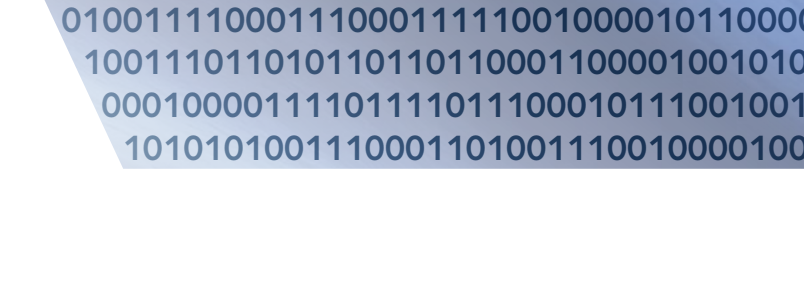
# Österreichische Strategie für Cybersicherheit 2021

ÖSCS 2021




# Österreichische Strategie für Cybersicherheit 2021

ÖSCS 2021

Wien, 2021

## Inhalt

# Vorwort

Sehr geehrte Leserinnen, sehr geehrter Leser!

Die Digitalisierung ist mittlerweile in fast all unseren Lebensbereichen angekommen: wir kaufen online ein, kommunizieren via Smartphone und erledigen unsere Bankgeschäfte digital. Warenverteilungssysteme werden über die Cloud koordiniert, Wasser- und Stromversorgung elektronisch gesteuert und auch in Krankenhäuser funktioniert schon längst nichts mehr ohne Computer.

All diese Entwicklungen bergen große Potentiale, sind aber auch mit Gefahren verbunden, die wir ernst nehmen müssen. Cybersicherheit, also der sichere Umgang im und mit dem Cyberraum, wird deshalb immer wichtiger.

Denn Cyberangriffe machen weder vor einzelnen Branchen noch vor Landesgrenzen halt. Es bedarf verstärkter Kooperation und eines verstärkten Informationsaustausches sowohl auf nationaler als auch auf internationaler Ebene, um die Gesellschaft im Cyberraum als Ganzes resilienter zu machen. Nur so kann es gelingen, langfristig auf die sich dynamisch entwickelnden Herausforderungen aus dem Cyberraum zu reagieren, Potentiale für Forschung und Wirtschaft zu nützen und die in diesem Bereich sehr limitierten Personalressourcen bestmöglich einzusetzen.

All diese Herausforderungen sollen mit der neuen Österreichischen Strategie für Cybersicherheit 2021 – kurz ÖSCS 2021 – bestmöglich gemeistert werden. Damit wird nicht nur ein wichtiger Bestandteil des aktuellen Regierungsprogrammes umgesetzt, sondern auch ein wichtiger Grundstein für die künftige, strukturierte Zusammenarbeit von Behörden, Forschung und Wirtschaft gelegt.

Zusätzlich ist die ÖSCS 2021 in die „Europäische Cybersicherheitsstrategie für die digitale Dekade“ eingebettet. Damit leistet Österreich nicht nur einen Beitrag zur Erhöhung der eigenen Sicherheit, sondern setzt sich auch für einen globalen, offenen, stabilen und sicheren Cyberraum ein. Das ist die Grundlage dafür, um die Chancen der Digitalisierung auch in den kommenden Jahren und Jahrzehnten bestmöglich und vor allem sicher nutzen zu können.

Karl Nehammer
Bundeskanzler

# 1

# Ausgangslage

> Die Vision der ÖSCS 2021 ist die langfristige Schaffung eines sicheren Cyberraums als Beitrag zur Steigerung der Resilienz Österreichs und der Europäischen Union durch einen gesamtstaatlichen Ansatz.

Im Zeitalter der Digitalisierung ist unsere Gesellschaft vernetzter denn je. Der Fortschritt in der digitalen Technologie hat unser tägliches Leben genauso verändert wie unseren Arbeitsalltag und unser Geschäftsleben. Bürgerinnen und Bürger sind auf digitale Dienste ebenso angewiesen wie Unternehmen und staatliche Einrichtungen, die bei der Erbringung ihrer Kernaufgaben von digitalen Netzen und Infrastrukturen abhängig sind. Doch genau mit dieser umfassenden Vernetzung und der fortschreitenden Abhängigkeit von digitalen Diensten steigt auch die Verwundbarkeit unserer Gesellschaft. Cyberangriffe und -vorfälle können durch die Beeinträchtigung von Dienstangeboten und die Unterbrechung von Geschäfts- und Behördenvorgängen massive Auswirkungen auf unsere Gesellschaft und Wirtschaft haben.

Die Steigerung der digitalen Widerstandsfähigkeit Österreichs und die Gewährleistung von Cybersicherheit in der digitalen Welt insgesamt sind daher sowohl für unseren Wohlstand als auch für unsere Sicherheit von großer Bedeutung. Für Österreich ist die Cybersicherheit daher eine der obersten Prioritäten und eine gemeinsame Herausforderung für Staat, Wirtschaft, Wissenschaft und Gesellschaft.

Cybersicherheit ist grenzübergreifend und Österreich ist ein Teil der Europäischen Union (EU). Bei der Bekämpfung der gegenwärtigen und zukünftigen Cyberbedrohungen setzt sich die EU aktiv für den Schutz der Gesellschaft, die Sicherung des Wohlstands und der Werte sowie der Grundrechte und -freiheiten in Europa ein. Sie leistet einen Beitrag, um die Abwehrfähigkeit, die strategische Autonomie und die technologischen Kapazitäten und Kompetenzen zu erhöhen und den Aufbau eines soliden Binnenmarktes zu fördern. Für die europäische und österreichische Wirtschaftsleistung sind der Schutz des digitalen Binnenmarktes und des Binnenmarktes für Cybersicherheit von wesentlicher Bedeutung und daher von Bedeutung für Österreich und die EU.

