationsanbieter (China Telecom, China Unicom, China Mobile) beeinflussen mit ihren Investitionen maßgeblich den Markt. Ihre von der Regierung gebilligten Entscheidungen geben vor, welche Technologien überhaupt entwickelt werden und legen damit auch die Rahmenbedingungen für die Branche und ihre Regularien fest.[4] Darüber hinaus fördert die Regierung eigene Technologiestandards durch staatliche Programme, meist in enger Kooperation mit chinesischen IT-Firmen wie ZTE, Lenovo, Datang Mobile und anderen.

Chinesische Unternehmen sind zunehmend erfolgreich im Bereich der IT-Infrastruktur – auch aufgrund der staatlichen Förderung. Neben den international bekannten Netzwerkausrüstern Huawei und ZTE etablieren sich neue Unternehmen: Firmen wie Inspur und Dawning Industries (曙光) entwickeln Server und Supercomputer für komplexe Rechenaufgaben mit chinesischer Technologie, bislang vor allem für den heimischen Markt (siehe Übersicht 1). **Diese Technologie ist für sichere Netze von besonderer Relevanz, da selbst kleine Fehler im Programmcode die Basis sicherer IT-Produkte zerstören.**

China wird in den kommenden Jahren unabhängiger von ausländischen IT-Produkten werden. Ob die Netzsicherheit dadurch insgesamt steigen wird, ist unter Experten jedoch umstritten. Ein wichtiges Kriterium für die Sicherheit von Software ist zum Beispiel die Einhaltung von Qualitätsstandards – etwa die Kontrolle der Lieferkette und eine unabhängige Prüfung des Quellcodes. Zahlreiche IT-Firmen in China beachten diese Standards aber nicht.

Auch bei der Verschlüsselung bestehen noch Probleme. Dieser Teil der IT-Infrastruktur schützt etwa Festplatten, Dokumente oder auch Internetverbindungen vor unbefugtem Zugriff. Chinesische Firmen dürfen internationale Standards wie den von vielen Regierungen und Konzernen genutzten RSA-Standard aufgrund strenger Importregelungen jedoch nur in Ausnahmefällen nutzen. Stattdessen sind sie auf chinesische Verschlüsselungsverfahren angewiesen – doch diese schützen nur teilweise. Denn chinesische Anbieter müssen eine Art „Generalschlüssel" bei der Nationalen Führungsgruppe für Verschlüsselung (国家密码管理局) hinterlegen (sog. *Key-Escrow*-Verfahren).[5] Damit sind die Informationen zwar vor Hackern und fremden Regierungen geschützt – doch die Regierung in Beijing kann sie durch den Zugriff auf die Generalschlüssel jederzeit auslesen.

2.2 Going Out – Chance und Herausforderung für chinesische Unternehmen

Chinesische IT-Firmen machen mit ihren IT-Produkten westlichen Firmen in Entwicklungs- und Schwellenländern zunehmend Konkurrenz.

Übersicht 1: Chinesische IT-Anbieter und ihre westlichen Konkurrenten. (Eigene Darstellung: Hauke Gierow)

用友 yonyou	**Gegründet:** 1988 **Umsatz:** 6,41 Mrd. USD (2011) **Aktivitäten:** Marktführer für Customer Relationship Management (CRM) und andere Business-Lösungen in China **Kunden:** mehr als 1,5 Millionen Unternehmenskunden, davon 60 Prozent der TOP 500 Unternehmen in China (nach eigenen Angaben)	SAP, ORACLE
inspur 浪潮	**Gegründet:** 2000 **Umsatz:** ca. 5,92 Mrd. USD (2011) **Aktivitäten:** Hersteller von Servern und Supercomputern **Kunden**: U.a. chinesische Banken und „strategisch wichtige Firmen"	IBM, HEWLETT PACKARD
HUAWEI	**Gegründet:** 1988 **Umsatz:** 39,7 Mrd. USD (2013) **Aktivitäten:** Hersteller von Mobilfunk-Basisstationen, Netzwerktechnologie und Mobiltelefonen, Erfinder des UMTS-Sticks **Kunden:** Mobilfunkprovider weltweit. Beliefert auch in Deutschland alle großen Netzbetreiber (T-Mobile, Vodafone, O2, E-Plus).	NOKIA, ERICSSON
360 www.360.cn ©merics	**Gegründet:** 2005 **Umsatz:** 329 Millionen USD (2012) **Aktivitäten:** Antivirus Software, Internet-Browser, App-Stores **Kunden:** Vor allem chinesische Firmen und Privatanwender	Norton by Symantec, KASPERSKY ANTIVIRUS

