Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)284 F

Chaos Computer Club

Stellungnahme zum Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

Linus Neumann, 17. April 2015

Vorbemerkungen

Probleme der IT-Sicherheit sind primär technische Probleme. Politische Lösungen für diese Probleme sind dann zielführend, wenn sie in einer tatsächlichen Erhöhung der IT-Sicherheit resultieren. Technisch kann dieses kann auf zwei Wegen erreicht werden:

1. **Härtung: Begrenzen des Schadenpotenzials möglicher Schwachstellen.**
   Hierunter sind Maßnahmen zu fassen, die einen Angreifer, der über eine unbekannte Schwachstelle in ein System eingedrungen ist, in den Möglichkeiten der Ausnutzung beschränken. Diese Maßnahmen haben den sekundären Effekt, die Attraktivität des Systems für Angreifer zu senken. Beispielhaft sei hier die Ende-zu-Ende-Verschlüsselung genannt: Sie bewahrt die Vertraulichkeit der Kommunikation von Nutzern eines Kommunikationsservers und senkt daher auch die Attraktivität dieses Servers als Angriffsziel. Ähnlich ermöglicht es das sogenannte *Monitoring*, erfolgreiche Angriffe zu detektieren und Gegenmaßnahmen zu ergreifen.
2. **Prävention: Beseitigung von Schwachstellen.**
   Der größere Teil der von Angreifern ausnutzbaren Schwachstellen in IT-Systemen ist unbekannt, bis die Schwachstellen entweder durch Sicherheitstests erkannt und entfernt werden oder bis ihre erfolgreiche Ausnutzung durch Angreifer bemerkt wird. Da letzterer Fall in der Regel mit Schaden einhergeht, ist eine vorherige Entdeckung anzustreben. Beispielhaft sei hier die als *Heartbleed* bekannt gewordene Schwachstelle in der Software-Bibliothek *OpenSSL* genannt, die einen Großteil der weltweiten Internet-Server betraf. Zwischen ihrer unbeabsichtigten Einführung und ihrer Entdeckung vergingen zwei Jahre, in denen alle betroffenen Systeme schutzlos waren.

IT-Sicherheit in Unternehmen

IT-Sicherheit stellt Unternehmen vor eine multi-dimensionale Herausforderung: Potenzielle Angreifer haben viele unterschiedliche Motivationen und Angriffsziele. Beispielsweise könnten ausgewählte Mitarbeiter zum Zwecke der Industriespionage gezielt angegriffen, kritische Systeme zum Zwecke der Sabotage in ihrer Funktion gestört oder Kunden- und Vertragsdaten kopiert werden. Die Liste möglicher Angriffsszenarien ist lang und lässt sich nur eingrenzen, indem die Motivation der potenziellen Angreifer (und damit die Wahrscheinlichkeit eines Angriffs) in Betracht gezogen wird.

Die treibende Kraft der IT-Sicherheit in Unternehmen ist daher eine Abwägung von Eintrittswahrscheinlichkeit und potenziellem Schaden eines Angriffs. So entsteht ein komplexer Verteidigungsraum, in dem viele Risikoszenarien den Geschäftsinteressen der Unternehmen direkt entgegenstehen, während andere nur geringe oder vernachlässigbare Auswirkungen hätten. Entsprechend werden auch die zur Verfügung stehenden Ressourcen eingesetzt: Große Geschäftsrisiken werden minimiert, geringere werden in Kauf genommen.

Dieser Fokus auf Geschäftsrisiken hat den Nebeneffekt, dass potenzielle Schäden für Dritte, insbesondere für Kunden, nur dann ausreichende Berücksichtigung finden, wenn sie mit einem nennenswerten direkten oder indirekten Geschäftsrisiko einhergehen. So ist es nachvollziehbar und nicht unüblich, dass beispielsweise geistiges Eigentum und interne geschäftsrelevante Daten einem höheren Schutzniveau unterliegen als beispielsweise Kundendaten. Aus gesellschaftlicher Perspektive ist diese Tendenz jedoch nicht wünschenswert.

Regulatorische Einflussmöglichkeiten

Ein Gesetz zur Erhöhung der IT-Sicherheit muss einen pro-aktiven Ansatz motivieren, bei dem Prävention und Härtung allgemein und insbesondere in unzureichend geschützten Bereichen über den Stand der Technik hinaus voran getrieben werden.

