DAS NEUE IT-SICHERHEITSGESETZ 2.0

Dr. Manfred Rack
Rechtsanwalt

Inhaltsverzeichnis

DAS NEUE IT-SICHERHEITSGESETZ 2.0

Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme
In Kraft getreten am 29.Mai 2021, BGBI. 2021 Teil 1 Nr. 25

Das neue IT-Sicherheitsgesetz wurde vom Bundestag am 23.04.2021 verabschiedet und vom Bundesrat am 7.5.2021 gebilligt. Es enthält durch Änderungen des BSIG zahlreiche neue Pflichten für Unternehmen sowie Anforderungen an das Bundesamt für die IT-Sicherheit (BSI) zur Stärkung der IT-Sicherheit in Deutschland. Der Gesetzgeber betont, dass die Gewährleistung von Cyber-Sicherheit nicht statisch sein kann, sondern eine ständige Anpassung und Weiterentwicklung der Abwehrstrategien erforderlich ist. Die Erfahrungen aus der Anwendung des 1. IT-Sicherheitsgesetzes sowie den Erkenntnissen aus Cyberangriffen bestimmen die Neuregelungen des IT-Sicherheitsgesetzes.

Erweiterter Kreis der Betreiber kritischer Infrastrukturen

Erweitert wurde der Kreis der Betreiber kritischer Infrastrukturen und der Verpflichteten nach dem BSIG. Nach den bisherigen Definitionen der BSI-KritisV sind rund 1.600 Kritis-Betreiber nach § 8a und 8b BSIG zur IT-Sicherheit verpflichtet. Mit der Definitionserweiterung kommen etwa 240 weitere Kritis-Betreiber dazu. Sie sind zum größten Teil der Stromerzeugung zuzurechnen. 160 sind dem Kritis-Sektor Energie zuzuordnen. Unternehmen haben sich selbst zu prüfen, ob sie unter die BSI-KritisV fallen, vor allem ob sie die Schwellenwerte erreichen. Über die wichtigsten Neuerungen soll im Folgenden ein Überblick vermittelt werden.

Neue Befugnisse des BSI gegenüber dem Bund

Neue Definitionen enthält **§ 2 BSIG.** Nach **§ 2 Abs. 3 Satz 1 BSIG** wird die Kommunikationstechnik des Bundes definiert. Nach **§ 4a BSIG** wird das BSI befugt, die Sicherheit der Kommunikationstechnik des Bundes und ihrer Komponenten, einschließlich technischer Infrastrukturen zu kontrollieren. Dem BSI ist Zugang zu gewähren. Es hat das Ergebnis seiner Kontrollen in Form von Vorschlägen zur Verbesserung der Informationssicherheit vorzuschlagen. Das BSI ist befugt gemäß § 8 BSIG Mindeststandards festzulegen.

Neue Erweiterungen des IT-Sicherheitsgesetzes auf Systeme zur Angriffserkennung

Definiert werden in § 2 BSIG IT-Produkte im Sinne dieses Gesetzes als Softwareprodukte sowie alle einzelnen oder miteinander verbundenen Hardwareprodukte. In **§ 2 Abs. 9b BSIG** werden Systeme zur Angriffserkennung im Sinne dieses Gesetzes definiert, als durch technische Werkzeuge und organisatorische Einbindungen unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch den Abgleich, der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten.

An dieser Definition wird das Hauptproblem der Angriffserkennung deutlich. Erforderlich sind Erfahrungssätze darüber, unter welchen tatsächlichen Umständen der Rückschluss auf einen Angriff erlaubt ist. Die Indizien und Erfahrungssätze zusammen lassen Rückschlüsse zu, ob ein Cyber-Angriff bevorsteht.

Neue Erweiterungen der IT-Sicherheit auf kritische Komponenten

Neu in § 2 BSIG ist die Erweiterung der Sachverhalte nach **§ 13 BSIG** auf kritische Komponente, unter denen das Gesetz IT-Produkte versteht, die in kriti-

schen Infrastrukturen eingesetzt werden, von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit dieser IT-Produkte zu einem Ausfall oder zu einer erheblichen Beeinträchtigungen der Funktionsfähigkeit kritischer Infrastrukturen oder zur Gefährdung für die öffentliche Sicherheit führen können. Der Anwendungsbereich des Gesetzes wird danach **auf kritischen Komponenten ausgeweitet.**

Neue IT-Sicherheitspflichten für „Unternehmen im besonderen öffentlichen Interesse“

In **§ 2 Abs. 14 BSIG** werden die **Pflichten des BSIG auf „Unternehmen im besonderen öffentlichen Interesse“ ausgeweitet,** die nicht Betreiber kritischer Infrastrukturen nach Abs. 10 sind, sondern nach § 60 Abs. 1 Nr. 1 u. 3 der Außenwirtschaftsverordnung geregelt sind, wozu zum Beispiel Rüstungsexporte gehören. Außerdem zählen die größten Unternehmen in Deutschland dazu, die von erheblicher volkswirtschaftlicher Bedeutung hinsichtlich der Wertschöpfung sind und als dritte Gruppe zählen Störfallbetriebe dazu, die der Störfallverordnung unterfallen. Die „Unternehmen im besonderen öffentlichen Interessen“ werden durch die Rechtsverordnung nach § 10 Abs. 5 BSIG bestimmt.

