Berlin, 03.12.2020

Notbremse für den Entwurf! - Stellungnahme der AG KRITIS zum 3. Entwurfs des IT-SiG 2.0

Am 21.11.2020 haben wir den dritten Referentenentwurf des IT-Sicherheitsgesetzes 2.0 in unserem Blog veröffentlicht. Den nun am 02.12.2020 durch das Bundesministerium des Inneren, für Bau und Heimat veröffentlichten Entwurf entspricht dieser Vorabversion mit nur geringfügigen Änderungen. Neben einigen Verbesserungen enthält der Gesetzesentwurf jedoch auch eine Reihe an erheblichen Mängeln, welche wir als sehr problematisch einschätzen. Auf Grund der zu kurzen Frist zur Stellungnahme und der laut netzpolitik.org geplanten Verabschiedung am 16. Dezember 2020 durch das Kabinett halten wir es für ausgeschlossen, dass notwendige Änderungen noch Einzug in den Gesetzesentwurf finden können.

Wir fordern daher einen **Aufschub des Gesetzgebungsverfahrens** und eine **echte Einbindung der** zahlreichen **zivilgesellschaftlichen und sonstigen Organisationen**, die sich mit der Cyber-Sicherheitspolitik beschäftigen.

Nicht erkennbare Strategie im dritten IT-SiG 2.0 - Entwurf

Der vorgelegte Gesetzesentwurf lässt keine klare Linie zur konsequenten Erhöhung des Sicherheitsniveaus der IT 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 verpflichtende Einführung eines Informationssicherheitsmanagementsystems (ISMS) sind nicht enthalten. Gute Ideen aus vorherigen Entwürfen fehlen nun ganz, dafür wurden mehrere verfassungsrechtlich höchst fragliche Passagen hinzugefügt.

Inhaltsverzeichnis

Gesetzesanpassungen mit Bauchgefühl statt Evaluierung

Die gesetzlich festgelegte Evaluierung des IT-SIG 1.0 gemäß Artikel 10 "*unter Einbezug eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag bestellt wird*" steht weiterhin aus. Auch laut § 9 KritisV muss die BSI-Kritisverordnung - und damit insbesondere auch die Schwellwerte, ab denen ein Betreiber als Kritische Infrastruktur betrachtet wird - alle zwei Jahre evaluiert werden. Diese Evaluierungen wurden inzwischen wiederholt versäumt.

Die zuvor genannte Evaluierung ist allerdings ein elementarer Bestandteil zur Prüfung der Wirksamkeit und muss durchgeführt werden, bevor eine Kompetenz- und Anforderungsausweitung mit dem neuen IT-SiG 2.0 vorgenommen wird. Stattdessen wird die Pflicht zur regelmäßigen Evaluierung mit diesem Entwurf vollständig entfernt.

Es ist darüber hinaus mehr als bedenkenswert, dass nun bzw. erst im Dezember 2020 die Stellungnahme von Interessensvertretungen, Verbänden und der Zivilgesellschaft erfolgen kann und ohne hinreichende Konsultationsfrist (vom 2. Dezember bis 6. Dezember, dann verlängert bis 9. Dezember, also nur 5 Werktage) eine unvollständige sowie nicht-zielführende Gesetzesänderung beschlossen werden soll. Eine Frist von nur einer Woche kann nicht dem demokratischen Gedanken entsprechen und spiegelt nicht die Wichtigkeit der geplanten Gesetzesanpassungen wider.

Die Kernidee des Schutzes kritischer Infrastrukturen kommt viel zu kurz. Stattdessen werden sachfremde Themen eingebracht. Vorhandene Möglichkeiten, die Unzulänglichkeiten bisheriger Gesetze zu beheben, konnten nicht genutzt werden, weil aufgrund der gesetzwidrig unterlassenen Evaluationen keine eigenen Informationen im BMI dazu vorlagen.

