Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)741 C

AG KRITIS

Stellungnahme für die Anhörung des Bundestagsausschusses für Inneres und Heimat

Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit Informationstechnischer Systeme 2.0 (IT-Sicherheitsgesetz 2.0)

am 01.03.2021

Manuel Atug

Gründer und Sprecher der unabhängigen AG KRITIS

Der Sachverständige dankt allen ehrenamtlich tätigen Expert:innen der AG KRITIS und den vielen Sicherheitsforscher:innen aus der Community für ihre Unterstützung.

Kontakt

Manuel Atug

E-Mail: HonkHase@ag.kritis.info

Twitter: @HonkHase

Webseite: https://ag.kritis.info

Inhalt

Vorbemerkungen zum bisherigen Verfahrensablauf

Über zwei Jahre hat das BMI hinter verschlossenen Türen vor sich hin gewerkelt und mit Referaten anderer Ministerien zu überaus umfangreichen Befugniserweiterungen verhandelt, so dass die Verhandlungsbasis eine überdimensioniert schwierige Ausgangsbasis dargestellt hat. Im ersten Quartal 2019[1] und im zweiten Quartal 2020[2] ist jeweils ein Referentenentwurf vorab geleaked worden, da eine Beteiligung der Wissenschaft, Wirtschaft, Zivilgesellschaft und Sicherheitsforscher:innen in diesem Zeitraum trotz derer wiederholten Bitten weder vorgesehen noch berücksichtigt wurde.

Diese Leaks war in den zwei Jahren somit leider der einzige Weg, dass auch Wissenschaft, Wirtschaft, Zivilgesellschaft und Sicherheitsforscher:innen sich frühzeitig einlesen und eigene Gedanken zum kommenden IT-SiG 2.0 machen können. Ein aktives einbringen war dabei zu den Zeitpunkten ebenfalls weder möglich noch vorgesehen.

Das BMI hat erst am 9.12.2020[3] erstmalig eine öffentlich verfügbare Verbändefassung auf ihrer Webseite bereitgestellt, um Betroffenen, Interessierten und fachkundigen Dritten die Beteiligung durch initiale Einsichtnahme zu ermöglichen.

Als das Verfahren diesen offiziellen Charakter angenommen hatte, ging es dann plötzlich Schlag auf Schlag. Von 19.11.2020 bis 16.12.2020 alleine gab es fünf veröffentlichte Versionen mit teils umfangreicheren Anpassungen[4], die aber in Teilen wiederum nur einigen beteiligten Wirtschaftsverbänden bereitgestellt wurden. Hierbei wurden an einigen Stellen betroffene Verbände nicht berücksichtigt, so dass diese in ihrer Stellungnahme darauf verwiesen hatten, dass sie eigeninitiativ reagieren mussten und daher nicht die angemessene Zeit erhalten hatten, um eine vollständige Analyse und Kommentierung vorzunehmen.

Dabei wurden grundsätzlich alle neuen Versionen des Gesetzesentwurfs lediglich als nicht editierbares PDF-Dokument ohne Hervorhebung von Änderungen bereitgestellt. Eine Synopse mit einfachem aufzeigen oder transparent erfolgtem Abgleich der Veränderungen wurde zu keinem Zeitpunkt ermöglicht.

Dies kam insbesondere bei der letzten Änderung zur Wirkung[5], so dass Stellungnahmen nicht mehr angepasst werden konnten, denn der Zeitraum zwischen Bereitstellung der überarbeiteten Version mit über 100 Seiten Text an Gesetzesentwurf und Fristablauf zur Einreichung der Stellungnahme hatte zuletzt dann auch nur noch unverschämte 26 Stunden Reaktionszeit beinhaltet.

Die AG KRITIS stellte hierzu bereits berechtigt fest: ***Eine so kurze Frist ist der ministerielle Mittelfinger ins Gesicht der Zivilgesellschaft!***[6]

Trotz dieser umfangreichen Widrigkeiten zur aktiven Verhinderung einer Beteiligung an diesem zukunftsweisenden Gesetz im Kontext der Cybersicherheit und digitalen Souveränität Deutschlands haben insgesamt 24 Stellungnahmen aus der privaten Wirtschaft sowie aus den

---

[1] https://ag.kritis.info/wp-content/uploads/2020/12/20190327-IT-Sicherheitsgesetz-2.0.pdf
[2] https://ag.kritis.info/wp-content/uploads/2020/12/20200507-IT-Sicherheitsgesetz-2.0.pdf
[3] https://ag.kritis.info/wp-content/uploads/2020/12/20201209-IT-Sicherheitsgesetz-2.0.pdf
[4] https://ag.kritis.info/2021/02/22/it-sicherheitsgesetz-2-0-alle-verfuegbaren-versionen/
[5] https://ag.kritis.info/wp-content/uploads/2020/12/20201211-IT-Sicherheitsgesetz-2.0.pdf
[6] https://ag.kritis.info/2020/12/09/it-sicherheitsgesetz-2-0-vierter-entwurf-jetzt-vom-bmi-nur-noch-24h-zeit-zur-kommentierung/

zivilgesellschaftlichen und sonstigen Organisationen das BMI erreicht.[7] Bedarf zur Beteiligung ist also offensichtlich umfassend vorhanden, nur hebt das BMI dieses Potenzial nicht, sondern lässt es brach liegen.

Diese umfassende Beteiligung macht aber die Bedeutung und Kritikalität des Gesetzes mehr als deutlich und das Versagen bei der effektiven Ermöglichung einer Beteiligung umso schwerwiegender. Ganz abgesehen davon, dass das BMI hier noch viel umfassendere Fachexpertise aus verschiedenen Blickwinkeln hätte frei Haus erhalten können.

So - und nur so - kann im Übrigen ein Stand der Technik[8], welcher schon im IT-SiG 1.0 verankert ist, erreicht werden.

Qualität der Strategie und der Ziele im IT-SiG 2.0

Das IT-SiG 2.0 zeigt unter anderem auch und insbesondere aufgrund dieser Vorgehensweise eine **eklatante Strategie- und Ziellosigkeit** des Gesetzgebers im Cyberraum auf.

Deutlich wird dabei auch an vielen Stellen der Konflikt der „Sicherheit“ aus Sicht der Sicherheitsbehörden und Nachrichtendienste im Kontext der Befugniserweiterungen und der Gefahrenabwehr auf der einen Seite. Und auf der anderen Seite „Sicherheit“ im Kontext der Erhöhung der Cyberresilienz aus KRITIS-Sicht, also der Sicht der robusten und widerstandsfähigen Versorgung der Zivilbevölkerung. Die im Übrigen auch genau deswegen in dieser Form im IT-SiG 1.0 in § 2 Abs. 10 BSIG[9] eingebracht wurde:

„Kritische Infrastrukturen im Sinne dieses Gesetzes sind […] von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.“

Untermauert wird diese beschriebene eklatante Strategie- und Ziellosigkeit darüber hinaus auch noch durch die immer noch ausstehende - gesetzlich vorgeschriebene[10] - Evaluierung der Wirksamkeit des IT-SiG 1.0. Ein IT-SiG 2.0 einzuführen, ohne das IT-SiG 1.0 analysiert zu haben und den daraus resultierenden Erkenntnisgewinn als Feedback einzubringen, zeugt von einer grundsätzlichen und prozessbedingten verminderten Qualität durch Kardinalsfehler im Prozessablauf.

Der vorgelegte Gesetzesentwurf lässt daher keine klare Linie zur konsequenten Erhöhung des Sicherheitsniveaus der IT-Systeme und Kritischen Infrastrukturen erkennen. Im gesamten Gesetzestext ist keine Strategie erkennbar, grundlegende Sicherheitsanforderungen zu stärken.

Vielmehr scheint es sich um eine bunte Mischung - teilweise sachfremder - Wünsche seitens einzelner Behörden zu handeln. Grundlegende Maßnahmen, die sinnvoll wären, wie die eindeutige

---

[7] https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/entwurf-zweites-it-sicherheitsgesetz.html

[8] https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/RechtsdurchsetzungUndBuerokratieabbau/HandbuchDerRechtsfoermlichkeit_deu.pdf?__blob=publicationFile&v=2

[9] https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html

[10] https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%255B@attr_id=%27bgbl115s1324.pdf%27%255D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1614244823027

und klarstellende verpflichtende Einführung eines Informationssicherheitsmanagementsystems (ISMS) mit Business Continuity Management (BCM) sind weiterhin nicht explizit erwähnt. Gute Ideen aus vorherigen Referentenentwürfen fehlen ganz, dafür wurden mehrere verfassungsrechtlich höchst fragliche Passagen hinzugefügt.

