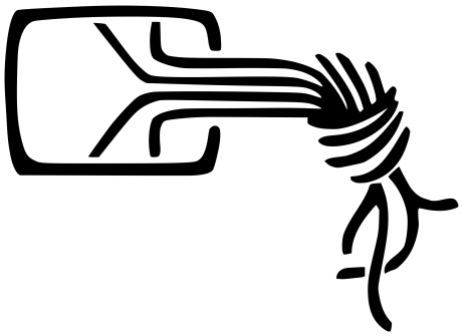
Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)741 F



Sicherheit gestalten statt Unsicherheit verwalten

Sachverständigenauskunft zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

Linus Neumann

Frank Rieger, Dirk Engling, Matthias Marx

Chaos Computer Club

01. März 2021

1. Einordnung

Dem vorliegenden Gesetzentwurf kann nicht ohne den Kontext vorangegangener und paralleler Gesetzgebungsvorhaben Rechnung getragen werden.

1.1 Das erste IT-Sicherheitsgesetz war ein Schuss in den Ofen.

Das erste IT-Sicherheitsgesetz[1] wurde 2015 diskutiert und verabschiedet. In seiner damaligen Sachverständigenauskunft an den Innenausschuss des Deutschen Bundestags kritisierte der Chaos Computer Club (CCC)[2]

- fehlende Ansätze zum Schutz von Endnutzerinnen,
- Steigerung der Bürokratie statt aktiver Erhöhung der IT-Sicherheit,
- Verwässerung der Sicherheitsstandards durch Vorschlagsrecht der Betreiber,
- höhere Risiken durch geschwächten Datenschutz und
- das Vertrauensproblem des BSI durch seine fehlende Unabhängigkeit vom BMI.

Das Fazit des CCC lautete:

> *Keiner der in diesem Gesetzentwurf 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.*

Mit Blick auf das tägliche Angriffsgeschehen und die resultierenden Schäden für Bürgerinnen und Wirtschaft stellen wir fest, dass unsere Befürchtungen eingetreten sind.

---

[1] Bundesanzeiger: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015

[2] CCC: Stellungnahme zum Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme - IT-Sicherheitsgesetz – Linus Neumann, 17. April 2015

Das BSI verwaltet Missstände, statt ihnen aktiv entgegen zu treten.

Ein Bundesamt für Sicherheit in der Informationstechnik (BSI) muss sich daran messen lassen, dass es aktiv auf eine Erhöhung der IT-Sicherheit hinwirkt. Die durch das erste IT-Sicherheitsgesetz mandatierten Aufgaben legen den Schwerpunkt jedoch in der bürokratischen Verwaltung von Schwachstellen.

Beispiel Wahlsoftware

Vor der Bundestagswahl 2017 enthüllte der CCC eklatante Sicherheitsmängel in den zur Auswertung der Wahl verwendeten IT-Systemen, insbesondere auch einer weit verbreiteten Software zur Erfassung und Aggregation der Stimmen.[3] Zuvor hatte sich die Öffentlichkeit über Monate vor einem Hackerangriff auf die Bundestagswahl gesorgt.

Die vom CCC veröffentlichten Schwachstellen ermöglichten ein mit geringem Aufwand zu realisierendes und verheerendes Angriffsszenario auf Bundestagswahlergebnisse in mehreren Ländern. BMI und BSI zeigten sich hilflos: Rechtliche Beschränkungen hinderten das BSI am beherzten Eingriff zur Absicherung der antiken Systeme. Auch eine rechtzeitige eigenständige Untersuchung der Wahlsysteme war offenbar außerhalb des Vorstellbaren gewesen.

Es folgten mehrere inkompetente und nicht zielführende Versuche der Herstellerin, die Schwachstellen zu beheben. Schließlich “spendete” der CCC den Fix zu Behebung der schwerwiegendsten Schwachstelle.[4]

Die darauffolgenden Aktivitäten des BSI im hochkritischen Bereich der Wahlsicherheit bestanden in der Formulierung von 18 Anforderungen[5] zur Absicherung von Schnellmeldungen für die Durchführung der Europawahl 2019[6] sowie eines Anforderungskatalogs für die Bundestagswahl 2021, der zeitnah veröffentlicht werden

---

[3] ccc.de: Software zur Auswertung der Bundestagswahl unsicher und angreifbar

[4] ccc.de: Open-Source-Spende: CCC schließt größte Schwachstelle in PC-Wahl

[5] insidas.de: Europawahl 2019: Wie Kommunen die Wahlergebnisse schützen sollten, abgerufen am 26. Februar 2021

[6] bsi.bund.de: Die Lage der IT-Sicherheit in Deutschland 2019

soll. Die Anforderungen richten sich dabei an einen üblichen IT-Verbund, in dem die mangelhafte Software betrieben werden soll, zu deren Verbesserung seit 2017 offenbar kein nennenswerter Beitrag geleistet wurde:

Ende 2020 präsentierten Sicherheitsforscher auf der Jahresabschlusskonferenz des CCC[7] eklatante Schwachstellen in einer Wahlsoftware, die von der Herstellerin auch heute noch mit vollmundigen Versprechen beworben wird:

> *Bei der Entwicklung von OK.VOTE wurde höchster Wert auf das Thema Sicherheit gelegt. Diese orientiert sich an den* ***Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI)*** *und der Non-Profit-Organisation Open Web Application Security Project (OWASP). Mit dem Einsatz von OK.VOTE in unserem* ***BSI-zertifizierten Outsourcing-Rechenzentrum*** *ist die Einhaltung der geforderten hohen Sicherheitsstandards gewährleistet.*[8]

Dieses Desaster zeigt abermals die Hilflosigkeit des BSI: Es ist gezwungen, Missstände zu verwalten, statt ihnen aktiv, kompromisslos und entschieden entgegentreten zu können.

Beispiel Ransomware

Kurz nach Verabschiedung des ersten IT-Sicherheitsgesetzes nahm der weltweite Trend zu Ransomware-Angriffen in Deutschland Fahrt auf: Im Jahr 2016 dominierte die Ransomware Locky[9] erstmals das Nachrichtengeschehen. In den Folgejahren konnten BSI und Bundesrepublik den Trend hilflos weiter beobachten:

- Im *Bundeslagebild Cybercrime 2016* stellt das BKA eine Zunahme um +94,4% fest,[10]

---

[7] media.ccc.de: Madl, Tobias & Obermaier, Johannes (2020): Hacking German Elections Insecure Electronic Vote Counting - How It Returned and Why You Don't Even Know About It

[8] akdb.de: OK.VOTE: Die IT-Lösung für die optimale Organisation, Vorbereitung und Durchführung von Wahlen, abgerufen am 26. Februar 2020

[9] Wikipedia: Locky

[10] BKA: Bundeslagebild Cybercrime 2016

- im *Bericht zur Lage der IT-Sicherheit in Deutschland* stellte das BSI fest, dass Ransomware "auch 2017 die maßgebliche Quelle für Schadprogramminfektionen geblieben" sei, [11]
- für das Jahr 2018 bemerkt das BKA, dass sich die "Ransomware-Szene durch eine zunehmende Professionalisierung auszeichne" [12] und
- auch im aktuellen *Bundeslagebild Cybercrime 2019* bleibt "Ransomware die größte Bedrohung für Wirtschaftsunternehmen"[13].

Während diese Gefahr über nunmehr fünf Jahre unverändert blieb, konnte in deutschen kritischen Infrastrukturen und Unternehmen nur sehr zögerlich Resilienz gegen derartige Angriffe aufgebaut werden. Dies geschah jedoch nicht wegen, sondern eher trotz des ersten IT-Sicherheitsgesetzes, dessen Untauglichkeit sich nicht nur in diesem eingängigen Beispiel illustrieren lässt.

Entsprechend nimmt auch die Problem- und Zieldefinition des vorliegenden Gesetzentwurfes (Drucksache 19/26106 in der Version vom 15.01.2021) direkt auf diese Angriffsklasse Bezug:

> *Die Schadsoftware „Emotet" dominiert bereits seit Jahren die Gefährdungslage. Vorfälle wie die Ransomware „WannaCry" verdeutlichen die Situation.*

Fehler sind nicht vergebens, wenn man aus ihnen lernt.

Es wäre natürlich wünschenswert, derartige Phänomene kritisch zu evaluieren, um mit einem zweiten IT-Sicherheitsgesetz pro-aktiv die IT-Sicherheit von morgen gestalten und künftig auf neue Trends im Angriffsgeschehen reagieren zu können. Eine Evaluation sollte natürlich nicht auf Basis anekdotischer Evidenz, sondern durch eine unabhängige und objektive Analyse erfolgen. Eine solche ist tatsächlich im ersten IT-Sicherheitsgesetz verankert, wurde jedoch von der Bundesregierung ignoriert. [14]

---

[11] BSI: Die Lage der IT-Sicherheit in Deutschland 2017

[12] BKA: Bundeslagebild Cybercrime 2018

[13] BKA: Bundeslagebild Cybercrime 2019

[14] Bundesanzeiger: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015

Insbesondere sollten die Maßnahmen zur Benennung und Regulierung der IT-Sicherheit von kritischen Infrastrukturen durch das BSI von unabhängigen Sachverständigen evaluiert werden.

Es ist bedauerlich, dass eine unabhängige Evaluation nicht erfolgt ist. Verwunderlich ist dies insbesondere, weil der vorliegende Gesetzentwurf laut Angabe der Autorinnen erstens "auf Erfahrungen mit der Anwendung der im ersten IT-Sicherheitsgesetz geregelten Befugnisse" basieren und zweitens die Regulierungsbefugnisse des BSI erheblich erweitern soll.

Empfehlung: Die Bundesregierung sollte gesetzeskonform zunächst die Evaluation des ersten IT-Sicherheitsgesetzes durchführen. Auf Basis dieser Evaluation könnte ein empirisch gestütztes IT-Sicherheitsgesetz Fehler des ersten IT-Sicherheitsgesetzes korrigieren.

1.2 Anforderungen an ein zeitgemäßes IT-Sicherheitsgesetz

Ziel eines *Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme* sollte die Erhöhung der Sicherheit informationstechnischer Systeme sein. Einleitend ist festzuhalten, dass es sich bei der IT-Sicherheit um einen zumindest theoretisch relativ fortgeschrittenen Forschungsbereich handelt: Alle *praktisch relevanten* Probleme sind *theoretisch* gelöst. Es gibt zurzeit keine essentiellen praktisch relevanten Herausforderungen, deren theoretische Lösung unbekannt wäre. Trotzdem ist der Zustand der IT-Sicherheit in der Praxis desaströs.

