Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)284 C

Freie Universität Berlin

Dept. Math. and Computer Science
Institute of Computer Science

Freie Universität Berlin, FB Mathematik und Informatik
Takustraße 9, 14195 Berlin, Germany

Deutscher Bundestag Innenausschuss
Herrn Ministerialrat Dr. Heynckes
Leiter Sekretariat PA 4
Platz der Republik 1
11011 Berlin

Computer Systems & Telematics
Prof. Dr.-Ing. Jochen H. Schiller
Takustraße 9
14195 Berlin

Telefon +49 30 838 75-213/-212
Fax +49 30 838 75194
E-Mail jochen.schiller@fu-berlin.de
Internet http://cst.mi.fu-berlin.de

Bearb.-Zeichen js
Bearbeiter Schiller

15. April 2015

Stellungnahme zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme / Drucksache 18/4096 vom 25.02.2015

Relativ leicht und schnell fallen heutzutage Begriffe wie *Industrie 4.0*, Cloud, Internet der Dinge, Smart Cities etc., wenn vom aktuellen Wandel in der IKT-Welt die Rede ist. Die Themenschwerpunkte großer Messen, wie CeBIT und Hannover Messe greifen dies auf und fügen natürlich auch die Sicherheit als Schwerpunkt mit hinzu. Alles soll mit allem vernetzt und dadurch auch „smarter“ werden.

Parallel dazu sind die Entwicklungen in Richtung *Gefahren 4.0* sichtbar, ohne dass man hier Schwarzmalerei betreiben muss. Dies umfasst nicht nur die viel zitierten und nur schwer quantifizierbaren Angriffe, sondern insbesondere auch schlichte Fehlkonfigurationen und Softwarefehler, die mehr und mehr auch auf Grund einer immer schwerer durchschaubaren Komplexität geschehen. Qualitativ neu ist hierbei, dass die Vielfalt vernetzter Systeme immer „einfacher“ angreifbar werden, da sie alle auf einer im Kern einheitlichen Technologie – der Internet-Kommunikationsprotokolle – beruhen. Diese Vereinheitlichung ist aber natürlich zeitgleich auch der große Vorteil – jetzt kann basierend auf der gleichen Technologie „alles mit allem“ kommunizieren und in komplett neue Bereiche einwirken – von der Gebäudesteuerung über Energienetze bis hin zum Fahrzeug.

Gleichzeitig betreiben wir aber vielleicht gerade einmal *Sicherheit 2.0*: Im Wesentlichen wird versucht, die gerade vernetzten Systeme mehr oder weniger gut voneinander abzuschotten und Lücken zu stopfen. Gesetzgebung und Regelungen hinken meist deutlich den technischen Entwicklungen hinterher und man sieht sich eher als Getriebener der Technologie denn als proaktiv Handelnden. Zurzeit kann man dies nicht gerade als eine sinnvolle, kontrollierte und beherrschte Entwicklung bezeichnen. Schließlich stellt sich auch die wichtige Frage, wo der Bürger in diesem ganzen Prozess bleibt, wie die IKT-Technologie zu seinem Nutzen gestaltet werden kann.

Exkurs

Ohne dass hier zu tief in die Technologie eingestiegen werden soll, ist es dennoch wichtig, dass grundlegende Eigenschaften der neuen Entwicklungen bekannt sind, damit so ein besseres Verständnis der Problematik erzeugt und Fehleinschätzungen vermieden werden können. Internet der Dinge, Industrie 4.0, Cloud-Techniken – sie alle basieren im Kern auf Internet-Technologien, wie dem *verbindungslosen* Internet-Protokoll IP oder auch *zustandslosen* Web Services. Diese einheitlichen „Sprachen", also die Kommunikationsprotokolle, ermöglichen die Vernetzung „von allem mit allem" und damit ist im Prinzip ein Durchgriff von allem auf alles möglich und machbar, aber sicher nicht immer erwünscht. Schon heute kann mit dem Smartphone der Zustand eines Kraftwerkes abgefragt werden, klare wirtschaftliche Vorteile und große Chancen für die deutsche Industrie zeichnen sich durch die nun mögliche hochflexible Produktion (Stichwort Losgröße 1) ab; die IT ist unverzichtbarer Bestandteil der Energiewende – ohne IT keine kleinteilige Energiegewinnung. IT steckt also in allem, vom Lichtschalter bis zur Kraftwerkssteuerung.

Leider bleibt es aber oft bei dieser schlagwortartigen Betrachtung, ohne zu verstehen was dahinter steckt. So sind die oft zitierten „smarten" Objekte, vom Leuchtmittel, Datenbrille, Handy, Lichtschalter, Umwälzpumpe, Bremsanlage, Notabschaltung über USB-Stick, Drucker, Fahrzeug bis hin zum Gebäude, Industrieanlage etc. immer mehr vollständige Computer mit Betriebssystem, Kommunikationssoftware etc. plus Zusatzhardware. Häufig finden sich schon komplette Webserver selbst auf den einfachsten vernetzten Gegenständen auf Grund der damit verbundenen einfacheren Konfigurierbarkeit. Damit „erben" sie automatisch alle Probleme, die wir vom „klassischen" PC kennen – von den Lücken und Anfälligkeiten gegenüber Angriffen, Viren, Trojaner etc. bis hin zu den regelmäßig notwendigen Softwareaktualisierungen.