Ein globaler, offener, stabiler und sicherer Cyberraum, in dem das Völkerrecht, insbesondere die Menschenrechte und das Humanitäre Völkerrecht angewendet werden, ist für die weitere Entwicklung Österreichs und der EU eine wichtige Grundlage. Daher tritt Österreich in der Cyberdiplomatie aktiv auf bilateraler und multilateraler Ebene für die Achtung des Völkerrechts, die Stärkung der freiwilligen Normen, Regeln und Prinzipien des verantwortungsvollen Staatenverhaltens und von vertrauensbildenden Maßnahmen im Cyberraum ein.

Die Österreichische Strategie für Cybersicherheit (ÖSCS) besteht aus zwei Teilen: Im ersten Teil wird ein langfristig ausgelegter strategischer Überbau dargestellt, mit einer Erläuterung zur Ausgangslage, den Herausforderungen und Chancen, dem Rahmen für die Umsetzung sowie dem Monitoring der Strategie. Im zweiten Teil sind die erforderlichen Maßnahmen der Strategie festgelegt, um die Ziele zu erreichen. Das Monitoring der Strategieumsetzung erfolgt über eine Onlineplattform.

Mit Hilfe dieser Struktur kann flexibel auf sich ständig weiterentwickelnde Bedrohungslagen sowie aktuelle Herausforderungen reagiert werden. Änderungen ergeben sich aus den politischen, technologischen, gesellschaftlichen und wirtschaftlichen Entwicklungen sowohl auf EU- und internationaler als auch auf nationaler Ebene.

## Europäischer, internationaler und österreichischer Rahmen

Die ÖSCS 2021 beruht auf den Grundsätzen der Österreichischen Sicherheitsstrategie (ÖSS) und ist eine Weiterentwicklung der ÖSCS 2013. Diese schuf die wesentlichen Grundstrukturen und -prozesse für den Aufbau einer umfassenden und zusammenhängenden Cybersicherheitspolitik. In der Strategie 2021 werden nun zusätzlich die Vorgaben des Regierungsprogramms 2020–2024 sowie das nachfolgend genannte Rahmenwerk auf europäischer und internationaler Ebene berücksichtigt.

Mit dem Inkrafttreten der NIS-Richtlinie[1] (NIS-RL) wurde zum ersten Mal ein umfassender Rechtsakt über Cybersicherheit in der EU geschaffen. Im Zentrum steht dabei die Definition von einheitlichen Sicherheitsstandards und Meldewegen für all jene Unternehmen, die für das Funktionieren des Binnenmarktes und damit der Staaten essentiell sind. In Österreich wurde die NIS-RL durch das Netz- und Informationssystemsicherheitsgesetz (NISG) umgesetzt. Damit wurden nicht nur einheitliche Sicherheitsanforderungen für Unternehmen der kritischen Infrastruktur festgelegt, sondern auch erstmals die Erstellung einer Cybersicherheitsstrategie gesetzlich verankert.

Die NIS-RL war allerdings erst der Anfang der intensiven Bemühungen auf europäischer Ebene.

1 Richtlinie (EU) 2016/1148 vom 6.7.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-RL)

Die EU passt regelmäßig ihren strategischen Rahmen an, um ein digitales Europa aufzubauen, in dem die Sicherheit, das Vertrauen, das Bewusstsein für seine Stärken, die Wettbewerbsfähigkeit und die Offenheit gegenüber der Welt sowie die Achtung der gemeinsamen Werte der EU im Zusammenhang mit einem offenen und sicheren Internet gestärkt werden. Seit 2019 bildet der EU-Rechtsakt für Cybersicherheit, mit welchem ENISA zu einer echten EU-Cybersicherheitsagentur aufgewertet und ein EU-rechtlicher Rahmen für IT-Sicherheitszertifizierungssysteme geschaffen wurde, einen Teil des europäischen Rahmens.[2] Die letzte große Aktualisierung des Politikrahmens zur Abwehr von Cyberbedrohungen fand 2020 statt, als die EU ein neues Cybersicherheitspaket vorlegte. Dieses umfasst eine modernisierte „EU-Cybersicherheitsstrategie für die digitale Dekade", eine überarbeitete Richtlinie über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union („NIS 2.0") sowie eine neue Richtlinie über die Widerstandsfähigkeit kritischer Einrichtungen.[3] Darüber hinaus errichtet die EU ein „Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung" und ein „Netz nationaler Koordinierungszentren", um Investitionen in Forschung, Technologie und industrielle Entwicklung im Bereich Cybersicherheit zielgerichtet zu bündeln und für eine bessere Koordinierung zu sorgen. Zudem soll eine „Kompetenzgemeinschaft für Cybersicherheit" die wichtigsten Interessensgruppen zusammenbringen, um das Fachwissen im Bereich Cybersicherheit EU-weit zu verbessern und zu verbreiten.