Das IT-SiG 2.0 droht insofern eine Sammlung von unabgestimmten und insbesondere ineffektiven Maßnahmen mit zahlreichen Redundanzen und Mehrfachregulierungen zu werden, die in Teilen keinen Sinn ergeben und keine klare Zielrichtung vorgeben. Es ist daher zu erwarten, dass dies darüber hinaus sogar Verwirrung stiften und Unklarheit fördern wird. So wird die geplante mehrspurige Autobahn zu einer Motocross Strecke wo jeder querfeldein agiert.

Aus Sicht der AG KRITIS kommt darüber hinaus die Kernidee des Schutzes kritischer Infrastrukturen (KRITIS) angesichts der Tatsache, dass KRITIS im IT-SiG 1.0 im Vordergrund standen, viel zu kurz. Was bedenklich stimmt ob der vermeintlichen und tatsächlichen Ziele des IT-SiG 2.0.

In Teilen wird dadurch sogar die Sicherheit gemindert, statt sie zu erhöhen. Das kann und darf kein Ergebnis dieses Prozesses und des daraus resultierenden Gesetzes sein!

Harmonisierung mit der EU

Im Übrigen ist im Entwurf eine EU Sicht und Angleichung oder Harmonisierung ebenfalls nicht als Strategie erkennbar.

Beispielsweise gibt es den deutschen Alleingang in § 9c BSIG „Freiwilliges IT-Sicherheitskennzeichen“ zusätzlich zur EU CSA Umsetzung in § 9a BSIG „Nationale Behörde für die Cybersicherheits-zertifizierung“.

Auch „Unternehmen im besonderen öffentlichen Interesse“ (UNBÖFI) stellen eine neue Kategorie parallel zu KRITIS dar, welche die EU ebenfalls weder in der EU NiS-Richtlinie[11] vorsieht noch auf sonstige Weise kennt oder vorsieht.

Dreigespann an Kritikalität

Offenbar sieht das IT-SiG 2.0 eine nicht sehr sinnvolle aber dafür verdeckte Dreiteilung von Schutzkategorien im Cyberraum Deutschlands vor:

1. **Besonders Kritisch**
   Hierbei handelt es sich um KRITIS Betreiber mit kritischen Komponenten gemäß § 9b BSIG
2. **Kritisch**
   Hierbei handelt es sich um KRITIS Betreiber nach § 2 Abs. 10 BSIG
3. **Leicht kritisch**
   Dies sind UNBÖFI nach § 2 Abs. 14, im umgänglichen Sprachgebrauch auch oft als „KRITIS light“ bezeichnet

[11] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016L1148

Die Sinnhaftigkeit hieraus erschließt sich nicht, denn der Schutzbedarf und ein daraus abgeleiteter Umfang von Maßnahmen ergibt sich aus der in § 8a BSIG vorgesehenen Methodik zur Umsetzung: *„angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen“*, sprich der eigentlich klassischen Umsetzung eines ISMS mit BCM nach Stand der Technik, die aber so explizit nicht in den Gesetzestext hineinformuliert wurde.

UNBÖFI einschließlich Rüstungsindustrie

Das IT-SiG 2.0 soll in § 2 Abs. 14 BSIG um drei verschiedenen Arten von Unternehmen erweitert werden, die nicht KRITIS Betreiber sind:

> *„1. die Güter nach § 60 Absatz 1 Nummer 1 und 3 der Außenwirtschaftsverordnung in der jeweils geltenden Fassung herstellen oder entwickeln,*
>
> *2. die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind oder*
>
> *3. die Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung in der jeweils geltenden Fassung sind oder nach § 1 Absatz 2 der Störfall-Verordnung diesen gleichgestellt sind.“*

Unter die Definition *„die Güter nach § 60 Absatz 1 Nummer 1 und 3 der Außenwirtschaftsverordnung“* fällt unter anderem auch die deutsche Rüstungsindustrie.

Die deutsche Rüstungsindustrie wird hier allerdings politisch strategisch mit dem Schutz der Zivilbevölkerung in Deutschland vermengt. Sie ist daher in anderen Gesetzen zu berücksichtigen und sollte aus der Sicht der nationalen Sicherheit adressiert werden und unter dem Kontext angemessene Berücksichtigung finden. Aber keinesfalls im Kontext des Zivilschutzes und der zivilen Fragestellungen und nur nach UNBÖFI-Vorgaben, die für diese Kritikalität viel zu unzureichend ausgestaltet sind.

UNBÖFI ist allerdings auch insgesamt als nichts Ganzes und nichts Halbes zu betrachten. Abgesehen davon, dass die militärnahe Rüstungsindustrie in Zivilgesetzen Einzug erhält und in unangemessener Weise Berücksichtigung finden soll, wird durch die Hintertür eine Art „KRITIS light“ eingeführt.

Was dieses „KRITIS light“ dabei genau sein soll und nach welchen genauen Kriterien ein Unternehmen UNBÖFI wird, ist nicht im Gesetz abgedeckt, sondern soll durch eine noch unbekannte Rechtsverordnung festgelegt werden. Diese ist allerdings nicht einmal im Entwurf öffentlich verfügbar. So wird es auch hier wieder ein intransparentes Verfahren. Und dann eben hoffentlich auch eine Verordnung, die auch ohne den Einbezug von Fachexpertise der Wissenschaft, Wirtschaft, Zivilgesellschaft und Sicherheitsforscher:innen in der ersten gültigen Fassung gut wird.

Unter die Definition *„Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung“* fallen unter anderem auch deutsche Unternehmen nach Störfall-Verordnung wie z. B. Chemieunternehmen. Aber auch Heizöl-Tanklager oder Raffinieren - die zwar als KRITIS erfasst sind, wenn sie über dem aktuellen Schwellenwert der BSI-Kritisverordnung[12] liegen, aber nicht, wenn sie darunter liegen.

Diese müssen dann allerdings - entgegen der KRITIS Betreiber - nur Teile der Maßnahmen und Vorgaben abdecken, da sie nicht als KRITIS sondern lediglich als UNBÖFI eingestuft werden.

Folgende Frage drängt sich daher naturgemäß auf: Wieso können Störfall-Verordnung relevante Unternehmen eigentlich UNBÖFI statt KRITIS sein?

Aus dem Schutz vor Gefahren einer Anlage ausgehend sollte auch Gefahr als KRITIS relevant angesehen werden. Verpflichtungen für Unternehmen nach Störfall-Verordnung müssten daher gleichwertig sein wie bei KRITIS Betreibern und diese dann damit eben nicht nur als UNBÖFI sondern immer als KRITIS eingestuft werden.

Dies bedeutet, dass diese Unternehmen daher nicht als KRITIS Betreiber berücksichtigt oder die Anforderungen gleichgesetzt wie bei KRITIS werden, da dann die gleichen angemessenen Anforderungen an deren IT-Sicherheit fällig werden.

Wenn diese Unternehmen aus dem Schutzbedarf so relevant sind, dass es eine Störfall-Verordnung gibt, wieso findet dann die IT Sicherheit nicht angemessene Berücksichtigung?

Die Berücksichtigung von unter die Störfall-Verordnung fallenden Unternehmen als UNBÖFI greift daher viel zu kurz. Denn diese Unternehmen stellen durch die Verarbeitung eine große Gefahr für die Zivilbevölkerung dar, daher sind für unter die Störfall-Verordnung fallenden Unternehmen nach § 8f BSIG auch die Anforderungen von § 8a BSIG vorzugeben.

Zurückhalten von Schwachstellen

Nach § 7b Abs. 3 BSIG sind die für den Betrieb eines IT-Systems verantwortlichen über die bei einem Scan des BSI gefundenen Sicherheitslücken bzw. Sicherheitsrisiken nur dann zu informieren, wenn „überwiegende Sicherheitsinteressen“ dem nicht entgegenstehen. Dies legt erneut den Verdacht nahe, dass es für das BSI als eine dem BMI unterstellte Behörde, Interessenkonflikte gibt. Diese Regelung schafft keinen rechtlichen Rahmen für den verantwortungsvollen Umgang mit Sicherheitslücken.

Als IT-Sicherheitsbehörde sollte das BSI sowohl Betreiber unsicherer Systeme als auch Hersteller von IT-Produkten immer über alle gefundenen Schwachstellen und Sicherheitslücken gemäß Responsible Disclosure Verfahren informieren. So sind diese in der Lage, mitigierende Maßnahmen einzuleiten und den Schutz der IT-Systeme aufrecht halten. Dies stellt eine konkrete Erhöhung der IT-Sicherheit dar.

Es ist aus dem Gesetzentwurf auch nicht ersichtlich, welche „überwiegenden Sicherheitsinteressen“ dem entgegenstehen sollten.