Neue Erweiterung des IT-Sicherheitsgesetzes auf den Verbraucherschutz

Neu in **§ 2 Abs. 14a BSIG** ist die **Regelung des Verbraucherschutzes** im Bereich Sicherheit in der Informationstechnik. Durch Beratung und Warnungen sollen Verbraucher in Fragen der Sicherheit in der Informationstechnik über unzureichende Sicherheitsvorkehrungen informiert werden. Nach § 4 BSIG wird die Regelung in § 4b BSIG und in § 8b BSIG ergänzt. Die **Aufgaben als zentrale Meldestelle werden erweitert.** Die gemeldeten Informationen zu Sicherheitslücken, Schadprogrammen und IT-Sicherheitsvorfällen sind zentral zu sammeln und auszuwerten. Sie sind zu einem Gesamtlagebild der Cyber-Sicherheit in Deutschland zusammenzufassen. Bisher fehlte eine Rechtsgrundlage für die **Übermittlung von Informationen durch Dritte aus der Wirtschaft oder durch Einzelpersonen an das BSI**. Sie wird nunmehr in § 4b BSIG begründet. Die Informanten sind nach § 4b BSIG nicht zur Meldung verpflichtet. Die Meldungen sind **freiwillig** und **anonym** möglich, um Hemmschwellen zu senken. Nach § 4b Abs. 3 BSIG soll das Bundesamt **andere Behörden, Dritte und die Öffentlichkeit** über Gefahren der Cyber- und Informationssicherheit **informieren**. Nach § 4b Abs. 2 BSIG werden die meldenden Personen geschützt. Das Bundesamt soll nach § 4b Abs. 3 BSIG die Meldungen ausnutzen, über Sicherheitslücken, Schadprogramme und erfolgte und versuchte Angriffe informieren, erforderlichenfalls die Öffentlichkeit nach § 7 BSIG warnen und die Betreiber kritischer Infrastrukturen und „Unternehmen im öffentlichen Interesse“ unterrichten.

§ 7 BSIG wird zur Stärkung der neuen **Aufgabe des Verbraucherschutzes** gemäß § 3 Nr. 14a BSIG geändert. Nach § 7 Abs. 1 Satz 1 Nr. 2 und Abs. 2 Satz 1 BSIG konnte bisher das BSI Produktempfehlungen nur für IT-Sicherheitsprodukte aussprechen, zum Beispiel für Virenscanner. Nunmehr wird im Interesse einer erhöhten Verbrauchertransparenz diese Befugnis des BSI allgemeiner für informationstechnische Produkte und Dienste durch § 7 Abs. 1 Satz 1 Nr. 1a BSIG ausgeweitet, zum Beispiel auf Router oder Smart-TV.[1]

Nach **§ 7a BSIG** kann das BSI zur Erfüllung seiner Aufgaben **Produkte und Systeme** untersuchen und Informationen über bestehende Sicherheitsrisiken auswerten, von Herstellern die notwendigen Auskünfte verlangen. Auch diese Befugnis dient dem Verbraucherschutz im Bereich der Informationssicherheit. Das BSI ist auf die **Informationen der IT-Hersteller durch Bereitstellung von Informationen angewiesen.** Diese Regelung zum Auskunftsverlangen an Hersteller entspricht den Befugnissen im Lebensmittel- und Chemikalienrecht. In der zunehmenden Digitalisierung ist der Verbraucher auf diese Informationen zur IT-Sicherheit angewiesen. Sichergestellt werden muss durch das BSI, dass die IT-Produkte nur die vom Hersteller

1 BT-Drs. 19/26106, S. 67.

zugesagten Funktionalitäten haben. Die Regelungen entsprechen nach der Gesetzesbegründung der Aufgabe des Staates und seiner Schutzpflicht gegenüber den Bürgern, indem er diese vor jeglichen Gefahren warnen und schützen muss.[2]

Zuwiderhandlungen gegen die Auskunftsverpflichtungen lösen ordnungswidrigkeitliche Sanktionen nach § 14b BSIG aus.

§ 7 Abs. 3 BSIG enthält eine Zweckbindung für die Erkenntnisse aus den Untersuchungen und den Auskünften. Die Digitalisierung soll durch hohe Sicherheitsstandards gefördert werden.

Nach **§ 7a Abs. 5 BSIG** hat das BSI die Befugnis, die Öffentlichkeit über verweigerte Auskünfte des IT-Herstellers zu informieren. Damit soll Druck auf die Hersteller ausgeübt werden, dem Auskunftsverlangen nachzukommen. Verweigert ein Hersteller die Auskunft, droht ihm ein Bußgeld nach § 14 Abs. 2 Nr. 1b BSIG für die Zuwiderhandlung einer vollziehbaren Anordnung nach § 7a Abs. 1 BSIG.

Die neue Befugnis des BSI zur Detektion von Sicherheitsrisiken für Netz- und IT-Sicherheit und von Angriffsmethoden durch Portscans