---

2 Verordnung (EU) 2019/881 vom 17.4.2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Cybersecurity Act)

3 https://ec.europa.eu/commission/presscorner/detail/de/ip_20_2391 (abgefragt am 21.12.2020)

Zur Prävention und Bewältigung von böswilligen Cyberaktivitäten stehen der EU, falls erforderlich in vollem Umfang, die Maßnahmen der gemeinsamen Außen- und Sicherheitspolitik zur Verfügung. Diese sogenannte Cyber Diplomacy Toolbox zielt auf Konfliktverhütung, die Eindämmung von Cyberbedrohungen und eine größere Stabilität in den internationalen Beziehungen ab. In diesem Rahmen sind Cyberdialoge mit Drittstaaten vorgesehen sowie gemeinsame diplomatische Reaktionen der EU auf böswillige Cyberattacken, bis hin zu Sanktionen.

Bei all diesen Maßnahmen ist die Zusammenarbeit der Mitgliedstaaten der EU von zentraler Bedeutung. Zur Erarbeitung wesentlicher Konzepte und Themenfelder der Cybersicherheit gibt es auf europäischer Ebene verschiedene Arbeitsgruppen und Netzwerke, an denen sich Österreich aktiv beteiligt.

Die Verhandlungsprozesse zu Cybersicherheit in den Vereinten Nationen (VN) werden in den nächsten Jahren auf breiter Basis weitergeführt. Dabei setzt sich Österreich für eine stärkere Zusammenarbeit mit Drittländern ein. Zur Konfliktverhütung im Cyberraum gilt es, die Anwendung von Völkerrecht sicherzustellen und die freiwilligen Normen für verantwortungsvolles Staatenverhalten umzusetzen und zu stärken. Als VN-Sitz wird Wien in den nächsten Jahren Schauplatz wichtiger Verhandlungen zu einer VN-Cybercrime Konvention sein, die dazu beitragen soll, die internationale Zusammenarbeit zur effektiven Bekämpfung der Cyberkriminalität zu stärken. Bei der Cyber-Konfliktverhütung spielt die in Wien ansässige Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) eine wichtige Rolle.

## Entstehungsprozess der ÖSCS 2021

Mittlerweile ist der Grad der Spezialisierung im Bereich der Cybersicherheit hoch und dynamisch. Um dieser Tatsache Rechnung zu tragen, haben Expertinnen und Experten aus den Bereichen Wirtschaft, Bildung, Forschung und Entwicklung sowie Expertinnen und Experten des Bundes die Inhalte der ÖSCS 2021 in einem mehrstufigen Prozess erarbeitet. Diese vielschichtige Herangehensweise stellt Cybersicherheit als eine gesamtgesellschaftliche Herausforderung und Aufgabe dar.

## Organisation und Prozesse in der hoheitlichen Verwaltung

Cybersicherheit ist eine gesamtstaatliche Querschnittsmaterie, daher sind wirksame Koordinierungsstrukturen und gesamtstaatliche kooperative Modelle notwendig. Mit der Bündelung aller Kräfte aus den Ressorts, die für Cybersicherheit zuständig sind, wird die Effektivität staatlicher Maßnahmen gegenüber Cyberbedrohungen und -vorfällen deutlich erhöht werden.

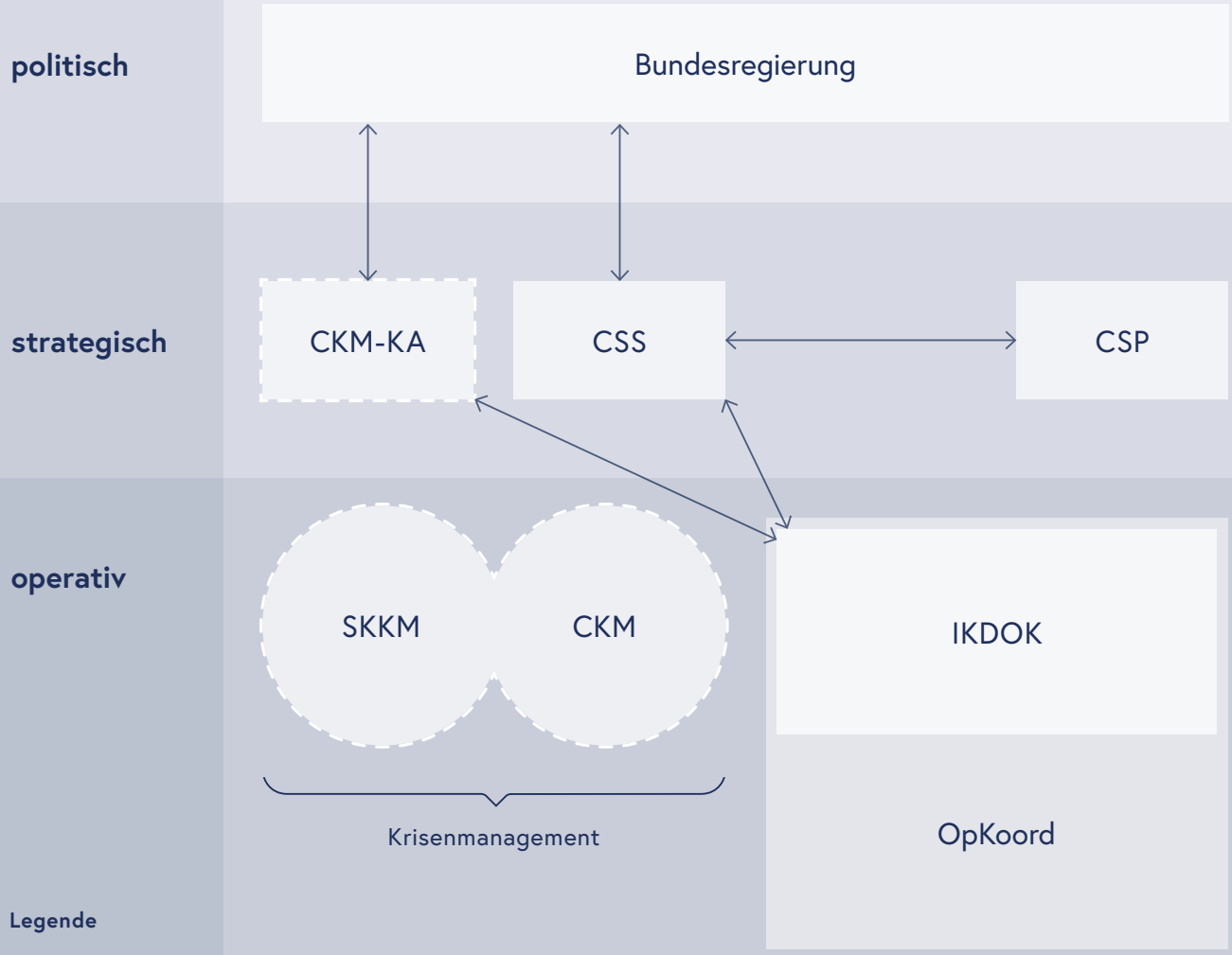
Die ÖSCS 2021 baut auf den nationalen Strukturen der ÖSCS 2013 auf. Diese ergeben sich aus den gesetzlichen Grundlagen und Zuständigkeitsbereichen sowie etablierten sektor- und ressortübergreifenden Gremien, Plattformen und Koordinierungsstrukturen.