Da unsichere IT-Systeme nicht nur für Betreiber und Kunden - also die Zivilgesellschaft und die Wirtschaft - eine Gefahr darstellen, sondern auch von Angreifern für Attacken auf weitere Dritte

[12] https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html

dienen können, müssen diese Unsicherheiten bedingungslos und konsequent abgestellt werden. Auch darum sind Betreiber der Systeme immer und über jeden möglichen Kanal gemäß Responsible Disclosure Verfahren zu informieren.

Der Gesetzentwurf legt nahe, dass dies das alleinige Ziel von § 7b BSIG ist.

Das BSI soll allerdings darüber hinaus durch Art. 10 GG geschützte Informationen ausschließlich zum Zwecke der Übermittlung nach § 5 Abs. 5 und 6 BSIG - also zur Weitergabe an die Polizeien und Nachrichtendienste - verwenden dürfen. Im Vordergrund darf aber nicht die Anreicherung von sensitiven Datenbergen (Stichwort Vorratsdatenspeicherung) bei Polizeien und Nachrichtendiensten stehen.

Hier ist selbstverständlich die Beseitigung von Sicherheitslücken vorrangig. Der entsprechende Satz ist daher ersatzlos zu streichen. Im darauffolgenden Satz ist weiterhin klarzustellen, dass die Art. 10 GG-Informationen (wie z.B. IP-Adressen) ausschließlich zur Warnung der Betroffenen verwendet werden dürfen und anschließend sofort vom BSI unwiederbringlich zu löschen sind.

Generell wird festgestellt, dass der Gesetzentwurf erstaunlich oft auf die Regelungen zur Weitergabe von Informationen über Schwachstellen und Sicherheitsprobleme an Polizeien und Nachrichtendiensten nach § 5 Abs. 5 und 6 BSIG verweist. So sollen an diese nach § 4b Abs. 2 BSIG auch Informationen über die Identität von Meldenden weitergegeben werden. Das dient nicht dem Zweck der IT-Sicherheit und hat in einem IT-Sicherheitsgesetz daher auch nichts zu suchen. Die digitale Souveränität in Deutschland lässt auch hier wieder deutlich Federn.

Das legt wiederum deutlich nahe, dass das BSI als Handlanger der Sicherheitsbehörden bzw. konkret der Polizeien und Nachrichtendienste instrumentalisiert werden soll. Dies wird nicht dadurch besser, dass Verfassungsschutz und Polizeibehörden Staatstrojaner einsetzen dürfen und dafür Schwachstellen benötigen, sowie dass die ZITiS ebenfalls Schwachstellen benötigt, um Sicherheitsbehörden und Nachrichtendienste zu unterstützen.

Das Gesetz sollte daher klarstellen, dass dem BSI gemeldete Informationen ausschließlich für den Schutz der IT-Sicherheit verwendet werden dürfen und der Einsatz oder die Verwendung für offensive oder invasive Zwecke nicht zulässig ist.

Um ein hohes Maß an IT-Sicherheit erreichen zu können, sind alle Sicherheitsbehörden wie z. B. BND, BKA, Bundespolizei, Verfassungsschutz, ZITiS und die Bundeswehr zu verpflichten, von ihnen gefundene oder erworbene Schwachstellen ausnahmslos an das BSI zu melden.

Es braucht diese ausnahmslose Meldepflicht entdeckter Sicherheitslücken, die für alle staatlichen Stellen gelten muss. Ohne ein solch klares Bekenntnis des Gesetzgebers - auch zur Rolle des BSI hin - droht ansonsten ein schwerwiegender Vertrauensverlust bei den relevanten Akteuren aus der Wissenschaft, Wirtschaft, Zivilgesellschaft und den Sicherheitsforscher:innen.

Der regelmäßige Austausch mit Sicherheitsforscher:innen zeigt bereits, dass viele aufgrund herrschender Vorbehalte nicht (mehr) gewillt sind, entdeckte Schwachstellen und Sicherheitslücken an das BSI zu melden, weil das BSI eben nicht gesetzlich unabhängig nur für Sicherheit im Sinne der Defensive und der Cyberresilienz steht, sondern klar davon auszugehen ist, dass es für das BMI und die nachgelagerten Sicherheitsbehörden auch zur Unterstützung der Offensive und den invasiven Tätigkeiten beiträgt - Beispielsweise durch das hier geforderte Zurückhalten von Schwachstellen.

Auch die private Wirtschaft und insbesondere KRITIS Betreiber trauen dem BSI nicht mehr vollständig, was sehr gefährliche Züge für die Gesamtsicherheit in Deutschland annimmt, da IT-Sicherheit vom vertrauensvollen Austausch aller Akteure lebt. Vertrauen wird nun mal mühselig

und langwierig aufgebaut, kann aber durch solche Handlungen oder Gesetzesinhalte schnell zerstört werden...

Das Zurückhalten von Sicherheitslücken ist darüber hinaus gar nicht erforderlich, denn bekannt gewordene Sicherheitslücken werden ohnehin nicht umgehend flächendeckend geschlossen. Sicherheitsbehörden und Geheimdienste könnten daher alle bekannten offenen und ungepatchten Lücken nutzen, bis deren Ziele diese gepatcht haben.

Wird dies nicht vollständig berücksichtigt, wird der Staat seiner Verantwortung in der Digitalisierung und in eine digitale Souveränität Deutschlands nicht gerecht!

Eine einfache aber relevante Regel lautet: Die Zurückhaltung von Schwachstellen betrifft immer(!) auch die Zivilgesellschaft weltweit(!) sowie auch die private Wirtschaft und KRITIS Betreiber weltweit(!).

Im Hinblick auf die möglichen Folgen von Ausfällen kann das Offenhalten oder Verzögern der Behebung von Sicherheitslücken in einer Gesamtabwägung daher niemals angemessen sein. Wichtig ist in diesem Zusammenhang insbesondere, dass Betroffene wie die KRITIS-Betreiber vom BSI schnellstmöglich über sie betreffende IT-Sicherheitslücken informiert werden.

Wie stark soll denn sonst der Vertrauensverlust in den demokratischen Rechtsstaat werden?

Wie auch von anderen Stellen bereits gefordert, sollten die zusätzlichen Kompetenzen des BSI einer umfassenden Transparenz und Kontrolle unterliegen. Eine Trennung der Aufsicht über defensive durch das BSI und Offensive bzw. invasive durch die Sicherheitsbehörden und Nachrichtendienste würde das Vertrauen in das BSI deutlich erhöhen.

Dass Menschen mehr Hilfestellung im Bereich IT-Sicherheit wünschen, wundert ja grundsätzlich nicht. Selbst Informatiker:innen und Sicherheitsforscher:innen scheitern an den maroden Benutzerinterfaces von angeflanschter Security. Integrierte Sicherheit nach dem Modell „Security by Design“ ist eben Mangelware, da der Motivator für Unternehmen fehlt. Unsichere Software („Insecure by lack of Design“) ist dafür wiederum überall verfügbar, aber eher getreu dem Designprinzip „Fail by Design“.

Der Staat fördert das nicht, wenn er Backdoors, Frontdoors und Staatstrojaner - z. B. via ZITiS - für Polizeibehörden, Nachrichtendienste und Militär gesetzlich legitimiert und auf dem 0day Trading Graumarkt einkaufen oder selbst erforschen und entwickeln lässt.

Denn wenn IT-Systeme und Software aufgrund von Lawful Interception Maßnahmen und Staatstrojanern „defekt by Design“ sind, was bringt dann ein vermeintlich sicher entwickeltes System? Es müsste ja doch wieder für die Vorgaben vom deutschen Staat zur Fütterung seiner Sicherheitsbehörden und Nachrichtendienste aufgebrochen werden...

Hackerparagraphen und die Frage der Haftung bei offensiven und invasiven BSI Handlungen

§ 7c Abs. 1 Nr. 2 BSIG sieht vor, dass technische Befehle zum Zwecke einer Fehlerbereinigung an betroffene IT-Systeme von Betreibern verteilt werden können, welche das BSI allerdings nicht im genauen Betriebs- und Konfigurationszustand kennt. Dies birgt Risiken bei der Veränderung der IT-Systeme mittels der hierbei vorgesehenen invasiven Eingriffsmöglichkeiten.

Führt das BSI gemäß § 7b BSIG z. B. Scans durch, haftet der Staat für ggf. eintretende Fehlerzustände der IT-Systeme. Aber wer trägt aufkommende Kosten für das Auslösen einer Notfallprozedur? Beispielsweise bei einem KRITIS Betreiber?

Und wie erfährt z. B. solch ein KRITIS Betreiber davon, dass das BSI gescannt hatte und die Ursache für den Ausfall war? Wie kann er also die Ansprüche dafür geltend machen?

