DER STAND DER TECHNIK IM RAHMEN DES NEUEN IT-SICHERHEITSGESETZES

Vanessa Kluge

Wissenschaftliche Mitarbeiterin (Postdoc), Technische Universität Berlin, Lehrstuhl für Wirtschafts-, Unternehmens- und Technikrecht
Straße des 17. Juni 135, 10623 Berlin, DE
vanessa.kluge@tu-berlin.de; www.wir.tu-berlin.de

Schlagworte: ***IT-Sicherheitsgesetz, Stand der Technik, Internet der Dinge, Cyberattacken***

Abstract: *Das Internet der Dinge hält vermehrt Einzug im Alltag und teils ungeahnte Sicherheitslücken eröffnen Einfallstore für kriminelle Handlungen. So werden internetfähige Geräte unter anderem dafür missbraucht, Webdienstleistungen lahmzulegen; dies zeigt, dass sich die Angriffsfläche vergrößert hat und die Netzstruktur durchaus verletzlich ist. Auf nationaler Ebene wurde bezogen hierauf unter anderem die Strategie zum Schutz Kritischer Infrastrukturen entwickelt, deren Kernelemente das IT-Sicherheitsgesetz (IT-SiG) und die Verordnung zur Bestimmung kritischer Infrastrukturen (BSI-KritisV) sind.*

1. Einleitung

Im letzten Jahrzehnt ist ein signifikanter Anstieg von Gefahren durch Cyber-Attacken[1] zu verzeichnen.[2] Dies ist nicht zuletzt darauf zurückzuführen, dass autonom agierende Systeme im Zeitalter der Digitalisierung neue Dimensionen von Netzwerken entstehen lassen. Der Informationsaustausch findet also nicht mehr ausschließlich zwischenmenschlich – via Internet – statt, sondern Gegenstände kommunizieren auch untereinander. Ausgehend vom Wortsinn ist Charakteristikum und gleichermaßen gemeinsamer Nenner von Cyberattacken der gezielte Angriff auf größere, für eine spezifische Infrastruktur wichtige Computernetzwerke von außen[3] – unabhängig vom Verursachertypus. Die Angriffe können mannigfaltig ausgestaltet sein und reichen von Schädigungen, die die Betriebsfähigkeit beeinträchtigen hin zu digitalen Erpressungen; sie beinhalten Unternehmensspionage genauso wie die Beschaffung von Zugangsdaten.[4]

Für Privatleute und insbesondere Unternehmen soll der Einsatz sog. Malware, insbesondere Ransomware, am bedrohlichsten sein;[5] aber auch DDosS-Angriffe nehmen stetig zu. So haben erst jüngst Unbekannte internetfähige Geräte (z.B. IP-Kameras, Drucker, Router, Babyfone, TV-Festplatten-Receiver) in den USA und Teilen Europas und Japans dafür missbraucht, um Webdienstleistungen (wie Twitter, Netflix, Spotify, Airbnb etc.) zu stören bzw. paralysieren. Ein künstlich aufgeblasener Internetverkehr mittels Massenanfragen führte zur Überlastung und Nichterreichbarkeit der Dienste. Dieses Beispiel zeigt eindrücklich, dass und wie sich die Angriffsfläche im Zeitalter des «Internet of Things»[6] vergrößert und wie durchlässig die Infrastruktur des Netzes gerade aufgrund der stetig zunehmenden Vernetzung ist.

2. Rechtliche Fragestellungen

Spiegelbildlich zur Bandbreite der tatsächlichen Erscheinungsformen von Cyberattacken gibt es generell eine Vielzahl diskussionswürdiger, rechtlicher Aspekte, die in diesem Rahmen nur überblicksartig dargestellt

---

1 Zu den Begriffen «Cybercrime» und «Internetkriminalität» vgl. auch Mehrbrey/Schreibauer 2016, S. 75 m.w.N.
2 MMR-Aktuell, 2016, 376372.
3 http://www.duden.de/rechtschreibung/Cyberattacke (alle Hyperlinks wurden am 3. bzw. 6. Januar 2017 zuletzt aufgerufen).
4 Hierzu mehr bei Mehrbrey/Schreibauer 2016, S. 75.
5 https://beck-online.beck.de/Dokument?vpath=bibdata%2Freddok%2Fbecklink%2F2002253.htm&pos=1&hlwords=on.
6 Bräutigam/Klindt 2015, S. 1137.

