Bundesministerium
des Innern
und für Heimat

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)210

Bundesministerium des Innern und für Heimat, 11014 Berlin

RD Michael Popp
Referatsleiter PK I 2

Alt-Moabit 140
10557 Berlin

Postanschrift
11014 Berlin

Tel +49 30 18 681-12594

Fax +49 30 18 681-512594

KabParl@bmi.bund.de
www.bmi.bund.de

-per elektronischer Post-

Stellvertretender Vorsitzender des
Ausschusses für Inneres und Heimat
Herrn Prof. Dr. Lars Castellucci, MdB

Vorsitzende des
Ausschusses für Digitales
Frau Tabea Rößner, MdB

Bericht zur Evaluierung des IT-Sicherheitsgesetzes 2.0

Az: KabParl-12003/1#1
Berlin, 3. Mai 2023
Seite 1 von 1

Sehr geehrte Frau Vorsitzende, sehr geehrter Herr stellvertretender Vorsitzender,

anliegend übersende ich Ihnen den oben erwähnten Bericht und bitte, diesen an die Mitglieder Ihres Ausschusses weiterzuleiten.

Mit freundlichen Grüßen
im Auftrag

Michael Popp

Anlage
-1- Bericht

Bundesministerium
des Innern
und für Heimat

Evaluierung des IT-Sicherheitsgesetzes 2.0

Evaluierung nach Artikel 6 Absatz 1 Nummer 1 des zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18. Mai 2021

02.05.2023

Inhaltsverzeichnis

Einleitung

Der vorliegende Bericht dient der Erfüllung der Berichtspflicht gemäß Artikel 6 Absatz 1 Nummer 1 des zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) vom 18. Mai 2021. Gemäß der vorgenannten Vorschrift berichtet das Bundesministerium des Innern und für Heimat (BMI) dem Deutschen Bundestag unter Einbeziehung von wissenschaftlichem Sachverstand über die Wirksamkeit der in diesem Gesetz enthaltenen Maßnahmen für die Erreichung der mit diesem Gesetz verfolgten Ziele hinsichtlich des § 2 Absatz 10, der §§ 8a, 8b, 8d und 8e sowie § 10 Absatz 1 des BSI-Gesetzes.

1. Sicherheitspolitische Standortbestimmung und europarechtliche Rahmenbedingungen

Der Rechtsrahmen für die Cybersicherheit Kritischer Infrastrukturen hat sich in den vergangenen Jahren sowohl national als auch auf europäischer Ebene dynamisch entwickelt. Im Jahr 2007 wurde aufbauend auf dem „Nationalen Plan zum Schutz der Informationsinfrastrukturen“ (NPSI)[1] der Bundesregierung sowie der „Nationalen Strategie zum Schutz Kritischer Infrastrukturen“ (KRITIS-Strategie)[2] der Bundesregierung gemeinsam von Wirtschaft und Staat die Kooperation UP-KRITIS[3] ins Leben gerufen. Der UP KRITIS ist eine öffentlich-private Zusammenarbeit zwischen Betreibern Kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen. Der UP KRITIS hat sich seitdem als effektive Plattform zur Kommunikation und Zusammenarbeit beim Schutz Kritischer Infrastrukturen in Deutschland etabliert. Ihm gehören zwischenzeitlich ca. 900 Betreiber Kritischer Infrastrukturen, Unternehmen, sowie Behörden und Verbände an. Der UP KRITIS spielt mit seinen Gremien eine maßgebliche Rolle bei der Weiterentwicklung des in Deutschland gewählten kooperativen Ansatzes von Wirtschaft und Staat zum Schutz Kritischer Infrastrukturen.

---

[1] https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/05-12-09/05-12-09-anlage-nr-16.pdf

[2] https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.pdf

[3] https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/UP-KRITIS/up-kritis_node.html

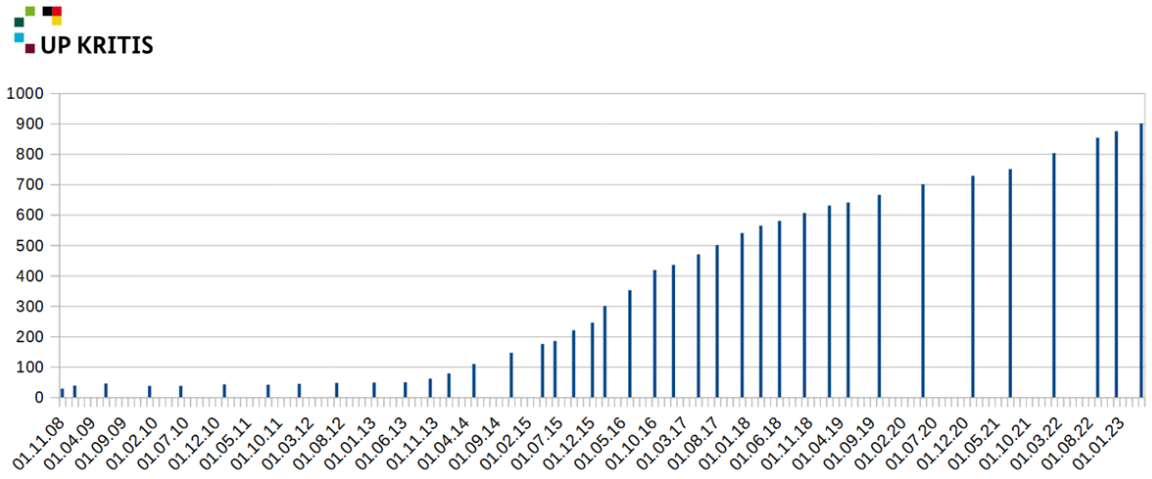


Abbildung 1: Entwicklung der Teilnehmerzahl im UP KRITIS, Quelle: eigene Darstellung

Mit dem ersten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) aus dem Jahr 2015 sowie dem IT-Sicherheitsgesetz 2.0 aus dem Jahr 2021 wurden schließlich die zentralen gesetzlichen Regelungen auf Bundesebene für die Cybersicherheit Kritischer Infrastrukturen (KRITIS) geschaffen. Diese fanden umfassend Eingang in das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) sowie weiteren sektorspezifischen Gesetzen[4], wie beispielsweise dem Telekommunikationsgesetz (TKG), dem Energiewirtschaftsgesetz (EnWG) oder dem Atomgesetz (AtG).

KRITIS-Betreiber wurden durch diese neuen Vorschriften verpflichtet, umfangreiche präventive Cybersicherheitsmaßnahmen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer für die Funktionsfähigkeit der Kritischen Infrastruktur maßgeblichen informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, hierüber regelmäßige Nachweise beim Bundesamt für Sicherheit in der Informationstechnik (BSI) zu erbringen, und Cybersicherheitsvorfälle an das BSI zu melden. Mit der Ermächtigung im BSIG für die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) wurde vorgesehen, dass das BMI als Verordnungsgeber erstmals verbindliche Festlegungen zur Identifikation von Kritischen Infrastrukturen treffen kann und somit den Anwendungsbereich der neu geschaffenen gesetzlichen Vorschriften zur Cybersicherheit Kritischer Infrastrukturen näher bestimmt. Der Ansatz der BSI-KritisV basiert dabei auf einer infrastrukturbezogenen Perspektive. Die Festlegungen (Sektoren, Bereiche, Anlagekategorien, Bemessungskriterien, Schwellenwerte) der BSI-KritisV geben Kriterien vor, anhand derer festgelegt wird, ob eine Anlage eine Kritische Infrastruktur ist. Die Betreiber prüfen dabei selbst die Kritikalität ihrer Anlage anhand dieser Kriterien und registrieren sich in diesem Fall beim BSI. Sollten notwendige Registrierungen seitens der Betreiber nicht erfolgen, kann das BSI diese auch selbst vornehmen. Mit der BSI-KritisV aus dem Jahr 2016 (Korb 1, Inkrafttreten: 30.05.2016) und aus dem Jahr 2017 (Korb 2, Inkrafttreten: 30.06.2017) sowie den Änderungsverordnungen aus den Jahren 2020 (Inkrafttreten: 01.01.2021) und 2023 (Inkrafttreten: 23.02.2023) wurden KRITIS-Betreiber in sieben Sektoren der Wirtschaft bestimmt; die dazugehörigen Bestimmungen für den mit dem IT-