Dies liegt einerseits an der mangelnden Umsetzung von technischem Basiswissen der IT-Sicherheit, andererseits an den Herausforderungen der organisatorischen IT-Sicherheit und der Mensch-Maschine-Interaktion. Jeder IT-Sicherheitsvorfall – ob klein, ob groß – lässt sich auf die Verletzung wohlbekannter Regeln und Prinzipien der IT-Sicherheit zurückführen. Das lapidar klingende Ziel muss sein, dass diese in der Breite auch kompromisslose Anwendung finden. Dass dieses Ziel zurzeit in weiter Ferne scheint, zeigt nur, wie dringend es verfolgt werden muss und wie eklatant es in den vergangenen Jahrzehnten vernachlässigt wurde.

Statt vorhandene Ressourcen zu nutzen und auszubauen, versucht das BMI, das Rad auf Basis der Quadratur des Kreises neu zu erfinden: Systeme sollen einerseits unsicher genug sein, dass Strafverfolgungsbehörden und Geheimdienste eindringen können, andererseits sollen Wirtschaft und Bürgerinnen auf „sichere“ IT vertrauen können. Dieser janusköpfige Ansatz ist zum Scheitern verurteilt.

Auch ein digitales Entwicklungsland muss sich *weiterentwickeln.*

Die Herausforderungen der SARS-CoV-2-Pandemie haben deutschen Bürgerinnen die mangelhafte digitale Infrastruktur und die daraus resultierende mangelnde Digitalisierung relevanter Lebens- und Wirtschaftsbereiche schmerzlich spüren lassen.

Die Bundesrepublik hat in den vergangenen Jahrzehnten zu jedem Zeitpunkt über die finanziellen Ressourcen verfügt, durch mutige Investition, Förderung und Bildung zur digitalen Vorzeigenation ausgebaut zu werden. Entsprechende Vorstöße waren jedoch immer halbherzig, wurden nicht zu Ende gedacht und kaputt-bürokratisiert, bevor sie ihr Potenzial entfalten konnten.

Zaghafte Ansätze im Bereich der IT-Sicherheit ereilte das gleiche Schicksal. Die *De-Mail*, das *besondere elektronische Anwaltspostfach* und der *elektronische Personalausweis* sind nur einige Beispiele für Projekte, die sich zur Geißel aller Beteiligten oder zu mahnenden Bauruinen mit Nutzungszahlen im hohen einstelligen Bereich entwickelten. Die Ursache war in allen Fällen die gleiche: Eine fehlende Strategie, um kompromisslos und mutig Digitalisierung und IT-Sicherheit einen Schritt voran zu bringen.

Auch in der Digitalisierung der Verwaltung fehlte jegliche Strategie – und wo es an einer Strategie mangelt, steht früher oder später die Konsolidierung ins Haus. Im Jahre 2015 erstmals groß angekündigt, hat diese bisher das dreifache Budget verschlungen, ohne dass ein Ende in Sicht wäre.[15] [16] Das Versagen hat System.

Und genau dieses System und dieses Versagen sind dafür verantwortlich, dass die Bundesrepublik sich ohne Einflussmöglichkeiten als Spielball im Feld der IT-Sicherheit bewegt, statt das Feld aktiv zu gestalten. So sieht dieses System aus:

[15] tagesschau.de: IT-Projekt des Bundes: 3,4 Milliarden Euro und kein Ende, abgerufen am 26. Februar 2021

[16] spiegel.de: Modernisierung der Bundes-IT: Verheerende Zwischenbilanz, abgerufen am 26. Februar 2021

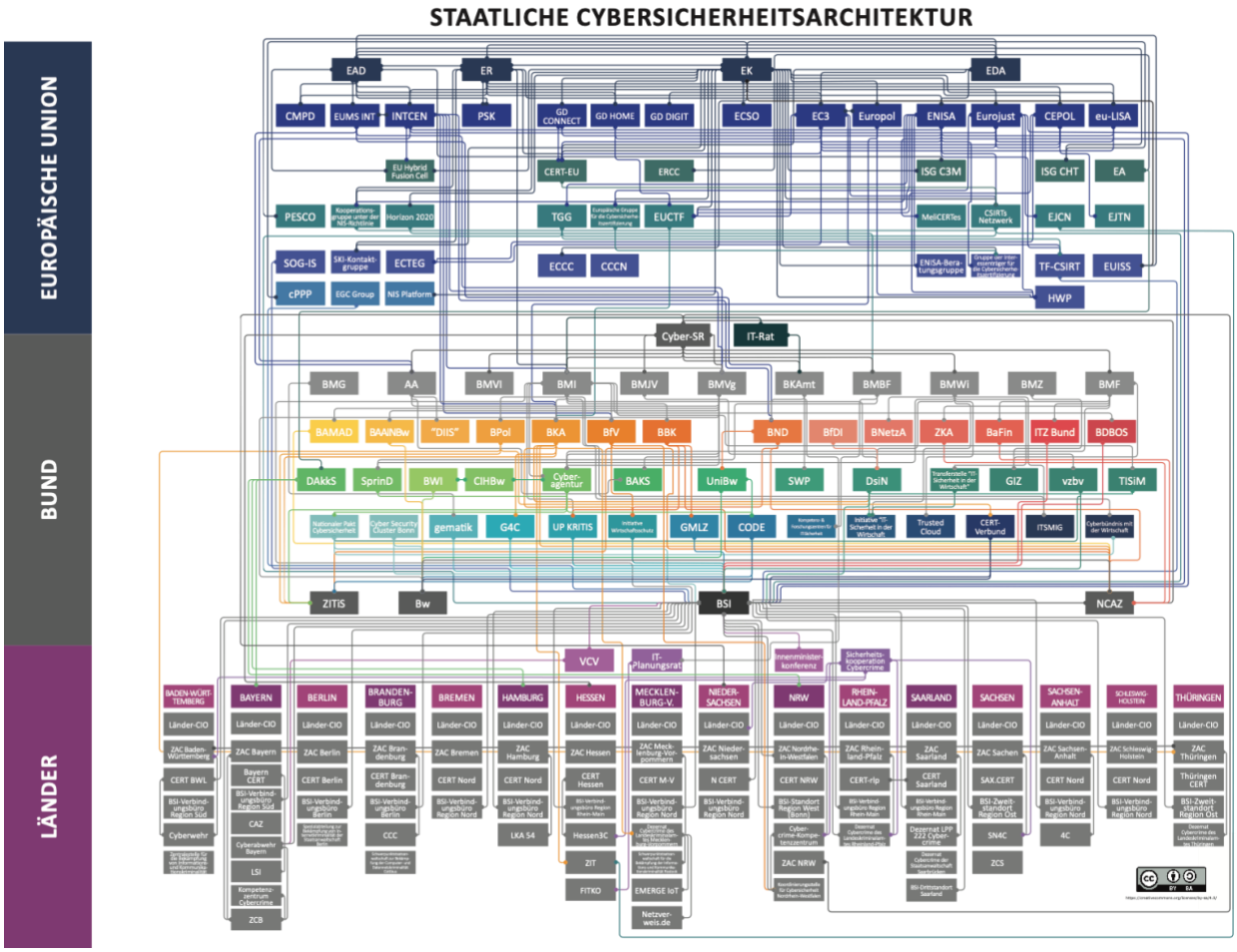


Abbildung 1. Staatliche Cybersicherheitsarchitektur. Aus: Herpig, Sven & Beigel, Rebecca (2020): Deutsche Cybersicherheits- und Cyberverteidigungspolitik: Staatliche Akteure und Zuständigkeiten (5. Auflage)[17]

Empfehlung: Der Deutsche Bundestag möge sich vom Bundesministerium des Innern, für Bau und Heimat das obige Schaubild erklären lassen oder eine Person finden, die dazu in der Lage ist.

[17] Herpig, Sven & Beigel, Rebecca (2020): Deutsche Cybersicherheits- und Cyberverteidigungspolitik: Staatliche Akteure und Zuständigkeiten (5. Auflage), zuletzt abgerufen am 26. Februar 2020. Für neue Auflagen siehe ggf. stiftung-nv.de: Akteure und Zuständigkeiten in der deutschen Cybersicherheitspolitik

Empfehlung: Die Bundes- und Länderregierungen mögen die Zuständigkeiten und Aufgaben in der deutschen IT-Sicherheitspolitik auf Interessenkonflikte, Verantwortungsdiffusion und Konsolidierungspotenziale untersuchen, Interessenkonflikte auflösen und Konsolidierungspotenziale realisieren.

IT-Sicherheit *gestalten* statt verwalten!

Es ist nicht möglich, *auch ein bisschen Digitalisierung* zu machen. Und es ist nicht möglich, *auch ein bisschen IT-Sicherheit* zu machen – vor allem *nicht nachträglich.*

Ein einzelner Brand muss gelöscht werden. Zu diesem Zweck wird es immer eine Feuerwehr geben müssen. Wenn aber die Brände in Frequenz und Anzahl die Kapazitäten jeder Feuerwehr um ein Vielfaches übersteigen, wird es Zeit, über Brandschutz nachzudenken: IT-Sicherheit muss schon beim Schreiben der ersten Zeile Code, vor dem Platzieren des ersten Elements im Netzwerk-Architekturdiagramm bedacht werden. Den Überlegungen muss ein Bedrohungsmodell zugrunde liegen und das obere Ziel muss immer die Verringerung von Angriffsfläche sein.

Werden diese Grundprinzipien nicht bedacht, verkommen nachträgliche Bemühungen zur Herstellung von IT-Sicherheit zur Sisyphos-Aufgabe. Leider müssen sich Bürgerinnen, Wirtschaft und kritische Infrastrukturen auch heute noch dieser Sisyphos-Aufgabe stellen, weil es an einer kompromisslosen IT-Sicherheitsstrategie und einer auf dieser Basis errichteten sicheren Basis mangelt.

Dass Betreiberinnen kritischer Infrastruktur auch heute meist keine andere Wahl haben, als hochkritische Komponenten mit hoffnungslos veralteten Systemen zu steuern, ist Ergebnis einer inzwischen jahrzehntelangen Strategielosigkeit, die sich im Verwalten von Schwachstellen und dem halbherzigen Ergreifen nicht abgestimmter Einzelmaßnahmen niederschlägt.

Von dieser mangelnden Strategielosigkeit und dem fehlenden Gestaltungswillen ist leider auch der vorliegende Gesetzentwurf geprägt.

IT-Sicherheit kennt keine Kompromisse.

Schwachstellen in der IT-Sicherheit kennen keine Kompromisse, kein gutes Zureden, keine Gnade und auch keine Nachsicht. Vor allem aber kennen sie nicht den Unterschied zwischen Gut und Böse. Systeme können nur entweder für alle Nutzerinnen sicher oder für alle Nutzerinnen unsicher sein.

Es wird Zeit, dass diese recht simple, aber fundamentale Erkenntnis sich auch in der IT-Sicherheitspolitik der Bundesrepublik Deutschland durchsetzt.

Empfehlung: Ein IT-Sicherheitsgesetz muss konkrete und kompromisslose Maßnahmen zur Erhöhung von IT-Sicherheit beschließen. Abwägungen und gezielte Schwächungen sind ebenso fehl am Platz wie ambitionslose Ansätze zur Verwaltung von Unsicherheit.

