Bundesverband

Positionspapier

Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme

IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)

Stand: 10. August 2020

Die Ausgangslage

Die deutsche Wirtschaft befindet sich mitten im Prozess der digitalen Transformation. Durch unterschiedliche nationale Regulierungen stellt dies insbesondere für global vernetzte Unternehmen eine enorme Herausforderung dar. Auch nach Einführung des IT-Sicherheitsgesetzes im Jahr 2015 hat sich die Cyber-Bedrohungslage trotz großer Anstrengungen seitens der Wirtschaft, der Wissenschaft und des Staates weiter verschärft. Abwehrmaßnahmen und die Sicherheitsinformationstechnologie haben nicht Schritt gehalten mit den erfolgten Cyberangriffen.

Für Kriminelle, wie auch für fremde Nachrichtendienste sind Cyberangriffe über das Internet hochattraktiv, da eine Vielzahl von Schwachstellen in Soft- und Hardwareprodukten permanent neue Ansatzpunkte für die Entwicklung von Schadprogrammen liefern und durch die Möglichkeiten der Anonymisierung die Zurechenbarkeit von Angriffen erschwert wird.

Umgekehrt hat unsere Gesellschaft ein vitales Interesse an sicheren und resilienten Wirtschaftsunternehmen – und dies beschränkt sich nicht nur auf Betreiber kritischer Infrastrukturen und deren Aufgaben für die öffentliche Daseinsvorsorge, sondern auch für Unternehmen mit hohem Schadenspotential bei Unfällen (z.B. durch Entweichen von Giften) als auch für Unternehmen, deren wirtschaftliches Gedeihen in hohem Maße bedeutsam für das Prosperieren unserer Volkswirtschaft ist.

Cybersicherheit ist ein entscheidender Erfolgsfaktor, da nur ein notwendiges Maß an Sicherheit für Anwender und Kunden Vertrauen in Digitalisierung schafft. Deshalb hat auch die Industrie selbst ein sehr hohes Eigeninteresse, ihre IT-Systeme abzusichern, nicht zuletzt, um die eigene wirtschaftliche Leistungs- und Wettbewerbsfähigkeit sicherzustellen.

Im Rahmen der Digitalisierung von Gesellschaft und Wirtschaft hat sich das Rollenverständnis von Staat und Wirtschaft gewandelt. Es ist erforderlich, dass der Staat angesichts der Bedeutung von Cybersicherheit stärkere Verantwortung in der Abwehr übernimmt, und dass gleichzeitig die Fähigkeiten der Anwender zur Selbstverteidigung durch Hilfe durch Selbsthilfe verbessert werden.

Daher begrüßen wir generell die Zielsetzung der Bundesregierung die Cyberresilienz für den Wirtschaftsstandort Deutschland zu erhöhen – auch über kritische Infrastrukturen hinaus, wie es im Referentenentwurf durch die Einbeziehung von „Infrastrukturen im besonderen öffentlichen Interesse“ vorgeschlagen wird. Damit dies gelingen wird, haben wir nachstehende acht Handlungsempfehlungen für den aktuellen Referentenentwurf zusammengestellt.

Frühzeitig mehr Transparenz zu Regelungen für betroffene Branchen und Unternehmen schaffen

Der Begriff „Unternehmen im besonderen öffentlichen Interesse“ führt nicht zu Klarheit, sondern zu Rechtsunsicherheit bei den möglicherweise betroffenen Unternehmen. Die Einführung des Terminus „Unternehmen im besonderen öffentlichen Interesse“ ist zu unbestimmt. Insbesondere fehlt eine Benennung konkreter Kriterien, warum eine Infrastruktur und deren Anlagen als „im besonderen öffentlichen Interesse“ eingestuft werden. Der Gesetzgeber sollte direkt im Gesetzgebungsprozess des BSI-G die Wesensmerkmale derartiger Infrastrukturen genauer spezifizieren sowie inhaltlich von den kritischen Infrastrukturen i.S.d. § 2 Absatz 10 BSIG-E abgrenzen.