Das chinesische Ministerium für Industrie und Informatisierung（中华人民共和国工业和信息化部) verfolgt seit 1999 die sogenannte *„Going Out"*-Strategie (走出去): Damit werden erfolgreiche chinesische Unternehmen gezielt auch international wettbewerbsfähig gemacht. Diese Strategie wurde auch auf den IT-Sektor ausgedehnt. Mit günstigen

Krediten und der tatkräftigen Unterstützung der chinesischen Botschaften will die Regierung die Wettbewerbsfähigkeit dieser nationalen Champions auf internationalen Märkten stärken.[6] Huawei etwa bekam von der China Development Bank einen zinsgünstigen Kredit über zehn Mrd. US-Dollar, um seine internationale Expansion zu finanzieren.[7]

Die gezielte Förderung des IT-Bereichs bringt jedoch auch Probleme für chinesische Firmen mit sich: Denn chinesische Technologie wird von verschiedenen Staaten als Sicherheitsbedrohung wahrgenommen – obwohl es bislang keine konkreten Hinweise auf von der Regierung platzierte Hintertüren in Routern, Handys oder anderen Geräten gibt. Ein Angebot von Huawei, die Londoner U-Bahn im Rahmen der Olympischen Spiele 2012 kostenfrei mit Mobilfunktechnologie im Wert von mehr als 500 Mio. CNY (ca. 65 Mio. EUR) auszurüsten, lehnte die britische Seite wegen Sicherheitsbedenken ab.[8]

Sowohl die Unternehmen als auch die chinesische Regierung versuchen nun, das Misstrauen in ihre Produkte zu zerstreuen: Huawei etwa begegnet den Bedenken in Europa mit einer Transparenzinitiative: In Großbritannien hat der Konzern ein Forschungszentrum errichtet, das unabhängige Sicherheitsuntersuchungen des Programmcodes durch die britische Regierung ermöglicht.[9]

Eine andere Taktik wendet der weltweit drittgrößte Handyhersteller Xiaomi (小米) an. Um Sorgen vor Hintertüren im eigenen Cloud-Dienst in China zu begegnen, errichtet die Firma in wichtigen Märkten wie Indien sogenannte „lokale Clouds“. Die Nutzer vor Ort können ihre Kontakte, Kalendereinträge und weitere Daten dort ablegen und müssen sie nicht in China speichern. Hierbei dürfte es sich jedoch in erster Linie um eine vertrauensbildende Maßnahme handeln.

In einigen ausländischen Märkten sind chinesische Unternehmen trotz Bedenken bereits äußerst erfolgreich. Auf dem Privatkundenmarkt in Europa und den USA zählen etwa Huawei und Lenovo zu den wichtigsten Herstellern für Informationstechnologie. Mit einem Marktanteil von knapp 17 Prozent lag Lenovo im Jahr 2014 bei PCs bereits vor dem bislang führenden Konzern HP.[10]

In der Mobilfunkinfrastruktur gehören chinesische IT-Firmen sogar schon zur Weltspitze. Während die chinesische UMTS-Alternative TD-SCMA außerhalb Chinas nur in Nicaragua und Zimbabwe genutzt wird, sind Netzwerke mit der neuen chinesischen Technologie FDD-LTE auch in Deutschland und anderen europäischen Ländern installiert.

