VERBAND DER INTERNETWIRTSCHAFT E.V.

Stellungnahme

zum Referentenentwurf des Bundesministeriums des Innern für ein Gesetz zur Stärkung der Cybersicherheit

Berlin, 17.03.2026

Der Referentenentwurf zielt darauf ab, die Cybersicherheitsarchitektur des Bundes zu stärken und die Handlungsfähigkeit der Sicherheitsbehörden bei Angriffen auf informationstechnische Systeme zu erweitern. Dieses Anliegen unterstützen wir grundsätzlich. Zugleich enthält der Entwurf Regelungen, die sehr weitreichende Eingriffe in digitale Infrastrukturen ermöglichen und erhebliche Mitwirkungspflichten für Anbieter vorsehen.

Für eine wirksame und zugleich verhältnismäßige Cyberabwehr braucht es klare Zuständigkeiten, eng begrenzte Befugnisse und einen konsequent kooperativen Ansatz mit der Wirtschaft. Insbesondere offensive oder quasi-offensive Gegenmaßnahmen im Cyberraum bergen hohe technische, rechtliche und außenpolitische Risiken. Vor diesem Hintergrund adressieren wir nachfolgend die aus unserer Sicht zentralen Punkte.

1. Begrifflichkeiten

Er Referentenentwurf verwendet an mehreren Stellen den Begriff „maliziöse Domains“, ohne dabei hinreichend trennscharf zwischen unterschiedlichen Fallgruppen zu unterscheiden. Für eine praxistaugliche und rechtssichere Anwendung sollte dabei jedoch klar zwischen Domains unterschieden werden, die gezielt für missbräuchliche Zwecke registriert wurden („maliciously registered“), und solchen, die ursprünglich legitim waren, aber nachträglich kompromittiert wurden („compromised domains“). Dies ist etwa der Fall, wenn Webserver Sicherheitslücken aufweisen, die von Angreifern ausgenutzt werden, um über die kompromittierten Server Spam zu versenden, Botnetze zu betreiben oder dort Webseiten für illegale Zwecke vorzuhalten. Gerade bei kompromittierten Domains besteht ein erhebliches Risiko unverhältnismäßiger Kollateralschäden. Domainbasierte Maßnahmen auf DNS-Ebene können regelmäßig nicht auf einzelne Pfade oder Inhalte begrenzt werden und treffen deshalb schnell auch rechtmäßige Angebote und unbeteiligte Dritte. Das gilt insbesondere in Konstellationen gemeinsamer Domain-Nutzung, etwa bei Franchise-Strukturen oder anderen Mehrnutzer-/Mandantenmodellen, in denen unterschiedliche Akteure unter derselben Domain auftreten. In solchen Fällen droht Overblocking, wenn wegen eines einzelnen betroffenen Teilbereichs faktisch die gesamte Domain „abgeschaltet“ oder für Nutzer unzugänglich gemacht wird. Vor diesem Hintergrund sollte der Entwurf den Begriff und Anwendungsbereich klar definieren und sicherstellen, dass bei kompromittierten Domains keine oder, wenn Maßnahmen auf DNS-Ebene geregelt werden sollen, was eco grundsätzlich ablehnt, vorrangig abgestufte, möglichst granulare, zeitlich eng befristete und reversible Vorgehensweisen sowie Prozesse vorgesehen werden, um einem Overblocking unverzüglich Abhilfe schaffen zu können. Einschneidende domainweite Maßnahmen sollten nur als ultima ratio in Betracht kommen.

2. § 11 BSI-G

Der Entwurf sieht vor, dass das BSI Informationen zu Domains, von denen Sicherheitsrisiken für die Informationstechnik ausgehen, entgegennimmt, auswertet und hierzu geeignete Informationen öffentlich bereitstellt. Zugleich sollen DNS-Diensteanbieter ab einer bestimmten Unternehmensgröße verpflichtet werden, ihren Kunden auf dieser Grundlage einen DNS-basierten Schutz anzubieten. Aus Sicht der Internetwirtschaft ist dabei zu berücksichtigen, dass bereits heute ein breites Spektrum kommerzieller und nicht-kommerzieller Threat-Intelligence-Angebote existiert, die einschlägige Indikatoren, etwa zu Phishing- und Malware-Infrastrukturen, bereitstellen. Wenn das BSI nun selbst eine öffentlich einsehbare Liste führen und Anbietern zur Verfügung stellen würde, würde es in direkte Konkurrenz zur Privatwirtschaft treten. Eine solche Wettbewerbsverzerrung sollte vermieden werden, zumal der Entwurf offenlässt, ob der Dienst ohne oder gegen Vergütung angeboten werden soll.

