Claudia Plattner – Präsidentin des BSI

Stellungnahme zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages am 4. November 2024

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)523 C

Der Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) ist aus meiner fachlichen Sicht grundsätzlich dazu geeignet, das Cybersicherheitsniveau in Deutschland anzuheben. Gleichwohl wäre im Sinne gesamtstaatlicher Cybersicherheit die Aufnahme von Kommunen wünschenswert und es besteht meines Erachtens erheblicher Nachbesserungsbedarf zur Stärkung des BSI als zentrale Stelle für Cybersicherheit, der nachfolgend dargelegt wird.

Übersicht

1 CISO Bund fest bei BSI verankern

Ein starker CISO Bund sollte beim BSI angesiedelt werden, weil dieses schon die notwendigen Fach- und Umsetzungskompetenzen besitzt und – verknüpft mit der unabhängigeren Stellung des BSI – als neutrale Stelle für Cybersicherheit wirkt. Weiterhin würde eine Verortung des CISO Bund beim BMI absehbar zu operativen Reibungsverlusten führen, beispielsweise wenn Behörden Sicherheitsvorgaben des BSI vor einer Umsetzung erst mit dem CISO Bund rückkoppeln. Wenn der CISO Bund beim BSI platziert wird, kann ein effektives prozessuales Verschränken zwischen den Befugnissen des BSI bezüglich der Cybersicherheit der Bundesverwaltung im Rahmen der NIS2-Richtlinie und dem operativen Wirken des CISO Bund sichergestellt werden. Dies wäre ein deutlicher Gewinn für die Informationssicherheit der Bundesverwaltung.

Aus diesen Gründen sollte die Rolle des CISO Bund explizit als zusätzliche Aufgabe des BSI im BSIG aufgenommen werden und dort mit einer klaren Zweckbestimmung versehen werden. Damit ein CISO Bund effektiv arbeiten kann und tatsächlich Wirkung entfaltet, ist es unabdingbar, dass die Position mit den erforderlichen Befugnissen ausgestattet wird, um die dazugehörigen Aufgaben zielgerichtet zu erfüllen. Das BSI verfügt bereits über entsprechende Durchsetzungsbefugnisse – es müsste daher nur festgelegt werden, dass diese ebenso dem CISO Bund zur Verfügung stehen, wenn die Rolle beim BSI verankert wird. Aus fachlicher Sicht des BSI sollten nachfolgende Änderungen umgesetzt werden:

a) Aufnahme des CISO Bund als zusätzliche Aufgabe des BSI
   Indem die Position unmittelbar hinter den Aufgaben des BSI in einem neuen § 3a aufgenommen wird, wird durch die Gesetzessystematik deutlich, dass es sich bei der Rolle um eine zusätzliche und wichtige Aufgabe des BSI handelt.

   ⇨ *Empfehlung für neuen § 3a BSIG „Die oder der Bundesbeauftragte für Informationssicherheit“:*

   „(1) Die Leitung des Bundesamtes nimmt die Aufgaben der oder des Bundesbeauftragten für Informationssicherheit (Bundesbeauftragte) wahr.

   Sie oder er muss über die für die Erfüllung ihrer oder seiner Aufgaben und Ausübung ihrer oder seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich der Informationssicherheit verfügen.

   (2) Die oder der Bundesbeauftragte wirkt gemeinsam mit dem Beauftragten der Bundesregierung für Informationstechnik auf ein angemessenes Verhältnis zwischen dem Einsatz von Informationstechnik und Informationssicherheit hin.

   (3) Die oder der Bundesbeauftragte wird bei allen Gesetzes-, Verordnungs- und sonstigen wichtigen Vorhaben beteiligt soweit sie Fragen der Informationssicherheit berühren.“

b) Festlegung der erforderlichen Zweckbestimmung der Rolle CISO Bund
Die Position „Bundesbeauftragte“ erfordert eine grundsätzliche Zweckbestimmung der Rolle. Für die Rolle des CISO Bund ist dies aus hiesiger Sicht die Koordinierung des Informationssicherheitsmanagements des Bundes.

⇨ *Empfehlung für neuen § 3b BSIG „Aufgaben der oder des Bundesbeauftragten“:*

„Die oder der Bundesbeauftragte koordiniert das Informationssicherheitsmanagement des Bundes. Im Benehmen mit den obersten Bundesbehörden entwickelt die oder der Bundesbeauftragte Programme zur Gewährleistung der Informationssicherheit des Bundes und schreibt diese fort. Sie oder er unterrichtet kalenderjährlich jeweils bis zum 30. Juni den Haushaltsausschuss des Deutschen Bundestages über den Umsetzungsstand der Programme.“

c) Festlegung der erforderlichen Befugnisse für zielgerichtete Aufgabenwahrnehmung
Zur zielgerichteten Aufgabenwahrnehmung kann die Rolle des CISO Bund ihre Wirkung nur entfalten, wenn damit die notwendigen Durchsetzungsbefugnisse in Sachen IT-Sicherheit verbunden werden.