Die strategische Koordination im Bereich der Cybersicherheit wird zentral durch das Bundeskanzleramt (BKA) wahrgenommen und umfasst neben der gesamtstaatlichen auch die europäische und internationale Koordination im Cyberbereich. Auf internationaler Ebene agiert das Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) im Rahmen der Außen- und Sicherheitspolitik. Im innerstaatlichen Bereich ist das Bundesministerium für Inneres (BMI) im Rahmen der Aufrechterhaltung der öffentlichen

Ruhe, Ordnung und Sicherheit im Bereich Cybersicherheit und Bekämpfung der Cyberkriminalität zuständig. Das BMI ist nach dem NISG zuständig für die konkrete Umsetzung von Cybersicherheitsmaßnahmen auf operativer Ebene. Dem Bundesministerium für Landesverteidigung (BMLV) obliegt die militärische Landesverteidigung im Cyberraum. Die für Cybersicherheit zuständigen Ressorts stimmen sich sowohl auf strategischer als auch auf operativer Ebene eng ab. Zuständigkeiten in Cyberangelegenheiten, welche die Wirkungsbereiche weiterer Ministerien betreffen, ergeben sich aus dem Bundesministeriengesetz (BMG). Die Zusammenarbeit mit den Ländern und Gemeinden erfolgt unter Berücksichtigung ihres eigenen Wirkungsbereichs im Rahmen des Prinzips der Selbstverwaltung durch aktiven regelmäßigen Austausch mit dem Bund.

In Österreich wurden im Bereich der Sicherheit von Netz- und Informationssystemen Strukturen zur Koordination auf operativer Ebene aufgebaut, in denen ständig ein Lagebild erstellt und der koordinierte Einsatz der Cyberkräfte bei der Bewältigung von Cybervorfällen ermöglicht wird. Diese sind die sogenannte Operative Koordinierungsstruktur (OpKoord) sowie der Innere Kreis der Operativen Koordinierungsstruktur (IKDOK). Die organisatorische Leitung in diesen Koordinationsstrukturen obliegt dem BMI. Der IKDOK, unterstützt durch die OpKoord, bildet im Krisenfall die direkte Schnittstelle zum gesamtstaatlichen Cyberkrisenmanagement (CKM). Das CKM stellt eine Plattform für die ressortübergreifende Koordination in krisenhaften Entwicklungen bereit. Dem BMI obliegt die Leitung und Koordination des CKM auf operativer Ebene. Kommt es im Falle einer Cyberkrise auch zur Ausrufung des militärischen Einsatzfalls im Cyberraum (z. B. zur Abwehr souveränitätsgefährdender Angriffe im Cyberraum), geht die Leitung der Einsatzführung vom BMI auf das BMLV über.

Auf strategischer Ebene wirken zusätzlich die Cyber Sicherheit Steuerungsgruppe (CSS) und die Cyber Sicherheit Plattform (CSP). Die CSS ist für die Umsetzung der ÖSCS verantwortlich. Die CSP stellt die zentrale Austausch- und Kooperationsplattform zwischen Wirtschaft, Wissenschaft und öffentlicher Verwaltung dar.