Darüber hinaus sind die Kriterien und Verfahren zur Aufnahme in eine solche Liste sowie zur Korrektur und Entfernung nicht transparent und nachvollziehbar. Zwar wird eine regelmäßige Aktualitätsprüfung sowie die Behandlung von Beschwerden erwähnt, es fehlt jedoch an klaren Maßstäben, Dokumentationsanforderungen und verlässlichen Abläufen, wie Betroffene eine Listung überprüfen lassen und eine zeitnahe Delistung erreichen können, was gegen das Agieren des BSI als Listenanbieter spricht.

Schließlich ist die Fokussierung auf Domains als alleinigen Indikator in der Praxis zumeist zu grob. Für eine zielgenaue Abwehr sind vielmehr konkrete URLs, Subdomains oder weitere technische Indikatoren (z. B. IP-Adressen oder Zertifikatsmerkmale) erforderlich. Rein domainbasierte Listungen und darauf aufbauende Schutzmaßnahmen bergen erhebliche Overblocking-Risiken, etwa wenn auf großen Plattformen oder unter gemeinsam genutzten Domains nur einzelne Unterseiten oder Angebote missbräuchlich genutzt werden, während die übrigen Inhalte rechtmäßig sind. Außerdem bleiben die missbräuchlichen Inhalte häufig weiterhin über weitere Adressen erreichbar. Daher empfiehlt eco stets den Ansatz, zuerst den Takedown solcher Inhalte zu erreichen.

3. Weitreichende Cyberabwehrbefugnisse der Bundespolizei in § 41a BPolG-E

Der Entwurf räumt der Bundespolizei in § 41a BPolG-E ein breites Spektrum an Abwehrmaßnahmen ein bis hin zu Eingriffen in Datenströme und technischen Maßnahmen an informationstechnischen Systemen. Aus Sicht der Internetwirtschaft bedarf es hier einer deutlich engeren Eingrenzung: Staatliche Stellen sollten nicht eigenständig in Netze und Systeme von Telekommunikations- und Diensteanbietern eingreifen, sondern, soweit erforderlich, klar definierte Maßnahmen gegen konkrete Gefahren anordnen können.

Zielführend erscheint alleinig eine klar begrenzte Anordnungsbefugnisse für defensive Maßnahmen, wie die Unterbindung von Botnet-Kommunikation oder die Umleitung eindeutig maliziösen Datenverkehrs. Ein solches Vorgehen kann effektiv sein, ohne die Integrität der Netze unnötig zu gefährden.

4. Staatliche Hackbacks kein verhältnismäßiges Abwehrmittel

Maßnahmen, die auf das Löschen oder Verändern von Daten durch technische Mittel abzielen und faktisch als „Hackback“ zu qualifizieren sind, sind aus Sicht der Internetwirtschaft hoch

problematisch. In der Praxis ist häufig bereits eine robuste, rein defensive Abwehr (z. B. Blockierung von Kommunikationsbeziehungen, Härtung betroffener Systeme, Isolierung kompromittierter Komponenten) geeignet, Angriffe zu stoppen oder einzudämmen.

Hinzu kommt, dass nicht verlässlich sichergestellt werden kann, dass Gegenmaßnahmen tatsächlich die Systeme der Angreifer treffen. Fehlende oder fehlerhafte Attribution sowie die Nutzung fremder Infrastruktur durch Angreifer erhöhen das Risiko, Unbeteiligte zu beeinträchtigen. Gerade vor dem Hintergrund grenzüberschreitender Angriffslagen ist zudem zu vermeiden, dass nationale Alleingänge zu Eskalations- oder völkerrechtlichen Konfliktszenarien führen.