⇨ *Empfehlung für neuen § 3c BSIG „Befugnisse der oder des Bundesbeauftragten“:*

„(1) Der oder die Bundesbeauftragte beaufsichtigt die Umsetzung der Programme zur Gewährleistung der Informationssicherheit des Bundes durch die Befugnisse des Bundesamtes nach diesem Gesetz.

(2) Zur Wahrnehmung ihrer oder seiner Aufgaben hat die oder der Bundesbeauftragte ein direktes Vortragsrecht vor dem Ausschuss für Inneres und Heimat und dem Haushaltsausschuss des Deutschen Bundestages des Deutschen Bundestages zu allen Themen der Informationssicherheit des Bundes.“

2 Unabhängigere Rolle des BSI etablieren

Mit der im Koalitionsvertrag vereinbarten unabhängigeren Aufstellung des BSI wird der bestehende Interessenskonflikt zwischen öffentlicher Sicherheit und Informationssicherheit im Geschäftsbereich des BMI entschärft und die fachliche Unabhängigkeit des BSI klargestellt. Mit Aufstellung des BSI als selbstständige Bundesoberbehörde, würde die Rolle des BSI bereits unabhängiger, ohne das Bundesamt aus dem Geschäftsbereich des BMI herauszulösen. Zudem könnte das BMI in einem neuen Aufsichtskonzept die Grundlinien der Fachaufsicht für das BSI festlegen und dort bspw. die gemeinsame Erstellung eines Jahresarbeitsprogramms für das BSI vorsehen. Um die Position des BSI als neutrale und unabhängige Beratungsinstanz für die Bundesressorts sicherzustellen, sollte die Berichtspflicht des BSI an das BMI bei der Zusammenarbeit mit anderen Ressorts entfallen. Aus fachlicher Sicht des BSI sollten hierfür nachfolgende Änderungen umgesetzt werden:

a) Aufstellung des BSI als selbstständige Bundesoberbehörde
Mittels dieser Statusänderung würde die Rolle des BSI bereits unabhängiger gestaltet und zugleich ein hoher Grad an demokratischer Legitimation erhalten bleiben.

⇨ *Empfehlung zur Änderung von § 1 Satz 1 BSIG:*

„Das Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) ist eine selbständige Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern und für Heimat."

b) Fixierung der wissenschaftlich-technischen Arbeitsgrundlage des BSI
Die Arbeit des BSI auf Grundlage rein wissenschaftlich-technischer Erkenntnisse sollte explizit im BSIG festgeschrieben werden, um die fachlich unabhängige Aufgabenwahrnehmung des BSI zu betonen und dadurch die Vertrauenswürdigkeit des BSI zu stärken.

⇨ *Empfehlung zur Änderung von § 1 Satz 3 BSIG:*

„Das Bundesamt führt seine Aufgaben fachlich unabhängig auf Grundlage wissenschaftlich-technischer Erkenntnisse durch."

c) Gemeinsame Erstellung eines Jahresarbeitsprogramms des BSI zwischen BMI und BSI
Im Rahmen einer neu gestalteten Fachaufsicht könnte das BMI in einem Aufsichtskonzept die Grundlinien der Fachaufsicht über das BSI festlegen und dort die Erstellung eines Jahresarbeitsprogramms für das BSI gemeinsam mit dem BSI vorsehen. Um eine angemessene Transparenz gegenüber dem Bundestag zu gewährleisten, könnte das BMI alle zwei Jahre das Parlament über die Aufsichtspraxis und Einzelweisungen an das BSI unterrichten.

⇨ *Empfehlung für neuen § 1 Satz 4 BSIG:*

„Das Bundesministerium des Innern und für Heimat erstellt Grundlinien der Aufsicht über das Bundesamt in einem Aufsichtskonzept und unterrichtet alle zwei Jahre den Deutschen Bundestag über die Aufsichtspraxis und Einzelweisungen an das Bundesamt."

d) Wegfall der Berichtspflicht des BSI an BMI bei der Zusammenarbeit mit anderen Ressorts
Mit Umsetzung des nachstehenden Vorschlags wäre es dem BSI möglich, andere Ressorts neutral und unabhängig zu beraten. Die bisherige negative Sonderstellung des BSI in der GGO ist sachlich nicht gerechtfertigt und im Hinblick auf die Funktion als zentraler Kompetenzträger für alle Stellen des Bundes in Sachen der IT-Sicherheit auch kontraproduktiv.