[4] Vgl. auch Bitkom (2022): Regulierungsmapping IT-Sicherheit, abrufbar unter https://www.bitkom.org/Bitkom/Publikationen/Regulierungsmapping-IT-Sicherheit

Sicherheitsgesetz 2.0 eingeführten neuen Sektor Siedlungsabfallentsorgung sind derzeit in Vorbereitung.

Das erste IT-Sicherheitsgesetz stellt hierbei gemeinsam mit dem Gesetz zur Umsetzung der NIS-Richtlinie (NIS-Richtlinien-Umsetzungsgesetz) aus dem Jahr 2017 die deutsche Umsetzung der Richtlinie (EU) 2016/1148 vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie) dar. Mit der NIS-Richtlinie wurde erstmals ein unionsweiter Rechtsrahmen für die Bestimmung von Betreibern wesentlicher Dienste bzw. Kritischer Infrastrukturen eingeführt, der die Einführung von Mindestanforderungen an diese Unternehmen im Bereich der Cybersicherheit, Meldepflichten sowie den Aufbau nationaler Kapazitäten für Cyber-Sicherheit und eine stärkere Zusammenarbeit der Mitgliedstaaten untereinander sowie mit Institutionen der Europäischen Union einführte.

Am 16. Januar 2023 sind mit der Richtlinie (EU) 2022/2555 für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) sowie der Richtlinie (EU) 2022/2557 über die Resilienz kritischer Einrichtungen (CER-Richtlinie) umfangreiche Neuerungen für einen weiter verbesserten Schutz Kritischer Infrastrukturen in Kraft getreten. Mit den Richtlinien wird ein unionsweit einheitlicher Schutz vor physischen Störungen und Cyberangriffen bei Kritischen Infrastrukturen aufgebaut. Beide Richtlinien sind jeweils bis zum 17. Oktober 2024 in nationales Recht umzusetzen. Entsprechende Gesetzentwürfe zur Umsetzung werden aktuell im BMI erarbeitet. In dieser Evaluierung identifizierte Handlungsbedarfe können daher dort einfließen, sofern sie mit den vorgenannten europarechtlichen Vorgaben im Einklang stehen.

2. Methodik der Evaluierung

Für die vorliegende Evaluierung wurde in einem mehrstufigen Verfahren ein möglichst breites Stimmungsbild der betroffenen Stakeholder eingeholt, um im Ergebnis aussagekräftige und zutreffende Evaluierungsergebnisse ermitteln zu können.

Durch das BSI wurde im Zeitraum vom 21. Februar bis 12. März 2023 im Auftrag des BMI eine quantitative und qualitative Erhebung in Form eines Online-Interviews (Computer Assisted Web Interviewing - CAWI) unter allen beim BSI gemäß § 8b Absatz 2 BSIG oder nach § 11 Absatz 1d EnWG als Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber) registrierten Unternehmen durchgeführt. Die Einladung zur Teilnahme erfolgte durch das BSI mit einem individualisierten Link. An der Erhebung haben insgesamt 379 von insgesamt ca. 1.800 registrierten Betreibern teilgenommen. Um repräsentative Gesamtergebnisse zu erzielen, wurde der vollständige Datensatz nach dem Merkmal Sektor (anhand der Verteilung der angeschriebenen Unternehmen) gewichtet.

Zusätzlich wurden durch BMI und BSI weitere Fachkreise mit der Bitte um Stellungnahme zur Wirksamkeit der in die Evaluierung einzubeziehenden Abschnitte des BSIG angeschrieben. Hierzu zählen der UP KRITIS und verschiedene Fachverbände Kritischer Infrastrukturen, einschlägige Universitäten und Forschungseinrichtungen im Bereich der IT-Sicherheit, das Institut der Wirtschaftsprüfer sowie Vertreter der Zivilgesellschaft, darunter die AG KRITIS und die Stiftung Neue Verantwortung[5]. Die nach § 10 Absatz 1 BSIG für die BSI-KritisV zu beteiligenden Bundesressorts

[5] Nicht alle von BMI und BSI angefragten Organisationen haben auch tatsächlich Stellungnahmen eingereicht.

wurden bei dieser Evaluierung einbezogen. Alle beim BMI und BSI eingegangenen Stellungnahmen sind in den vorliegenden Evaluierungsbericht eingeflossen.

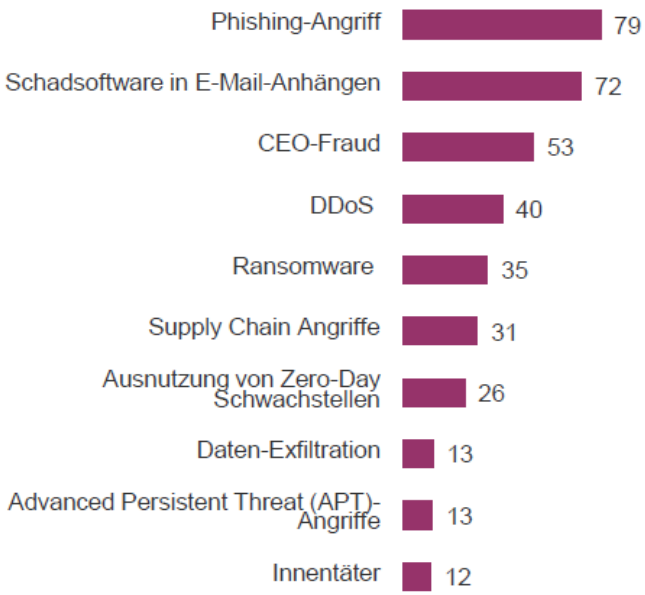
3. Evaluierungsergebnisse

Die in diesem Kapitel aufgeführten Evaluierungsberichte basieren auf der in Kapitel 2 genannten Umfrage unter KRITIS-Betreibern, den eingegangenen Stellungnahmen zur Evaluierung sowie den Erfahrungen von BMI und BSI in Bezug auf die Umsetzung des BSI-Gesetzes. Neben Aussagen zur Wirksamkeit der gesetzlichen Maßnahmen lassen die Umfrageergebnisse auch insbesondere Rückschlüsse auf die von den Betreibern wahrgenommene Bedrohungslage und die grundsätzliche Erforderlichkeit von gesetzlichen Maßnahmen zur Verbesserung der Cybersicherheit in Kritischen Infrastrukturen erkennen.