Nach **§ 7b BSIG** räumt das Gesetz dem Bundesamt die Befugnis ein im Rahmen seiner Aufgaben nach § 3 BSIG Sicherheitslücken und andere Sicherheitsrisiken zu ermitteln (Detektion), beschränkt auf Unternehmen kritischer Infrastrukturen, Anbieter digitale Dienste und der Unternehmen im besonderen öffentlichen Interesse (nach § 2 Abs. 10, 11 und 14 BSIG. **Befugt ist das Bundesamt zu sogenannten Portscans.** Vorausgesetzt wird, dass Tatsachen die Annahme rechtfertigen, dass die informationstechnischen Systeme „ungeschützt" im Sinne von § 7b Abs. 2 BSIG sein können und dadurch in ihrer Sicherheit oder Funktionsfähigkeit gefährdet sein können. Zu verstehen ist ein Port in der Programmierung als eine logische Verbindungsstelle und im spezifischen bei Benutzung des Internetprotokolls (IP) tcp/ip, die Technik, wie ein Clientprogramm ein bestimmtes Server-Programm auf dem Computer innerhalb eines Netzwerks adressiert. Ein Port stellt einen Anschluss an ein System dar. Mit einem Portscanner lässt sich testen, ob bei Ports eine IP-Adresse offen ist. Offene Ports sind eine Gefahr für Router, Server und Geräte. In der Portkommunikation können Sicherheitslücken durch Software- und Konfigurationsfehler vorkommen. Diese Sicherheitslücken müssen unverzüglich geschlossen werden. Sicherheitslücken werden regelmäßig auf allgemein zugänglichen Plattformen im Internet veröffentlicht und sind im Sinne des § 7b Abs. 2 BSIG öffentlich bekannt.[3] Befugt ist das Bundesamt nur bei den genannten Adressaten, den Betreibern kritischer Infrastruktur, digitaler Dienste und den „Unternehmen im besonderen öffentlichen Interesse". Das Bundesamt erstellt eine Liste von IP-Adressbereichen und passt diese an.

Bei Portscans handelt es sich um ein Verfahren, das grundsätzlich jedermann zugänglich ist und das regelmäßig auch zu Angriffszwecken von Kriminellen genutzt wird. Das Bundesamt ist an den Sicherheitslücken interessiert, um sie zu schließen, während Kriminelle daran interessiert sind, die Sicherheitslücken zu missbrauchen und sich unbefugten Zugang über einen lückenhaften Port zu verschaffen. Zum Zwecke der Detektion sendet das Bundesamt Anfragen an einen oder mehrere Ports der Betreiber eines informationstechnischen Systems und wertet die vom System gelieferte Antwort aus.[4] Beim Portscan geht es darum, dass die Sicherheitslücken vom Bundesamt erfasst werden, noch bevor sie von Kriminellen missbraucht werden können. Allen Adressaten des BSIG werden technische Merkmale zur Verfügung gestellt, damit diese geeignete Vorkehrungen treffen können, um einen nach dieser Vorschrift durchgeführten Portscan im Rahmen der Befugnisse des Bundesamtes von einem unbefugten Angriff zu unterscheiden.[5]

2 BT-Drs. 19/26106, S. 68.

3 BT-Drs. 19/26106, S. 69 zu „Portscan".

4 BT-Drs. 19/26106, S. 69.

5 BT-Drs. 19/26106, S. 70.

Im Ergebnis muss man die Maßnahme des Bundesamtes beim Portscannen als simulierten Angriff verstehen, um die Lücke zeitlich noch vor Cyberkriminellen im System zu erfassen. Portscans müssten deshalb von Betreibern kritischer Infrastruktur unterstützt werden.

Werden Sicherheitslücken durch den Portscan erkannt, sind die für das informationstechnische Systeme Verantwortlichen darüber zu informieren.

In **§ 7 Abs. 2 BSIG** wird der Begriff **„ungeschützt"** definiert. Die Definition der **„Sicherheitslücke"** findet sich in § 2 Abs. 6 BSIG. Erfasst werden Kommunikationsnetze, als auch informationstechnische Systeme, die ohne Schutzmechanismen arbeiten oder deren Systeme faktisch wirkungslos sind. Als Beispiel führt die Gesetzesbegründung den Fall an, dass vom Hersteller ein stets identisches Passwort vergeben wird.[6] Aus § 7 Abs. 3 BSIG ergibt sich die Pflicht des Bundesamtes über die Sicherheitsprobleme zu informieren und zwar zunächst die Betriebsverantwortlichen, hilfsweise die Provider.

Die Befugnis des BSI zu Honeypots

Nach § 7b Abs. 4 BSIG wird **das Bundesamt befugt** sogenannte **aktive Honeypots zu betreiben,** dass gestellte Sicherheitslücken aufweist und Angreifer mit Schadsoftware anlockt, wodurch das Bundesamt in die Lage versetzt wird, Schadsoftware zu analysiere, kennenzulernen, Funktionsweise und Infektionswege nachvollziehen zu können, um sich selbst in die Lage zu versetzen, vor neuen Angriffsmethoden zu warnen und Systeme kritischer Infrastrukturen oder die Bundeseinrichtung zu schützen.

Die Befugnis des BSI zur Anordnung an Diensteanbieter zur Beseitigung von Störungen