⇨ *Empfehlung zur Streichung der Nennung des BSI aus § 26 Abs. 1 S. 2 GGO*

3 Operative Abwehrfähigkeiten des BSI weiter stärken

Stärkung der Cyberabwehrfähigkeiten gegen Botnetze

Das BSI setzt seit mehreren Jahren Maßnahmen zur Abwehr von Botnetzen um, darunter auch die Umleitung von Domainnamen durch Internetprovider. Gleichwohl nutzen Botnetze zunehmend neue Techniken wie DNS over HTTPS, bei denen eine vom BSI angeordnete Umleitung von Domainnamen durch Provider keinen flächendeckenden Schutz bietet, da viele Nutzende auch andere zulässige Möglichkeiten zur Auflösung von Domainnamen verwenden. Dies liegt darin begründet, dass nur die Kunden großer deutscher Internetanbieter (>100.000 Kunden) geschützt werden, die auch tatsächlich den vorgegebenen DNS-Dienst des Anbieters nutzen. Die angeordnete Domain bleibt weiterhin für alle anderen Internetnutzer international aktiv und weiterhin erreichbar. Nur durch eine Dekonnektierung der Domain auf Ebene der Nameserver kann ein vollständiger Schutz für alle Nutzer umgesetzt werden. Damit das BSI auch weiterhin in der Lage ist, Botnetze zu analysieren und zu entschärfen, ist eine Ausdehnung der bisherigen Anordnungsbefugnis auf Domainregistare dringend geboten, um die operativen Handlungsmöglichkeiten des BSI an die technischen Entwicklungen anzupassen. Aus fachlicher Sicht des BSI sollte hierfür nachfolgende Änderung umgesetzt werden:

- ⇨ *Empfehlung zur Einführung eines neuen § 17a BSIG „Anordnungen des Bundesamtes gegenüber Top Level Domain Name Registries und Registraren“:*

  „(1) Zur Abwehr konkreter erheblicher Gefahren für die in Absatz 2 genannten Schutzgüter kann das Bundesamt gegenüber Top Level Domain Name Registries oder Registraren im Sinne dieses Gesetzes anordnen, dass sie

  a) die Nameserver Einträge einer vom Bundesamt benannten Domain ändern, neue Einträge hinzufügen oder die Domain auf Ebene der Nameserver dekonnektieren oder
  b) dem Bundesamt die Inhaberschaft an einer bestimmten Domain übertragen,

  sofern und soweit der Diensteanbieter dazu technisch in der Lage ist und es ihm wirtschaftlich zumutbar ist. Widerspruch und Anfechtungsklage gegen die Anordnungen nach Satz 1 haben keine aufschiebende Wirkung. Im Fall des Absatz 1 Satz 1 Nummer 2 benennt das Bundesamt die zur Übertragung der Inhaberschaft notwendigen Ansprechpartner.

  (2) Schutzgüter gemäß Absatz 1 Satz 1 sind die Verfügbarkeit, Integrität oder Vertraulichkeit

  a) der Kommunikationstechnik des Bundes, einer Kritischen Einrichtung oder einer besonders wichtigen Einrichtung oder einer wichtigen Einrichtung,
  b) von Informations- oder Kommunikationsdiensten oder

c) von Informationen, sofern deren Verfügbarkeit, Unversehrtheit oder Vertraulichkeit durch unerlaubte Zugriffe auf eine erhebliche Anzahl von telekommunikations- oder informationstechnischen Systemen von Nutzern eingeschränkt wird.

(3) Ordnet das Bundesamt eine Maßnahme nach Absatz 1 Satz 1 lit. a) an, so kann es gegenüber einer Top Level Domain Name Registry oder einem Registrar auch anordnen, die an eine bestimmte Domain gerichteten Nameserveranfragen an einen vom Bundesamt benannten Nameserver umzuleiten.

(4) Das Bundesamt darf Daten, die von einer Top Level Domain Name Registry oder einem Registrar nach Absatz 1 Satz 1 lit. a und Absatz 3 umgeleitet wurden, verarbeiten, um Informationen über Schadprogramme oder andere Sicherheitsrisiken in informationstechnischen Systemen zu erlangen. Die übermittelten Daten dürfen durch das Bundesamt so lange gespeichert werden, wie dies für die Erfüllung des in Satz 1 genannten Zwecks erforderlich ist, längstens jedoch für drei Monate. § 5 Absatz 7 Satz 2 bis 8 gilt entsprechend. Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des Folgejahres über die Gesamtzahl der angeordneten Nameserverumleitungen.

(5) Die nach Absatz 1 Satz 1 lit. b) übertragenen Inhaberschaften müssen vom Bundesamt aufgegeben werden, wenn feststeht, dass

a) von den Domains keine Gefahren nach Absatz 1 Satz 1 mehr ausgehen, und
b) über die Inhaberschaft an den Domains keine Informationen über Schadprogramme oder andere Sicherheitsrisiken in informationstechnischen Systemen mehr zu erlangen sind.

In diesem Fall wird das Bundesamt die Inhaberschaften durch Veranlassung der Löschung der Domains bei der zuständigen Top Level Domain Name Registry oder dem zuständigen Registrar veranlassen."