		Unternehmensgröße		Bekanntheit IT-Sicherheitsgesetz 2.0	
		KMU	Großunternehmen	geringe/mittlere Vertrautheit	hohe Vertrautheit
erhöhte IT-Bedrohungslage wahrgenommen	71	63	76	69	73
*darunter (Mehrfachnennungen)**					
Ukraine-Krieg, geopolitische Bedrohung, weltpolitische Lage	31	28	32	21	35
Zunehmende und gezielte Angriffe auf kritische Infrastruktur	26	31	24	22	24
Ransomware, Schadsoftware	20	18	22	21	23
Spam, Phishing-Mails	20	19	21	13	23
Sonstige Bedrohungen und Angriffe im IT- /Cyberbereich	12	8	13	11	14
Hacking, Softwareschwachstellen, Zero-Day-Exploits	10	13	9	5	14
Informationen über IT-Bedrohungen, BSI-Meldungen	10	11	10	15	9
Finanzielle Engpässe, fehlende Ressourcen, Fachkräftemangel	4	0	7	8	4
Allgemeine Verunsicherung, Bedrohungsgefühl	4	3	5	6	3
Sonstiges	6	4	6	9	4

Abbildung 2: Nehmen Sie gegenwärtig eine erhöhte IT-Bedrohungslage für Ihr Unternehmen war? Falls ja: Inwiefern? (n=269; Angaben in Prozent)

Nahezu drei Viertel (71 %) der befragten KRITIS-Betreiber, die an der Befragung teilgenommen haben, nehmen gegenwärtig eine erhöhte Cyber-Bedrohungslage wahr. Großunternehmen zeigten sich hier alarmierter (76 %) als kleine und mittlere Unternehmen (KMU) (63 %). Besonders besorgt äußern sich Unternehmen, die dem BSI-Gesetz einen stark positiven Einfluss zuschreiben (80 %). Zu den Ursachen für die gewachsene Cyber-Bedrohung gehört für rund ein Drittel der besorgten Betreiber (31 %) der russische Angriffskrieg auf die Ukraine bzw. die aktuell angespannte geopolitische/ weltpolitische Lage. Jeder vierte Betreiber (26 %) rechnet mit zunehmenden und gezielten Angriffen auf Kritische Infrastrukturen. Weitere konkrete Befürchtungen sind Ransomware/ Schadsoftware (20 %), Spam/ Phishing-Mails (20 %) und Hacking/ Softwareschwachstellen/ Zero-Day-Exploits (10 %). 10 Prozent der befragten Betreiber nennen Informationen über IT-Bedrohungen und BSI-Meldungen als Ursache für ihre gestiegene Sorge (Mehrfachnennungen waren möglich, vgl. Abbildung 2).



	Unternehmensgröße		Bekanntheit IT-Sicherheits-gesetz 2.0	
	KMU	Großunter-nehmen	geringe/mittlere Vertrautheit	hohe Vertrautheit
Phishing-Angriff	84	77	74	78
Schadsoftware in E-Mail-Anhängen	69	73	71	71
CEO-Fraud	53	53	51	51
DDoS	40	41	26	49
Ransomware	25	39	39	40
Supply Chain Angriffe	27	32	25	31
Ausnutzung von Zero-Day Schwachstellen	22	27	27	28
Daten-Exfiltration	5	17	11	15
Advanced Persistent Threat (APT)-Angriffe	12	14	8	17
Innentäter	11	13	10	14

Abbildung 3: Falls Ihr Unternehmen in den letzten 2 Jahren aktiv auf Cyber-Angriffe reagieren musste, um welche Art von Cyber-Angriff handelte es sich dabei? (n=153, Angaben in Prozent)

Eine erhöhte IT-Gefährdungslage durch häufigere Cyber-Angriffe auf das eigene Unternehmen stellten in den vergangenen zwei Jahren 45 Prozent der Befragten fest, Großunternehmen hierbei (52 %) deutlich häufiger als KMU (35 %). 40 Prozent der befragten Betreiber mussten in diesem Zeitraum aktiv auf Cyber-Attacken reagieren. Bei den erlebten Angriffen handelte es sich mit Abstand am häufigsten um Phishing (79 %) und Schadsoftware in E-Mail-Anhängen (72 %). Rund die Hälfte der Unternehmen hatte mit CEO-Fraud zu tun (53 %), 40 Prozent mit DDoS-Attacken, 35 Prozent mit Ransomware, 31 Prozent mit Supply-Chain-Angriffen und 26 Prozent mit dem Ausnutzen von Zero-Day-Schwachstellen. Seltenere Nennungen sind Daten-Exfiltration (13 %), APT-Angriffe (13 %) und Innentäter (12 %) (vgl. Abbildung 3).

Allgemein

In Folge des ersten IT-SiG und des IT-SiG 2.0 setzte die überwiegende Mehrheit der Betreiber neue Sicherheitsmaßnahmen um oder zog sie zeitlich vor: Nach der Einführung der IT-SiG 1.0 und 2.0 lässt sich unter den befragten Betreibern ein Schub bei der Umsetzung bzw. Planung von technischen und organisatorischen Sicherheitsmaßnahmen, Audits und Schulungen beobachten.

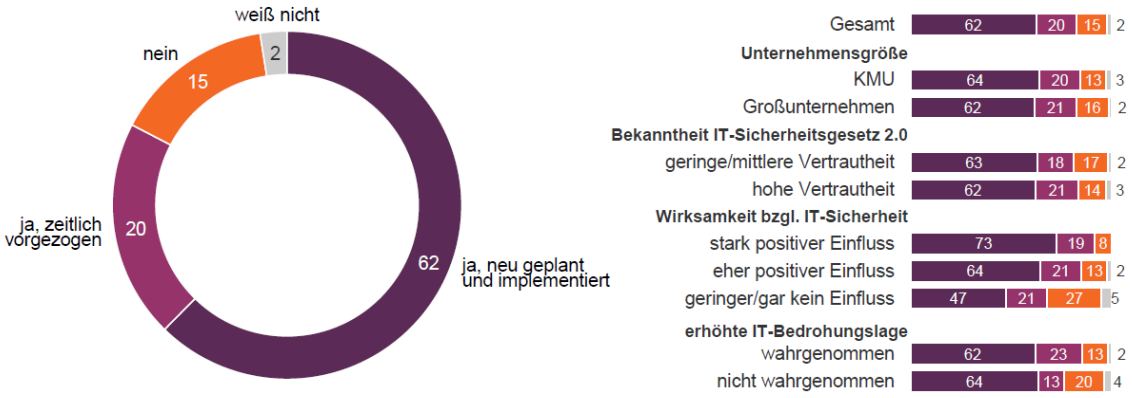


Abbildung 4: Wurden aufgrund der geänderten IT-Sicherheitsgesetzgebung in Ihrem Unternehmen neue Projekte zur Erhöhung der IT-Sicherheit umgesetzt? (n=308; Angaben in Prozent)

Anhand der Umfrageergebnisse lässt sich ein besonders hoher Einfluss der Änderungen durch das erste IT-SiG am BSI-Gesetz insbesondere auf die Umsetzung organisatorischer Sicherheitsmaßnahmen erkennen: Anders als technische Maßnahmen, die mancherorts schon vor dem ersten IT-SiG in Teilen umgesetzt waren, wurden insbesondere organisatorische Sicherheitsmaßnahmen mehrheitlich erst zwischen 2015 bis 2020 realisiert. Hierzu zählen in besonderem Maße die Maßnahmen zur Aufrechterhaltung eines stets aktuellen Informationsstands im Unternehmen (66 % in diesem Zeitraum) sowie die Einführung von Informationssicherheitsmanagementsystemen (ISMS) (60 %). Auch das IT-SiG 2.0 führte zu einer verstärkten Umsetzung von weiteren technischen und organisatorischen Sicherheitsmaßnahmen. Der Anteil der Betreiber, welche die Umsetzung zusätzlicher Maßnahmen in der Umfrage nannte, stieg bei nahezu allen abgefragten Maßnahmen um 13 bis 16 Prozent, die einzigen Ausnahmen waren das Assetmanagement (9 %) und die sichere Dokumentenerstellung (8 %). Die Mehrheit der befragten Unternehmen führte im Zusammenhang mit dem ersten IT-SiG und dem IT-SiG 2.0 Schulungen durch. Sechs von zehn Unternehmen (60 %) schulten ihre Mitarbeitenden firmenintern, rund ein Drittel (35 %) entschied sich für einen externen Anbieter (Mehrfachnennungen waren möglich). In 30 Prozent der Unternehmen fanden keine gesonderten Informationsveranstaltungen statt.