Schwachstellen schließen, Sicherheitsniveau erhöhen!

Seit vielen Jahren wiederholt der CCC die Forderung nach einem kompromisslosen und unabhängigen BSI. Der vorliegende Gesetzentwurf zeigt in besonderer Tragik auf, wie wichtig diese Forderung ist.

Zurückgehaltene Schwachstellen betreffen immer alle betroffenen Systeme und damit auch die des Staates, der Zivilgesellschaft, Wirtschaft und kritischen Infrastrukturen. Die mitunter katastrophalen Konsequenzen einer solchen Geheimhaltung kann man am Beispiel der Angriffe “Wannacry” und “Notpetya” sehen, die im Gesetzentwurf und seiner Begründung selbst mehrmals exemplarisch herangezogen werden.

Empfehlung: Unter keinen Umständen sollte das BSI jemals berechtigt sein, bei Kenntnis von Schwachstellen etwas anderes zu tun, als die Betroffenen zu informieren, auf eine Beseitigung hinzuarbeiten und zu gegebenem Zeitpunkt die Öffentlichkeit zu warnen.

Bürokratie ist Feindin der IT-Sicherheit.

Wenngleich sich dieser Eindruck einer Bürgerin der Bundesrepublik Deutschland vielleicht nicht unmittelbar aufdrängt, handelt es sich bei der IT und deren Sicherheit um ein sehr dynamisches Feld, in dem auch nur zeitweiser Stillstand unmittelbaren Rückschritt bedeutet.

Implizite Maßgaben wie *„never change a running system“*, denen die Annahme zugrunde liegt, ein einmal geprüftes System würde sicher bleiben, bedeuten genau diesen Rückschritt. Implizit auf solchen Maßgaben basierende Zertifizierungen und bürokratische Hürden gehen daher mit enormen Opportunitätskosten einher: Sie verhindern aktiv die Weiterentwicklung und dynamische Auseinandersetzung mit zukünftigen Herausforderungen.

Empfehlung: Ein IT-Sicherheitsgesetz sollte IT-Sicherheit fördern, statt sie durch Bürokratie auszubremsen.

Vertrauen ist gut, Kontrolle ist besser!

Im ewigen Wettlauf zwischen Angriff und Verteidigung können nur nachhaltige Sicherheitsmaßnahmen dauerhaften Vorsprung bieten. Fehlt schon das Vertrauen in eine sichere Basis, kann keine sichere Infrastruktur geschaffen werden.

Insbesondere kritische Infrastrukturen und nicht zuletzt die Einrichtungen des Bundes sind seit jeher von mangelndem Vertrauen in IT-Systeme geplagt. Möglichkeiten, eine sichere, nachhaltige und quelloffene Basis bereitzustellen, bleiben ungenutzt.

Durch die Bündelung von Ressourcen und das freie Zugänglichmachen der Ergebnisse in Open-Source-Projekten könnte die Bundesrepublik wichtige Grundlagen für nachhaltige technologische Souveränität legen.

Schaffung eines Pools von auditierter Open-Source-Software

Moderne Software und Systeme beruhen auf einer Vielzahl von Einzelkomponenten aus verschiedensten Quellen. Dabei ist die Sicherheit des Gesamtsystems höchstens so gut wie die der einzelnen Komponenten. Nicht selten handelt es sich bei sicherheitskritischen Software-Bibliotheken um von Freiwilligen in ihrer Freizeit programmierte Open-Source-Software mit stark schwankenden Sicherheitseigenschaften. Im Sinne einer nachhaltigen, dauerhaften Verbesserung der IT-Sicherheit – auch für die vom BSI direkt betreuten Behörden – ist es unerlässlich, die Sicherheit und Qualität möglichst vieler Open-Source-Komponenten dauerhaft zu steigern.

Empfehlung: Schaffung eines Pools von auditierter Open-Source-Software

1. Bereitstellung von Ressourcen für die unbürokratische und schnelle Auditierung existierender Open-Source-Komponenten.

2. Schaffung einer Organisation, die die langfristige Förderung der Entwicklung sicherer Open-Source-Software unter einer permissiven Lizenz, die auch den Einsatz in der Wirtschaft erlaubt, zum Ziel hat.

3. Unbürokratische dauerhafte Förderung von Entwicklungsprojekten für Hard- und Software-Komponenten durch diese Organisation, die bisher fehlen oder für die nur Optionen in nicht ausreichender Qualität verfügbar sind.

Nachhaltige Verbesserung der Bildung und Ausbildung im Bereich IT-Sicherheit

Ohne gut ausgebildetes Personal ist keine Verbesserung der IT-Sicherheit zu erzielen. Auch im Jahre 2021 verlassen Informatik-Absolventinnen deutsche Universitäten, ohne auch nur ein Seminar zum Thema IT-Sicherheit oder sicherem Programmieren belegt zu haben.

Empfehlung: Nachhaltige Verbesserung der Bildung und Ausbildung im Bereich IT-Sicherheit durch

1. Verpflichtende Einführung von Bildungskomponenten für die sichere Konfiguration von Systemen und Programmierung von Software in allen Bildungswegen, deren Absolventinnen IT-Systeme entwickeln (Ausbildung und Studium).

2. Bereitstellung von kostenfreiem, hochqualitativen Bildungsmaterial für IT-Sicherheit und sichere Software-Entwicklung für alle Bildungswege durch den Bund.

Überprüfung eigener Infrastruktur ermutigen statt kriminalisieren!

Zur Überprüfung der IT-Sicherheit eigener Infrastruktur gehört der regelmäßige und kontrollierte Einsatz von Angriffsprogrammen. Jedoch wird der Einsatz solcher Programme zur Erforschung ihrer Wirkweise und Folgen mit § 202c StGB kriminalisiert.[18] Dies benachteiligt den Industrie- und IT-Sicherheitsstandort Deutschland und setzt Forscherinnen, Betreiberinnen und Prüferinnen einem realitätsfremden Rechtsrisiko aus.

Empfehlung: § 202c StGB sollte gestrichen werden, um die Überprüfung eigener Infrastruktur durch den kontrollierten Einsatz von Angriffsprogrammen nicht nur ohne Rechtsrisiko zu ermöglichen, sondern auch zu ermutigen.

[18] ccc.de: § 202c StGB gefährdet den IT-Standort Deutschland

1.3 Einbettung in sonstige Vorhaben im Bereich der IT-Sicherheit

Der vorliegende Gesetzentwurf hat zum Ziel, die *"Cyber- und Informationssicherheit"* für die *"Digitalisierung aller Lebensbereiche"* zu *"gewährleisten."* Schon im ersten Absatz wird korrekt festgestellt:

> *Voraussetzung hierfür ist eine sichere Infrastruktur.*

Das Ziel einer sicheren Infrastruktur wird im vorliegenden Gesetzentwurf jedoch nur halbherzig verfolgt, in anderen Initiativen des BMI sogar aktiv verhindert.

Da die Bundesregierung in parallelen Gesetzesvorhaben und Initiativen auf EU-Ebene eine gezielte Schwächung digitaler Infrastrukturen vorantreibt, kann der vorliegende Entwurf nicht ohne diesen Kontext in Gänze bewertet werden. Im Folgenden werden daher zunächst exemplarisch gleichzeitige Bemühungen der Bundesregierung zusammengefasst, die eine Schwächung der digitalen Infrastrukturen zum erklärten Ziel haben. Aufgrund der Fülle dieser Bemühungen konzentrieren wir uns dabei ohne Anspruch auf Vollständigkeit auf die wichtigsten Vorstöße seit Inkrafttreten des ersten IT-Sicherheitsgesetzes:

Ausweitung des Einsatzes von staatlicher Schadsoftware

Die Befugnisse zum Einsatz von Schadsoftware zur Durchführung der so genannten "Quellen-Telekommunikationsüberwachung" und "Online-Durchsuchung" wurden 2017 im Rahmen der Änderung der Strafprozessordnung massiv ausgeweitet[19]. Der CCC warnte in seiner Sachverständigenauskunft an den Rechtsausschuss des Bundestags vor *Risiken für die innere Sicherheit beim Einsatz von Schadsoftware in der Strafverfolgung*[20], weil die IT-Sicherheit der Endgeräte dafür erheblich beeinträchtigt wird. Seitdem wurde die Befugnis zur Quellen-TKÜ auf insgesamt 44 Straftatbestände ausgeweitet. Mehrere Gesetzentwürfe weiten auch die Befugnis zur Online-Durchsuchung aus.

---

[19] netzpolitik.org: Wir veröffentlichen den Gesetzentwurf der Großen Koalition zum massenhaften Einsatz von Staatstrojanern, abgerufen am 26. Februar 2021

[20] ccc.de: Risiken für die innere Sicherheit beim Einsatz von Schadsoftware in der Strafverfolgung

Um diese Maßnahmen umzusetzen, werden Schwachstellen in den Systemen der Zielpersonen benötigt. Schwachstellen können jedoch nur in allen Systemen gleichzeitig vorhanden oder nicht vorhanden sein. Sie sind politisch neutral und stehen grundsätzlich allen Angreiferinnen zur Verfügung. Zwar lassen sich staatliche Hintertüren theoretisch mit wirksamem Zugriffsschutz versehen, doch diese Hintertüren ließen sich nicht geheim halten. Es wäre daher töricht anzunehmen, dass Kriminelle Geräte mit derartigen Schwachstellen und Hintertüren nutzen würden. Geschwächt bleiben deutsche Bürgerinnen und die deutsche Wirtschaft, während Kriminelle auf sichere – und obendrein potenziell illegale! – Systeme ausweichen.

Dem für diese Schwächung verantwortlichen Bundesministerium des Innern, für Bau und Heimat untersteht auch das Bundesamt für Sicherheit in der Informationstechnik, das sogar aktiv an der Entwicklung eines deutschen Staatstrojaners mitgewirkt hat.[21] Der Chaos Computer Club hat diesen Staatstrojaner 2011 analysiert und nachgewiesen, dass die verfassungsrechtlich vorgeschriebenen Grenzen der Schadsoftware in vielerlei Hinsicht weit überschritten wurden.[22]

Es stellt sich die Frage, wie das BSI mit so offensichtlichen Interessenkonflikten und zweifelhafter Vorgeschichte in Zukunft glaubwürdig zur IT-Sicherheit in Deutschland beitragen soll, solange es der Weisungsbefugnis des BMI unterliegt.

Gesetz zur Anpassung des Verfassungsschutzrechts

Um diese Schwächung der Endgeräte komfortabler vornehmen zu können, sollen mit dem *Gesetz zur Anpassung des Verfassungsschutzrechts*[23] nun sogar Netzbetreiberinnen in die Pflicht genommen werden, durch gezielte Umleitung von Internetverkehr Angriffe auf die eigenen Kundinnen zu ermöglichen. Dies ist ein katastrophaler Eingriff in das Vertrauensverhältnis zwischen Infrastrukturanbietern und Bundesbürgerinnen.