Unternehmen und Organisationen müssen incentiviert oder gezwungen werden, Defizite in der IT-Sicherheit nicht nur nachträglich zu beheben, sondern aktiv danach zu suchen und zu beseitigen. Da IT-Sicherheit im Allgemeinen von der Abwendung direkter Geschäftsrisiken getrieben wird, ist ein regulativer Eingriff insbesondere dann geboten, wenn keine oder unzureichende ökonomische Anreize bestehen, ein akzeptables Maß an Schutz herbeizuführen.

Entsprechende Anreize können durch ein Anheben vorgeschriebener Sicherheitsstandards über das aktuelle Niveau hinaus, und komplementär durch eine klar definierte Haftung gegenüber Dritten im Schadensfall gesetzt werden.

Bewertung des vorliegenden Entwurfs

Im Folgenden sind die zentralen Kritikpunkte am vorliegenden Gesetzesentwurf (Deutscher Bundestag, Drucksache 18/4096) zusammengefasst.

Fehlende Ansätze zum Endnutzerschutz

Der vorliegende Gesetzesentwurf bezieht sich in großen Teilen auf die Betreiber kritischer Infrastruktur zum Zwecke der Vermeidung eines Ausfalls von IT-Systemen. Gezielte Maßnahmen zum Schutz der Endnutzer werden nicht verlangt.

Diese Schwerpunktsetzung ist vor dem Hintergrund der im BSI-Bericht zur Lage der IT-Sicherheit in Deutschland 2014[1] dokumentierten Risikolandschaft nicht nachvollziehbar. Im Bericht werden Angriffe auf Bundeseinrichtungen, Privatanwender und Wirtschaft unterschieden.

Bundeseinrichtungen. Nach Angaben des BSI werden *„täglich 15 bis 20 Angriffe auf das Regierungsnetz entdeckt, die durch normale Schutzmaßnahmen nicht erkannt worden wären."* Dabei handele es sich bei *„durchschnittlich einem Angriff pro Tag […] um einen gezielten Angriff mit nachrichtendienstlichem Hintergrund."*

→ Hier zeigt sich ein hoher Angriffsdruck, dem mittels Monitoring wirksam entgegengetreten wird.

Im vorliegenden Gesetzesentwurf soll die Rolle des BSI in diesem Bereich ausgebaut werden. Dabei ist festzuhalten, dass beim Monitoring von kritischen Angriffszielen auch das dementsprechende Wissen über fortgeschrittene Angriffstechniken erlangt wird.

Dieses Wissen kann zur wirksamen Verhinderung der Angriffe ebenso verwendet werden, wie zu deren Weiterentwicklung und Zweitverwertung. Eine kompromisslose und rein defensive Ausrichtung des BSI wäre daher Grundvoraussetzung für das Übertragen dieser Verantwortung. Diese Voraussetzungen sind nicht gegeben, solange das BSI dem BMI und seinen offensiven Ambitionen[2] untersteht. Siehe hierzu auch Absatz *Das Vertrauensproblem des BSI wird nicht gelöst*, Seite 9.

---

[1]Bundesamt für Sicherheit in der Informationstechnik (2014): *Bericht zur Lage der IT-Sicherheit in Deutschland,* Version vom 15.12.2014, abgerufen unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf

[2] ZEIT Online vom 13. November 2014: *Die geheime Überwachungswunschliste des BND*, abgerufen unter http://www.zeit.de/digital/internet/2014-11/bnd-bundesnachrichtendienst-ueberwachung-ausbau/komplettansicht

→ Ein Missbrauch des im BSI gesammelten Wissens über Angriffstechniken ist nicht auszuschließen und in Anbetracht der Eingliederung ins BMI sogar als wahrscheinlich einzustufen.

Privatanwender. Nach Angaben des BSI wurden allein im Jahr 2014 *„zwei Identitätsdiebstähle publik, bei denen Angreifer Zugriff auf Benutzernamen und Passwörter von 16 bzw. 18 Millionen Internetnutzern erlangen konnten."* Angaben über eventuelle Überschneidungen der beiden Datensätze werden nicht gemacht. Die Privatanwender waren zwar Opfer dieser Identitätsdiebstähle, doch es ist unwahrscheinlich, dass sie auch zu einem signifikanten Anteil Quelle der erbeuteten Information waren.

Typischerweise stammen solche Daten aus größeren Angriffen auf die Anbieter von Online-Diensten, also Online-Shops, E-Mail-Anbieter oder sogenannte Soziale Netzwerke, die in diesem Fall die betroffenen Nutzer nicht ausreichend geschützt und – gedeckt vom BSI – auch nicht über den erfolgten Angriff informiert haben.