Nach **§ 7c BSIG** ist das Bundesamt gegenüber Diensteanbietern mit mehr als 100.000 Kunden befugt, anzuordnen, dass der Anbieter die in § 109a Abs. 5 und 6 des TKG zu bezeichnende Maßnahmen trifft oder technische Befehle zur Bereinigung von einem konkret benannten Schadprogramm an Betroffene informationstechnischer System verteilt. Danach werden die Störungen bei der Nutzung des Telekommunikationsdienstes geregelt. Der Diensteanbieter darf die Nutzung zur Beendigung der Störung einschränken, umleiten oder unterbinden, soweit dies erforderlich ist, um die Beeinträchtigung zu beseitigen oder zu verhindern. Nach § 109a Abs. 6 TKG darf der Diensteanbieter den Datenverkehr zu Störungsquellen einschränken oder unterbinden, soweit dies erforderlich ist. Die Maßnahmen des Dienstanbieters stehen in dessen Ermessen. Deshalb wird das Bundesamt berechtigt, zur Aufrechterhaltung betriebsfähiger sicherer IT-Strukturen eine **bundesweit einheitliche Gefahrenabwehr** zu ordnen und zwar zur Aufrechterhaltung der öffentlichen Sicherheit und Ordnung im Bereich des Rechts der Wirtschaft gemäß Art. 74 Abs. 1 Nr. 11 GG. Ob der Diensteanbieter die Maßnahmen zur Beseitigung der Störung ergreift oder nicht, darf nicht seinem Ermessen überlassen bleiben. Das Bundesamt muss bundesweit einheitlich zur Gefahrenabwehr vorgehen können. Eine erfolgreiche Gefahrenabwehr ist nur durch eine zentrale Stelle wie das Bundesamt gewährleistet. Als Beispiel nennt die Gesetzesbegründung Gefahren durch Botnetze. Botnetze entstehen durch unbemerkte Installation einer Schadsoftware auf dem Datenverarbeitungssystem eines Nutzers. Ein Täter hat vollständigen Zugriff auf die kompromittierten Systeme. Sie werden ohne Wissen der Nutzer durch den Täter kontrolliert und gesteuert. Das Mittel der Tat sind sogenannte Command-and-Control-Server (C&C-Server). Die Netze aus C&C-Server und Bots werden Botnetze genannt. Der Täter kann Daten der Nutzer von Bots ausleiten und das Botnetz für DDoS-Angriffe (Distributed-Denial-of-Service) einsetzen. Diese Art von Angriffen haben sich nach dem Bundeslagebild Cybercrime im Vergleich zum Vorjahr verdoppelt.[7] In aller Regel werden Nutzerdaten ausgeleitet. Verletzt werden die Vertraulichkeit und die Verfügbarkeit der Systeme. Die Anordnungsbefugnis ist begrenzt auf Anbieter, die mehr als 100.000 Kunden haben. Nach

6 BT-Drs. 19/26106, S. 71.

7 BT-Drs. 19/26106.

§ 8 BSIG legt das BSI im Einvernehmen mit den **Ressorts Mindeststandards für die Sicherheit der Informationstechnik des Bundes von Stellen des Bundes, Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts auf Bundesebene und öffentliche Unternehmen, die mehrheitlich im Eigentum des Bundes stehen und die IT-Dienstleistungen für Bundesverwaltung erbringen, fest.** Erreicht werden soll ein gleich hohes IT-Sicherheitsniveau bei jeder Einrichtung des Bundes unabhängig von der Organisationsform. Kontrollrechte des Bundesamtes werden eingeführt, um das gleich hohe IT-Sicherheitsniveau zu halten. Ein einheitliches Schutzniveau wird angestrebt. Nach § 8 BSIG erarbeitet das Bundesamt verbindliche Mindeststandards für die Sicherheit der Informationstechnik des Bundes. Ebenfalls ist neu geregelt, dass neben den Stellen des Bundes die Mindeststandards zukünftig ausdrücklich auch für IT-Dienstleister gelten, soweit sie Dienstleistungen für die Kommunikationstechnik des Bundes erbringen.

Die neue Regelungen des Beginns der Verpflichtung von Betreibern kritischer Infrastruktur

Neu sind ebenfalls weitere Kontrollrechte des Bundesamtes, ob die hohen IT-Sicherheitsstandards eingehalten werden. In der gesamten Bundesverwaltung soll die Einhaltung des Mindeststandards ein einheitliches Schutzniveau und eine wirksame Prävention gegen Angriffe und Cyber-Sicherheitsvorfälle erreicht werden. Das BSI soll möglichst frühzeitig bei wesentlichen Digitalisierungsvorhaben einbezogen werden.

§ 8a BISG verpflichtet die Betreiber kritischer Infrastrukturen zu angemessenen organisatorischen technischen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit über informationstechnische Systeme, Komponente oder Prozesse zu treffen. Bisher bestand die Pflicht, den Stand der Technik einzuhalten.

Neu geregelt ist, ab wann diese Verpflichtung gilt, nämlich erstmalig oder erneut, wenn feststeht, dass eine kritische Infrastruktur nach § 10 Abs. 1 BSIG betrieben wird. Die Einstufung als kritische Infrastruktur hängt von den Schwellenwerten ab, die in der Rechtsverordnung geregelt sind.

Die neue Pflicht zu Angriffserkennungssysteme

Neu wird in § 8a Abs. 1a BSIG die Pflicht geregelt, Systeme zur Angriffsanerkennung einzusetzen. Die Pflicht gilt ab dem 1. Mai 2023. Die Systeme müssen geeignete Parameter und Merkmale aus den laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Diese Systeme unterscheiden sich in der Methode zur Erkennung von Cyber-Angriffen. Beispielsweise nennt die Gesetzesbegründung den Abgleich mit statischen Mustern zur Software und Kommunikation, von denen bekannt ist, dass sie im Zusammenhang mit Cyber-Angriffen stehen. Eine weitere Methode besteht nach der Gesetzesbegründung darin, zunächst den störungsfreien Normalbetrieb zu erfassen und Abweichungen davon zur Detektion zu verwenden. Es handelt sich um die sogenannte **Anomalie-Detektion.** Alle Abweichungen vom Normalbetrieb werden als Indizien für einen drohenden Angriff oder eine Störung gewertet. Informationen müssen als Erkennungsmuster für Cyberangriffe eingesetzt werden. Diese einmal festgestellten Erkennungsmuster müssen ständig aktuell gehalten werden, weil die Cyberkriminalität ihre Angriffsmethoden verändert. Ein Erfahrungsaustausch über Informationen zu Schadsoftware wird auf der **Sharing-Plattform MISP des Bundesamtes** bereitgestellt.