werden können. Im öffentlichen Recht wird beispielsweise diskutiert, ob und inwieweit neuartige Formen der Kriegsführung, zu denen auch Cyberattacken zählen sollen, einen völkerrechtlich relevanten «bewaffneten Angriff» (Art. 51 UN-Charta) darstellen.[7] Im Strafrecht verschärft sich der Blick auf Cyber-Kriminalität[8], den e-crime-Täter[9] und das Tatmittel Internet.[10] Zivilrechtlich interessieren vornehmlich Haftungsszenarien, Zuordnungsfragen und damit einhergehende Versicherungskonzepte.[11] Im Weiteren soll vorwiegend das nationale Sicherheitskonzept als solches und das IT-SicherheitsG im Besonderen Beachtung finden. Ausgehend von der Prämisse, dass die größtmögliche Sicherheit vor Cyberattacken präventiv[12] – im eigenen Unternehmen, in eigener Verantwortung – ansetzen soll, gilt es zu fragen, wie greifbar die formulierten Vorgaben für den Rechtsanwender sind.

3. Nationales Sicherheitskonzept

Die fortschreitende Digitalisierung birgt neben dem enormen Innovationspotenzial auch bislang ungeahnte Gefährdungslagen in sich.

Um dem Schutzauftrag des Staates gerecht zu werden, wurde in den vergangenen Jahren schrittweise ein umfassendes Konzept entwickelt, an dessen Anfang 2011 die Cyber-Sicherheitsstrategie («Grundstein»[13]) der Bundesregierung stand. Ausfluss der sich daran anschließenden Digitalen Agenda ist das im Juli 2015 in Kraft getretene IT-Sicherheitsgesetz (IT-SiG)[14]. Das Gesetz zielt darauf ab, dass Betreiber kritischer Anlagen aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen in Zukunft einen Mindeststandard an IT-Sicherheit einhalten und gewichtige IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik melden. Besagte Meldungen werden dann dort einer Bewertung unterzogen und den Betreibern wiederum zeitnah weiterführende Materialien an die Hand gegeben. Das IT-SiG bildet somit den übergreifenden Rechtsrahmen für die Gewährleistung von Cybersicherheit in Deutschland[15] und soll seinen Beitrag dazu leisten, die IT-Systeme und digitalen Infrastrukturen Deutschlands zu den sichersten weltweit zu machen.[16]

Am 3. Mai 2016 ist nun der zweite Meilenstein, nämlich die das Gesetz konkretisierende Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV[17]) in Kraft getreten. Mit Hilfe der BSI-KritisV sollen Betreiber eruieren können, ob die von ihnen betriebenen Anlagen kritische Infrastrukturen sind und hernach dem IT-Sicherheitsgesetz unterstehen. Spätestens nach einer Übergangsfrist von sechs Monaten müssen einschlägige Betreiber dem BSI eine Kontaktstelle benennen (§ 8b Abs. 3 IT-SiG) und erhebliche Störungen melden (§ 8b Abs. 4 IT-SiG). Innerhalb der nächsten zwei Jahre ist der Nachweis der Einhaltung der Mindeststandards zu erbringen (§ 8a Abs. 1 IT-SiG).

---

7 Vgl. Schmidt-Radefeldt 2015, Art. 115a, Rn. 4.

8 Zur Begrifflichkeit siehe Reindl-Krauskopf 2014, S. 563, 564.

9 Zur Begrifflichkeit siehe Erichsen 2015, S. 247–248.

10 Im Jahr 2015 wurden 244.528 Fälle erfasst, die unter Nutzung des Tatmittels Internet begangen wurden; überwiegend handelte es sich hierbei um Betrugsdelikte (z.B. Bitcoins). Computerkriminalität ist im Jahr 2015 um 5,2% gesunken, vgl. BKA 2015, S. 8–9.