Hinzu kommt, dass viele dieser „smarten Objekte" vergleichbar mit dem Smartphone immer kommunikationstechnisch mit dem Internet verbunden sind („always on"). Gerade das Smartphone zeigt schön die Problematik einer vereinfachten Denkweise: Viel wird über Angriffe auf Smartphones geschrieben, über die Sicherheit des Betriebssystems, der zu installierenden Apps – ohne jedoch weiter zu beachten, dass jedes Smartphone noch mindestens ein weiteres Betriebssystem auf dem Funkmodem besitzt, welches den direkten Funkkontakt mit der Umgebung unterhält und von keinen Schutzmechanismen welchen Betriebssystems auch immer geschützt wird. Diverse Angriffe auf dieses System sind bekannt – weitere Betriebssysteme finden sich auf dem SIM und ggf. weiteren Funkadaptern (WLAN, Bluetooth, GPS …), sogar auf den Speicherkarten.

Bereits bei dem heutigen größtenteils „klassischen" Internet, d.h. Geräte wie ein PC oder Smartphone, welche Dienste von Servern anfordern, wie Webseiten oder Cloud-Speicherplatz, stellt sich die Frage nach der Beherrschbarkeit der Komplexität. Niemand kann heute genau sagen, wo welche Daten entlanglaufen. Zwar ist die physische Infrastruktur bekannt und auch zuordenbar, weit schwieriger gestaltet sich dies bei der logischen Infrastruktur, welcher die Datenpakete folgen. So ist es heute ein Leichtes, Verkehrsströme umzuleiten oder, absichtlich oder ungewollt, Bereiche des Internets abzuschalten. Mögen manche dieser Probleme beim privaten „surfen" im Netz noch tolerierbar sein, so können sie sich katastrophal auswirken, wenn Notrufe

nicht mehr abgesetzt werden können (nach und nach werden alle Telefone in Deutschland nur noch mit Internet-Technologien kommunizieren), Industrieanlagen nicht mehr kontrollierbar sind oder Börsensysteme nicht mehr ordnungsgemäß funktionieren.

Gerade die eingebetteten Systeme, welche weit über 90% aller Computer ausmachen, müssen hier im besonderen Fokus stehen, steuern sie doch fast alles in unserem Alltag – von der Waschmaschine über das Überdruckventil in einer Raffinerie bis hin zum Beatmungsgerät. Man muss nicht gleich die „großen" Szenarien, wie ein Cyberwar oder die OK bemühen – einfache Konfigurationsfehler oder Angriffe auf weit entfernte Systeme können als Kettenreaktion Schäden verursachen, bei denen hinterher kaum noch feststellbar ist, wer eigentlicher Verursacher war.

Wird beispielsweise der smarte Backofen von einem eingebetteten System gesteuert, so verfügt er natürlich auch über einen Webserver, mit dessen Hilfe über diverse Webdienste der Zustand abgefragt, aber auch der Ofen programmiert werden kann. Natürlich können auch neue Backprogramme über das Internet mit Hilfe einer Smartphone-App auf den Backofen geladen werden. Auf Grund einer wie auch immer gearteten Lücke findet nun Schadsoftware ihren Weg in die Backofensteuerung, so dass beispielsweise die Temperaturabschaltung nicht mehr ordnungsgemäß funktioniert und ein Brandschaden entsteht. Es wird sich nun als sehr schwierig herausstellen, den Schuldigen für den Schaden zu finden, noch schwieriger, diesen in Haftung zu nehmen. Ist es der Backofenhersteller, welcher keine geeignete Firewall im Backofen hatte, nicht die aktuellsten Sicherheitsupdates automatisch installiert hat? Ist es der Nutzer, der seinen Backofen nicht aktualisiert hat? Ist es der Hersteller des Handys, der ermöglicht hat, dass Schadsoftware auf dem Handy die Steuerungsapp manipuliert hat? Ist es letztendlich der schwer greifbare Hacker, der entsprechende Software auf dem Handy installiert hat, dies aber nur konnte, weil der Betriebssystemhersteller des Handys Lücken in seinem Betriebssystem hat?