2.3 Alternative Ökosysteme: Eigene App-Stores und Betriebssysteme mit Sicherheitslücken

Die Nutzer in China bewegen sich zum großen Teil in einem eigenen digitalen Ökosystem. Für viele Anwendungen aus dem Westen wurden chinesische Alternativen entwickelt.

In Deutschland laden Nutzer von Android-Geräten Apps oder digitale Inhalte wie Filme und Bücher vor allem über den Google-eigenen App-Store *Google Play* herunter. Doch in China ist *Google Play* gesperrt, und Unternehmen wie Baidu, Tencent oder Qihoo 360 bieten alternative App-Stores an. Im Vergleich zu *Google Play* weisen sie jedoch erhebliche Sicherheitsmängel auf: Eine Untersuchung von 7.000 mit Viren infizierten Apps ergab: 95 Prozent der Viren stammten aus chinesischen Quellen. [11] Ein von einem Studenten entwickelter Handy-Virus zeigte die Gefahren: Innerhalb weniger Stunden infizierte er mehr als 100.000 Android-Geräte in China. Der Virus verbreitete sich über das Adressbuch weiter und erlaubte die Kontrolle fast aller Telefonfunktionen.[12]

Auch auf dem PC-Markt möchte die chinesische Regierung alternative Systeme verbreiten: Seit mehr als fünf Jahren forciert sie daher die Entwicklung eigener Betriebssysteme. Von 2015 an sollen jedes Jahr jeweils 15 Prozent der Behördencomputer von Windows auf chinesische Betriebssysteme umgestellt werden. Die bekanntesten sind *NeoKylin OS* und *Red Flag Linux.*

Komplett ausgereift sind die chinesischen Technologien aber noch nicht: Nutzer klagen über Kompatibilitätsprobleme, fehlende Software und mangelnde Benutzerfreundlichkeit – ein Defizit, das der eingangs erwähnte Zusammenschluss von IT-Firmen beseitigen soll.

2.4 Hohe Kosten der Internetzensur

Abschottung und Protektionismus bringen für chinesische IT-Unternehmen ein weiteres Problem mit sich: die Verpflichtung zur Internetzensur. Diese betrifft demnach nicht nur die Meinungsfreiheit, sondern auch die Wirtschaft.

In China ein soziales Netzwerk zu betreiben ist kostspielig. Der Nationale Arbeitsstab für Internet-Information (国家互联网信息办公室) macht hohe Auflagen: Um der Internetkontrolle zu genügen, müssen die Anbieter pro 50.000 Nutzer zwei bis drei Zensoren beschäftigen.[13] Für Sina Weibo mit seinen rund 300 Millionen Nutzern heißt das: 15.000 Mitarbeiter werden allein für die Kontrolle der Inhalte beschäftigt. Das ist ein gewaltiger, mit finanziellen Nachteilen verbundener Aufwand. Zum Vergleich: Beim Branchenprimus Facebook arbeiten nach eigenen Angaben weltweit gerade einmal 8.500 Beschäftigte.[14]

Internetzensur behindert zudem die Entwicklung von Software oder Apps. Google und andere Anbieter stellen Entwicklern weltweit kostenfrei Programmbibliotheken und Webschriftarten zur Verfügung. Dieser Service ist für die Programmierer hilfreich, denn er spart Zeit und Kosten. Weil die Daten in China durch die Internetzensur blockiert sind, müssen die dortigen Programmierer sie eigens nochmal selbst entwickeln.[15]

3 *Cyber Security* als Standortfaktor für ausländische Unternehmen

3.1 Zensur und Cyber-Angriffe behindern das Geschäft

Ausländische Unternehmen müssen in China immer strengere Regeln im IT-Bereich beachten – darunter leiden der Schutz ihrer Geschäftsgeheimnisse und die internationale Kooperation.

