Vorblatt

Ziel(e)

- Schaffung der Voraussetzungen für die Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen

Inhalt

Das Vorhaben umfasst hauptsächlich folgende Maßnahme(n):

- Weiterentwicklung und Koordination einer neuen Strategie für die Sicherheit von Netz- und Informationssysteme
- Einrichtung von nationalen Koordinierungsstrukturen zur Prävention sowie zur Bewältigung von Sicherheitsvorfällen
- Einrichtung von Computer-Notfallteams zur Unterstützung der Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen des Bundes und der Länder bei der Bewältigung von Risiken, Vorfällen und Sicherheitsvorfällen
- Ermittlung der Betreiber wesentlicher Dienste
- Pflicht zur Setzung geeigneter Sicherheitsvorkehrungen; Informations- und Meldepflichten
- Einrichtung und Betrieb einer Meldesammelstelle und einer zentralen Anlaufstelle
- Betrieb und Nutzung von IKT-Lösungen

Finanzielle Auswirkungen auf den Bundeshaushalt und andere öffentliche Haushalte:

In den finanziellen Auswirkungen sind folgende Posten berücksichtigt:

- Einrichtung und Betrieb von Organisationseinheiten im BKA laut Vorgaben der NIS-Richtlinie

- Einrichtung und Betrieb von Organisationseinheiten im BMI laut Vorgaben der NIS-Richtlinie
- Sachaufwendungen für den Betrieb von IKT-Lösungen durch BMI

Finanzierungshaushalt für die ersten fünf Jahre

in Tsd. €	2019	2020	2021	2022
Nettofinanzierung Bund	**-5.438**	**-6.565**	**-5.787**	**-6.466**

Auswirkungen auf die Verwaltungskosten für Unternehmen:

Die rechtsetzende Maßnahme enthält 2 neue Informationsverpflichtung/en für Unternehmen. Es wird durch diese für alle Unternehmen insgesamt eine Belastung von rund € 643.000,- pro Jahr verursacht.

Die NIS-Richtlinie sieht vor, dass bestimmte private und öffentliche Anbieter angemessene IT-Sicherheitsmaßnahmen ergreifen, um den Risiken für ihre Netzwerk- und Informationssysteme sowie konkreten Störfällen entsprechend begegnen zu können. Ferner unterliegen sie einer Meldepflicht für erhebliche Störfälle. Die von der NIS-Richtlinie erfassten Anbieter werden in zwei Gruppen unterteilt: Betreiber wesentlicher Dienste und Digitale Diensteanbieter.

In den weiteren Wirkungsdimensionen gemäß § 17 Abs. 1 BHG 2013 treten keine wesentlichen Auswirkungen auf.

Verhältnis zu den Rechtsvorschriften der Europäischen Union:

Das Vorhaben dient unter anderem der Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union. Eine Übererfüllung von unionsrechtlichen Vorgaben, die zu einer Mehrbelastung der betroffenen Unternehmen führen würde, liegt nicht vor.

Besonderheiten des Normerzeugungsverfahrens:

Zweidrittelmehrheit im Nationalrat im Hinblick auf eine vorgesehene Verfassungsbestimmung (§ 1 NISG) und Zustimmung des Bundesrates mit Zweidrittelmehrheit gemäß Art. 44 Abs. 2 B-VG.

Wirkungsorientierte Folgenabschätzung

Bundesgesetz, mit dem das Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG) erlassen wird

Einbringende Stelle:	Bundeskanzleramt
Vorhabensart:	Bundesgesetz
Laufendes Finanzjahr:	2018
Inkrafttreten/ Wirksamwerden:	2019

Problemanalyse

Problemdefinition

Netz- und Informationssysteme mit den zugehörigen Diensten spielen eine zentrale Rolle in der heutigen Gesellschaft. Für wirtschaftliche und gesellschaftliche Tätigkeiten ist es daher von entscheidender Bedeutung, dass sie verlässlich und sicher sind. Mit diesem Bundesgesetz werden daher Maßnahmen festgelegt, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen der in den Anwendungsbereich fallenden Einrichtungen erreicht werden soll.

Mit der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (im Folgenden: NIS-RL), die am 8. August 2016 in Kraft getreten ist, soll dies auch EU-weit erreicht werden. Vor diesem Hintergrund sollen die Mitgliedstaaten eine nationale NIS-Strategie zur Bestimmung der Ziele und der damit verbundenen Regulierungsmaßnahmen erarbeiten, nationale (strategische und operative) Behörden und Computer-Notfallteams benennen und bestimmte, für das Gemeinwohl wichtige private und öffentliche Anbieter (Betreiber wesentlicher Dienste und digitale Diensteanbieter) zu angemessenen Sicherheitsmaßnahmen und Meldung erheblicher Störfälle verpflichten. Die von der NIS-RL vorgesehenen Maßnahmen zielen darauf ab, die Zusammenarbeit zwischen den Mitgliedstaaten in strategischer und operationeller Hinsicht zu stärken.

Betreiber eines wesentlichen Dienstes stellen einen Dienst der in Anhang II der NIS-RL genannten und im Folgenden aufgelisteten Sektoren zur Verfügung: Energie (Elektrizität, Erdöl, Erdgas), Verkehr (Luftverkehr, Schienenverkehr, Schifffahrt, Straßenverkehr), Bankwesen (Kreditinstitute), Finanzmarktinfrastrukturen (Betreiber von Handelsplätzen, zentrale Gegenparteien), Gesundheitswesen (Einrichtungen der medizinischen Versorgung, einschließlich Krankenhäuser und Privatkliniken), Trinkwasserlieferung und -versorgung (Lieferanten von und Unternehmen der Versorgung mit "Wasser für den menschlichen Gebrauch"), Digitale Infrastruktur (Internet Exchange Points, DNS-Diensteanbieter, TLD-Name-Register). Ferner sollen Einrichtungen des Bundes und der Länder im Rahmen der österreichischen Umsetzung berücksichtigt werden.

