Vorblatt

Ziele

Ziel 1: Optimierte Rahmenbedingungen für ein hohes Cybersicherheitsniveau in Österreich
Ziel 2: Synergieeffekte innerhalb der zivilen staatlichen Cybersicherheits-Strukturen in Österreich
Ziel 3: Schutz und Prävention gegenüber Angriffen auf Netz- und Informationssysteme in Österreich

Inhalt

Das Vorhaben umfasst hauptsächlich folgende Maßnahmen:

Maßnahme 1: Errichtung eines nationalen Cybersicherheitszentrums (NCSZ) zur Bündelung der Kompetenzen
Maßnahme 2: Umsetzung und Durchführung von Unionsrechtsakten im Bereich der Cybersicherheit
Maßnahme 3: Weiterentwicklung und Koordination einer neuen nationalen Cybersicherheitsstrategie
Maßnahme 4: Benennung einer zentralen Anlaufstelle für Cybersicherheit (SPOC)
Maßnahme 5: Benennung einer nationalen Behörde für das Management von Cybersicherheitsvorfällen großen Ausmaßes
Maßnahme 6: Benennung von Computer-Notfallteams (CSIRTs) zur Unterstützung der wesentlichen und wichtigen Einrichtungen
Maßnahme 7: Vorschriften zum Austausch von Cybersicherheitsinformationen
Maßnahme 8: Pflicht zur Setzung geeigneter Aufsichts- und Durchsetzungsmaßnahmen
Maßnahme 9: Pflicht zur Setzung geeigneter Risikomanagementmaßnahmen und Berichtspflichten
Maßnahme 10: Pflicht zur Führung eines Registers der wesentlichen und wichtigen Einrichtungen

Wesentliche Auswirkungen

Das Vorhaben hat wesentliche Auswirkungen auf folgende Wirkungsdimension(en):

Finanzielle Auswirkungen

Unternehmen

Finanzierungshaushalt für die ersten fünf Jahre:

in Tsd. €	2024	2025	2026	2027	2028
Nettofinanzierung Bund	-7.912	-32.003	-36.111	-40.036	-40.696
Nettofinanzierung Länder	0	-13.000	-8.248	-8.780	-9.039
Nettofinanzierung Gemeinden	0	0	0	0	0
Nettofinanzierung SV-Träger	0	0	0	0	0
Nettofinanzierung Gesamt	**-7.912**	**-45.003**	**-44.359**	**-48.816**	**-49.735**

Finanzielle Auswirkungen pro Maßnahme

Maßnahme (in Tsd. €)	2024	2025	2026	2027	2028

Errichtung einer Cybersicherheitsbehörde zur Bündelung der Kompetenzen (BKA)	0	-1.066	-1.066	-1.066	-1.066
Errichtung einer Cybersicherheitsbehörde zur Bündelung der Kompetenzen (BMI)	0	1.066	1.066	1.066	1.066
	0	0	0	0	0
	0	0	0	0	0
	0	0	0	0	0

Beschreibung der finanziellen Auswirkungen:

Die Kosten des Vertrags mit der Cert GmbH (459.00€ im Jahr 2023 zzgl. VPI von 6% ergeben 486.000€ für 2024) werden im Jahr 2024 noch vom BKA getragen. Ebenfalls werden die Kosten für die Inbetriebnahme des NCC in Höhe von 580.000€ (davon 298.000€ für den FFG-Vertrag, 273.000€ für Arbeitskraftüberlassungen und 9.000€ Reiskosten) im Jahr 2024 vom BKA getragen. Da im Jahr 2024 noch keine Verträge übergehen, wird dies im Jahr 2024 mit "0" dargestellt.

Somit fließen 1.066.000€ in die 1.Maßnahme "Errichtung einer Cybersicherheitsbehörde zur Bündelung der Kompetenzen". Ab 2025, mit der Übernahme der Verträge ins BMI, werden die Kosten von der UG11 getragen.

Die finanziellen Auswirkungen des Vorhabens aufseiten der Gemeinden und SV-Träger werden mit null abgeschätzt, da diese Auswirkungen zwar eintreten werden, aber zum gegenwärtigen Zeitpunkt mangels Erfahrungswerte nicht seriös abschätzbar sind.

Einnahmen auf Grund der Ausweitung des Strafrahmens:

Die finanziellen Einnahmen durch die Bezirksverwaltungsbehörden sind a priori nicht bewertbar, da es aufgrund der Änderung der Prüfsystematik, der Steigerung der Normunterworfenen und der starken Ausweitung des Strafrahmens einer belastbaren Kalkulationsgrundlage ermangelt. Eine Extrapolation aus der bisherigen Verwaltungspraxis ist zudem derzeit auch deswegen nicht möglich, da einerseits bestehende Kenngrößen nur sehr bedingt auf die neuen Regelungen umlegbar sind, andererseits unter der derzeitigen Gesetzeslage eine Rückmeldung zu tatsächlich verhängten Strafhöhen an die NIS Behörden nicht vorgesehen ist.

Verhältnis zu den Rechtsvorschriften der Europäischen Union

Das Vorhaben dient der Umsetzung einer EU-Richtlinie

Besonderheiten des Normerzeugungsverfahrens

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

Wirkungsorientierte Folgenabschätzung

NISG 2024

Einbringende Stelle:	BKA		
Titel des Vorhabens:	Bundesgesetz, mit dem ein Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024) erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden		
Vorhabensart:	Gesetz	Inkrafttreten/ Wirksamwerden:	2024
Erstellungsjahr:	2023	Letzte Aktualisierung:	4. April 2024

Beitrag zu Wirkungsziel oder Maßnahme im Bundesvoranschlag

Beitrag zu:

- Wirkungsziel: Hoher Beitrag des Bundeskanzleramts für ein friedliches, sicheres und chancengleiches Zusammenleben der Bevölkerung in Österreich (Untergliederung 10 Bundeskanzleramt - Bundesvoranschlag 2024)
- Wirkungsziel: Ausbau des hohen Niveaus der öffentlichen Ruhe, Ordnung und Sicherheit in Österreich, insbesondere durch bedarfsorientierte polizeiliche Präsenz, Verkehrsüberwachung und Schutz kritischer Infrastrukturen. (Untergliederung 11 Inneres - Bundesvoranschlag 2024)
    - Maßnahme: Stärkung der Cyber-Sicherheit
- Wirkungsziel: Sicherstellung der außen-, sicherheits-, europa- und wirtschaftspolitischen Interessen Österreichs in Europa und in der Welt. Weiterer Ausbau des Amtssitzes Wien als Hub und Konferenzort für Sicherheit und Nachhaltigkeit mit einem Schwerpunkt auf Energie, Entwicklung und Klimadiplomatie, sowie zur Stärkung der Beziehungen zu den Internationalen Organisationen. Umfassende Stärkung des internationalen Menschenrechtsschutzes, insbesondere der Rechte von Frauen und Kindern. (Untergliederung 12 Äußeres - Bundesvoranschlag 2024)
- Wirkungsziel: (Untergliederung 15 Finanzverwaltung - Bundesvoranschlag 2024)
- Wirkungsziel: (Untergliederung 42 Land- und Forstwirtschaft, Regionen und Wasserwirtschaft - Bundesvoranschlag 2024)
- Wirkungsziel: Objektive, faire und unabhängige Führung und Entscheidung von Verfahren durch Gerichte, Staatsanwaltschaften und die Datenschutzbehörde in angemessener Dauer. (Untergliederung 13 Justiz - Bundesvoranschlag 2024)
- Wirkungsziel: (Untergliederung 17 Öffentlicher Dienst und Sport - Bundesvoranschlag 2024)
- Wirkungsziel: (Untergliederung 31 Wissenschaft und Forschung - Bundesvoranschlag 2024)
- Wirkungsziel: (Untergliederung 30 Bildung - Bundesvoranschlag 2024)
- Wirkungsziel: (Untergliederung 21 Soziales und Konsumentenschutz - Bundesvoranschlag 2024)
- Wirkungsziel: (Untergliederung 20 Arbeit - Bundesvoranschlag 2024)
- Wirkungsziel: (Untergliederung 41 Mobilität - Bundesvoranschlag 2024)
- Wirkungsziel: Erhaltung und Verbesserung der Umweltqualität und der biologischen Vielfalt einschließlich der ökosystemaren Leistungen, die die Natur für Menschen und Gesellschaft

erbringt, für die Erhaltung der Lebensqualität sowie Schutz vor ionisierender Strahlung (Untergliederung 43 Klima, Umwelt und Energie - Bundesvoranschlag 2024)

- Wirkungsziel: Nachhaltige Nutzung von Ressourcen, Forcierung der Kreislaufwirtschaft, Entkoppelung des Anteils an zu beseitigenden Abfällen vom Wirtschaftswachstum (Untergliederung 43 Klima, Umwelt und Energie - Bundesvoranschlag 2024)
- Wirkungsziel: (Untergliederung 40 Wirtschaft - Bundesvoranschlag 2024)

Problemanalyse

Problemdefinition

Vor dem Hintergrund einer anhaltend steigenden Computerkriminalität sowie einer wachsenden Abhängigkeit von Staat, Wirtschaft und Gesellschaft von funktionierenden Infrastrukturen gewinnt besonders der Schutz von Netz- und Informationssystemen und der zugehörigen Dienste immer mehr an Bedeutung. Die Staaten der Europäischen Union im Allgemeinen und Österreich im Speziellen sind als hochentwickelte Wirtschaftsländer substanziell vom kontinuierlichen Funktionieren eben dieser Netz- und Informationssysteme abhängig.

Die Richtlinie (EU) 2022/2555 vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) ist am 16. Jänner 2023 in Kraft getreten und sieht eine massive Steigerung der zu beaufsichtigenden Entitäten durch Ausweitung der betroffenen Sektoren vor. Neue Sektoren sind beispielsweise die der öffentlichen Verwaltung, Abwasser, Verwaltung von IKT-Diensten, Abfallbewirtschaftung und noch einige mehr. Zudem fallen auch Einrichtungen der Landesverwaltung in den Anwendungsbereich. Das konkrete Ausmaß an betroffenen Einrichtungen wird in einem Register des nationalen Cybersicherheitszentrums (NCSZ) ersichtlich sein. Die betroffenen Einrichtungen haben sich selbst du deklarieren.

Ebenfalls sieht die NIS-2-Richtlinie eine erhebliche Ausweitung des Aufgabenspektrums der NIS-Behörden vor.

Die staatlichen Kompetenzen zu Cybersicherheit sind derzeit extrem stark fragmentiert und auf eine Vielzahl an Ressorts aufgeteilt. Diese historisch gewachsene Situation hat unter anderem problematische Auswirkungen auf folgende Themen:

- Verwaltungsoverhead: Durch die derzeitige Aufteilung auf mehrere Ministerien besteht ein Verwaltungsoverhead durch ressortübergreifende Prozesse.

- Kompetenzkonflikte: Cybersicherheit ist eine Querschnittsmaterie, die zahlreiche unterschiedliche Materien berühren kann (vgl. Luftfahrtsicherheit). Die Vergangenheit war oft geprägt von (negativen) Kompetenzkonflikten.

- Fachkräftemangel: Derzeit herrscht ein signifikanter Fachkräftemangel in den Bereichen IT-Sicherheit und Cybersicherheit. Die Fragmentierung der staatlichen Kompetenzen im Bereich der Cybersicherheit durch Führen von Parallelstrukturen verschärft dieses Problem nachhaltig.

- Umsetzung und Durchführung von EU-Rechtsakten: Die derzeitige fragmentierte Cybersicherheits-Landschaft in Österreich erschwert und verhindert teilweise eine rechtskonforme Umsetzung von EU-Rechtsakten.

Nullszenario und allfällige Alternativen

Im Falle der Nichtumsetzung der NIS-2-Richtlinie droht ein mögliches Vertragsverletzungsverfahren gemäß Art. 258 ff AEUV. Folglich findet bei Nichtumsetzung der vorgeschlagenen Maßnahmen keine Konsolidierung der staatlichen Cybersicherheits-Landschaft in Österreich statt. Die Fortführung dieser gegenwärtigen stark fragmentierten und auf eine Vielzahl an Ressorts aufgeteilten staatlichen Cybersicherheits-Landschaft führt zu einer nicht effektiven und effizierten Behandlung dieser für hochentwickelte Wirtschaftsländer so substanziellen Thematik. Dies würde zu einer Schwächung der Cybersicherheitslandschaft Österreichs führen. Alternativen gibt es keine.

Weiterführende Hinweise/Vorhandene Studien/Folgenabschätzungen

Titel	Jahr	Weblink
NIS-2-Richtlinie EU 2022/2555	2022	https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32022L2555

Interne Evaluierung

Zeitpunkt der internen Evaluierung: 2028

- Kontrolle des Rechtssetzungsaktes hinsichtlich der verfolgten Ziele (Umsetzung der Richtlinie (EU) 2022/2555)

- Allfällige Rückmeldungen der Europäischen Kommission

- Rückmeldungen aus der Praxis und allfällige Anregungen für Anpassungen

- Einholung von Datenmaterial von der NCSZ

- Programmkoordination in Form von regelmäßigen (jährlichen) Zwischenberichten mit Erhebung wesentlicher Indikatoren.