Wie soll dies alles letztendlich einem Bürger klar gemacht werden, dass man es hier mit einem Gemisch aus Gefährdungen zu tun hat, die einerseits einem TKG unterliegen (wenn es denn über die Telekommunikation zum Schaden kam) oder andererseits einem TMG, da es sich ja um einen Webservice handelt? Wie kann verständlich gemacht werden, dass viele Begrifflichkeiten (wie der der „Verbindung") aus dem TKG und die daraus abgeleiteten Möglichkeiten nicht immer wirklich zu der oft verbindungslosen Welt des Internets passen?[1] Der Bürger hat in diesem Beispiel den Schaden – richtig verantwortlich ist niemand, da die Vernetzung eine neue, noch nicht wirklich beherrschte Komplexität eingeführt hat, bei der insbesondere auch die Gesetzeslage nicht hinterherkommt.

[1] Ein drastisches Beispiel von „technologisch veraltetem Gesetz" ist sicherlich §108 TKG, welcher in der Quintessenz unter anderem verhindert, dass clevere Notruf-Apps für Smartphones unter der Nutzung von Internet-Telefonie eingesetzt werden dürfen, da bei Notrufen zu 110/112 stets eine „Verbindung" vorausgesetzt wird und somit das verbindungslose Internetprotokoll ausgeschlossen ist. Apps für „Stille Notrufe", eine bessere Unterstützung Behinderter etc. werden damit erschwert.

Selbstverständlich wird man den Backofen nicht als Kritische Infrastruktur im Sinne des Gesetzesentwurfs sehen, sondern dies sollte nur ein einfaches, zur heutigen IT in Kritischen Infrastrukturen analoges Beispiel sein. Die Darstellung der IT in Kritischen Infrastrukturen würde den Rahmen der Stellungnahme sprengen, aber analog könnten Beispiele aus dem Bereich Banken, Industrie, Logistik – der gesamten Kritischen Infrastrukturen – herangezogen werden. Entsprechende Schilderungen von Vorfällen finden sich auch im BSI-Bericht zur Lage der IT-Sicherheit in Deutschland 2014.

Generelles zum IT-Sicherheitsgesetz

Bevor auf einige Gesichtspunkte des Gesetzesentwurfs eingegangen wird, muss festgehalten werden, dass dieses Gesetz ein absolut notwendiger, wenngleich sicherlich nicht der letzte Schritt in die richtige Richtung ist. Notwendig ist dieser Schritt, da es längst mehr als überfällig ist, dass zumindest gefordert wird den „Stand der Technik" bei allen hier Addressierten einzuhalten[2]. Auch wenn dieser Mindeststandard der aus dem letzten Jahrhundert aus Sicht der Wissenschaft ist, so ist dies doch bei Weitem besser, als der fahrlässige Umgang mit dem Thema Sicherheit, wie wir es heute leider an vielen Stellen feststellen müssen. Grundsätzlich positiv ist auch die Meldepflicht für Sicherheitsvorfälle, auch in der abgestuften Form (anonym bzw. mit Nennung je nach Schwere des Vorfalls).

Das Gesetz ist sicherlich nicht vollumfassend und abschließend, kann dies aber auch nie wirklich sein. Sicherheit ist ein dynamischer Prozess und so muss stets die aktuelle Situation überprüft, müssen Regelungen angepasst und ggf. auch Gesetze geändert werden. Wichtig ist nun, dass mit diesem Gesetz – so unvollständig es an manchen Stellen noch sein mag – ein deutlicher Bewusstseinswandel bei allen Betroffenen angestoßen wird. IT-Sicherheit ist nicht (nur) das *update* auf dem heimischen Rechner, sondern ein Prozess, der Technik, Anwendungen, Nutzung und auch ganz wesentlich die Aus- und Weiterbildung umfasst. Auch wenn dies in dem vorliegenden ersten Schritt im Wesentlichen auf die Betreiber Kritischer Infrastrukturen beschränkt ist – eigentlich sollte Sicherheit alles und alle umfassen – so ist dies doch ein wichtiger Anfang.

Es kann hier nicht sein, dass weitere Jahre zunächst analysiert wird, wer und was exakt unter den Begriff Kritischer Infrastrukturen fällt – dies ändert sich permanent und muss daher laufend unter Einbeziehung aller Akteure angepasst werden (daher ist auch das Instrument einer Rechtsverordnung das flexiblere). Beispielsweise sind Elektrofahrzeuge heute noch keine Kritische Infrastruktur, wenn jedoch ein relativ hoher Prozentsatz dieser Fahrzeuge solche mit Verbren-

[2] Falls aus juristischer Sicht der Begriff „berücksichtigen" in § 8a (1) BSIG-E nicht wirklich „einhalten" bedeutet, wie z.B. auch auf S. 31, letzter Absatz, des Entwurfs in der Begründung ausgeführt, so ist der Begriff „berücksichtigen" durch „einhalten" zu ersetzen um hier eine Eindeutigkeit zu erzielen – ansonsten ist von der Idee her das gesamte Gesetz aus technischer Sicht hinfällig, denn es geht ja gerade darum, verpflichtend zumindest Mindeststandards in allen hier adressierten IT-Systemen zu erreichen

nungsmotoren verdrängt hat und gleichzeitig die Elektrofahrzeuge auch zur Energiezwischenspeicherung in einem smarten Energieversorgungskonzept genutzt werden, dann kann die Situation ganz anders aussehen.