Die Rechtsgrundlage für die eventuelle Verarbeitung personenbezogener Daten des IT-Systems durch Betreiber kritischer Infrastruktur ergibt sich aus Artikel 6 Abs. 1 Buchstabe f DSGVO. Die Betreiber kritischer Infrastrukturen haben nach § 8a Abs. 3 Satz 1 BSIG die Pflicht, die Erfüllung der Anforderungen alle zwei Jahre ab dem 1. Mai 2023 nachzuweisen.

Die neue Anwendung der Pflicht zur IT-Sicherheit auf „Unternehmen im besonderen öffentlichen Interesse“

Nach der Neufassung des **§ 8b BSIG** zur zentralen Stelle für die Sicherheit der Informationstechnik kritischer Infrastrukturen ist der **Anwendungsbereich auf Unternehmen im besonderen öffentlichen Interesse erweitert worden.** Die Betreiber kritischer Infrastruktur haben zusätzlich die Pflicht, ihre Betriebe in kritischen Infrastrukturen beim Bundesamt zu registrieren und eine Kontaktstelle zu benennen. Die Registrierung kann vom Bundesamt selbst vorgenommen werden, wenn die Betreiber ihre Registrierungspflicht nicht erfüllen. Erfüllt der Betreiber diese Pflicht zur Registrierung nicht, kann das Bundesamt von ihm verlangen, die erforderlichen Unterlagen vorzulegen und Auskunft zu erteilen, soweit nicht Geheimschutzinteressen oder überwiegende Sicherheitsinteressen entgegenstehen. Nach § 8b Abs. 4a BSIG kann das BSI zur Bewältigung der Störung die Herausgabe der notwendigen Informationen einschließlich bezogener Daten verlangen.

Neue Pflichten für Anbieter digitaler Dienste

§ 8c BSIG verpflichtet die **Anbieter digitaler Dienste.** Sie haben **technische und organisatorische Maßnahmen zu treffen,** um die Risiken für die Sicherheit der Netze und Informationssysteme zu bewältigen, die sie zur Bereitstellung der digitalen Dienste innerhalb der europäischen Union nutzen.

§ 8e BSIG regelt das Auskunftsverlangen Dritter gegenüber dem Bundesamt. **Das BSI kann nur Auskunft erteilen,** wenn die Interessen betroffener Betreiber kritischer Infrastruktur oder Unternehmen im besonderen öffentlichen Interesse oder dem Anbieter digitaler Dienste nicht entgegenstehen. Sicherheitsinteressen dürfen nicht durch die Auskunft beeinträchtigt werden. Bevor also das BSI Auskünfte über Erfahrungen von Angriffen und Störern gegen dritte Betreiber kritischer Infrastruktur weitergibt, muss es prüfen, ob nicht schutzwürdige Interessen verletzt werden können.

Die Pflichten zur IT-Sicherheit von „Unternehmen im öffentlichen Interesse“

Nach **§ 8f BSIG werden Unternehmen im besonderen öffentlichen Interesse den Unternehmen kritischer Infrastruktur gleichgestellt.** Definiert werden sie in § 2 Abs. 14 BSIG. Sie werden durch die Rechtsverordnung nach § 10 Abs. 5 BSIG bestimmt. Nach § 8f BSIG haben sie die Pflicht eine **Selbsterklärung** zur IT-Sicherheit beim Bundesamt vorzulegen, und zwar

- **erstens** über die Zertifizierung im Bereich der IT-Sicherheit in den letzten 2 Jahren,
- **zweitens** welche Sicherheitsaudits in den letzten 2 Jahren durchgeführt wurden und
- **drittens** wie sichergestellt wird, dass die schützenswerten informationstechnischen Systeme, Komponenten und Prozesse angemessen geschützt werden und ob dabei der Stand der Technik eingehalten wird.

Nach **§ 8f Abs. 5 BSIG** haben sie die Pflicht nach Vorlage der ersten Selbsterklärung sich beim Bundesamt zu registrieren und eine Kontaktstelle zu benennen. Nach § 8f Abs. 7 BSIG haben sie Meldepflichten. Von den Meldepflichten betroffen sind die Unternehmen im besonderen öffentlichem Interesse nach § 2 Abs. 14 Satz 1 Nummer 1 und 2 BSIG über Störungen, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der Wertschöpfung geführt haben, oder führen können. Die Meldungen müssen die tatsächlichen und vermuteten Ursachen, die betroffene Informationstechnik und die Art der betroffenen Einrichtungen und Anlangen enthalten.

Die Pflichten zur IT-Sicherheit von Störfallbetrieben

Nach **§ 8f Abs. 8 BSIG** sind die Störfallbetriebe nach § 2 Abs. 14 Satz 1 Nummer 3 BSIG zur Meldung verpflichtet. Dabei handelt es sich um die Störfallbetriebe, die verpflichtet sind Störungen unverzüglich zu melden.