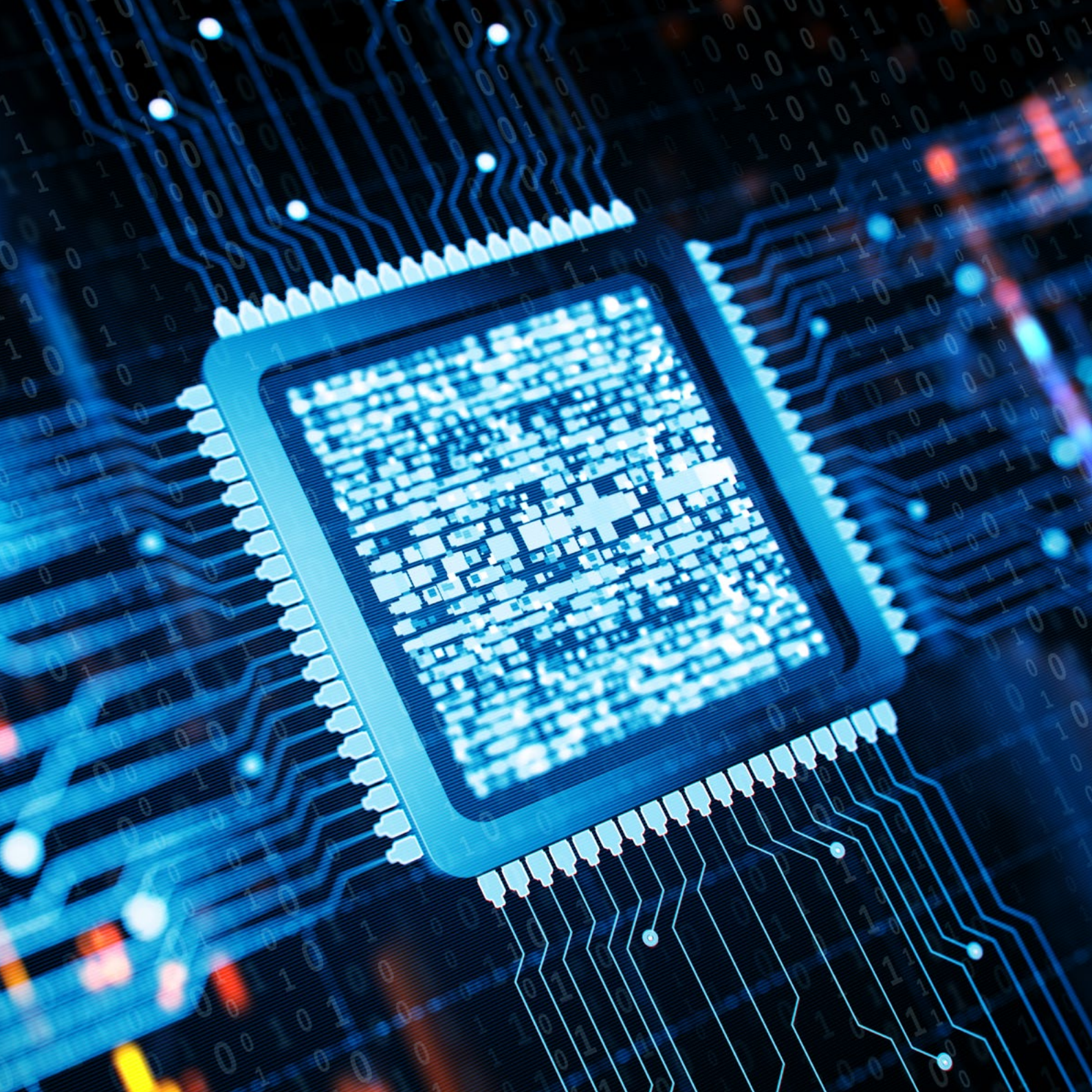

**Legende**

| | |
|---|---|
| – – – – | anlassbezogen |
| CKM | Cyberkrisenmanagement |
| CKM-KA | CKM-Koordinationsausschuss |
| CSP | Cyber Sicherheit Plattform |
| CSS | Cyber Sicherheit Steuerungsgruppe |
| IKDOK | Innerer Kreis der Operativen Koordinierungsstruktur |
| OpKoord | Operative Koordinierungsstruktur |
| SKKM | Staatliches Krisen- und Katastrophenschutzmanagement |

# 2

# Herausforderungen

> Eine zukunftsorientierte Cybersicherheitspolitik ermöglicht es, die enormen Chancen und Potentiale der Digitalisierung umfänglich und sicher zu nutzen.



Die Digitalisierung und ihre Rolle in der globalen Vernetzung ermöglicht wirtschaftlichen und gesellschaftlichen Fortschritt, birgt aber auch Risiken. Aus diesen Risiken erwachsen Bedrohungsszenarien, die auch das Potential zur Gefährdung und Destabilisierung Österreichs und seiner Gesellschaft in sich tragen. Die Szenarien lassen sich unterteilen in:

1. **Bedrohungen, die das Ergebnis der missbräuchlichen Nutzung von Informationstechnik (IT) sind**
   Staatliche und nichtstaatliche Akteure verwenden den Cyberraum als Aktionsfeld für ideologisch, politisch und kriminell motivierte Cyberangriffe. Diese reichen von Cyberkriminalität über Cyberspionage, die eigenständig oder als Teil hybrider Bedrohungsszenarien auftreten können, bis hin zur Cyberkriegsführung.

   Auch die bewusste Nutzung des IT-gestützten Informationsraums zu Zwecken der Manipulation, Beeinflussung und Destabilisierung demokratischer Meinungsbildungsprozesse fällt in diesen Bereich.