Ziele

Ziel 1: Optimierte Rahmenbedingungen für ein hohes Cybersicherheitsniveau in Österreich

Beschreibung des Ziels:

Mit dem Bundesgesetz soll ein hohes gemeinsames Cybersicherheitsniveau festgestellt werden, um das Funktionieren des Binnenmarktes zu verbessern.

Umsetzung durch:
Maßnahme 1: Errichtung eines nationalen Cybersicherheitszentrums (NCSZ) zur Bündelung der Kompetenzen
Maßnahme 2: Umsetzung und Durchführung von Unionsrechtsakten im Bereich der Cybersicherheit
Maßnahme 3: Weiterentwicklung und Koordination einer neuen nationalen Cybersicherheitsstrategie
Maßnahme 4: Benennung einer zentralen Anlaufstelle für Cybersicherheit (SPOC)
Maßnahme 5: Benennung einer nationalen Behörde für das Management von Cybersicherheitsvorfällen großen Ausmaßes
Maßnahme 6: Benennung von Computer-Notfallteams (CSIRTs) zur Unterstützung der wesentlichen und wichtigen Einrichtungen
Maßnahme 7: Vorschriften zum Austausch von Cybersicherheitsinformationen
Maßnahme 8: Pflicht zur Setzung geeigneter Aufsichts- und Durchsetzungsmaßnahmen
Maßnahme 9: Pflicht zur Setzung geeigneter Risikomanagementmaßnahmen und Berichtspflichten
Maßnahme 10: Pflicht zur Führung eines Registers der wesentlichen und wichtigen Einrichtungen

Wie sieht Erfolg aus:

Indikator 1 [Meilenstein]: Abdeckung eines größeren Teils der Wirtschaft und Gesellschaft

Ausgangszustand: 2023-08-29	Zielzustand: 2027-01-01
Mit dem derzeit geltenden NISG werden nur	Durch die Ausweitung von NIS 2 auf achtzehn

sieben Sektoren der Wirtschaft und Gesellschaft erfasst, weshalb das Cybersicherheitsniveau in Österreich aufbaufähig ist.	Sektoren wird ein umfassender Teil der Wirtschaft und Gesellschaft abgedeckt, was zu einer Erhöhung des Cybersicherheitsniveaus in Österreich beiträgt.

Indikator 2 [Meilenstein]: Nationales Koordinierungszentrum

Ausgangszustand: 2023-08-29	Zielzustand: 2027-01-01
Österreich verfügt über ein nationales Koordinierungszentrum im BKA, in welchem Generalisten tätig sind, die über kein spezifisches Fachwissen in Forschung und Technologie auf dem Gebiet der Cybersicherheit verfügen.	Österreich verfügt über ein nationales Koordinierungszentrum in der Cybersicherheitsbehörde, in welchem mindestens zwei Spezialist*innen mit Fachwissen in Forschung und Technologie auf dem Gebiet der Cybersicherheit arbeiten.

Ziel 2: Synergieeffekte innerhalb der zivilen staatlichen Cybersicherheits-Strukturen in Österreich

Beschreibung des Ziels:

Um den Anforderungen einer effektiven und effizienten Abdeckung der für hochentwickelte Wirtschaftsländer so substanziellen Thematik der Cybersicherheit gerecht zu werden, besteht das Ziel, die staatlichen, zivilen Cybersicherheits-Strukturen in Österreich nachhaltig zu konsolidieren.

Umsetzung durch:
Maßnahme 1: Errichtung eines nationalen Cybersicherheitszentrums (NCSZ) zur Bündelung der Kompetenzen
Maßnahme 2: Umsetzung und Durchführung von Unionsrechtsakten im Bereich der Cybersicherheit

Wie sieht Erfolg aus:

Indikator 1 [Meilenstein]: Ansprechpartner für Cybersicherheit

Ausgangszustand: 2023-08-29	Zielzustand: 2027-01-01
Es besteht kein einheitlicher Ansprechpartner im Bereich der Cybersicherheit.	Die Cybersicherheitsbehörde im Bundesministerium für Inneres (BMI) stellt einen Ansprechpartner im Bereich der Cybersicherheit dar.

Indikator 2 [Kennzahl]: Erhöhung Spezialist*innen

Ausgangszustand 2023: 12 Anzahl	Zielzustand 2027: 148 Anzahl
BMI Personalstatistik	

Indikator 3 [Meilenstein]: Konsolidierung staatlicher Cybersicherheits-Landschaft in Österreich

Ausgangszustand: 2023-08-29	Zielzustand: 2027-01-01
Staatliche Kompetenzen – ohne einheitlichen Ansprechpartner – zu ziviler Cybersicherheit sind derzeit auf zwei Ressorts aufgeteilt. Dies bedingt ineffiziente Prozesse, Kompetenzkonflikte und Parallelstrukturen.	Staatliche Kompetenzen zu ziviler Cybersicherheit und ein einheitlicher Ansprechpartner sind in der Cybersicherheitsbehörde im BMI. Die Prozesse wurden gebündelt und Doppelgleisigkeiten wurden bereinigt.

Ziel 3: Schutz und Prävention gegenüber Angriffen auf Netz- und Informationssysteme in Österreich

Beschreibung des Ziels:

Um den Anforderungen einer effektiven und effizienten Abdeckung des dieser für hochentwickelte Wirtschaftsländer so substanziellen Thematik gerecht zu werden, besteht das Ziel, die staatlichen Cybersicherheits-Landschaft in Österreich nachhaltig zu konsolidieren.

Umsetzung durch:
Maßnahme 1: Errichtung eines nationalen Cybersicherheitszentrums (NCSZ) zur Bündelung der Kompetenzen
Maßnahme 2: Umsetzung und Durchführung von Unionsrechtsakten im Bereich der Cybersicherheit
Maßnahme 3: Weiterentwicklung und Koordination einer neuen nationalen Cybersicherheitsstrategie
Maßnahme 4: Benennung einer zentralen Anlaufstelle für Cybersicherheit (SPOC)
Maßnahme 5: Benennung einer nationalen Behörde für das Management von Cybersicherheitsvorfällen großen Ausmaßes
Maßnahme 6: Benennung von Computer-Notfallteams (CSIRTs) zur Unterstützung der wesentlichen und wichtigen Einrichtungen
Maßnahme 7: Vorschriften zum Austausch von Cybersicherheitsinformationen
Maßnahme 8: Pflicht zur Setzung geeigneter Aufsichts- und Durchsetzungsmaßnahmen
Maßnahme 9: Pflicht zur Setzung geeigneter Risikomanagementmaßnahmen und Berichtspflichten
Maßnahme 10: Pflicht zur Führung eines Registers der wesentlichen und wichtigen Einrichtungen

Wie sieht Erfolg aus:

Indikator 1 [Kennzahl]: Pool an geeigneten Fachkräften

Ausgangszustand 2023: 12 Anzahl	Zielzustand 2027: 63 Anzahl

BMI Personalstatistik

Maßnahmen

Maßnahme 1: Errichtung eines nationalen Cybersicherheitszentrums (NCSZ) zur Bündelung der Kompetenzen

Beschreibung der Maßnahme:

Zur Umsetzung der Ziele 1, 2 und 3 und 4 ist es erforderlich, ein nationales Cybersicherheitszentrum zu schaffen. Dies umfasst die Bündelung der staatlichen Kompetenz im Bereich der zivilen Cybersicherheit aus mehreren Ressorts (insb. BKA und BMI) in einer Organisationseinheit (Cybersicherheitsbehörde im BMI).

Umsetzung von:
Ziel 1: Optimierte Rahmenbedingungen für ein hohes Cybersicherheitsniveau in Österreich
Ziel 2: Synergieeffekte innerhalb der zivilen staatlichen Cybersicherheits-Strukturen in Österreich
Ziel 3: Schutz und Prävention gegenüber Angriffen auf Netz- und Informationssysteme in Österreich

Maßnahme 2: Umsetzung und Durchführung von Unionsrechtsakten im Bereich der Cybersicherheit

Beschreibung der Maßnahme:

Das nationale Cybersicherheitszentrum muss fristgerecht eine Reihe von verbindlichen EU-Rechtsakten im Bereich der Cybersicherheit umsetzen bzw. durchführen. Dazu gehören insbesondere die Verordnung (EU) 2021/887.

Umsetzung von:
Ziel 1: Optimierte Rahmenbedingungen für ein hohes Cybersicherheitsniveau in Österreich
Ziel 2: Synergieeffekte innerhalb der zivilen staatlichen Cybersicherheits-Strukturen in Österreich
Ziel 3: Schutz und Prävention gegenüber Angriffen auf Netz- und Informationssysteme in Österreich

Maßnahme 3: Weiterentwicklung und Koordination einer neuen nationalen Cybersicherheitsstrategie

Beschreibung der Maßnahme:

Die Österreichische Strategie für Cybersicherheit (ÖSCS) aus dem Jahr 2021 bildet den strategischen Rahmen für die nationale Cybersicherheitspolitik und dient der langfristigen Schaffung eines sicheren Cyberraumes als Beitrag zur Steigerung der Resilienz Österreichs und der Europäischen Union durch einen gesamtstaatlichen Ansatz. Die Vorgaben aus der NIS-2-RL sind nicht vollständig berücksichtigt. Auf Basis der ÖSCS wird die Strategie vor dem Hintergrund der in der NIS-2-RL genannten Aspekte weiterentwickelt und koordiniert. Neben den Vorgaben aus der NIS-2-RL sollen auch aktuelle Entwicklungen und Bedrohungsszenarien berücksichtigt werden.

Umsetzung von:
Ziel 1: Optimierte Rahmenbedingungen für ein hohes Cybersicherheitsniveau in Österreich
Ziel 3: Schutz und Prävention gegenüber Angriffen auf Netz- und Informationssysteme in Österreich

Maßnahme 4: Benennung einer zentralen Anlaufstelle für Cybersicherheit (SPOC)

Beschreibung der Maßnahme:

Jeder Mitgliedstaat hat gemäß Art. 8 Abs. 3 NIS-2-RL eine nationale zentrale Anlaufstelle zu benennen. Die zentrale Anlaufstelle ist für die Koordinierung im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen und für die grenzüberschreitende Zusammenarbeit auf Unionsebene zuständig. Sie dient daher als Verbindungsstelle zu Behörden in anderen Mitgliedstaaten und gegebenenfalls mit der Kommission und ENISA.

Die zentrale Anlaufstelle wird im nationalen Cybersicherheitszentrum im Bundesministerium für Inneres (BMI) eingerichtet.

Umsetzung von:
Ziel 1: Optimierte Rahmenbedingungen für ein hohes Cybersicherheitsniveau in Österreich
Ziel 3: Schutz und Prävention gegenüber Angriffen auf Netz- und Informationssysteme in Österreich

Maßnahme 5: Benennung einer nationalen Behörde für das Management von Cybersicherheitsvorfällen großen Ausmaßes

Beschreibung der Maßnahme:

Jeder Mitgliedstaat hat gemäß Art. 9 Abs. 1 der NIS-2-RL eine nationale Behörde für das Management von Cyberkrisen zu benennen, welche Mittel und Verfahren im Fall eines Cybersicherheitsvorfalles großes Ausmaßes festlegen, als auch einen nationalen Plan für die Reaktion solcher.

Die Aufgaben des Managements von Cybersicherheitsvorfällen großen Ausmaßes bzw Cyberkrisen nimmt das nationale Cybersicherheitszentrum im Bundesministerium für Inneres (BMI) wahr.

Umsetzung von:
Ziel 1: Optimierte Rahmenbedingungen für ein hohes Cybersicherheitsniveau in Österreich
Ziel 3: Schutz und Prävention gegenüber Angriffen auf Netz- und Informationssysteme in Österreich

Maßnahme 6: Benennung von Computer-Notfallteams (CSIRTs) zur Unterstützung der wesentlichen und wichtigen Einrichtungen

Beschreibung der Maßnahme:

Zur Unterstützung der wesentlichen und wichtigen Einrichtungen bei der Bewältigung von Cyberbedrohungen, Schwachstellen und Cybersicherheitsvorfällen dienen die Computer-Notfallteams.

Die Computer-Notfallteams gelten als erste Anlaufstelle für alle in den Anwendungsbereich des vorliegenden Gesetzesentwurf fallende Einrichtungen.

Die wesentlichen und wichtigen Einrichtungen können sektorenspezifische CSIRTs einrichten, um das für den jeweiligen Sektor erforderliche Fachwissen abzudecken. Wurde noch kein sektorenspezifisches Computer-Notfallteam eingerichtet, fallen die im vorliegenden Gesetzesentwurf umschriebenen Aufgaben von Computer-Notfallteams dem nationalen Computer-Notfallteam zu. Das nationale Computer-Notfallteam soll – in Ermangelung eines sektorenspezifischen Computer-Notfallteams – für alle wesentliche und wichtige Einrichtungen zuständig sein und jene Aufgaben sektorenübergreifend erfüllen, die einem Computer-Notfallteam nach dem vorliegenden Gesetzesentwurf zukommen.