Die Pflicht zur Berechnung der Wertschöpfung

Erfüllen Unternehmen im besonderen öffentlichen Interessen ihre Pflicht zur Selbsterklärung nach § 8f Abs. 5 BSIG nicht, kann das BSI eine **rechnerische Darlegung** verlangen, wie hoch die vom Unternehmen erbrachte inländische Wertschöpfung nach der in § 10 Abs. 5 BSIG festgelegten Berechnungsmethode ist oder eine entsprechende Bestätigung einer anerkannten Wirtschaftsprüfungsgesellschaft, dass das Unternehmen kein Unternehmen im besonderen öffentlichem Interesse nach § 2 Abs. 14 Satz Nr. 2 ist. Die IT-Sicherheit bei Unternehmen im besonderen öffentlichen Interesse nach § 8f BSIG wird wie die Unternehmen der kritischen Infrastruktur vom BSIG geregelt, weil es sich um volkswirtschaftlich besonders wichtige Unternehmen handelt, weil sie in sicherheitsrelevanten Branchen aktiv sind oder aufgrund ihrer Größe und entsprechender wirtschaftlicher Leistungsfähigkeit bestmöglich sicherzustellen ist, dass Cyber-Angriffe oder sonstige IT-Störungen nicht zu länger andauernden Produktionsausfällen führen können. Diese Unternehmen werden wegen ihrer volkswirtschaftlichen Bedeutung verpflichtet, mittels einer Selbsterklärung gegenüber dem Bundesamt darzulegen, welche Maßnahmen zur Verbesserung ihrer IT-Sicherheit vorgesehen sind und durchgeführt werden. **Große Unternehmen werden somit im Interesse der Volkswirtschaft zur IT-Sicherheit gezwungen.** Sie werden zum Beispiel zum BSI-Grundschutz, zu Audits und Zertifizierungen verpflichtet. Durch die Selbsterklärung der Unternehmen und die Einbeziehung des BSI erhalten die Unternehmen die Möglichkeit, ihre IT-Sicherheit zu verbessern und sie auf ein fiktives Schutzniveau zu heben. Sie werden verpflichtet, bestimmte Angriffe und Vorfälle zu melden, wenn die Wertschöpfung beeinträchtigt werden kann. **Geschützt werden Unternehmen im besonderen öffentlichen Interesse nicht nur vor Cyber-Angriffen,** sondern **auch vor Störungen.** Eine Störung im Sinne des BSIG liegt dann vor, wenn die eingesetzte Technik die ihr zugedachten Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken. Dazu zählen Fälle von Sicherheitslücken, Schadprogrammen, außergewöhnliche und unerwartete technische Defekte mit IT-Bezug, versuchte und abgewehrte Angriffe auf die IT-Sicherheit.[8] Durch die Meldepflicht an das BSI können Erkenntnisse gewonnen werden, wie solche Störungen erkannt, behoben und vermieden werden können. Ein Ausfall der Wertschöpfung wäre meldepflichtig, da hierbei ein entsprechend bedeutendes Unternehmen faktisch still gelegt wäre. Die gemeldeten Erkenntnisse können mit anderen Unternehmen geteilt werden und das IT-Sicherheitsniveau in Deutschland erhöht werden, ohne dass das meldende Unternehmen selbst an die Öffentlichkeit gehen muss, um andere Unternehmen zu warnen oder zu informieren. Das Gesetz strebt mit den Pflichten nach § 8f BSIG einen vertrauensvollen Austausch zwischen Bundesamt und Unternehmen an.[9]

Die Pflicht von Störfallbetrieben zur IT-Sicherheit

Nach **§ 2 Abs. 14 Satz 1 Nummer 3 BSIG sind Störfallbetriebe verpflichtet,** Störungen an das Bundesamt zu melden, die zu einem Störfall nach der Störfallverordnung geführt haben oder führen können. Es handelt sich um Störungen, die das Leben oder die Gesundheit von Menschen bedrohen oder durch die die Gesundheit einer großen Zahl von Menschen beeinträchtigt werden kann.

Nach **§ 9b BSIG** wird in die **Gefahr durch kritische Komponenten geregelt, auf die Unternehmen kritischer Infrastruktur angewiesen sind,** die deshalb kritisch sind, weil Störungen dieser IT-Produkte zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit und letztlich zur Gefährdung für die öffentliche Sicherheit führen können. Nach § 9b Abs. 1 BSIG sind die Betreiber kritischer Infrastruktur verpflichtet, den geplanten erstmaligen Einsatz einer kritischen Komponente dem Bundesinnenminister anzuzeigen. Das Bundesministerium kann den Einsatz untersagen oder Anordnungen erlassen, wenn der Einsatz die öffentliche Ordnung oder Sicherheit vor-

8 BT-Drs. 19/26106, S. 82.

9 BT-Drs. 19/26106, S. 82.

aussichtlich beeinträchtigt. Durch die Betreiber kritischer Infrastruktur ist eine Erklärung des Herstellers der kritischen Komponente einzuholen, dass dieser in der Lage ist, die gesetzlichen geforderten Bestimmungen sowie auch weitergehende flankierende Pflichten selbst einzuhalten. Dies gilt nach § 9b Abs. 3 BSIG für kritische Komponenten, für die eine gesetzliche Zertifizierungspflicht besteht. Der Hersteller hat eine Garantieerklärung abzugeben. Vermieden werden müssen Risiken für die drei Schutzziele und für die öffentliche Sicherheit und Ordnung.

Der Bundesinnenminister kann den Einsatz der kritischen Komponente untersagen oder Anordnungen erlassen, wenn die öffentliche Sicherheit und Ordnung voraussichtlich beeinträchtigt wird und der Hersteller der kritischen Komponente nicht vertrauenswürdig ist. In den Anzeigen ist die Art des Einsatzes (Abs. 1 Satz 2) darzustellen. Dazu gehört die Funktion und Verortung in der kritischen Infrastruktur. Jeder Betreiber kann über die Funktion und den Einsatz Auskunft geben.

