Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)523 H

Stellungnahme zum Entwurf des NIS2-Umsetzungsgesetzes

Prof. Dr. Haya Schulmann
ATHENE Nationales Forschungszentrum für angewandte Cybersicherheit &
Institut für Informatik, Goethe-Universität Frankfurt am Main

1. November 2024

Vorbemerkung

Im Folgenden beziehen wir uns auf den "Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung", Bundestagsdrucksache 20/13184 vom 02.10.2024, kurz: NIS-2-Umsetzungsgesetz. Verweise auf bestimmte Paragraphen beziehen sich jeweils auf Artikel 1 des NIS2-Umsetzungsgesetzes, also die Neufassung des BSI-Gesetzes.

Die Digitalisierung von Staat, Wirtschaft und Gesellschaft schreitet rasant voran, in Deutschland und weltweit. Im internationalen Vergleich belegt Deutschland in der Digitalisierung allerdings nur mittlere Plätze, und das gilt gleichermaßen für Wirtschaft und Verwaltung.[1] Gleichzeitig herrscht Einigkeit, dass eine beschleunigte und bessere Digitalisierung eine Voraussetzung für die Wahrung unseres Wohlstands und die Ankurbelung des Wachstums in Deutschland und Europa insgesamt ist.

Digitalisierung, Cybersicherheit und der Schutz der Privatsphäre sind eng miteinander verwoben. Digitalisierung ohne ausreichenden Schutz vor Cyberangriffen und Datenschutzverletzungen ist offensichtlich unverantwortlich. Umgekehrt profitieren Cybersicherheit und Privatsphärenschutz von einer umfassenden Digitalisierung, da hierdurch manuelle Eingriffe und Medienbrüche, also typische Angriffspunkte vermieden werden.

Statistiken wie die im Gesetzesentwurf zitierte BITKOM-Umfrage zu den jährlichen Schäden für die deutsche Wirtschaft durch Cyber-Ereignisse belegen eindrücklich die Größe des Cyber-Sicherheitsproblems. Die BITKOM-Umfrage vom August 2024 ergab einen geschätzten Schaden von ca. 266 Mrd. Euro – das entspräche als Summe fast 60% des Bundeshaushalts für 2024. Nicht enthalten in dieser Statistik sind die Schäden für

[1] Digitalisierung der Wirtschaft in Deutschland – Digitalisierungsindex 2023; BMWK, Berlin 2024
https://www.de.digital/DIGITAL/Redaktion/DE/Digitalisierungsindex/Publikationen/publikation-digitalisierungsindex-2023-kurzfassung.pdf?__blob=publicationFile&v=3

Staat und Verwaltungen, Hochschulen und Forschungseinrichtungen, Vereine und Stiftungen, politische Parteien und direkt für Bürgerinnen und Bürger. Auch unsere eigenen Studien in ATHENE zur Verwundbarkeit der IT-Infrastrukturen einzelner Organisationen und Sektoren (z.B. politische Parteien, Landesverwaltungen, Forschungseinrichtungen und Universitäten, Großunternehme, Medien) bestätigen die insgesamt sehr hohe Verwundbarkeit und damit den dringenden Handlungsbedarf.

Die Zunahme der Risiken im Cyberraum ist eine unvermeidliche Begleiterscheinung der Erfolge in der Digitalisierung und des Fortschritts in der IT, insbesondere in der künstlichen Intelligenz. Zusätzlich wirken sich die zunehmenden geopolitischen Spannungen auch auf den Cyberraum aus, insbesondere die Spannungen mit Russland, China, Iran und den jeweiligen Verbündeten. Alle drei sind sehr aktiv im Bereich von Cyberangriffen, Desinformation und kognitiver Kriegführung und tragen wesentlich zur angespannten Cybersicherheitslage in Deutschland bei.[2]

Es ist deshalb sehr zu begrüßen, dass sich die EU zunehmend im Bereich der Cybersicherheit engagiert und eine Anhebung des Cyber-Sicherheitsniveaus in Europa und eine Harmonisierung und Vereinheitlichung in den Mitgliedsstaaten anstrebt. Die NIS2-Richtlinie der EU (2022/2555) und das deutsche NIS2-Umsetzungsgesetz gehen zweifellos in die richtige Richtung. Im Detail sehen wir allerdings in einigen Bereichen einen Verbesserungs- oder Ergänzungsbedarf, den wir in den folgenden sechs Empfehlungen zusammenfassen.