Hier zeigt sich ein hoher Angriffsdruck, dem nur unzureichende Schutzmaßnahmen entgegenstehen. Für die betroffenen Anbieter stand der Schutz der Nutzerdaten nicht im Fokus ihrer ökonomischen Interessen und wurde daher vernachlässigt. Durch die halbherzige Bearbeitung des Falles durch das BSI wurden die Anbieter in dieser Maxime bestärkt, da sie – trotz des hohen Schadens für die Nutzer – weder zur Rechenschaft gezogen wurden noch angemessene Maßnahmen zur Wiederherstellung des Schutzes ergreifen mussten: Eine umfassende Informierung der Nutzer sowie deren Re-Identifikation und darauffolgende Änderung der Zugangsdaten wäre absolut notwendig gewesen.

→ Obwohl Privatnutzer die häufigsten Opfer von Angriffen auf informationsverarbeitende Systeme sind, findet sich im vorliegenden Gesetzesentwurf weder eine Initiative noch eine Absichtserklärung zur Änderung dieser Situation. Diese Schwerpunktlegung ist insbesondere auch in Anbetracht der vom BSI selbst dokumentierten Bedrohungslage nicht nachvollziehbar.

Wirtschaft. Für das Jahr 2014 berichtet das BSI von einem einzigen Fall von Wirtschaftssabotage, bei dem ein Stahlkraftwerk in Folge eines ausgefeilten Social-Engineering-Angriffs massiv beschädigt wurde. Beim Social Engineering werden nicht IT-Systeme angegriffen, sondern deren Nutzer getäuscht, um sie zum Absenken vorhandener Sicherheitsvorkehrungen zu verleiten. Erst durch den freiwillig gewährten Zugriff konnten die Angreifer ihr technisches Detailwissen zum Einsatz bringen und die Anlage durch absichtliche Fehlbedienung massiv beschädigen.

Typischerweise sind in kleinen und mittelständischen Unternehmen (KMU) – im Gegensatz zu Großunternehmen – die Sensibilität für IT-Sicherheit allgemein, für die Gefahren des Social Engineerings und das Befolgen von Sicherheitsregeln noch wenig präsent. Die Awareness für diese Thematik durch die in den Medien vermehrt berichteten Fälle ist zwar zu beobachten und führt in den Unternehmen zu einer deutlichen Entlastungen, dennoch sind Schulungen zwingend nötig.

Der Verlauf des vom BSI beschriebenen Angriffs zeigt eindrücklich, dass kein technisches Schutzsystem in der Lage ist, die „Schwachstelle Mensch“ zu kompensieren. Dieses Risiko bezieht sich nicht nur auf die Täuschung von Administratoren und Nutzern mit Zugriff auf kritische Daten und Systeme: Nicht selten missbrauchen Innentäter vorsätzlich die ihnen anvertrauten Daten für persönliche Zwecke oder die Interessen konkurrierender Unternehmen. Dies ist ein zentrales Argument für Datensparsemkeit.

Die „Schwachstelle Mensch“ ist auch ein ebenso großes Risiko für Endnutzer und Privatpersonen. Vorrangig wird sie im Bereich des Online-Banking-Betrugs und des Identitätsdiebstahls unter Vortäuschung falscher Tatsachen ausgenutzt.

Aufklärung, Schulungen und Weiterbildungen erscheinen als einzige erfolgsversprechende Möglichkeiten, die Anfälligkeit für Social Engineering und prinzipiell soziale Einfallstore nachhaltig zu verringern.

→ Technische Maßnahmen zur IT-Sicherheit werden sehr häufig aus Unwissen über das Risiko, oft versehentlich und in einigen Fällen auch absichtlich außer Kraft gesetzt. Umfassende Aufklärung und Bildungsmaßnahmen in diesem Bereich sind notwendig, um einen höheren Schutz in Bevölkerung und Wirtschaft zu erlangen und die Unternehmenskulturen hinsichtlich IT-Sicherheit zu verändern.