Für Apple ist China der wichtigste Markt weltweit, das iPhone ist sehr beliebt. Im Oktober 2014 wurde bekannt, dass chinesische Hacker gezielt die Datenübermittlung an den *iCloud*-Dienst des Unternehmens ausspioniert hatten. Aufgrund der Komplexität des Hacks vermuteten IT-Experten, dass die chinesische Regierung hinter dem Angriff steckte oder zumindest Kenntnis davon hatte.[16] Sicher ist jedoch nur: Wenige Tage später reiste Apple-Chef Tim Cook nach Beijing und führte in der Parteizentrale Zhongnanhai (中南海) Gespräche mit wichtigen Entscheidungsträgern. Der Fall zeigt, dass Beijing sich mit den Sicherheitsbedenken großer westlicher Firmen trotz seiner Marktmacht auseinandersetzen muss.[17]

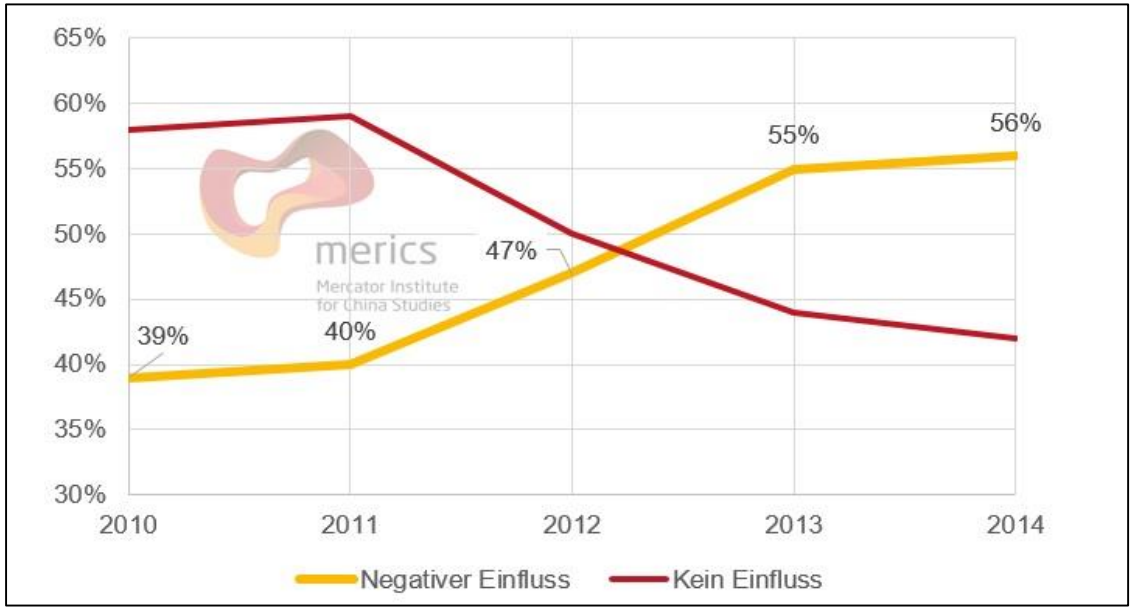
Auch andere Unternehmen bekommen die Folgen von *Cyber*-Angriffen und Zensur zu spüren: Die internationale Zusammenarbeit mit Diensten wie *Gmail*, *Google Docs* oder *Dropbox* funktioniert immer seltener. Ebenso der Gebrauch von Virtuellen Privaten Netzwerken (VPN), mit denen die Nutzer Informationen und Geschäftsgeheimnisse schützen wollen.[18] Auch die alltäglichen Arbeitsabläufe

globaler Konzerne funktionieren in der Volksrepublik China nur eingeschränkt. So werden in internationalen Unternehmen viele Business-Anwendungen wie Statistik- oder Datenbankprogramme nicht auf dem lokalen Rechner, sondern auf Servern in der Unternehmenszentrale ausgeführt. Bei langsamen Verbindungen oder instabilen VPNs sind sie von China aus nicht immer zu erreichen. Allein die Übertragung einzelner Dateien an Kollegen im Ausland kann zum Geduldsspiel werden.