Wünschenswert wäre eine klare gesetzliche Regelung für die betroffenen Branchen anstatt diesbezüglich auf die weitere Konkretisierung durch die ausführende Rechtsverordnung nach § 10 Abs. 5 BSIG-E zu verweisen.

Schwellwerte und Zeitspanne für Implementierung an der Praxis ausrichten

Besorgniserregend ist, dass trotz Einführung des ersten IT-SiGe in 2015 die Bedrohungslage weiter gestiegen ist. Deswegen ist es umso wichtiger, dass bei der Novellierung auf den Erfahrungen der letzten vier Jahre aufgebaut wird. Wir fordern weiterhin den Austausch über eindeutige quantitative und qualitative Schwellenwerte zu Meldepflichten. Vorteilhaft wäre es hier nicht nach Trial and Error vorzugehen, sondern dazu aus den bisherigen praktischen Erfahrungen zu den Meldungen aus den aktuellen KRITIS-Sektoren zu lernen.

Bußgelder – keine Sanktionierung bei unklaren Regelungen

Solange es keine Klarheit zu den konkreten Anforderungen gibt, darf es keine Sanktionierung geben. Dies gebieten allein schon grundlegende Rechtsprinzipien, wie Normenklarheit und Normenbestimmtheit.

Generell sind die Unternehmen aus eigenem Antrieb höchst interessiert IT-Ausfälle zu vermeiden und ihrer unternehmerischen Verantwortung gegenüber Kunden, Aktionären und Investoren nachzukommen. Es bedarf daher keiner weiteren Motivation durch Bußgelder.

Zudem ist eine Analogie zu den Bußgeldern aus der EU-Datenschutzgrundverordnung nicht angemessen (§ 14 Abs. 2 BSIG). Ein Verstoß gegen Datenschutzvorschriften mag vertriebliche Vorteile generieren und daher ist eine Kopplung der Strafen an den Umsatz nachvollziehbar. Eine versäumte Meldepflicht bei IT-Angriffen bringt keinen unternehmerischen Vorteil. Ein gehacktes Unternehmen würde schon mit der Abwehr des Angriffs und zusätzlichen Security Maßnahmen finanziell belastet. Ein zusätzliches Bußgeld wäre daher eine weitere Bürde, die gegebenenfalls der Finanzierung von wirksamen Sicherheitsmaßnahmen entgegensteht.

Informationsanspruch der Unternehmen (§ 4b BSIG-E)

Sofern Meldepflichten notwendig sind, um ein Lagebild zu bekommen, wäre es wünschenswert, dass der Meldeverpflichtung der Unternehmen auch ein Recht gegenübersteht, bevorzugt mit den Informationen versorgt zu werden, die für ihre Sicherheit von Bedeutung sind. Diese Forderung begründet sich in der Einstufung dieser Unternehmen als Teil der Sicherheitsarchitektur der Bundesrepublik Deutschland.

Wir sehen die dringende Notwendigkeit, zukünftig (a) die erhaltenen Informationen einzelfallbezogenen zu beantworten, (b) zielgruppengerecht aufzubereiten und (c) in anonymisierter Form pro Quartal ein detailliertes Lagebild zu publizieren. Dieses gesamtdeutsche Lagebild muss mit der deutschen Wirtschaft sowie weiteren relevanten Stellen geteilt werden, um zur Stärkung der Cyberresilienz Deutschlands einen wichtigen Beitrag leisten zu können.

Grundsätzlich ist es begrüßenswert, dass das BSI zukünftig als allgemeine Meldestelle gemäß § 4b BSIG-E fungieren soll. Es wird hiermit der Versuch unternommen, eine dringend benötigte freiwillige anonyme Meldeplattform für IT-Sicherheitsvorfälle aufzubauen. Es ist ebenfalls von Vorteil, dass hierfür auf etablierte technische Lösung wie die Malware Information Sharing Platform (MISP) zurückgegriffen werden soll, wie aus der Begründung des Referentenentwurfes hervorgeht. Jedoch ist die Beschreibung der Meldemöglichkeiten in § 4 Abs. 2 S. 2 BSIG-E unzulänglich. Eine klar definierte Anforderung an die Ausgestaltung einer solchen Meldeplattform ist dringend notwendig, um das Vertrauen der Unternehmen in die Plattform zu stärken.