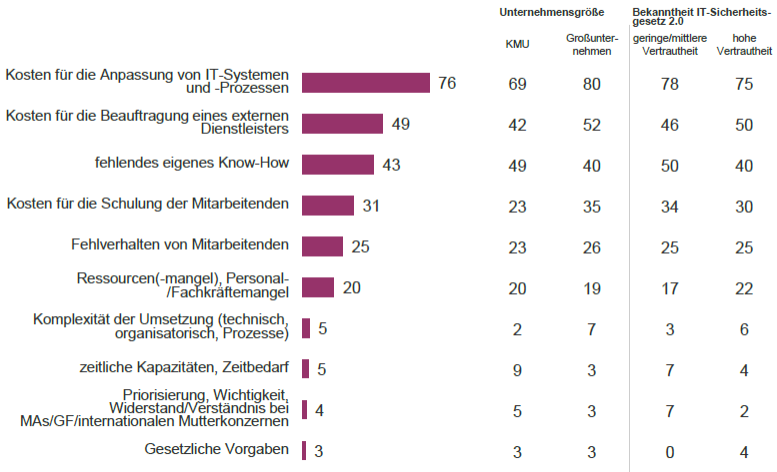


Abbildung 5: Welche Herausforderungen gab oder gibt es bei der Umsetzung der gesetzlichen Vorgaben zum Thema IT-Sicherheit konkret in Ihrem Unternehmen? (n = 308, Angaben in Prozent, Mehrfachnennung möglich)

Als mit Abstand größte Herausforderung für die Umsetzung der gesetzlichen Maßnahmen wurden durch die Betreiber die Kosten für die Anpassung von IT-Systemen/ -Prozessen genannt, gefolgt von Kosten für externe Dienstleister und fehlendem Knowhow. Weitere häufig genannte Hürden sind die Kosten für Schulungen (31 %), Fehlverhalten von Mitarbeitenden (25 %) und Ressourcen-/ Personal-/ Fachkräftemangel (20 %) (vgl. Abbildung 5). Im Durchschnitt liegt der prozentuale Anteil für Cyber-Sicherheit im IT-Budget bei 14 Prozent, bei KMU etwas höher (16 %) als bei Großunternehmen (12 %). Die Mehrheit der Betreiber (58 %) hat dafür nur einen Anteil von unter 10 Prozent eingestellt. Ein gutes Viertel (28 %) wendet 11 bis 20 Prozent des IT-Budgets für Sicherheitsmaßnahmen auf, nur bei 14 Prozent liegt der Anteil höher.

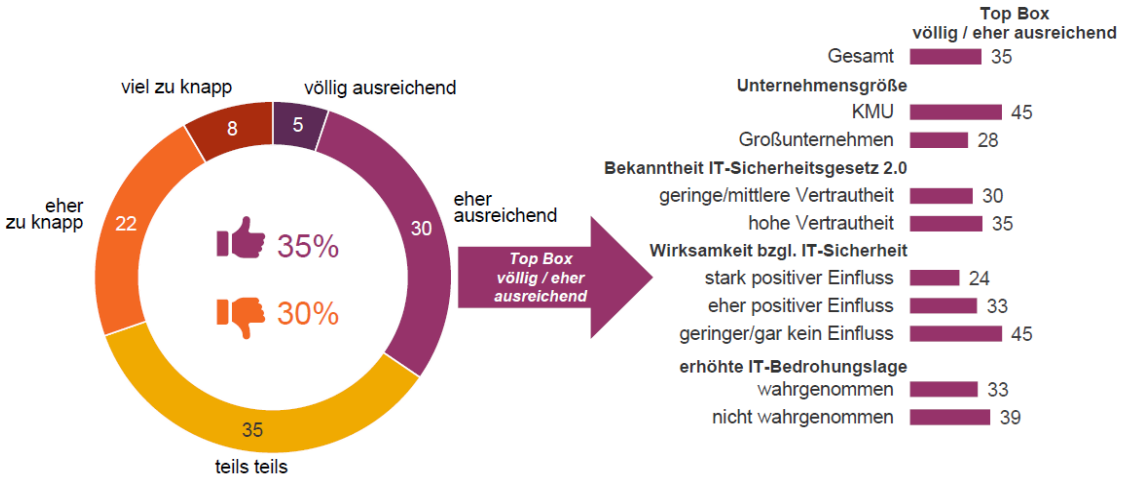


Abbildung 6: Ist Ihr IT-Sicherheitsbudget aus Ihrer Sicht ausreichend? (n=379)

Die meisten Unternehmen halten jedoch das ihnen zur Verfügung stehende IT-Sicherheitsbudget hierbei nicht für angemessen. Nur gut ein Drittel hält es für „eher“ (30 %) oder „völlig“ (5 %) ausreichend. Dem stehen 30 Prozent gegenüber, die ihr Budget als „eher“ (22 %) oder „viel“ zu knapp (8 %) einschätzen. 35 Prozent ordnen sich mit der Antwort „teils/ teils“ dazwischen ein. Vor allem bei Großunternehmen ist die Zufriedenheit gering: Nur 28 Prozent halten ihr Budget für „völlig/ eher“ ausreichend, bei KMU sind es 45 Prozent.

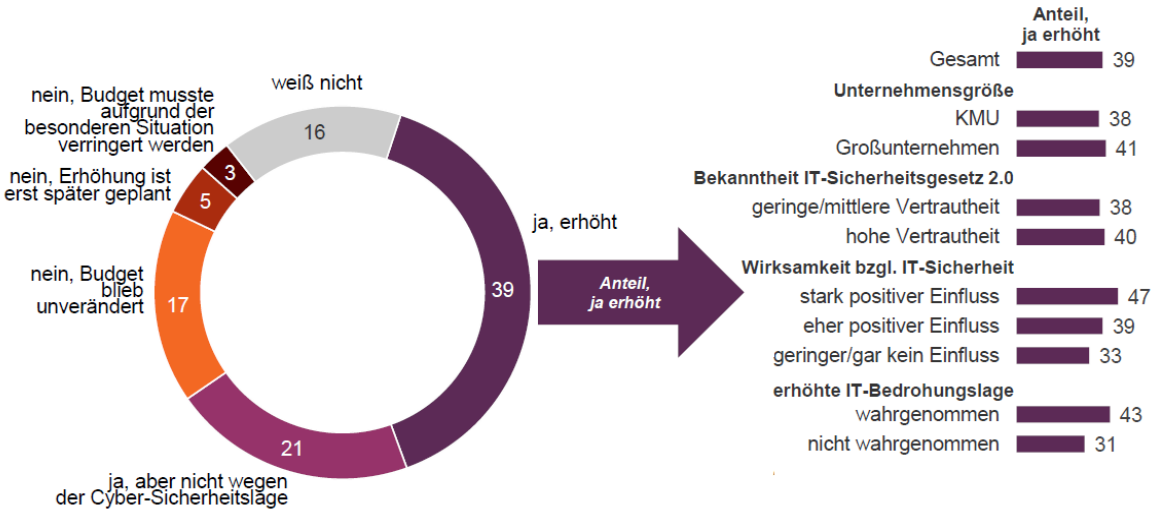


Abbildung 7: Haben Sie Ihr IT-Sicherheitsbudget aufgrund der Cyber-Sicherheitslage in den letzten 2 Jahren erhöht? (n=379)