Wichtig ist jedoch, dass das Gesetz dem „Vernetztheitscharakter“ der Sicherheit gerecht wird. Auf der technischen Ebene, den Ebenen der Kommunikationsprotokolle, spricht mehr und mehr „alles mit allem“, wie weiter oben aufgezeigt. Auf der Ebene der Anwendungen ergeben sich damit domänenübergreifend neue, vielversprechende Anwendungen. Passend dazu müssen aber auch alle öffentlichen, behördlichen oder branchenübergreifenden Prozesse „vernetzt“ gedacht werden. Dies bedeutet aber auch, dass hier klassische Abgrenzungen in z.B. Bund, Länder Kommunen oder auch Medien vs. Kommunikation neu gedacht und ggf. angepasst werden müssen.

Haftung und Sanktionierungsmöglichkeiten

Parallel zur Ausgestaltung des IT-Sicherheitsgesetzes muss sicherlich auch die Anpassung der gesetzlichen Regelungen zur Haftung bei Schäden angegangen werden. Wenn die im Entwurf gesetzten Mindeststandards, also der Stand der Technik, nicht erfüllt waren und ein Schaden entstanden ist, so ist auch folgerichtig, dass der (Mit-)Verursacher hierfür (mit-)haftet. Aus technischer Sicht ist es auf jeden Fall fahrlässig, den seit langem bekannten Stand der Technik nicht einzuhalten (und wesentliche Mehraufwände basierend auf dem IT-Sicherheitsgesetz haben vorrangig diejenigen, welche bisher den Mindeststandard nicht erfüllt haben).

Gerade im Bereich der Software- wie Hardware-Entwicklung und auch dem Betrieb von IT-Systemen ist seit langem bekannt, wie Systeme zu entwickeln und zu betreiben sind, welche Richtlinien eingehalten werden müssen. Typische Beispiele aus dem IT-Bereich sind die ISO/IEC 27000-Reihe oder der IT-Grundschutz nach BSI. Diese könnten auch Basis der in § 8a (3) BSIG-E geforderten Nachweise sein.

In vielen Bereichen, wie z.B. dem Flugzeugbau, wird strikt auf die Einhaltung von Sicherheitsrichtlinien geachtet – leider nicht überall, so dass sich sowohl in proprietären, abgeschlossenen Systemen (z.B. in diversen SCADA-Systemen), als auch in open source Produkten (z.B. Heartbleed/openSSL) immer wieder leicht vermeidbare Fehler finden – leider meist erst, wenn sie bereits Schäden verursacht haben und ausgenutzt wurden. Ungeprüfte Übernahme von Software, mangelhafte Verschlüsselungsverfahren oder auch die Vernetzung bisher unvernetzter Systeme ohne eine Überprüfung auf die damit ggf. verbundenen Einfallstore entsprechen nicht dem Stand der Technik.

Es ist aber auch klar, dass es hierbei Grenzen der Zumutbarkeit hinsichtlich der Überprüfung gibt. So kann letztendlich ein Dienstanbieter nicht bis ins kleinste Detail wissen, welche Komponenten z.B. in der Hardware zum Einsatz kommen, die er selbst nutzt. Daraus kann aber im Umkehrschluss nicht gefolgert werden, dass hierfür keinerlei Verantwortung vorliegt. In der klassischen, analogen Welt kann der Nutzer auch davon ausgehen, dass der Anbieter eines Dienstes

oder Produktes die Funktion desselben gewährleistet. Dies gilt auch dann, wenn eine Teilkomponente für eine Störung verantwortlich ist, welche gar nicht im direkten Einflussbereich des Dienstanbieters oder Produzenten liegt. Beispiele hierfür wären die Elektronik eines Automobils, welche meist von Zulieferern kommt, bei deren Fehlfunktion ein Kunde sich jedoch an den Autohersteller wendet. Analog haftet die Bahn als Dienstleister bei Verspätungen auch dann, wenn z.B. der Grund ein von ihr gar nicht selbst gefertigtes Antriebsaggregat war. Es ist Aufgabe des Dienstleisters bzw. Produzenten durch entsprechende Verträge mit den Zulieferern auf diese zurückgreifen zu können – damit propagiert sich auch das anfangs erwähnte IT-Sicherheitsbewusstsein in Richtung der IT-Hersteller. Letztendlich kann es für einen Nutzer eines Dienstes oder Produktes nur eine Schnittstelle für den Dienst, für die Verantwortung, für die Haftung geben und kein Weiterleiten der Zuständigkeiten.