Weiterhin führt das BSI die im Jahr 2014 bekannt gewordenen Schwachstellen *Heartbleed* und *Shellshock* als signifikante Bedrohungen für deutsche Unternehmen an. Das Alter bei Entdeckung betrug bei *Heartbleed* zwei Jahre, bei *Shellshock* sogar ein Vierteljahrhundert. In dieser Zeit waren die Sicherheitslücken öffentlich unbekannt und konnten theoretisch unbemerkt von Angreifern ausgenutzt werden. Im Falle von *Heartbleed* war die für verschlüsselte Verbindungen genutzte Bibliothek *OpenSSL* betroffen, eine zentrale Säule der Sicherheit beim Online-Banking. Ziel des vorliegenden Gesetzesentwurfs muss eine Verkürzung dieser Zeit bis zur Entdeckung sowie die Reduktion der Anzahl an Sicherheitslücken sein.

Dass hochkritische Software, auf deren Sicherheit milliardenschwere Geschäftsmodelle und die Sicherheit von hochkritischen Informationen basieren, so lange Zeit derart schwerwiegende unentdeckte Sicherheitslücken in sich tragen konnte, lässt sich mit dem sozialen Dilemma bei der Qualitätssicherung von Open-Source-Software erklären, das bereits in einer Stellungnahme an den Bundestagsausschuss „Digitale Agenda“ ausgeführt ist[3]:

Für Unternehmen besteht kein Anreiz, in die Prüfung, Auditierung und das Testen von Allgemeingütern zu investieren, da kein wirtschaftlicher Vorteil oder ein Alleinstellungsmerkmal zu erreichen ist: Die Allgemeinheit und somit auch

---

[3] Linus Neumann, Chaos Computer Club (2014): *Effektive IT-Sicherheit fördern – Stellungnahme zur 7. Sitzung des Ausschusses „Digitale Agenda“ des Deutschen Bundestages*, abgerufen unter http://www.bundestag.de/blob/278506/7bfa0b746372768036e3780f49b96ae0/stellungnahme_linus_neumann-pdf-data.pdf

die Konkurrenz würde von den individuellen Investitionen in das öffentliche Gut ebenso profitieren. So wird eine Trittbrettfahrer-Mentalität befördert, die darin mündet, dass alle Betreiber ihre Verantwortung als erfüllt ansehen, indem sie auf dem Stand der Technik operieren.

Eine staatliche Förderung der Sicherheit dieses „Stands der Technik" ist daher im allgemeinen Interesse von Privatpersonen, Bundeseinrichtungen und Wirtschaft gleichermaßen. Insbesondere in der Wirtschaft würden nicht nur große Anbieter, sondern auch KMU profitieren, die im vorliegenden Gesetzesentwurf ebenso wenig berücksichtigt werden wie Privatpersonen.

Zur Erhöhung der Sicherheit von weit verbreiteter sicherheitskritischer Software sind folgende Maßnahmen geeignet:

1. Regelmäßige unabhängige Prüfungen von Open-Source-Software

Überprüfungen können gezielt in Auftrag gegeben werden und durch das Ausschreiben sogenannter *Bug Bounties* flankiert werden. Diese „Kopfgelder" werden als Belohnung für das Finden und Beseitigen kritischer Sicherheitslücken ausgelobt.

Die Befunde müssen veröffentlicht und die daraus resultierenden Verbesserungen der Allgemeinheit zugänglich gemacht werden. Eine intransparente und unkontrollierte Auswertung durch das BSI steht in diametralen Gegensatz zu den Schutzzielen.

→ Die Sicherheit von weitverbreiteter Open-Source-Software ist im öffentlichen Interesse und sollte durch Auditierungen und Bug Bounties aktiv gefördert werden.

2. Haftung für proprietäre Software:

Proprietäre Software entzieht sich durch Intransparenz der Möglichkeit zur unabhängigen Überprüfung durch Dritte. Gleichzeitig operieren kommerzielle Software-Lieferanten und Dienste-Anbieter größtenteils unter dem Ausschluss jeglicher Haftung. Dies ist auch aus ökonomischer Perspektive schwer nachvollziehbar: Eine Haftung würde konkrete Anreize zur Qualitätssicherung schaffen, die bisher grundsätzlich fehlen und die strukturelle Basis für die mangelnde Qualität vieler Software-Projekte sind.

Selbstverständlich muss eine solche Haftung von klaren Anforderungen hinsichtlich der Fahrlässigkeit und Schuldhaftigkeit flankiert werden und würde großen Widerstand aus dem letzten verbliebenen Wirtschaftszweig erfahren, der noch unter Ausschluss jeglicher Haftung operieren darf. Dennoch sei an dieser Stelle sei der Hinweis erlaubt, dass sich in einer solchen Haftung auch die Chance verbirgt, dem für IT-Produkte oft erfolglos beanspruchten Qualitätsmerkmal „Made in Germany" zu nennenswerter Reputation zu verhelfen.