Digitale Diensteanbieter sind – ab einer gewissen Größe – sämtliche Anbieter eines Online-Marktplatzes, einer Online-Suchmaschine oder eines Cloud-Computing Dienstes.

Mit dem vorliegenden Gesetzesvorhaben wird die NIS-RL umgesetzt und darüber hinaus ein Regelwerk zu den in Österreich bereits seit vielen Jahren bestehenden Koordinationsstrukturen im Bereich der Sicherheit von Netz- und Informationssystemen geschaffen.

Nullszenario und allfällige Alternativen

Ohne die Implementierung von Maßnahmen würde das Sicherheitsniveau von Netz- und Informationssystemen in Österreich nicht gehoben werden können, weil derzeit (nicht alle) potenziell von Sicherheitsvorfällen betroffene Einrichtungen weder präventive Sicherheitsvorkehrungen treffen, noch bereits entstandene Sicherheitsvorfälle melden müssen. Fehlen die notwendigen rechtlichen Grundlagen für die behördlichen und nicht-behördlichen Strukturen in diesem Bereich, kann nicht gewährleistet werden, dass – insbesondere im Bereich der Betreiber wesentlicher Dienste – angemessen auf gravierende

Sicherheitsvorfälle reagiert werden kann. Auch die Information anderer potenziell betroffener Unternehmen sowie der Öffentlichkeit über die aktuelle Bedrohungslage wäre nicht möglich.

Vorhandene Studien/Folgenabschätzungen

"IMPACT ASSESSMENT Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union": http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013SC0032

Interne Evaluierung

Zeitpunkt der internen Evaluierung: 2022

Evaluierungsunterlagen und -methode: Zum Zeitpunkt der Evaluierung sind die vom Anwendungsbereich des vorliegenden Gesetzentwurfs erfassten Betreiber wesentlicher Dienste identifiziert. Betreiber wesentlicher Dienste, Anbieter digitaler Dienste sowie die Einrichtungen des Bundes und der Länder treffen geeignete Sicherheitsvorkehrungen innerhalb ihrer Organisationsstruktur und erbringen (soweit gesetzlich vorgesehen) die erforderlichen Nachweise über die umgesetzten Maßnahmen.

Ziele

Ziel: Schaffung der Voraussetzungen für die Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen

Wie sieht Erfolg aus:

Ausgangszustand Zeitpunkt der WFA	Zielzustand Evaluierungszeitpunkt
Betreiber wesentlicher Dienste, Anbieter digitaler Dienste sowie Einrichtungen des Bundes und der Länder sind nicht dazu verpflichtet, Sicherheitsvorkehrungen im Bereich der Netz- und Informationssysteme zu treffen oder durch mangelnde Sicherheitsvorkehrungen verursachte Sicherheitsvorfälle zu melden. Dies kann unter Umständen zu Versorgungsengpässen führen und die öffentliche Sicherheit sowie die Funktionsfähigkeit staatlicher Einrichtungen gefährden.	Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen des Bundes und der Länder treffen organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer Netz- und Informationssysteme. Bei Vorliegen eines Sicherheitsvorfalls erstatten die genannten Einrichtungen unverzüglich Meldung an das jeweils zuständige Computer-Notfallteam, welches die Meldungen an die Behörden weiterleitet.
Um angemessen auf Sicherheitsvorfälle im Bereich der Netz- und Informationssystemsicherheit zu reagieren, bestehen derzeit keine gesetzlich festgelegten Organisations- und Koordinierungsstrukturen.	Neue Koordinierungsstrukturen schaffen einen geeigneten Rahmen um angemessen auf Sicherheitsvorfälle zu reagieren. Dabei werden Meldungen über Sicherheitsvorfälle und aktuelle Bedrohungslagen gesamtstaatlich analysiert und regelmäßig Lagebilder erstellt. Ein nationales Computer-Notfallteam unterstützt die Betreiber wesentlicher Dienste sowie die Anbieter digitaler Dienste bei der Prävention, Erkennung, Reaktion und Folgenminderung von Sicherheitsvorfällen im Bereich von Netz- und Informationssystemen. Sektorenspezifische Computer-Notfallteams sind eingerichtet.

Maßnahmen

Maßnahme 1: Weiterentwicklung und Koordination einer neuen Strategie für die Sicherheit von Netz- und Informationssysteme

Beschreibung der Maßnahme:

Die Österreichische Strategie für Cyber Sicherheit (ÖSCS) aus dem Jahr 2013 ist ein umfassendes und proaktives Konzept zum Schutz des Cyber Raums und der Menschen im virtuellen Raum unter Gewährleistung ihrer Menschenrechte. Die Vorgaben aus der NIS-RL und aktuelle Entwicklungen im Bereich Cyber Sicherheit sind nicht berücksichtigt. Auf Basis der ÖSCS wird diese Strategie vor dem Hintergrund der in der NIS-RL genannten Aspekte weiterentwickelt und koordiniert. Die neue Strategie zur Sicherheit für Netz- und Informationssysteme in Österreich soll daher neben den Vorgaben aus der NIS-RL auch aktuelle Entwicklungen und Bedrohungsszenarien berücksichtigt.