Natürlich kann ein IT-Dienstanbieter nicht generell z.B. für Störungen bei Nutzern ausgelöst durch von ihm übertragene Inhalte haftbar gemacht werden. Es gibt aber sicherlich dann eine Mithaftung, wenn diese Inhalte insbesondere deswegen eine Störung auslösen konnte, weil der Dienstanbieter im Vorfeld keine dem Stand der Technik folgenden Sicherheitsmaßnahmen ergriffen hat und somit z.B. bereits bekannte Lücken zum Schaden eines Nutzers ausgenutzt werden konnten.

Ein weiterer offener Punkt der aktuellen Vorlage ist sicherlich das Fehlen weitergehender Sanktionierungsmöglichkeiten. Sicherlich würde die notwendige Bewusstseinsänderung hinsichtlich der IT-Sicherheit durch erweiterte Haftungsmöglichkeiten bzw. Bußgelder unterstützt, ebenso durch die namentliche Nennung von z.B. Betreibern Kritischer Infrastrukturen bei erheblichen Störungen. Wichtig wäre jedoch, dass §8a BSIG-E auch tatsächlich umgesetzt wird. Ob ein reines „Verlangen“ der Beseitigung von Sicherheitsmängeln ausreichen wird ist mehr als fraglich.

Rolle des BSI

Die vorgesehene Stärkung des BSI ist auf jeden Fall zu begrüßen, auch der Wandel zu einer „nationalen Informationssicherheitsbehörde“ ist nur folgerichtig. Trotz mehr oder weniger berechtigter Kritik am BSI und seiner bisherigen Konstruktion ist diese Einrichtung inzwischen einer *der* Ansprechpartner national wie auch international bei IT-Sicherheitsfragen von Bürgern, Verwaltungen und auch Unternehmen (wenngleich bei letzteren deutlich zögerlicher bis hin zu Überlegungen der Industrie zu weiteren eigenen IT-Sicherheitseinrichtungen). Es ist daher auch konsequent, dass das BSI von neutraler Warte aus IT-Produkte auf deren Sicherheitsniveau überprüft und auch überwacht, dass „branchenspezifische Sicherheitsstandards“ nicht hinter den Stand der Technik zurückfallen – dieser ist ein Mindeststandard und sollte nicht aufgeweicht werden.

Zu hinterfragen ist allerdings die Konstruktion des BSI als eine Behörde innerhalb eines Ministeriums. Ein sichtbares Zeichen für eine umfassende Stärkung der IT-Sicherheit ist eine neutrale, unabhängige Einrichtung mit der entsprechenden Ausstattung. Sicherheitsfragen und -vorfälle sind weder ressortgebunden noch berücksichtigen sie gesetzgeberische Grenzen oder föderale

Strukturen. Hier wäre eine zentrale Anlaufstelle mit den entsprechenden Kompetenzen wünschenswert, welche die im IT-Sicherheitsgesetz geforderten Mindeststandards dann auch wirklich überall durchsetzen kann.

Zur Unterstützung dieser Rolle sind außer der (relativen) Unabhängigkeit weitere Komponenten relevant: passende Gehaltsstrukturen, um wirklich attraktiv für IT-Fachkräfte zu sein, noch weitergehende Kooperation mit Forschungseinrichtungen, um auf das dort vorhandene Wissen zurückzugreifen, und auch das vermehrte Einbringen BSI-relevanter Fragestellungen z.B. in Forschungsprogramme des BMBF, so dass hier in einer gemeinsamen Anstrengung die IT-Sicherheit verbessert werden kann. Hier gibt es zwar schon viele Ansätze, aber noch viel zu oft landen gute Ideen in Abschlussberichten statt in relevanten Anwendungen.

Rolle der KMUs

Es ist sicherlich richtig in einem ersten Wurf des IT-Sicherheitsgesetzes KMUs/Kleinstunternehmen zunächst von §8a BSIG-E auszuklammern. Der Schwerpunkt liegt hier klar auf den „klassischen“ Kritischen Infrastrukturen betrieben von größeren Unternehmen. Dies bedeutet jedoch aus technischer Sicht keineswegs, dass es nicht auch sinnvoll wäre, gerade kleinere Unternehmen in einem ersten Schritt explizit in den Informationsfluss über IT-Sicherheitslücken und Vorfälle zu integrieren und in einem späteren Schritt ähnliche Maßstäbe wie §8a BSIG-E anzulegen. Der Hintergrund ist einfach und wurde auch z.B. in der BMBF-Förderung zur Sicherheitsforschung erkannt (Bekanntmachung vom 5.8.2013): Weit über 75% der Angriffe im Cyberspace richten sich derzeit gegen KMUs, diese sind meist deutlich schlechter auf Angriffe vorbereitet – und können dennoch selbst im Hinblick auf Kritische Infrastrukturen relevant sein.