Erweiterte Befugnis zur Messung der Resilienz deutscher IT-Systeme gegenüber aktuellen Schwachstellen

Derzeit darf das BSI gemäß § 7b BSIG (nach Regierungsentwurf zukünftig § 15 BSIG) Resilienz-Messungen bei öffentlich erreichbaren IT-Systemen nur in einem sehr eingeschränkten Bereich durchführen. Bisher sind davon lediglich die Einrichtungen des Bundes, Kritische Infrastrukturen, Digitale Dienste (z.B. Online-Marktplätze,-Suchmaschinen und Cloud-Computing-Dienste) sowie Unternehmen im besonderen öffentlichen Interesse umfasst.

Mit einer Erweiterung der Befugnisse, solche Resilienz-Messungen hinsichtlich der Verwundbarkeit aufgrund öffentlich bekannter Schwachstellen für alle im deutschen IP-Raum erreichbaren IT-Systeme durchzuführen, würde ein signifikanter Mehrwert für die IT-Sicherheit

deutschlandweit generiert. Ausschließliches Ziel dieser Messungen ist die Warnung der Betroffenen, damit diese möglichst zeitnah Schutzmaßnahmen ergreifen können. Dem BSI wäre es dann möglich, in einem transparenten Verfahren alle Betroffenen schnell und effektiv über die Verwundbarkeit ihrer IT-Systeme zu informieren. Dies kann über die Möglichkeit für das BSI sichergestellt werden, Provider entsprechend zur Information ihrer Kundinnen und Kunden anzuweisen.

Die Befugniserweiterung dient ausdrücklich nicht zur heimlichen Suche nach Schwachstellen in deutschen IT-Systemen, um diese auszunutzen. Das BSI wird also nicht zu einer „Hackerbehörde". Im Gegenteil bleibt mit der Befugniserweiterung auch die unverzügliche Benachrichtigungspflicht bestehen (§ 15 Abs. 2 BISG-E), die für maximale Transparenz sorgt: Das BSI sucht nach Schwachstellen, um die Betroffenen zeitnah über ihre Verwundbarkeit zu informieren, damit diese ihre Systeme schnellstmöglich sichern können. Es handelt es sich somit um eine Befugnis des Bundesamtes mit strenger Zweckbindung. Die entsprechenden Detektionsmaßnahmen dürfen nur zur Aufgabenerfüllung genutzt werden.

Insbesondere bei weit verbreiteten kritischen Schwachstellen, z.B. in Microsoft Exchange Servern, wäre es dem BSI mit dieser erweiterten Befugnis möglich, binnen kürzester Zeit, verwundbare Systeme zu identifizieren und die Betreiber mittels schneller Warnung zum Schließen der Schwachstellen zu animieren. Aktuell wird die Betroffenheit von den Betreibern zu oft erst nach erfolgreichen Angriffen bekannt. Für die IT-Sicherheit in Deutschland würde diese Befugniserweiterung daher einen deutlichen Gewinn bei minimalem zusätzlichen Ressourcenaufwand bedeuten. Ergänzend dazu ließe sich mit den Gefährdungsübersichten aus den erweiterten Resilienz-Messungen das gesamtdeutsche Cybersicherheits-Lagebild noch weiter schärfen. Aus fachlicher Sicht des BSI sollten die Befugniserweiterung nachfolgende Änderung umgesetzt werden:

- ⇨ *Empfehlung zur Anpassung des § 15 Abs. 1 BSIG-E (vormals § 7b BSIG) zur Erweiterung der Befugnis zur Resilienz-Messung von deutschen IT-Systemen:*

  „(1) Das Bundesamt kann im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 2, 20 oder 24 zur Detektion von bekannten Schwachstellen und anderen Sicherheitsrisiken ~~bei Einrichtungen der Bundesverwaltung, bei besonders wichtigen Einrichtungen oder bei wichtigen Einrichtungen~~ Abfragen an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen durchführen,

  ~~1.~~ um festzustellen, ob diese Schnittstellen unzureichend geschützt und dadurch in ihrer Sicherheit oder Funktionsfähigkeit gefährdet sein können~~, oder~~

  ~~2. wenn die entsprechenden Einrichtungen der Bundesverwaltung, besonders wichtige oder wichtige Einrichtungen darum ersuchen~~.
  Die dadurch gewonnenen Erkenntnisse dürfen nur zum Zweck der Information nach Absatz 2 verwendet werden. Erlangt das Bundesamt dabei Informationen, die durch Artikel 10 des Grundgesetzes geschützt sind, sind diese unverzüglich zu löschen."