---

[21] netzpolitik.org: BSI programmierte und arbeitete aktiv am Staatstrojaner, streitet aber Zusammenarbeit ab, abgerufen am 26. Februar 2021

[22] ccc.de: Analyse einer Regierungsmalware

[23] bundestag.de Gesetz zur Anpassung des Verfassungsschutzrechts

Des Weiteren sollen neben den Strafverfolgungsbehörden auch alle 19 Geheimdienste die Befugnis zum Einsatz von Staatstrojanern erhalten.

Es ist schwer vorstellbar, wie sich diese weitreichenden Eingriffe zur Schwächung von Infrastruktur- und Kommunikationssicherheit mit dem vorliegenden Gesetzentwurf in Einklang bringen lassen sollen.

Gesetz zur Modernisierung der Rechtsgrundlagen der Bundespolizei

Mit dem geplanten *Gesetz zur Modernisierung der Rechtsgrundlagen der Bundespolizei* sollen Staatstrojaner sogar gegen Menschen eingesetzt werden dürfen, die nicht einmal einer Straftat verdächtigt werden, wenn beispielsweise angenommen wird, dass eine Person eine *Straftat in der Zukunft begehen wird*, oder *angenommen wird, dass ihr Endgerät von einer verdächtigten Person benutzt werden wird.* [24]

Auch hier führt das BMI einen kompromisslosen Kampf gegen die Vertraulichkeit der Kommunikation und damit die IT-Sicherheit der Bürgerinnen.

Kooperation mit zweifelhaften Herstellern

Das BKA ist seit 2012 Kunde des Unternehmenskonglomerats "Gamma/Finfisher",[25] gegen das sich seit Mitte 2019 strafrechtliche Ermittlungen des Zollkriminalamts richten. Auslöser für diese Ermittlungen ist eine Strafanzeige der Gesellschaft für Freiheitsrechte, Reporter ohne Grenzen, dem Europäischen Zentrum für Verfassungs- und Menschenrechte sowie netzpolitik.org. In diesem Rahmen hat auch der Chaos Computer Club eine Analyse durchgeführt, die eindeutige Hinweise für den Einsatz der Schadsoftware gegen demokratische Oppositionelle in der Türkei und somit das Umgehen von Exportrestriktionen durch das Firmenkonglomerat zusammenträgt.[26]

---

[24] bundestag.de: Gesetzentwurf der Fraktionen der CDU/CSU und SPD zum Entwurf eines Gesetzes zur Modernisierung der Rechtsgrundlagen der Bundespolizei, abgerufen am 26. Februar 2021

[25] netzpolitik.org: Bundeskriminalamt kauft international bekannten Staatstrojaner FinFisher/FinSpy von Gamma, abgerufen am 26. Februar 2021

[26] ccc.de: CCC analysiert Münchner Staatstrojaner FinSpy

Anfang Oktober 2020 wurden von der Staatsanwaltschaft München I in Zusammenarbeit mit dem Zollkriminalamt insgesamt 15 Geschäftsräume und Privatwohnungen rund um München und ein Unternehmen aus dem Umfeld des Konglomerats in Rumänien durchsucht.

Während hinsichtlich der strafbewehrten Umgehung von Exportrestriktionen bisher nur ein Verdacht besteht, der Auslöser für die umfassenden Ermittlungsmaßnahmen war, ist der weltweite, wiederholte und grobe Verstoß gegen rechtsstaatliche Prinzipien durch Gamma/Finfisher öffentlich seit Jahren über jeden Zweifel erwiesen. Ihre Produkte wurden mindestens eingesetzt:

- gegen die demokratische Opposition in Ägypten,[27]
- gegen Aktivistinnen in Bahrain,[28]
- gegen US-Bürgerinnen auf Betreiben Äthiopiens,[29]
- gegen die Opposition in Uganda,[30]
- etc. pp.

Diese Angriffe finden unter Ausnutzung menschlicher und technischer Schwachstellen seit über einem Jahrzehnt statt und werden von der Bundesregierung offenbar nicht nur nicht bekämpft, sondern das Betreiben der Unternehmensgruppe sogar durch aktive Kundschaft gefördert.

---

[27] amnesty.org: German-made FinSpy spyware found in Egypt, and Mac and Linux versions revealed, abgerufen am 26. Februar 2021

[28] privacyinternational.org: Bahraini Government, With Help From FinFisher, Tracks Activists Living In The United Kingdom, abgerufen am 26. Februar 2021

[29] citizenlab.ca: You Only Click Twice – FinFisher's Global Proliferation, abgerufen am 26. Februar 2021

[30] privacyinternational.org: Ugandan Government Deployed FinFisher Spyware To 'Crush' Opposition, Track Elected Officials And Media In Secret Operation During Post-Election Protests, Documents Reveal, abgerufen am 26. Februar 2021

Die eigentlich im Arbeitsauftrag des BSI liegenden Maßnahmen zur Bekämpfung der Schadsoftware, beispielsweise durch die öffentliche Bereitstellung von Analyse-Tools, Detektionsregeln[31] und Forschungsergebnissen[32], werden derweil vom CCC geleistet.

Vor diesem Hintergrund ist kaum verwunderlich, dass staatliche Bestrebungen scheitern, die IT-Sicherheit für Bürgerinnen und Wirtschaft zu erhöhen.

Automatisierter Angriff auf die Vertraulichkeit von Messenger-Kommunikation

Der CCC engagiert sich seit vielen Jahren für den *Ausstieg aus unverschlüsselter Kommunikation*.[33] Dieses Schutzziel teilt die Bundesregierung offenbar nicht: In einer Stellungnahme an den Innenausschuss des Bundestags 2020 musste der CCC sogar der Forderung nach einem kompromisslosen *Recht auf Verschlüsselung* Nachdruck verleihen.[34]

Das groß angekündigte Verschlüsselungsprojekt De-Mail wird inzwischen selbst von den Betreiberinnen als "überkomplizierter" und "toter Gaul" bezeichnet. Trotz Investitionen in dreistelliger Millionenhöhe habe es "nie jemanden gegeben, der dieses Produkt genutzt hat."[35] Der Chaos Computer Club hatte in mehreren Sachverständigenauskünften vor der Untauglichkeit des Systems gewarnt.[36][37]

Nachdem auch das *besondere elektronische Anwaltspostfach (beA)* gelinde gesagt suboptimale Ergebnisse hervorbrachte, sind verschlüsselte Messenger die derzeit einzige niederschwellige und massenhaft zur Verfügung stehende

---

[31] github.com: Schröder, Thorsten & Neumann, Linus (2018): FinSpy-Tools, abgerufen am 26. Februar 2021

[32] github.com: Neumann, Linus & Schröder, Thorsten (2018): FinSpy-Dokumentation, abgerufen am 26. Februar 2021

[33] ccc.de: CCC fordert Ausstieg aus verschlüsselter Kommunikation

[34] ccc.de: CCC fordert kompromissloses Recht auf Verschlüsselung

[35] Jungundnaiv.de: Tim Höttges, Vorstandsvorsitzender der Deutschen Telekom AG, "Jung und Naiv" Folge 498, abgerufen am 26. Februar 2021

[36] ccc.de: Gutachten unterstreicht Untauglichkeit der De-Mail für rechtsverbindliche Kommunikation

[37] ccc.de: Chaos Computer Club erneuert Kritik am Gesetzentwurf zur De-Mail

Verschlüsselungslösung zum Schutz deutscher Bürgerinnen und Unternehmen. Statt diesen überfälligen Zugewinn an Sicherheit zu begrüßen und zu fördern, ist das BMI stets bemüht, die gewonnene Sicherheit wieder abzubauen.

Auf EU-Ebene engagiert sich die Bundesregierung für Scanner und Filter, die Kommunikation auf illegale Inhalte prüfen sollen. Dass dabei sämtliche Kommunikationsinhalte gescannt werden, wird geflissentlich ignoriert. Um dies zu ermöglichen, sollen sogar aktiv die Anforderungen der e-Privacy-Richtlinie abgeschwächt werden,[38] weil diese derartige Scanner aktiv verbieten.

ZITIS: Behörde mit dem erklärten Ziel der Schwächung von IT-Sicherheit

Seit April 2017 unterhält das BMI eine eigene Bundesanstalt zur gezielten Schwächung der IT-Sicherheit. Zu deren vier Geschäftsfeldern gehören die Telekommunikationsüberwachung und Kryptoanalyse zum gezielten Brechen verschlüsselter Kommunikationsinhalte. Als Bedarfsträgerinnen der "Zentralen Stelle für Informationstechnik im Sicherheitsbereich" gelten BKA, BfV und BPOL, im Beirat haben weiterhin BND, MAD, ZKA und BMI Gaststatus.

Alle genannten Behörden befinden sich – ebenso wie das BSI – im Geschäftsbereich des BMI. Es bleibt unerklärlich, wie das BSI seinem Arbeitsauftrag ungehindert nachkommen soll, wenn die eigene Dienstherrin mit so ausgeprägter Verve gegenteilige Interessen verfolgt.

Angriff auf Kommunikationsnetze durch den BND

Im Mai 2020 hat das Bundesverfassungsgericht die Internetüberwachung durch den Bundesnachrichtendienst für grundgesetzwidrig erklärt. Der BND betreibt diese Überwachung seit Jahren ohne gesetzliches Mandat, welches ihm durch die BND-Gesetznovelle erstmals – gemäß dem Motto "Das Gesetz verstößt gegen den

---

[38] europa.eu: Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über eine vorübergehende Ausnahme von bestimmten Vorschriften der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates hinsichtlich der Verwendung von Technik durch Anbieter nummernunabhängiger interpersoneller Kommunikationsdienste zur Verarbeitung personenbezogener und anderer Daten zwecks Bekämpfung des sexuellen Missbrauchs von Kindern im Internet, abgerufen am 26. Februar 2021

Geheimdienst" – erteilt worden war. Auch der zweite, aktuell stattfindende Versuch, ein grundgesetzkonformes BND-Gesetz zu formulieren, droht derweil an schlichter Ignoranz gegenüber dem Grundgesetz und dem Urteil des Bundesverfassungsgerichts zu scheitern.

Mit der zum Zeitpunkt des Schreibens dieser Stellungnahme noch nicht beschlossenen Novelle des BND-Gesetzes soll der BND ermächtigt werden, ohne Wissen der jeweiligen Betreiberin auf Bestands-, Verkehrs- und Inhaltsdaten zuzugreifen und hierzu *mit heimlichen Mitteln und/oder unter Zugriff auf informationstechnische Systeme von Telekommunikationsanbietern Sicherungsmaßnahmen zu überwinden*.[39] Damit werden alle Diensteanbieterinnen von Telekommunikation, Clouddiensten und sonstigen Telemediendiensten im Ausland erklärte Ziele staatlichen Hackings.[40][41]

Diese aktive Ermächtigung zum Angriff auf die Vertraulichkeit internationaler Kommunikationsnetze und deren Betreiberinnen ist insbesondere im Hinblick auf den geplanten *§ 9b (2) Untersagung des Einsatzes kritischer Komponenten* relevant. Siehe hierzu *Definition "vertrauenswürdiger Anbieter" greift ins Leere (§ 9b)*, Seite 33.