2. **Bedrohungen, die das Ergebnis von falscher Nutzung der IT sind**
   Neben der missbräuchlichen und böswilligen Nutzung von IT kann auch die nicht sachgemäße Nutzung zu Herausforderungen führen. Unsachgemäße Nutzung entsteht meistens aufgrund fehlender Anwenderkenntnisse. Zusätzlich führen Sorglosigkeit und Fahrlässigkeit seitens der Anwenderinnen und Anwender zu einer Realisierung zahlreicher Risiken. Diesen kann auch mit Sicherheitstechnologien nur bedingt begegnet werden. Unzureichende Vorbereitung auf Angriffe als auch fahrlässiger Betrieb von IT machen Unternehmen und Organisationen zu besonders einfachen Zielen. Dies gilt für den gesamten Wertschöpfungs- und Produktionsprozess inklusive aller involvierten "Lieferanten". Gerade letzteres gilt es im Zuge des Risikomanagements umfassend mit zu beurteilen.

3. **Bedrohungen, die das Ergebnis der Abhängigkeit von IT sind**
   Herausforderungen entstehen neben unsicheren IT-Produkten und Diensten auch durch die zunehmende Abhängigkeit von der Verfügbarkeit dieser. Somit kann schon der Ausfall von ursprünglich sicheren Technologien zu wirtschaftlichem Schaden und zu Gefahren führen. In diesem Sinne kann etwa die Nutzung von Cloud-Technologien neue Risiken mit sich bringen. In Bezug auf die zunehmende Abhängigkeit stellt auch der Mangel an Fachkräften im Bereich Cybersicherheit eine Herausforderung dar.

   Durch die fortschreitende Digitalisierung wird sich die Abhängigkeit von IT künftig weiter erhöhen und angesichts digitaler Geopolitik von Staaten, Komplexität der Internet Governance, Ressourcenknappheit und zunehmender Abhängigkeit von Weltraum-Infrastruktur werden neue Herausforderungen entstehen.

4. **Bedrohungen durch neue Technologien**
   Mit der Digitalisierung von Bereichen und Vorgängen, bei denen bisher keine IT eingesetzt wurde, ergeben sich neue sicherheitsrelevante Herausforderungen. Darüber hinaus kann auch die Verdrängung von bisher im Einsatz befindlichen IT-Anwendungen durch neue Technologien zu solchen Herausforderungen führen. Das wird in Zukunft vor allem durch Entwicklungen im Bereich Künstlicher Intelligenz (KI), Internet of Things (IoT) und weiteren Emergenten und Disruptiven Technologien (EDT), etwa der Quantentechnologie, erwartet. Ebenso kann auch der Funktionswandel von IT neue Risiken umfassen, vor allem, wenn bisher unterstützende IT-Anwendungen zum tragenden oder kontrollierenden Bestandteil werden. Neben sicherheitsrelevanten Herausforderungen gehen damit oft auch technische und ethische Fragestellungen einher.

Zur Bewältigung dieser Herausforderungen stellt die ÖSCS 2021 einen wesentlichen Beitrag dar.

# 3

# Strategisches Leitbild

”Die Gewährleistung von Freiheit und Sicherheit sind Kernaufgaben des Staates, die auch im Cyberraum wahrgenommen werden müssen.

## Bekenntnis zur gesamtstaatlichen Cybersicherheitsvorsorge und Beitragsleistung zur Cybersicherheit der Europäischen Union

Österreich bekennt sich zu einer gesamtstaatlichen Cybersicherheitsvorsorge und zur Schaffung eines sicheren Cyberraums, die Teil der Umfassenden Landesverteidigung (ULV) und einer umfassenden Sicherheitsvorsorge sind. Die gesamtstaatliche Cybersicherheitsvorsorge hat die Aufgabe, Österreichs staatliche Souveränität nach außen zu gewährleisten.

Dies wird durch eine umfassende Cybersicherheitspolitik umgesetzt, die ein Teil der nationalen Sicherheit ist. Zu ihr gehören weit mehr als außen-, verteidigungs- und sicherheitspolitische Aspekte. Sie wird insbesondere auch durch die cybersicherheitsrelevanten Aspekte der Wirtschafts-, Infrastruktur- und Finanzpolitik sowie der Bildungs-, Wissenschafts- und Forschungspolitik unterstützt.

Die Verwirklichung der Cybersicherheitsvorsorge benötigt einen gesamtstaatlichen Ansatz, in dem Staat, Wirtschaft, Wissenschaft und Gesellschaft eine gemeinsame Verantwortung tragen. Die Wirkung der Strategie betrifft somit ganz Österreich.

Österreich ist zudem Beitragsleister und auch Profiteur der Cybersicherheitsarchitektur der EU. Aufgrund des transnationalen Charakters des Cyberraums und wechselseitiger Abhängigkeiten kann Sicherheit und Resilienz im Cyberraum langfristig nur durch einen europaweiten Ansatz gewährleistet werden. Jegliche Stärkung der Cybersicherheit der EU ist auch eine Stärkung der österreichischen Cybersicherheit. Österreich bekennt sich daher zur Förderung und Umsetzung der Cybersicherheitsstrategie der EU.

## Vision und Ziele

Aus dem Bekenntnis zur gesamtstaatlichen Cybersicherheitsvorsorge ergibt sich folgende Vision:

> Die Vision der ÖSCS 2021 ist die langfristige Schaffung eines sicheren Cyberraums als Beitrag zur Steigerung der Resilienz Österreichs und der Europäischen Union durch einen gesamtstaatlichen Ansatz.