5. Mitwirkungspflichten für Anbieter präzisieren und begrenzen

Die im Entwurf vorgesehenen Mitwirkungspflichten für Telekommunikations- und digitale Diensteanbieter sind derzeit zu unbestimmt. Insbesondere ist unklar, was eine „unverzügliche Mitwirkung“ im Einzelfall umfasst und welche technischen oder organisatorischen Leistungen hierunter fallen sollen.

Mitwirkungspflichten sollten sich auf klar definierte, verhältnismäßige Unterstützungsleistungen beschränken (z. B. Umsetzung einer rechtmäßigen Anordnung zur Umleitung/Blockierung eindeutig maliziösen Verkehrs, Erteilung erforderlicher Auskünfte). Eine Verpflichtung privater Anbieter zur Unterstützung von Hackback-Maßnahmen ist abzulehnen. Offensive Gegenmaßnahmen sind, wenn überhaupt, Teil staatlicher Gefahrenabwehr im Rahmen des Gewaltmonopols und dürfen nicht in Verantwortung, Haftungsrisiken oder operative Abläufe der Privatwirtschaft verlagert werden.

6. Erforderlichkeit klarer Definitionen, Ultima-Ratio-Prinzip, Schwachstellenmanagement

Sollten Gegenmaßnahmen im Cyberraum im weiteren Verfahren dennoch erwogen werden, braucht es einen klaren gesetzlichen Begriffsrahmen und strikte Voraussetzungen, insbesondere einen engen zeitlichen und sachlichen Zusammenhang zwischen Angriff und Gegenmaßnahme, die strikte Beachtung des Gebots des mildesten Mittels einschließlich eines Ultima-Ratio-Vorbehalts, die höchste Priorität für den Schutz Unbeteiligter verbunden mit wirksamer Vermeidung von Kollateralschäden sowie belastbare Transparenz-, Bericht- und Kontrollmechanismen.

Unbedingt auszuschließen sind Reaktionsketten, die eine Verbindung zu konventionellen Mitteln militärischer Gewalt herstellen könnten. Ebenso darf ein möglicher Hackback-Rechtsrahmen nicht dazu führen, dass staatliche Stellen Sicherheitslücken für operative Zwecke zurückhalten. Ein konsequentes Schwachstellenmanagement mit Vorrang für Schließung und verantwortungsvolle Offenlegung ist Grundvoraussetzung für Cybersicherheit.

7. Kooperative Ausgestaltung des Datenaustauschs mit dem BSI nach § 15 Abs. 6 BSIG-E

Die Pflicht zur Bereitstellung umfassender Verkehrs-, Steuerungs- und technischer Daten an das BSI ist in der derzeitigen Ausgestaltung zu weitreichend. Statt einer einseitigen Herausgabepflicht sollte ein Kooperationsmodell mit klaren Zweckbindungen und beiderseitigem Nutzen im Vordergrund stehen. Dafür braucht es zunächst Transparenz darüber, wofür das „Lagebild“ konkret genutzt wird, welche Stellen daran beteiligt sind und welche Folgemaßnahmen bei einem negativen Lagebild überhaupt vorgesehen sind. Gleichzeitig sollte der Austausch ausdrücklich wechselseitig angelegt werden. Das BSI sollte verpflichtet sein, sicherheitsrelevante Informationen

und Erkenntnisse zeitnah, strukturiert und in einer für die betroffenen Unternehmen verwertbaren Form zurückzuspielen.

Da es sich um hochsensible Daten handelt, müssen Vertraulichkeit und Schutz besonders abgesichert werden. Zugriff und Weitergabe von Daten sind strikt auf das zwingend Erforderliche zu begrenzen und durch geeignete technisch-organisatorische Maßnahmen abzusichern. Ebenso sollten die technischen Rahmenbedingungen des Austauschs praxistauglich geregelt werden, indem Schnittstellen, Kanäle und Formate standardisiert und Ende-zu-Ende abgesichert sind einschließlich einer etwaigen Weitergabe von Erkenntnissen durch das BSI. Schließlich ist sicherzustellen, dass sämtliche Übermittlungen DSGVO-konform und streng zweckgebunden erfolgen und der Grundsatz der Datenminimierung eingehalten wird. Personenbezogene Daten sollten, soweit im Einzelfall erforderlich, über die bestehenden Verfahren der Bestandsdatenauskunft unter Einbindung der hierfür spezialisierten Stellen angefragt werden. Nicht zuletzt ist der erhebliche Ressourcenaufwand für die Erhebung und Aufbereitung zu berücksichtigen. Eine angemessene Kostenerstattung sollte vorgesehen werden, um insbesondere spezialisierte Cybersicherheitsdienstleister nicht zu benachteiligen.