Thema verfehlt: verpflichtende Systeme zur Angriffserkennung

Artikel 12, Seite 15 - Änderungen an § 8a Absatz 1, 1a, 1b... BSI § 8a 1b), EnWG § 11 1d)

Über den bestehenden § 8a BSIG ist bereits jetzt die Umsetzung eines ISMS und damit einhergehend eine Risikoanalyse mit anschließender Definition der Maßnahmen vorgegeben. Sofern sich hieraus ergibt, dass die Einführung und der Betrieb von Systemen zur Angriffserkennung (IDS oder IPS) als spezifische Maßnahme erforderlich ist, wird dieses bereits dadurch verpflichtend.

Die gesetzliche Vorgabe einzelner technischer Maßnahmen in einem Gesetz, wie z.B. einem IDS oder IPS, vollkommen unabhängig von einer Risikoanalyse der konkreten technischen Infrastruktur, ist nicht sinnvoll. Im Zweifel führt dies zu überflüssigen Aufwand und bindet Ressourcen die im Einzelfall bei wichtigeren Maßnahmen notwendig wären. Darüber hinaus ist

es unüblich, eine technische Maßnahme in dieser Konkretheit im Gesetz vorzugeben. Wenn überhaupt nötig, könnten Vorgaben auf einem solchen Detaillevel für einzelne Anlagenkategorien differenziert als Rechtsverordnung in der Kritis-Verordnung vorgegeben werden.

Anonym und überflüssig: Speicherung von Protokolldaten

Logdaten von KRITIS-Betreibern

§ 8a Absatz 1b BSIG

Eine Anonymisierung von Logdateien in Verbindung mit gleichzeitiger Umsetzung eines ISMS ist technisch ohne Duplizierung von Daten unmöglich. Es muss grundsätzlich davon ausgegangen werden, dass anonymisierte Logdateien nicht dem Stand der Technik zur Detektion und Reaktion auf Sicherheitsvorfalle im Rahmen des ISMS entsprechen. Ein Betreiber muss grundsätzlich in der Lage sein, Handlungen konkreten Personen zuzuordnen. Die Verpflichtung Logdaten zu speichern widerspricht zumindest für den Sektor Energie den Anforderungen, die aus dem Sicherheitskatalog der BNetzA abgeleitet werden können, denn im Sicherheitskatalog wird ein ISMS mit entsprechenden Maßnahmen gefordert.

Da eine IP-Adresse nach Einschätzung des Bundesbeauftragten für den Datenschutz in der Informationstechnik (BfDI) ein personenbezogenes Datum ist und daher diese Information entfernt werden müsste, ist der entstehende Datenhaufen nicht verwendbar und enthält keine Aussagekraft mehr.

> *Begründung dieser Änderung: "Eine Schätzung des Erfüllungs-Aufwands, im Wesentlichen die Kosten für die Systeme zur Angriffserkennung selbst sowie Personal, ist insoweit nicht möglich. Denn zum einen sind solche Systeme teilweise bereits bei Betreibern Kritischer Infrastrukturen im Einsatz, sodass für diese Betreiber durch die Neuregelung überhaupt keine zusätzlichen Kosten entstehen. Zum anderen sind die Kosten für diese Systeme sehr unterschiedlich."*

Das BMI sagt in der Begründung, das die Schätzung des Erfüllungsaufwands nicht möglich sei - denn solche Systeme seien ja bereits im Einsatz. Dabei übersieht das BMI, dass bei Betreibern viele Gigabyte, in manchen Fällen sogar Terabytes, pro Tag an Logdaten entstehen - diese Datenmenge für vier Jahre zu speichern lässt enorme Mehrkosten bei allen Betreibern entstehen und erzeugt aufgrund der vorgeschriebenen Anonymisierung keinen Mehrwert. Eine Analyse solcher Datenmengen ist extrem rechenaufwendig. Es ist fraglich, ob am Markt verfügbare Großcomputer in der Lage sein können, Logdateien dieser Größenordnung innerhalb angemessener Zeit - während eines Angriffs in der Regel nur Stunden oder weniger - auszuwerten. Schon der Transfer solcher Datenmengen zu einer entsprechenden

Großrechenanlage würde Wochen benötigen und einen erheblichen logistischen Aufwand mit sich bringen.

Diese Änderung belegt die Realitätsferne des zuständigen Referats im BMI - keiner der Mitarbeiter hat wohl jemals Logdaten eines KRITIS-Betreibers gesehen oder Informationen über den Prozess der Auswertung erlangt, ansonsten wäre diese Formulierung so nicht entstanden.