In einer Umfrage der Amerikanischen Handelskammer in China gaben mehr als die Hälfte der befragten US-Unternehmen an, dass Internetzensur ihr Geschäft negativ beeinflusse (siehe Übersicht 2).[19] Die zuletzt deutlich verstärkte Blockade von Webseiten und Online-Werkzeugen hat diese Tendenz weiter verschärft: Mehr als 80 Prozent der europäischen Firmen in China sprechen von negativen Auswirkungen auf ihre Geschäftsaussichten. 13 Prozent haben Investitionen in Forschung und Entwicklung auf Grund der aktuellen Ereignisse verschoben.[20]

Medienberichten zufolge verlagern erste internationale Konzerne wie General Motors ihre Asienzentralen bereits nach Singapur, Japan oder Vietnam. Als Gründe gelten neben der Zensur auch Faktoren wie die schlechte Luftqualität oder mangelnder Schutz geistigen Eigentums.[21]

Übersicht 2: Internetzensur und Wettbewerbsfähigkeit. (Eigene Darstellung: Hauke Gierow)



Fragestellung: Inwieweit beeinflusst die Zensur von Inhalten im Internet die Fähigkeit Ihrer Firma, in China normale Geschäfte zu tätigen? Quelle: AmCham China (2014): 15f.

Darüber hinaus beklagen viele Firmen seit Jahren Industriespionage, auch im digitalen Bereich. Geschäftsgeheimnisse und Konstruktionspläne sind begehrte Ziele chinesischer Hacker.

Amerikanische *Cyber-Security*-Firmen und auch das FBI beschuldigen die chinesische Regierung, die Hacker zu unterstützen oder sogar zu beauftragen. Konkrete Belege gibt es kaum. Professionelle Hacker sind in der Lage, ihre Spuren gut zu verwischen oder falsche Fährten zu legen.[22]

3.2 Technische Parallelstandards als Herausforderung für westliche Unternehmen

Westliche Anbieter auf dem chinesischen Markt müssen sich chinesischen IT-Parallelstandards anpassen. Dies zeigt sich am Beispiel der chinesischen WLAN-Technologie WAPI (*WLAN Authentication and Privacy Infrastructure)*. Obwohl sich international die Verschlüsselung nach dem Standard WPA2 durchgesetzt hat, geht China seit 2003 bewusst eigene Wege. Für ausländische Anbieter von Routern und WLAN-fähigen Geräten bedeutet dies: Sie müssen ihren Quellcode mit einer von elf lizensierten chinesischen IT-Firmen teilen und an der Entwicklung des WAPI-Standards mitwirken. Die erste Version des Apple iPhone durfte 2010 wegen mangelnder WAPI-Unterstützung in China nicht verkauft werden – bis das Unternehmen nachbesserte.[23]

Apple wird künftig sogar als erstes westliches IT-Unternehmen seine Produkte in China auf Kompatibilität mit dortigen Sicherheitsstandards untersuchen lassen. Dies hat Lu Wei, Chef des Nationalen Arbeitsstabes für Internet-Information, im Januar 2015 angekündigt. Dabei teilt das Unternehmen vermutlich vertrauliche Informationen mit der Regierung.[24] Wenn sie dauerhaften Zugang zum chinesischen Markt behalten wollen, werden auch IT-Firmen wie CISCO, Qualcomm und Microsoft um Zugeständnisse nicht herum kommen.[25]

Übersicht 3:Angebote krimineller Hackernetzwerke (Auswahl). (Eigene Darstellung: Hauke Gierow)

Angebot	Preis	Angebot	Preis	Angebot	Preis
Bankentrojaner		**Hacken von Accounts**		**Versand von Spam-E-Mails**	
• Bronze Level	1.273 USD	• Forennutzer	81 USD	• 1.000 Adressen	13 USD
• Silber Level	1.596 USD	• Administrator	323 USD	• 10.000 Adressen	97 USD
• Gold Level	2.080 USD	• QQ Account	32 USD	• 20.000 Adressen	161 USD
• Diamanten Level	3.856 USD	• Taobao Account	323 USD		© merics

Quelle: Trend Micro (2013).