Maßnahme 2: Einrichtung von nationalen Koordinierungsstrukturen zur Prävention sowie zur Bewältigung von Sicherheitsvorfällen

Beschreibung der Maßnahme:

Auf Basis sowie unter Einbindung bestehender operativer Strukturen wird eine neue Struktur zur Koordination auf der operativen Ebene (OpKoord) geschaffen. Diese Koordinierungsstruktur besteht aus einem sogenannten "Inneren Kreis" und einem "Äußeren Kreis". Die Arbeiten im Rahmen der OpKoord werden unter Einbindung der Ressorts und operativer Strukturen aus Wirtschaft und Forschung vom Bundesminister für Inneres koordiniert.

In ihrem Rahmen sollen insbesondere ein periodisches und anlassbezogenes Lagebild erstellt, erörtert und aktualisiert sowie über zu treffende Maßnahmen auf der operativen Ebene beraten werden. Darüber hinaus soll durch Sammeln, Bündeln, Auswerten und Weitergeben von relevanten Informationen ein kontinuierlicher Überblick über die aktuelle Situation im Bereich der NIS gewährleistet sein. Dabei ist auch die Wirtschaft in geeigneter Form einzubinden und zu informieren. Der permanent und gemeinsam erarbeitete Status zur Situation im Bereich der NIS soll allen Beteiligten als Grundlage für zu treffende planerische, präventive und reaktive Maßnahmen dienen.

Zur Wahrnehmung strategischer Aufgaben im Zusammenhang mit dem Gesetzesvorhaben richtet der Bundeskanzler Organisationseinheiten ein. Der Bundesminister für Inneres wird die operativen Aufgaben wahrnehmen und richtet dazu ebenfalls Organisationseinheiten ein.

Maßnahme 3: Einrichtung von Computer-Notfallteams zur Unterstützung der Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen des Bundes und der Länder bei der Bewältigung von Risiken und Sicherheitsvorfällen

Beschreibung der Maßnahme:

Zur Unterstützung der Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen des Bundes und der Länder bei der Bewältigung von Risiken, Vorfällen und Sicherheitsvorfällen im Bereich der Netz- und Informationssystemsicherheit sollen sog. Computer-Notfallteams eingerichtet werden. Die Computer-Notfallteams gelten als erste Anlaufstelle für alle in den Anwendungsbereich des vorliegenden Gesetzentwurfs fallenden Einrichtungen.

Betreiber wesentlicher Dienste können je ein sektorenspezifisches Computer-Notfallteam einrichten, um das für den jeweiligen Sektor erforderliche Fachwissen abzudecken. Wurde noch kein sektorenspezifisches Computer-Notfallteam eingerichtet, fallen die im vorliegenden Gesetzentwurf umschriebenen Aufgaben von Computer-Notfallteams dem nationalen Computer-Notfallteam zu. Das nationale Computer-Notfallteam soll – in Ermangelung eines sektorenspezifischen Computer-Notfallteams – für alle Betreiber wesentlicher Dienste und Anbieter digitaler Dienste zuständig sein und jene Aufgaben sektorenübergreifend erfüllen, die einem Computer-Notfallteam nach dem vorliegenden Gesetzentwurf zukommen.

Für die Einrichtungen des Bundes und der Länder erfüllt das GovCERT die Aufgaben eines Computer-Notfallteams. Das beim Bundeskanzler eingerichtete GovCERT ist daher das sektorenspezifische Computer-Notfallteam für den öffentlichen Bereich.

Zu den Hauptaufgaben der Computer-Notfallteams zählen die Entgegennahme von Meldungen über Sicherheitsvorfälle oder Störungen und deren Weiterleitung an den Bundesminister für Inneres.

Maßnahme 4: Ermittlung der Betreiber wesentlicher Dienste

Beschreibung der Maßnahme:

Der Bundeskanzler ermittelt im Einvernehmen mit dem Bundesminister für Inneres jene Einrichtungen, die einen wesentlichen Dienst im Sinne von § 14 Abs. 2 des vorliegenden Gesetzentwurfs erbringen.

Mit Verordnung werden die Faktoren, die zur Ermittlung der Betreiber wesentlicher Dienste herangezogen werden sollen, näher konkretisiert. In dieser Verordnung werden insbesondere die Schwellenwerte bestimmt, die für die Beurteilung der Wesentlichkeit eines betriebenen Dienstes heranzuziehen sind.

Maßnahme 5: Pflicht zur Setzung geeigneter Sicherheitsvorkehrungen; Informations- und Meldepflichten

Beschreibung der Maßnahme:

Betreiber wesentlicher Dienste, Anbieter digitaler Dienste sowie Einrichtungen des Bundes und der Länder haben geeignete und dem Stand der Technik entsprechende Sicherheitsvorkehrungen zu treffen. Diese können sowohl technischer als auch organisatorischer Art sein und sollen Störfälle im Bereich der Netz- und Informationssysteme vermeiden, die unter Umständen einen Sicherheitsvorfall herbeiführen können.

Die Einhaltung der Sicherheitsvorkehrungen wird periodisch überprüft, indem die Betreiber wesentlicher Dienste den Bundesminister für Inneres die Erfüllung der Anforderungen in geeigneter Weise informieren. Anbieter digitaler Dienste haben einen solchen Nachweis nur im Anlassfall zu erbringen.