Logdaten von Kommunikationstechnik des Bundes

§ 5 Absatz 2 BSIG

Die Erweiterung der Speicherfrist von Logdaten aus dem Betrieb der Kommunikationstechnik des Bundes in von drei auf zwölf Monate begrüßen wir trotzdem - aufgrund der bisher rückständigen Digitalisierung der Bundesbehörden ist das Problem der zu großen Menge an Logdaten auf absehbare Zeit dort zumindest nicht zu befürchten - auch zeigen vergangene Angriffe auf Bundesbehörden wie z.B. den Bundestag, dass diese erst nach deutlich mehr als drei Monaten detektiert werden - hier benötigt es also die erweiterte Speicherdauer, um einen Angriff im Nachhinein noch nachvollziehen zu können.

UNBÖFI - Es braucht kein "KRITIS light"

Neuschaffung des § 8f BSIG

Die Unternehmen in besonderem öffentlichen Interesse (UNBÖFI), ehem. ISBÖFI stellen eine Art KRITIS-light da, die unnötig sind.

Rüstungsindustrie via Außenwirtschaftsverordnung

„Man muss Gesetze kompliziert machen, dann fällt es nicht so auf“, sagte Bundesinnenminister Horst Seehofer im Juni 2019. An dieses Mantra hält man im BMI wie gewohnt auch im IT-SiG 2.0 konsequent fest. Im Entwurf von 2019 fand sich noch die Formulierung, dass die Rüstungsindustrie zur sog. ISBÖFI, jetzt UNBÖFI gehören soll. Die „UNBÖFI“ ist quasi eine Art „KRITIS light“. Nicht alle KRITIS Pflichten werden auferlegt, aber manche. Im aktuellen IT-SiG2-Entwurf findet sich das Wort „Rüstung“ weiterhin nicht mehr, trotzdem gehört Rüstung weiterhin zu UNBÖFI. Dies wird durch die verschleiernde Erwähnung des „§ 60 AWV Absatz 1 Satz 1-5“ festgelegt und auch in den Begründungen zum Gesetz weder erläutert noch aufgeklärt.

Die Rüstungsindustrie ist weder KRITIS, noch kann sie zu einer Art „KRITIS light“ gehören - denn die Rüstungsindustrie gehört eben nicht zu solchen Diensten *„die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der*

Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind und deren Störung oder Zerstörung erhebliche Auswirkungen hätte“. (KRITIS-Definition aus der EU NiS Richtlinie).

Die Rüstungsindustrie bedient allerdings militärische Bedürfnisse. Daher hat sie nichts in einem zivilen IT-Sicherheitsgesetz als "KRITIS light" zu suchen, wo aus der eigentlich erforderlichen Sicht der nationalen Sicherheit viel zu handzahme Vorgaben vorgesehen werden. Der aus staatlicher Sicht sogar begrenzt nachvollziehbare Wunsch, der Rüstungsindustrie höhere Auflagen für Resilienz in ihrer IT-Infrastruktur aufzuerlegen, kann nicht über die UNBÖFI-Gesetzgebung erfüllt werden. Die Rüstungsindustrie soll auch im Spannungs- und Verteidigungsfall noch funktionieren können. Dies erfordert grundlegend andere Vorgehensweisen und Maßnahmen, als die vorhandenen UNBÖFI-Vorgaben hergeben. Die Rüstungsindustrie gehört daher in das Weißbuch des Verteidigungsministeriums und im IT-SiG konsequent gestrichen.

Wir kritisieren, dass die genauen Kriterien nach denen ein Unternehmen "UNBÖFI" wird, nicht im Gesetz stehen, sondern durch Rechtsverordnung festgelegt werden.