→ Klare Haftungsregeln würden zu einem starken ökonomischen Anreiz für die Hersteller von proprietärer Software führen, IT-Sicherheit pro-aktiv zu betreiben.

Oft unterliegen IT-Systeme Patch-Zyklen im Bereich mehrerer Monate und befinden sich in entsprechend hoffnungslos veraltetem Zustand, ohne dass einer Ausnutzung durch sekundäre Maßnahmen vorgebeugt wird. Bei fahrlässigen

Verschleppungen sollten verantwortliche Anbieter oder Dienstleister im Schadensfall haften. So würde ein klarer ökonomischer Anreiz entstehen, Systeme auf einem aktuellen Stand, und damit die Angriffsfläche möglichst gering zu halten.

→ Haftung würde als unmittelbarer monetärer Anreiz eine sehr viel konkretere Wirkung entfalten, als die im vorliegenden Gesetzesentwurf vorgesehenen zwei-jährlichen Nachweispflichten.

Kritische Infrastruktur. Das einzige vom BSI dokumentierte Angriffsmuster, das 2014 im Bereich der kritischen Infrastrukturen stattgefunden hat, ist erneut das Social Engineering. Ziel dieses Angriffs war jedoch das *„Übermitteln einer Kopie eines amtlichen Lichtbildausweises und [der] Bankverbindung des Gehaltskontos"* der Opfer – eine klassisches Täuschungsszenario, bei dem Privatpersonen um ihr Vermögen erleichtert werden. Und so wurden mittels *„gefälschten Unterschriften die Bankkonten der Betroffenen aufgelöst oder neue EC-Karten samt PIN an eine neue Adresse in China angefordert."* Auf einen Ausfall der Infrastruktur wurde von Seiten der Angreifer nicht hingewirkt. Auch für vorherige Jahre[4,5] ist nicht ein einziger derartiger Vorfall dokumentiert. Entsprechend attestiert das BSI schon im Jahr 2009[6]:

Bei den Betreibern der so genannten Kritischen Infrastrukturen können IT-Sicherheitsbewusstsein und -kompetenz sowohl auf Managementebene als auch in der Umsetzung durchweg als hoch eingeschätzt werden.

→ Auch wenn der Chaos Computer Club diese Einschätzung nicht teilt[7], so ist der einseitige Fokus auf ein bisher nicht realisiertes Bedrohungsszenario schwer nachvollziehbar, während häufig

---

[4] Bundesamt für Sicherheit in der Informationstechnik (2013): *Fokus IT-Sicherheit,* Version vom 13.11.2013, abgerufen unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Fokus_IT-Sicherheit_2013_nbf.pdf

[5] Bundesamt für Sicherheit in der Informationstechnik (2011): *Die Lage der IT-Sicherheit in Deutschland,* barrierefreie Version vom 16.06.2011, abgerufen unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011.pdf

[6] Bundesamt für Sicherheit in der Informationstechnik (2009): *Die Lage der IT-Sicherheit in Deutschland,* Version vom Januar 2009, abgerufen unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2009_pdf.pdf

[7] Nord, Friedrich (2014): *Stellungnahme zur Konsultation des „IT-Sicherheitskatalog" gem. §11 Abs. 1a Energiewirtschaftsgesetz*, Version vom 12.02.2014, abgerufen unter http://ccc.de/system/uploads/143/original/BNetzA-Konsultation-ITSicherheit-Stromnetz.pdf

erfolgreiche Angriffe mit hohen Anzahlen an geschädigten Personen vollständig ignoriert werden.

Steigerung der Bürokratie statt aktiver Erhöhung der Sicherheit

Die für IT-Sicherheit verantwortlichen Abteilungen in deutschen Unternehmen sind hauptsächlich mit der bürokratischen Verwaltung ausführlicher Checklisten beschäftigt. Der Verwaltungsaufwand zur Einhaltung von allerlei Zertifizierungsvorgaben und Normen geht dabei nicht selten zulasten pro-aktiver technischer Maßnahmen zur nennenswerten Erhöhung der IT-Sicherheit: Allein die Verwaltung der Compliance-Vorgaben einer mittelgroßen Organisation erschöpft schon die vorhandenen Ressourcen. So verkommt das dynamische Feld der IT-Sicherheit nicht selten zu einem steifen Korsett, das Innovation und Agilität verhindert, ohne dabei signifikant zur IT-Sicherheit beizutragen, geschweige denn Raum zur Steigerung zu lassen.