Darüber hinaus haben Betreiber wesentlicher Dienste, Anbieter digitaler Dienste sowie die Einrichtungen des Bundes und der Länder Sicherheitsvorfälle unverzüglich an das für sie jeweils zuständige Computer-Notfallteam zu melden.

Maßnahme 6: Einrichtung und Betrieb einer Meldesammelstelle und einer zentralen Anlaufstelle

Beschreibung der Maßnahme:

Die Meldestruktur von Sicherheitsvorfällen und Störungen nach dem NIS-Gesetz sieht vor, dass die Meldungen, die an das zuständige Computer-Notfallteam gegangen sind, an die beim Bundesminister für Inneres eingerichtete Organisationseinheit weitergeleitet werden sollen. Um die Meldungen zentralisiert zu erfassen und entsprechend zu verarbeiten, bedarf es einer Meldesammelstelle.

Zudem hat jeder Mitgliedstaat gemäß Art. 8 Abs. 3 NIS-RL eine für die Sicherheit von Netz- und Informationssystemen zuständige nationale zentrale Anlaufstelle zu benennen. Diese zentrale Anlaufstelle (Single Point Of Contact, SPOC) dient insbesondere als Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit der Behörden der Mitgliedstaaten und der Zusammenarbeit mit den entsprechenden Behörden in anderen Mitgliedstaaten.

Sowohl die Meldesammelstelle, als auch die zentrale Anlaufstelle werden beim Bundesamt für Verfassungsschutz und Terrorismusbekämpfung eingerichtet und deren Betrieb in weiterer Folge durch Dienstplan und Rufbereitschaften rund um die Uhr sichergestellt.

Maßnahme 7: Betrieb und Nutzung von IKT-Lösungen

Beschreibung der Maßnahme:

Der Betrieb und Nutzung von IKT-Lösungen betrifft einerseits die jeweilige Einrichtung eines IOC-basierten Frühwarnsystems durch den Bundesminister für Inneres, andererseits die Verwendung von Honeypots, Honeypot-ähnlichen-Ansätzen sowie Sinkholes durch den Bundesminister für Inneres und das GovCERT. Die IKT-Lösungen dienen einerseits dazu, Cyberangriffe zu vermeiden bzw. deren Auswirkungen so gering wie möglich zu halten, und andererseits Muster und Vorgehensweisen bei Cyberangriffen zu analysieren.

Abschätzung der Auswirkungen

Finanzielle Auswirkungen für alle Gebietskörperschaften und Sozialversicherungsträger

Finanzielle Auswirkungen für den Bund

– Ergebnishaushalt

in Tsd. €	2019	2020	2021	2022
Personalaufwand	2.468	3.251	3.316	3.382
Betrieblicher Sachaufwand	2.376	2.023	2.066	2.139
Werkleistungen	200	250	450	800
Aufwendungen gesamt	**5.044**	**5.524**	**5.832**	**6.321**

Aus dem Vorhaben ergeben sich keine finanziellen Mehraufwendungen für Länder, Gemeinden und Sozialversicherungsträger.

Auswirkungen auf die Verwaltungskosten für Bürger/innen und für Unternehmen

Auswirkungen auf die Verwaltungskosten für Unternehmen

IVP	Kurzbezeichnung	Fundstelle	Be-Entlastung (in Tsd. €)
1	Meldung von Sicherheitsvorfällen an das zuständige Computer-Notfallteam	§ 19 Abs. 1 und § 21 Abs. 2	41
2	Nachweis über die getroffenen Sicherheitsvorkehrungen	§ 17 Abs. 3 und § 21 Abs. 4	602

Betreiber wesentlicher Dienste und Anbieter digitaler Dienste haben Sicherheitsvorfälle unverzüglich zu melden. Der Gesetzentwurf sieht weiters vor, dass die Einhaltung der Sicherheitsvorkehrungen periodisch zu überprüfen ist. Dafür haben die betroffenen Betreiber wesentlicher Dienste dem Bundesminister für Inneres die Erfüllung der Anforderungen in geeigneter Weise nachzuweisen.

Anhang

Detaillierte Darstellung der finanziellen Auswirkungen

Bedeckung

in Tsd. €			2019	2020	2021	2022
Auszahlungen/ zu bedeckender Betrag			5.438	6.565	5.787	6.466
in Tsd. €	Betroffenes Detailbudget	Aus Detailbudget	2019	2020	2021	2022
gem. BFRG/BFG	10.01.04 Dienststellen und ausgegliederte Bereiche		797	813	830	846
gem. BFRG/BFG	11.02.08 Zentrale Sicherheitsaufgaben		5.461	4.686	5.197	5.220

Erläuterung der Bedeckung

Die Bedeckung ist im Detailbudget 0104 bzw. 0208 in der BFRG-Planung zu berücksichtigen.

Laufende Auswirkungen – Personalaufwand

	2019		2020		2021		2022	
Körperschaft	Aufw. (Tsd. €)	VBÄ	Aufw. (Tsd. €)	VBÄ	Aufw. (Tsd. €)	VBÄ	Aufw. (Tsd. €)	VBÄ
Bund	2.467,82	33,00	3.251,03	43,00	3.316,05	43,00	3.382,37	43,00

Es wird darauf hingewiesen, dass der Personalaufwand gem. der WFA-Finanziellen Auswirkungen-VO valorisiert wird.