Es wird oft argumentiert, dass z.B. der Ausfall eines kleinen Betreibers einer nur „lokal kritischen“ Infrastruktur, z.B. ein lokaler Wasserversorger, keine größeren Auswirkungen hat. Es wird dabei aber vernachlässigt, dass beispielsweise sehr viele Wasserversorger ähnliche wenn nicht sogar identische Steuerungssysteme nutzen. Eine gezielt ausgenutzte Schwachstelle in diesen Systemen kann damit eine große Anzahl dieser „kleinen Betreiber“ stören und so in der Gesamtheit sehr wohl eine erhebliche Störung im Sinne des Gesetzes verursachen. Aus diesem Grund ist es unabdingbar, dass sich die o.g. Bewusstseinsänderung gerade auch in Richtung der KMUs fortsetzt und in einem weiteren Schritt das Gesetz entsprechend angepasst wird.

Vernetzung auf allen Ebenen

Wie eingangs erwähnt und auch auf allen aktuellen Veranstaltungen durch viele Redner immer wieder betont, ist der aktuelle Trend der zur Vernetzung von „allem mit allem“. Auch wenn für spezielle Zwecke sicherlich noch getrennte Netze verfügbar sind, so werden selbst für BOS-Netze Architekturen mit Nutzung kommerzieller Netze angedacht, laufen sicherheitskritische öffentliche Anwendungen (verschlüsselt) über kommerzielle Netze und greifen vielfältig Behörden auf zahlreiche Dienste im Internet zu.

Wenn also auf der technischen Ebene „alles mit allem“ nach und nach vernetzt wird und daher auch die entsprechenden Sicherheitsproblematiken alle vernetzten Systeme betreffen, dann ist es nicht konsequent und unter Umständen sogar gefährlich, wenn Teilbereiche der Verwaltungen oder Sektoren, wie Kultur und Medien, ausgeklammert werden. Sicherlich gibt es hier, wie S. 38 des Gesetzentwurfs auch erwähnt, gesonderte Regelungen bzw. Grenzen der Gesetzgebungskompetenz des Bundes, jedoch werden sich Sicherheitsvorfälle, Fehlkonfigurationen und Angriffe nicht an diese Abgrenzungen halten sondern unter Umständen in den hier nicht erfassten Bereichen ausbrechen und dann doch eine Kritische Infrastruktur bundesweit betreffen.

Hier muss nach und nach ein ganzheitlicher Ansatz im Sinne der „Vernetzten Sicherheit“ geschaffen werden, so dass das hier gestartete IT-Sicherheitsbewusstsein auch in alle Bereiche vordringen kann. Dass hier Nachholbedarf besteht sieht man am teilweise leichtfertigen Umgang mit sicherheitsrelevanten Daten in Cloud-Diensten, dem Nutzen ungesicherter privater Smartphones für dienstliche Zwecke oder dem Glauben, dass ein IT-System sicher sei, wenn die Kommunikationsstrecken verschlüsselt betrieben werden etc.

Rolle von TKG und TMG

Im Rahmen der Diskussionen zum IT-Sicherheitsgesetz werden als betroffene Bereiche z.B. Betreiber von Webseiten, Telekommunikationsunternehmen, Industrie 4.0, Cloud-Technologie etc. in einem Atemzug genannt, ohne wirklich zu bedenken, was es heißt, dass hier je nach Beispiel unterschiedliche Gesetze zur Anwendung kommen. Hinzu kommt, dass insbesondere das TKG noch von der „klassischen Denkweise“ des analogen Telefonnetzes mit verbindungsorientierter Übertragung geprägt ist.

Wie bereits erwähnt, finden sich Webserver – in abgespeckten Versionen – heute auf den kleinsten eingebetteten Systemen bis hin zu per SmartphoneApp steuerbaren Leuchten, aber auch in mehr und mehr industriellen Steuerungssystemen. Webserver bieten ihre Web-Dienste oft mit Hilfe einfacher Standardbefehlen an, die verbindungslos an den Server gerichtet werden können – insbesondere muss keine klassische „Telekommunikationsverbindung“ im Sinne des TKG aufgebaut werden. Diese Web-Dienste bzw. deren Anbieter fallen unter das TMG. Gerade aber industrielle Steuerungssysteme kritischer Infrastrukturen können Ziel eines Angriffs sein – nach TMG gibt es aber keine mit dem TKG vergleichbaren Instrumente um erforderliche Daten für eine Angriffserkennung zu erheben. Das TMG geht von Nutzern eines Web-Dienstes im Sinne z.B. eines Web-Surfers aus. Es wurde dabei nicht bedacht, dass technisch identische Verfahren zum Angriff genutzt werden können – es ist lediglich eine andere Ebene, als die vom TKG erfasste „technische“ Kommunikation. Diese Denkweise findet sich auch z.B. in der Begriffsdefinition § 3 Nr. 25 TKG „telekommunikationsgestützte Dienste“, welche verlangen, dass „die Inhaltsleistung noch während der Telekommunikationsverbindung erfüllt wird“.