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

Umsetzung von:
Ziel 1: Optimierte Rahmenbedingungen für ein hohes Cybersicherheitsniveau in Österreich
Ziel 3: Schutz und Prävention gegenüber Angriffen auf Netz- und Informationssysteme in Österreich

Maßnahme 7: Vorschriften zum Austausch von Cybersicherheitsinformationen

Beschreibung der Maßnahme:

Wesentliche und wichtige Einrichtungen und Einrichtungen, die nicht in den Anwendungsbereich dieses Bundesgesetzes fallen, können einander auf freiwilliger Basis einander relevante Cybersicherheitsinformationen übermitteln.

Das nationale Cybersicherheitszentrum unterstützt die Einrichtungen bei der Ausarbeitung von Vereinbarungen eines Informationsaustausches.

Umsetzung von:
Ziel 1: Optimierte Rahmenbedingungen für ein hohes Cybersicherheitsniveau in Österreich
Ziel 3: Schutz und Prävention gegenüber Angriffen auf Netz- und Informationssysteme in Österreich

Maßnahme 8: Pflicht zur Setzung geeigneter Aufsichts- und Durchsetzungsmaßnahmen

Beschreibung der Maßnahme:

Dem nationalen Cybersicherheitszentrum obliegt die Wahrnehmung der Aufsicht in Bezug auf wesentliche und wichtige Einrichtungen und kann entsprechende Durchsetzungsmaßnahmen setzen.

Umsetzung von:
Ziel 1: Optimierte Rahmenbedingungen für ein hohes Cybersicherheitsniveau in Österreich
Ziel 3: Schutz und Prävention gegenüber Angriffen auf Netz- und Informationssysteme in Österreich

Maßnahme 9: Pflicht zur Setzung geeigneter Risikomanagementmaßnahmen und Berichtspflichten

Beschreibung der Maßnahme:

Wesentliche und wichtige Einrichtungen haben geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen zu ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme zu beherrschen und die Auswirkungen von Sicherheitsvorfälle zu verhindern oder möglichst gering zu halten.

Darüber hinaus haben wesentliche und wichtige Einrichtungen erhebliche Sicherheitsvorfälle unverzüglich an das für sie zuständige CSIRT, andernfalls dem nationalen CSIRT, zu melden.

Umsetzung von:
Ziel 1: Optimierte Rahmenbedingungen für ein hohes Cybersicherheitsniveau in Österreich
Ziel 3: Schutz und Prävention gegenüber Angriffen auf Netz- und Informationssysteme in Österreich

Maßnahme 10: Pflicht zur Führung eines Registers der wesentlichen und wichtigen Einrichtungen

Beschreibung der Maßnahme:

Das nationale Cybersicherheitszentrum führt ein Register der wesentlichen und wichtigen Einrichtungen sowie der Einrichtungen, die Domänennamen-Registrierungsdienste erbringen.

Mit Verordnung durch den Bundesminister für Inneres werden die Details zur Registrierung näher konkretisiert.

Umsetzung von:
Ziel 1: Optimierte Rahmenbedingungen für ein hohes Cybersicherheitsniveau in Österreich
Ziel 3: Schutz und Prävention gegenüber Angriffen auf Netz- und Informationssysteme in Österreich

Abschätzung der Auswirkungen

Finanzielle Auswirkungen auf den Bundeshaushalt und andere öffentliche Haushalte

Ergebnishaushalt – Gesamt für die ersten fünf Jahre (in Tsd. €)

Angaben über die ersten 5 Jahre hinausgehend finden sich im Anhang.

in Tsd. €	Summe	2024	2025	2026	2027	2028
Erträge	**3.600**	**0**	**0**	**0**	**1.800**	**1.800**
davon Bund	3.600	0	0	0	1.800	1.800
davon Länder	0	0	0	0	0	0
davon Gemeinden	0	0	0	0	0	0
davon SV-Träger	0	0	0	0	0	0
Aufwendungen	**199.357**	**7.726**	**44.859**	**44.456**	**50.717**	**51.599**
davon Bund	160.290	7.726	31.859	36.208	41.937	42.560
davon Länder	39.067	0	13.000	8.248	8.780	9.039
davon Gemeinden	0	0	0	0	0	0
davon SV-Träger	0	0	0	0	0	0
Nettoergebnis	**-195.757**	**-7.726**	**-44.859**	**-44.456**	**-48.917**	**-49.799**
davon Bund	-156.690	-7.726	-31.859	-36.208	-40.137	-40.760
davon Länder	-39.067	0	-13.000	-8.248	-8.780	-9.039
davon Gemeinden	0	0	0	0	0	0
davon SV-Träger	0	0	0	0	0	0

Finanzierungshaushalt – Gesamt für die ersten fünf Jahre (in Tsd. €)

Angaben über die ersten 5 Jahre hinausgehend finden sich im Anhang.

in Tsd. €	Summe	2024	2025	2026	2027	2028
Einzahlungen	**3.600**	**0**	**0**	**0**	**1.800**	**1.800**
davon Bund	3.600	0	0	0	1.800	1.800
davon Länder	0	0	0	0	0	0
davon Gemeinden	0	0	0	0	0	0
davon SV-Träger	0	0	0	0	0	0
Auszahlungen	**199.425**	**7.912**	**45.003**	**44.359**	**50.616**	**51.535**
davon Bund	160.358	7.912	32.003	36.111	41.836	42.496
davon Länder	39.067	0	13.000	8.248	8.780	9.039
davon Gemeinden	0	0	0	0	0	0
davon SV-Träger	0	0	0	0	0	0
Nettofinanzierung	**-195.825**	**-7.912**	**-45.003**	**-44.359**	**-48.816**	**-49.735**
davon Bund	-156.758	-7.912	-32.003	-36.111	-40.036	-40.696
davon Länder	-39.067	0	-13.000	-8.248	-8.780	-9.039
davon Gemeinden	0	0	0	0	0	0
davon SV-Träger	0	0	0	0	0	0

Es wird darauf hingewiesen, dass die Zusatzkosten der Länder bzw. der öffentlichen Verwaltung nicht erst aus diesem Bundesgesetz sondern bereits aus der NIS 2 EU-Richtlinie resultieren.

Finanzielle Auswirkungen pro Maßnahme

Maßnahme (in Tsd. €)	2024	2025	2026	2027	2028
Errichtung einer Cybersicherheitsbehörde zur Bündelung der Kompetenzen (BKA)	0	-1.066	-1.066	-1.066	-1.066
Errichtung einer Cybersicherheitsbehörde zur Bündelung der Kompetenzen (BMI)	0	1.066	1.066	1.066	1.066
	0	0	0	0	0
	0	0	0	0	0
	0	0	0	0	0

Beschreibung der finanziellen Auswirkungen:

Die Kosten des Vertrags mit der Cert GmbH (459.00€ im Jahr 2023 zzgl. VPI von 6% ergeben 486.000€ für 2024) werden im Jahr 2024 noch vom BKA getragen. Ebenfalls werden die Kosten für die Inbetriebnahme des NCC in Höhe von 580.000€ (davon 298.000€ für den FFG-Vertrag, 273.000€ für Arbeitskraftüberlassungen und 9.000€ Reiskosten) im Jahr 2024 vom BKA getragen. Da im Jahr 2024 noch keine Verträge übergehen, wird dies im Jahr 2024 mit "0" dargestellt.

Somit fließen 1.066.000€ in die 1.Maßnahme "Errichtung einer Cybersicherheitsbehörde zur Bündelung der Kompetenzen". Ab 2025, mit der Übernahme der Verträge ins BMI, werden die Kosten von der UG11 getragen.

Die finanziellen Auswirkungen des Vorhabens aufseiten der Gemeinden und SV-Träger werden mit null abgeschätzt, da diese Auswirkungen zwar eintreten werden, aber zum gegenwärtigen Zeitpunkt mangels Erfahrungswerte nicht seriös abschätzbar sind.

Einnahmen auf Grund der Ausweitung des Strafrahmens:

Die finanziellen Einnahmen durch die Bezirksverwaltungsbehörden sind a priori nicht bewertbar, da es aufgrund der Änderung der Prüfsystematik, der Steigerung der Normunterworfenen und der starken Ausweitung des Strafrahmens einer belastbaren Kalkulationsgrundlage ermangelt. Eine Extrapolation aus der bisherigen Verwaltungspraxis ist zudem derzeit auch deswegen nicht möglich, da einerseits bestehende Kenngrößen nur sehr bedingt auf die neuen Regelungen umlegbar sind, andererseits unter der derzeitigen Gesetzeslage eine Rückmeldung zu tatsächlich verhängten Strafhöhen an die NIS Behörden nicht vorgesehen ist.

Unternehmen

Auswirkungen auf die Kosten- und Erlösstruktur

Betroffen sind jene Unternehmen, die eine Tätigkeit im Sinne des Anhangs I oder II der NIS-2-Richtlinie erbringen und größer als ein Kleinunternehmen sind. Es kann davon ausgegangen werden, dass die betroffenen Unternehmen alle drei Jahre mit Kosten für die Audits rechnen müssen. Mangels Erfahrungswerte sind diese und darüber hinausgehende Kosten nicht seriös abschätzbar. Es kann zudem

keine genaue Abschätzung über die Adaption der Infrastruktur der Unternehmen getroffen werden (iE: welche Mehrkosten den Unternehmen für eine NIS 2 Compliance entstehen, nachdem manche Unternehmen hinsichtlich ihrer Cybersicherheit schon sehr gut aufgestellt sind und andere nicht).

14 von 52

Anhang

Detaillierte Darstellung der finanziellen Auswirkungen

Bedeckung Bund

Finanzielle Auswirkungen auf den Bundeshaushalt (in Tsd. €)

in Tsd. €	2024	2025	2026	2027	2028
Auszahlungen/ zu bedeckender Betrag	7.912	32.003	36.111	41.836	42.496
Einsparungen / reduzierte Auszahlungen	0	0	0	0	0

Bedeckung erfolgt durch	Betroffenes Detailbudget	Aus Detailbudget	2024	2025	2026	2027	2028
gem. BFG bzw. BFRG	100101 Ressortübergreifende Vorhaben		0	-1.066	-1.066	-1.066	-1.066
gem. BFG bzw. BFRG	100102 Zentralstelle		0	648	661	673	686
gem. BFG bzw. BFRG	110305 Legistik, Wahlen und rechtliche Angelegenheiten		106	261	266	271	276
gem. BFG bzw. BFRG	110103 EU und Internationales		21	87	89	90	92
gem. BFG bzw. BFRG	110404 Direktion Digitale Services		7.652	19.746	23.639	29.283	29.672
gem. BFG bzw. BFRG	120102 Vertretungsbehörden		133	2.224	2.219	2.082	2.123
gem. BFG bzw. BFRG	130104 Datenschutzbehörde		0	231	236	240	245
gem. BFG bzw. BFRG	130207 Bundesverwaltungsgericht		0	689	703	717	731
gem. BFG bzw. BFRG	150101 Zentralstelle		0	1.021	1.042	1.062	1.084

gem. BFG bzw. BFRG	170101 Öffentl. Dienst u. Zentralstelle	0	648	661	673	686
gem. BFG bzw. BFRG	200301 Zentralstelle	0	648	661	673	686
gem. BFG bzw. BFRG	400101 Zentralstelle	0	1.202	1.225	1.249	1.275
gem. BFG bzw. BFRG	210101 Zentralstelle	0	3.059	3.120	3.182	3.245
gem. BFG bzw. BFRG	300101 Zentralstelle	0	684	698	711	726
gem. BFG bzw. BFRG	310101 Zentralstelle und Serviceeinrichtungen	0	584	594	607	619
gem. BFG bzw. BFRG	410101 Zentralstelle	0	324	330	336	343
gem. BFG bzw. BFRG	430201 Umwelt und Kreislaufwirtschaft	0	324	331	337	343
gem. BFG bzw. BFRG	420401 Zentralstelle	0	689	702	716	730

Erläuterung zur Bedeckung:

Die budgetäre Bedeckung ist im geltenden Bundesfinanzrahmengesetz 2024-2027 sichergestellt und wird in den zukünftigen Bundesfinanzrahmengesetzen sichergestellt werden.

ad 2024: Die Kosten der Verträge mit der Cert GmbH (459.000€ im Jahr 2023 zzgl. VPI von 6% ergeben 486.000€ für 2024) und betr. NCC-FFG (580.000€) werden zu Lasten der UG 10 bedeckt.

ad 2025 ff: Die Kosten der Verträge mit der Cert GmbH (486.000€) und betr. NCC-FFG (580.000€) werden zu Lasten der UG 11 bedeckt (DB 11.04.04.00)

Personalaufwand

in Tsd. €	2024	2025	2026	2027	2028

16 von 52

Körperschaft	Aufwand	VBÄ	Aufwand	VBÄ	Aufwand	VBÄ	Aufwand	VBÄ	Aufwand	VBÄ
Bund	2.413		19.506		23.567		24.027		24.508	
Länder										
Gemeinden										
Sozialversicherungsträger										
GESAMTSUMME	2.413		19.506		23.567		24.027		24.508	

Es wird darauf hingewiesen, dass der Personalaufwand gem. der WFA-Finanzielle-Auswirkungen-Verordnung valorisiert wird.