Die Inhalte der Garantieerklärung werden durch eine Allgemeinverfügung des Bundesinnenministeriums vorgegeben. Die Garantieerklärung wird sich auf verschiedene Kritis-Sektoren erstrecken, für die spezifische Inhalte vorgegeben werden müssen. Die Garantieerklärung muss auch mögliche Gefahren und Verstöße gegen bestimmte Handlungspflichten abdecken, die sich aus der Organisationsstruktur oder möglichen sonstigen rechtlichen Verpflichtungen des Herstellers ergeben.[10]

Nach **§ 9 BSIG** besteht ein Untersagungsvorbehalt. Die Betreiber müssen eine Entscheidung über den Einsatz einer kritischen Komponente abwarten, bevor der Einsatz gestattet ist.[11] Das Bundesinnenministerium beteiligt verschiedene Ressorts um die jeweiligen Risiken zu analysieren. In der Gesetzesbegründung werden „interministeriale jour fixes“ erwähnt, um eine umfassende Sachverhaltsaufklärung als Voraussetzung für eine Entscheidung nach Abs. 3 in den knappen Entscheidungsfristen von einem Monat nach Anzeige zu ermöglichen. Auf Ministerebene müsste für den Einsatz kritischer Komponente ein Konsens erzielt werden. Im Falle eines Dissenses hat die Bundesregierung nach den Vorgaben der gemeinsamen Geschäftsordnung der Bundesregierung (GO BReg) über den Streit zu beraten mit dem Ziel, eine einvernehmliche Entscheidung voranzutreiben (§ 15 Abs. 1 GO BReg). In § 9b Abs. 4 BSIG wird der weitere Einsatz der Komponente nach der Zulassung geregelt. Überprüft wird die Einhaltung der Vorgaben der Garantieerklärung im laufenden Betrieb. Auch der laufende Betrieb einer Komponente kann untersagt werden und zum Rückbau führen. Die Pflichten aus der Garantieerklärung müssen auch nach dem Einbau im laufenden Betrieb eingehalten werden.

Die Bußgeldregelung nach § 14 BSIG

Mit der Gesetzesänderung wurde der Bußgeldrahmen erhöht, die Bußgeldvorschriften systematisiert und ergänzt. Der Katalog der Tatbestände zur Wahrnehmung der übertragenden Aufgaben im Bereich kritischer Infrastrukturen wurde präzisiert und erweitert. Die Bußgeldvorschriften sind in vier Stufen aufgebaut.

Nach **§ 14 Abs. 1 BSIG** werden alle Fälle sanktioniert, in denen Betreiber ihre zur erbringenden Nachweise, Nachforderungen, Auskünfte und Kennzahlen vorsätzlich falsch oder nicht vollständig erbringen. Begründet wird diese Regelung damit, dass das BSI darauf angewiesen ist, den Stand der umgesetzten Maßnahmen zur Sicherung der IT-Sicherheit von den Betreibern selbst tätig und zuverlässig nachgewiesen werden. Das BSI benötigt den tagesaktuellen Überblick über den Stand des IT-Sicherheitsniveaus und über die Entwicklung der laufenden IT-Vorfälle, um die Prävention, Detektion und Angriffsbewältigung unterstützen zu können. Das BSI ist auf die Nachweise durch die Betreiber und deren Zulieferer angewiesen. **Der Unrechtsgehalt wird auf das vorsätzliche Zurückhalten durch die Betreiber in Kenntnis ihrer Pflicht begründet.** Das öffentliche Interesse wird zugunsten der Individualinteressen der Betreiber missbilligt. Die fahrlässige Vernachlässigung

10 BT-Drs. 19/26106.

11 BT-Drs. 19/26106, S. 85.

der Informationspflichten wird nach § 14 Abs. 1 BSIG nicht sanktioniert.

Nach **§ 4 Abs. 2 Nr. 1a, b und c BSIG** werden Zuwiderhandlungen gegen vollziehbare Anordnungen nach § 5 Abs. 6 BSIG vorgesehen, wenn **Hersteller eines informationstechnischen Systems** gegen dem Verlangen des Bundesamtes **nicht oder in unzureichender Form an der Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen Systems mitwirken.** Es betrifft die Bestandsdaten, Auskunft auf Verlangen des Bundesamtes. Verpflichtet ist der Anbieter geschäftsmäßiger Telekommunikationsdienste und zwar in Fällen der drohenden Gefahr nach § 2 Abs. 10 Nr. 1 BSIG und die Funktionsfähigkeit informationstechnischer Systeme der kritischen Infrastruktur oder eines Unternehmens von besonderem öffentlichem Interesse abzuwehren sind. Auf die Mitwirkung der Herstellern sind alle Betroffenen angewiesen, da in der Regel nur bei den Hersteller der vollständige Zugang zur Dokumentation von Hard- und Softwarekomponenten vorhanden ist. Der **drohende Ausfall und die Betroffenheit an einer Vielzahl von Bürgern rechtfertigt die Androhung des Bußgelds.** Die Wiederherstellung der Sicherheit durch Sicherheitspatches ist nur mit dem betriebsinternen Know-how des Herstellers zu bewältigen. Auch die Eilbedürftigkeit rechtfertigt die Sanktionen im öffentlichen Interesse. Die Bußgeldbewehrung hilft der Vollziehung von Anordnungen des BSI. Auch die Bußgeldbewehrung einer Zuwiderhandlung gegen eine vollziehbare Anordnung nach § 8 Abs. 3 Satz 5 BSIG soll sicherstellen, dass die Beseitigung von Sicherheitsmängeln bei Betreibern kritischer Infrastruktur wirksam durchgesetzt werden kann, insbesondere wenn der Betreiber die Erfüllung einer Anordnung verweigert.