4 Wirksamkeit des BSI verbessern

Zielführende Anpassung von Einvernehmenserfordernissen im Bereich KRITIS

Der aktuelle Regierungsentwurf sieht für das BSI deutlich mehr Einvernehmenserfordernisse beim Aufsichtshandeln vor, als dies für die BNetzA der Fall ist. Es sollte sichergestellt werden, dass für ein gleichmäßiges Wahrnehmen der behördlichen Aufsicht die Einvernehmens- und Benehmenserfordernisse für BSI und BNetzA symmetrisch ausgestaltet werden. Insbesondere bei der einfachen Durchsetzung formaler gesetzlicher Pflichten bezüglich der Registrierung von Unternehmen nach § 33 Abs. 3 BSIG-E sollte auf ein Einvernehmen des BSI mit den jeweils zuständigen Aufsichtsbehörden verzichtet werden, um unnötigen bürokratischen Mehraufwand zu vermeiden. Auch bei der Herausgabe von Informationen durch Unternehmen im Zuge eines erheblichen Sicherheitsvorfalls (§ 40 Abs. 5 BSIG-E) sollte unbedingt auf das derzeit im Entwurf vorgesehene Einvernehmenserfordernis für das BSI verzichtet werden. Während eines solchen Sicherheitsvorfalls hat die zeitnahe Bewältigung oberste Priorität. Die Herstellung des Einvernehmens durch das BSI mit den jeweils zuständigen Aufsichtsbehörden des Bundes nur für die Herausgabe von notwendigen Informationen steht dem diametral entgegen.

Dagegen ist die Einvernehmensregelung bei einer Anordnung zur Mängelabstellung sinnvoll, weil dadurch die Aufsichtsbehörde inhaltlich mitbewerten kann. Zudem sollte auch der Katalog von IT-Sicherheitsanforderungen für Betreiber von Energieanlangen und –versorgungsnetzen nur im Einvernehmen mit dem BSI durch die BNetzA festgelegt und aktualisiert werden, anstatt wie bisher im Regierungsentwurf vorgesehen, lediglich im Benehmen (§ 5c Abs. 1,2 EnWG-E). Dies entspricht zugleich auch der bestehenden Gesetzeslage im Bereich der Telekommunikation (vgl. § 167 Abs. 1 TKG). Eine unterschiedliche Behandlung der Sektoren ist nicht erklärbar und würde zu einer auch verfassungsrechtlich problematischen, divergierenden Ausgestaltung von IT-Sicherheitsanforderungen zwischen diesen führen. Aus fachlicher Sicht des BSI sollten demzufolge nachfolgende Änderungen umgesetzt werden:

- ⇨ *Empfehlung zur Anpassung von § 33 Abs. 3 BSIG-E bezüglich der Registrierungspflicht von Unternehmen:*

  „(3) Die Registrierung von besonders wichtigen Einrichtungen und wichtigen Einrichtungen und Domain-Name-Registry-Diensteanbietern kann das Bundesamt ~~im Einvernehmen mit den jeweils zuständigen Aufsichtsbehörden~~ auch selbst vornehmen, wenn ihre Pflicht zur Registrierung nicht erfüllt wird.“

- ⇨ *Empfehlung zur Anpassung von § 40 Abs. 5 Satz 1 BSIG-E bezüglich der Herausgabe von Informationen zur laufenden Vorfallsbewältigung:*

  „(5) Während eines erheblichen Sicherheitsvorfalls gemäß § 32 Absatz 1 kann das Bundesamt ~~im Einvernehmen mit der jeweils zuständigen Aufsichtsbehörde des Bundes~~ von den betroffenen Betreibern kritischer Anlagen die Herausgabe der zur

Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten verlangen."

⇨ *Empfehlung zur Anpassung von § 5c Abs. 1, 2 EnWG-E zur Ergänzung des Einvernehmens des BSI hinsichtlich des IT-Sicherheitskatalogs für Energieversorgungsnetze und Energieanlagen:*

„(1) (...) Die Bundesnetzagentur bestimmt im Einvernehmen ~~Benehmen~~ mit dem Bundesamt für Sicherheit in der Informationstechnik durch Festlegung nach § 29 Absatz 1 in einem Katalog von Sicherheitsanforderungen (IT-Sicherheitskatalog) die Anforderungen an den angemessenen Schutz. Dabei beteiligt die Bundesnetzagentur die Betreiber von Energieversorgungsnetzen und deren Branchenverbände. Die Bundesnetzagentur überprüft den IT-Sicherheitskatalog alle zwei Jahre und aktualisiert ihn bei Bedarf im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik. (...)

(2) (...) Die Bundesnetzagentur bestimmt im Einvernehmen ~~Benehmen~~ mit dem Bundesamt für Sicherheit in der Informationstechnik durch Festlegung nach § 29 Absatz 1 in einem IT-Sicherheitskatalog die Anforderungen an den angemessenen Schutz. Dabei beteiligt die Bundesnetzagentur die Betreiber nach Satz 1 und deren Branchenverbände. Die Bundesnetzagentur überprüft den IT-Sicherheitskatalog alle zwei Jahre und aktualisiert ihn bei Bedarf im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik. (...)"