Maßnahme / Leistung	Körperschaft	Verwendungs-gruppe	2024		2025		2026		2027		2028	
			Fallzahl	Zeit (h)	Fallzahl	Zeit (h)	Fallzahl	Zeit (h)	Fallzahl	Zeit (h)	Fallzahl	Zeit (h)
GL + stv. GL ab Juni	Bund	VB-VD-Höh. Dienst 1 v1/5-v1/7	2	980,00								
Büroleiter und RL ab August	Bund	VB-VD-Höh. Dienst 2 v1/4	4	700,00								
AL NCSZ/17 ab Juni	Bund	VB-VD-Höh. Dienst 1 v1/5-v1/7	1	980,00								
V1 Legistik ab August	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	3	700,00								
NCSZ/a V1 ab Oktober	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	5	420,00								
NCSZ/b V1 ab Oktober	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	1	420,00								
NCSZ/c V1 ab Oktober	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	2	420,00								
NCSZ/15/b V1 ab Oktober	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	3	420,00								
NCSZ/17/a V1 ab November	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3;	3	280,00								

		a				
NCSZ/17/b V1 ab November	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	4	280,00		
NCSZ/17/c V1 ab November	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	2	280,00		
NCSZ/a V2 ab Oktober	Bund	VB-VD-Gehob. Dienst2 v2/4	3	420,00		
NCSZ/b V2 ab Oktober	Bund	VB-VD-Gehob. Dienst2 v2/4	1	420,00		
NCSZ/c V2 ab Oktober	Bund	VB-VD-Gehob. Dienst2 v2/4	2	840,00		
NCSZ/15/a V2 ab November	Bund	VB-VD-Gehob. Dienst2 v2/4	1	280,00		
NCSZ/17/c V2 ab November	Bund	VB-VD-Gehob. Dienst2 v2/4	1	280,00		
NCSZ/SEKR V3 ab Oktober	Bund	VB-VD-Fachdienst v3; c; h1, p1	2	420,00		
NCSZ/15/a V3 ab Oktober	Bund	VB-VD-Fachdienst v3; c; h1, p1	1	420,00		
Cyberattache ab Oktober	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	1	420,00		
NCSZ/a V1 ab April	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a			2	1.260,00
NCSZ/b V1 ab April	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a			1	1.260,00
NCSZ/c V1 ab April	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a			1	1.260,00
NCSZ/14/a V1 ab April	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a			2	1.260,00

18 von 52

NCSZ/14/b V1 ab Oktober	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	1	420,00	2	420,00					
NCSZ/15/a V1 ab Oktober	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	2	420,00	3	420,00					
NCSZ/17/a V1 ab Oktober	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a			1	420,00					
NCSZ/17/b V1 ab Oktober	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a			5	420,00					
NCSZ/17/c V1 ab Oktober	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a			3	420,00					
NCSZ/a V2 ab April	Bund	VB-VD-Gehob. Dienst2 v2/4			2	1.260,00					
NCSZ/b V2 ab April	Bund	VB-VD-Gehob. Dienst2 v2/4			3	1.260,00					
NCSZ/c V2 ab April	Bund	VB-VD-Gehob. Dienst2 v2/4			1	1.260,00					
NCSZ/15/a V2 ab oktober	Bund	VB-VD-Gehob. Dienst2 v2/4			2	420,00					
NCSZ/15/b V2 ab Oktober	Bund	VB-VD-Gehob. Dienst2 v2/4			2	420,00					
NCSZ/17/c V2 ab Oktober	Bund	VB-VD-Gehob. Dienst2 v2/4			1	420,00					
NCSZ/SEKR V3 ab April	Bund	VB-VD-Fachdienst v3; c; h1, p1			2	1.260,00					
GL + stv. GL	Bund	VB-VD-Höh. Dienst 1 v1/5-v1/7			2	1.680,00	2	1.680,00	2	1.680,00	2	1.680,00
Büroleiter und RL	Bund	VB-VD-Höh. Dienst 2 v1/4			4	1.680,00	4	1.680,00	4	1.680,00	4	1.680,00
AL NCSZ/17	Bund	VB-VD-Höh. Dienst 1 v1/5-v1/7			1	1.680,00	1	1.680,00	1	1.680,00	1	1.680,00
V1 Legistik	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a			3	1.680,00	3	1.680,00	3	1.680,00	3	1.680,00

NCSZ/a V1	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	5	1.680,00	7	1.680,00	7	1.680,00	7	1.680,00
NCSZ/b V1	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	1	1.680,00	2	1.680,00	2	1.680,00	2	1.680,00
NCSZ/c V1	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	2	1.680,00	3	1.680,00	3	1.680,00	3	1.680,00
NCSZ/14/a V1	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a			2	1.680,00	2	1.680,00	2	1.680,00
NCSZ/14/b V1	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	1	1.680,00	3	1.680,00	3	1.680,00	3	1.680,00
NCSZ/15/a V1	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	2	1.680,00	5	1.680,00	5	1.680,00	5	1.680,00
NCSZ/15/b V1	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	3	1.680,00	3	1.680,00	3	1.680,00	3	1.680,00
NCSZ/17/a V1	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	3	1.680,00	4	1.680,00	4	1.680,00	4	1.680,00
NCSZ/17/b V1	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	4	1.680,00	9	1.680,00	9	1.680,00	9	1.680,00
NCSZ/17/c V1	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	2	1.680,00	5	1.680,00	5	1.680,00	5	1.680,00
NCSZ/a V2	Bund	VB-VD-Gehob. Dienst2 v2/4	3	1.680,00	5	1.680,00	5	1.680,00	5	1.680,00
NCSZ/b V2	Bund	VB-VD-Gehob. Dienst2 v2/4	1	1.680,00	4	1.680,00	4	1.680,00	4	1.680,00
NCSZ/c V2	Bund	VB-VD-Gehob. Dienst2 v2/4	2	1.680,00	3	1.680,00	3	1.680,00	3	1.680,00
NCSZ/15/a V2	Bund	VB-VD-Gehob. Dienst2 v2/4	1	1.680,00	3	1.680,00	3	1.680,00	3	1.680,00
NCSZ/15/b V2	Bund	VB-VD-Gehob.			2	1.680,00	2	1.680,00	2	1.680,00

20 von 52

		Dienst2 v2/4								
NCSZ/17/c V2	Bund	VB-VD-Gehob. Dienst2 v2/4	1	1.680,00	2	1.680,00	2	1.680,00	2	1.680,00
NCSZ/SEKR V3	Bund	VB-VD-Fachdienst v3; c; h1, p1	2	1.680,00	4	1.680,00	4	1.680,00	4	1.680,00
NCSZ/15/a V3	Bund	VB-VD-Fachdienst v3; c; h1, p1	1	1.680,00	1	1.680,00	1	1.680,00	1	1.680,00
Cyberattache	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	1	1.680,00	1	1.680,00	1	1.680,00	1	1.680,00
BMJ DSB	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	1	1.680,00	1	1.680,00	1	1.680,00	1	1.680,00
BMJ DSB	Bund	VB-VD-Gehob. Dienst2 v2/4	2	1.680,00	2	1.680,00	2	1.680,00	2	1.680,00
BMJ BVwG	Bund	RS-Höh. Dienst 3 R 1a, R 1b, St 1; Ri I, Sta I; Richter d.BG/GH1; Staatsanw.	3	1.680,00	3	1.680,00	3	1.680,00	3	1.680,00
BMJ BVwG	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	2	1.680,00	2	1.680,00	2	1.680,00	2	1.680,00
BMJ BVwG	Bund	VB-VD-Gehob. Dienst2 v2/4	2	1.680,00	2	1.680,00	2	1.680,00	2	1.680,00
BMF Leiter	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	1	1.680,00	1	1.680,00	1	1.680,00	1	1.680,00
BMF Cyberreferent	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	5	1.680,00	5	1.680,00	5	1.680,00	5	1.680,00
BMKÖS Leiter	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	1	1.680,00	1	1.680,00	1	1.680,00	1	1.680,00
BMKÖS Cyberreferent	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	3	1.680,00	3	1.680,00	3	1.680,00	3	1.680,00

BML Cyberreferent	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	3	1.680,00	3	1.680,00	3	1.680,00	3	1.680,00
BMK Leiter	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	1	1.680,00	1	1.680,00	1	1.680,00	1	1.680,00
BMK Cyberreferent	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	3	1.680,00	3	1.680,00	3	1.680,00	3	1.680,00
BMAW Leiter UG20	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	1	1.680,00	1	1.680,00	1	1.680,00	1	1.680,00
BMAW Cyberreferent UG20	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	3	1.680,00	3	1.680,00	3	1.680,00	3	1.680,00
BKA Leiter	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	1	1.680,00	1	1.680,00	1	1.680,00	1	1.680,00
BKA Cyberreferent	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	3	1.680,00	3	1.680,00	3	1.680,00	3	1.680,00
BMSGPK	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	1	1.680,00	1	1.680,00	1	1.680,00	1	1.680,00
BMEIA 1*CISO	Bund	VB-VD-Höh. Dienst 2 v1/4	1	1.680,00	1	1.680,00	1	1.680,00	1	1.680,00
BMEIA 2*ISMS-Refernet:innen	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	2	1.680,00	2	1.680,00	2	1.680,00	2	1.680,00
BMEIA 1*operative IKT-Security	Bund	VB-VD-Gehob. Dienst1 v2/5-v2/6	1	1.680,00	1	1.680,00	1	1.680,00	1	1.680,00
BMEIA 1*Cyberbotschafter:in	Bund	VB-VD-Höh. Dienst 2 v1/4	1	1.680,00	1	1.680,00	1	1.680,00	1	1.680,00
BMEIA 1* RL Kapazitätenaufbau, Forschungsprojekte, Projekte zu Cybersicherheit und	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	1	1.680,00	1	1.680,00	1	1.680,00	1	1.680,00

22 von 52

Cyberkriminalität													
BMEIA 2*Referent:innen Cyber Außenpolitik	Bund	VB-VD-Höh. Dienst 3 v1/1-v1/3; a	2	1.680,00	2	1.680,00	2	1.680,00	2	1.680,00			

in €		2024		2025		2026		2027		2028	
Maßnahme / Leistung	Körperschaft	Anzahl	Aufwand	Anzahl	Aufwand	Anzahl	Aufwand	Anzahl	Aufwand	Anzahl	Aufwand
AL RIVIT1 ab Juli	Bund	3	71.351,56								
NCSZ/c RIVIT2 ab Oktober	Bund	1	31.352,34								
NCSZ/14/a RIVIT2 ab November	Bund	1	20.901,56								
NCSZ/14/b RIVIT2 ab November	Bund	1	20.901,56								
NCSZ/15/b RIVIT2 ab November	Bund	1	20.901,56								
NCSZ/16/a RIVIT2 ab Oktober	Bund	3	31.352,34								
NCSZ/16/b RIVIT2 ab Oktober	Bund	2	31.352,34								
NCSZ/17/a RIVIT2 ab November	Bund	1	20.901,56								
NCSZ/a RIVIT3 ab November	Bund	1	17.298,14								
NCSZ/c RIVIT3 ab November	Bund	1	17.298,14								
NCSZ/14/a RIVIT3 ab Oktober	Bund	2	25.947,21								
NCSZ/14/b RIVIT3 ab Oktober	Bund	2	25.947,21								
NCSZ/15/a RIVIT3 ab November	Bund	2	17.298,14								

NCSZ/15/b RIVIT3 ab November	Bund	2	17.298,14	
NCSZ/17/c RIVIT3 ab November	Bund	1	17.298,14	
NCSZ/16/a RIVIT4 ab Oktober	Bund	1	21.623,77	
NCSZ/16/b RIVIT4 ab Oktober	Bund	1	21.623,77	
NCSZ/c RIVIT5 ab Oktober	Bund	1	19.460,41	
NCSZ/14/a RIVIT5 ab November	Bund	3	12.973,61	
NCSZ/14/b RIVIT5 ab November	Bund	3	12.973,61	
NCSZ/17/c RIVIT5 ab November	Bund	2	12.973,61	
NCSZ/16/b RIVIT6 ab November	Bund	2	11.531,37	
NCSZ/16/a RIVIT2 ab April	Bund			1 95.938,15
NCSZ/16/b RIVIT2 ab April	Bund			1 95.938,15
NCSZ/17/a RIVIT2 ab April	Bund			1 95.938,15
NCSZ/c RIVIT3 ab April	Bund			2 79.398,47
NCSZ/14/a RIVIT3 ab April	Bund			2 79.398,47
NCSZ/14/b RIVIT3 ab April	Bund			2 79.398,47
NCSZ/15/a RIVIT3 ab April	Bund			1 79.398,47
NCSZ/15/b RIVIT3 ab Oktober	Bund			1 26.466,16
NCSZ/16/a RIVIT3 ab Oktober	Bund	2	25.947,21	2 26.466,16