Unternehmen im besonderen öffentlichen Interesse werden im Referentenenwurf des IT-SiG 2.0 in drei Unterkategorien unterteilt: (§ 2 Absatz 14 Satz)

1. sicherheitsrelevante Unternehmen (Rüstung / IT-Sicherheitstechnik für die Bundesrepublik)
2. volkswirtschaftlich relevante Unternehmen (gemäß inländischer Wertschöpfung, in einer Verordnung genauer zu definieren)
3. potenziell umwelt- / gesundheitsgefährdende Unternehmen (die unter die Störfallverordnung, Betriebsbereich oberer Klasse fallen)

Unternehmen nach Satz 2, also volkswirtschaftlich relevante Unternehmen, sollen durch das neue Gesetz nun auch die Möglichkeit haben unter Umständen unter eine Art KRITIS-light (UNBÖFI) zu fallen - dies stellt eine Ungleichbehandlung gegenüber kleineren Unternehmen dar. Auch ging es bisher um die Sicherstellung der Versorgung der Bevölkerung mit grundlegendsten Dienstleistungen - und eben nicht um die volkswirtschaftliche Wertschöpfung. Diese Änderung am Prinzip der KRITIS-Gesetzgebung ist so nicht sinnvoll und weicht die Trennschärfe der Regelung insgesamt auf.

Änderung an den Sektoren

§ 2 Absatz 10 BSIG

Wir begrüßen die Aufnahme von Siedlungsabfallentsorgung als neuen Kritische Infrastruktur Sektor. Weiterhin fehlt allerdings der Sektor Chemie. Für diesen werden zwar in der Störfall-Verordnung diverse Vorsichtsmaßnahmen zum Schutz vor Unfällen festgelegt, der Bereich der Prozessleittechnik wird dort aber nicht betrachtet. Dabei ist die Prozessleittechnik, welche u.A. aus informationstechnischen Systemen besteht, genau der Teil, welcher erhöhte Sorgfalt durch den Betreiber benötigen würde um Versorgungsausfälle und Freisetzungen von Schadstoffen unwahrscheinlicher zu machen.

"UNBÖFI nach Störfallverordnung" ist leider nur "besser als nichts" weil es zu kurz greift. Nachhaltiger und sinnvoller wäre die Aufnahme von "Chemie" als eigener Sektor mit entsprechenden detaillierten Anlagenkategorien in der Kritis-Verordnung. In der Chemie-Branche geht es nicht nur um die Herstellung von wichtigen Grundstoffen für das produzierende Gewerbe und die Landwirtschaft, auch die Freisetzung von gefährlichen Schadstoffen im Schadensfall ist zu befürchten.

Keine Krisenreaktionspläne und keine BBK-Stärkung

Im Mai 2020 haben wir den Punkt der Krisenreaktionspläne in unserer Stellungnahme zum 2. Entwurf des ITSiG als besonders positiv hervorgehoben.

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 Cyberhilfswerks - wie von uns im Februar 2020 vorgestellt - und verortet die Kompetenzen und Verantwortlichkeiten an den richtigen Stellen, nämlich dem BSI gemeinsam mit dem Partner BBK.

Dieser Paragraph ist leider im 3. Entwurf ersatzlos gestrichen worden - obwohl Krisenreaktionspläne als auch ein Zuwachs beim BBK dringend notwendig ist. Eine 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 zusätzliche Stellen beim BBK.

Offensive Maßnahmen gegen IT-Grundrechte

> *§ 7c Anordnungen des Bundesamtes gegenüber Diensteanbietern*
> *(1) Zur Abwehr konkreter erheblicher Gefahren für die in Absatz 2 genannten Schutzziele kann das Bundesamt gegenüber einem Anbieter von Telekommunikationsdiensten im Sinne des Telekommunikationsgesetzes (Diensteanbieter) mit mehr als 100.000 Kunden anordnen, dass er*
> *1. [...]*
> *2. technische Befehle zur Bereinigung von einem konkret benannten Schadprogramm an betroffene informationstechnische Systeme verteilt,*

Die in § 7c Abs. 1 S. 2 geplanten aktiven Maßnahmen stellen einen Eingriff in die Integrität informationstechnischer Systeme dar. Somit handelt es sich auch um einen Eingriff in das IT-Grundrecht, an den das BVerfG hohe Anforderungen stellt. Diese Anforderungen können hier nicht erfüllt werden. Darüber hinaus wird dieser Grundrechtseingriff in das IT-Grundrecht nicht einmal durch die Exekutive durchgeführt, sondern privaten Unternehmen auferlegt - so funktioniert das Gewaltmonopol nicht. Wir gehen davon aus, dass derartige Regelungen nicht verfassungskonform sein können und daher nicht wirksam werden dürfen.