Und was ist mit dem daraus resultierenden Risiko von drohendem Versorgungsengpass oder gar Versorgungsausfall der kritischen Dienstleistung wie z. B. Strom und Wasser bei KRITS Betreibern? Was sieht der Gesetzgeber dann für den betroffenen Teil der Bevölkerung vor? Stellt er Notstrom und Wasserrationen deutschlandweit in die Bevorratung und hält diese für solche Szenarien vor?

Es gibt immer wieder bestätige und validierte Vorfälle, wo IT-Systeme und Netzwerkkomponenten nach einem Scan in einen Fehlerzustand fallen, rebooten oder sogar komplett einfrieren. Ja, solche Systeme sind auch direkt und ungefiltert an das Internet angebunden. Wurde die dafür erforderliche Ethik in Netzwerk Systemen daher hinreichend berücksichtigt und vorgegeben, z. B. „Philosophy meets Internet Engineering: Ethics in Networked Systems Research“[13] oder „Network Systems Ethics Guidelines“[14]?

Das BSI sollte daher mindestens solche Konzepte entwickeln, die diese Risiken adressieren. Diese sind als Vorgabe im Gesetzesentwurf mit aufzunehmen.

Grundsätzlich gilt aber: Invasiv auf IT-Systemen agieren ist gefährliches und nicht hervorsagbares rumpfuschen und stellt eine OP am offenen Herzen dar. Dies ist daher die schlechteste Variante einer Umsetzungsmöglichkeit zur Zielerreichung und darüber hinaus auch nicht notwendig!

Die relevanten Gefahren können mittels angemessener Gefahrenabwehr nach § 7c Abs. 1 Nr. 1 BSIG dargestellt und adressiert werden. Sogar ein MIRAI Botnetz[15] kann damit abgedeckt werden.

Neutralitätsdefizit des BSI

Der Schutz Kritischer Infrastrukturen als auch die Erhöhung von IT-Sicherheit sind auf die Zusammenarbeit von Wissenschaft, Wirtschaft, Zivilgesellschaft und Sicherheitsforscher:innen im Allgemeinen angewiesen.

Eine fehlende Neutralität der staatlichen und für KRITIS zuständigen Aufsichtsbehörde mindert das essentiell notwendige Vertrauen unnötig und behindert so diesen essentiellen Austausch durch die Zusammenarbeit für das gemeinsame Ziel.

Das BSI stellt sich oftmals als neutral und unabhängig in der Außendarstellung dar. Diese Unabhängigkeit ist aber faktisch nicht gegeben, solange es gemäß § 1 Satz 2 BSIG dem BMI unterstellt ist: *„Es untersteht dem Bundesministerium des Innern, für Bau und Heimat.“*

Das BSI ist innerhalb des BMI der Abteilung CI, Cyber- und Informationssicherheit zugeordnet. Diese Abteilung adressiert des Weiteren sowohl „Wirtschaft und Gesellschaft“ als auch die Sicherheitsbehörden, das BfV und das BKA.

[13] https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/41/2015/09/ENSR-Oxford-Workshop-report.pdf
[14] http://networkedsystemsethics.net/index.php?title=Networked_Systems_Ethics_-_Guidelines
[15] https://de.wikipedia.org/wiki/Mirai_(Computerwurm)

Diese beiden Gruppen von Behörden haben oftmals diametrale Ziele, so dass zwei konträre Herzen in einer Brust an einer zentralen Stelle im BMI schlagen und Zielkonflikte dadurch vorprogrammiert sind. Bei der oben aufgezeigten Gewichtung wird deutlich, wie ein Pendel „Sicherheit im defensiven Sinne eines BSI“ vs „Sicherheit im Sinne von Ermittlungs- und Sicherheitsbehörden als auch nachrichtendienstlicher Behörden“ innerbehördlich ausschlagen wird, so dass berechtigt von einem systemimmanenten Neutralitätsdefizit gesprochen werden muss.

Das BSI hat daher Ultima Ratio die Vorgaben des BMI einzuhalten und auszuführen und agiert somit weder neutral noch unabhängig. Die Option des Einwirkens wird durchaus auch seitens BMI bei Bedarf gezogen, wie z. B. bei der angeordneten Unterstützung für den Staatstrojaner vor einigen Jahren oder auch durch aktives Zurückhalten von Schwachstellen.

Der Koalitionsvertrag aus der 19. Legislaturperiode besagt interessanter Weise im Widerspruch hierzu auf Seite 44 ab Zeile 1970:

„Wir wollen das BSI als nationale Cybersicherheitsbehörde ausbauen und in seiner Rolle als unabhängige und neutrale Beratungsstelle für Fragen der IT-Sicherheit stärken“

Um das Ziel der Unabhängigkeit und Steigerung des Vertrauens zu erreichen ist zwingend erforderlich, dass das BSI mindestens(!) eine fachliche Unabhängigkeit vom BMI erhält, wie sie zum Beispiel das statistische Bundesamt erhalten hat. Konkret ist daher § 1 Satz 2 BSIG zur Grundlage technisch-wissenschaftlicher Erkenntnisse unter Einbezug von fachlich verantwortlichen Ministerien wir folgt anzupassen:

"Das BSI führt seine Aufgaben auf der Grundlage wissenschaftlich-technischer Erkenntnisse nach den Anforderungen der jeweils fachlich zuständigen Ministerien durch."

Diese Maßnahme stärkt das notwenige Vertrauen, welches für die Zusammenarbeit von Wissenschaft, Wirtschaft, Zivilgesellschaft und Sicherheitsforscher:innen im Allgemeinen notwendig ist.

Digitale Souveränität & Kritische Komponenten

§ 9b BSIG führt kritische Komponenten ein und fordert zünftig eine Vertrauenswürdigkeitserklärung von Herstellern kritischer Komponenten.

Dabei ist schon der Begriff und das Verständnis, was genau eine kritische Komponente ist und was sie wiederum nicht ist, nicht ausreichend rechtlich begriffsbestimmt. Wie wird also diese ominöse Vertrauenswürdigkeit rechtssicher definiert und wie kann diese überhaupt in einer Form überprüft werden, die dem Anspruch und der Intention dahinter genügen kann?

Es drängt sich daher die Frage auf, was das Ziel der Zertifizierung von kritischen Komponenten ist, wie dies funktionieren soll und ob dies generell Sinn macht. Mit einer Zertifizierung kann das Einschmuggeln einer Sicherheitslücke durch fremde Nachrichtendienste nicht vermieden werden. Welche Hoffnung soll also damit verbunden und was genau verhindern werden?

Darüber hinaus stellt sich die Frage, warum sich diese Regelung im Gegensatz zu den anderen IT-SIG Regelungen nicht auf alle KRITIS Betreiber sondern auf ausgewählte Komponenten von einigen KRITIS Sektoren beziehen soll.

Dasselbe Unternehmen könnte im Übrigen auch als nicht vertrauenswürdiger Hersteller kritischer Komponenten eingestuft und trotzdem KRITIS Betreiber sein, wenn es z. B. Software defined Radio oder Software defined Networking selber entwickelt.

Müsste ein solches Unternehmen diese kritischen Komponenten dann aber vor dem eigenen Einsatz sich selbst bescheinigen und zertifizieren lassen?

Auch stellt sich die Frage, ob ein Hersteller überhaupt alle Betreiber gemäß § 9b Abs. 5 BSIG kennen und informieren kann, wenn Reseller zum Einsatz kommen oder gebrauchte kritische Komponenten weiterverkauft werden.

§ 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.“

Das entspricht von der Formulierung auch jeder Lawful Interception-Schnittstelle. Sind diese dann in allen kritischen Komponenten nicht mehr zulässig und müssen daher konsequent unterbunden werden?

Bedeutet das dann letztlich auch, dass Vordertüren statt Backdoors, Lawful Interception-Schnittstellen und angeordnetes Ausleiten der Daten dafür sorgen, dass diese Komponenten nicht als kritische Komponenten eingesetzt werden dürften, weil es bei Schnittstellen naturgemäß immer die Möglichkeit gibt, dass darauf eingewirkt werden kann?

Insgesamt stellt die Einführung der kritischen Komponenten auch eine neue Form der Erlaubnis zum Marktzugang als auch der Marktbeschränkung dar. Wie kann daher eine langfristige Verhinderung der Monopolbildung für kritischen Komponenten sichergestellt werden?

Wenn durch die Vertrauenswürdigkeitserklärung der Kreis der Hersteller reduziert wird, wie wird sichergestellt, dass sich diese dann nicht als effektives Ziel herausstellen wie bei SolarWinds?

Wenn beispielsweise mittelfristig der einzige (Monopol) oder die einzigen beiden (Oligopol) verbleibenden Hersteller kritischer Komponenten als Single Point of Failure kompromittiert werden sollten, entstehen weitreichende Probleme großen Ausmaßes. Wurde dies angemessen berücksichtigt?