NCSZ/16/b RIVIT3 ab Oktober	Bund	3	25.947,21	4	26.466,16						
NCSZ/c RIVIT4 ab April	Bund			1	66.168,74						
NCSZ/16/a RIVIT4 ab April	Bund			1	66.168,74						
NCSZ/16/b RIVIT4 ab April	Bund			3	66.168,74						
NCSZ/c RIVIT5 ab April	Bund			2	59.398,85						
NCSZ/14/a RIVIT5 ab April	Bund			4	59.398,85						
NCSZ/14/b RIVIT5 ab April	Bund			4	59.398,85						
NCSZ/15/b RIVIT5 ab Oktober	Bund	2	19.460,41	4	19.849,62						
NCSZ/16/a RIVIT5 ab Oktober	Bund	1	19.460,41	3	19.849,62						
NCSZ/16/b RIVIT5 ab Oktober	Bund	4	19.460,41	8	19.849,62						
NCSZ/15/b RIVIT6 ab April	Bund			1	52.928,97						
NCSZ/16/b RIVIT6 ab Oktober	Bund			1	17.642,99						
NCSZ/17/c RIVIT6 ab Oktober	Bund			1	17.642,99						
AL RIVIT1	Bund			3	145.557,18	3	148.468,32	3	151.437,69	3	154.466,44
NCSZ/c RIVIT2	Bund			1	127.917,53	1	130.475,88	1	133.085,40	1	135.747,11
NCSZ/14/a RIVIT2	Bund			1	127.917,53	1	130.475,88	1	133.085,40	1	135.747,11
NCSZ/14/b RIVIT2	Bund			1	127.917,53	1	130.475,88	1	133.085,40	1	135.747,11
NCSZ/15/b RIVIT2	Bund			1	127.917,53	1	130.475,88	1	133.085,40	1	135.747,11

NCSZ/16/a RIVIT2	Bund	3	127.917,53	4	130.475,88	4	133.085,40	4 135.747,11
NCSZ/16/b RIVIT2	Bund	2	127.917,53	3	130.475,88	3	133.085,40	3 135.747,11
NCSZ/17/a RIVIT2	Bund	1	127.917,53	2	130.475,88	2	133.085,40	2 135.747,11
NCSZ/a RIVIT3	Bund	1	105.864,63	1	107.981,92	1	110.141,56	1 112.344,39
NCSZ/c RIVIT3	Bund	1	105.864,63	3	107.981,92	3	110.141,56	3 112.344,39
NCSZ/14/a RIVIT3	Bund	2	105.864,63	4	107.981,92	4	110.141,56	4 112.344,39
NCSZ/14/b RIVIT3	Bund	2	105.864,63	4	107.981,92	4	110.141,56	4 112.344,39
NCSZ/15/a RIVIT3	Bund	2	105.864,63	3	107.981,92	3	110.141,56	3 112.344,39
NCSZ/15/b RIVIT3	Bund	2	105.864,63	3	107.981,92	3	110.141,56	3 112.344,39
NCSZ/16/a RIVIT3	Bund	2	105.864,63	4	107.981,92	4	110.141,56	4 112.344,39
NCSZ/16/b RIVIT3	Bund	3	105.864,63	7	107.981,92	7	110.141,56	7 112.344,39
NCSZ/17/c RIVIT3	Bund	1	105.864,63	1	107.981,92	1	110.141,56	1 112.344,39
NCSZ/c RIVIT4	Bund			1	89.989,49	1	91.789,28	1 93.625,06
NCSZ/16/a RIVIT4	Bund	1	88.224,99	2	89.989,49	2	91.789,28	2 93.625,06
NCSZ/16/b RIVIT4	Bund	1	88.224,99	4	89.989,49	4	91.789,28	4 93.625,06
NCSZ/c RIVIT5	Bund	1	79.398,47	3	80.986,44	3	82.606,17	3 84.258,30
NCSZ/14/a RIVIT5	Bund	3	79.398,47	7	80.986,44	7	82.606,17	7 84.258,30
NCSZ/14/b RIVIT5	Bund	3	79.398,47	7	80.986,44	7	82.606,17	7 84.258,30

NCSZ/15/b RIVIT5	Bund	2	79.398,47	6	80.986,44	6	82.606,17	6	84.258,30
NCSZ/16/a RIVIT5	Bund	1	79.398,47	4	80.986,44	4	82.606,17	4	84.258,30
NCSZ/16/b RIVIT5	Bund	4	79.398,47	12	80.986,44	12	82.606,17	12	84.258,30
NCSZ/17/c RIVIT5	Bund	2	79.398,47	2	80.986,44	2	82.606,17	2	84.258,30
NCSZ/15/b RIVIT6	Bund			1	71.983,40	1	73.423,07	1	74.891,53
NCSZ/16/b RIVIT6	Bund	2	70.571,96	3	71.983,40	3	73.423,07	3	74.891,53
NCSZ/17/c RIVIT6	Bund			1	71.983,40	1	73.423,07	1	74.891,53
BML CISO RIVIT 2	Bund	1	127.917,53	1	130.475,88	1	133.085,40	1	135.747,11
BMSGPK RIVIT1	Bund	1	145.557,18	1	148.468,32	1	151.437,69	1	154.466,44
BMSGPK RIVIT2	Bund	2	127.917,53	2	130.475,88	2	133.085,40	2	135.747,11
BMSGPK RIVIT3	Bund	5	105.864,63	5	107.981,92	5	110.141,56	5	112.344,39
BMSGPK RIVIT4	Bund	5	88.224,99	5	89.989,49	5	91.789,28	5	93.625,06
BMBWF RIVIT2 UG 30	Bund	3	127.917,53	3	130.475,88	3	133.085,40	3	135.747,11
BMBWF RIVIT2 UG 31	Bund	3	127.917,53	3	130.475,88	3	133.085,40	3	135.747,11
BMAW RIVIT2 UG 40.01	Bund	3	127.917,53	3	130.475,88	3	133.085,40	3	135.747,11
BMAW RIVIT3 UG 40.01	Bund	3	105.864,63	3	107.981,92	3	110.141,56	3	112.344,39

Als Basis für die Personalberechnung wird wie folgt ausgegangen:

bestehendes Personal (IV/S/2):

31 Personen

Der für NIS2 benötigte Personalzuwachs stellt sich wie folgt dar:
2024: 90 Personen
2025: 83 Personen

Personalstand pro Jahr stellt sich wie folgt dar:
Ende 2024: 121
ab Ende 2025: 204

Die Personalzuwächse nach Verwendungsgruppen stellen sich wie folgt dar:

Verwendungsgruppe	Personenanzahl
2024	
V1/5-V1/7	3 Personen
V1/4	4 Personen
V1/1-V1/3	23 Personen
V2/4	8 Personen
V3	3 Personen
Rivit1	3 Personen
Rivit2	10Personen
Rivit3	16 Personen
Rivit4	2 Personen
Rivit5	16 Personen
Rivit6	2 Personen
2025	
V1/1-V1/3	20 Personen
V2/4	11 Personen
V3	2 Personen
Rivit2	4 Personen
Rivit3	14 Personen

Rivit4	5 Personen
Rivit5	25 Personen
Rivit6	3 Personen

Abschließend wird das Nationale Cybersicherheitszentrum einen Personalstand von 204 aufweisen.

Für die legistischen Maßnahmen der Sektion III des BMI werden weiters 3 Personen berücksichtigt.

Ein Platz für einen Cyberattaché wird berücksichtigt.

Die in der WFA nicht darstellbaren RIVIT-Verwendungsgruppen wurden wie folgt berechnet:

laut GÖD Gehaltstabelle wurde ausgehend vom Einstiegsgehalt das Jahresbrutto errechnet. Anschließend wurde der errechnete Betrag um den Dienstgeberanteil erhöht. Die Folgejahre wurden jeweils mit 2 % valorisiert.

	Monat/brutto	Jahr/Brutto	Jahr/brutto+Dienstgeberanteil
RIVIT 1	7.722,03	108.108,42	142.703,11
RIVIT 2	6.786,22	95.007,08	125.409,35
RIVIT 3	5.616,28	78.627,92	103.788,85
RIVIT 4	4.680,47	65.526,58	86.495,09
RIVIT 5	4.212,21	58.970,94	77.841,64
RIVIT 6	3.743,95	52.415,30	69.188,20
RIVIT 7	2.924,85	40.947,90	54.051,23

Geplanter Aufbau der Organisation:

Das Nationale Cybersicherheitszentrum (NCSZ) innerhalb der Sektion IV beinhaltet ein

- zentrales Sekretariat
- Programmdirektion
- Büro NCSZ/a Ressourcen und Support

und gliedert sich in die Bereiche:

- Bereich: Aufsicht und Durchsetzung
- Bereich: Kooperation

Programmdirektion:
- Leitung des Programmes zur Umsetzung von „EU-Cybersicherheitspaketen“
- Wahrnehmung der Aufgaben auf nationaler und internationaler Ebene
- Selbständige Entwicklung, Planung, Koordination, Umsetzung und Kontrolle aller Programmmaßnahmen und der dazugehörigen Projekte und IT-Projekte

Der Bereich Aufsicht und Durchsetzung:
- Steuernde Tätigkeiten innerhalb des Bereiches Aufsicht und Durchsetzung
- Stellvertretung der Direktor:in der Direktion für Cybersicherheit

Der Bereich Kooperation:
- Steuernde Tätigkeiten innerhalb des Bereiches Kooperation
- Stellvertretung der Direktor:in der Direktion für Cybersicherheit

Die Tätigkeiten innerhalb der Direktion, Bereiche und Abteilungen lassen sich wie folgt zusammenfassen:

NCSZ (Nationale Cybersicherheitszentrum):
- Wahrnehmung der Aufgaben des Bundesministers für Inneres auf dem Gebiet der Cybersicherheit gemäß dem Bundesgesetz für Netz- und Informationssystemsicherheit
- Vertreter des Bundesministers für Inneres auf Executive-Ebene im europäischen "Cyber Crisis Liaison Organisations Network" (CyCLONe)
- Repräsentation des "Inneren Kreises der operativen Koordinierungsstruktur" (IKDOK) im Cyberkrisenmanagement-Koordinationsausschuss
- Leitung der Cybersicherheit Steuerungsgruppe (CSS)

Abteilung IV/NCSZ (Ressourcen und Support)
- Budget-, Organisations-, Ressourcen-, Wirtschafts- und Controlling-Angelegenheiten der Direktion, soweit diese übertragen sind

oder daran mitzuwirken ist

- Koordination des Prozessmanagements, Risikomanagements und Wissensmanagements in der Direktion
- Programmdirektion für Programme zur Umsetzung von „EU-Cybersicherheitspaketen“

Büro IV/NCSZ/a (Ressourcen und Support)

- Personalangelegenheiten der Direktion, soweit diese übertragen sind oder daran mitzuwirken ist
- Bewirtschaftung des zugewiesenen Budgets nach den Grundsätzen und Leitlinien der Sektion I
- Controlling innerhalb der Direktion
- Koordination des Prozessmanagements in der Direktion
- Projektabwicklung, -unterstützung und -controlling für alle Projekte der Direktion
- Vernetzungsmanagement
- Steuerung und Leitung des internen Strategieprozesses der Direktion
- Koordination und Leitung des Risikomanagements der Direktion
- Koordination und Leitung des Wissensmanagements der Direktion
- Allgemeine rechtliche Angelegenheiten der Direktion

Bereich Aufsicht und Durchsetzung (1. stv. Direktor:in)

Büro IV/NCSZ/b (Verfahrensführung)

- Verwaltungsverfahren nach dem NISG
- Führen von Beschwerdeverfahren
- Schnittstelle zu den Verwaltungsstrafbehörden

Abteilung IV/DCS/14 (Prüfung und Aufsicht)

Referat IV/NCSZ/14/a

(Prüfung und Aufsicht von technischen Risikomanagementmaßnahmen)

- Analyse von Prüfberichten über den Stand der technischen Risikomanagementmaßnahmen bei Normunterworfenen
- Durchführen von Prüfungen der verpflichtenden technischen Risikomanagementmaßnahmen bei den Normunterworfenen
- Ableiten von technischen Maßnahmen zur Erreichung bzw. Verbesserung der Risikomanagementmaßnahmen

Referat IV/NCSZ/14/b

(Prüfung und Aufsicht von organisatorischen Risikomanagementmaßnahmen)

- Analyse von Prüfberichten über den Stand der organisatorischen Risikomanagementmaßnahmen bei Normunterworfenen
- Durchführen von Prüfungen der verpflichtenden organisatorischen Risikomanagementmaßnahmen bei den Normunterworfenen
- Ableiten von organisatorischen Maßnahmen zur Erreichung bzw. Verbesserung der Risikomanagementmaßnahmen

Abteilung IV/NCSZ/15 (Steuerung und Zulassung)

- Aufsichtsangelegenheiten der qualifizierten Prüfer und unabhängigen Stellen und der Computernotfallteams
- Führung der Register gemäß NIS-Richtlinie
- Steuerung zur Sicherstellung eines qualitativ hochwertigen Vollzugs

Referat IV/NCSZ/15/a

(Zulassung und Kontrolle von qualifizierten Prüfern und Computernotfallteams)

- Aufsicht über qualifizierte Prüfer und unabhängige Stellen gemäß der aktuellen NIS-Richtlinie
- Aufsicht über Computernotfallteams