Um diese Vision verwirklichen zu können, verfolgt die ÖSCS 2021 folgende **Ziele:**

1. Österreich verfügt über ausreichende finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, als solche zu erkennen, abzuwehren sowie derartige Angriffe strafrechtlich zu verfolgen;

2. Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen und zu verteidigen;

3. In Österreich wird Cybersicherheit als gemeinschaftliche Aufgabe von Gesellschaft, Wirtschaft und Staat wahrgenommen; Verantwortlichkeiten und Zuständigkeiten sind klar definiert und werden von allen Beteiligten gelebt;

4. Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert sowie Awareness geschaffen;

5. In Österreich ist eine sichere Partizipation am gesellschaftlichen und politischen Leben im Cyberraum für Bürgerinnen und Bürger möglich;

6. Österreich hat klare gesetzliche und operative Möglichkeiten, um ein sicheres und attraktives Unternehmensumfeld im Cyberraum zu bieten und gegebenenfalls eine adäquate Strafverfolgung zur gewährleisten;

7. Österreich engagiert sich aktiv im Cyberbereich und arbeitet intensiv mit allen Stakeholdern auf nationaler, europäischer und internationaler Ebene;

8. Österreich kann im Zusammenwirken mit der EU seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen;

9. In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit;

10. Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Resilienz im Bereich Cybersicherheit zu erhöhen, die Nachfrage des Arbeitsmarktes zu erfüllen und die Cyberkriminalität nachhaltig zu bekämpfen;

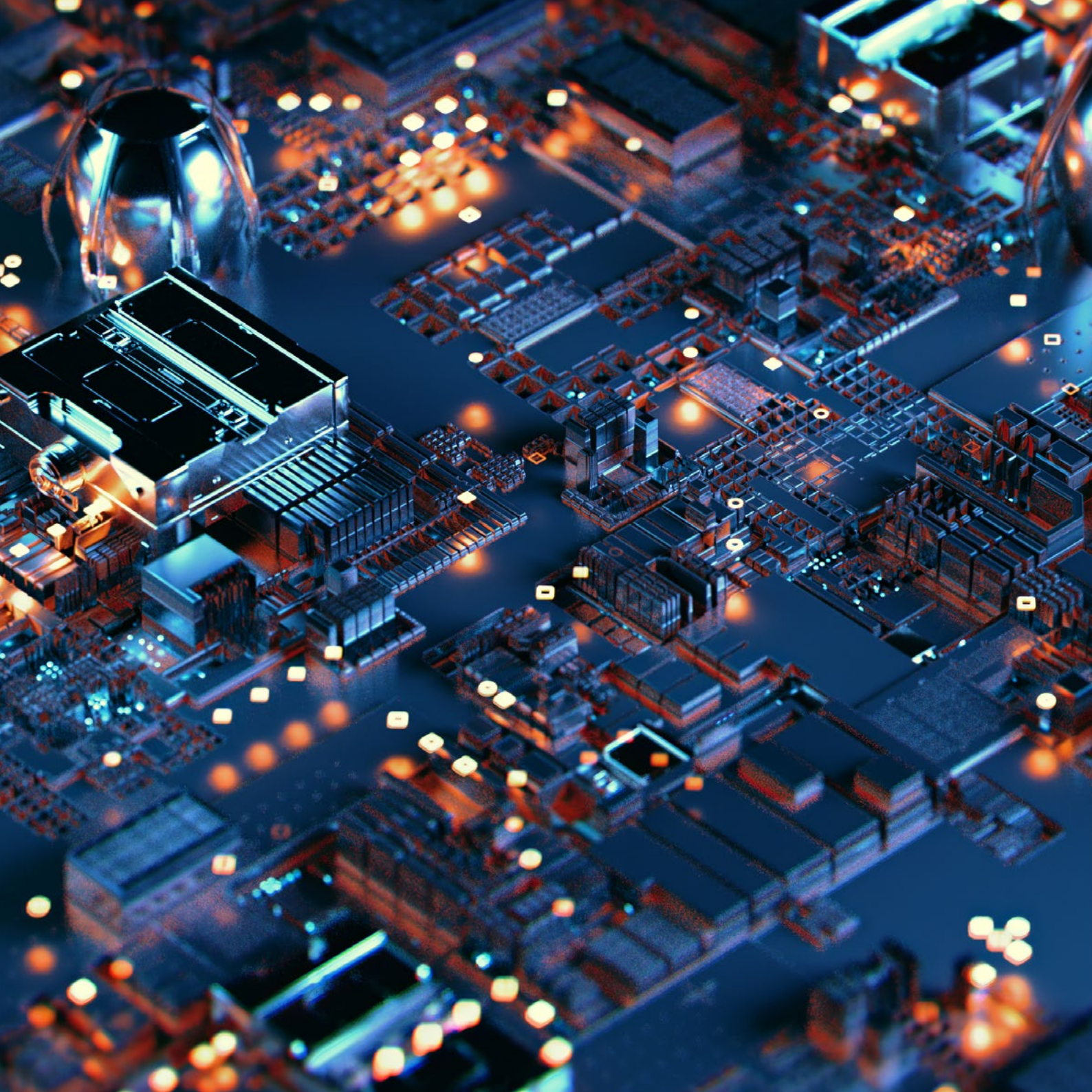
11. Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;

12. Österreich arbeitet in einem gesamtstaatlichen Ansatz stetig an der Weiterentwicklung seiner Rechtsgrundlagen zur Erhöhung der Cybersicherheit und Bekämpfung der Cyberkriminalität.

Mit der konkreten Umsetzung der Maßnahmen im Maßnahmenkatalog wird das Erreichen der Ziele verfolgt.