Angreifer hingegen agieren frei von regulatorischen und organisatorischen Zwängen und konzentrieren sich auf real-existierende Schwächen. Zur effizienten Verteidigung muss daher technische Innovation von individuellen Sicherheitskonzepten flankiert, und die Agilität auch in der Abwehr erhalten bleiben.

Im vorliegenden Gesetzesentwurf wird ein gegenteiliger Schwerpunkt gelegt: In der Regel bereits bestehende Sicherheitskonzepte sollen einheitlich verschriftlicht, und Auditierungen lückenlos protokolliert werden. So werden die neu zu bestimmenden Alarmierungskontakte hauptsächlich damit befasst sein, ihre Auskunfts-, Dokumentations- und Berichtspflichten zu erfüllen.

→ Eine weitere Bürokratisierung der IT-Sicherheit geht zulasten dringend notwendiger pro-aktiver Maßnahmen zur effektiven Erhöhung der IT-Sicherheit.

Bedauerlicherweise wird im vorliegenden Gesetzesentwurf zusätzlich die Gelegenheit versäumt, durch eine vorgeschriebene Sicherheitsanforderungen eine pro-aktive Herangehensweise zu erzwingen, oder zumindest zu incentivieren: Insbesondere im Bereich der kritischen Kommunikationsinfrastrukturen besteht nennenswertes Verbesserungspotenzial über den viel zitierten „Stand der Technik“ hinaus:

- Zentrale Strukturen sollten aufgebrochen werden, um die Resilienz zu erhöhen, und gleichzeitig Angriffsfläche und Schadenspotenzial zu verringern.
- Starke Sicherheitsstandards sollten vorgeschrieben werden. Insbesondere sollte eine Ende-zu-Ende-Verschlüsselung zum Standard bei Kommunikationsdiensten gehören.

Vorschlagsrecht der Betreiber führt gewünschten Effekt der Sicherheitsstandards ad absurdum

Der neu formulierte §8a BSI-Gesetz verpflichtet Betreiber kritischer Infrastrukturen, *angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und*

Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen.

Diese Vorkehrungen seien als angemessen anzusehen, wenn sie

1. dem Stand der Technik entsprechen,
2. der Aufwand nicht außer Verhältnis zum Schadensfall steht.

→ Die Festlegung auf den „Stand der Technik" schließt jedes Potenzial für eine nennenswerte, pro-aktive Verbesserung der Schutzvorkehrungen kategorisch aus.

Gleichzeitig sind diese Anforderungen so unscharf definiert, dass sie eine große Rechtsunsicherheit in sich bergen, die offenbar durch die Absätze 2 und 3 beseitigt werden soll:

Darin wird den Betreibern kritischer Infrastrukturen ein Vorschlagsrecht für branchenspezifische Sicherheitsstandards eingeräumt. Auf Antrag stellt das BSI fest, ob diese den Anforderungen nach Absatz 1 genügen und beseitigt somit die drohende Rechtsunsicherheit. Das Erfüllen dieser Sicherheitsstandards sollen Betreiber dann mindestens alle zwei Jahre nachweisen, indem eine *Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel* übermittelt wird.

Bei der Abstimmung der spezifischen Sicherheitsstandards besteht für die Branchenvertreter zunächst die Herausforderung, die jeweils bestehenden Standards miteinander zu vergleichen und in eine gemeinsame Sprache zu überführen. Der Vergleich wird einen großen Bereich an Sicherheitsanforderungen ergeben, der von allen Branchenvertretern abgedeckt wird, sowie mehrere Teilbereiche, in denen einige Vertreter stärkere Schutzmaßnahmen ergriffen haben als andere.

Im Sinne einer Erhöhung der IT-Sicherheit aller Betreiber wäre es natürlich wünschenswert, dass mindestens die Summe aller Maßnahmen als neuer Standard definiert wird oder im Idealfall gar darüber hinaus gehende Ziele definiert werden.

Die ökonomischen Anreize der Branchenvertreter stehen diesem Ziel jedoch diametral entgegen: Wenn stattdessen der Minimalkonsens als Branchenstandard beschlossen und vorgeschlagen wird, werden Investitionskosten und das potenzielle Risiko, die eigenen Sicherheitsvorgaben nicht erfüllen zu können, vermieden.

→ Das Vorschlagsrecht für branchenspezifische Standards wird dazu führen, dass bereits bestehende Minimalstandards festgeschrieben werden. Auch hier ist jedes Potenzial für eine nennenswerte, pro-aktive Verbesserung der Schutzvorkehrungen ausgeschlossen.