§ 9b Abs. 5 Nr. 4 BSIG besagt:

„Ein Hersteller einer kritischen Komponente ist nicht vertrauenswürdig, wenn […] 4. er bekannte oder bekannt gewordene Schwachstellen oder Manipulationen nicht unverzüglich dem Betreiber der Kritischen Infrastruktur meldet und beseitigt“

Ab dann ist der Hersteller also nicht mehr Vertrauenswürdig. Das BSI wiederum soll aber nach § 7b BSIG das Zurückhalten von Schwachstellen für den deutschen Staat vornehmen und exakt das in § 9b BSIG vorgegebene *„bekannte oder bekannt gewordene Schwachstellen oder Manipulationen nicht unverzüglich dem Betreiber der Kritischen Infrastruktur meldet und beseitigt“* unterlassen. Dies stellt einen erheblichen Wiederspruch dar.

Weiterhin stellt sich die Frage, wie die Aufrechterhaltung der kritischen Geschäftsprozesse - trotz Untersagung durch das BMI - sichergestellt werden soll. Wie kann dann die Vermeidung von Versorgungsengpässen oder -ausfällen durch die KRITIS Betreiber gewährleistet werden?

Der Gesetzesentwurf sieht ja die Untersagung oder z. B. einen Rückbau von verbauten Komponenten als Anordnung vor. Hier können also KRITIS Sektoren durch nicht durchdachte aber politisch motivierte Regulierungen lahmgelegt und die Bevölkerung unnötig gefährdet werden.

Über den Sektor IT und TK hinaus betrifft dies mindestens auch die Sektoren Energie und Wasser, da diese durch den Betrieb von Werks-Telekommunikationsnetzen ebenfalls betroffen sein werden. Ob das alles in allem daher Zweckdienlich ist, bleibt stark zu bezweifeln.

Die Regelungen in § 9b BSIG gehen weit über BSI Verantwortlichkeiten hinaus, daher wird in diesem Zusammenhang nur noch das BMI genannt, was die politische getriebene Motivation statt der Erhöhung der IT-Sicherheit auch an dieser Stelle deutlich aufzeigt.

Digitale Souveränität & der Detailgrad

Derzeit können nicht alle unter § 8a BSIG fallenden KRITIS Betreiber vollständig adressiert werden, weil einige z. B. die Anerkennung, KRITIS Betreiber zu sein, per Gerichtsstreit gegenüber dem BSI verweigern.

Darüber hinaus liegt bei anderen der Schwellenwert so niedrig, dass er wie im Sektor Wasser weniger als 50 von ca. 5.000 Wasserwerken als KRITIS Betreiber einstuft.

Weiterhin verzögern viele KRITIS Betreiber die fristgerechte Nachweiserbringung nach § 8a Abs. 3 BSIG.

Wenn dadurch also die kritischen Dienstleistungen der Versorgung mit Strom, Wasser usw. noch nicht bestmöglich nach den Vorgaben in § 8a BSIG komplett abgedeckt werden, was bringt uns dann eine Zertifizierung von kritische Komponenten und kritische Funktionen?

Wollen wir also mehr Anforderungen im Detail, weil die grundsätzliche und übergeordnete Strategie fehlt oder nicht erreicht wird? Bedeutet dies, dass das IT-SiG 1.0 bei der Zielerreichung in Teilen versagt hat, aber dies mangels Evaluierung nicht angemessen und sinnvoll nachjustiert werden kann? Soll aber dafür eine weitere sehr kontroverse Zertifizierung auf Detailebene eingeführt werden, um dies zu kaschieren?

Grundsätzlich ist alles Relevante und Wesentliche zum Schutz kritischer Infrastrukturen bereits vorhanden, nämlich die Umsetzung eines angemessenen und branchenspezifischen Stand der Technik nach § 8a BSIG. Sprich einem ISMS mit BCM. Genau dies ist daher als eines der wesentlichen Ziele des IT-SiG 2.0 zu fördern, zu intensivieren und zu verstärken.

Wo soll ansonsten die Reise nach einem Versagen der Zertifizierung von kritischen Komponenten und kritische Funktionen im nächsten Schutzschritt hinführen? In die Gesinnungsprüfung der Entwickler des Quellcodes von kritischen Komponenten?

Eine Beteiligung und Integration von Wissenschaft, Wirtschaft, Zivilgesellschaft und Sicherheitsforscher:innen ist deutlich angebracht, um den technisch-wissenschaftlichen Sinn und Unsinn solcher hochpolitischen Maßnahmen gleich aufzuzeigen und zielgerichtete Lösungsansätze zu erarbeiten, die ihre Wirkung auch erreichen können.

Digitale Souveränität & Open Source Untersagung

Durch die Anforderung einer Vertrauenswürdigkeitserklärung wird auch der Einsatz von Open Source bzw. FOSS im Bereich der kritischen Komponenten und damit bei betroffenen KRITIS Betreibern faktisch nicht mehr zulässig.

Wobei aber eben genau durch Open Source KRITIS Betreibern ermöglicht wird, kritische Komponenten länger als bei proprietärer Software üblich kontinuierlich zu Warten und zu pflegen (oder warten und pflegen zu lassen) und dadurch dauerhaft sicher zu betreiben und eben keinen Austausch vornehmen zu müssen, der ggf. einen Versorgungsengpass bei der kritischen Dienstleistung - wie der Verfügbarkeit von Strom oder Wasser - bewirkt.

EU Cyber Security Act (CSA) und freiwilliges IT-Sicherheitskennzeichen

§ 9c BSIG fordert ein freiwilliges IT-Sicherheitskennzeichen, zusätzlich zur Umsetzung des EU CSA in § 9a BSIG. Die Regelungen des § 9c BSIG sind dabei allerdings im Kern deckungsgleich mit den in § 9a BSIG geregelten Sachverhalte.

Ein freiwilliges IT-Sicherheitskennzeichen einzuführen doppelt sich mit der in § 9a BSIG erforderlichen Umsetzung des EU CSA, denn dieser behandelt bereits alle erforderlichen Aspekte zu Zertifizierungen, welche sich auch auf Consumer Devices erstrecken können.

Nutzer:innen von Consumer Devices lassen sich sehr grob in zwei Kategorien einteilen.

Zum einen in technik- und sicherheitsaffine Menschen, die ein IT-Sicherheitskennzeichen nicht benötigen und sich selber sachkundig informieren können und daher ohne das Kennzeichen informieren werden.

Und zum anderen in alle anderen Menschen, welche im Wesentlichen schon beim Scan eines QR-Codes mit dem Smartphone überfordert sein werden und darüber hinaus ein solches Kennzeichen nicht als solches erkennen können, geschweige denn richtig interpretieren werden. Darüber hinaus werden diese Nutzer:innen auch mit einem solchen Kennzeichen weder was anfangen können, noch ein gesteigertes Interesse an Sicherheitsinformationen haben, welche sie erst über den Umweg der Nutzung einer Technologie - und nur dann - angezeigt bekommen.

Ein freiwilliges IT-Sicherheitskennzeichen ist dafür aber sicherlich für Marketing- und Vertriebsverantwortliche bei Herstellerfirmen eine interessante Option. Aus dieser Position heraus könnte das Produktionsteam gefragt werden, wie lange ein Produkt, das aktiv vermarktet werden soll, mit Sicherheitspatches versorgt werden soll. Und genau für den Zeitraum würde das freiwillige IT-Sicherheitskennzeichen aktiv eingesetzt und vermarktet werden.

Kurz vor Ablauf der Versorgung mit Sicherheitspatches könnte das freiwillige IT-Sicherheitskennzeichen entfernt bzw. für genau dieses Produkt aufgekündigt werden. Damit steht selbst ein mittelmäßiger bis schlechter Hersteller gut da und hätte ein Produkt im Portfolio (gehabt), welches für den Hauptzeitraum am Markt mit einer zugelassenen und vom BSI amtlich wirkenden „Sicherheitsprüfung“ beworben wird. Hersteller, die kein Interesse an Sicherheit haben, werden das freiwillige IT-Sicherheitskennzeichen schlicht ignorieren, da kein Marktdruck durch den Wettbewerb zu erwarten ist.

Davon abgesehen ist eine Selbstauskunft auf Dokumentenbasis bereits ausreichend, das freiwillige IT-Sicherheitskennzeichen zu erhalten. Eine technische Prüfung eines Sachkundigen oder sogar eines unabhängigen Dritten ist dabei nicht vorgesehen.

Auch hier stellt sich wieder die Frage, ob bedingt durch diese zukünftig vorgesehenen Zertifizierungen und Konformitätsbewertungen nach § 9a BSIG oder § 9c BSIG Open Source und FOSS benachteiligt wird.