11 Exemplarisch Mehrbrey/Schreibauer 2016, S. 75 ff.

12 Und nicht erst mit der Ermittlung/Ahndung von Straftaten und der Geltendmachung zivilrechtlicher Ansprüche.

13 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf?__blob=publicationFile&v=5.

14 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015, BGBl. 2015 Teil I Nr. 31, ausgegeben zu Bonn am 24. Juli 2015.

15 Gitter/Meissner/Spauschus 2015, S. 512.

16 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf?__blob=publicationFile&v=5.

17 Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) vom 22. April 2016, BGBl. 2016 Teil I Nr. 20, ausgegeben zu Bonn am 2. Mai 2016.

Im Hinblick darauf, dass die gewünschte Sicherheit primär nicht durch Verwaltungshandeln, sondern mittels Selbstprüfung und -regulierung[18] der Anlagenbetreiber erreicht werden soll, gilt es vor allem zu ermitteln, wonach konkret sich der «Stand der Technik» im Sinne des § 8a Abs. 1 IT-SiG bemisst.

4. Stand der Technik

§ 8a Abs. 1 IT-SiG verlangt, dass der «Stand der Technik» innerhalb des Umsetzungserfordernisses, also der bei der Schaffung angemessener organisatorischer und technischer Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, zu berücksichtigen ist. Hierbei handelt es sich nicht um eine unmittelbar messbare Größe[19], sondern um einen unbestimmten und daher ausfüllungsbedürftigen Rechtsbegriff; dieser ist nicht starr, sondern dynamisch.

Im Rahmen des sog. Kalkar-Beschlusses des Bundesverfassungsgerichts von 1978[20] wurden die drei sicherheitsrechtlich belangvollen Standards erläutert und grundsätzlich in Beziehung gesetzt. Das Fundament bilden die «allgemein anerkannten Regeln der Technik», die sich für den Anwender in der bloßen Ermittlung der vorherrschenden Meinung im technischen Praktikerumfeld erschöpfen. Auf höchster Stufe ist der «Stand von Wissenschaft und Technik» angesiedelt, der im Produkthaftungskontext als Theorie-Praxis-Beziehung verstanden wird.[21] Dazwischen oszilliert der «Stand der Technik», bei dem das Hauptaugenmerk auf das technisch Machbare und praktisch Bewährte gerichtet ist, wobei die Ermittlung der technischen Notwendigkeit, Angemessenheit und Vermeidbarkeit zum Aufgabenspektrum des Anwenders zählt.

Dem Bedürfnis nach Flexibilität beikommend, hat der Gesetzgeber sich beim IT-SiG gegen eine Legaldefinition[22] entschieden; allein die Gesetzesbegründung gibt Aufschluss. Demgemäß ist «Stand der Technik» in diesem Sinne der «Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt. […] insbesondere einschlägige internationale, europäische und nationale Normen und Standards heranzuziehen, aber auch vergleichbare Verfahren, Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt wurden».[23]

Das gesetzgeberisch intendierte Erfordernis der Beachtung des Standes der Technik wurde zwischenzeitlich auch in das Telemediengesetz transferiert (§ 13 Abs. 7 TMG) – ebenfalls unter Verzicht auf eine Legaldefinition; ähnlich verhält es sich mit Art. 32 Abs. 1 EU-DSGVO.

Der Gesetzesbegründung zum IT-SiG lassen sich im Wesentlichen zwei Parameter entnehmen: «fortschrittlich» einerseits und «gesichert» andererseits. In der Ära der Digitalisierung mitsamt den rasanten technologischen Innovationen erscheint es ambitioniert, den Spagat zwischen gesicherten Erkenntnissen und technischem Fortschritt zu bewerkstelligen. Der Verweis auf Normen und Standards als Hilfestellung für den Rechtsanwender verfängt hier nur bedingt, da auch sie in dieser kurzlebigen Zeit permanent aktualisiert werden müssten.[24] Die gewählte Formulierung hat Berührungspunkte zu den «anerkannten Regeln der Technik» und strahlt gleichsam in Richtung «Stand von Wissenschaft und Technik» aus. Die so geschaffene Rechtsunsicherheit verträgt sich nicht dem avisierten Ziel der Cybersicherheit. Anzuregen ist die Aufnahme katalogisierter, konkre-