		2019	2020	2021	2022
Maßnahme / Leistung	Körpersch.	VBÄ	VBÄ	VBÄ	VBÄ
BKA Leitung	Bund	1,00	1,00	1,00	1,00

BKA Stellvertretung	Bund	1,00	1,00	1,00	1,00
BKA Fachreferenten	Bund	4,00	4,00	4,00	4,00
BKA Teamassistenz	Bund	1,00	1,00	1,00	1,00
BMI Leitung	Bund	2,00	2,00	2,00	2,00
BMI Exekutivdienst	Bund	1,00	2,00	2,00	2,00
BMI Fachreferenten	Bund	16,00	22,00	22,00	22,00
		5,00	8,00	8,00	8,00
BMI Juristische Referenten	Bund	1,00	1,00	1,00	1,00
BMI Assistenz	Bund	1,00	1,00	1,00	1,00

Einrichtung einer Organisationseinheit beim Bundeskanzler:

1. Parameter

Zu den gesetzlichen Aufgaben gehören unter anderem:

. Weiterentwicklung und Pflege der Österreichischen Strategie für Cyber Sicherheit und die Erstellung des Cyber Sicherheit Jahresberichts.

. Vertretung von Österreich in der europäischen NIS-Kooperationsgruppe, sowie in anderen EU-weiten und internationalen Gremien für Netz- und Informationssystemsicherheit, denen strategische Aufgaben zugewiesen sind.

. Koordination der öffentlich-privaten Zusammenarbeit im Rahmen der Österreichischen Strategie für Cyber Sicherheit (ÖSCS) und der Cybersicherheitsstrategie der Europäischen Union.

. Ausarbeitung und Veröffentlichung von Leitlinien zu den Umständen, unter denen Betreiber wesentlicher Dienste Sicherheitsvorfälle melden müssen, sowie für die Parameter zur Feststellung des Ausmaßes der Auswirkungen eines Sicherheitsvorfalls.

. Festlegen von Standards für die von den Betreibern zu ergreifenden Sicherheitsvorkehrungen.

. Information der Öffentlichkeit über einen Sicherheitsvorfall, der die vom Anwendungsbereich des vorliegenden Gesetzesvorhabens umfassten Sektoren betrifft.

. Konsultation mit den zuständigen Behörden anderer Mitgliedstaaten, wenn

o ein Betreiber wesentlicher Dienste diese auch außerhalb Österreichs erbringt

o wenn Anbieter digitaler Dienste ihre Hauptniederlassung in Österreich haben, sich aber ihre Netz- und Informationssysteme in einem anderen Mitgliedstaat befinden.

. Pflege und laufende Aktualisierung einer Liste aller Unternehmen, die von der Umsetzung der europäischen Richtlinie in Österreich betroffen sind.

. Pflege und laufende Aktualisierung einer Liste aller Dienste, die von der Umsetzung der europäischen Richtlinie in Österreich betroffen sind.

. Ernennung von Computer-Notfallteams zu behördlichen Sektor Meldestellen für meldepflichtige Vorfälle und laufende Überprüfung der Kriterien dafür.

. Pflege und Wartung aller Kriterien, Grenzwerte und Sicherheitsvorgaben für die Betreiber wesentlicher Dienste in Österreich

. Veröffentlichung aller Informationen, Ausstellung von Erlässen und Bescheiden

. Einrichtung einer Anlaufstelle für Beratung, Informationen und Beschwerden für die Betreiber wesentlicher Dienste.

. Berichtlegung an die Europäische Kommission bezüglich Festlegung von neuen Strategien für die Netz- und Informationssystemen.

Daraus ergeben sich die zentralen Themenbereiche der Organisationseinheit:

Strategien, Internationale Koordination, Öffentlich Private Kooperation, Standards und Kriterien, Management von Betreibern wesentlicher Dienste, Kriterien und Grenzwerte, und abgeleitet die dafür notwendigen Bereiche Gesamtstaatliche Analysen, Cyber Sicherheit Themen, Awareness/Öffentlichkeitsarbeit, Forschung & Innovation und Capacity Building. Aus den abgeleiteten Themen ergeben sich Aufgaben, die zwingend notwendig sind, um die gesetzlichen Aufgaben umzusetzen.

2. Zum zeitlichen Verlauf

Die Einrichtung der Behörde ist abhängig von der Verfügbarkeit von qualitativ geeigneten Ressourcen am internen und externen Arbeitsmarkt und anderen Ressourcen wie Arbeitsplatz und notwendigen Ausstattungen. Zu berücksichtigen sind auch das Einrichten der notwendigen Strukturen und Prozesse, die Ausbildung der neuen Mitarbeiter und das Heranführen an ihre vorgesehenen Aufgaben.

Der gesetzlich verpflichtende Betrieb kann direkt proportional zu der Verfügbarkeit der benötigten Ressourcen eingerichtet werden. Dabei wird Rücksicht genommen auf die Priorität der Aufgaben zum Zeitpunkt des gesetzlichen Starts. Kann der geplante Aufbau nicht wie vorgesehen umgesetzt werden, wird ein Notbetrieb eingerichtet und sukzessive erweitert.

Einrichtung einer Organisationseinheit durch den Bundesminister für Inneres:

1. Parameter

Alle Vorgaben der europäischen NIS-Richtlinie mit operativem Charakter müssen von der gesetzlich einzurichtenden Organisationseinheit umgesetzt werden. Dieses wird im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung eingerichtet.