Empfehlung 1:
Einheitlichkeit über Sektoren und Ebenen hinweg herstellen

Die NIS2-Richtlinie strebt völlig zurecht eine weitgehende Vereinheitlichung der Cybersicherheit über die Verwaltung und die anderen wichtigen Sektoren an. Es soll übergreifend ein Mindestsicherheitsniveau erreicht werden. Die Zusammenarbeit und der Informationsaustausch zwischen Organisationen soll verbessert werden, wodurch Kosten reduziert und Synergieeffekte genutzt werden können. Ein organisationsübergreifendes Vorgehen verbessert die Angriffserkennung und Lagebilderstellung und sie vereinfacht und beschleunigt die Abwehr.

Werden einzelne wichtige Einrichtungen oder ganze Sektoren herausgenommen oder die Anwendung für optional erklärt, verzichtet man umgekehrt auf ein einheitliches Mindestniveau, vergibt Synergieeffekte und akzeptiert eine Verschlechterung der Erkennung und Abwehr für alle.

---

[2] Haya Schulmann, Michael Waidner: Von Desinformation zur kognitiven Kriegsführung; FAZ 13.11.2023
https://www.faz.net/aktuell/wirtschaft/cybersicherheit-von-deep-fakes-zur-kognitiven-kriegsfuehrung-19310389.html

Leider enthält der vorliegende Gesetzesentwurf bereits auf der Bundesebene, die eigentlich komplett durch das Gesetz abgedeckt werden sollte, durch § 29 eine Vielzahl solcher Ausnahmen. Einrichtungen werden teilweise ganz ausgenommen (z.B. das Auswärtige Amt), teilweise wird die Anwendung für optional erklärt. Diese Ausnahmen sollten vermieden und auf das Notwendigste reduziert werden. Ausnahmen sollten zudem inhaltlich nachvollziehbar begründet sein.

Eine weitere, unserer Meinung nach ungerechtfertigte und kontraproduktive Ausnahme betrifft die Forschung. Forschungseinrichtungen gehören laut Anlage 1 des BSIG zu den "wichtigen Einrichtungen". Die Liste der Cyberangriffe auf Forschungseinrichtungen steigt stetig an. Unsere eigenen Studien in ATHENE zur Sicherheit der Universitäten und außeruniversitären Forschung belegen die sehr hohe Verwundbarkeit gerade dieses Sektors.[3] §2(12) stellt allerdings klar, dass mit "Forschungseinrichtungen" im NIS2-Umsetzungsgesetz nur solche gemeint sind, die primär, also zu mehr als 50%, angewandte Forschung und experimentelle Entwicklung im Hinblick auf kommerzielle Zwecke durchführen. Damit verschärft das NIS2-Umsetzungsgesetz die Sprechweise der NIS2-Richtlinie. Alle Universitäten sind damit ausgeklammert, ebenso wie die außeruniversitären Forschungsgesellschaften mit Ausnahme der Fraunhofer-Gesellschaft. Angesichts der Bedeutung der Forschung insgesamt, der vielen Cyberangriffe und der unzureichenden Cybersicherheit in diesem Sektor sollte diese Ausnahme gestrichen werden. Forschungseinrichtungen sollten generell als wichtige Einrichtungen im Sinne des NIS2-Umsetzungsgesetzes gelten. Ausnahmen sollten sich auch hier an Größe und Risiko orientieren.

Das NIS2-Umsetzungsgesetz betrifft unmittelbar nur die Verwaltungen auf Bundesebene, die Verantwortung für die Umsetzung auf Landesebene liegt bei den Ländern. Durch die Länder wiederum wurden die kommunalen Verwaltungen und die Hochschulen aus der NIS2-Umsetzung ausgenommen. Damit ist eine uneinheitliche Vorgehensweise zwischen den Ländern vorprogrammiert, und es werden zwei besonders wichtige, aber auch besonders angreifbare Sektoren komplett herausgenommen.