Gleichzeitig haben vier von zehn Betreibern (39 %) ihr IT-Sicherheitsbudget in den letzten zwei Jahren wegen der Cyber-Sicherheitslage erhöht (Großunternehmen: 41 %, KMU: 38 %), weitere 21 Prozent stockten es aus anderen Gründen auf. Bei 17 Prozent blieb das Budget gleich, weitere 5 Prozent haben eine spätere Erhöhung eingeplant. 3 Prozent der Betreiber mussten ihr Budget in diesem Zeitraum kürzen.

Etwa jeder zehnte Betreiber erlebt die gesetzlichen Anforderungen als sehr hoch oder komplex (11 %) bzw. sich stetig verändernd (10 %). Gleichzeitig hält mit 83 Prozent Zustimmung die überwiegende Mehrheit der Betreiber die vollständige Umsetzung aller gesetzlichen Vorgaben zur IT-Sicherheit für „sehr wichtig“ (53 %) oder sogar „extrem wichtig“ (30 %). „Eher unwichtig“ ist sie nur für 2 Prozent der Befragten, völlig „unwichtig“ für niemanden.

Insofern beobachten nach Umsetzung der Maßnahmen auch über drei Viertel (78 %) der Betreiber - unabhängig von ihrer Größe - einen positiven Einfluss auf ihre IT-Sicherheit („eher“: 57 %; „stark“: 21 %). Nur 22 Prozent stellten einen „eher geringen“ (20 %) oder „gar keinen“ (2 %) Einfluss fest.

Auch die Sensibilisierung von Mitarbeitenden und Geschäftsführung wurden durch die Umsetzung der gesetzlichen Maßnahmen „eher“ (55 %) oder sogar „stark“ (17 %) positiv beeinflusst. Nur 24 Prozent schätzen den Einfluss als „eher gering“ ein, 4 Prozent sehen überhaupt keine Wirkung.

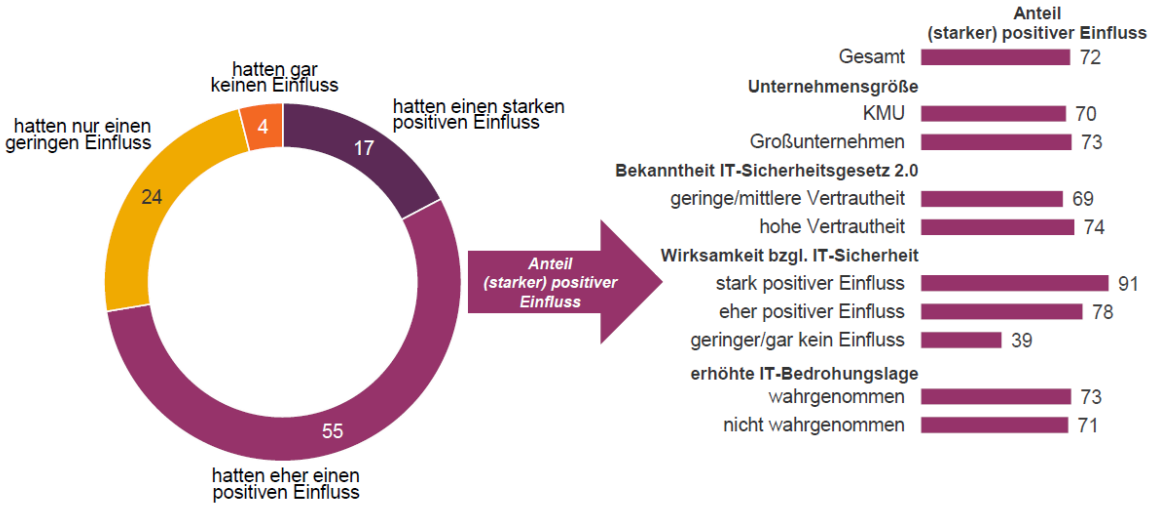


Abbildung 8: Wie wirksam waren die durch das erste IT-SiG und das IT-SiG 2.0 geforderten Maßnahmen im Hinblick auf die Sensibilisierung der Mitarbeitenden und der Geschäftsführung für das Thema IT-Sicherheit? (n=308, Angaben in Prozent)

Zwischen der Vertrautheit mit den IT-SiG und dem Umsetzungsstand der gesetzlichen Vorgaben lässt sich ein Zusammenhang beobachten: In Unternehmen, die die Gesetzgebung und die Anforderungen „Absicherungen nach dem Stand der Technik“ und zur Nachweispflicht nicht gut kennen, ist der Umsetzungsstand auch überdurchschnittlich häufig niedriger. Hier sollten Wege gefunden werden, diesen Betreibern durch konkrete Handlungsempfehlungen und Hilfestellungen die Gesetzesinhalte nahe zu bringen, und das nötige Sicherheitsbewusstsein und Hintergrundwissen zu stärken.

§ 2 Absatz 10 BSIG Begriffsbestimmungen

Die Begriffsbestimmung für Kritische Infrastrukturen im Sinne des BSI-Gesetzes hat sich aus Sicht des BMI grundsätzlich bewährt, konkrete Änderungsbedarfe aufgrund der Erfahrungen seit dem ersten IT-Sicherheitsgesetz wurden in der Evaluierung nicht festgestellt.

Jedoch wird im Zuge der Umsetzung der NIS-2-Richtlinie voraussichtlich eine grundsätzliche Neustrukturierung der Begrifflichkeiten erforderlich werden, da die NIS-2-Richtlinie den Anwendungsbereich der betroffenen Unternehmen mit den neuen Begriffskategorien „wichtige

Einrichtungen“ und „wesentliche Einrichtungen“ erheblich ausweitet. Anders als in der Vorgängerrichtlinie NIS-1 aus dem Jahr 2016 werden die von der Richtlinienumsetzung einzubeziehenden Unternehmen künftig nicht mehr anhand ihrer Versorgungskritikalität bestimmt, sondern unionsweit einheitlich nach ihrer Unternehmensgröße in Bezug auf die Mitarbeiterzahl und den Umsatz (sog. „Size-Cap“).