4 Illegale IT-Schattenwirtschaft

4.1 Piraterie als Sicherheitsproblem

Die Auseinandersetzungen um Marktanteile und Marktzugang zwischen chinesischen und westlichen IT-Unternehmen sind für die Sicherheit der Nutzer in China eher zweitrangig: Für sie ist es entscheidend, dass sie sicher online einkaufen und ihre PCs nicht gehackt werden können.

In Städten wie Shenzhen und Hongkong gibt es große Elektronikmärkte. Besucher können aus einem breiten Angebot an Soft- und Hardware auswählen – vieles davon wird illegal hergestellt und vertrieben.

Die Software-Piraterie schadet nicht jedoch nur westlichen Herstellern. Eigenen Angaben zufolge gehen ihnen Lizenzgebühren in Milliardenhöhe verloren. Der ehemalige Microsoft-Chef Steve Ballmer gab an, dass 90 Prozent der firmeneigenen Produkte in China illegal genutzt würden.[26]

Raubkopien erhalten zudem in der Regel keinerlei Sicherheits-Updates. Insbesondere bei Kernkomponenten wie Betriebssystemen ist dies problematisch. Die anfälligen Geräte sind nicht nur ein Sicherheitsrisiko für ihre Nutzer, sondern bedrohen

die Netzsicherheit weltweit.[27] Denn wenn Sicherheitslücken nicht geschlossen werden, können sich Kriminelle Zugang zu den Geräten verschaffen und sie als sogenannte „Zombie-Rechner" in *Botnetzen* einsetzen. Damit können sie weitere Zugangsdaten stehlen oder Angriffe auf Webseiten oder Netzinfrastruktur durchführen. Illegale Betriebssysteme enthalten darüber hinaus häufig „von Haus aus" mutwillig eingeschleuste Viren.

4.2 Hackernetzwerke in China

Kriminelle Hacker bedrohen den Wohlstand und die Privatsphäre chinesischer Internetnutzer. Illegale Dienste werden ohne Scheu in offenen Foren angeboten, die Angst vor Strafverfolgung ist offensichtlich gering.

Die Art und Weise, wie in China illegale Dienste angeboten und kommuniziert werden, unterscheidet sich grundlegend von der in westlichen Ländern. Während der Handel mit gestohlenen Passwörtern oder Kreditkartendaten im Westen meist über verschlüsselte Netzwerke abläuft, koordinieren chinesische Hacker ihre illegalen Aktivitäten in offenen Chat-Gruppen von QQ oder Foren von Baidu. Dies liegt auch daran, dass der Anonymisierungsdienst Tor[28] in China blockiert ist.

Die angebotenen Dienste sind vielfältig – und häufig günstig. Kriminelle können sich Zugang zu Servern kaufen, mit deren Hilfe sie Nutzer mit Malware infizieren oder Spam-Nachrichten verschicken können. Auch maßgeschneiderte Trojaner oder die Anfertigung gefälschter Login-Seiten für Banken und soziale Netzwerke sind zu haben – damit lassen sich PCs und Smartphones von Nutzern gezielt ausspionieren (siehe Übersicht 3).

5 Deutsche Politik gegen chinesischen Protektionismus

Chinas konsequenter Ausbau einer eigenen IT-Industrie und die zunehmende Abschottung vor ausländischen Produkten hat massive Auswirkungen auf internationale Hersteller. Auch die deutsche *Cyber*-Außenpolitik gegenüber China muss sich auf Konflikte einstellen. China wird sich auf Dauer nicht in ein von westlichen Vorstellungen geprägtes *Cyber Security*-System einbinden lassen. Stattdessen arbeitet Beijing schon jetzt mit anderen Schwellenländern an Parallelstandards zur bislang westlich dominierten *Internet Governance.*

Bei IT-Angeboten für die Hochtechnologie – etwa im Bereich Industrie 4.0 und spezialisierter Business-Software – können sich deutsche Firmen auf ihre Wettbewerbsfähigkeit gegenüber chinesischen Wettbewerbern verlassen. Doch wie lange noch?