Referat IV/NCSZ/15/b

(Durchsetzung, Steuerung und Risikoanalysen)

- Durchsetzungsmaßnahmen in Bezug auf wesentliche und wichtige Einrichtungen
- Führung des Registers über wesentliche und wichtige Einrichtungen
- Überwachung der Einhaltung der Berichtspflichten der Normunterworfenen
- Cybersicherheitsrisikoanalysen
- Laufende Analyse von Standards, Normen, Richtlinien und Berücksichtigung des Rechtsrahmens zur Sicherstellung eines qualitativ hochwertigen Vollzugs
- Erarbeitung und Weiterentwicklung von Kriterien und Handreichungen zu den Risikomanagementmaßnahmen

Bereich Kooperation (2. stv. Direktor:in)

Büro IV/NCSZ/c (Cyberlagezentrum)

- Wahrnehmen der Aufgaben der zentralen Anlaufstelle gemäß der aktuellen NIS-Richtlinie

- Cyberlagezentrum
- Angelegenheiten des Cyberkrisenmanagements

Abteilung IV/NCSZ/16 (Unterstützung und technische Vernetzung)

- Wahrnehmung der Aufgaben des Bundesministeriums für Inneres in technischen Cybersicherheitsangelegenheiten nach dem NISG für Unterstützungsaufgaben und technische Vernetzung - soweit nicht die Zuständigkeit anderer Organisationseinheiten gegeben ist
- Leitung des Computer Emergency Response Team für die öffentliche Verwaltung- GovCERT
- Teilnahme an europäischen SOC Netzwerken auf Executive Ebene
- Technisches Innovationsmanagement der Direktion

Referat IV/NCSZ/16/a
(GovCERT – Computernotfallteam des Bundes)

- Wahrnehmen der Aufgaben des Computernotfallteams des Bundes gem. NISG
- Nationale und internationale Vernetzung mit anderen Computernotfallteams
- Mitwirkung bei der koordinierten Offenlegung von Schwachstellen

Referat IV/NCSZ/16/b
(Nationale SOC Plattform)

- Fachlicher Betrieb der technischen Einrichtungen nach dem NISG
- Fachlicher Betrieb der nationalen SOC-Plattform und des IOC basierten Frühwarnsystems
- Internationale Zusammenarbeit mit Nationalen SOC-Plattformen anderer EU-Mitgliedsstaaten
- Sicherstellen der Zurverfügungstellung von aufbereiteten Informationen an GovCERT und das Cyberlagezentrum zu weiteren Veranlassungen

Abteilung IV/NCSZ/17 (Strategie und Zusammenarbeit)

- Laufende Weiterentwicklung der österreichischen Strategie für Cybersicherheit (ÖSCS)
- Koordination und Veröffentlichung des jährlichen gesamtstaatlichen Cybersicherheitsberichts
- Leitung, Koordination und Einberufung der Cybersicherheitssteuerungsgruppe (CSS) und des CSS-Teams

- Strategische nationale Grundsatzpositionen des Bundesministeriums für Inneres zum Thema Cybersicherheit
- Strategische Leitlinien, Grundsätze und Koordination im Bereich Cybersicherheit
- Entwicklung von Vorschlägen zur Weiterentwicklung von nationalen und EU-Förderprogrammen im Bereich der Cybersicherheit
- Administration und Organisation der operativen Koordinierungsstrukturen gemäß NIS-Gesetz

Referat IV/NCSZ/17/a
(Strategie und nationale Cyberzusammenarbeit)

- Laufende Weiterentwicklung der österreichischen Strategie für Cybersicherheit (ÖSCS)
- Koordination und Veröffentlichung des jährlichen gesamtstaatlichen Cybersicherheitsberichts
- Strategische Grundsatzpositionen des Bundesministeriums für Inneres zum Thema Cybersicherheit
- Strategische Leitlinien, Grundsätze und Koordination im Bereich Cybersicherheit
- Entwicklung von Vorschlägen zur Weiterentwicklung von nationalen und EU-Förderprogrammen im Bereich der Cybersicherheit
- Administration und Organisation der operativen Koordinierungsstrukturen gemäß NIS-Gesetz
- Abstimmungen mit anderen relevanten nationalen Behörden, insb. Resilienz kritische Einrichtungen (RKE) Behörde, Datenschutzbehörde und Digital Operational Resilience Act (DORA) Behörde
- Koordination von staatlichen Cyber-Übungen
- Abstimmungen mit anderen relevanten nationalen Behörden, insb. RKE Behörde, Datenschutzbehörde, DORA Behörde und RTR
- Governance der fachlich betriebenen Systeme
- Policy Analyse von Bedrohungen, Risiken und aktuellen Trends im Bereich der Cybersicherheit, inkl. Bewertung des politischen und sicherheitspolitischen Kontextes

Referat IV/NCSZ/17/b
(EU und internationale Cyberangelegenheiten)

- Vertretung in europäischen Cybersicherheitsgremien
- Vertretung in internationalen Cybersicherheitsgremien (insb UN, GFCE etc)
- Strategische Planung, Grundsatzpositionierung in EU-Angelegenheiten im Bereich Cybersicherheit
- Vorbereitung und Organisation von internationalen Expertentreffen im In- und Ausland im Bereich Cybersicherheit
- Teilnahme an und Koordination von Peer Reviews gemäß der aktuellen NIS-Richtline

34 von 52

Referat IV/NCSZ/17/c

(Nationales Cyberkoordinationszentrum (NCC) und öffentlich-private Zusammenarbeit)

- Wahrnehmung der Aufgaben des Nationalen Cyberkoordinierungszentrums (NCC) gem. VERORDNUNG (EU) 2021/887 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren
- Awareness
- CSP, PPP
- Koordination von staatlichen Cyber-Übungen

Ergebnis der Ressourcenanalyse bzgl. der Ressorts:

Die Ressorts wurden entsprechend der Rückmeldungen in 2 Gruppen eingeteilt,

1. Flächen-Ressorts (BMBWF, BMSGPK, BMEIA, BMF, BMAW VerwB Wirtschaft UG40)

Flächen-Ressorts haben eine überproportionale Anzahl an Bediensteten und viele nachgeordnete Dienststellen bzw. Außenstellen.

2. Nicht-Flächen-Ressorts (BKA, BMAW VerwB Arbeit UG 20, BMK, BML, BMKÖS)

Nicht-Flächen-Ressorts bestehen vorwiegend aus einer Zentralstelle bzw. wenigen Dienststellen.

Unter Berücksichtigung der obig dargestellten Methodik und der bekannten Informationen ergab dies für die Flächen-Ressorts hinsichtlich der zusätzlich erforderlicher Ressourcen:

- Sachleistungen jährlich: 500.000 €
- Personalbedarf: 6 Personen (1 x Leiter + 5 MA)

Für Nicht-Flächen-Ressorts ergab dies zusätzlich erforderliche Ressourcen von:

- Sachleistungen jährlich: 300.000 €
- Personalbedarf: 4 Personen (1 x Leiter + 3 MA)

Bei der Ressourcenanalyse fanden jene Aufwände Berücksichtigung, die zur Leistung des NIS-2-Regimes erforderlich sind (z.B. Einführung eines ISMS). Ressort-spezifische Leistungen, die als "State of the Art" im Bereich der Cybersicherheit zu bezeichnen sind (z.B. Vorhandensein einer Organisation für Cybersicherheit) stellen in diesen Zusammenhang daher keinen zusätzlichen Ressourcenbedarf dar.

Das BMSGPK hat 14 Personen (1x V1/3, 1x RIVIT1, 2x RIVIT2, 5x RIVIT3, 5x RIVIT4) eingemeldet, somit kommt obiges nicht zum Tragen. Insbesonders handelt es sich hierbei um den Aufbau des sektorspezifischen Computernotfallteams (auch CSIRT) für den Sektor Gesundheitswesen.

Das BMEIA hat 8 Personen (1x VB-VD-Höh.Dienst 2, 2x VB-VD-Höh.Dienst 3, 1x VB-VD-Gehob.Dienst 1, 1x VB-VD-Höh.Dienst 2, 1x VB-VD-Höh.Dienst 3 und 2x VB-VD-Höh.Dienst 3) eingemeldet, somit kommt obiges nicht zum Tragen.

Das BMBWF hat 6 Personen (alle RIVIT 2) sowie 2x 250.000 € eingemeldet, somit kommt obiges nicht zum Tragen.

Das zusätzliche Personal für die Datenschutzbehörde begründet sich auf die zu erwartenden steigenden Meldungen, die durch den direkten Meldeweg an die Datenschutzbehörde entstehen werden.

Der Mehrbedarf des Bundesverwaltungsgericht wird durch die zu erwartende gesteigerte Anzahl der ergriffenen Rechtsmittel gegen Bescheide oder Erkenntnisse der Bezirksverwaltungsbehörden begründet.

Aufgrund der vielen zu-/nachgeordneten Dienststellen bzw. Außenstellen (BWB, BMobV, BHÖ, Beschussämter & BEV; zusammen über 60 Standorte) wird der VerwB Wirtschaft UG 40 des BMAW der Gruppe „Flächen-Ressort“ zugerechnet. Daher wurden 6 Personen (3x RIVIT2 und 3x RIVIT3) aufgenommen.

Arbeitsplatzbezogener betrieblicher Sachaufwand

Körperschaft (Angaben in Tsd. €)	2024	2025	2026	2027	2028
Bund	0	0	0	0	0
Länder					
Gemeinden					
Sozialversicherungsträger					
GESAMTSUMME					

Sonstiger betrieblicher Sachaufwand

Körperschaft (Angaben in Tsd. €)	2024	2025	2026	2027	2028
Bund	2.843	8.816	9.151	12.775	12.898
Länder					
Gemeinden					
Sozialversicherungsträger					
GESAMTSUMME	2.843	8.816	9.151	12.775	12.898

36 von 52

in €		2024		2025		2026		2027		2028	
Bezeichnung	Körperschaft	Menge	Aufwand	Menge	Aufwand	Menge	Aufwand	Menge	Aufwand	Menge	Aufwand
Umbaukosten Europlaza	Bund	1	1.302.000,00								
Mobiliar	Bund	90	1.500,00	83	1.500,00						
BMBWF UG 30	Bund			1	500.000,00						
BMEIA ISMS&DSMS Aufbau	Bund	1	133.333,00	1	133.333,00	1	133.334,00				
BMEIA BCMS Aufbau	Bund			1	88.889,00	1	44.444,00				
CTI Feeds	Bund	1	234.000,00	1	234.000,00	1	234.000,00	1	234.000,00	1	234.000,00
Veranstaltungen	Bund	1	100.000,00	1	200.000,00	1	250.000,00	1	270.000,00	1	270.000,00
Dienstreisen	Bund	1	300.000,00	1	415.000,00	1	415.000,00	1	415.000,00	1	415.000,00
Ausbildung	Bund	1	515.000,00	1	707.000,00	1	707.000,00	1	707.000,00	1	707.000,00
KFZ	Bund	1	50.000,00	1	51.000,00	1	52.020,00	1	53.060,00	1	53.060,00
Diverse Lizenzen Software	Bund	1	73.500,00	1	101.000,00	1	101.000,00	1	101.000,00	1	101.000,00
laufende Wartung Sensoren	Bund							1	3.456.000,00	1	3.456.000,00
Miet- und Betriebskosten	Bund			1	916.000,00	1	916.000,00	1	916.000,00	1	916.000,00
BMF	Bund			1	500.000,00	1	510.000,00	1	520.200,00	1	530.604,00
BMSGPK	Bund			1	1.600.000,00	1	1.632.000,00	1	1.664.640,00	1	1.697.933,00
BMBWF	Bund					1	510.000,00	1	520.200,00	1	530.604,00
BMKÖS	Bund			1	300.000,00	1	306.000,00	1	312.120,00	1	318.362,00
BML	Bund			1	300.000,00	1	306.000,00	1	312.120,00	1	318.362,00
BMK	Bund			1	300.000,00	1	306.000,00	1	312.120,00	1	318.362,00
BMAW UG20	Bund			1	300.000,00	1	306.000,00	1	312.120,00	1	318.362,00

BKA	Bund	1	300.000,00	1	306.000,00	1	312.120,00	1	318.362,00
BMEIA laufende Audits	Bund	1	25.000,00	1	25.500,00	1	26.010,00	1	26.530,00
BMEIA MA-Schulungen	Bund	1	136.845,00	1	139.582,00	1	142.374,00	1	145.221,00
BMEIA SOC & SIEM	Bund	1	583.333,00	1	595.000,00	1	606.900,00	1	619.038,00
BMEIA Kapazitätenaufbau von Drittstaaten im Bereich Cybersicherheit	Bund	1	500.000,00	1	510.000,00	1	520.200,00	1	530.604,00
BMAW (VerwB Wirtschaft; UG40)	Bund	1	500.000,00	1	510.000,00	1	520.200,00	1	530.604,00

An Kosten für Mobiliar wurden pro neuen Mitarbeiter:in 1.500 € angenommen:

2024: 90 MA à € 1.500 = 135.000 €

2025: 83 MA à € 1.500 = 124.500 €

Bei CTI Feeds handelt es sich um Cyber Threat Intelligence (CTI) Lizenzen, die nicht eigenständig generierbare Erkennungsmuster darstellen. Zu den Aufgaben der Abteilung IV/S/2 gehört die Koordination und Erstellung des gesamtstaatlichen Cyberlagebilds. Analysen auf Basis des Inputs einer in Österreich und Europa verbreiteten Sensorik, wie es das Produkt bietet, dienen der Verdichtung des Lagebilds auf Basis von tatsächlich gemessener Betroffenheit – zusätzlich zu den bereits einfließenden Erkenntnissen aus freiwilligen und verpflichtenden Meldungen, der Anzeigenstatistik, der CERT-Informationen und der strategisch-analytischen Betrachtung des Cyberraums. An Kosten für die CTI Lizenzen fallen 234.000 € pro Jahr an.