Gleichzeitig hat sich aus Sicht des BMI jedoch die derzeit im BSI-Gesetz angelegte Bestimmung Kritischer Infrastrukturen mit einem Fokus auf die tatsächlich für die Erbringung der Kritischen Dienstleistung erforderlichen Anlagen und einem durch sie erbrachten kritischen Versorgungsgrad als sinnvoll erwiesen, da hierdurch eine zielgenauere Adressierung Kritischer Infrastrukturen erfolgen kann als durch andere allgemeine Kriterien wie die Mitarbeiteranzahl oder den Umsatz. Eine Beibehaltung der Kategorie von Kritischen Infrastrukturen bzw. Kritischen Anlagen als höchste Kategorie mit besonders strengen gesetzlichen Mindestanforderungen neben den mit NIS-2 neu einzuführenden neuen Kategorien „wichtige Einrichtungen“ und „wesentliche Einrichtungen“ erscheint daher sinnvoll. Hierbei sollte sichergestellt werden, dass in der nationalen Umsetzung Begriffe verwendet werden, aus denen sich auch semantisch[6] die Abstufung der drei Begriffskategorien (Kritische Infrastrukturen, wesentliche Einrichtungen, wichtige Einrichtungen) unmittelbar ergibt. Ebenfalls sollte sichergestellt werden, dass für die Umsetzungen der CER-Richtlinie und der NIS-2-Richtlinie in Deutschland möglichst einheitliche Begrifflichkeiten und Definitionen verwendet werden. Beim BMI eingegangene Stellungnahmen aus der Wirtschaft unterstützen dieses Vorgehen ausdrücklich.

§ 8a BSIG Sicherheit in der Informationstechnik Kritischer Infrastrukturen

Die Umsetzung angemessener organisatorischer und technischer Maßnahmen durch die KRITIS-Betreiber ist alle zwei Jahre gegenüber dem BSI nachzuweisen. Diesbezüglich wurde seitens mancher Betreiber in der Evaluierung angeregt, für diejenigen Unternehmen, die einen Nachweis auf Grundlage internationaler Normen beispielsweise aus der ISO/IEC 27000 Reihe erbringen, entsprechend dem internationalen Prüfzyklus auch einen Nachweis alle drei Jahre zu ermöglichen. Eine Wahlmöglichkeit für die Unternehmen, ob der Nachweis in einem zwei- oder dreijährigen Rhythmus erfolgen soll, ist jedoch aufgrund der erforderlichen Gleichbehandlung der Unternehmen nicht möglich. Gegen eine grundsätzliche Umstellung des gesamten Nachweiszyklus auf einen dreijährigen Rhythmus spricht zudem, dass die KRITIS-Aufsicht hierdurch weniger engmaschig wäre und zwischen den Nachweiszyklen zu große Zeiträume lägen, die der Cyberbedrohungslage und den dynamischen technischen Weiterentwicklungen nicht gerecht würde. Um dennoch das grundsätzlich nachvollziehbare Anliegen der Betreiber aufzunehmen, die Aufwendungen für erforderliche Nachweise wenn möglich effizienter zu gestalten, sollte im Zuge der NIS2-Umsetzung und damit einhergehenden grundlegenden Änderungen an den entsprechenden Vorschriften eine Vereinbarkeit von ISO-Zwischenaudits und den gesetzlich erforderlichen KRITIS-Nachweisen nach BSIG geprüft werden.

In Bezug auf die die konkreten durch die Betreiber umzusetzenden Maßnahmen liegen dem BMI Stellungnahmen vor, die bei der Abwägung der Angemessenheit der Maßnahmen auch eine explizite Nennung einer erforderlichen Wirksamkeit der Maßnahmen fordern. Dies wird im Zuge der NIS2-Umsetzung ohnehin erforderlich und sollte daher auch bei einer Neuformulierung entsprechend

[6] Im Sinne der NIS-2-Richtlinie wird die Einrichtungskategorie mit erhöhten Anforderungen als „wesentlich“ (engl. „essential“) bezeichnet, die übrige Einrichtungskategorie als „wichtig“ (engl. „important“).

aufgenommen werden. Hierbei sollte sichergestellt werden, dass KRITIS-Betreibern auch das nach § 8b Abs. 4 BSIG verpflichtend aufzubauende Meldewesen im Zuge der Nachweiserbringung dokumentieren.

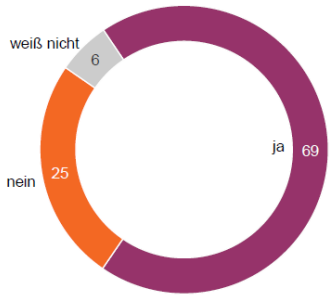


Abbildung 9: Bringt der Branchenspezifische Sicherheitsstandard (B3S) für Ihr Unternehmen einen Mehrwert? (n=211, Angaben in Prozent)

Für die vorgenannten Nachweise können KRITIS-Betreiber und ihre Branchenverbände branchenspezifische Sicherheitsstandards (sog. „B3S“) vorschlagen, die nach einer Feststellung der Eignung des BSI als Grundlage für Nachweise genutzt werden können. Zwei Drittel der im Rahmen der Umfrage befragten Unternehmen (68 %) haben derzeit einen B3S. Die überwiegende Mehrheit der Unternehmen, für die ein B3S vorliegt (80 %), setzt diesen auch für das Nachweisregime ein. 69 Prozent der befragten Unternehmen mit B3S sind der Überzeugung, dass dieser Standard ihnen einen Mehrwert bringt. Auch im Zuge der Evaluierung eingeholte Stellungnahmen aus der Wirtschaft waren diesbezüglich durchweg positiv. Dieses Vorgehen hat sich somit aus Sicht des BMI bewährt und gibt den KRITIS-Betreibern und ihren Branchenverbänden die Möglichkeit, innerhalb einer Branche abgestimmte Verfahren zur Absicherung der relevanten IT vorzuschlagen, die ggf. auch auf bereits vorhandene Branchenempfehlungen oder andere Branchenspezifika angemessen eingehen können. Ein ähnliches Vorgehen sollte daher auch für zukünftige Vorgaben angestrebt werden.

Der mit dem IT-Sicherheitsgesetz 2.0 eingeführte verpflichtende Einsatz von Systemen zur Angriffserkennung nach Stand der Technik führt auch aus Sicht der eingegangenen Stellungnahmen aus der Wissenschaft dazu, dass künftig voraussichtlich ein größerer Anteil der Angriffe erkannt wird und Beseitigungsmaßnahmen bei eingetretenen Störungen effektiver einsetzbar sind. Dem BMI liegen Stellungnahmen aus der Wissenschaft vor, dass insbesondere bei Kritischen Infrastrukturen, die einen besonders hohen Schutzbedarf ihrer IT haben, zusätzlich auch ein regelmäßiger Scan ihrer externen Angriffsfläche erforderlich werden kann. Solche „External Attack Surface“ (EAS) Scans identifizieren die direkt oder indirekt zur Organisationen gehörenden IT-Ressourcen und schließen insbesondere auch relevante Teile der Lieferkette (engl. Supply Chain) mit ein. Sie können signifikant zu einer Reduktion der Angriffsoberfläche und somit zu einer proaktiven Absicherung beitragen. Eine neu aufzunehmende verpflichtende Einführung von EAS Scans für KRITIS-Betreiber sollte daher geprüft werden.

§ 8b BSIG Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen

Was die Kommunikation von Sicherheitsvorfällen angeht, steht das BSI bei den befragten Unternehmen mit Abstand an erster Stelle: 87 Prozent der Unternehmen nennen es als wichtigsten Adressat. 52 Prozent informieren kooperierende Unternehmen, 44 Prozent andere Behörden. 38 Prozent geben Kunden, 37 Prozent Lieferanten Bescheid.

In Bezug auf den Informationsaustausch zwischen BSI und den KRITIS-Betreibern wurde seitens der Wirtschaft eine engere Anbindung an das Lagezentrum des BSI gewünscht, um hier schneller auch detaillierte Informationen und technische Indikatoren erhalten zu können und somit schneller, ggf. auch gemeinsam mit dem BSI, eine etwaige branchenspezifische Betroffenheit identifizieren zu können.