Auch die Befugnisse in § 7c (3) sind rechtlich fragwürdig, da sie sehr allgemein und weitreichend formuliert sind.

> *§ 7c (3) "Ordnet das Bundesamt eine Maßnahme nach Absatz 1 Satz 1 Nummer 1 an, so kann es gegenüber dem Diensteanbieter auch anordnen, den Datenverkehr an eine vom Bundesamt benannte Anschlusskennung umzuleiten"*

Der Detailgrad von §7c Abs. S. 3 ist unzureichend. Maßnahmen, die sich aus §7c Abs. S. 3 ergeben, sind zum Beispiel Sinkholing oder Nullrouting. Diese Maßnahmen sollten explizit auf den Schutz von KRITIS oder der Zivilbevölkerung beschränkt werden und nicht zu allgemeinen Befugniserweiterung der Behörden führen. Es müssen klare Vorgaben gemacht werden, welche Art von Netzwerkverkehr (unter Wahrung von Datenschutz und Grundrechten) unter diese Maßnahmen fallen können.

Übertragung von Aufgaben der Staatsanwaltschaften auf Diensteanbieter

Änderung des TMG - § 15d Absatz 2 ff.

Bisher müssen Ermittlungsbehörden - und nur mit einem Richtervorbehalt - die Diensteanbieter anfragen um vom Betreiber die strafrechtlich benötigten Daten herausgeben zu lassen, sofern die Anfrage als berechtigt angesehen wird. Hier sollen zukünftig allerdings die Diensteanbieter eigenständig entscheiden müssen, was strafrechtlich relevant ist und dies dann

direkt an das BKA übermitteln. Ein Richtervorbehalt ist dabei nicht mehr vorgesehen und wird umgangen - die private Wirtschaft wird zum Erfüllungsgehilfen der Staatsanwaltschaften und muss Aufgaben der Rechtspflege selbst übernehmen.

Diensteanbieter werden genötigt, Teile der Entscheidung ob eine Straftat vorliegt, selbst zu treffen, proaktiv Daten zu erheben und dem Bundeskriminalamt zuzuleiten. Dies bedeutet eine Umkehr der Entscheidung über die Einleitung eines Strafverfahrens, da der Diensteanbieter nicht mehr unterstützend von der Staatsanwaltschaft und nach Beschluss eines Richters hinzugezogen wird.

Nach den bestehenden Datenschutzregelungen sind die Betreiber verpflichtet die Geschädigten bei Verlust von personenbezogenen Daten zu informieren, die im Anschluss eine Anzeige erstatten können. Die Einführung einer Meldepflicht bei den Diensteanbietern ist auch deswegen nicht nachvollziehbar, zumal Geschädigte ein Interesse haben könnten, die Strafverfolgungsbehörden nicht einbinden zu wollen.

Umgehung des Nationalen Cyber Abwehrzentrum (NCAZ)

Änderung des TMG - § 15d Absatz 1 ff.

Die vorliegende Formulierung stellt eine Umgehung des extra für diesen Fall geschaffenen "Nationalen Cyber-Abwehrzentrum" (NCAZ) im BSI dar. Im NCAZ sind alle Sicherheitsbehörden vertreten, die für die Vorfallsbehandlung zuständig sein könnten - wer wirklich zuständig ist, steht erst nach einer erfolgreichen Attributierung des Vorfalls zu einem Täter, seinem Ziel und der Nationalität des Täters fest. Nur im Fall, dass der Täter die deutsche Staatsbürgerschaft hat und zivile Diensteanbieter, Infrastruktur oder deutsche Bürger angegriffen worden sind, wäre tatsächlich das BKA zuständig - in allen anderen Fällen wären andere Sicherheitsbehörden zuständig. Zum Zeitpunkt der Feststellung einer Tatsache, die die Annahme rechtfertigt, dass eine Straftat nach § 202a ff vorliegen könnte, ist diese Attributierung jedoch noch nicht erfolgt - folgerichtig sollte der Vorfall daher im NCAZ erstbearbeitet werden.