ASW Bundesverband | Allianz für Sicherheit in der Wirtschaft e.V.
Bayerischer Platz 6 | 10779 Berlin
Telefon +49 (0)30 246 37 175 | Telefax +49 (0)30 200 77 056
info@asw-bundesverband.de | www.asw-bundesverband.de

Zudem fehlt es an einer klaren Verpflichtung des BSI, die zugelieferten Informationen in einem bestimmten kurzen Zeitraum auszuwerten und mit Dritten (Unternehmen) zu teilen. Nur so kann es gelingen, Malwareverbreitung einzudämmen und potenzielle Schwachstellen von Systemen vor einem möglichen Angriff zu schließen. Der Informationsfluss darf keine Einbahnstraße sein. Eine Hortung von Informationen beim BSI ohne gesetzliche Verpflichtung des Rückflusses der Cyber Threat Intelligence in Form von rechtzeitigen Warnungen stellt ansonsten einen Mehraufwand für die Unternehmen ohne sicherheitsfördernden Nutzen dar.

Daher ist es zwingend erforderlich das BSI zur Informationsweitergabe zu verpflichten. Das in § 4b Abs. 3 BSIG-E eingeräumte Ermessen („kann") muss zu einer gebundenen Entscheidung („muss") abgeändert werden. Der Gesetzestext definiert die Meldewege durch Dritte an das BSI nicht eindeutig. Ebenso fehlt es an der gesetzlichen Definition des Informationsflusses vom BSI an die Unternehmen. Eine entsprechende Ergänzung ist erforderlich. Insofern kann eine Angleichung des § 4b BSIG-E an die Ausgestaltung der Rolle des BSI als zentrale Meldestelle für die IT-Sicherheit des KRITIS-Betreiber gemäß § 8b BSIG-E angestrebt werden.

Konkrete Hilfestellungen und gemeinsames Krisenmanagement: Betrieb einer Plattform durch Beliehene als konkreten Vorschlag

Im Angriffsfall bedarf es einer konkreten Hilfestellung durch das BSI. Es sollte daher über ein Rahmenwerk zur Ergänzung bzw. Erweiterung der mobilen Eingreiftruppen durch Public-Private-Partnerships nachgedacht werden. Dazu gehört auch die Einbindung der Wirtschaft in das Nationale Cyber-Abwehrzentrum und ein Konzept zur gemeinsamen Incident Response von Staat und Wirtschaft. Als Beispiel kann die US National Cyber-Forensics & Training Alliance genannt werden, wo staatliche und privatwirtschaftliche Akteure gemeinsam erfolgreich an der Aufklärung von Cyberattacken und an der Analyse von Tatwerkzeugen arbeiten.

Unter den vorgenannten Gesichtspunkten ist es erforderlich, dass das Cyber-Threat-Intelligence-System überdacht wird. Aus dem derzeitigen Gesetzestext geht nicht hervor, dass das BSI dazu verpflichtet sein wird, Cyber Threat Intelligence in Echtzeit auszutauschen. Es muss das Ziel sein, diese Informationen möglichst vielen Unternehmen, nicht nur den KRITIS-Betreibern oder Betreibern von Infrastruktur im besonderen öffentlichen Interesse, zukommen zu lassen. Aus diesem Grunde fordert die ASW, eine solche Plattform da anzusiedeln, wo die Ressourcen und das Knowhow über Einrichtung und Betrieb von Cyber-Threat-Intelligence-Plattformen besteht. Diese Aufgabe können die zahlreich in Deutschland vorhanden und international angesehenen Cybersicherheitsunternehmen übernehmen.