Deutschland sollte deswegen auf eine Politik[29] setzen, die sich auch in anderen Feldern bewährt. Das bedeutet: Statt auf eine Umwälzung der chinesischen *Cyber Security*-Politik hinzuarbeiten, sollte sich die Bundesregierung auf pragmatische erreichbare Ziele beschränken: Drängende Themen sind zahlreich vorhanden. Etwa der bessere Schutz geistigen Eigentums oder gesicherter Marktzugang für deutsche Firmen.

Ansprechpartner für diesen China Monitor:
Hauke Gierow
Hauke.Gierow@merics.de
Redaktion: Silke Ballweg

Impressum:
Mercator Institute for China Studies
Klosterstraße 64
10179 Berlin
Tel: +49 30 3440 999 – 0
Mail: info@merics.de
www.merics.org

[1] Zhang, Yu (2014). „Homegrown developers look to unseat Microsofts dominant OS". http://www.globaltimes.cn/content/887716.shtml. Zugriff: 24.10.2014.
[2] Zhangwei 张卫 (2012). „信息安全的机遇与挑战" (Chancen und Herausforderungen der Informationssicherheit). http://news.sohu.com/20120416/n340660958.shtml. Zugriff: 15.09.2014.
[3] Zhonghua renmin gongheguo guowuyuan 中华人民共和国国务院 (2012). „国务院出台意见推进信息化发展切实保障信息安全" (Der Staatsrat veröffentlicht ein Dokument zur Förderung der Entwicklung der Informatisierung und für den Schutz der Informationssicherheit). http://politics.gmw.cn/2012-07/17/content_4571519.htm. Zugriff: 14.08.2014.
[4] Ernst, Dieter und Naughton, Barry (2008). „China's emerging industrial economy: insight from the IT industry". In: Mc Nally, Christopher A. (2008). *China's Emergent Political Economy – Capitalism in the dragon's lair*, 39-59. London und New York: Routledge.
[5] Cloutier, Christopher T. und Cohen, Jane Y (2011). „Casting a wide net: China's encryption restrictions". http://www.kslaw.com/imageserver/KSPublic/library/publication/2011articles/11-11WorldECRCloutierCohen.pdf. Zugriff: 15.08.2014.
[6] Wang, Yukai 汪玉凯 (2014). „中央网络安全与信息化领导小组的由来及其影响" (Die Ursprünge und der Einfluss der Zentralen Führungsgruppe für Netzwerksicherheit und Informatisierung). http://theory.people.com.cn/2014/0303/c40531-24510897.html. Zugriff: 22.10.2014.
[7] Nolan, Peter (2014). *Chinese Firms, Global Firms: Industrial Policy in the Era of Globalisation*. New York: Routledge.
[8] Fauna (2011). „Huawei's London Underground Bid Blocked, Chinese Reactions". http://www.chinasmack.com/2011/stories/huaweis-london-underground-bid-blocked-chinese-reactions.html. Zugriff: 30.11.2014.
[9] Kan, Michael (2013). „UK to probe Huawei's cybersecurity evaluation center". http://www.pcworld.com/article/2044722/uk-to-probe-huaweis-cybersecurity-evaluation-center.html. Zugriff: 22.10.2014.
[10] Gartner (2014). „Gartner Says Worldwide PC Shipments Declined 6.9 Percent in Fourth Quarter of 2013". http://www.gartner.com/newsroom/id/2647517. Zugriff: 22.09.204.
[11] Eddy, Max (2013). „Nearly 7,000 Malicious Android Apps Infest China's Appstores". http://securitywatch.pcmag.com/mobile-security/315218-nearly-7-000-malicious-android-apps-infest-china-s-appstores. Zugriff: 22.09.2014.
[12] Muncaster, Phil (2014). „Chinese Heart App Virus Slams 100,000 Android Phones". http://www.infosecurity-magazine.com/news/chinese-virus-100000-android-phones/. Zugriff: 22.09.2014.