An Kosten für Klausuren, Veranstaltungen und Verpflegung wurde ein Betrag für 2024 von 100.000 € veranschlagt. Da im Jahr 2025 mit einer deutlichen Steigerung der Veranstaltungen zu rechnen ist, wurde ein Betrag von 200.000 € veranschlagt. In den darauffolgenden Jahren wird mit einer geringeren Steigerung an Veranstaltungen gerechnet. Dementsprechend wurden für 2026 250.000 € und für 2027 270.000 € geplant.

An Kosten für Dienstreisen wurde im Mittel ein Betrag von rund 2.000 € pro Person pro Jahr angenommen. Somit ergeben sich die folgenden Beträge:

2024: 300.000 €

38 von 52

ab 2025: 415.000 €

An Kosten für Ausbildungen wurde im Mittel ein Betrag von rund 3.500 € pro Person pro Jahr angenommen. Somit ergeben sich die folgenden Beträge:

2024: 515.000 €
ab 2025: 707.000 €

Die Kalkulation von 50.000 € im Jahr 2024 von Dienst-KFZ (inkl. Leasing Rate, Versicherung und Treibstoff) basiert auf einer Anzahl von 4 Fahrzeugen. Für die darauffolgenden Jahre wurde eine Valorisierung von 2% angewendet.

An Kosten für diverse Software Lizenzen für die Aufgabenerfüllung wurde im Mittel ein Betrag von 500 € pro Person pro Jahr angenommen. Somit ergeben sich die folgenden Beträge:

2024: 73.500 €
ab 2025: 101.000 €

2027 ff: Beginn der Wartung der Sensoren: Eine Wartung kostet 4.000€ netto pro Sensor pro Monat.
Daher ergibt sich aus der Rechnung brutto 4.800€ mal 60 Sensoren mal 12 Monaten ein Betrag von 3.456.000€

Die derzeitige Unterbringung der IV/S/2 ist im Europlaza Objekt 3. Es ist gemäß dem geplanten Personalzuwachs die Quadratmeter in diesem Objekt zu erweitern.
Die Darstellung der Mietkosten + BK Europlaza basieren auf den Mietkosten laut WFA Europlaza von 14.161,18 € für ca. 650m2. Es wurde von der Annahme ausgegangen, dass in etwa 3.500m2 für das Personal benötigt werden. Diese Annahme beruht auf dem Fakt, dass Desk Sharing zum Einsatz kommt. Somit ergibt sich ein Betrag von 916.000 € im Jahr 2025, welcher für die weiteren Jahre mit 2% valorisiert wurde.

Es wird von Umbaukosten von rund 1.302.000 € im Jahr 2024 auf Basis der bisherigen Erfahrungswerte ausgegangen.

Alle Beträge verstehen sich inkl. Ust., Rundungsdifferenzen sind möglich.

Ergebnis der Ressourcenanalyse bzgl. der Ressorts:

Die Ressorts wurden entsprechend der Rückmeldungen in 2 Gruppen eingeteilt,

1. Flächen-Ressorts (BMBWF, BMSGPK, BMEIA, BMF, BMAW VerwB Wirtschaft UG40)

Flächen-Ressorts haben eine überproportionale Anzahl an Bediensteten und viele nachgeordnete Dienststellen bzw. Außenstellen.

2. Nicht-Flächen-Ressorts (BKA, BMAW VerwB Arbeit UG 20, BMK, BML, BMKÖS)

Nicht-Flächen-Ressorts bestehen vorwiegend aus einer Zentralstelle bzw. wenigen Dienststellen.

Unter Berücksichtigung der obig dargestellten Methodik und der bekannten Informationen ergab dies für die Flächen-Ressorts hinsichtlich der zusätzlich erforderlicher Ressourcen:

- Sachleistungen jährlich: 500.000 €
- Personalbedarf: 6 Personen (1 x Leiter + 5 MA)

Für Nicht-Flächen-Ressorts ergab dies zusätzlich erforderliche Ressourcen von:

- Sachleistungen jährlich: 300.000 €
- Personalbedarf: 4 Personen (1 x Leiter + 3 MA)

Bei der Ressourcenanalyse fanden jene Aufwände Berücksichtigung, die zur Leistung des NIS-2-Regimes erforderlich sind (z.B. Einführung eines ISMS). Ressort-spezifische Leistungen, die als "State of the Art" im Bereich der Cybersicherheit zu bezeichnen sind (z.B. Vorhandensein einer Organisation für Cybersicherheit) stellen in diesen Zusammenhang daher keinen zusätzlichen Ressourcenbedarf dar.

Das BMEIA hat eigene Zahlen eingemeldet, somit kommen obigen Ausführungen nicht zum Tragen. Das BMBWF hat 500.000 € insgesamt, die sich auf die UG 30 mit 60% und UG 31 mit 40% aufteilen eingemeldet.

Die Kosten des BMSGPK gliedern sich wie folgt auf:

Weiterentwicklung des Informationssicherheitsmanagement-Systems (ISMS): 175.000 €

Laufende Koordination der Risikomanagementmaßnahmen nach § 32 NISG Entwurf 2024 i.V.m. der Anlage 3, Z 1-13: 50.000 €

Durchgehende Besetzung (24/7) der IT-Operatoren für kritische Services im Sinne einer Bereitschaft (extern): 175.000,00 €

Ausbau des Security Information and Event Management. (SIEM) zu einem Security Operations Center (SOC): 350.000,00 €

Abwicklung der Anforderungen für die Sicherheit in der Lieferkette: 40.000,00 €

Mailverschlüsselung, Netzwerksicherheit, Netzwerksegmentierung: 352.500,00 €

Sicherer Betrieb von kritischen IT-Anwendungen für Bürger:innen: 235.000,00 €

Beschaffung und Betrieb von diversen ISMS-Anwendungen (Dokumentenmgmt., Risikomgmt, Compliance-Assessment, BCM): 172.500,00 €

Aktualisierung und Erstellung von zusätzlichen ISMS-Richtlinien: 50.000,00 €

40 von 52

Pro Jahr wurde eine Valorisierung von 2% angenommen.

Werkleistungen

Körperschaft (Angaben in Tsd. €)	2024	2025	2026	2027	2028
Bund	2.411	3.453	3.373	5.014	5.090
Länder					
Gemeinden					
Sozialversicherungsträger					
GESAMTSUMME	2.411	3.453	3.373	5.014	5.090

in €		2024		2025		2026		2027		2028	
Bezeichnung	Körperschaft	Menge	Aufwand	Menge	Aufwand	Menge	Aufwand	Menge	Aufwand	Menge	Aufwand
Reqpool	Bund	1	110.000,00								
Vertrag Cert.at	Bund			1	515.000,00						
ICG	Bund	1	120.000,00	1	60.000,00						
Personalrecruiting	Bund	1	110.000,00	1	85.000,00	1	85.000,00	1	75.000,00		
NCCC Kooperation FFG	Bund			1	680.000,00	1	780.000,00	1	880.000,00	1	980.000,00
nationales CSIRT	Bund	1	2.021.000,00	1	2.062.000,00	1	2.456.000,00	1	2.506.000,00	1	2.556.120,00
Inhousevergabe (BBG, Statistik Austria,etc.)	Bund	1	50.000,00	1	51.000,00	1	52.020,00	1	53.060,40	1	54.121,61
BRZ	Bund							1	1.500.000,00	1	1.500.000,00

Es ist geplant den derzeitigen Vertrag mit der Forschungsförderungsgesellschaft (FFG), der mit dem Bundeskanzleramt abgeschlossen wurde, im BMI ab 2025 weiterzuführen. Aufgrund des zu erwartenden Anstiegs der Förderungen wurde der Betrag von 580.000 € für das Jahr 2024 mit einer jährlichen Steigerung von ca. 100.000 € kalkuliert.

Nationales CSIRT: 2024 rund 2.000.000 € mit einer Valorisierung von 2% für die Folgejahre.

CSIRT ist das Akronym für Computer Security Incident Response Team (Reaktionsteam für Computersicherheitsverletzungen). Der Begriff CSIRT wird vorwiegend in Europa verwendet. Ein nationales CSIRT (auch Gov CERT genannt) wird als Ansprechpartner für Sicherheitsfragen eines Landes angesehen.

Aufgaben eines CSIRTs:

Reaktive Dienste: Alarm- und Warnmeldungen, Behandlung von Sicherheitsvorfällen, Analyse von Sicherheitsvorfällen, Unterstützung bei der Reaktion auf Sicherheitsvorfälle.

Proaktive Dienste: Bekanntgaben, Technologieüberwachung, Sicherheitsaudits oder -analysen, Konfiguration und Pflege des Sicherheitssystems.

Behandlungen von Artefakten: Analyse von Artefakten, Reaktion auf Artefakte, Kontinuität des Geschäftsbetriebs und Wiederherstellung nach Notfällen, Beratung in Sicherheitsfragen.

Zur gesetzlichen Aufgabenerfüllung der Absicherung von Netz- und Informationssystemen werden Computer-Notfallteams eingerichtet. Diese kümmern sich um die Prävention, Erkennung, Reaktion und Folgenminderung bei Risiken, Vorfällen und Sicherheitsvorfällen.

Für diese Aufgaben sind zwei CSIRT-Tribes in einem hierarchischen Pyramidensystem vorgesehen. Ein CSIRT-Tribe besteht aus:

1x Rivit2 (Senior), 3x Rivit3 (Regular) und 6x Rivit5 (Junior).

Zwei CSIRT-Tribes ergeben somit insgesamt 20 Personen, welche sich um die anfallenden Aufgaben des CSIRTS kümmern.

In den Jahren 2024 und 2025 ist ein Betrieb mit 16 Personen vorgesehen.

Ab dem Jahr 2026 erfolgt der Betrieb mit der vollen Personenanzahl von 20 VBÄs. Die Werte sind Annäherungen und ergeben sich daraus, wie die Personen besoldet wären, wenn sie im Bund arbeiten würden.

Die Personalkosten wurden mit 2% valorisiert und gliedern sich auf die Jahre wie folgt auf (Gesamtkosten sind gemäß dem WFA-Tool gerundet):

Jahr	Wertigkeit	Kosten	Gesamtkosten
2024	2x Rivit2	117.193,62€	234.000€
	4x Rivit3	96.989,49€	388.000€
	10x Rivit5	72.742,11€	727.000€
2025	2x Rivit2	119.537,49€	239.000€
	4x Rivit3	98.929,28€	396.000€
	10x Rivit5	74.196,96€	742.000€
2026	2x Rivit2	121.928,24€	244.000€
	6x Rivit3	100.907,86€	605.000€
	12x Rivit5	75.680,90€	908.000€

42 von 52

2027	2x Rivit2	124.366,81€	249.000€
	6x Rivit3	102.926,02€	618.000€
	12x Rivit5	77.194,51€	926.000€

Um einen reibungslosen Betrieb im CSIRT gewährleisten zu können, fallen folgende Kosten an betrieblichen Sachaufwand an (jährliche Valorisierung 2%):

Jahr	Bezeichnung	Kosten
2024	Rechenzentrum Miete, Server, Firewall Ersatzsysteme	172.000€
	Büromiete, Hardware Versicherung	300.000€
	Lizenzen (Schwachstellenscan, Forensik Threat Intel.)	150.000€
2025	Rechenzentrum Miete, Server, Firewall Ersatzsysteme	175.440€
	Büromiete, Hardware Versicherung	306.000€
	Lizenzen (Schwachstellenscan, Forensik Threat Intel.)	153.000€
2026	Rechenzentrum Miete, Server, Firewall Ersatzsysteme	178.948€
	Büromiete, Hardware Versicherung	312.120€
	Lizenzen (Schwachstellenscan, Forensik Threat Intel.)	156.060€
2027	Rechenzentrum Miete, Server, Firewall Ersatzsysteme	182.526€
	Büromiete, Hardware Versicherung	318.362€
	Lizenzen (Schwachstellenscan, Forensik Threat Intel.)	159.181€

Für etwaige Werkleistungen sind 50.000€ pro Jahr mit einer 2%igen Valorisierung vorgesehen.