Einschränkungen bei der Fehlersuche im Schadsoftware-Erkennungssystem aufheben

Das BSI betreibt ein Schadsoftware-Erkennungssystem (SES) mit Detektoren, um die Netze des Bundes und die Kommunikation zwischen Behörden zu schützen. Beim Ausfall eines Detektors aufgrund von Datenfehlern läuft dieser bis zur Fehlerbehebung nicht weiter, wodurch die Schutzwirkung des SES gemindert ist. Aktuell besteht jedoch eine Beschränkung bei der anlassbezogenen Auswertung in solchen Ausnahmefällen auf Protokolldaten nach § 5 BSIG und erschwert die schnelle Fehlerbehebung und damit den Einsatz des Detektors im laufenden Betrieb. Denn in der Praxis lassen sich Fehlerquellen nicht über diesen Weg finden, wenn die Fehlerquelle in den Schnittstellendaten liegt. Die bestehende Auswertungsbefugnis des BSI für die Fehlersuche im SES sollte daher zielführend angepasst werden, um die bestehende Lücke bei der Absicherung der Netze des Bundes zu schließen. Aus fachlicher Sicht des BSI sollte hierfür nachfolgende Änderung umgesetzt werden:

⇨ *Empfehlung zur Änderung von § 8 Absatz 3 BSIG-E:*

„(3) Zur Sicherstellung einer fehlerfreien automatisierten Auswertung dürfen Protokolldaten vor ihrer Pseudonymisierung und Speicherung sowie Schnittstellendaten manuell verarbeitet werden.
Liegen Hinweise vor, dass die fehlerfreie automatisierte Auswertung wegen eines erheblichen Fehlers erschwert wird, darf der Personenbezug von Protokolldaten zur

Sicherstellung der fehlerfreien automatisierten Auswertung wiederhergestellt werden, sofern dies im Einzelfall erforderlich ist; Absatz 2 Satz 3 bis 6 gilt entsprechend."

Lagebild weiter vervollständigen durch „Nullmeldungen" der Nachrichtendienste

Für ein vollständiges Lagebild ist es für das BSI relevant zu erfahren, wie häufig sicherheitsrelevante Meldungen vonseiten der Nachrichtendienste bspw. aufgrund von Geheimschutzregelungen oder Vereinbarungen mit Dritten nicht an das BSI weitergegeben werden. Ist diese „Dunkelziffer" dem BSI dagegen nicht vollumfänglich bekannt, reduziert diese Unklarheit die fachlich fundierte Einschätzung der aktuellen Cybersicherheitslage Deutschlands. Der Regierungsentwurf formuliert hierfür richtigerweise eine jährliche verpflichtende Weitergabe der Gesamtzahl solcher Nichtmeldungen anderer Behörden an das BSI – davon ausgenommen sind im Entwurf jedoch der Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz. Seitens des BSI wird von einer kleinen Zahl solcher Nichtmeldungen ausgegangen, sodass durch die zahlenmäßige Erfassung bei BND und BfV kaum Aufwände erzeugt werden dürften. Würde die Zahl der Nichtmeldungen eine erhebliche Größe annehmen, entstünde ein Informationsdefizit im BSI, welches aus Sicht des BSI für die IT-Sicherheit des Bundes nicht akzeptabel wäre. Die Ausnahme für BND und BfV sollte daher entfallen. Aus fachlicher Sicht des BSI sollte hierfür nachfolgende Änderung umgesetzt werden:

⇨ *Empfehlung zur Streichung von § 43 Abs. 5 Satz 5 BSIG-E:*

„Ausgenommen von der Pflicht nach Absatz 5 Satz 3 sind der Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz."

5 Zuständigkeiten im Bereich Energie klar zuordnen

Der Regierungsentwurf führt in Verbindung mit § 5c EnWG zu gedoppelten Zuständigkeiten von BNetzA und BSI für Betreiber im Energiesektor. Zugleich bestände aber aufgrund der derzeitigen Ausgestaltung im Gesetzesentwurf für die betroffenen Unternehmen entweder keine Nachweispflicht über die Absicherung der IT bzw. Teile eines Unternehmens müssten dem BSI und andere Teile der BNetzA entsprechende Nachweise erbringen. Letzteres würde einen erheblichen bürokratischen Mehraufwand für die Betreiber nach sich ziehen. Daher sollte unbedingt eine Zersplitterung der Zuständigkeiten für die IT-Sicherheit in KRITIS-Sektoren vermieden werden. Wie im Koalitionsvertrag vereinbart sollte daher das BSI als zentrale Stelle für Cybersicherheit gestärkt werden und die Zuständigkeit für den Schutz der Cybersicherheit Kritischer Infrastrukturen gebündelt beim BSI verortet werden. Mindestens jedoch sollte die Office-IT in jedem Fall unter BSI-Aufsicht stehen, um eine gleiche Regulierung über alle Sektoren hinweg sicherzustellen und somit die IT-Sicherheit und Versorgungssicherheit zu erhöhen sowie die Anwendbarkeit für Betreiber zu erleichtern. Aus fachlicher Sicht des BSI sollte hierfür nachfolgende Änderung umgesetzt werden:

⇨ *Empfehlung zur Anpassung von § 28 Abs. 4 BSIG-E:*

„(4) Die §§ 30, 31, 32, 35, 36, 38, 39, 61 und 62 sind nicht anzuwenden auf besonders wichtige Einrichtungen und wichtige Einrichtungen, ~~die~~ soweit sie

1. ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen;
2. Energieversorgungsnetze oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 1 des Gesetzes vom 14. Mai 2024 (BGBl. 2024 I Nr. 161) geändert worden ist, betreiben und den Regelungen des § 5c des Energiewirtschaftsgesetzes unterliegen. (...)“

⇨ *Empfehlung zur Anpassung von § 5c Abs. 3 EnWG-E:*

- Streichen von Nr. 12 in § 5c Abs. 3 Satz 3 EnWG-E

6 Effektives Informationssicherheitsmanagementsystem für den Bund sicherstellen

Damit der CISO Bund nicht ein rein koordinierender „Papiertiger“ wird, muss er ein funktionierendes, effektives Informationssicherheitssystem mit Durchschlagskraft beaufsichtigen. Um dem Anspruch gerecht zu werden, ein hohes Niveau in der Cybersicherheit für die gesamte Bundesverwaltung sicherzustellen, müssen aus hiesiger Sicht drei wesentliche Aspekte erfüllt sein: Entsprechende IT-Sicherheitsvorgaben müssen für die gesamte Bundesverwaltung gelten; die Einrichtungen des Bundes müssen ihre Pflichten eigenverantwortlich umsetzen; die Rechtslage muss es dem BSI ermöglichen, Sicherheitsvorgaben flexibel und zeitnah an die technischen Entwicklungen anzupassen – auch um bürokratischen Mehraufwand für alle Beteiligten zu vermeiden. Aus fachlicher Sicht des BSI sollte hierfür nachfolgende Änderungen umgesetzt werden:

a) <u>Erfassung der gesamten Bundesverwaltung unter Beibehaltung bestehender Ausnahmen</u>
Um effektiv ein hohes Cybersicherheitsniveau für den Bund gewährleisten zu können, muss auch die Bundesverwaltung zur Einhaltung angemessener IT-Sicherheitsvorgaben verpflichtet werden. Während der Regierungsentwurf die Vorgaben für die Wirtschaft maßgeblich erhöht, werden die Pflichten für den öffentlichen Sektor dagegen reduziert. Damit würden die IT-Sicherheitsvorgaben für den Bund im Vergleich zum aktuellen Stand sogar verringert.
Der Regierungsentwurf beschränkt die IT-Sicherheitsvorgaben für die Bundesverwaltung auf das Bundeskanzleramt und die Mehrheit der Bundesministerien. Die jeweils nachgeordneten Einrichtungen der Ressorts fallen nicht unter die verpflichtenden Vorgaben. Dies unterminiert das Ziel eines durchgehend hohen IT-Sicherheitsniveaus in der gesamten Bundesverwaltung. Zudem sieht der Gesetzesentwurf neue Ausnahmen von den Sicherheitsvorgaben für das Auswärtige Amt (AA) und das Bundesministerium

der Verteidigung (BMVg) vor, die weit über die bestehenden Ausnahmen gemäß IT-SiG 2.0 hinausgehen. Sachgründe für diese geplante Erweiterung gibt es aus Sicht des BSI nicht. Die bestehenden Ausnahmen im BSIG für AA und BMVg sollten nicht erweitert werden, um einer Fragmentierung des Cybersicherheitsniveaus auf Bundesebene entgegenzuwirken.

⇨ *Empfehlung für einheitliche IT-Sicherheitsvorgaben für die gesamte Bundesverwaltung und Beibehaltung der bestehenden Ausnahmen für AA und BMVg:*

1. Die Begrifflichkeit "Einrichtungen der Bundesverwaltung" durch "*Einrichtungen des Bundes*" im gesamten Gesetz ersetzen.

2. Weitere Anpassungen:
   § 2 Abs. 1 BSIG-E um folgende Definition ergänzen:
   „9a. Einrichtungen des Bundes die Bundesbehörden, einschließlich derjenigen öffentlichen Stellen, die zur Erfüllung der öffentlichen Aufgaben dieser Behörden Informationstechnik betreiben."

   und es wird ergänzt:
   „Das Bundesamt kann für öffentliche Stellen, die nicht bereits Absatz 1 Nummer 9a unterfallen, im Benehmen mit der für diese Stelle zuständigen obersten Bundesbehörde feststellen, dass die Stelle eine Einrichtung des Bundes im Sinne dieses Gesetzes ist, wenn sich andernfalls Risiken für die Informationstechnik des Bundes ergeben."

   § 29 BSIG-E wird ersetzt mit:
   „(1) Für Einrichtungen des Bundes, die nicht von § 28 erfasst sind, gelten die Pflichten für besonders wichtige Einrichtungen dieses Teils entsprechend.