18 https://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/kritis-vo-kabinett.pdf?__blob=publicationFile.
19 Michaelis 2016, S. 458.
20 BVerfGE 49, 89, 135 ff. – Kalkar I.
21 Vertiefend: Müller 2012, S. 29.
22 Anders z.B. § 3 Abs. 1 S. 1 PatG oder § 3 Abs. 6 BimSchG.
23 BT-Drucks. 18/4096, S. 26.
24 Michaelis 2016, S. 459.

tisierender Kriterien nach dem Vorbild der Anlage zu § 3 Abs. 6 BImSchG[25], sog. Kriterien zur Bestimmung des Standes der Technik.

5. Fazit

Der steigenden Bedrohung durch Online-Kriminalität und Cyber-Attacken[26] will der Gesetzgeber mit einer neuen Risikokultur begegnen.[27] Für Unternehmen, respektive Betreiber kritischer Anlagen, bedeutet dies wiederum ein Umdenken in Sachen Risikomanagement und Compliance; sie stehen vor der Herausforderung, die neuen Vorgaben basierend auf dem IT-SiG in die Praxis umzusetzen.[28] Im Kern geht es dabei um die Einhaltung von Mindeststandards und die Beachtung des «Standes der Technik». Die Regelungen sind im Ergebnis zu begrüßen, da sie gleichermaßen einen prophylaktischen Schutzwall gegen Angriffe von außen darstellen und aus Unternehmensperspektive auf Organisationsebene haftungsmindernd wirken können. Zu bemängeln bleibt die mangelnde Griffigkeit, so dass es nicht verwundern würde, wenn alsbald der Ruf nach einer Spezifizierung laut wird und ggf. Nachjustierungen vorgenommen werden.

6. Literatur

BKA, Polizeiliche Kriminalstatistik 2015, S. 8–9.

Bräutigam, Peter/Klindt, Thomas, Industrie 4.0, das Internet der Dinge und das Recht, NJW 2015, S. 113.

Erichsen, Sven, Cyber-Risiken und Cyber-Versicherung, CCZ 2015, S. 247–248.

Gitter, Rotraud/Meissner, Alexander/Spauschus, Philipp, Das neue IT-Sicherheitsgesetz, ZD 2015, S. 512.

Michaelis, Patrick, Der «Stand der Technik» im Kontext regulatorischer Anforderungen, DuD 2016, S. 458.

MMR-Aktuell, 2016, 376372.

Müller, Stefan, in: Ensthaler, Jürgen/Gesmann-Nuissl, Dagmar/Müller, Stefan (Hrsg.), Technikrecht – Rechtliche Grundlagen des Technologiemanagements, Springer, Berlin-Heidelberg 2012, S. 29.

Reindl-Krauskopf, Susanne, Cyber-Kriminalität, ZaöRV 2014, S. 563, 564.

Schmidt-Radefeldt, Roman, in: Epping, Volker/Hilgruber, Christien (Hrsg.), Beck'scher Online-Kommentar GG, Stand 1. September 2015, Art. 115a, Rn. 4.

Wyl, Christian de/Weise, Michael/Bartsch, Alexander, Neue Sicherheitsanforderungen für Netzbetreiber, N&R 2015, S. 23.

[25] Gesetz zum Schutz von schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche Vorgänge (Bundes-Immissionsschutzgesetz – BImSchG) vom 15. März 1974, in der Fassung der Bekanntmachung vom 17. Mai 2013 (BGBl. 2013 Teil I Nr. 25, ausgegeben zu Bonn am 27. Mai 2013), das durch Artikel 1 des Gesetzes vom 30. November 2016 (BGBl. 2013 Teil I Nr. 43, ausgegeben zu Bonn am 31. Juli 2013) geändert worden ist.

[26] https://beck-online.beck.de/Dokument?vpath=bibdata%2Freddok%2Fbecklink%2F2002253.htm&pos=1&hlwords=on.

[27] http://www.bmi.bund.de/cae/servlet/contentblob/544770/publicationFile/27031/kritis.pdf.

[28] Für Netzbetreiber und Versorger vgl. Wyl/Weise/Bartsch 2015, S. 23.