Unterlassene Hilfeleistung: Fehlende Warnung von Betreibern

Scanning-Befugnisse des BSI zu eng gefasst

Wir begrüßen, dass das BSI zukünftig Netze untersuchen darf, um Systeme mit Sicherheitsrisiken zu identifizieren und die Betroffenen zu warnen. Die konkrete Ausgestaltung des § 7b BSIG ist aus technischer Sicht aber leider zu eng definiert.

"Detektion von Sicherheitslücken und anderen Sicherheitsrisiken an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen

Telekommunikationsnetzen" wird durch Scanmaßnahmen erreicht, die in § 7b (1) aber bereits voraussetzen, dass die Systeme als unzureichend geschützt bekannt sind. Durch dieses Kausalitätsproblem wird die Überprüfung auf Schwachstellen unnötig erschwert oder gänzlich verhindert. Daher sollten Port- und Schwachstellenscans durch das BSI grundsätzlich möglich sein.

Mit einfachen "Portscans" ohne weitergehende Interaktion mit dem gescannten System wird sich jedoch nicht überprüfen lassen, ob das System von Schwachstellen wie zum Beispiel Shitrix oder Eternal Blue betroffen ist. Daher sind zwar Portscans als erster Schritt zu begrüßen, zur Identifikation von Schwachstellen aber nicht ausreichend.

Die Einschränkung auf KRITIS, Bundessysteme und UNBÖFI sorgen dafür, dass das BSI eine Liste anlegen müsste von Systemen, die vom BSI gescannt werden dürfen. Eine solche Liste sollte jedoch nicht angelegt werden, weil diese Liste ein high-value-target für Cyberkriminelle wäre und diesen wertvolle Ziel-Informationen liefern würde.

In der Begründung ist die Argumentation zur Beschränkung auf statische IP Adressen technisch unsinnig da einerseits auch KRITIS Systeme hinter dynamischen IPv4 Adressen stecken können und andererseits in Zukunft IPv6 immer statisch ist. Weiterhin könnten auch Privatnutzer über eine Benachrichtigung durch ihre Provider profitieren.

Der Einsatz von spezialisierten (weitestgehend passiven) Suchmaschinen, wie Shodan oder Censys, wäre im vorliegenden Einsatz zum Beispiel nicht abgedeckt.

Damit ist der vorgeschlagene § 7b (1) BSIG zu eng gefasst um sein Ziel erfüllen zu können.

Unterlassung von Warnungen an KRITIS Betreiber sind intolerabel

§ 7b (3) BSIG:
Wird durch Maßnahmen gemäß Absatz 1 eine 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.

Wenn konkrete Sicherheitslücken bei Systemen der Kritischen Infrastrukturen erkannt wurden, kann es keine überwiegenden Sicherheitsinteressen geben die der Benachrichtigung der für das informationstechnische System Verantwortlichen entgegenstehen. Die Betroffenen müssen immer umgehend informiert werden, damit der Betrieb der Kritischen Infrastruktur schnellstmöglich abgesichert werden kann. Dies gilt insbesondere da diese Lücken auch von Dritten in derselben Art und Weise jederzeit erkannt und ausgenutzt werden können.

Auch in § 4b (5) BSIG wird für gemeldete oder bekannt gewordene Informationen zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen die Meldung nach §

8b Absatz 2 Nummer 4 Buchstabe a) an Betreiber Kritischer Infrastrukturen potenziell aufgrund von sonstigen "Übermittlungshindernissen" unterschlagen. Informationen zu Schwachstellen müssen konsequent zur Behebung derselben und zur Absicherung von Systemen genutzt werden und dürfen nicht zur Schwächung der IT-Sicherheit zurückgehalten oder z.B. für die Entwicklung von Staatstrojanern an andere Stellen wie Sicherheitsbehörden oder Geheimdienste weitergegeben werden.

Vertrauenswürdige Hersteller - Lex Huawei für KRITIS?

§ 9b (5) S. 3 (et al.)