Aufgrund der bestehenden Verantwortungsverteilung zwischen Bund und Ländern kann das NIS2-Umsetzungsgesetz an diesem Umstand zwar nichts ändern. Dennoch stellt diese Aufteilung ein erhebliches Cyber-Sicherheitsrisiko für Deutschland dar und sollte deshalb dringend durch die Gesetzgeber in Bund und Land überdacht und geändert werden.

In den Ländern haben sich unterschiedliche IT-Architekturen entwickelt, die sich auf die Implementierungsdetails der Cybersicherheit auswirken können. Insgesamt haben aber alle Verwaltungen, Bund und Länder, mehr oder weniger dieselben

[3] Haya Schulmann, Michael Waidner: Kein Fortschritt an Hochschulen; Behörden Spiegel, November 2024, Seite 30

Cyber-Sicherheitsprobleme. Damit haben alle Verwaltungen, Bund und Land, nahezu identische Bedarfe an Wissen und Schulungen, Scans und Analysen, Mindestanforderungen, Hilfestellungen. Hinzu kommt, dass verwundbare Verwaltungen – egal auf welcher Ebene – für Cyberangreifer ein besonders attraktives Sprungbrett zum Angriff auf weitere Organisationen darstellen. Solche Sprungbretter dienen z.B. zum sehr überzeugenden Phising, zur Verteilung von Schadsoftware, zur Verbreitung und Kontrolle eines Botnetzes. Je höhe die Reputation eines solchen Sprungbretts, desto attraktiver ist es für Cyberangreifer.

Es wäre deshalb wünschenswert, wenn sich Bund, Länder und Kommunen auf ein gemeinsames Vorgehen einigen würden. Der unten vorgeschlagene Expertenrat könnte die dafür notwendigen Analysen und Empfehlungen entwickeln.

Empfehlung 2:
Nationale Cyber-Sicherheitsorganisation stärken

Deutschland verfügt auf Bundesebene mit dem BSI über eine etablierte und gut funktionierende zentrale Cyber-Sicherheitsbehörde und damit im Kern über eine gute nationale Cyber-Sicherheitsarchitektur.

Mit §48 wird die Position eines Koordinators für Informationssicherheit auf Bundesebene eingeführt, also ein “CISO Bund”, allerdings ohne diese Position inhaltlich oder strukturell näher zu beschreiben. In der Fachwelt herrscht weitgehend Einigkeit, was die Rechte und Pflichten eines CISO bzw. einer CISO-Organisation sind. Besonders wichtig sind eine hohe persönliche Fachkompetenz, die strategische und operative Verantwortung für die Cybersicherheit der Organisation, die Möglichkeit der direkten Berichterstattung an die obersten Entscheidungsträgern und ein qualifiziertes Vetorecht gegenüber allen Maßnahmen innerhalb der Organisation (also hier des Bundes), die sich negativ auf die Cybersicherheit auswirken könnten. Ein CISO ist stets Teil der Organisation, für deren Cybersicherheit er verantwortlich ist, benötigt aber ein hohes Maß an Autonomie hinsichtlich Kommunikation in und außerhalb der Organisation und hinsichtlich der Ausübung seines Vetorechts.

Die Funktion des CISO Bund sollte in §48 entsprechend konkretisiert werden. Die meisten der üblichen CISO-Funktionen liegen heute und auch nach dem NIS2-Umsetzungsgesetz beim BSI. Die CISO-Funktion sollte daher dem BSI zugeordnet werden. Andernfalls besteht die Gefahr kontraproduktiver Doppelstrukturen und einer Gefährdung der Autorität und Autonomie des BSI.