Es wird daher empfohlen, den § 9c BSIG ersatzlos zu streichen und die unnötige Bindung von Personal und weiteren Ressourcen hierdurch zu vermeiden.

Sanktionen & (nicht vorhandene) Incentivierungen

In § 14a BSIG muss das BSI für Institutionen der sozialen Sicherung aufgrund des Einvernehmens mit den zuständigen Aufsichtsbehörden mögliche Sanktionen von diesen bestätigen lassen. Die Aufsichtsbehörden sollen grundsätzlich geeignete Durchsetzungsmittel zur Verfügung stellen können, welche im Falle des Falles auch bedeuten, Zwangsmittel androhen können. Diese Zwangsmittel wären aber in jedem Fall günstiger als nur eine Maßnahme zur Informationssicherheit umzusetzen.

Durch seine Vorbildfunktion sollte der Staat sich und seine Behörden - in diesem Fall die Institutionen der sozialen Sicherung - nicht von Sanktionen ausnehmen. Eine Sonderstellung kann an dieser Stelle weder als vertrauensfördernd noch als Erhöhung der IT-Sicherheit verstanden werden und ist daher ersatzlos zu streichen.

Weiterhin stellt sich die Frage, ob auch zusätzlich zur Erweiterung der Sanktionierungsmaßnahmen eine Incentivierung und somit positive Motivation zur Erhöhung der IT-Sicherheit hinreichende Berücksichtigung gefunden hat. Wurden Möglichkeiten dieser Option nicht evaluiert oder in Betracht gezogen?

So könnten beispielsweise Unternehmen, die ein ISMS mit BCM aufsetzen und zertifizieren, diese Betriebsausgaben für ihre IT-Systeme steuermindernd geltend machen. Dies wird mittel- bis langfristig dazu führen, dass IT-Sicherheit durch den im ISMS vorgesehenen iterativen Prozess zum Lernen und zur Verbesserung der Sicherheitsmaßnahmen gemäß Demingkreis[16] kontinuierlich gesteigert wird.

Ausstehende Evaluierung des IT-SiG 1.0

Inzwischen liegen sechs Jahre zwischen dem ersten IT-SiG (2015) und der aktuellen Gesetzesfassung des IT-SiG 2.0 (2021). Daher müsste man eigentlich davon ausgehen können, dass das in die Wege gebrachte Gesetz zunächst in seiner Wirkung evaluiert und der Gesetzgeber dann die vorgesehenen Nachbesserungen damit begründet. Und um genau diese Vorgehensweise sicherzustellen, wurde im IT-SiG 1.0[17] sogar eine Evaluierung in Artikel 10 „Evaluierung“ rechtlich vorgeschrieben.

[16] https://de.wikipedia.org/wiki/Demingkreis

[17] https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1614281214462

Hierbei ist bereits nach vier Jahren *„unter Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag bestellt wird, zu evaluieren“*.

Die immer noch ausstehende aber gesetzlich vorgegebene Evaluierung der Wirksamkeit der aktuellen Gesetzesfassung sorgt weiterhin dafür, dass die Gesetzesbegründung und Kritiken daran mangels Evidenz-Erhebung an vielen Stellen einer gesicherten Erkenntnisgrundlage entbehren.

Das IT-SiG 2.0 enthält auf den ersten Blick zwar einige sinnvolle Regelungsansätze, viele der Neuerungen scheinen aber noch nicht zu Ende gedacht. Auch die erheblichen Kritiken seit dem ersten öffentlich gewordenen Entwurf des IT-SiG 2.0 aus 2019 sind beim Gesetzgeber bisher offenbar weitestgehend stumm verklungen. Eine Evaluierung der bereits bestehenden gesetzlichen Maßnahmen ist daher vor diesem Hintergrund nicht nur wünschenswerter denn je, sondern Voraussetzung für die Zielerreichung einer Erhöhung der IT-Sicherheit in Deutschland.

Daher verwundert es doch sehr, dass immer noch an der Einführung des IT-SiG 2.0 geklammert wird, ohne dass eine vollständige Evaluierung des IT-SiG 1.0 abschließend vorgenommen wurde. Es stellt sich daher die Frage, wieso der Gesetzgeber eine Gesetzesüberabreitung und -erweiterung vornimmt, wenn das bisherige nicht evaluiert wurde.

Eine entsprechende Anfrage zur „Evaluierung IT Sicherheitsgesetz“ über FragDenStaat[18] wurde im Oktober 2019 vom BMI damit ablehnend begründet, dass die BSI-Kritisverordnung (BSI-KritisV) *„am 03. Mai 2016 erstmals in Kraft getreten“* sei.

Vier Jahre später gab es aber immer noch keine Evaluierung.

Eine erneute Anfrage[19] ergab dann einen plötzlich folgenden Sinneswandel zur Auslegung einer Begründung für eine erneute Verzögerung:

„Im Hinblick auf die Sektoren Finanzen, Transport und Verkehr sowie Gesundheit wurde die BSI-KritisV erst mit Inkrafttreten des zweiten Korbs am 30. Juni 2017 vervollständigt.“

Nach dieser neuen - zugegebenermaßen sehr kreativen Rechenart des BMI zur zuletzt gültigen Version der BSI-KritisV - würde die Evaluierung erst zum 30. Juni 2021 fällig werden. Allerdings wird mindestens durch die Einführung des neuen KRITIS Sektors Siedlungsabfallentsorgung eine neue BSI-KritisV fällig werden und sich die Evaluierung erneut um vier Jahre verschieben können.

Des Weiteren würde mit der im IT-SiG 2.0 beschriebenen Neuregelung der Evaluierung in Artikel 6 selbige zeitlich sogar noch weiter nach hinten geschoben. Es soll zudem keine Evaluierung des für KRITIS wesentlichen Anwendungsbereichs der §§ 8a und 8b BSIG erfolgen, denn gemäß Artikel 6 Abs. 2 wird vorgesehen, dass *„Artikel 10 des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme vom 17. Juli 2015 (BGBl. I S. 1324)“* ersatzlos aufgehoben wird.

Dies würde aktuell daher auch bedeuten, dass keine IT-SiG 1.0 Evaluierung mehr vorzunehmen ist. Dadurch bleiben alle im IT-SiG 1.0 vorgenommenen Regelungen von 2015 bis 2021 außen vor!

Daher ist Artikel 6 Abs. 2 zu streichen und umgehend zu evaluieren, was die §§ 8a und 8b BSIG gebracht haben, da diese ja kaum verändert werden, aber im ersten IT-SiG eingeführt wurden und jetzt hätten evaluiert werden müssen.

[18] https://fragdenstaat.de/anfrage/evaluierung-it-sicherheitsgesetz/
[19] https://fragdenstaat.de/anfrage/evaluierung-it-sicherheitsgesetz-1/

Ansonsten würden diese grundsätzlichen Regelungen zum Kern Kritischer Infrastrukturen erst zwei Jahre später evaluiert werden, sprich in 2023. Lernkurven oder „Lessons Learned“ lassen sich so in jeglicher Form sträflich missen. Es erweckt daher eher den Anschein, als wolle der Gesetzgeber bei der Versorgungssicherheit der Bevölkerung durch kritische Infrastrukturen nach „Trial and Error“ Methode[20] verfahren.

Durch die fehlende Evaluierung kann nicht nachvollzogen werden, ob z. B. die aktuellen Schwellenwerte die vorgegebenen Schutzziele erreichen oder daran vorbei schlittern und Risiken zur Gefährdung der Versorgungssicherheit angemessen adressiert werden. Drei Beispiele hierzu:

- Im Sektor Wasser sind lediglich unter 50 von ca. 5.000 Wasserwerken KRITIS Betreiber. Reicht dies aus? Wenn ja, warum?
- Sektorübergreifende KRITIS Betreiber und die damit verbundenen kumulierenden Risiken - z. B. bei kommunalen Energie- und Wasserwerksbetreibern einschließlich öffentlichem Transport & Verkehr - wurden bisher nicht betrachtet. Ist das nicht relevant? Wenn nicht, warum?
- Wechselwirkungen und Abhängigkeiten von KRITIS Betreibern untereinander – z. B. die Abhängigkeit von Strom und Wasser bei einem KRITIS Betreiber aus einem anderen Sektor - wurden nicht berücksichtigt. Ist das nicht relevant? Wenn nicht, warum?