Der § 9b ist in seiner Ausprägung nicht sinnvoll: Wesentliche Aspekte sind unvollständig oder hinsichtlich ihres Zwecks unklar. Eigentlich müsste man diesen Abschnitt "Lex Huawei" nennen, da offensichtlich ist, dass es hier um die juristische Möglichkeit des Ausschlusses bestimmter Hersteller geht. Auch wenn es im Mobilfunk- und Kommunikationsbereich durchaus auch andere Hersteller gibt, so ist das nicht in allen Sektoren der Fall. Resilienz darf nicht auf dem Verbot einzelner Hersteller basieren, sondern Betreiber und Hersteller müssen aktiv dabei unterstützt werden Resilienz zu fördern und zu realisieren.

Wir begrüßen grundsätzlich, dass Hersteller von Software für Kritische Infrastruktur und Betreiber Kritischer Infrastrukturen selbst an einer Sicherheitsüberprüfung (bspw. Penetrationstest) mitwirken müssen - dies kann zu einem hohen Maß an Sicherheit und Transparenz führen. Nichtsdestotrotz erscheint die Norm insgesamt aber problematisch und zweifelhaft, z.B. weil die Komponenten nicht direkt vom Hersteller an die Betreiber verkauft werden, sondern im Rahmen einer Wertschöpfungskette - an der Reseller und Systemhäuser und andere Unternehmen teilnehmen - in Kritische Infrastrukturen verbaut werden. Viele Lieferanten wissen nicht (bzw. können gar nicht wissen) in welchen Infrastrukturen ihre Produkte eingesetzt werden - die Pflicht den Betreiber nach Satz 4 zu warnen kann daher gar nicht nachgekommen werden.

Hinzu kommt dass es Kritische Komponenten gar nicht geben sollte (siehe Abschnitt "Resilienz kommt zu kurz"). Die Maßnahmen im § 9b sind für den Schutz Kritischer Infrastrukturen schlichtweg nicht zielführend.

Auf eine Option zum Umgang mit Herstellern, die ein Quasimonopol in einzelnen Sektoren haben, wird im vorliegenden Entwurf nicht eingegangen. Gleiches gilt für die Berücksichtigung von Lieferketten und zuliefernden Herstellern.

Es muss sichergestellt werden, dass Transparenz und Kooperation von Herstellern hinsichtlich des Umgangs mit Sicherheitsschwachstellen, nicht zu einer Schlechterstellung gegenüber Mitbewerbern oder gar der Untersagung des Einsatzes führen dürfen. Die Möglichkeit, dass die

eigenen Produkte in der Folge einer ordnungsgemäßen Meldung einer Schwachstelle vom Einsatz ausgeschlossen werden können wird dazu führen, das Hersteller Schwachstellen trotz gesetzlicher Verpflichtung eher nicht melden werden. Dieses Gesetz setzt so also falsche Anreize.

Die vollständige Untersagung nach Absatz 7 kann in dieser Pauschalität nicht zielführend sein - Fehler passieren, und Hersteller müssen die Chance haben, andere Produkte als die zuvor vom BMI bemängelten, weiterhin am Markt verkaufen zu können - wenn die IT-Sicherheit dieser Produkte nicht zu bemängeln ist.

Auch umgeht diese Regelung das Prinzip der Schutzbedarfsfeststellung und Risikoanalyse - Systeme die z.B. an keine Datennetze angebunden sind müssen auch nicht zwingend in der vom § 9b beschriebenen Variante geprüft werden. Die Entscheidung welche Risiken und Gefahren vom Einsatz eines Systems ausgehen hängt maßgeblich von der Art und Weise der Integration in die Infrastruktur ab und der verarbeiteten Daten.

Resilienz kommt zu kurz: Kritische Infrastruktur vs. Kritische Komponenten

Die Begründung zur Einführung des Begriffs Kritische Komponenten zeigt, dass ein wesentlicher Aspekt des Schutzes Kritischer Infrastrukturen nicht berücksichtigt wurde. Das Zusammenspiel aller relevanten Komponenten in der Architektur ist Wesentlich für die Versorgung, nicht einzelne Komponenten. Da die IT-technische Architektur aber bereits die Anforderungen zur Gewährleistung einer zuverlässigen Versorgung erfüllen muss, bedarf es dieser besonders kontrollierten Kritischen Komponenten aus technischer Sicht nicht.

