Bundesverband

Kommentierung: Prof. Timo Kob, Volker Wagner

IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)

Zweites Gesetz zur Erhöhung der Sicherheit informations-technischer Systeme

Stand: 8. Juli 2019

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 Cyberangriffen.

Für Kriminelle wie 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.

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 und 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 zur 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 Handlungsempfehlungen für den aktuellen Referentenentwurf zusammengestellt.

Frühzeitig mehr Transparenz zu Regelungen für betroffene Branchen und Unternehmen schaffen

Der Begriff „Infrastruktur im besonderen öffentlichen Interesse“ führt nicht zu Klarheit, sondern zu Rechtsunsicherheit bei den möglicherweise betroffenen Unternehmen. Die Einführung des Terminus „Infrastrukturen 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 IT-Sicherheitsgesetzes die Wesensmerkmale derartiger Infrastrukturen genauer spezifizieren sowie inhaltlich von den kritischen Intrastrukturen i.S.d. § 2 Absatz 10 BSIG sowie von „Cyberkritikalität“ i.S.d. § 8g BSIG n.F. 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 zu verweisen.

Durch § 8f würden Betreiber von Infrastrukturen im besonderen öffentlichen Interesse mit den gleichen Auflagen versehen wie KRITIS-Infrastrukturen.

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

Ob dies in jeder betroffenen Branche sinnvoll ist, sollte nach genauer Klärung der betroffenen Branchen zu diskutieren sein. Es sollte daher die Möglichkeit einer Abstufung zwischen KRITIS-Infrastrukturen und Infrastrukturen im besonderen öffentlichen Interesse geben, die im Einvernehmen von Branchenvertretern und staatlichen Institutionen zu fixieren ist.

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 Einführung der zweiten Welle auf den Erfahrungen der letzten vier Jahre aufgebaut wird. Insbesondere fordern wir die gemeinsame Festlegung von eindeutigen quantitativen und qualitativen Schwellwerten zu Meldepflichten. Vorteilhaft wäre es hier nicht 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.

Generell sind die Unternehmen aus eigenem Antrieb höchstinteressiert 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 von Cyber kriminellen Handlungen betroffenes Unternehmen würde schon mit der Abwehr des Angriffs und zusätzlichen Security Maßnahmen finanziell belastet. Sofern Personenbezogene Daten dabei beteiligt sind, greifen ohnehin schon die Regeln der DS-GVO. Ein zusätzliches Bußgeld wäre daher eine weitere Bürde, die gegebenenfalls der Finanzierung von Security Maßnahmen entgegensteht.

Informationsanspruch der KRITIS Unternehmen

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 auf Seiten des BSI die dringende Notwendigkeit, (a) zukünftig 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.

Insbesondere sollte geregelt werden, wie die Meldung von Cybersicherheitsvorfällen zwischen den verschiedenen Meldestellen abgeglichen werden sollen und für Transparenz gesorgt wird. Aus unserer Sicht sollte der Grundsatz gelten: Datenschutz Incidents müssen an die Datenschutzbehörde erfolgen, Cybersicherheitsvorfälle an das BSI.

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

Stärkung internationaler politischer Zusammenarbeit zur Bekämpfung der Cyber-kriminalität

Eine Harmonisierung des IT SiGe mit europäischen und internationalen Gesetzen zur IT Sicherheit ist notwendig für international agierende Konzerne. Nicht abgestimmte, nationalstaatliche Einzelmaßnahmen können gerade für weltweit tätige Unternehmen enorme zusätzliche Kosten und damit Wettbewerbsnachteile für deutsche Unternehmen bedeuten.

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 sowie intensiv gegen Cyberkriminalität vorgegangen wird. 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 Cyberkriminalität wirksam zu bekämpfen. Hier muss auf internationaler Ebene, über die Multi-Stakeholder-Ansätze hinaus, noch intensiver zusammengearbeitet werden.

Konkrete Hilfestellungen und gemeinsames Krisenmanagement

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 dann 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 an der Aufklärung von Cyberattacken und an der Analyse von Tatwerkzeugen arbeiten.

Der Referentenentwurf vernachlässigt bei der Erarbeitung von Krisenreaktionsplänen durch das BSI gemeinsam mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und der jeweils zuständigen Aufsichtsbehörde des Bundes die Beteiligung einer wichtigen Akteursgruppe – die betroffenen Betreiber Kritischer Infrastrukturen, Betreiber weiterer Anlagen im öffentlichen Interesse sowie den Betreibern und den Lieferanten der Kernkomponenten.

Staatliche Nutzung von Schwachstellen begrenzen

Gewonnene Erkenntnisse über Schwachstellen müssen unbedingt mit den KRITIS-Unternehmen 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. Die Ausnutzung von Sicherheitslücken durch staatliche Stellen stellt eine Vertrauenshypothek in eine sichere Datenverarbeitung dar. Es sollte in Betracht gezogen werden, dass auch staatliche Stellen anderer Länder die gleichen Sicherheitslücken bereits kennen und ggf. auch zum Nachteil von KRITIS-Unternehmen ausnutzen können. Der Vorteil für nationale staatliche Stellen scheint daher nur eingeschränkt zu existieren und sollte gegenüber der genannten Hypothek abgewogen 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

Qualitätssicherung über Stichprobenüberprüfung von IT-Komponenten

Wir unterstützen das Vorhaben der Bundesregierung im Projekt IT-Sicherheitskennzeichen an der Einführung eines Gütesiegels für IT-Sicherheit zu arbeiten.

Perspektivisch müssen alle Wertschöpfungspartner entlang der Cybersicherheitswertschöpfungskette (Hersteller von Routern, Switches, Kernkomponenten aus 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. Eine reine Vertrauenswürdigkeitserklärung für Hersteller von KRITIS-Kernkomponenten ist aus unserer Sicht jedoch nicht ausreichend. Die Haftungssituation sollte im Gesetz eindeutig geklärt werden, um die Hersteller in Verantwortung nehmen zu können.

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.

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