8. Regelungen des § 16a BSIG-E

Die in § 16a BSIG-E vorgesehene Befugnis zielt darauf ab, über Eingriffe in die DNS-Auflösung (bis hin zur Änderung von Nameserver-Einträgen) den Zugriff auf bestimmte Inhalte zu unterbinden bzw. Nutzer auf eine vom BSI bereitgestellte Informationsseite umzuleiten. Ein solch „quellennahes“ Instrument ist jedoch besonders eingriffsintensiv, weil es nicht nur einzelne Inhalte adressiert, sondern typischerweise die Erreichbarkeit ganzer Domains beeinflusst. Damit stellt sich in besonderer Weise die Frage der Verhältnismäßigkeit sowie der praktischen Umsetzbarkeit für Registries und Registrare, die die Maßnahme auf Anordnung kurzfristig technisch umzusetzen hätten. Zugleich besteht ein erhebliches Risiko von Overblocking, wenn unter einer Domain auch rechtmäßige Angebote oder unbeteiligte Dritte betroffen sind. Zusätzlich sind Transparenzanforderungen zu berücksichtigen, damit nachvollziehbar bleibt, auf welcher Grundlage eine Umleitung erfolgt und wie lange sie andauert.

Besonders kritisch ist zudem, dass nach der vorgesehenen Ausgestaltung Rechtsbehelfe gegen die Anordnung keine aufschiebende Wirkung entfalten. Damit tritt die faktische Korrektur einer möglicherweise fehlerhaften Listung oder Anordnung erst nachträglich ein, obwohl die Maßnahme unmittelbar erhebliche Auswirkungen auf betroffene Anbieter und Nutzer haben kann. Vor diesem Hintergrund halten wir es für erforderlich, dass § 16a BSIG-E nur unter eng definierten Voraussetzungen, mit klaren Verfahrensgarantien, einer wirksamen und schnellen Überprüfbarkeit sowie mit möglichst granularen, zeitlich befristeten und reversiblen Maßnahmen ausgestaltet wird.

9. Befugnisse des BKA nach §§ 62 b – e BKAG-E

Die im BKAG-E vorgesehenen Cyberabwehrbefugnisse entsprechen in wesentlichen Teilen den Regelungen zur Bundespolizei, gehen jedoch durch eine generalklauselartige Ausgestaltung teilweise darüber hinaus. Für das BKA müssen mindestens dieselben strengen Anforderungen gelten: klare Tatbestandsvoraussetzungen, eng umgrenzte Maßnahmenkataloge, wirksame Kontrolle und ein Vorrang defensiver, kooperativer Instrumente. Soweit der Entwurf die Möglichkeit eröffnet, auch

nicht ausdrücklich geregelte Maßnahmen zu ergreifen, halten wir dies für besonders kritisch und revisionsbedürftig.

10. § 50 Abs. 1 BSIG-E

Nach § 50 Abs. 1 BSIG-E entfällt für privilegierte Behörden (§ 2 Nr. 2 Buchst. a sowie c–e) die bisherige Pflicht, ein berechtigtes Interesse darzulegen. Übrig bleibt jedoch das Tatbestandsmerkmal, dass der Zugang „soweit dies für die Erfüllung ihrer Aufgaben erforderlich ist“ gewährt werden soll.