Zu den gesetzlichen Aufgaben gehören insbesondere:

- Betrieb einer zentralen Anlaufstelle (SPOC) für die Sicherheit von Netz- und Informationssystemen

- Koordination der Operativen Koordinierungsstruktur (OpKoord) und deren Inneren Kreises (IKDOK)

- Entgegennahme und Analyse von Meldungen über Sicherheitsvorfälle und sonstige Störungen von Betreibern wesentlicher Dienste, Anbietern digitaler Dienste und Einrichtungen des Bundes und der Länder bzw. deren zuständigen Computer-Notfallteams in einer Meldesammelstelle

- Regelmäßige Erstellung eines Lagebildes und die Weiterleitung der Meldungen sowie des Lagebildes und zusätzlicher relevanter Informationen an inländische Behörden oder Stellen

- Betrieb und Nutzung von IKT-Lösungen (IOC-basiertes Frühwarnsystem, Honeypots und Sinkholes)

- Funktion des Auftragsverarbeiters für die gemeinsame Datenanwendung von BMI und BKA

- Erstellung und Weitergabe von zur Gewährleistung der Sicherheit von Netz- und Informationssystemen relevanten Informationen zur Vorbeugung von Sicherheitsvorfällen

- Festlegung der Voraussetzungen von qualifizierten Stellen und deren Überprüfung

- Laufende Überprüfung der Sicherheitsvorkehrungen der Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen des Bundes und der Länder sowie die Einhaltung deren Meldepflicht

- Unterrichtung der Öffentlichkeit über einzelne Sicherheitsvorfälle

- Leitung und Koordination des Cyberkrisenmanagements auf operativer Ebene

Die sich daraus ergebenden zentralen Themenbereiche der Organisationseinheit im BMI sind folgende:

Lagebild / Cyberanalyse, Cyberprävention / Cyberkrisenmanagement, Cyber Threat Intelligence, Entwicklung, Audit, SPOC / Meldesammelstelle, IKDOK, Administrative Unterstützung, IOC-basiertes Frühwarnsystem

2. Zum zeitlichen Verlauf

Da ein Vollausbau der Behörde in diesem kurzen Zeitraum nicht möglich ist, muss der Aufbau nach einem Stufenplan erfolgen. In einem 4-Jahres-Plan soll fachlich geeignetes Personal der Behörde für die Erfüllung der Aufgaben bzw. zentralen Themenbereiche zugeführt werden. Da insbesondere die Meldesammelstelle und die zentrale Anlaufstelle einsatzfähig sein müssen, liegt der Fokus zunächst auf deren Strukturen und Prozessen. Zudem bedarf der Betrieb der IKT-Lösungen (IOC-basiertes Frühwarnsystem) zunehmend eines erhöhten Personalaufwands, da dieser von einem Probebetrieb mit wenigen IKT-Lösungen zu einem Vollbetrieb ausgebaut werden soll.

***

Über eine allfällige Abweichung zwischen Ergebnis- und Finanzierungshaushalt kann aus heutiger Sicht keine Angabe gemacht werden. Die Verteilung der Aufwendungen zwischen den Gebietskörperschaften ist nicht vorgesehen.

***

Laufende Auswirkungen – Arbeitsplatzbezogener betrieblicher Sachaufwand

Körperschaft (Angaben in €)	2019	2020	2021	2022
Bund	863.736,44	1.137.860,44	1.160.617,65	1.183.829,99

Laufende Auswirkungen – Sonstiger betrieblicher Sachaufwand

Körperschaft (Angaben in €)	2019	2020	2021	2022
Bund	1.500.000,00	700.000,00	700.000,00	700.000,00

		2019		2020		2021		2022	
Bezeichnung	Körperschaft	Menge	Aufw. (€)	Menge	Aufw. (€)	Menge	Aufw. (€)	Menge	Aufw. (€)
Einrichtung Organisationseinheit im BMI	Bund	1	1.500.000,00						
Betrieb des IOC-basierten Frühwarnsystems, Raumanmietung und Ausstattung BMI	Bund			1	700.000,00	1	700.000,00	1	700.000,00

Beim Bundesminister für Inneres wird eine Organisationseinheit eingerichtet, das entsprechend den Vorgaben der NIS-Richtlinie und des NIS-Gesetzes folgende Kernaufgaben erfüllen soll:

- Einrichtung und Betrieb einer zentralen Anlaufstelle (SPOC)
- Koordination der Operativen Koordinierungsstruktur (OpKoord) und deren Inneren Kreis (IKDOK)
- Einrichtung und Betrieb einer Meldesammelstelle
- Einrichtung und Betrieb eines IOC-basierten Frühwarnsystems
- Einrichtung und Betrieb bzw. Nutzung von Honeypots, Honeypot-ähnlichen-Ansätzen und Sinkholes
- Überprüfung der Sicherheitsvorkehrungen und die Einhaltung der Meldepflicht
- Cyberkrisenmanagement.

Um den Anforderungen gerecht zu werden, müssen auch hochwertige technische Systeme eingerichtet und betrieben sowie Prozesse innerhalb der Behörde abgebildet werden. Funktionell wird das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung mit diesen Kernaufgaben betraut. Die betrieblichen Sachaufwendungen sind in der Einrichtungsphase höher angesetzt und setzen sich in den Folgejahren insbesondere aus Betriebs-, Material- und Mietkosten zusammen.