Finden also Angriffe auf Kritische Infrastrukturen im Geltungsbereich des TMG statt, so hat der Angegriffene rechtlich keinerlei Möglichkeiten analog zu § 100 TKG Daten aufzuzeichnen, welche die Störung erkennen lassen und dann ggf. Maßnahmen einleiten. Hier müsste zumindest eine konsistente Regelung in TMG und TKG geschaffen werden bzw. noch besser die Gesetze

derart neugestaltet werden, dass nicht mehr zeitgemäße technische Begriffe (wie „Verbindung“ im Sinne des TKG) durch Funktionen und Leistungsmerkmale beschrieben werden. Für einen Nutzer bzw. Betreiber von Diensten ist es letztendlich irrelevant, ob der Dienst auf einer Verbindung beruht, verbindungslos angeboten wird, ein Web-Dienst ist etc. – aus Sicherheitssicht sollte alles gleich behandelt werden.

Eine schnelle Anpassung wäre die (erneute) *Angleichung* von §15 TMG an §100 TKG-E. Die im IT-Sicherheitsgesetz derzeit vorgesehenen Änderungen des TMG haben eher den klassischen Web-Surfer als Nutzer von Web-Diensten im Sinn, weniger die o.g. Industriesteuerungssysteme. Bleibt es bei diesem Stand verbietet sich die Nutzung zahlreicher Analysesysteme z.B. zur Erkennung von ausgefeilteren, mehrschrittigen Angriffen, welche sich über einen längeren Zeitraum hinziehen können. Ebenso wird eine nachträgliche Analyse von Schäden schwer ohne die dafür notwendige vorab gespeicherte Datenbasis möglich sein.

Störungen und Datensammlung

Störungen, hervorgerufen durch z.B. Softwarefehler, Angriffe oder Fehlkonfigurationen, sind in heutigen Internet-basierten Kommunikationsnetzen und ihren Diensten etwas grundlegend anderes, als sie dies in klassischen Telekommunikationsnetzen waren. In klassischen Netzen hat eine Störung meist zeitnah direkt etwas bewirkt, beispielsweise eine Funktionsstörung hervorgerufen. In heutigen Netzen können z.B. Angriffe lange im Voraus vorbereitet und Schadsoftware in Systemen hinterlegt werden, ohne dass dadurch bereits eine Störung hervorgerufen wird. Es reicht dann ein kleiner, als solcher kaum erkennbarer Befehl, um die Störung hervorzurufen. Ebenso kann beispielsweise eine schlechte Systemkonfiguration oder ein nur unzureichend abgesichertes System jahrelang problemlos funktionieren, bis sich die Umgebungsparameter ändern – z.B. das System mit dem Internet verbunden wird. Typische Beispiele sind hierfür Industriesteuerungssysteme, welche auch heute noch häufig aus Gründen der vereinfachten Wartung mit fest voreingestellten Passwörtern versehen sind (oft auf Kundenwunsch!), und schlagartig angreifbar werden, sobald sie nicht mehr losgelöst sondern vernetzt arbeiten.

Wie schon mehrfach erwähnt, ist die Kommunikationswelt schon heute stark von eingebetteten Systemen geprägt, die Maschine-zu-Maschine-Kommunikation wird immer dominanter; schon heute kommunizieren mehr Dinge als Menschen im Internet. Gerade im Hinblick auf Kritische Infrastrukturen muss daher ein besonderes Augenmerk auf Störungen in diesen Systemen gelegt werden.

Um wirksam die Sicherheit von IT-Systemen zu erhöhen kann nicht erst dann gehandelt werden, wenn tatsächlich eine Funktionsstörung aufgetreten ist. Im Vorfeld müssen bereits zahlreiche Maßnahmen ergriffen werden, um ein möglichst gutes Lagebild zu erhalten. Dies kann von relativ einfachen Maßnahmen, wie der Erfassung des Umsetzungsgrades von Maßnahmen des IT-Grundschutzes bis hin zu detaillierten Verkehrsanalysen gehen. Gerade die „schlummernden“ Bedrohungen, von Vorbereitungen zu Angriffen via Bot-Netze bis hin zu mangelhaften Konfigurationen und alten Softwareständen, sind wesentlich im Hinblick auf die Vulnerabilität Kritischer Infrastrukturen. Es ist dabei auch wichtig, dass ein solches Lagebild auch möglichst viele Systeme

im Sinne einer vernetzten Sicherheit erfasst. Es ist bei weitem nicht so wirksam, wenn je nach Sektoren, Branchen, Behörden etc. getrennte Lagebilder erstellt werden. Gerade Störungen im IT-Bereich können sehr schnell viele Bereiche erfassen, beispielsweise wenn Schwachstellen in Systemen auftreten, welche fast überall genutzt werden (z.B. Router eines Herstellers).