Es ist zu begrüßen, dass das NIS2-Umsetzungsgesetz die Rolle und Stellung des BSI als Bundesoberbehörde im Geschäftsbereich des BMI grundsätzlich unverändert lässt. Ein

CISO sollte generell unabhängig vom CIO sein, und entsprechend sollte die Autonomie des BSI gegenüber dem BMI gestärkt werden, etwa indem die Fachaufsicht durch das BMI auf das Notwendigste beschränkt wird und das BSI volle Autonomie hinsichtlich der Kommunikation mit anderen Behörden und nach außen erhält. Eine vollständige Unabhängigkeit ist für die meisten Aufgaben des BSI aber weder notwendig noch hilfreich.

Wie oben erläutert, ist es für die Cybersicherheit in Deutschland wichtig, die derzeitige föderale Cyber-Sicherheitsarchitektur zu einer einheitlichen, nationalen Cyber-Sicherheitsarchitektur umzubauen und das BSI zu einer Zentralstelle für Cybersicherheit auch für die Länder und Kommunen zu entwickeln. Das NIS2-Umsetzungsgesetz kann aufgrund der derzeitigen Kompetenzverteilungen zwischen Bund und Ländern eine so weitreichende Änderung zwar nicht leisten, aber ich halte dies für eine der wichtigsten strategischen Empfehlungen für Bundestag und die Landesparlamente zur Verbesserung der Cybersicherheit in Deutschland.

Die wissenschaftlich-technische Fachwelt steht nahezu einhellig hinter dieser Empfehlung, dennoch scheitert bislang die politische Umsetzung. Um in Zukunft solche und ähnlich wichtige und grundsätzliche Entscheidungen fachlich und unabhängig von anderen politischen Erwägungen vorbereiten zu können, empfehlen wir die Einrichtung eines unabhängigen Expertenrates für Cybersicherheit der Bundesregierung. Dieser Rat sollte aus unabhängigen Sachverständigen aus Forschung, Gesellschaft, Wirtschaft und Verwaltung mit großer, ausgewiesener persönlicher Fachexpertise bestehen. Die Berufung von Funktionsträgern ohne ausgewiesene persönliche Expertise in der Cybersicherheit muss vermieden werden. Der Rat sollte regelmäßig die Cybersicherheitslage in Deutschland begutachten und auch quantitativ anhand von beauftragten und eigenen Studien bewerten. Er sollte eine inhaltlich treibende Rolle bei der Weiterentwicklung und Umsetzung der Cybersicherheitsstrategie Deutschlands übernehmen und hierzu mit hoher Kompetenz entsprechende Empfehlungen aussprechen können.

Empfehlung 3:
Erweiterte Lagebilderstellung

Für die Cybersicherheit einer Organisation, eines Sektors, eines Landes ist es entscheidend, jederzeit über ein möglichst aktuelles, umfassendes und qualitativ hochwertiges Bild der eigenen IT und ihrer Verwundbarkeiten, der Anzeichen für laufende oder frühere erfolgreiche Angriffe (z.B. im Darknet), derzeit eingesetzte Angriffstechniken und aktive Angreifer, und weiterer Risikofaktoren zu haben. Solche Lagebilder unterstützen die Abwehr aktueller Angriffe, die Priorisierung von Maßnahmen und die Bewertung der Entwicklung von Risiken und der Cybersicherheit

insgesamt über die Zeit. Die Erstellung von Lagebildern ist technisch anspruchsvoll; die Fortentwicklung ist eines der zentralen Themen der angewandten Forschung und Entwicklung in ATHENE. Vollständigkeit, Qualität und Aufwand der Lagebilderstellung profitieren sehr deutlich davon, Lagebilder über größere, zusammenhängende Einheiten hinweg zu erstellen.

Es ist zu begrüßen, dass das NIS2-Umsetzungsgesetzes insbesondere in § 15 dem BSI eine zentrale Rolle in der Lagebilderstellung gibt. Wie schon an anderer Stelle erwähnt, wäre es vorteilhaft, diese Lagebilderstellung nicht nur auf die Bundesverwaltung und (besonders) wichtige Einrichtungen zu beschränken, sondern zumindest auch die Länder und als Angebot weitere Einheiten von Wirtschaft und Gesellschaft einzubeziehen. Je umfassender das Lagebild ist, desto wertvoller ist es für die Verbesserung der nationalen Cybersicherheit.