Der Begriff der „Erforderlichkeit“ ist ein unbestimmter Rechtsbegriff des Verwaltungs- und Polizeirechts. Seine Bewertung setzt regelmäßig Kenntnis der konkreten Aufgabenwahrnehmung sowie der zugrunde liegenden Gefahren- oder Ermittlungszusammenhänge voraus. Diese Bewertung kann realistischerweise nur durch die antragstellende Behörde selbst erfolgen. Die Normadressaten verfügen in der Regel weder über die notwendige Sachnähe noch über die rechtliche Kompetenz, um beurteilen zu können, ob eine konkrete Datenabfrage tatsächlich für die Aufgabenerfüllung der ersuchenden Behörde erforderlich ist. Hinzu kommt, dass die Normadressaten nicht überprüfen können, ob eine anfragende Stelle die geltend gemachten Aufgaben tatsächlich wahrnimmt oder ob die Datenabfrage in einem hinreichenden sachlichen Zusammenhang mit diesen Aufgaben steht.

Die Norm führt damit faktisch dazu, dass die Normadressaten eine Prüfung der Voraussetzungen vornehmen müssen, ohne über die hierfür erforderlichen Informationen oder Prüfmaßstäbe zu verfügen. Mithin sollte, wenn denn die seitens eco abzulehnende Aufweichung umgesetzt werden soll, ergänzt werden, dass der ersuchende Zugangsnachfrager im Antrag zu erklären hat, dass die Abfrage für die Erfüllung seiner gesetzlichen Aufgaben erforderlich ist.

Auch die vorgesehene Ergänzung, nach der „die Verantwortung für die Zulässigkeit des Antrags die ersuchenden Zugangsnachfrager tragen“, löst dieses Problem nur zum Teil. Die Normadressaten bleiben weiterhin verpflichtet, innerhalb einer Frist von 72 Stunden über die Herausgabe personenbezogener Daten zu entscheiden, wobei sie zugleich die Anforderungen der DSGVO zu beachten haben. Ohne eine nachvollziehbare Darlegung der rechtlichen Grundlage oder des berechtigten Interesses besteht für die Anbieter das Risiko einer rechtlichen Pflichtenkollision: Eine vorschnelle Herausgabe kann einen Verstoß gegen die DSGVO darstellen, während eine zurückhaltende oder verzögerte Herausgabe als Verstoß gegen § 50 BSIG gewertet werden könnte.

Zusätzlich problematisch ist die geplante Öffnung des § 50 Abs. 1 BSIG für „sonstige Zugangsnachfrager“. Damit würde das BSIG, dessen Zweck primär in der Stärkung der Cybersicherheit liegt, zu einem Instrument allgemeiner privater Rechtsdurchsetzung erweitert. Für die Durchsetzung zivilrechtlicher Ansprüche existieren jedoch bereits etablierte und prozedural abgesicherte Instrumente wie § 21 TDDDG sowie die spezialgesetzlichen Auskunftsansprüche in § 19 MarkenG, § 101 UrhG und § 140b PatG. Diese Regelungen enthalten differenzierte Voraussetzungen. Die Schaffung einer parallelen Auskunftsstruktur im BSIG würde demgegenüber eine Vielzahl fachfremder Anfragen ohne unmittelbaren Bezug zur IT-Sicherheit erzeugen.

Für die Normadressaten entstünde dadurch eine zusätzliche Prüfrolle unter erheblichem Zeitdruck. In vergleichbaren Auskunftsregelungen des Immaterialgüterrechts wird die Herausgabe von Daten regelmäßig an qualifizierte Voraussetzungen wie das Vorliegen einer offensichtlichen Rechtsverletzung geknüpft. Demgegenüber würde § 50 BSIG-E bereits die bloße Darlegung eines berechtigten Interesses genügen lassen und zugleich die Prüfung dieser Voraussetzung auf die Normadressaten verlagern.

Der Begriff des berechtigten Interesses ist ein unbestimmter Rechtsbegriff, dessen Vorliegen eine materiell-rechtliche Bewertung des zugrunde liegenden Sachverhalts erfordert. Für die Normadressatenstellt sich damit die Frage, anhand welcher Kriterien sie beurteilen sollen, ob das geltend gemachte Interesse tatsächlich rechtlich anerkennenswert ist. Insbesondere bei Anfragen privater Akteure fehlt es den Anbietern an der notwendigen Sachnähe sowie an Ermittlungs- und Bewertungsbefugnissen, um behauptete Rechtsverletzungen, etwa im Bereich der Marken-, Kennzeichen- oder Urheberrechte, innerhalb der vorgesehenen 72-Stunden-Frist rechtssicher zu beurteilen.