Laufende Auswirkungen – Werkleistungen

Körperschaft (Angaben in €)	2019	2020	2021	2022
Bund	200.000,00	250.000,00	450.000,00	800.000,00

		2019		2020		2021		2022	
Bezeichnung	Körpersch.	Menge	Aufw. (€)	Menge	Aufw. (€)	Menge	Aufw. (€)	Menge	Aufw. (€)
IOC-basiertes Frühwarnsystem BMI	Bund	1	150.000,00	1	200.000,00	1	250.000,00	1	300.000,00
IOC-Lizenzen BMI	Bund	1	50.000,00	1	50.000,00	1	200.000,00	1	500.000,00

Für das BMI ergeben sich jährliche Werkleistungen von Dritten für die Einrichtung und den Betrieb des IOC-basierten Frühwarnsystems, die die Bereiche Software-Support/Wartung, Software-Customizations, Hardware-Support der IKT-Lösungen und IT-Beratung ergeben. Die Höhe der Aufwände für den Hardware-Support der IKT-Lösungen ist dabei von der Anzahl der betriebenen IKT-Lösungen abhängig und daher dem Szenario des IOC-basierten Frühwarnsystems mit Probe- und Vollbetrieb angepasst. Zu den Werkleistungen sind auch die Kosten für die IOC-Lizenzen zu zählen, deren Höhe auch mit dem Szenario korreliert.

Laufende Auswirkungen – Investitionen

Vermögens-, Finanzierungs- und Ergebnishaushalt

in Tsd. €	2019	2020	2021	2022
Anschaffungswert	406	1.226	160	400
Auszahlung	406	1.226	160	400
Abschreibung	13	185	205	255

Ansch.dat.	Bezeichnung	Anlagentyp	Körperschaft	ND	Menge	Anschaffungskosten €	Gesamt €
01.02.2019	Systemsoftware für den	Software (aus Kauf	Bund	0	1	300.000,00	300.000,00

	Betrieb des IOC-basierten Frühwarnsystems BMI	oder Lizenz)					
01.02.2019	Server für den Betrieb des IOC-basierten Frühwarnsystems BMI	Großrechensysteme, Server-, Netzwerk- und Kommunikationssysteme einschließlich der erforderlichen Komponenten	Bund	7	1	26.000,00	26.000,00
01.01.2020	Server für den Betrieb des IOC-basierten Frühwarnsystems BMI	Großrechensysteme, Server-, Netzwerk- und Kommunikationssysteme einschließlich der erforderlichen Komponenten	Bund	7	1	26.000,00	26.000,00
01.01.2020	Key-Management-System für das IOC-basierte Frühwarnsystem BMI	Großrechensysteme, Server-, Netzwerk- und Kommunikationssysteme einschließlich der erforderlichen Komponenten	Bund	7	1	300.000,00	300.000,00
02.02.2019	Technische Einrichtung für das IOC-basierten Frühwarnsystems BMI	Sonstige elektronische Maschinen und Büromaschinen, Postabfertigungsmaschinen	Bund	8	2	40.000,00	80.000,00
01.01.2020	Technische Einrichtung für das IOC-basierte Frühwarnsystem BMI	Sonstige elektronische Maschinen und Büromaschinen, Postabfertigungsmaschinen	Bund	8	5	40.000,00	200.000,00
01.01.2021	Technische Einrichtung für das IOC-basierte Frühwarnsystem BMI	Sonstige elektronische Maschinen und Büromaschinen, Postabfertigungsmaschinen	Bund	8	4	40.000,00	160.000,00
01.01.2022	Technische Einrichtung für das IOC-basierte	Sonstige elektronische Maschinen und	Bund	8	10	40.000,00	400.000,00

	Frühwarnsystem BMI	Büromaschinen, Postabfertigungsmaschinen					
01.01.2020	Krypto-System für das IOC-basierte Frühwarnsystem BMI	Großrechensysteme, Server-, Netzwerk- und Kommunikationssysteme einschließlich der erforderlichen Komponenten	Bund	7	1	700.000,00	700.000,00

Die Investitionen des BMI beziehen sich auf die Einrichtung und den Betrieb des IOC-basierten Frühwarnsystems. Die Berechnung basiert auf dem derzeitigen Szenario, das einen Probebetrieb des IOC-basierten Frühwarnsystems 2019 und einen Vollbetrieb spätestens 2021 vorsieht. Dementsprechend erhöht sich die Anschaffung der IKT-Lösungen laufend. Für das IOC-basierte Frühwarnsystem sind eine zentrale Betriebssoftware für die Steuerung des Systems, das mit 2 Servern betrieben werden soll, sowie ein Key-Management-System für mögliche Akkreditierungen im Bereich der Informationssicherheit erforderlich. Um den Betrieb mit klassifizierten und nicht-klassifizierten IOCs gewährleisten zu können, bedarf es eines Verschlüsselungssystems bzw. Krypto-Systems, das für den Vollbetrieb des IOC-basierten Frühwarnsystem notwendig ist.

Es ist hinzuweisen, dass es sich um ein Szenario mit Schätzwerten handelt, da eine genaue Festsetzung der Kosten nach derzeitigem Stand nicht möglich ist.

Laufende Auswirkungen – Erträge aus der op. Verwaltungstätigkeit und Transfers

Es ist ein Kostenersatz der Teilnehmer am IOC-basierten Frühwarnsystem des BMI angedacht, der aus derzeitiger Sicht nicht betraglich festgemacht werden kann, da dieser von mehreren Faktoren abhängt.

Detaillierte Darstellung der Berechnung der Verwaltungskosten für Unternehmen

Informationsverpflichtung 1	Fundstelle	Art	Ursprung	Verwaltungslasten (in €)
Meldung von Sicherheitsvorfällen an das zuständige Computer-Notfallteam	§ 19 Abs. 1 und § 21 Abs. 2	neue IVP	Europäisch	40.810

Begründung für die Schaffung/Änderung der Informationsverpflichtung: Betreiber wesentlicher Dienste und Anbieter digitaler Dienste haben Sicherheitsvorfälle unverzüglich zu melden. Die Meldung erfolgt an das jeweils zuständige Computer-Notfallteam, das ist das sektorenspezifische Computer-Notfallteam, sofern ein solches vorhanden ist und unterstützt wird, andernfalls das nationale Computer-Notfallteam.