Erforderlich hierfür wäre eine klare Regelung, welche Rolle diese Cybersicherheitsunternehmen als Betreiber der Plattformen einnehmen sollen. Ihre Aufgaben und Befugnisse müssen klar festgelegt werden. Insofern ist die Schaffung einer gesetzlichen Regelung erforderlich, die nachfolgende Aspekte zum Gegenstand haben soll:

- Der Rechtscharakter der Einbindung der Cybersicherheitsunternehmen soll als Beliehenenschaft ausgestaltet sein. Die Beleihung ist dem BSIG nicht fremd und findet sich im § 9 BSIG-E bezüglich der Zertifizierung von IT-Sicherheitsdienstleistern. Hierbei erfolgt die Zertifizierung durch das BSI, die Prüfung hinsichtlich der Erfüllung der Anforderungen jedoch durch den Beliehenen. Ausgehend hiervon sollte das BSI geeignete Cybersicherheitsunternehmen als Plattformbetreiber zertifizieren.

- Erforderlich ist dann eine Registrierung von Unternehmen, die vom Informationsfluss (z.B. Warnung vor Sicherheitslücken) durch die Plattform profitieren wollen. Die Erfüllung von Mindeststandards der Plattformteilnehmer schafft gegenseitiges Vertrauen in die Technologie. Die hierfür erforderlichen Zulassungsbeschränkungen über die Teilnahme an einer Plattform sollen durch das BSI in einem Anforderungskatalog festgelegt werden. Die Prüfung der Erfüllung der Anforderungen im konkreten Einzelfall der Zugang des erbittenden Unternehmens würde dem beliehenen Cybersicherheitsunternehmen (Plattformbetreiber) zukommen.

- Dem BSI kommt die Rolle der Aufsichtsbehörde zu, worüber Kontroll- und Steuerungsrechte des Staates gewahrt werden. Das BSI soll folglich ein Fachweisungsrecht gegenüber dem Beliehenen besitzen.

- Verortung: Die Beleihung bedarf einer gesetzlichen Grundlage, welche im § 4b BSIG-E aufgenommen werden soll. Die weitere Ausgestaltung soll in einer Verordnung geregelt werden.

Staatliche Nutzung von Schwachstellen begrenzen

Gewonnene Erkenntnisse über Schwachstellen müssen unbedingt mit den KRITIS Unternehmen und den Unternehmen im besonderen öffentlichen Interesse geteilt werden. Generell sollte gelten, dass staatliche Stellen entsprechend angewiesen werden, bekanntgewordene Sicherheitslücken unverzüglich zu melden. Wir haben Verständnis für das Bedürfnis zur Nutzung von Schwachstellen, um Terrorismus und Kriminalität effektiv bekämpfen zu können. Daher muss dies in begrenztem Umfang – unter Anwendung von klaren Regeln und Transparenz – ermöglicht werden. Beispielhaft könnten für die Nutzung von Lücken eine zeitliche Begrenzung oder Schwellwerte bezüglich der Anzahl bzw. der Kritikalität der betroffenen Systeme festgelegt werden. Im Zweifelsfall muss gelten: Schließen statt Nutzen.

Qualitätssicherung über Stichprobenüberprüfung von IT-Komponenten

Wir unterstützen das Vorhaben der Bundesregierung im Projekt IT-Sicherheitskennzeichen ein Gütesiegel für IT-Sicherheit einzuführen.

Perspektivisch müssen alle Wertschöpfungspartner entlang der Cybersicherheitswertschöpfungskette (Hersteller von Routern, Switches, Kernkomponenten aus der Produktion) entsprechend ihrer Verantwortung für die Gewährleistung von IT-Sicherheit verpflichtet werden – dies betrifft im besonderen Maße Hard- und Softwarehersteller. Grundsätzlich ist die Erfassung der Kernkomponenten sowie der Hersteller ein erster richtiger Schritt.