Die Bußgeldbewehrung nach **§ 14 Abs. 2 Nummer 1 BSIG** haben gemeinsam, dass sie eine vollziehbare Anordnung voraussetzen und der Verpflichtete das Ausmaß der Pflicht kennt und die darüber hinaus vollziehbar ist. Gegen Herstellern informationstechnischer Systeme und die Betreibern kritischer Infrastruktur rechtswidrig stehen Rechtsmittel zur Verfügung, wenn das BSI rechtswidrige Anordnungen erlassen würde.

Nach **§ 14 Abs. 2 Nummer 2 BSIG** wird der Verstoß gegen Pflichten zur Vorkehrungen nach dem Stand der Technik sanktioniert. Die Vorkehrungen ergeben sich aus der Rechtsverordnung nach § 10 Abs. 1 Satz 1 BSIG.

Nach **§ 14 Abs. 2 Nummer 3 BSIG** wird der Verstoß gegen die Pflicht zum Nachweis der Vorkehrungen nach dem Stand der Technik sanktioniert. Ohne die Angaben des Betreibers kann das BSI seine Aufsichts- und Unterstützungsaufgaben nicht erfüllen. Zu den Kernaufgaben gehört es, den tagesaktuellen Überblick über den Stand des IT-Sicherheitsniveaus und über die Entwicklung der laufenden IT-Vorfälle zu behalten, wovon die effektive Prävention, Detektion und Angriffsbewältigung abhängt.

Nach **§ 14 Abs. 2 Nummer 4 BSIG** wird die Pflicht des Betreibers kritischer Infrastruktur sanktioniert Unterlagen rechtzeitig vorzulegen, eine Auskunft zu erteilen oder keine oder nur unzulässige Unterstützung zu gewähren. Das Auskunftsverlangen bei Vorortkontrollen soll durch die Sanktionen besser durchgesetzt werden können. Auch hier hat die Sanktion eine Beugefunktion. Dem BSI wird die Kontrolle über den Zustand der IT-Sicherheit erschwert, wenn der Betreiber seine Unterstützung verweigert.

Nach **§ 14 Abs. 2 Nummer 5 BSIG** wird die Pflicht des Betreibers kritischer Infrastruktur sanktioniert, die kritische Infrastruktur zu registrieren und eine Kontaktstelle zu benennen.

Nach **§ 14 Abs. 2 Nummer 6 BSIG** wird die Pflicht des Betreibers kritischer Infrastruktur nach § 8b Abs. 3 Satz 4 BSIG sanktioniert die Erreichbarkeit durch die Kontaktstelle zu gewährleisten.

Nach **§ 14 Abs. 2 Nummer 7 BSIG** wird die Pflicht des Betreibers sanktioniert, Störungsmeldungen nicht, falsch, unvollständig oder nicht rechtzeitig abzugeben.

Nach **§ 14 Abs. 2 Nummer 8 BSIG** wird die Pflicht eines Anbieters digitaler Dienste sanktioniert, Sicherheitsmaßnahmen zu treffen um Risiken für die Sicher-

heit der Netz- und Informationssysteme abzuwenden, die sie zur Bereitstellung der digitalen Dienste innerhalb der EU nutzen.

Nach **§ 14 Abs. 2 Nummer 9 BSIG** wird die Pflicht von Unternehmen im besonderen öffentlichem Interesse sanktioniert, eine Selbsterklärung zur IT-Sicherheit dem Bundesamt vollständig und rechtzeitig vorzulegen.

Nach **§ 14 Abs. 2 Nummer 10 BSIG** wird die Pflicht der Konformitätsbewertungsstelle sanktioniert, ohne Befugnis durch das BSI nicht tätig zu werden.

Nach **§ 14 Abs. 2 Nummer 11 BSIG** wird die Pflicht des Verwenders eines IT-Sicherheitskennzeichens sanktioniert, auf einem Produkt ohne Freigabe durch das BSI zu verwenden.

Nach **§ 14 Abs. 3 BSIG** wird die Pflicht des Betreibers kritischer Infrastruktur sanktioniert, die Nachweise, die Nachforderungen von Auskünften fahrlässig zu erbringen. Nach § 14 Abs. 4 BSIG werden Verstöße gegen die Vorgaben zu Konformitätserklärungen sanktioniert.[12]

§ 14 Abs. 5 BSIG regelt die Höhe der Bußgelder. Die Androhung des Bußgeldrahmens in Höhe von bis zu 2 Millionen drückt den erhöhten Unwertgehalt einer Missachtung behördlich angeordneter Maßnahmen aus.[13] Die Sanktionen müssen wirksam, angemessen und abschreckend sein, um auch die Umsetzung der NIS-RL sicherzustellen. Die Höhe des Bußgelds berücksichtigt, dass im Bereich der Kritis-Betreiber umsatzstarke Konzerne nur mit hohen Bußgeldandrohungen zu ordnungsgemäßem Verhalten angehalten werden können. Nur durch die Höhe der Sanktionen können sie generalpräventiv wirken.

12 BT-Drs. 19/26106, S. 89 f.

13 BT-Drs. 19/26106, S. 94.

RACK
RECHTSANWÄLTE • NOTARE

ALLES AUS EINER HAND

Rechtsinhalte, Software & präventive Rechtsberatung

Nutzen Sie unsere gespeicherten **Erfahrungen aus 29 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt.

Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 19.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 8.200 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 62.000 vorformulierte Betriebspflichten. **46.000 Unternehmensrisiken sind mit 62.000 Rechtspflichten 3,3 Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko, eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de