Die Meldungen haben alle notwendigen Angaben und Informationen zum Sicherheitsvorfall zu enthalten, die es braucht, um die Lage der betroffenen Einrichtung, Erheblichkeit des Sicherheitsvorfalls generell und allfällige Auswirkungen auf andere Sektoren oder die Öffentlichkeit bewerten zu können.

Eine elektronische Umsetzung der Informationsverpflichtung ist nicht vorgesehen.

Unternehmensgruppierung 1: Betreiber wesentlicher Dienste	Zeit (hh:mm)	Gehalt/h in €	Externe Kosten	Afa	Kosten (in €)	Lasten (in €)
Verwaltungstätigkeit 1: Ausfüllen oder Eingabe von Anträgen, Meldungen, Nachweisen, Ansuchen oder Berichten bzw. Inspektionen	20:00	53	0,00	0	1.060	1.060

Unternehmensanzahl	150
Frequenz	0,25
Sowieso-Kosten in %	0

Unternehmensgruppierung 2: Anbieter digitaler Dienste	Zeit (hh:mm)	Gehalt/h in €	Externe Kosten	Afa	Kosten (in €)	Lasten (in €)
Verwaltungstätigkeit 1: Ausfüllen oder Eingabe von Anträgen, Meldungen, Nachweisen, Ansuchen oder Berichten bzw. Inspektionen	20:00	53	0,00	0	1.060	1.060

Fallzahl	1
Sowieso-Kosten in %	0

Informationsverpflichtung 2	Fundstelle	Art	Ursprung	Verwaltungslasten (in €)
Nachweis über die getroffenen Sicherheitsvorkehrungen	§ 17 Abs. 3 und § 21 Abs. 4	neue IVP	Europäisch	601.920

Begründung für die Schaffung/Änderung der Informationsverpflichtung: Der Gesetzentwurf sieht vor, dass die Einhaltung der Sicherheitsvorkehrungen periodisch zu überprüfen ist. Dafür haben die betroffenen Betreiber wesentlicher Dienste dem Bundesminister für Inneres die Erfüllung der Anforderungen in geeigneter Weise nachzuweisen. Hiefür sollen insbesondere eine Aufstellung der vorhandenen Sicherheitsvorkehrungen sowie ein Nachweis von Zertifizierungen oder durchgeführten Überprüfungen durch qualifizierte Stellen erbracht werden. Anbieter digitaler Dienste haben einen solchen Nachweis nur im Anlassfall zu erbringen.

Eine elektronische Umsetzung der Informationsverpflichtung ist nicht vorgesehen.

Unternehmensgruppierung 1:	Zeit	Gehalt/h	Externe	Afa	Kosten	Lasten (in

Betreiber wesentlicher Dienste	(hh:mm)	in €	Kosten		(in €)	€)
Verwaltungstätigkeit 1: Kommunikation, Training von Mitarbeitern	100:00	53	0,00	0	5.300	5.300
Verwaltungstätigkeit 2: Externe Gutachten	40:00	53	0,00	0	2.120	2.120
Verwaltungstätigkeit 3: Ausfüllen oder Eingabe von Anträgen, Meldungen, Nachweisen, Ansuchen oder Berichten bzw. Inspektionen	20:00	53	0,00	0	1.060	1.060
Verwaltungstätigkeit 4: Erläuterungen erstellen	80:00	46	0,00	0	3.680	3.680

Unternehmensanzahl	150
Frequenz	0,33
Sowieso-Kosten in %	0

Unternehmensgruppierung 2: Anbieter digitaler Dienste	Zeit (hh:mm)	Gehalt/h in €	Externe Kosten	Afa	Kosten (in €)	Lasten (in €)
Verwaltungstätigkeit 1: Externe Gutachten	40:00	53	0,00	0	2.120	2.120
Verwaltungstätigkeit 2: Ausfüllen oder Eingabe von Anträgen, Meldungen, Nachweisen, Ansuchen oder Berichten bzw. Inspektionen	20:00	53	0,00	0	1.060	1.060
Verwaltungstätigkeit 3: Erläuterungen erstellen	80:00	53	0,00	0	4.240	4.240
Verwaltungstätigkeit 4: Kommunikation, Training von Mitarbeitern	100:00	53	0,00	0	5.300	5.300

Angaben zur Wesentlichkeit

Nach Einschätzung der einbringenden Stelle sind folgende Wirkungsdimensionen vom gegenständlichen Vorhaben nicht wesentlich betroffen im Sinne der Anlage 1 der WFA-Grundsatzverordnung.

Wirkungs-dimension	Subdimension der Wirkungsdimension	Wesentlichkeitskriterium
Unternehmen	Finanzielle Auswirkungen auf Unternehmen	Mindestens 10 000 betroffene Unternehmen oder 2,5 Mio. € Gesamtbe- bzw. entlastung pro Jahr
Unternehmen	Auswirkungen auf die Phasen des Unternehmenszyklus	Mindestens 500 betroffene Unternehmen

Diese Folgenabschätzung wurde mit der Version 5.4 des WFA – Tools erstellt (Hash-ID: 764099778).

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2018-11-21T14:57:57+01:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	