Wir verstehen die Bestrebungen, das BSI als eine Konformitätsbewertungsstelle zu etablieren. Angesichts der Erfahrungen rund um die Zertifizierung von IT-Grundschutz und ISO27001 warnen wir aber vor den Problemen im Kontext „Akkreditierungsstellen“. Weder erscheint eine Einordnung des BSI unter der DaKKS (Deutsche Akkreditierungsstelle GmbH) sinnvoll, noch ist bisher der Weg einer zweiten parallellaufenden Akkreditierungsstelle durch europäisches Recht vorgesehen.

Zudem begrüßen wir den in § 7a BSIG-E eingeschlagenen Weg zur Untersuchung der Sicherheit der Informationstechnik. Dies kann aber nur gelingen, wenn ein Weg aufgezeigt wird, wie wirklich allen Marktteilnehmern die gleichen Bedingungen geboten werden. Es ist zwingend eine komplette Abdeckung des Marktes erforderlich. Keinesfalls darf es dazu führen, dass z.B. kleine deutsche Start-ups Marktnachteile verlieren, weil sie nicht zeitnah

die gleichen Sicherheitsnachweise durch das BSI erhalten wie etablierte Anbieter. Kernkomponenten müssen regelmäßig getestet werden. Der Fokus muss neben dem Test von Prototypen auf Stichprobenüberprüfung von Routern und Switches aus der laufenden Produktion liegen, denn dies sind die Komponenten, die in den kritischen Infrastrukturen tatsächlich verbaut werden. In anderen Kontexten sind solche Stichprobenkontrollen bei Gefahrstoffen oder Dual-Use-Produkten seit Jahren etabliert. Solche Konzepte könnten übertragen werden. Dies kann auch in Form von Public-Private-Partnerships realisiert werden. Wir fordern eine Konkretisierung des Vorgehens, wenn der Einsatz von Produkten untersagt wird, diese aber bereits im Einsatz sind. Müssen diese dann auch nachträglich entfernt werden? In welchem Zeitraum ist dies erforderlich? Wird es Ausnahmetatbestände geben, z.B. wenn der Tausch eines Produktes zwangsläufig zu Architekturänderungen führen würde? Wird es die Möglichkeit geben, den Austausch durch zusätzliche risikomitigierende Maßnahmen zu vermeiden? Wer trägt bei einer solchen Entscheidung die Kosten für den Umbau?

Die letzten Jahre haben weltpolitisch leider gezeigt, dass alte, als unverbrüchlich geltende staatliche Beziehungen ihren Wert verlieren und auch heute bereits die Auswahl von Produkten in zunehmendem Maße international, politisch beeinflusst werden. Betreiber benötigen hier Investitionssicherheit und die Sicherheit nicht indirekt zum politischen Spielball zu werden.

Stärkung internationaler politischer Zusammenarbeit zur Bekämpfung der Cyberkriminalität

Im Rahmen der Cyberaußenpolitik muss sich die Bundesregierung dafür einsetzen, dass jeder Staat seine Bemühungen zur Erhöhung der Cybersicherheit intensiviert und kritische IT-Infrastrukturen besser gegen Attacken geschützt werden. Außerdem muss intensiv gegen Cyberkriminalität vorgegangen werden. Mittelfristiges Ziel muss die Verabschiedung eines verbindlichen Abkommens für verantwortliches Handeln im Cyberraum sein. Darüber hinaus bedarf es eines intensiveren Ressourcen- und Kapazitätsaufbaus im Verantwortungsbereich der Staaten, um – gerade häufig auch supranationale – Cyberkriminalität wirksam zu bekämpfen. Hier muss auf internationaler Ebene, über die Multi-Stakeholder-Ansätze hinaus, noch intensiver zusammengearbeitet werden.

ASW Bundesverband | Allianz für Sicherheit in der Wirtschaft e.V.
Bayerischer Platz 6 | 10779 Berlin
Telefon +49 (0)30 246 37 175 | Telefax +49 (0)30 200 77 056
info@asw-bundesverband.de | www.asw-bundesverband.de