Wie schon zuvor erwähnt, sind TKG und TMG hier gleichermaßen hinsichtlich Störungen zu betrachten. Es ist aus Sicht der Technik nicht sinnvoll im Rahmen des TMG lediglich einen Schutz vor gewissen Störungen vorzuschreiben, basierend auf dem TKG jedoch weitergehende Möglichkeiten der Datensammlung vorzusehen.

Datensammlung zur Erkennung von Störungen, auch von solchen, welche erst in der Zukunft dann beispielsweise zu Funktionsausfällen führen können (i.S.v. §100 Abs. 1 TKG-E) muss aus technischer Sicht nicht notwendigerweise das anlasslose Sammeln aller Daten inklusive der Analyse aller Inhalte der Datenpakete umfassen. Sicherlich mag es Fälle geben, in denen man – meist im Nachhinein – anhand von umfangreichen (selten vollständigen) Datensammlungen bestimmten Angriffsmustern auf die Spur kommen kann. Sinnvoll, angemessen und auch wirtschaftlich vertretbar sind aber meist mehrstufige Verfahren, welche in einem ersten Schritt z.B. Anomalien im Datenstrom erkennen können, ohne alle Daten zu sammeln. Im Verdachtsfall kann dann im nächsten Schritt ein Verfahren folgen, welches „genauer hinschaut“ (also z.B. Paketinhalte überprüft). Bei vielen Verfahren genügt es dabei vollkommen, auf pseudonymisierten Daten, auf aggregierten Daten oder lediglich auf Statistiken und Stichproben zu arbeiten. Gerade bei großangelegten, verteilten Angriffen spielen die Daten eines Einzelnen eine untergeordnete Rolle – wichtiger sind hier z.B. die Strukturen der Datenverteilung.

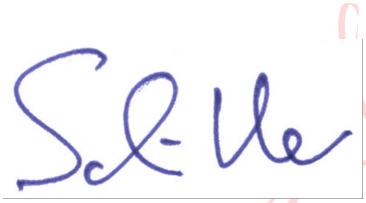
Zusammenfassung

Die IT-Sicherheit in vielen Bereichen bleibt heutzutage meist weiter hinter dem Möglichen zurück, auch immer noch weit hinter dem im Gesetzesentwurf immer wieder zitierten Stand der Technik. Derzeit gültige Regelungen, wie das TKG oder das TMG sind nicht wirklich an die Anfordernisse der IKT-Systeme und deren Nutzer angepasst. Der jetzt vorliegende Entwurf eines IT-Sicherheitsgesetzes ist ein notwendiger und wichtiger erster Schritt in die richtige Richtung (wenn denn die Mindeststandards auch wirklich von allen hier Adressierten *einzuhalten* sind), der nicht dadurch ausgebremst werden darf, dass sicherlich noch nicht alle relevanten Szenarien abgedeckt oder Teilkonstrukte aus technischer Sicht nicht ideal sind. IT-Sicherheit ist ein dynamischer Prozess und kann schon deshalb nicht in ein statisches Gesetz in seiner Gänze gegossen werden. Das IT-Sicherheitsgesetz kann zu einem Startschuss für eine Bewusstseinsänderung hinsichtlich einer IT-Sicherheitskultur werden, die dann nach und nach möglichst alle Bereiche der IT durchdringt. Die Konzentration auf gewisse Bereiche, die Kritischen Infrastrukturen, erscheint logisch, damit es zumindest einmal losgehen kann.

Gewisse Aspekte könnten jetzt noch in das Gesetz einfließen, ohne zu einer wesentlichen Verzögerung beizutragen. Begleitend zu den Forderungen des IT-Sicherheitsgesetzes müssen Haftungsfragen (z.B. Produkthaftung) an die heutigen Gegebenheiten angepasst werden. Ebenso muss klar sein, welche Konsequenzen ein Nichtbefolgen des IT-Sicherheitsgesetzes nach sich

zieht. Weiterhin ist unabdingbar, dass TKG und TMG konsistent gemacht werden, denn es gibt aus Sicht der Technologie und der Angriffsmöglichkeiten keinen Grund für eine differenzierte Betrachtung.

Weitere Schritte im Rahmen eines IT-Sicherheitsgesetzes wären zur Steigerung der Akzeptanz des BSI das Überdenken dessen Konstruktion in Richtung einer unabhängigeren Einrichtung, die genauere Betrachtung von KMUs und das Überwinden von gesetzlich definierten Barrieren (z.B. Verhältnis Bund/Land/Kommune), die Sicherheitsvorfälle so nicht kennen, im Sinne einer vernetzten Sicherheit zum Wohle der Bürger.



Digitally signed by Jochen Schiller
DN: c=DE, st=Berlin, l=Berlin, o=Freie Universitaet Berlin, ou=Fachbereich Mathematik und Informatik, cn=Jochen Schiller
Date: 2015.04.15 23:40:40 +02'00'

Univ.-Prof. Dr.-Ing. habil. Jochen H. Schiller