Gerade der aktualisierte Formulierungsvorschlag des § 2 (13) BSIG aus dem zweiten zum dritten Referentenentwurf legt eine rein politische Motivation nahe. Wo im Mai 2020 noch vorgesehen war, dass das BSI die Liste Kritischer Komponenten aus fachlichen und abgestimmten Erwägungen heraus festlegt, so steht jetzt nur noch lapidar "Alle übrigen kritischen Komponenten werden gesetzlich festgelegt". Eine tatsächliche Verbesserung der Resilienz oder der Versorgungssicherheit ist nicht erkennbar.

Keine Änderung an Strafprozessordnung und am Strafgesetzbuch

Die Abschnitte zur Strafprozessordnung und am Strafgesetzbuch, welche in einem früheren Entwurf enthalten waren, sind in diesem Entwurf nicht mehr enthalten, was wir begrüßen.

Herausgabe von Informationen zur Bewältigung einer erheblichen Störung

Seite 16 - Änderung von § 8b Absatz 4a

Es ist nicht nachvollziehbar, warum im Fall einer erheblichen Störung das BSI zur Herausgabe von Informationen das Einvernehmen mit der für den jeweiligen Betreiber zuständigen Aufsichtsbehörde suchen muss - die Bewältigung der Störung muss Priorität über die Befindlichkeiten der zuständigen Aufsichtsbehörde haben. Unserer Ansicht nach würde es vollkommen ausreichen, die zuständige Aufsichtsbehörde in Kenntnis zu setzen. Dieses Detail halten wir für einen groben handwerklichen Fehler, der die Bewältigung einer erheblichen Störung unnötig verzögert.

KRITIS bekommt Zähne: erhöhte BSI Bußgelder

§ 14 Abs. 2 BSIG

Grundsätzlich begrüßen wir, dass die BSI Bußgeldstelle nun durch die Erhöhung des Bußgeldberechnungsrahmen Zähne bekommt und Kritische Infrastrukturen ernst genommen werden. Die Höhe von maximal 2 Mio. € in Verbindung mit dem § 30 Absatz 2 Satz 3 des Ordnungswidrigkeitengesetz (OWiG) beträgt dann für juristische Personen 20 Mio. € - also die gleiche Summe, die auch in der DSGVO vorgesehen ist.

Dies drängt die Frage auf: Sind Kritische Infrastrukturen genau so wichtig wie das Recht auf informationelle Selbstbestimmung und der Datenschutz der Bürger, oder sind Kritische Infrastrukturen wichtiger?

Die bisher fehlende Evaluierung des IT-Sicherheitsgesetz hätte die Möglichkeit geboten, sich nicht nur unkreativ an der DSGVO zu orientieren, sondern auf Basis von tatsächlicher Evidenz einen Bußgeldrahmen festzulegen, der von KRITIS-Betreibern nicht einfach eingepreist werden kann und tatsächlich wirksam ist.

Deutscher Alleingang: IT-Sicherheitskennzeichen

Die Regelungen des § 9c sind im Kern deckungsgleich mit den in § 9a geregelten Sachverhalten. Genau diese Aufgabe übernimmt bereits der § 9a. Um unnötige Doppelstrukturen und deutsche Alleingänge zu verhindern, muss der § 9c BSIG ersatzlos gestrichen werden. Die Umsetzung des EU Cyber Security Acts (CSA) behandelt bereits notwendige Aspekte zu Zertifizierungen - diese können sich auch auf Consumer Devices erstrecken - daher empfehlen wir die Bindung von Personal (Ressourcen) durch den § 9c zu verhindern und sind der Überzeugung, dass wir diese Themen gesamteuropäisch regeln müssen.

Vorherige Stellungnahme der AG KRITIS

https://ag.kritis.info/2020/05/13/kommentar-zum-neuen-referentenentwurf-des-it-sicherheitsgesetz-2-0-it-sig2/

Bei weiteren sachdienlichen Hinweisen wenden Sie sich bitte an Ihre nächste Kontaktperson der AG KRITIS.

Für Risiken und Nebenwirkungen kontaktieren Sie Ihre Abgeordneten im deutschen Bundestag und Ihren Bundesminister für Heimat, Bau und Inneres.