Ein entsprechendes Vorhaben wird aktuell durch das BMI unter dem Stichwort „sektorspezifische CERTs“ geprüft und mit Wirtschaftsvertretern erörtert. Je nach genauer Ausgestaltung kann eine entsprechende Weiterentwicklung des § 8b BSIG bzw. der sektorspezifischen Gesetze notwendig werden.

Auch die geplante Einrichtung eines BSI Information Sharing Portals (BISP) kann zur Verbesserung der zur Verfügung stehenden Lageinformationen führen. Durch den bidirektionalen und stärker automatisierten Ansatz des BISP können insbesondere technische Indikatoren schneller bereitgestellt und mit aktuellen Erkenntnissen angereichert werden.

In Bezug auf verpflichtend zu meldende Vorfälle wurde seitens der KRITIS-Betreiber das Anliegen vorgetragen, dass künftig nur noch diejenigen Vorfälle meldepflichtig sein sollten, die tatsächlich zu erheblichen Beeinträchtigungen der Funktionsfähigkeit der Kritischen Infrastrukturen geführt haben, nicht jedoch solche, die lediglich zu Beeinträchtigungen führen könnten oder die mitunter regelmäßig im Tagesgeschäft auftreten, und keine tatsächliche Gefährdung der Versorgung bedeuten. Eine Einschränkung der Meldepflicht auf lediglich diejenigen Vorfälle, die zu tatsächlichen Versorgungsausfällen geführt haben, würde jedoch zu einem Ausschluss von der Meldepflicht für alle Vorfälle führen, die von den Betreibern rechtzeitig mitigiert werden konnten. Dies kann regelmäßig auch neuartige Cyberangriffe oder -bedrohungen bedeuten, und eine Meldepflicht für derartige Fälle ist daher aus Sicht des BMI wichtig und erforderlich, um das BSI in die Lage zu versetzen, andere KRITIS-Betreiber vor ggf. auftretenden neuartigen Bedrohungen oder Angriffsmethoden zu warnen. Auch die NIS-2 Richtlinie sieht daher eine Meldeverpflichtung für Vorfälle vor, welche die Erbringung von Versorgungsdienstleistungen beeinträchtigen könnten, jedoch nicht zu tatsächlichen Beeinträchtigungen geführt haben. Im Zuge der NIS2-Umsetzung sollte daher geprüft werden, inwieweit eine weitere Konkretisierung meldepflichtiger Vorfälle im BSIG erfolgen kann, um den Betreibern bessere Hilfestellungen zu geben, welche Vorfälle im Interesse der Sicherheit Kritischer Infrastrukturen eine Meldepflicht auslösen, und welche nicht.

Stellungnahmen aus der Wissenschaft regen eine Prüfung an, ob Forschungseinrichtungen, insbesondere aus dem Bereich der angewandten Forschung, zu einer Meldung von durch Forschungsaktivitäten bekannt gewordenen Schwachstellen, Angriffswegen oder zu aktuell laufenden Angriffen auf Kritische Infrastrukturen verpflichtet werden können. Hierbei ist insbesondere eine Vereinbarkeit mit der gesetzlich geschützten Freiheit der Forschung (§ 4 Abs. 3 Hochschulrahmengesetz) zu prüfen.

Die Möglichkeit der freiwilligen Meldung von Schwachstellen durch Sicherheitsforschende wurde durch die Veröffentlichung der „Coordinated Vulnerability Disclosure Policy“ des BSI, die insbesondere die Möglichkeit der Anonymen Meldung vorsieht, bereits vereinfacht. Die Cybersicherheitsstrategie wird gemäß der NIS-2-Richtlinie weitere Schritte zur Förderung und Vereinfachung der koordinierten Offenlegung von Schwachstellen, gerade auch im Hinblick auf die Rechtssicherheit von Sicherheitsforschenden, enthalten.

Seitens der KRITIS-Betreiber wurde zudem das Anliegen vorgebracht, das Melde- und Informationswesen des BSI-Gesetzes möglichst synchron zum neu aufzubauenden Störungsmonitoring des KRITIS-Dachgesetzes zur Umsetzung der CER-Richtlinie zu gestalten. Dieses Anliegen ist aus Sicht des BMI nachvollziehbar und soll auch in der NIS2-Umsetzung so erreicht werden.

§ 8d BSIG Anwendungsbereich

Das BSI-Gesetz formuliert grundsätzlich horizontale Cybersicherheitsanforderungen für alle KRITIS-Sektoren, jedoch bestehen in bestimmten Teilsektoren derzeit sektorspezifische Ausnahmeregelungen, beispielsweise im AtG, TKG und EnWG. Um in allen KRITIS-Sektoren ein vergleichbares Sicherheitsniveau zu gewährleisten, sind bestehende sektorspezifische gesetzliche Vorgaben regelmäßig auf ihre Angemessenheit zu prüfen und ggf. an Änderungen im BSI-Gesetz anzupassen. Insbesondere im Energiesektor existieren derzeit geteilte Zuständigkeiten, da einige KRITIS-Betreiber unter das BSI-Gesetz und das hiesige Aufsichtsregime im Zuständigkeitsbereich des BSI fallen, und andere KRITIS-Betreiber unter das EnWG und das dortige Aufsichtsregime im Zuständigkeitsbereich der Bundesnetzagentur. Manche Betreiber unterliegen hierbei aufgrund ihrer erbrachten Versorgungsleistung gleichzeitig einer Regulierung des BSI-Gesetzes und des EnWG. Im Sinne möglichst vergleichbarer Vorgaben zur Gewährleistung eines einheitlichen Sicherheitsniveaus sollten daher geprüft werden, ob die bestehenden Ausnahmeregelungen im BSI-Gesetz für Betreiber von Energieversorgungsnetzen und Energieanlagen gestrichen werden, oder ob alle im Energiebereich tätigen Unternehmen unter die Vorgaben des EnWG fallen sollten.

Durch das Inkrafttreten der Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (DORA-Verordnung) werden künftig weite Teile des Finanzsektors unmittelbar durch europarechtliche Vorschriften geregelt. Um hier ein effizientes und effektives Zusammenspiel zwischen den zuständigen nationalen Behörden, insbesondere dem BSI und der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zu gewährleisten, sollte in der Umsetzung der entsprechenden europarechtlichen und nationalen gesetzlichen Vorschriften ein eng abgestimmtes Vorgehen zwischen BMI und BMF sichergestellt werden. Dies beinhaltet insbesondere zu treffende Verwaltungsvereinbarungen zwischen den zuständigen Behörden und ggf. auch gesetzliche Regelungen.