[39] bundestag.de: Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts in der Version vom 25. Januar 2021, abgerufen am 26. Februar 2021

[40] netzpolitik.org: BND-Gesetz: Sachverständige kritisieren Hacken und Ausspähen unter Freunden, abgerufen am 26. Februar 2021

[41] netzpolitik.org: BND-Gesetz: Eine neue Lizenz zum Hacken, abgerufen am 26. Februar 2021

Fazit

Die Bundesregierung verwendet mehr Energie auf den gezielten Abbau von IT-Sicherheit als auf ihre aktive Förderung. Dieses Engagement steht im diametralen Gegensatz zum Schutzbedarf der deutschen Bürgerinnen und der Wirtschaft der Bundesrepublik Deutschland.

Empfehlung: Bundestag und Bundesregierung sollten IT-Sicherheit zum konkreten und kompromisslosen Ziel der Innenpolitik der Bundesrepublik Deutschland machen und dieses Ziel auch aktiv verfolgen.

Bestrebungen zur Schwächung der IT-Sicherheit von Endgeräten und digitalen Infrastrukturen sind umgehend einzustellen.

Bereits erlassene Gesetze zur Schwächung der IT-Sicherheit von Endgeräten und digitalen Infrastrukturen sind entsprechend zu revidieren.

2. Kritik am vorliegenden Entwurf

Im Folgenden werden ausgewählte Aspekte des vorliegenden Gesetzentwurfs einer eingehenden Bewertung unterzogen. Grundsätzlich ist hervorzuheben, dass dem BSI in seiner aktuellen organisatorischen Einbindung aufgrund des offensichtlichen Interessenkonflikts mit der Dienstherrin keinerlei Befugnisse zum aktiven Eingreifen in IT-Systeme oder zur Sammlung sensibler Daten gewährt werden sollten.

Empfehlung: Das BSI muss als eigenständige und unabhängige Bundesbehörde aus dem Aufsichtsbereich des BMI herausgelöst werden, um seinem gesetzmäßigen Auftrag kompromisslos nachgehen zu können.

Siehe hierzu insbesondere auch *"Überwiegende Sicherheitsinteressen"*, Seite 27.

Vertrauensverlust durch zweifelhaften Umgang mit Schwachstellen

Der vorliegende Gesetzentwurf räumt dem BSI weitreichende Kompetenzen ein, hochsensibles Wissen über kritische Schwachstellen zu erlangen und anzuwenden. Mittels automatisierter Scanner soll das BSI nicht nur nach Schwachstellen suchen, sondern auch mittels *Brute-Force*-Angriffen aktiv unberechtigten Zugriff auf Systeme anstreben.

Im Sinne der Verteidigung gehören derartige Angriffsversuche zum Standardrepertoire der IT-Sicherheit: Schwachstellen werden gefunden, um sie zu schließen. Der vorliegende Gesetzentwurf versäumt aber, das BSI zur Einhaltung minimaler ethischer Standards der IT-Sicherheitsforschung zu verpflichten. Stattdessen wird das BSI explizit zur Verletzung ethischer Standards ermächtigt: Breitflächige Ausnahmetatbestände sollen es dem BSI erlauben, entgegen seinem erklärten Auftrag Schwachstellen *nicht* zu melden, betroffene IT-Systeme *wissentlich* unsicher zu lassen und aktive Angriffe wissentlich *zu ermöglichen, statt sie zu verhindern*.

Empfehlung: Unter keinen Umständen sollte das BSI jemals berechtigt sein, bei Kenntnis von Schwachstellen etwas anderes zu tun, als die Betroffenen zu informieren, auf eine Beseitigung hinzuarbeiten und zu gegebenem Zeitpunkt die Öffentlichkeit zu warnen.

Unwirtschaftliche und zweifelhafte Befugnis zu Portscans (§ 7b)

Mit *„§7b Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden“* soll dem BSI die Befugnis eingeräumt werden, mittels Portscans vorher bestimmte informationstechnische Systeme *„des Bundes oder kritischer Infrastrukturen, digitaler Dienste und der Unternehmen im besonderen öffentlichen Interesse“* auf Sicherheitslücken zu prüfen.

Wirtschaftlichkeit

Der Erfüllungsaufwand wird mit einmalig 1.7 Mio. und jährlich mehr als 1.1 Mio. Euro beziffert:

> *Um diese neue Aufgabe effektiv umzusetzen, benötigt das Bundesamt 10 Planstellen/Stellen (7 hD; 3 gD) mit Personalkosten in Höhe von jährlich 0,94 Mio. Euro sowie Sacheinzelkosten in Höhe von 0,25 Mio. Euro jährlich. Zusätzlich wird mit einmaligen Sachkosten in Höhe von 1,7 Mio. Euro gerechnet.*

Es ist zutreffend, dass es sich bei Portscans *um ein Verfahren handelt, das grundsätzlich jedermann zugänglich ist und das regelmäßig auch zu Angriffszwecken von Kriminellen genutzt wird*. Eine Reihe privatwirtschaftlicher Anbieterinnen führt diese bereits regelmäßig durch und stellt die Ergebnisse teils kostenlos öffentlich zur Verfügung. Tiefergehende Analysen, Suchfunktionen und Auswertungen von unterschiedlicher Qualität und Aussagekraft werden teils von unseriösen, teils von seriösen Anbieterinnen zu moderaten Preisen angeboten.

Empfehlung: Im Rahmen der Wirtschaftlichkeit sollte das BSI die bestehenden kommerziellen Angebote hinsichtlich ihrer Aussagekraft evaluieren.

Unrealistische Ziele

Der Kreis der potenziellen Ziele für Portscans durch das BSI ist eng gewählt und deckt Privatanschlüsse und KMU nicht mit ab. Dadurch wird zumindest sichergestellt, dass die Empfängerinnen der Portscans von ihrem Glück wissen, in Zukunft neben den vielen täglichen Portscans auch regelmäßig das BSI in den Logfiles begrüßen zu dürfen.

Systeme, die einem Portscan nicht standhalten, werden schon das “Internet-Grundrauschen” an Angriffsaktivität nicht überleben. Zwischen den avisierten Portscans durch das BSI und dem Vorgehen von tatsächlichen Angreiferinnen gibt es

jedoch einen entscheidenden Unterschied: Angreiferinnen automatisieren nicht nur die Suche nach Schwachstellen, sondern auch deren direkte Ausnutzung.

Es ist daher höchst unwahrscheinlich, dass das BSI eine *öffentlich bekannte Schwachstelle* schneller findet, als interessierte Angreiferinnen und diese schneller melden und beheben lassen kann, als Angreiferinnen für die automatisierte Ausnutzung brauchen.

Empfehlung: Die Ressourcen des BSI sollten in aussichtsreichere Aktivitäten investiert werden, die Schwachstellen am Entstehen zu hindern.

"Überwiegende Sicherheitsinteressen"

In §7b Absatz 3 erfährt die Informationspflicht des BSI gegenüber den Betreiberinnen betroffener Geräte eine empfindliche Einschränkung:

> *Wird durch [Portscans] eine Sicherheitslücke oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems erkannt und* ***stehen überwiegende Sicherheitsinteressen nicht entgegen,*** *sind die für das informationstechnische System Verantwortlichen darüber zu informieren.*

Diese Einschränkung ist ein weiteres von unzähligen Beispielen für die Unterordnung der Sicherheitsinteressen der kritischen Infrastrukturen der Bundesrepublik Deutschland gegenüber den Unsicherheitsinteressen des BMI. Es ist nicht weniger als eine durchschaubare Frechheit, Befugnisse zum Aufspüren von Sicherheitslücken zum Zwecke der Information der Betroffenen einzufordern und sich noch auf der gleichen Seite des Gesetzentwurfs von der Informationspflicht zu entbinden.

Die konkrete Motivation zur wissentlichen Geheimhaltung von Schwachstellen wird inzwischen nicht einmal mehr galant geleugnet. So betont beispielweise das BKA freimütig, dass es Kenntnis von Schwachstellen hat, diese aktiv ausnutzt, und die verantwortlichen Stellen nicht darüber in Kenntnis setzt:

Zum anderen [würden] die Anbieter kommerzieller Hard- und Software in die Lage versetzt, die von der Überwachungssoftware genutzten Angriffsvektoren (Schwachstellen etc.) zu ***schließen*** *und den Einsatz der Software unter Umständen* ***dauerhaft zu verhindern****. Dies hätte eine schwerwiegende* ***Beeinträchtigung*** *der Fähigkeiten der zuständigen Sicherheitsbehörden zur Sachverhaltsaufklärung im Rahmen der Strafverfolgung bzw. Gefahrenabwehr insbesondere in den Kriminalitätsfeldern Terrorismus/Extremismus und der Organisierten Kriminalität zur Folge.*[42] [43]

Schwachstellen werden demnach wissentlich geheim gehalten und ihre Ausnutzung durch Dritte in Kauf genommen.

Empfehlung: Unter keinen Umständen sollte das BSI jemals berechtigt sein, bei Kenntnis von Schwachstellen etwas anderes zu tun, als die Betroffenen zu informieren, auf eine Beseitigung hinzuarbeiten und zu gegebenem Zeitpunkt die Öffentlichkeit zu warnen.

[42] fragdenstaat.de: ZV 32-21-5391.04-2/18 – Widerspruchsbescheid zur Anfrage *Überprüfung von Produkten der ITÜ*, abgerufen am 26. Februar 2021

[43] netzpolitik.org: Das BKA verhindert, dass Sicherheitslücken geschlossen werden, abgerufen am 26. Februar 2021

Überbordende Befugnisse zum Eingriff in IT-Systeme (§7c)

Mit §7c soll das BSI ermächtigt werden, a) die Umleitung von Internetverkehr und b) das Versenden *„technischer Befehle zur Bereinigung von einem konkret benannten Schadprogramm an betroffene informationstechnische Systeme“* anzuordnen. Während die Umleitung von Internetverkehr schon heute gängige Praxis ist, würde mit dem aktiven Eingriff in potenziell befallene Systeme riskantes Terrain betreten. Die vorgeschlagenen rechtlichen Rahmenbedingungen sind weder dem Risiko noch dem Missbrauchspotenzial angemessen.

Unklare Grenzen der Anordnungsbefugnis

In § 7c Abs. 1 wird die Verpflichtung von Anbieterinnen im Sinne des Telekommunikationsgesetzes so unscharf definiert, dass nicht ersichtlich ist, ob auch Anbieterinnen von nicht rufnummern- oder leitungsgebundenen Telekommunikationsdiensten unter die Verpflichtung fallen.