Geschwächter Datenschutz führt zu höheren Risiken

Schon beim Blick auf die aktuell gültige Version des TKG vom 25. Juli 2014 ist aus technischer Perspektive nicht nachvollziehbar, auf welche Weise die Bestandsdaten der Nutzer zum Erkennen, Eingrenzen oder Beseitigen von Fehlern oder Störungen eines technischen Gerätes von Bedeutung sein könnten.

Störungen und Fehler sind akute Phänomene, bei denen die Funktionalität des betroffenen Systems beeinträchtigt ist. Das Erkennen gestaltet sich demnach nicht schwierig und wird durch langfristige Datenvorhaltung nicht erleichtert. Hingegen ist im Rahmen der Beseitigung und des Eingrenzens ein temporäres Speichern von Verkehrsdaten durchaus hilfreich und teilweise notwendig. Der Verwendung von Bestandsdaten kommt jedoch in keinem dieser Fälle eine Notwendigkeit zu.

Schon heute nehmen Anbieter unter Berufung auf § 100 Abs. 1 TKG eine für diesen Zweck unnötige Speicherung von Verkehrsdaten über mehre Tage oder Wochen vor. Dabei werden Informationen über Telefonverbindungen, Standorte und Internetverbindungen aller Kunden auf Vorrat gespeichert. Nach einer Erhebung des AK Vorratsdatenpeicherung variieren die Vorhaltezeiten zwischen 3 und 180 Tagen.[8] Schon diese große Spannbreite zeigt eindrücklich, dass den gesammelten Daten keine Bedeutung für den Erhalt des Systembetriebs zukommt: Selbst eine mehr als drei oder gar 180 Tage andauernde Störung ließe sich wohl kaum noch mit Hilfe von Verkehrsdatensammlungen beheben. Dies gilt auch für den Bereich von *„Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können."*

Der vorliegende Gesetzesentwurf soll Risiken der IT-Sicherheit minimieren, Einbrüche in informationstechnische Systeme verhindern und Möglichkeiten zum Datenmissbrauch einschränken. Eine langfristige Speicherung trägt dazu nicht bei, sondern führt umgekehrt zu einer Erhöhung des Angriffsrisikos und zu einer Erhöhung des Schadenspotenzials möglicher Angriffe.

Die 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. und 19. März 2015 in Wiesbaden[9] bringt daher valide Argumente gegen diese umfassende Vorratsdatenspeicherung vor, die auch in der Stellungnahme des Bundesrats[10] zum vorliegenden Gesetzesentwurf bekräftigt werden.

→ Sowohl dem bestehenden als auch dem hier vorgeschlagenen § 100 Abs. 1 TKG kommt keine Bedeutung bei der Erkennung, Eingrenzung und Behebung von technischen Störungen, Fehlern und Angriffen zu.

---

[8] Arbeitskreis Vorratsdatenspeicherung (2015): *Speicherdauer (Übersicht)*, Version vom 26. März 2015, abrufbar unter http://wiki.vorratsdatenspeicherung.de/index.php?title=Speicherdauer&oldid=128634

[9] Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015: *IT-Sicherheitsgesetz nicht ohne Datenschutz!* abrufbar unter https://www.datenschutz.hessen.de/k89.htm#entry4320

[10] Bundesrat Drucksache 643/1/14, abrufbar unter http://www.bundesrat.de/SharedDocs/drucksachen/2014/0601-0700/643-1-14.pdf?__blob=publicationFile&v=1

→ Eine Beschränkung des zulässigen Verwendungszwecks der Daten ist dringend geboten.

→ Konkrete zeitliche Einschränkungen der zulässigen Vorhaltungsdauer sind dringend geboten.

Das Vertrauensproblem des BSI wird nicht gelöst

Zusammen mit dem IT-Fachverband BITKOM betreibt das BSI seit November 2012 eine Meldestelle für Angriffe auf Computersysteme im Rahmen der *Allianz für Cyber-Sicherheit*. Bisher blieb diese Initiative bahnbrechende Erfolgsmeldungen schuldig, und das BSI konnte sich in der Industrie nicht als Ansprechpartner erster Wahl etablieren. Im vorliegenden Gesetzesentwurf sollen Betreiber kritischer Infrastrukturen nun zur Zusammenarbeit mit der Behörde verpflichtet werden.