2024	50.000€
2025	51.000€
2026	52.020€
2027	53.060€

Übersicht über die Berechnungen (gerundet gemäß dem WFA-Tool)

2024	Personalaufwand	1.349.000€
	Betrieblicher Sachaufwand	622.000€
	Werkleistungen	50.000€
Summe		2.021.000€

2025	Personalaufwand	1.377.000€
	Betrieblicher Sachaufwand	634.000€
	Werkleistungen	51.000€
Summe		2.062.000€

2026	Personalaufwand	1.757.000€
	Betrieblicher Sachaufwand	647.000€
	Werkleistungen	52.000€
Summe		2.456.000€

2027	Personalaufwand	1.793.000€
	Betrieblicher Sachaufwand	660.000€
	Werkleistungen	53.000€
Summe		2.506.000€

2028 letztjährige Summe mit 2% valorisiert, somit 2.556.120€

Vertrag Cert.at

Im Jahr 2024 ist die Übernahme des CERT Vertrags des BKAs sicherzustellen, um alle notwendigen CSIRT Aufgaben gemäß NIS2 abwickeln zu können. Dieser Vertrag wurde am 14.12.2020 nach erfolgtem Vergabeverfahren (GZ 2020-0.800.257-1-A) beauftragt. Gleichzeitig ist die Ausschreibung des GovCERT Vertrags zur Erfüllung aller in der NIS2 Richtlinie geforderten Aufgaben in einem Vergabeverfahren geplant.

Ausgehend von einem Betrag von ca. 459.000€ für das Jahr 2023 wurde eine Verbraucherpreisindexanpassung von 6% gerechnet, somit ergeben sich für das Jahr 2024 ca. 486.000€ und 2025 ca. 515.000€. Ab dem Jahr 2026 sollten diese Kosten in den Kosten des nationalen Csirt beinhaltet sein.

Personalrecruiting

Durch die geplante große Anzahl an Neuaufnahmen wird eine externe Unterstützung für das Personalrecruiting eingeplant. Angenommene Kosten pro Jahr:

44 von 52

2024: 110.000 €
2025: 85.000 €
2026: 85.000 €
2027: 75.000 €

Beratungsdienstleistungen ICG
2024:
Tagsatz: 1.560 € inklusive UST --> Berechnung für ca. 76 Tage – entspricht gerundet 120.000 €. Es wurde mit einem Mischtagessatz Senior und Expert gerechnet.
2025
Tagsatz: 1.560 € inklusive UST --> Berechnung für ca. 38 Tage – entspricht gerundet 60.000 €. Es wurde mit einem Mischtagessatz Senior und Expert gerechnet.

Inhousevergabe (BBG, Statistik Austria,etc.) 2024 rund 50.000 €, 2025 ff mit einer jährlichen Valorisierung von 2%.
Um sicherzustellen, dass das nötige fachliche spezielle Know How vorhanden ist (z.B. Vergabeverfahren) wurden in der Kalkulation Inhousevergaben berücksichtigt.

BRZ 2027 ff
Das IOC-Frühwarnsystem soll mit Hilfe des BRZ betrieben werden. Dafür werden ab dem Jahr 2027 rund 1.500.000 € veranschlagt.

ReqPOOL GmbH 2024
Tagsatz: 1.380 € inkl. UST --> Berechnung für ca. 80 Tage – entspricht rund 110.000 € inkl. 20% UST.

Rundungsdifferenzen sind möglich.

Transferaufwand

Körperschaft (Angaben in Tsd €)	2024	2025	2026	2027	2028
Bund					
Länder		13.000	8.248	8.780	9.039
Gemeinden					
Sozialversicherungsträger					

45 von 52

GESAMTSUMME	0	13.000	8.248	8.780	9.039

in €		2024		2025		2026		2027		2028	
Bezeichnung	Körperschaft	Empf.	Aufwand	Empf.	Aufwand	Empf.	Aufwand	Empf.	Aufwand	Empf.	Aufwand
Niederösterreich	Länder			1	2.388.232,00	1	1.515.195,00	1	1.613.084,00	1	1.660.402,00
Burgenland	Länder			1	374.810,72	1	237.795,71	1	253.158,47	1	260.584,59
Kärnten	Länder			1	741.560,99	1	470.477,53	1	500.872,68	1	515.565,22
Oberösterreich	Länder			1	2.282.016,13	1	1.447.807,18	1	1.541.342,59	1	1.586.556,14
Salzburg	Länder			1	827.365,73	1	524.915,68	1	558.827,79	1	575.220,38
Steiermark	Länder			1	1.680.342,87	1	1.066.080,31	1	1.134.954,31	1	1.168.246,92
Tirol	Länder			1	1.123.912,12	1	713.057,20	1	759.124,18	1	781.392,23
Vorarlberg	Länder			1	638.465,29	1	405.069,28	1	431.238,73	1	443.888,63
Wien	Länder			1	2.944.012,72	1	1.867.805,70	1	1.988.475,08	1	2.046.804,75

Bei den Kosten der Länder handelt es sich nicht um Transferaufwand, sondern um eine tabellarische Aufstellung der Kosten der Länder aus Vereinfachungsgründen und zur Gewährleistung der Übersichtlichkeit.

Niederösterreich:

Personalkosten:

2x Unternehmensrisikomanagement:

Jahreskosten pro Person: € 88.952,00

2025: € 177.904,00

2026: € 181.462,00

2027: € 188.793,00

2028: € 196.420,00

1x Lieferantenmanagement:

Jahreskosten pro Person: € 82.293,00

2025: € 82.293,00

46 von 52

2026: € 83.939,00
2027: € 87.330,00
2028: € 90.858,00
1x Security Operations Center:
Jahreskosten pro Person: € 82.293,00
2025: € 82.293,00
2026: € 83.939,00
2027: € 87.330,00
2028: € 90.858,00
2x Security Operations Center:
Jahreskosten pro Person: € 74.730,00
2025: € 149.460,00
2026: € 152.449,00
2027: € 158.608,00
2028: € 165.016,00
2x Security Operations Center:
Jahreskosten pro Person: € 70.798,00
2025: € 141.596,00
2026: € 144.428,00
2027: € 150.263,00
2028: € 156.334,00
2x Informationssicherheitsrisikomanagement:
Jahreskosten pro Person: € 82.293,00
2025: € 164.586,00
2026: € 167.878,00
2027: € 174.660,00
2028: € 181.716,00

Personalkosten gesamt:
2025: € 798.132,00

2026: € 814.095,00
2027: € 846.984,00
2028: € 881.202,00

Sachkosten:
Unternehmensrisikomanagement:
Hardware Wartung:
2025: € 4.300,00 2026: € 4.400,00 2027: € 4.500,00 2028: € 4.600,00
Lizenz Wartung:
2025: - 2026: € 8.000,00 2027: € 8.000,00 2028: € 8.000,00
Security Operations Center:
Hardware Wartung:
2025: € 50.000,00 2026: € 52.000,00 2027: € 53.100,00 2028: € 54.000,00
Lizenz Wartung:
2025: € 84.000,00 2026: € 86.000,00 2027: € 88.000,00 2028: € 90.000,00
Betriebskosten:
2025: € 466.800,00 2026: € 476.200,00 2027: € 485.800,00 2028: € 494.700,00

Sachkosten gesamt:
2025: € 605.100,00 2026: € 633.100,00 2027: € 646.100,00 2028: € 658.200,00

Investitionskosten:
Unternehmensrisikomanagement:
Hardware Beschaffung:
2025: € 16.000,00
Lizenz Beschaffung:
2025: € 54.000,00
Security Operations Center:
Hardware Beschaffung:
2025: € 292.000,00

48 von 52

Lizenz Beschaffung:
2025: € 438.000,00
Informationssicherheitsrisikomanagement:
Lizenz Beschaffung:
2025: € 15.000,00

Investitionskosten gesamt:
2025: € 815.000,00
keine weiteren Kosten in den anderen Jahren

Werk- & Dienstleistungen:
Verpflichtende Security Awarness Maßnahmen für das Management:
2025: € 35.000,00 2026: € 36.000,00 2027: € 37.000,00 2028: € 38.000,00
Lieferantenmanagement:
2025: € 47.000,00 2026: € 32.000,00 2027: € 33.000,00 2028: € 33.000,00
NIS-2 Einführungsunterstützung:
2025: € 70.000,00
NIS-2 Prüfung, sofern das Amt der Landesregierung zum Sektor mit hoher Kritikalität zugerechnet wird:
2027: € 50.000,00 2028: € 50.000,00
Unternehmensrisikomanagement Einführungsunterstützung:
2025: € 18.000,00

Werk- & Dienstleistungen gesamt:
2025: € 170.000,00 2026: € 68.000,00 2027: € 120.000,00 2028: € 121.000,00

Niederösterreich Jahreskosten gesamt:
2025: € 2.388.232,00 2026: € 1.515.195,00 2027: € 1.613.084,00 2028: € 1.660.402,00

Niederösterreich, das derzeit den Vorsitz der Landeshauptleutekonferenz inne hat, dient als Grundlage für die Berechnung der anderen Bundesländer. Die Summe der einzelnen Jahre für Niederösterreich werden mit Hilfe des Verteilungsschlüssels pro Bundesland hochgerechnet.

Als Grundlage für den Verteilungsschlüssel dient die Einwohnerzahl und er stellt sich wie folgt dar:

Burgenland: 2,88 %

Kärnten: 5,70 %

Niederösterreich: 18,37 %

Oberösterreich: 17,55 %

Salzburg: 6,36 %

Steiermark: 12,93 %

Tirol: 8,65 %

Vorarlberg: 4,91 %

Wien: 22,64 %

Investitionen

Vermögens-, Finanzierungs- und Ergebnishaushalt

in Tsd. €	2024	2025	2026	2027	2028
Anschaffungswert	245	228	20	20	
Auszahlung	245	228	20	20	
Abschreibung	59	84	117	121	64
Einzahlung					

Ansch.dat	Bezeichnung	Anlagentyp	Körperschaft	ND	Menge	Anschaffungskosten in €	Gesamt in Tsd. €
2024-01-01	IT-Ausstattung	Arbeitsplatzausstattung	Bund	4	90	2.500,00	225
2025-08-16	IT-Ausstattung	Arbeitsplatzausstattung	Bund	4	83	2.500,00	208
2024-01-01	Spezial Hardware	Großrechensysteme, Server-, Netzwerk-	Bund	7	20	1.000,00	20

50 von 52

		und Kommunikationssysteme einschließlich der erforderlichen Komponenten					
2025-01-01	Spezial Hardware	Großrechensysteme, Server-, Netzwerk- und Kommunikationssysteme einschließlich der erforderlichen Komponenten	Bund	7	20	1.000,00	20
2026-01-01	Spezial Hardware	Großrechensysteme, Server-, Netzwerk- und Kommunikationssysteme einschließlich der erforderlichen Komponenten	Bund	7	20	1.000,00	20
2027-01-01	Spezial Hardware	Großrechensysteme, Server-, Netzwerk- und Kommunikationssysteme einschließlich der erforderlichen Komponenten	Bund	7	20	1.000,00	20

Verk.dat.	Bezeichnung	Körperschaft	Menge	Verkaufspreis in €	Gesamt in Tsd. €
	IT-Ausstattung	Bund	90	0,00	0
	IT-Ausstattung	Bund	83	0,00	0
	Spezial Hardware	Bund	20	0,00	0
	Spezial Hardware	Bund	20	0,00	0
	Spezial Hardware	Bund	20	0,00	0
	Spezial Hardware	Bund	20	0,00	0

51 von 52

Geschätzte IT-Ausstattung pro neuem:r Mitarbeiter:in gestaffelt nach Jahren 2024-2027 rd. 2.500 € inkl. USt. (wie Notebook samt Zubehör, Dockingstation, Monitor)

An Spezial Hardware (z.B. Notebooks mit erhöhter Kapazität) wurden jährlich 20.000 € angenommen.

Erträge aus der operativen Verwaltungstätigkeit und Transfers

Körperschaft (Angaben in Tsd. €)	2024	2025	2026	2027	2028
Bund				1.800	1.800
Länder					
Gemeinden					
Sozialversicherungsträger					
GESAMTSUMME				1.800	1.800

in €		2024		2025		2026		2027		2028	
Bezeichnung	Körperschaft	Menge	Ertrag	Menge	Ertrag	Menge	Ertrag	Menge	Ertrag	Menge	Ertrag
Einnahmen aus IOC Frühwarnsystem	Bund							1	1.800.000,00	1	1.800.000,00

Einnahmen aus IOC Frühwarnsystem

Da laut NISG §13 ein Pauschalbetrag (Verordnung derzeit noch in Ausarbeitung) eingehoben werden darf, werden derzeit 2.500€ pro Sensor pro Monat angenommen.

52 von 52

Dokumentinformationen

Vorlagenversion: V2.015
Schema: BMF-S-WFA-v.1.9
Deploy: 2.8.8.RELEASE
Datum und Uhrzeit: 04.04.2024 16:18:42
WFA Version: 1.30
OID: 1362
A0|B2|D0|I2

Bundesministerium Finanzen	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.bmf.gv.at/verifizierung
	Datum/Zeit	2024-04-04T16:18:49+02:00
Unterzeichner	Bundesministerium für Finanzen	
Aussteller-Zertifikat	CN=a-sign-corporate-07,OU=a-sign-corporate-07,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT	
Serien-Nr.	874736968	
Dokumentenhinweis	Dieses Dokument wurde amtssigniert.	