Durch die geplante Ausweitung des Kreises der Verpflichteten im Telekommunikations-Modernisierungsgesetz entsteht hier auch eine potentielle Ausweitung der Auswirkung der Eingriffsbefugnisse auf einen weiten Kreis von Anbieterinnen mit erheblichen Konsequenzen für die Schwere des Eingriffs.

Empfehlung: Die Anordnungsbefugnis muss Anbieterinnen von nicht rufnummern- oder leitungsgebundenen Telekommunikationsdiensten, Betriebssystemen, App Stores etc. explizit *ausschließen* und darf sich nur auf Anbieterinnen von „Datenleitungen“ im engsten Sinne des Wortes beziehen.

„Sinkholing“ ist schon heute gängige Praxis

Die Befugnisse des BSI zur Anordnung eines Eingriffs in die Telekommunikation werden nicht beschränkt auf Fälle, in denen die TK-Anbieterin nicht selbst in der Lage ist, notwendige Maßnahmen zur Eindämmung von weit verbreiteten Schadprogrammen zu treffen.

Das BSI soll mit einer uneingeschränkten Befugnis ausgestattet werden, die einen unnötigen Interessens- und Verantwortungskonflikt erzeugt: Insbesondere große TK-Anbieterinnen sind bereits heute entsprechend der in § 100 9a Abs. 5 und 6 des TKG erteilten Befugnisse dazu in der Lage und auch erfolgreich beim Erreichen der

definierten Schutzziele. Die Kooperation von Unternehmen bei der Bekämpfung von Schadsoftware und Botnetzen ist ein eingespielter Prozess, in den das BSI nur eingreifen sollte, wenn er nicht funktioniert. Das BSI würde hier in einem funktionierenden und bestehenden Prozess als unnötige dritte Partei eingefügt.

Empfehlung: Die Befugnisse des BSI zur Anordnung von „Sinkholing" sollten sich auf solche Fälle beschränken, in denen TK-Anbieterinnen nicht selbst in der Lage sind, entsprechende Maßnahmen zu treffen oder umzusetzen.

Missbrauchspotenzial

Die in Abs. 2 eingeräumte Befugnis zur Umleitung von Datenverkehr ist nicht hinreichend spezifisch definiert. Die derzeitige Formulierung lässt es auch zu, Verkehr zu Servern umleiten zu lassen, die Informationen bereitstellen, die im weitesten Sinne den Schutzzielen zuwiderlaufen. Dabei wäre bei der derzeitigen Formulierung auch eine Zensur von Informationen rechtens, die nur im weitesten Sinne als schädlich für die definierten Schutzziele angesehen werden können.

Empfehlung: Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme müssen zumindest post-hoc durch ein unabhängiges Aufsichtsgremium geprüft werden.

Eingriff in die Vertraulichkeit und Integrität informationstechnischer Systeme

Die in § 7c Abs. 1 Satz 2 vorgeschlagene Befugnis zur Anordnung der Verbreitung *„technischer Befehle zur Bereinigung von einem konkret benannten Schadprogramm an betroffene informationstechnische Systeme"* ist vage und unzureichend definiert. Dieses Versäumnis ist von besonderer Schwere, da es sich um eine potenziell folgenschwere Ermächtigung zum Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[44] handelt.

Weder wird eindeutig geklärt, ob sich diese Befugnis auch auf Systeme von Kunden der betroffenen TK-Anbieterin, also hinter dem Router befindliche Computer,

[44] Wikipedia: Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Industrieanlagen, Krankenhaussysteme etc. erstreckt, noch wird definiert, welchen Beschränkungen diese „technischen Befehle“ unterliegen.

Dem Eingriff werden auch keine Qualitätsanforderungen zugrunde gelegt. Gleichzeitig bleibt die Haftung für eventuelle Schäden und Nebenwirkungen (z. B. Datenverlust oder Verlust der Verfügbarkeit von Systemen) ungeklärt.

Empfehlung: Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme müssen von eng definierten Voraussetzungen, ausführlicher Transparenz und streng eingegrenzten Zielen flankiert werden.

Die Befugnis verletzt den Verhältnismäßigkeitsgrundsatz, nach dem insbesondere bei Eingriffen in Grundrechte von möglichen Maßnahmen nur diejenige ergriffen darf, die die Betroffenen und die Allgemeinheit am wenigsten beeinträchtigt.

Empfehlung: Das Ergreifen von Maßnahmen geringerer Eingriffstiefe sollte zur Voraussetzung für einen derartigen Eingriff vorgeschrieben werden.

Wenn etwa die in Frage stehende „Schadsoftware“ nicht hinreichend gut verstanden wurde und beispielsweise verborgene Routinen zur Löschung oder Verschlüsselung von Daten des betroffenen Systems enthält, kann ein gegenüber der Ausgangssituation viel schwerwiegenderer Schaden entstehen.

Empfehlung: Die Haftungsfrage ist zu klären.

Von besonderer Schwere ist die fehlende Definition der Eigenschaften eines *„konkret benannten Schadprogramms“* zu dessen *„Bereinigung“* das BSI ermächtig werden soll: Insbesondere mit Hinblick auf die Paragraphen § 202a-c StGB würde mit § 7c ein willkürlicher Ermessenspielraum mit ausgiebigem Missbrauchspotenzial geschaffen.

Empfehlung: Der Begriff „Schadprogramm“ muss eng und konkret definiert werden, um das Missbrauchspotenzial einzugrenzen.

Mangelnde Transparenz

Der vorliegende Gesetzentwurf enthält keine Pflichten zur öffentlichen Dokumentation der eingesetzten *„technischen Befehle“*, des *„konkret benannten Schadprogramms“* oder

der betroffenen Systeme. Dadurch wird Betroffenen im Schadensfall ein Regress erheblich erschwert. Ebenso gibt es keine Möglichkeit nachzuvollziehen, ob die *„technischen Befehle“* nachvollziehbar dem proklamierten Zweck – und nur diesem – dienten.

Die Einbeziehung der Bundesnetzagentur und der Bundesbeauftragten für den Datenschutz und Informationsfreiheit ist keine ausreichende Absicherung gegen Kollateralschäden einer automatisierten Ausführung von *„technischen Befehlen“* durch das BSI auf potentiell Millionen betroffener Systeme.

Empfehlung: Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme müssen zumindest post-hoc durch ein unabhängiges Aufsichtsgremium geprüft werden. Das Aufsichtsgremium muss vollständigen Einblick in den Vorgang, sowie die Möglichkeit zur Sanktionierung haben.

Fazit

Die Zielsetzung, eine effektive Handlungsmöglichkeit zur zeitnahen Bekämpfung von weit verteilter Schadsoftware zu erlangen, ist nachvollziehbar. Die derzeitige vorgeschlagene Regelung ist jedoch unnötig unspezifisch und weist keine Regelung für Schadensfälle auf, die durch solche Eingriffe entstehen. Im Ergebnis bietet sie ein weit über den intendierten Anwendungszweck hinausgehendes Missbrauchspotenzial.

Grundsätzlich ist der Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme hochkritisch und sollte nur im eng definierten absoluten Ausnahmefall als Ultima Ratio zugelassen sein. Beschränkungen oder enge Voraussetzungen wie bspw. die Verpflichtung zur vorherigen Anwendung von Maßnahmen mit geringerer Eingriffstiefe finden sich jedoch nicht im vorliegenden Gesetzentwurf.

Insbesondere vor dem Hintergrund der nach aktuellen Gesetzesvorhaben verstärkten Einbindung des BSI in den Bereich der öffentlichen Sicherheit entsteht ein umfangreicher Vertrauensverlust. Dieser macht es zwingend erforderlich, derartige Eingriffsbefugnisse mit effektiven Hürden und Kontrollmechanismen zu versehen.

Definition “vertrauenswürdiger Anbieter” greift ins Leere (§ 9b)

Die Rolle chinesischer Netzwerkausrüstungsunternehmen wird weltweit seit 2018 emotional und von Fakten weitgehend unbelastet geführt. Wir möchten einleitend unmissverständlich klarstellen, dass diese Diskussion völlig lächerlich und fehlgeleitet ist. Sie ist ein herausragendes Beispiel für die Hilflosigkeit, Strategielosigkeit und Ahnungslosigkeit der bundesdeutschen IT-Sicherheitspolitik.

Wir äußern uns hierzu nur widerwillig und mit dem primären Ziel, diese Debatte auf eine sachliche Grundlage zu stellen.

Beweise liegen nicht vor

Einen humorvollen Höhepunkt erreichte die Diskussion im März 2019, als hochrangige US-Diplomaten der Bundesregierung mit der Einstellung der Geheimdienstkooperation drohten, sofern diese beim Aufbau eines 5G-Netzes Komponenten einer chinesischen Herstellerin zulasse.[45] Ungeachtet dessen, ob eine solche Kooperation überhaupt im Interesse der Bundesbürgerinnen ist, erscheint sie doch als relativ geschmackloses Druckmittel zur Durchsetzung handelspolitischer Interessen.

Ein Beweis für die mangelnde Vertrauenswürdigkeit der genannten Herstellerin wurde der interessierten Öffentlichkeit bisher nicht präsentiert – wenngleich Medienberichten zu entnehmen ist, dass die Bundesregierung spätestens seit Beginn 2020 über einen solchen Beweis verfügen soll.[46]

Vorliegende Beweise werden ignoriert

Bisher hat die Bundesregierung jedoch keinerlei Maßnahmen unternommen, um der Verwendung entsprechender Komponenten Einhalt zu gebieten. Der Öffentlichkeit bleibt indes unbekannt, ob die von den USA präsentierten Beweise nicht glaubwürdig sind, oder schlichtweg ignoriert werden. Letzteres kommt in Betracht, weil die Bundesregierung sogar bei Herstellerinnen, deren mangelnde Vertrauenswürdigkeit

---

[45] Der Spiegel: USA stellen wegen Huawei Geheimdienst-Kooperation infrage, abgerufen am 26. Februar 2021

[46] Handelsblatt: „Smoking gun“: Streit um Beweise gegen Huawei, abgerufen am 26. Februar 2021

öffentlich unwiderlegbar dokumentiert ist, keinen Anlass zum Handeln sieht: Die Aktivitäten der US-Geheimdienste in diesem Bereich sind seit Ende 2013 öffentlich ausführlich dokumentiert,[47] [48] ohne dass die Bundesregierung daraus Konsequenzen gezogen hätte. Der bekannteste mit Hilfe dieser Infrastruktur durchgeführte Angriff auf Mitgliedstaaten der Europäischen Union ist die Infiltration des Belgacom-Netzwerks, das unter anderem die Kommunikationsinfrastruktur für das EU-Parlament in Brüssel stellt.[49] Ungeachtet der tatsächlichen Bewertung der Vertraulichkeit einer spezifischen Herstellerin ist also festzuhalten, dass derartige Angriffe auf Kommunikationsinfrastruktur stattfinden.