Entscheidend ist, in die Lagebilderstellung nicht nur die IT der Einrichtungen selbst einzubeziehen, sondern auch die IT der jeweiligen Lieferketten, also z.B. externe Dienstleister, Cloud-Computing-Dienstleister. Nur so kann ein Gesamtbild entstehen. Dies bedeutet, dass das BSI beispielsweise auch die IT-Infrastrukturen (Netzes, Server) von Cloud-Computing-Diensten und anderer externer Dienstleister scannen muss, auch wenn diese sich im Ausland und außerhalb der Aufsichtspflicht des BSI befinden.

Darüber hinaus sollte ergänzt werden, dass die Formulierung in §15(1) nicht bedeutet, dass das BSI nur bekannte Schwachstellen identifizieren darf. Die Erläuterung zum Gesetzesentwurf, “§ 15 ermächtigt indes nicht zur Entdeckung von besonders sensiblen, unbekannten Schwachstellen (auch: Zero-Day-Schwachstellen).” legt allerdings nahe, dass genau dies gemeint ist. Tatsächlich sollte das BSI ausdrücklich auch Zero-Day-Schwachstellen aufdecken dürfen, da diese eine besonders große Gefahr darstellen. Bedenken, dass Zero-Day-Schwachstellen vom BSI zurückgehalten und an andere Behörden weitergegeben werden könnten, könnten leicht durch eine entsprechend konkretisierte Verpflichtung zur zeitnahen Information an die Hersteller ausgeräumt werden.

In § 59 wird das BSI als zuständige Aufsichtsbehörde für alle (besonders) wichtigen Einrichtungen, kritischen Anlagen und Einrichtungen der Bundesverwaltung benannt. In § 60 wird dies für internationale Einrichtungen auf diejenigen eingeschränkt, die ihren Hauptsitz in Deutschland haben. Dies ist sinnvoll, um Doppelungen in den Zuständigkeiten zu vermeiden, bedeutet aber, dass ein Großteil der Lieferketten nicht der Aufsicht des BSI unterstellt ist. Es muss sichergestellt sein, dass in der praktischen Umsetzung das BSI auch diese Teile der Lieferketten vollumfänglich in die eigene Lagebilderstellung einbeziehen und z.B. scannen und analysieren kann, und dies auch tatsächlich tut.

Empfehlung 4:
Konkrete Verpflichtungen jenseits IT-Grundschutz

In § 4(2) wird für das Bundeskanzleramt und die Bundesministerien die Umsetzung des IT-Grundschutzes verbindlich vorgeschrieben. Dies ist sehr zu begrüßen und sollte auf alle betrachteten Einrichtungen ausgeweitet werden.

Generell sind konkrete Vorgaben sehr zu begrüßen. Der IT-Grundschutz deckt allerdings nicht alle notwendigen Bereiche der Cybersicherheit ab. Sinnvoll wäre beispielsweise ebenso die verbindliche Umsetzung von Zero-Trust-Prinzipien, ähnlich wie dies im Mai 2021 durch die Bundesregierung der USA per Executive Order für die US-Bundesverwaltung gemacht wurde.[4]

Völlig zurecht spielt in der NIS2-Richtlinie die Sicherheit des Internets eine herausragende Rolle. Das Internet ist die mit Abstand größte und wichtigste und damit auch kritischste Kommunikationsinfrastruktur unserer Zeit. In § 28 (2) werden als besonders wichtige Einrichtungen unter anderen Top Level Domain Name Registries und DNS-Diensteanbieter genannt. Dies ist zu begrüßen, blendet aber aus, dass es neben DNS weitere, für die Internetsicherheit genauso wichtige Systeme gibt. Zu nennen ist hier insbesondere die Routing-Sicherheit, für die RPKI das zentrale System ist. Auch hier hat die US-Bundesregierung ein gutes Beispiel gegeben mit der im September 2024 vom White House veröffentlichten "Roadmap to enhancing Internet Routing Security", die verbindliche Vorgaben für die Netzbetreiber der USA macht.[5] Diese Roadmap bezieht sich ausführlich auf unsere Forschung und die Empfehlungen, die wir in ATHENE gemacht haben.