Auch fehlende Befugnisse für das BSI und Defizite in den Vorgaben durch das BSI wurden offenbar nicht evaluiert und im Gesetzesentwurf berücksichtigt. Dieser wurde daher inzwischen durch die Realität eingeholt. Hier ein Auszug von inzwischen offensichtlichen Fragestellungen im genannten Zusammenhang:

- Wieso haben immer noch nicht alle KRITIS Betreiber ein vernünftiges ISMS mit BCM implementiert und leben dieses aktiv im Betrieb?
- Wieso gibt es Prüfer, die nicht ordentlich und angemessen Prüfen oder ausreichende Fachkenntnisse nachweisen können?
- Wieso gibt es keine sog. Mockup Audits der Prüfer und keine Akkreditierung der Prüfenden Stellen KRITIS?
- Wieso gibt es kein definiertes Prüfverfahren wie beim IT-Grundschutz?
- Wieso haben viele KRITIS relevante Informationen des BSI nur empfehlenden Charakter in Form von Orientierungshilfen und sind daher nicht verbindlich oder gesetzlich bindend?
- Wieso kann jeder Schulungsanbieter die „zusätzliche Prüfverfahrenskompetenz für § 8a BSIG“ für KRITIS Prüfer beliebig gestalten?
  Beispielsweise mit oder ohne Prüfung, ein oder zwei Tage, vor Ort bzw. persönlich oder aufgezeichnete Websession.

Vorhandene Defizite in den Kompetenzen der KRITIS Prüfer als auch in der Qualität der Durchführung von KRITIS Prüfungen sollte das BSI mittels konkreter und verbindlich einzuhaltender Vorgaben in § 8a Abs. 5 BSIG gegensteuern. Und darüber hinaus diese auch regelmäßig selber prüfen, beispielsweise durch Mockup-Audits der einzelnen KRITIS Prüfer und durch eine verbindlich

[20] https://de.wikipedia.org/wiki/Versuch_und_Irrtum

vorgegebene und formale Akkreditierung der Prüfenden Stellen, in der Art vergleichbar wie beim IT-Grundschutz.

Die implizite Formulierung in § 8a BSIG ergibt, dass ein ISMS mit BCM zu betreiben ist, was auch das BSI erwartet. Dies wird allerdings nicht explizit in diesem Paragraphen erwähnt. Dies wäre ebenfalls ein Beispiel, einen Teil der erwähnten Defizite aufzulösen, den Gesetzestext für Betroffene lesbarer zu gestalten und den Diskussionen hierzu durch Klarstellung im Gesetzestext Einhalt zu gebieten.

Die ausstehende Evaluierung ist daher unverzüglich in die Wege zu leiten und die daraus gewonnenen Erkenntnisse vor Verabschiedung des IT-SiG 2.0 zwingend in dieses einzuarbeiten. Die Ergebnisse der Evaluierung sollten dabei abstrakt öffentlich gemacht werden, damit Transparenz geschaffen wird, ob und welche Ziele erreicht wurden.

In Artikel 6 ist daher darüber hinaus vorzusehen, dass die Evaluierung nicht nur in Teilen, sondern vollumfänglich und darüber hinaus auch nach wissenschaftlichen Standards durch eine unabhängige Stelle zu erfolgen hat. Die Ergebnisse sind auf der Homepage des BMI zu veröffentlichen.

Gestrichene Themen und Optimierungspotential

Im Entwurf von Mai 2020 waren die Krisenreaktionspläne noch vorhanden und wurden positiv begrüßt. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) sollte im zuvor enthaltenen § 5c BSIG wichtige Aufgaben und weitere Personalstellen zugeteilt bekommen, um erstmalig in die Lage versetzt zu werden, auch für IT-Katastrophen Krisenreaktionspläne auszuarbeiten. Auch wäre der neu geschaffene § 5c BSIG fast schon wie die initiale rechtliche Grundlage für den Einsatz eines zu schaffenden Cyber-Hilfswerks[21] - wie von der AG KRITIS im Februar 2020 auf der DefensiveCon[22] erstmalig öffentlich vorgestellt[23] - und verortet die Kompetenzen und Verantwortlichkeiten an den richtigen Stellen, nämlich dem BSI gemeinsam mit dem Partner BBK.

Dieser Paragraph ist leider ersatzlos gestrichen worden - obwohl Krisenreaktionspläne als auch ein Zuwachs beim BBK dringend notwendig sind. Resilienz erfordert auch die Fähigkeit, auf Krisen angemessen reagieren zu können - nur mit einer Mehrausstattung von BMI und Cyber-Kräften kann diesem nicht genüge getan werden. Es erfordert daher zusätzliche Stellen beim BBK, was sich gerade in diesen Zeiten der Pandemie klarer als je zuvor darstellt und auf der Hand liegt.

Viele der Branchenspezifischen Sicherheitsstandards (B3S)[24] sind nicht öffentlich verfügbar. Wieso sind B3S nicht verpflichtend auf der BSI Webseite zu veröffentlichen und freizustellen, damit der angemessene und branchenspezifische Stand der Technik eingesehen und transparent dargestellt

[21] https://ag.kritis.info/chw-konzept/
[22] https://www.defensivecon.org
[23] https://media.ccc.de/v/dcon2020-18-cyberhilfswerk-konzeption-fr-eine-cyberwehr-2-0
[24] https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Stand-der-Technik-umsetzen/Uebersicht-der-B3S/uebersicht-der-b3s_node.html

werden kann? Eine Verpflichtung zur Veröffentlichung, um ein Peer Review des in den B3S enthaltenen Stand der Technik zu erreichen und diesen öffentlich zu diskutieren erscheint daher zielführend im Sinne des Gesetzes.

Um diese Peer Reviews für den Stand der Technik zu ermöglichen ist als Vorgabe im Verfahren nach § 8a Abs. 2 BSIG vorzugeben, dass ein B3S nach erfolgreich vorgenommener Eignungsfeststellung auf der Webseite des BSI zu veröffentlichen ist.

Der Stand der Technik wird im Handbuch der Rechtsförmlichkeit[25] beschrieben und definiert.

In § 3 Abs. 20 BSIG wird die *„Entwicklung und Veröffentlichung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte."* durch das BSI beschrieben. An dieser Stelle sollte besser die vorherige verwendete Formulierung verwendet werden: *„Entwicklung und Veröffentlichung sicherheitstechnischer Anforderungen an IT-Produkte."*, da der Stand der Technik nicht von einer Stelle festgelegt, sondern von der herrschenden Mehrheit der Fachexperten wie z. B. Fachgremien gefestigt wird.

Als negatives Beispiel seien hier die Passwortrichtlinien im IT-Grundschutz angegeben, wo das BSI mit seinem bis letztes Jahr gültigen regelmäßigen Passwortwechsel recht alleine auf weiter Flur stand, da alle anderen maßgeblichen Sicherheitsstandards schon die Formulierungen auf den neueren und allgemein anerkannten Stand der Technik umgestellt hatten.

Symptomatisch handlungsunfähig im Cyberraum

Das ganze IT-SiG 2.0 ist leider symptomatisch dafür, wie unsystematisch das Thema Informationssicherheit in Deutschland betrieben wird.

Das zeigt sich schon an der langen Liste staatlicher Akteure in der Cybersicherheitsarchitektur Deutschlands alleine auf Bundesebene, die in der Übersicht der SNV[26] regelmäßig erweitert werden muss.

Es zeigt sich aber auch in der Cybersicherheitsstrategie Deutschlands 2016, die ausschließlich BMI Zuständigkeiten widerspiegelt, als ob Deutschland nur aus den vom BMI verantworteten Bereichen besteht. Die Frage nach der digitalen Souveränität muss sich Deutschland daher gar nicht erst stellen, die Antwort liegt auf der Hand. Oder besser gesagt in der Hand… des BMI.

Ein übergreifendes strategisches Konzept, dass auch Länder, Kommunen, Wissenschaft & Forschung, Bildung, Wirtschaft, Zivilgesellschaft und Sicherheitsforscher:innen sinnvoll einbettet, fehlt völlig.

Hier wurde erneut die Chance vertan, das BSI ordentlich als zentrale Stelle zur Vernetzung all dieser weiteren Akteure möglichst unabhängig aufzustellen und in dieser Rolle zu stärken. Stattdessen wird es zu Teilen zum Handlanger oder verlängerten Arm von Sicherheitsbehörden und Nachrichtendiensten.

---

25 https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/RechtsdurchsetzungUndBuerokratieabbau/HandbuchDerRechtsfoermlichkeit_deu.pdf?__blob=publicationFile&v=2

26 https://www.stiftung-nv.de/sites/default/files/snv_papier_cybersicherheitsarchitektur_final.pdf

Die Regelung der Zusammenarbeit der staatlichen Stellen, z.B. im Cyber-Abwehrzentrum wird auch weiterhin nicht auf eine ordentliche gesetzliche Grundlage gestellt. Dies ist längst überfällig, da sich dort inzwischen eine Vielzahl von Behörden ohne jede transparente Regelung austauschen. Das Trennungsgebot von Polizei und Nachrichtendiensten wird dadurch unterlaufen.