Eine nicht vertrauenswürdige Herstellerin könnte hierbei zumindest theoretisch eine Unterstützung leisten. Für die Herstellerin hätte dies jedoch einen potenziell sehr hohen Preis: das Ende sämtlicher internationaler Handelsbeziehungen – sofern Regierungen oder Netzbetreiberinnen auf solche Angriffe Konsequenzen folgen lassen würden.

Um der Argumentation der Autorinnen des vorliegenden Gesetzentwurfs zu folgen, sei davon ausgegangen, dass eine nicht vertrauenswürdige Herstellerin zur Beeinträchtigung der IT-Sicherheit der Kommunikationsinfrastruktur der Bundesrepublik Deutschland verpflichtet sei.

Bugdoors

Statt offensichtlich als solche gedachte Backdoors in gelieferten Systemen zu verstecken, wäre eine nicht vertrauenswürdige Anbieterin besser beraten, die gelieferten Systeme mit schwer zu entdeckenden, komplexen Schwachstellen auszustatten: Im Fall einer Entdeckung könnten diese plausibel als unbeabsichtigte Sicherheitslücken behandelt und beseitigt werden, ohne dass Zweifel an der Vertrauenswürdigkeit der Anbieterin entstünden.

---

[47] Wikipedia: NSA ANT catalog

[48] Wikipedia: Tailored Access Operations

[49] Wikipedia: Operation Socialist

Um ausgewählten staatlichen Stellen ein Ausnutzen der absichtlichen Schwachstellen zu ermöglichen, würde die nicht vertrauenswürdige Anbieterin das Wissen über diese Schwachstellen und die Möglichkeit derer Ausnutzung heimlich weitergeben.

Realistische Angriffe richten sich gegen Vertraulichkeit

Eine nicht vertrauenswürdige Anbieterin könnte grundsätzlich Schwachstellen bereitstellen, die zur Beeinträchtigung der Verfügbarkeit, Integrität oder Vertraulichkeit eines Kommunikationsnetzes geeignet sein könnten. Hier lohnt es sich, die Konsequenzen einer Ausnutzung jeweils deren Nutzen gegenüber zu stellen.

1. **Verfügbarkeit:** Das Sabotieren einer Kommunikationsinfrastruktur wäre ein kriegerischer Akt, der aufgrund der hohen Abhängigkeit vom Kommunikationssystem unvorhersehbare Schäden zur Folge haben könnte. Der Vorfall würde unmittelbar bekannt und ließe sich mit großer Wahrscheinlichkeit sowohl nachweisen als auch attribuieren. Die ökonomischen Konsequenzen für die nicht vertrauenswürdige Herstellerin wären fatal.
2. **Integrität:** Die Beeinträchtigung der Integrität des Kommunikationsnetzes könnte beispielsweise im Umlenken von Verbindungen bestehen. Ein solches hoch dynamisches Vorgehen würde einen breitbandigen Zugang zum manipulierten Ziel-Netz voraussetzen. Die Netzwerkbetreiberin hätte jedoch gute Möglichkeiten, diese Zugriffe zu erkennen und zu unterbinden, da relevante Teile der kritischen Kommunikationsinfrastrukturen nicht ungehindert über das Internet administrativ erreichbar sind.
3. **Vertraulichkeit:** Die Schwächung eines Kommunikationsnetzes zum Zweck der Spionage bietet für Angreiferinnen langfristige Vorteile bei gleichzeitig geringer Entdeckungswahrscheinlichkeit. Würde beispielsweise die Verschlüsselung auf der Luftschnittstelle geschwächt, wäre das Abhören der Netzverbindungen für Eingeweihte mit einfachen Mitteln möglich, ohne dass netzwerkseitige Auffälligkeiten zur Entdeckung führen könnten.

Vor dem Hintergrund dieser einfach nachvollziehbaren Überlegungen scheint es am wahrscheinlichsten, dass durch eine nicht vertrauenswürdige Anbieterin absichtlich platzierte Schwachstellen zum Zweck der *Vertraulichkeitsverletzung* ausgenutzt würden.

Insbesondere ist hierbei festzuhalten, dass mit der geplanten Novelle des BND-Gesetzes der Auslandsgeheimdienst der Bundesrepublik spezifisch zu solchen Angriffen ermächtigt werden soll. Die geplanten Angriffe sollen dabei ausschließlich die *Vertraulichkeit* der Kommunikationsnetze, *nicht* jedoch deren Verfügbarkeit oder Integrität beeinträchtigen.

Dieses wahrscheinlichste Angriffsszenario wird jedoch durch den vorliegenden Gesetzesvorschlag explizit ignoriert, indem nur *Verfügbarkeit und Integrität* als Schutzziele genannt werden, und die Vertraulichkeit im Gegensatz zu allen anderen Stellen im Gesetzestext, die die Schutzziele der Informationssicherheit behandeln, *ausgeklammert wird*. § 9b Abs. 5 Nr. 5 besagt:

> *Ein Hersteller einer kritischen Komponente ist nicht vertrauenswürdig, wenn […] 5. die kritische Komponente über technische Eigenschaften verfügt oder verfügt hat, die geeignet sind oder waren, missbräuchlich auf die* ***Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit*** *der Kritischen Infrastruktur einwirken zu können.*

Der aufmerksamen Leserin ist sicherlich nicht entgangen, dass ausgerechnet das Schutzziel der Vertraulichkeit in dieser Auflistung überraschenderweise fehlt.

Empfehlung: Die Schutzziele der Informationssicherheit sind Verfügbarkeit, Integrität und *Vertraulichkeit*.[50]

[50] wikipedia.org: Informationssicherheit

Empfehlung: Die Definition „vertrauenswürdiger Anbieterinnen" muss sich nicht auf die Herkunft der Anbieterin, sondern auf die tatsächliche und prüfbare technische Sicherheit und Sicherbarkeit ihrer Produkte erstrecken.

Alle Anbieterinnen von Komponenten kritischer Infrastruktur – unabhängig von ihrem Herkunftsland – sollten nur zulässig sein, wenn sichergestellt ist, dass das tatsächlich im Einsatz befindliche System auditiert werden kann. Entsprechende Auditierungen sollten regelmäßig stattfinden.

Die technischen Voraussetzungen (Reproducible Builds, Bereitstellung von unabhängigen Audit-Ressourcen entsprechend dem Update-Tempo, Nachweis von „Best Practices" für Mitigation in Architektur, Coding-Praxis, Build-Prozess etc.) sollten in die Anforderungen für alle Anbieterinnen aufgenommen werden.

Empfehlung: Damit es für diese Prozesse der Überprüfung vertrauenswürdig ist, darf das BSI nicht zum Dienstleister für Behörden werden, die Sicherheitslücken im Rahmen ihrer Tätigkeit zu benötigen glauben, verheimlichen und ausnutzen (BND, BfS, MAD, BKA, LKAs), da sich hierdurch ein nicht glaubwürdig auflösbarer Interessenskonflikt ergibt:

Das BSI muss ein striktes Mandat zur schnellstmöglichen Behebung aller ihm egal auf welchem Wege bekanntwerdenden Sicherheitslücken bekommen, für das keine Ausnahmen zugelassen sind.

Integration von Netzwerkomponenten

Würde eine nicht vertrauenswürdige Herstellerin zur Beihilfe bei der Beeinträchtigung der Verfügbarkeit oder Integrität von Kommunikationsnetzen verpflichtet, so ist es aus den oben genannten Gründen unwahrscheinlich, dass die Beeinträchtigung über das Internet per Mausklick auf einen großen roten Knopf ausgelöst werden könnte. Insbesondere ist dies unwahrscheinlich, weil die Komponenten in nicht öffentlich zugänglichen Netzen administriert werden.

Tatsache ist aber, dass Zulieferinnen und Dienstleisterinnen im Rahmen ihrer Tätigkeit detaillierte Kenntnis von Netzwerkarchitektur, Zugangsvoraussetzungen und Sicherheitssystemen der Kommunikationsnetze erlangen, in denen ihre Produkte eingesetzt werden. Dieses Wissen erstreckt sich auch über die Komponenten anderer Anbieterinnen im *vendor mix:* Aus naheliegenden Gründen kommt in Kommunikationsnetzen zur Vermeidung einseitiger Abhängigkeiten eine Mischung von Komponenten unterschiedlicher Hersteller zum Einsatz.

Tatsächliche Trägerinnen von sicherheitsrelevantem Wissen sind daher weniger die internationalen Produzentinnen, sondern die in Deutschland ansässigen Unternehmen, die entsprechender Jurisdiktion unterliegen.

Empfehlung: Zusätzlich zu fortlaufenden, vollständigen Sicherheits-Audits aller Netzwerk-Komponenten sollten Betreiberinnen von TK-Netzen verpflichtet werden, innerhalb ihrer Netze Systeme zur Detektion von Anomalien in der Kommunikation zwischen den verwendeten Komponenten zu betreiben. Diese sollten geeignet sein, Anzeichen für Kompromittierung durch Angreiferinnen oder eine Ausnutzung von Back- und Bugdoors zu detektieren. Auf diese Weise lassen sich unabhängig vom Herkunftsland der Herstellerinnen Angriffe und Anomalien im Betrieb erkennen.

Technologische Souveränität

Schon heute sind europäische Netzwerkkomponenten nicht in der Lage, mit chinesischen Produkten zu konkurrieren: Chinesische Anbieterinnen liefern inzwischen technisch überlegenes Equipment zu günstigeren Preisen. Es ist daher leicht nachvollziehbar, dass deutsche und europäische Mobilfunknetze zu großen Teilen mit chinesischer statt europäischer Technik ausgerüstet werden.

Unabhängig von der Frage der Vertrauenswürdigkeit der Anbieterinnen ist es im Interesse der Bundesrepublik und der Europäischen Union, die europäische Technik konkurrenzfähig im Markt zu halten. Beim Bau von Mobilfunknetzen der sechsten oder siebten Generation droht sonst eine Situation, in der europäische Ausrüster nicht mehr Teil des Angebots sind.

Um dem entgegenzuwirken, bieten sich jedoch etablierte und “ehrliche” Mittel der Marktverzerrung wie Förderungen, Subventionen und Zölle an. Es bedarf nicht eigens

des Arguments von einer in der IT-Sicherheit konzeptuell fremden "Vertrauenswürdigkeit."

Konsequenzen für Betreiberinnen

Würde eine massenhaft eingesetzte Herstellerin plötzlich als "nicht vertrauenswürdig" erkannt, wäre ein Rückbau bzw. Ersatz der verbauten Infrastruktur die zwingend logische Konsequenz.

Dieser Rückbau ginge jedoch mit erheblichen Einschränkungen und finanziellen Belastungen einher – sofern überhaupt Alternativen verfügbar sind.