§ 8e BSIG Auskunftsverlangen

Bei den gesetzlichen Vorschriften zum Umgang mit Auskunftsersuchen Dritter in Bezug auf Kritische Infrastrukturen besteht sowohl aus Sicht der KRITIS-Betreiber als auch aus Sicht des BMI weitergehender Konkretisierungsbedarf. Insbesondere ist aus Sicht des BMI sicherzustellen, dass durch Auskunftsersuchen und etwaige Transparenzvorgaben keine potenziellen Sicherheitsrisiken für Kritische Infrastrukturen entstehen. Aufgrund seiner Tätigkeiten als zuständige Behörde, CSIRT und zentrale Anlaufstelle erhält das BSI bereits aktuell und auch künftig nach Umsetzung der NIS-2 Richtlinie eine Vielzahl sensibler Informationen über Kritische Infrastrukturen, weitere besonders schützenswerte Unternehmen und deren IT-Sicherheitsgefährdungen. Diese können sowohl einzeln als auch in Summe sensibel sein. Das Informationsfreiheitsgesetz (IFG) sieht eine Versagung nur dann vor, wenn die herausgegebene Information für sich genommen sensibel ist und lässt daher eine Ausforschung durch Informationszugangsanträge zu, die für sich genommen auf unsensible Informationen gerichtet sind, aber in Summe die Zusammenfügung zu einem sensiblen Bild der Informationssicherheit Kritischer Infrastrukturen ermöglichen. Im Hinblick auf die sich seit dem russischen Angriffskrieg auf die Ukraine zuspitzende geopolitische Lage und die zunehmende Gefahr von Cyberangriffen müssen diese Informationen daher besonders geschützt werden. Auch die NIS-2 Richtlinie schreibt entsprechend die Sicherstellung der Vertraulichkeit für die bei den zuständigen Behörden vorliegenden Informationen vor. Im Zuge der NIS-Umsetzung sollten daher hier weitergehende Einschränkungen der verpflichtenden Informationsweitergabe vorgesehen werden. Das

grundgesetzlich geschützte parlamentarische Auskunfts- und Fragerecht bleibt von diesen Änderungen unberührt.

§ 10 Absatz 1 BSIG Ermächtigung zum Erlass von Rechtsverordnungen

Die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) wurde erstmals 2016 und 2017 erlassen und seitdem regelmäßig überarbeitet. Die letzte Änderungsverordnung zur Aufnahme von LNG-Terminals und Seekabelanlandestationen ist am 23. Februar 2023 in Kraft getreten. Das Verfahren zum Erlass der BSI-KritisV im Einvernehmen mit den jeweils zuständigen Ressorts und nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und Wirtschaftsverbände hat sich aus Sicht des BMI bewährt. Konkrete Änderungswünsche am Verfahren wurden durch die von BMI im Zuge der Evaluierung beteiligten Institutionen nicht genannt. Es sollte daher auch zukünftig im Zuge der NIS2-Umsetzung in vergleichbarer Form beibehalten werden. Insbesondere sollte hier aus Sicht des BMI künftig sichergestellt werden, dass die Umsetzungen der CER-Richtlinie und der NIS-2 Richtlinie in Deutschland möglichst einheitlich erfolgt. Grundlage hierfür sind einheitliche Begriffsbestimmungen. Dies wird im Zuge der NIS2-Umsetzung voraussichtlich auch zu systematischen Änderungen an dieser Vorschrift führen, wobei auch für eine mögliche Nachfolgerverordnung zur BSI-KritisV ein vergleichbares Verfahren angestrebt werden sollte.

4. Fazit, Ausblick

Aus den Ergebnissen der Befragung lässt sich eine Wirksamkeit der in den IT-Sicherheitsgesetzen formulierten Maßnahmen und Ziele bei den KRITIS-Betreibern ablesen. Herausforderungen für die Umsetzung der gesetzlichen Vorgaben und somit auch indirekt für die Wirksamkeit der gesetzlichen Vorschriften werden demnach primär in den Rahmenbedingungen gesehen, unter denen die Unternehmen agieren müssen, darunter die mitunter schwierige Ausstattung mit erforderlichen Finanzmitteln.

Die Notwendigkeit der vollständigen Umsetzung der gesetzlichen Vorgaben erhält eine sehr hohe Zustimmung. Fast alle Betriebe halten den Maßnahmenkatalog für sinnvoll, und auch ihr Einfluss auf die interne IT-Sicherheit wird mehrheitlich als positiv eingeschätzt. Das erste IT-SiG und das IT-SiG 2.0, die als Reaktion auf die gestiegene Gefährdungslage entstanden, haben insofern neben den konkreten umzusetzenden Maßnahmen auch eine weitere wichtige Funktion für die Betreiber: Sie helfen dabei, das Problembewusstsein und die Management-Awareness hochzuhalten, und zwar insbesondere auch bei solchen Unternehmen, die bislang nicht von Cyber-Angriffen betroffen waren. Die Umsetzung der konkreten gesetzlichen Maßnahmen sowie der enge Austausch mit dem BSI führen demnach dazu, dass die KRITIS-Betreiber Schritt für Schritt ihre Abwehrmechanismen verbessern können und die Cybersicherheit für Kritische Infrastrukturen insgesamt somit nachhaltig gestärkt wird.

Die gesetzlichen Vorgaben werden bei den befragten KRITIS-Betreibern allgemein neben der hohen Akzeptanz auch insgesamt als wirksam erlebt: Neun von zehn befragten Unternehmen halten sie für sinnvoll, über drei Viertel bestätigen ihren positiven Einfluss auf die IT-Sicherheit. Knapp drei Viertel beobachten eine höhere Sensibilisierung von Mitarbeitenden und Geschäftsführung.

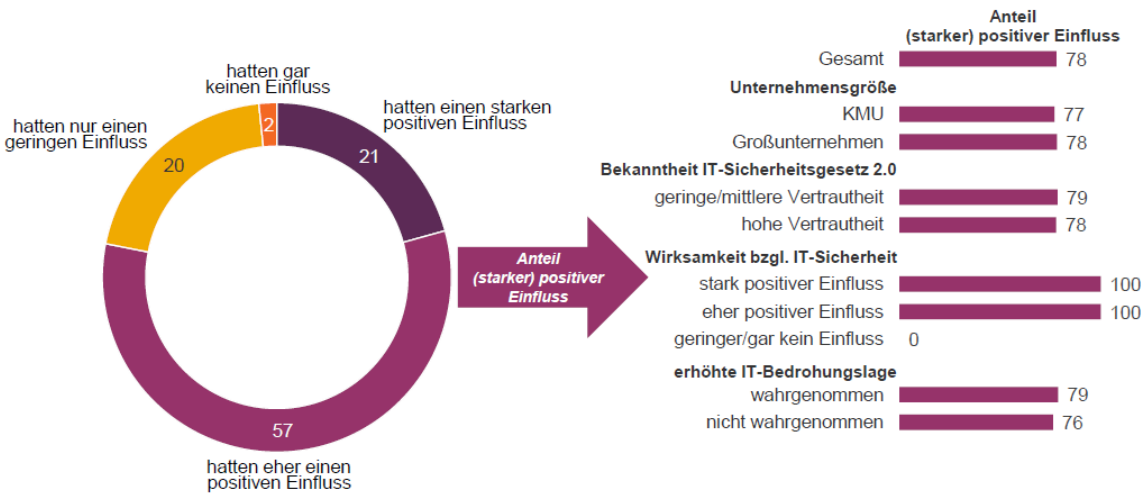


Abbildung 13: Wie wirksam waren die durch das erste IT-SiG und das IT-SiG 2.0 geforderten Maßnahmen und deren Umsetzung im Hinblick auf die IT-Sicherheit in Ihrem Unternehmen? (n=308, Angaben in Prozent)

Die Wirksamkeit des ersten IT-SiG sowie des IT-SiG 2.0 kann daher insgesamt als gut bewertet werden. Gleichwohl wurden in der Evaluierung an einigen Stellen Wirksamkeitslücken sowie konkrete Änderungs- und Konkretisierungsbedarfe festgestellt. Sie sollten, wenn möglich, im Zuge der NIS-2 Umsetzung oder weiterer erforderlicher Gesetzesanpassungen sowie im Rahmen zur Verfügung stehender Haushaltsmittel umgesetzt werden.

Impressum

Herausgeber
Bundesministerium des Innern und für Heimat, 11014 Berlin
Internet: www.bmi.bund.de

Stand
02.05.2023