Auch der aktuelle Entwurf löst das Problem von mehrfachen Behördenzuständigkeiten nicht auf. So müssen Meldungen nach § 109 TKG weiterhin sowohl an das BSI als auch an die Bundesnetzagentur erfolgen. Das erzeugt bei den Betreibern Mehraufwände, ohne dass dem ein Mehrwert gegenübersteht. Warum die im IT-Sicherheitsgesetz von 2015 noch vorgesehene Weitergabe der Meldung von einer Behörde an die andere nicht ausreicht, ist unklar.

Die Kostenschätzung für die Wirtschaft ist eher kreativ plump ausgefallen als transparent und nachvollziehbar. Der Aufwand für die Wirtschaft ist deutlich zu niedrig geschätzt worden. Das Jahresgehalt einer gut ausgebildeten IT-Sicherheitsfachfrau liegt laut Mineralölwirtschaftsverband e.V. (MWV) bei etwa 80.000 € zzgl. Sozialabgaben. Der MWV stellt unter anderem durch detailliertere Kostenaufstellungen in seiner Stellungnahme[27] dar, dass die Berechnungen des BMI haltlos und viel zu niedrig angesetzt sind.

Das gleiche gilt für die Kostenschätzungen für Angriffserkennungssysteme nach § 8a Abs. 1a BSIG. Mit dem Betrieb, der Hard- und Software einschließlich Lizenzgebühren, dem Personal und den zugehörigen Prozessen sind diese durchaus deutlich teurer anzusetzen. Der Erfüllungsaufwand für die Wirtschaft ist daher insgesamt nicht nachvollziehbar beziffert.

In diesem Zusammenhang ist auch festzustellen, dass es unsinnig ist, dass bestimmte Einzelmaßnahmen wie Angriffserkennungssysteme explizit als neue Regelung im Gesetz eingeführt werden sollen. Denn welche konkreten Maßnahmen zur Absicherung ergriffen werden müssen, ergibt sich aus einer Risikoanalyse im Rahmen des ISMS mit BCM nach § 8a BSIG.

Wenn Angriffserkennungsmaßnahmen durch die explizite Nennung im Gesetzestext entsprechende Priorität einzuräumen ist, fehlen die dafür aufzuwendenden Ressourcen im Zweifel bei den Maßnahmen, die nach der Risikoanalyse wichtiger und dringend nötiger sind, z. B. eine angemessen abgesicherte Fernwartung nach Stand der Technik, wie sie im Wasserwerk in Texas[28] nicht vorhanden war. Auch in Deutschland sind aktuell solche Szenarien im Betrieb via Fernwartung weiterhin Alltag.

Diese Neuregelung ist auch deswegen nicht nachvollziehbar, weil Angriffserkennungssysteme auch bisher schon zu den technischen Maßnahmen zählen, die nach § 8a Abs. 1 BSIG umzusetzen sind. In der Gesetzesbegründung zum IT-Sicherheitsgesetz 2015 werden solche Detektionsmaßnahmen explizit als Teil der Pflichten nach § 8a Abs. 1 BSIG genannt. [29]

Auch im KRITIS-Sektor Staat und Verwaltung gibt es noch deutliches Verbesserungspotential. Es ist erfreulich zu sehen, dass mit § 4a BSIG und § 8 BSIG auch neue Regelungen für den Bereich der Bundesbehörden eingeführt werden. Diese reichen in der derzeitigen Form allerdings nicht aus. Es ist

[27] https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/entwurf-zweites-it-sicherheitsgesetz.html
[28] https://www.lebensraumwasser.com/hackerangriff-auf-wasserwerk-in-den-usa/
[29] BT-Drucksache 18/4096, Seite 25

nicht nachvollziehbar, warum wichtige und wesentliche Bereiche wie das Auswärtige Amt oder weite Teile des BMVg ausgenommen sind. Dass an diesen Stellen eine Kontrolle durch eine zentrale Stelle sinnvoll ist, hat der Angriff auf das Auswärtige Amt medienwirksam belegt.

Auch im Bereich der KRITIS-Prüfungen von KRITIS Betreibern ist daher richtigerweise eine unabhängige Prüfung der ergriffenen IT-Sicherheitsmaßnahmen durch § 8a Abs. 3 BSIG und Nr. 1.4.2. der Orientierungshilfe des BSI[30] vorgesehen.

Warum für den Sektor Staat und Verwaltung in Teilen von diesem Grundsatz abgewichen werden soll, ist daher absolut unverständlich.

Ebenfalls fragwürdig ist es, dass das BSI die einzuhaltenden Mindeststandards für die Bundesverwaltung nach § 8 Abs. 1 BSIG nur im Einvernehmen mit den anderen Ressorts festlegen kann. Diese werden sich - anders als das BSI - bei der Frage im Zweifel nicht nur an den Erfordernissen der IT-Sicherheit orientieren. Sie werden sich wohl eher davon leiten lassen, den eigenen Aufwand für die Umsetzung möglichst gering zu halten. Im Sinne der IT-Sicherheit ist es daher erforderlich, dass die Mindeststandards vom BSI festgelegt werden.

Dabei muss das BSI die Positionen der Ressorts sicherlich berücksichtigen. Das richtige Instrument dafür ist daher die Herstellung des Benehmens. Schon beim ersten IT-Sicherheitsgesetz 2015 wurde daher für § 8 Abs. 1 BSIG das Einvernehmen durch das Benehmen ersetzt. Warum das jetzt geändert werden soll, ist nicht nachvollziehbar.

Bei den Krisenbewältigungsaufgaben des BSI ist nicht nachvollziehbar, warum das BSI nach dem neuen § 8b Abs. 4a BSIG im Fall einer erheblichen Störung zur Herausgabe von Informationen das Einvernehmen mit der für den jeweiligen Betreiber zuständigen Aufsichtsbehörde suchen muss. Die Bewältigung der Störung muss hier Priorität gegenüber den Befindlichkeiten der zuständigen Aufsichtsbehörde haben. Es würde daher vollkommen ausreichen, die zuständige Aufsichtsbehörde in Kenntnis zu setzen. Dieses Detail zeigt erneut einen groben handwerklichen Fehler, der die Bewältigung einer erheblichen Störung unnötig verzögert. Dieses Einvernehmenserfordernis ist daher aus § 8b Abs. 4a BSIG zu streichen.

Es muss sich auch die Frage gestellt werden, ob das BSI wirklich alleine in der Lage ist, alle neuen Aufgaben im Bereich der Cybersicherheit zu übernehmen. Mit jeder neuen Aufgabe besteht die Gefahr, dass das BSI zwar neue Aufgaben bekommt, diese aber nicht alle erfüllen können wird. So kann man z. B. das BSI Mobile Incident Response Team sicherlich weiter ausbauen, aber zur Bewältigung drohender Cyber-Großschadenslagen mit vielen Betroffenen in ganz Deutschland werden sie trotzdem nie ausreichen können. Die Wahrscheinlichkeit einer solchen Cyber-Großschadenslage steigt aber durch die fortschreitende Digitalisierung - auch in der Prozessautomatisierung - kontinuierlich und stetig an.

[30] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/Orientierungshilfe_8a_3_v11.pdf

Daher sollte an einem Gesamtkonzept für die Cybersicherheit in Deutschland gearbeitet werden, welches auch die Einbettung des von der AG KRITIS konzipierten Cyber-Hilfswerk[31] zur Unterstützung mittels ehrenamtlich tätiger Expert:innen Berücksichtigung findet.

Fazit

Der Gesetzesentwurf zum IT-SiG 2.0 stellt in seiner aktuellen Form ein strategieloses Bürokratiemonster dar, welches der Anforderung zur Erhöhung der IT-Sicherheit nicht gerecht wird.

Die Cybersicherheit und die digitalen Souveränität Deutschlands bleiben dabei auf der Strecke.

Auch und insbesondere, dass in diesem Gesetzesentwurf keine Alternative unter Punkt C angegeben wird, lässt tief blicken. Es ist schlichtweg nicht nachvollziehbar, dass bei solch umfassenden Zielvorgaben keine einzige Alternative benannt wird. Dies ist sicherlich insbesondere auf die fehlende Evaluierung der Effektivität aller im IT-SiG 1.0 vorgegebenen Maßnahmen zur Erhöhung der Sicherheit informationstechnischer Systeme zurückzuführen.

Viele Alternativen wurden trotz alledem in dieser Stellungnahme aufgezeigt und finden hoffentlich ihren konstruktiven Weg in den Gesetzesentwurf, um nichts weniger als die Cybersicherheit zum Schutz der Zivilgesellschaft zu gewährleisten.

Die AG KRITIS steht hierfür gerne weiterhin ehrenamtlich beratend für den Gesetzgeber und die demokratischen Parteien zur Verfügung.

[31] https://ag.kritis.info/chw-konzept/