Hierbei ist insbesondere zu berücksichtigen, dass schon heute deutsche Mobilfunknetze der dritten und vierten Generation zu überwiegenden Teilen aus Hardware zweier von der Bundesregierung potenziell als "nicht vertrauenswürdig" beurteilter Herstellerinnen bestehen.

Fazit

Das Konzept der *"nicht vertrauenswürdigen Anbieter"* verfehlt sein Schutzziel. Wenn der Bundesregierung Beweise für die mangelnde Vertrauenswürdigkeit einer Herstellerin vorliegen, so möge sie diese der Öffentlichkeit präsentieren und daraus Konsequenzen ziehen.

Empfehlung: Wenn es der Bundesregierung daran gelegen ist, die technologische Souveränität im Bereich des Mobilfunks aufrecht zu erhalten, dann möge sie mit Förderprogrammen die mangelnde Konkurrenzfähigkeit europäischer Herstellerinnen kompensieren. Hierzu bieten sich breit angelegte Programme zur Förderung von kritischen Software-Stacks als Open-Source an, für die im Rahmen der Förderung auch die Ressourcen für sichere Architekturen und fortlaufende Auditierung bereitgestellt werden.

Ressourcenverschwendung durch „IT-Sicherheitskennzeichen“ (§ 9c)

Besonders offiziell erscheinende IT-Sicherheitskennzeichen wünschen sich insbesondere deutsche Herstellerinnen schon seit längerem, um damit die höheren Preise ihrer Produkte zu rechtfertigen.

Wirtschaftsförderungsmaßnahme ohne Realweltkonsequenzen

Solange mangelhafte Konkurrenzprodukte ihren Preisvorteil durch geringe Investition und Nachsorge im Bereich der IT-Sicherheit ungehindert ausspielen können, ist allerdings nicht mit einer effektiven und nachhaltigen Erhöhung der bundesdeutschen IT-Sicherheit zu rechnen.

Die Konsequenzen gehen dabei nicht immer nur zulasten von Kundinnen der unsichereren Produkte: In Botnetzen zusammengeschlossene IoT-Geräte werden in der Regel weniger gegen ihre Eigentümerinnen als vielmehr gegen unbeteiligte Dritte eingesetzt. Die reine Existenz eines unsicheren Produkts in ausreichender Menge kann so zu Bedrohung für die nationale und internationale IT-Sicherheit werden.

Vor diesem Hintergrund auf freiwillige Sicherheitskennzeichen zu setzen, lässt ähnlich durchschlagenden Erfolg erwarten, wie bei der Eindämmung einer Pandemie auf Eigenverantwortung der Bürgerinnen zu hoffen: Es wäre wirklich zu schön, scheitert aber an der Realität.

Fehlende Überprüfung

Herstellerinnen sollen ihre Produkte durch Selbstzertifizierung ohne unabhängige Prüfung mit dem IT-Sicherheitskennzeichen des BSI schmücken dürfen. Dafür werden laut Gesetzentwurf für den Aufwand des BSI veranschlagt:

> *25 zusätzliche Planstellen/Stellen (17 hD; 8 gD) mit Personalkosten in Höhe von jährlich 2,33 Mio. Euro sowie Sacheinzelkosten in Höhe von 0,62 Mio. Euro jährlich.*

Empfehlung: Die 25 Planstellen sollten stattdessen einer zielgerichteten Aufgabe zugeführt werden, die auf eine tatsächliche Erhöhung der IT-Sicherheit ausgerichtet ist und so den Angestellten inhaltliche Erfüllung und eine berufliche Perspektive bieten kann.

Alternativen

Der CCC empfiehlt bei jeder sich bietenden Gelegenheit die Einführung einer Produkthaftung im Bereich der IT-Sicherheit zur Aktivierung der Selbstheilungskräfte der Herstellerinnen untauglicher Produkte sowie einen Update-Zwang bzw. ein "Mindesthaltbarkeitsdatum" als Markteintrittsvoraussetzung.[51][52]

Haftung

In vielen Bereichen des Verbraucherschutzes hat sich die Produkthaftung als erfolgreiches Mittel erwiesen, Herstellerinnen zu einer effizienten und zielgerichteten Qualitätssicherung zu motivieren.

Eine entsprechende Haftung für Software-Produkte und Ansätze, auch für Open-Source-Software eine sinnvolle Lösung zu finden, hat der CCC bereit in einer früheren Stellungnahme erörtert[53] und zuletzt in einer Stellungnahme zum *Gesetzentwurf zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen Entwürfe zur Umsetzung der Richtlinie über digitale Inhalte und zu den vertraglichen Regelungen der Modernisierungsrichtlinie* eingebracht.[54]

Empfehlung: Der Chaos Computer Club rät zur Ausweitung der Produkthaftung auf den Bereich der IT-Sicherheit. Die Haftung sollte dann greifen, wenn die Herstellerin innerhalb eines angemessenen Zeitraums keine Abhilfe für bekannte IT-Sicherheitsmängel ihres Produkts geleistet hat.

---

[51] ccc.de: Stellungnahme des CCC zu Fragen der IT-Sicherheit in der Post-Snowden-Ära

[52] ccc.de: Update nicht verfügbar: Lieferant nicht zu erreichen

[53] ccc.de: Stellungnahme des CCC zu Fragen der IT-Sicherheit in der Post-Snowden-Ära

[54] bmjv.de: Chaos Computer Club: Anmerkungen und Ergänzungen zum Entwurf zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, abgerufen am 26. Februar 2021

Updatezwang bzw. Mindesthaltbarkeitsdatum

Da IT-Sicherheit kein Zustand, sondern ein Prozess ist, kann diese durch Herstellerinnen nur glaubhaft und nachhaltig gewährleistet werden, wenn eine entsprechende Nachsorge betrieben wird: Wird ein Produkt oder eine Software-Lösung von der Herstellerin nicht mehr mit Updates versehen, wird die weitere Verwendung zum potenziell fahrlässigen Risiko.

Auch technisch einwandfreie Produkte können auf diese Weise zu teurem Elektroschrott oder Risiken für die nationale Sicherheit werden. Es ist daher unersichtlich, dass das Einsparen der unverzichtbaren Produktnachsorge weiterhin zum Marktvorteil gereicht.

Empfehlung: Der Chaos Computer Club rät zur Einführung eines "Mindesthaltbarkeitsdatums" hinsichtlich der IT-Sicherheit von Software und Geräten. Bis zum Ablauf des Mindesthaltbarkeitsdatums muss die Herstellerin verpflichtet sein, Sicherheitsupdates für das entsprechende Produkt bereitzustellen. Stellt die Herstellerin den Geschäftsbetrieb ein, oder die Nachsorge für ein Produkt vor Ablauf des Mindesthaltbarkeitsdatums ab, muss sie zur öffentlichen Bereitstellung des Quellcodes verpflichtet sein, um unabhängige Nachsorge zu ermöglichen.

Falscher Fokus auf "Unternehmen im besonderen öffentlichen Interesse"

Mit dem vorliegenden Gesetzentwurf soll das BSI auch Zuständigkeit für Unternehmen in besonderem öffentlichem Interesse erhalten. Als diese sollen Unternehmen gelten, die nicht unter die kritischen Infrastrukturen fallen, jedoch

a) Güter im Bereich der Kriegswaffen oder Produkte mit IT-Sicherheitsfunktionen zur Verarbeitung von staatlichen Verschlusssachen herstellen,

b) nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören, oder

c) Gefahrenstoffe in großen Mengen an ihren Betriebsstätten vorhalten.

Während die Kriterien a) und c) grundsätzlich zumindest nachvollziehbar sind, erscheinen die Ressourcen des BSI bei den größten Unternehmen Deutschlands fehlinvestiert: Mängel und Unvermögen im Bereich der IT-Sicherheit sind vor allem in

kleineren Unternehmen prävalent, denen die Ressourcen und Verantwortlichkeiten für eine zeitgemäße IT-Sicherheit fehlen.

Während große Unternehmen individuelle, fähige und reife IT-Sicherheitsinfrastrukturen zu unterhalten in der Lage sind oder sein sollten, bleiben die gebetsmühlenartig gelobten “Hidden Champions”, die den deutschen Mittelstand und das Herz der deutschen Wirtschaft ausmachen sollen, vom Gesetzentwurf weiterhin unbeachtet.

Für kleine und mittelständische Unternehmen (KMU) hält der Gesetzentwurf die IT-Sicherheitskennzeichen bereit, die Herstellerinnen sich ohne unabhängige Prüfung selbst ausstellen können. Hier ist kein nennenswerter Effekt zu erwarten. Das ist tragisch, weil sich insbesondere bei den vielen KMU die Verwundbarkeit der Deutschen Wirtschaft offenbart und potenziert.

Empfehlung: Der Bundestag möge prüfen, welche Unternehmen im besonderen öffentlichen Interesse der Bundesrepublik liegen und welche davon tatsächlich besondere Aufmerksamkeit des BSI benötigen.

Empfehlung: Zum Schutz der KMU rät der CCC zur Förderung und Bereitstellung einer auf kompromisslose IT-Sicherheit ausgelegten Infrastruktur, zur Einführung einer Produkthaftung sowie zur Einführung eines Mindesthaltbarkeitsdatums.

Abschließende Bemerkungen

Der vorliegende Gesetzentwurf wird seit über zwei Jahren in unterschiedlichsten Varianten – meist unter Ausschluss der Öffentlichkeit – diskutiert. Von einigen besonders schlechten Ideen früherer Entwürfe wurde in der Zwischenzeit Abstand genommen.

Die Bemühungen des BMI, eine öffentliche Diskussion und zivilgesellschaftliche Beteiligung zu verhindern, haben dabei insgesamt eine neue Qualität erreicht. Höhepunkt dieser Bemühungen war das Einräumen einer Frist von 28 Stunden zur Kommentierung eines um 16 Seiten erweiterten Referentinnenentwurfs für ein zweites IT-Sicherheitsgesetz.

Der Chaos Computer Club hat dieses Vorgehen öffentlich streng kritisiert[55] und gehört zu den Unterzeichnerinnen eines offenen Briefes,[56] in dem eine Vielzahl digitalpolitischer Organisationen *„Angemessene Fristen statt Scheinbeteiligung"* fordert.

Unerlässlich sind hierbei:

1. Angemessene Fristen für die Kommentierung von Gesetzesentwürfen,
2. Bereitstellung von Synopsen zur besseren Vergleich- und Nachvollziehbarkeit,
3. Veröffentlichung der Referentenentwürfe auf den Webseiten der Ministerien und
4. eine Öffnung des Partizipationsprozesses

Empfehlung: Um ein drittes *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme* in angemessener Qualität vorschlagen zu können, sollte das BMI seine Bemühungen zur aktiven Unterdrückung sachverständigen Rats einstellen.

[55] ccc.de: Innenministerium sabotiert sachkundige Diskussion zum IT-Sicherheitsgesetz 2.0

[56] ccc.de: Offener Brief an die Bundesregierung: Angemessene Fristen statt Scheinbeteiligung