[13] King, Gary, Pan, Jennifer und Roberts, Margaret E. (2014). „Reverse-engineering censorship in China: Randomized experimentation and participant observation". Science 345 (6199): 1-10.
[14] Facebook Newsroom (2014). Company Info. http://newsroom.fb.com/company-info/. Zugriff: 30.11.2014.
[15] Bradsher, Keith und Mozur, Paul (2014). „China Clamps Down on Web, Pinching Companies Like Google". http://www.nytimes.com/2014/09/22/business/international/china-clamps-down-on-web-pinching-companies-like-google.html?_r=0. Zugriff: 25.09.2014.
[16] Franceschi-Bicchierai, Lorenzo (2014). „Apple Addresses iCloud Attacks While China Denies Hacking Allegations". http://mashable.com/2014/10/21/apple-icloud-attacks-china/. Zugriff: 22.10.2014.
[17] Lovejoy, Ben (2014). „Tim Cook meets with Chinese vice premier in Beijing following iCloud phishing attack". http://www.techgreatest.com/apple-news/tim-cook-meets-with-chinese-vice-premier-in-beijing-following-icloud-phishing-attack/. Zugriff: 03.12.2014.
[18] Arthur, Charles (2011). „China cracks down on VPN use" http://www.theguardian.com/technology/2011/may/13/china-cracks-down-on-vpn-use. Zugriff: 03.12.2014.
[19] American Chamber of Commerce in China (2013). „Business Climate Survey 2013". http://web.resource.amcham-china.org/cmsfile/2013/03/29/0640e5a7e0c8f86ff4a380150357bbef.pdf. Zugriff: 24.09.2014.
[20] The European Chamber of Commerce in China (2015). „Internet Restrictions Increasingly Harmful to Business, say European Companies in China". http://www.europeanchamber.com.cn/en/press-releases/2235/internet_restrctions_increasingly_harmful_to_business_says_european_companies_in_china. Zugriff: 17.02.2015.
[21] Bradsher, Keith (2014). „Looking Beyond China, Some Companies Shift Personnel". http://www.nytimes.com/2014/09/10/business/international/looking-beyond-china-some-companies-shift-personnel.html?_r=0. Zugriff: 30.11.2014.
[23] Ricker, Thomas (2010). „Chinese iPhone approved with WAPI WiFi". http://www.engadget.com/2010/05/04/chinese-iphone-approved-with-wapi-wifi/. Zugriff: 30.11.2014.
[24] Shouji zhongguo wang 手机中国网 (2015). „苹果成全球首个接受中方网络安全审查的公司" (Apple wird als weltweit erstes Unternehmen eine Prüfung der Netzwerksicherheit durch die chinesische Seite durchführen lassen). http://t.m.china.com.cn/convert/c_uPId9W.html. Zugriff: 22.01.2015.
[25] Mozur, Paul (2015). „New Rules in China Upset Western Tech Companies". http://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html?ref=business&_r=0. Zugriff: 02.02.2015.
[26] Brodkin, Jon (2011). „Ballmer to Hu: 90% of Microsoft customers in China using pirated software". http://www.networkworld.com/article/2199038/software/ballmer-to-hu--90--of-microsoft-customers-in-china-using-pirated-software.html. Zugriff: 30.11.2014.
[27] Gantz, John F. et al. (2013). „The Dangerous World of Counterfeit and Pirated Software". White Paper no. 239751. http://news.microsoft.com/download/presskits/antipiracy/docs/IDC030513.pdf. Zugriff: 22.10.2014.
[28] The Onion Routing (Tor). Ein Verfahren zur Umgehung von Internetzensur.
[29] Heilmann, Sebastian (2014). „Lob der Nischenpolitik-Deutschland spielt in Europas China-Politik heute die Rolle des Impulsgebers". In: Internationale Politik, September / Oktober S. 34-43.