Empfehlung 5:
Aktive Maßnahmen zur Cyberabwehr

Das NIS2-Umsetzungsgesetz bewahrt die bestehenden, sehr begrenzten Möglichkeiten des BSI, aktiv gegen laufende und absehbare Cyberangriffe vorzugehen, erweitert aber in keiner Weise die Möglichkeiten des BSI oder anderer Behörden für weitere aktive Maßnahmen zur Cyberabwehr wie z.B. in unserem Artikel in der FAZ vom 25. April 2022 beschrieben.[6] Es wäre wünschenswert, als Teil der nationalen

---

[4] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[5] Report by the White House Office of the National Cyber Director: Roadmap to Enhancing Internet Routing Security; Washington DC, September 2024
https://www.whitehouse.gov/wp-content/uploads/2024/09/Roadmap-to-Enhancing-Internet-Routing-Security.pdf

[6] Haya Schulmann, Michael Waidner: Der Weg zur aktiven Cyberabwehr, FAZ 25.04.2022
https://www.faz.net/pro/digitalwirtschaft/cybersicherheit-der-weg-zur-aktiven-cyberabwehr-17980091.html; leicht überarbeitet
https://www.forschung-it-sicherheit-kommunikationssysteme.de/dateien/forschung/2023-03-impulspapier-aktive-cyberabwehr.pdf

Cyber-Sicherheitsarchitektur einen vollständigen Rechtsrahmen auch für diese Maßnahmen zu schaffen.

Empfehlung 6:
Vertrauenswürdige IT

Eine der zentralen und bislang nicht zufriedenstellend gelösten Herausforderungen für die Cybersicherheit ist die Sicherstellung eines ausreichenden Angebots an geeigneten und vertrauenswürdigen IT-Lösungen, insbesondere im Bereich der Cybersicherheit. Die große und asymmetrische Abhängigkeit Deutschlands in der Digitalisierung, IT und IT-Sicherheit wie auch die Auswirkung auf unsere digitale Souveränität sind hinlänglich bekannt.[7]

Einerseits braucht es mehr und international erfolgreiche innovative Unternehmen in Deutschland und Europa, die aufgebaut und gefördert werden müssen, andererseits müssen wir Methoden entwickeln und anwenden, wie Angebote als nicht vertrauenswürdig erkannt und vom Markt teilweise oder ganz ausgeschlossen werden können.

Diese Aspekte werden im NIS2-Umsetzungsgesetz kaum bzw. nur indirekt behandelt. Es gibt einen großen Fokus auf Zertifizierungen. Diese funktionieren aber letztlich nur dann gut, wenn ein Produkt oder Dienst von einem a priori vertrauenswürdigen Hersteller oder Dienstleister kommt.

Die Möglichkeiten des BSI, Warnungen aufgrund erkannt mangelhafter Vertrauenswürdigkeit auszusprechen, werden durch das NIS2-Umsetzungsgesetz weder konkretisiert noch geändert. Wie problematisch dies ist, zeigte sich 2022 in der Diskussion um die Warnung des BSI vor der Antivirensoftware des russischen Herstellers Kaspersky.[8] Diese Warnung war unserer Meinung nach notwendig und berechtigt, ihre Rechtmäßigkeit wurde aber von vielen in Zweifel gezogen. Die Möglichkeiten, vor Produkten aber auch vor einzelnen Herstellern zu warnen, sollten deutlich konkretisiert und ausgeweitet werden.

---

[7] Haya Schulmann, Michael Waidner: Wieso Deutschland in digitaler Abhängigkeit verharrt, FAZ 27.06.2024
https://www.faz.net/aktuell/wirtschaft/unternehmen/digitale-souveraenitaet-warum-deutschland-in-abhaengigkeit-verharrt-19809000.html

[8] Haya Schulmann, Michael Waidner: Wie Deutschland mit nicht vertrauenswürdiger IT besser umgehen kann; FAZ 24.10.2022
https://www.faz.net/pro/digitalwirtschaft/kaspersky-virenschutz-wie-deutschland-it-systeme-besser-schuetzen-kann-18408167.html