   (2) Die Ausnahmen nach § 7 Absätze 6 und 7 gelten für die Pflichten nach diesem Teil entsprechend."

   und in § 28 Abs. 1 BSIG-E wird Satz 2 gestrichen:
   „~~Davon ausgenommen sind Einrichtungen der Bundesverwaltung, sofern sie nicht gleichzeitig Betreiber kritischer Anlagen sind~~."

   und in § 28 Abs. 2 BSIG-E wird Satz 2 gestrichen:
   „~~Davon ausgenommen sind besonders wichtige Einrichtungen und Einrichtungen der Bundesverwaltung~~."

b) Klarstellung der Pflichten und Mittelallokation für Informationssicherheit

Damit Nachweispflichten für die Einrichtungsleitungen in der Bundesverwaltung nicht durch fehlende Bestimmung ins Leere laufen, ist eine rechtliche Erläuterung notwendig, was mit „Gewährleistung der Informationssicherheit" gemeint ist. Durch klare Vorgaben wird Rechtssicherheit geschaffen. Ergänzend dazu sollte festgehalten werden,

dass zur Gewährleistung der Informationssicherheit auch die Bereitstellung einer angemessenen Finanzierung zählt.

⇨ *Empfehlung zur Ergänzung § 43 Abs. 1 BSIG-E um nachfolgende Sätze 2 und 3:*

„Die Informationssicherheit wird grundsätzlich durch die Einhaltung der Risikomanagementpflichten nach § 30 gewährleistet. Zu den Voraussetzungen zur Gewährleistung der Informationssicherheit zählt der Einsatz angemessener finanzieller Mittel."

c) Möglichkeit zur flexiblen Anpassung der Sicherheitsvorgaben durch BSI

Damit das BSI die erforderlichen Sicherheitsvorgaben für die Bundesverwaltung an technologische Weiterentwicklungen zeitnah anpassen kann, sollte keine rechtliche Festlegung ausschließlich auf Mindestandards und IT-Grundschutz erfolgen. Vielmehr sollte das Gesetz technologieoffen ausgestaltet sein und stattdessen den Begriff der „Vorgaben" verwenden. Durch die unten vorgeschlagene Anpassung im Regierungsentwurf würde ein einheitlicher Schutzstandard für alle gesellschaftskritischen Tätigkeiten, unabhängig davon, ob Staat oder Wirtschaft, etabliert. Gleichzeitig bleibt es dem BSI möglich, verwaltungsintern weitere bedarfsgerechte Vorgaben zu machen, bspw. für die digitale Verarbeitung von Verschlusssachen in IT-Systemen.

⇨ *Empfehlung zur Anpassung des § 44 BSIG-E:*

Die bisherigen § 44 Absätze 1-3 werden mit einem neuen Absatz 1 ersetzt:

„(1) Soweit erforderlich legt das Bundesamt im Benehmen mit den Ressorts Vorgaben für die Sicherheit der Informationstechnik des Bundes zu den nach § 30 zu erfüllenden Anforderungen für die Einrichtungen des Bundes fest. Für die in § 2 Absatz 1 Nummer 18 genannten Gerichte und Verfassungsorgane haben die Vorschriften nach Satz 1 empfehlenden Charakter."

Absatz 4 wird zu Absatz 2;

Absatz 5 wird Absatz 3;

und § 44 Absatz 6 wird zu Absatz 4 und wie folgt gefasst:

„(4) Die oder der Bundesbeauftragte für Informationssicherheit kann im Benehmen mit den Ressorts festlegen, dass die Einrichtungen des Bundes verpflichtet sind, nach § 19 bereitgestellte IT-Sicherheitsprodukte beim Bundesamt abzurufen. Eigenbeschaffungen sind in diesem Fall nur zulässig, wenn das spezifische Anforderungsprofil den Einsatz abweichender Produkte erfordert. Dies gilt nicht für die in § 2 Nummer 21 genannten Gerichte und Verfassungsorgane."

7 Schwachstellenmanagement des BSI

Aus fachlicher Sicht des BSI sollten Sicherheitslücken grundsätzlich dem koordinierten Prozess zur Schließung zugeführt werden. Dies erfüllt das BSI bereits über seinen etablierten CVD-Prozess. Um die Unabhängigkeit des BSI bei dieser Aufgabe sicherzustellen und den Anreiz zur Meldung von Schwachstellen an das BSI zu erhöhen, sollte sichergestellt werden, dass das BSI bei der Meldung von Sicherheitslücken an Hersteller keinen Weisungen durch das BMI unterliegt. Aus fachlicher Sicht des BSI sollten hierfür nachfolgende Änderungen umgesetzt werden:

- ⇨ *Empfehlung zur Anpassung von § 5 BSIG-E:*

  An § 5 Abs. 1 BISG-E wird folgender Satz angefügt:
  „Das Bundesamt wirkt unverzüglich auf die Behebung von Schwachstellen hin."

  An § 5 Abs. 5 BSIG-E wird folgender Satz angefügt:
  „Weisungen an das Bundesamt, die eine Weitergabe von Informationen über Sicherheitslücken in Produkten an den Hersteller dieser Produkte untersagen, sind unzulässig."