Dass sich eine vertrauensvolle freiwillige Zusammenarbeit nicht etablieren konnte, ist der Vertrauenskrise des BSI geschuldet, für die es zwei Auslöser gibt:

1. Das BSI steht nicht im Ruf, im akuten Fall kompetente und zeitnahe Unterstützung leisten zu können.
2. Es bestehen konkrete Anlässe zum Zweifel daran, dass das BSI ausschließlich der Sicherheit von Computern und Netzen verpflichtet ist und nicht im Rahmen von Aufgaben bei der sogenannten „inneren Sicherheit“ gezielt auf eine Schwächung von Endgeräten und Kommunikationsinfrastrukturen hinarbeitet.

So war das BSI schon im Jahr 2007 an zentraler Stelle an der Entwicklung einer Schadsoftware zum Einsatz gegen Bundesbürger beteiligt[11] und hat mit dem Standard De-Mail einen gezielt geschwächtes System definiert. Die akkreditierten Anbieter gehen inzwischen in eigenständigen Initiativen freiwillig über das verlangte Sicherheitsniveau hinaus[12], um das öffentliche Ansehen des Systems zu retten.

---

[11] Bundesamt für Sicherheit in der Informationstechnik (2009): *Bedrohung der Informationssicherheit durch den gezielten Einsatz von Schadprogrammen*, Version 1.1 vom 3.04.2007, abrufbar unter

- https://netzpolitik.org/wp-upload/Leitfaden-Schadprogramme-0-Deckblatt.pdf
- https://netzpolitik.org/wp-upload/Leitfaden-Schadprogramme-1-Ueberblick.pdf
- https://netzpolitik.org/wp-upload/Leitfaden-Schadprogramme-2-Massnahmen.pdf
- https://netzpolitik.org/wp-upload/Leitfaden-Schadprogramme-3-Kurztest.pdf

[12] Pressemitteilung der Deutschen Telekom vom 9. März 2015: *De-Mail: Ende-zu-Ende-Verschlüsselung kommt*, abrufbar unter http://www.telekom.com/medien/produkte-fuer-privatkunden/271200

Wurzel der Zweifel an der Unabhängigkeit des BSI ist seine mangelnde Unabhängigkeit vom BMI. Insbesondere in Anbetracht der im Gesetzesentwurf geforderten Berichtspflichten, die das im BSI gesammelte Wissen über Schwachstellen und Angriffe potenzieren wird, muss diese Unabhängigkeit zwingend hergestellt werden: Die Begehrlichkeiten des BMI zum Erwerb des Wissens über ausnutzbare Sicherheitslücken zur Nutzung in Angriffen sind ausführlich dokumentiert[13], und eine entsprechende Sekundärverwertung des beim BSI gesammelten Wissens ist nicht nur nicht auszuschließen, sondern im Gegenteil sogar sehr wahrscheinlich.

→ Die Ausweitung des Aufgabenbereichs des BSI sowie die Kritikalität der beim BSI gesammelten Informationen über Sicherheitslücken erfordert zwingend die Aufstellung des BSI als unabhängige Bundesbehörde mit unzweideutigem Sicherheitsauftrag.

[13] ZEIT Online vom 9. November 2014: *BND will Sicherheitslücken kaufen und ausnutzen*, abgerufen unter http://www.zeit.de/digital/internet/2014-11/bnd-zero-day-exploit-sicherheit

Fazit

Keiner der in diesem Gesetzesentwurf vorgesehenen Schritte ist geeignet, zu einer sinnvollen Erhöhung der IT-Sicherheit in Deutschland beizutragen. Die Auskunfts-, Dokumentations- und Berichtspflichten, die Unternehmen auferlegt werden sollen, erhöhen im Gegenteil den Bürokratieaufwand und gehen daher zulasten von Ressourcen, die andernfalls für pro-aktive Maßnahmen zur tatsächlichen Erhöhung der IT-Sicherheit verwendet werden könnten.

Den großflächigen Angriffen auf Privatpersonen und den daraus resultierenden Schäden wird nicht entgegen getreten. Stattdessen soll durch zentrale und intransparente Strukturen Angriffswissen auf Regierungsebene zusammen getragen werden.

Für die im Gesetzesentwurf mandatierte langfristige Vorhaltung von Verkehrsdaten zum Zwecke der Störungsaufklärung gibt es aus technischer Perspektive keine Grundlage. Demgegenüber steht ein erhöhtes Missbrauchspotenzial, das zu einer effektiven Erhöhung des Risikos führt.