Die Anbieter stehen daher vor der Wahl, entweder durch eine vorschnelle Datenherausgabe datenschutzrechtliche Risiken einzugehen oder durch eine ablehnende Entscheidung gegen die Auskunftspflichten nach § 50 BSIG zu verstoßen.

Wenn private Akteure tatsächlich Opfer einer erheblichen Cybergefahr werden, steht ihnen der rechtsstaatlich vorgesehene Weg über die zuständigen Sicherheitsbehörden offen. Diese verfügen über die erforderlichen gesetzlichen Befugnisse und die fachliche Expertise, um Gefährdungslagen zu bewerten und im Rahmen der Gefahrenabwehr oder Strafverfolgung erforderliche Datenabfragen vorzunehmen.

Eine unmittelbare Abfragebefugnis privater Akteure im Kontext der Cybersicherheit ist daher weder erforderlich noch systematisch überzeugend. Es besteht vielmehr die Gefahr, dass die Norm zu umfangreichen Datenabfragen ohne hinreichende Vorprüfung führt und somit „Fishing Expeditions“ sowie Data-Mining unter dem Deckmantel der eines Gesetzes zur Stärkung der Cybersicherheit erleichtert.

Fazit

Der Referentenentwurf adressiert die Stärkung der Cybersicherheit und eine bessere staatliche Reaktionsfähigkeit. In der vorliegenden Fassung bleibt jedoch offen, ob die vorgesehenen Instrumente dieses Ziel tatsächlich erreichen, ohne unverhältnismäßige Eingriffe, Overblocking-Risiken und erhebliche Umsetzungsprobleme zu erzeugen.

Wirksamer Schutz gelingt nur, wenn Befugnisse klar begrenzt, rechtssicher ausgestaltet und in der Umsetzung eng mit der Wirtschaft verzahnt werden. Dazu gehören präzise Begrifflichkeiten, insbesondere die trennscharfe Abgrenzung zwischen missbräuchlich registrierten und kompromittierten Domains, sowie Maßnahmen, die Overblocking und Kollateralschäden vermeiden.

Mit dem Entwurf werden DNS-Diensteanbieter zu DNS-basierten Schutzmaßnahmen verpflichtet. Gerade weil der Regelungsrahmen zugleich domainweite Eingriffe bis hin zur in der Begründung ausdrücklich genannten „Dekonnektierung“ ermöglicht, müssen die Voraussetzungen eng begrenzt, die Verfahren transparent und die Overblocking-Risiken wirksam minimiert werden. Besonders kritisch ist dabei, dass Rechtsbehelfe nach § 16a BSIG-E keine aufschiebende Wirkung haben.

Ebenso sollten behördliche Eingriffsbefugnisse strikt defensiv ausgerichtet bleiben. Hackback-Ansätze sind technisch riskant und rechtlich wie außenpolitisch hoch problematisch. Beim Datenaustausch mit dem BSI braucht es klare Zweckbindungen, hohe Schutzstandards, wechselseitigen Mehrwert und praktikable Verfahren. Schließlich sind bei Auskunftspflichten nach § 50 BSIG-E Rechtsklarheit, Datenschutzkonformität und eine Vermeidung fachfremder, privater Rechtsdurchsetzung sicherzustellen. Insgesamt sollte der Entwurf auf Resilienz, schnelle

Bereinigung/Takedown, Schwachstellenmanagement und Kooperation setzen statt auf weitreichende Eingriffe mit hohen Folgerisiken.

Über eco: Mit rund 1.000 Mitgliedsunternehmen ist eco (www.eco.de) der führende Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, schafft Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. eco hat Standorte in Köln, Berlin und Brüssel. eco setzt sich in seiner Arbeit vorrangig für ein leistungsfähiges, zuverlässiges und vertrauenswürdiges Ökosystem digitaler Infrastrukturen und Dienste ein.