# 4

# Strukturen und Zielgruppen



# Strukturen

Die für die Umsetzung der ÖSCS 2021 erforderlichen Strukturen werden aufbauend auf den bereits durch die ÖSCS 2013 definierten strukturellen Vorgaben weiterentwickelt.

## Strategische Ebene

### Cyber Sicherheit Steuerungsgruppe

Die Cyber Sicherheit Steuerungsgruppe (CSS) ist das zentrale, strategisch-planende Organ der Cybersicherheit in Österreich. Sie entwickelt und koordiniert sämtliche Maßnahmen der ÖSCS. Darüber hinaus überwacht sie die Umsetzung der ÖSCS (Monitoring), aktualisiert den Maßnahmenkatalog und erstellt einen jährlichen Bericht zur Cybersicherheit.

Die CSS setzt sich aus hochrangigen Vertreterinnen und Vertretern mit Cybersicherheitsexpertise der im Nationalen Sicherheitsrat vertretenen Ressorts zusammen. Ferner gehören dem Gremium die Ressorts an, denen die Angelegenheiten der Telekommunikation und der Digitalisierung obliegen. Themenorientiert kann die CSS Vertreterinnen und Vertreter weiterer Einrichtungen der öffentlichen Verwaltung (EdöV) zur Teilnahme einladen (CSS+). Dazu zählen insbesondere jene Ressorts, die entweder selbst direkt durch die Maßnahmen der ÖSCS 2021 betroffen sind bzw. deren Wirkungsbereich tangierte Organisationen und/oder Unternehmen umfasst.

### Cyberkrisenmanagement–Koordinationsausschuss (CKM-KA)

Mit dem NISG wurde zur Feststellung des Vorliegens einer Cyberkrise und für den Beschluss operativer Maßnahmen zur Bewältigung einer Cyberkrise ein Koordinationsausschuss eingerichtet. Dieser wird vom Generaldirektor für die öffentliche Sicherheit geleitet und setzt sich aus dem Chef des Generalstabs, dem Generalsekretär des Bundeskanzleramtes und dem Generalsekretär für auswärtige Angelegenheiten

zusammen. Der Ausschuss ist um weitere Vertreter von Bundes- oder Landesbehörden, Betreiber wesentlicher Dienste und Computer-Notfallteams sowie Einsatzorganisationen zu erweitern, wenn dies zur Bewältigung der Cyberkrise erforderlich ist.[4]

## Operative Ebene

### Innerer Kreis der Operativen Koordinierungsstruktur (IKDOK)

Der IKDOK ist eine interministerielle Struktur zur Koordination auf der operativen Ebene im Bereich der Cybersicherheit und er wurde durch das NISG eingerichtet. Der IKDOK erörtert und aktualisiert das nationale Lagebild im Bereich der Cybersicherheit und unterstützt den Koordinationsausschuss im CKM.

Der IKDOK wird ausgebaut und soll zukünftig über die erforderlichen Ressourcen verfügen, um im Auftrag der CSS in Fragen der Cybersicherheit Empfehlungen und Einschätzungen für die Bundesverwaltung abgeben zu können.

### Operative Koordinierungsstruktur (OpKoord)

Die OpKoord ist eine Struktur zur Koordination auf der operativen Ebene im Bereich der Cybersicherheit. Sie besteht aus dem IKDOK sowie den Computer-Notfallteams nach dem NISG und kann um Vertreterinnen und Vertreter von Betreibern wesentlicher Dienste, von Anbietern digitaler Dienste (AdD) sowie Einrichtungen der öffentlichen Verwaltung (EdöV), einschließlich von Computer-Notfallteams, die bei diesen eingerichtet sind, erweitert werden.

---

4 Siehe NISG § 25. (1)f

# Zielgruppen

Gesellschaft, Wirtschaft, Bildung, Forschung und Entwicklung sowie der öffentliche Sektor sind die zentralen Zielgruppen der ÖSCS 2021. Die einzelnen Maßnahmen zur Zielerreichung werden den jeweiligen Zielgruppen schwerpunktmäßig zugeordnet.

## Gesellschaft

**Themenbereich Vertrauen und Privatsphäre**
Das Vertrauen in IT-Produkte und -Dienste ist von besonderer Bedeutung. Es soll durch Transparenz, Datenschutz und Datensicherheit sowie den Schutz der Privatsphäre erreicht werden. Eine sichere Kommunikation ist die Grundvoraussetzung für die Teilhabe am gesellschaftlichen Leben sowie für die Ausübung von Grund- und Menschenrechten im Cyberraum.

Sowohl im privaten Umfeld als auch in der Wirtschaft und bei Serviceangeboten des Staates und der Verwaltung sind der digitale Identitätsnachweis sowie sichere Kommunikationskanäle von zentraler Bedeutung. Der Zugriff auf personenbezogene und besonders schützenswerte Daten muss nachweisbar dokumentiert und auf das nötige Maß beschränkt sein. Eine qualitativ hochwertige elektronische Identifizierung ist essentiell, um Datenschutz und Datensicherheit zu gewährleisten und ist bereits bei der Konzeptionierung mitzuberücksichtigen. Schließlich sind Datenschutz und Datensicherheit sowie das Vertrauen in deren umfassende Berücksichtigung im elektronischen Identitätsnachweis (E-ID) - System eine essentielle Grundlage für die tatsächliche Nutzung. Die „E-ID und digitale Ausweise“ haben bei entsprechender Entwicklung nach dem Stand der Technik das Potential, die Cybersicherheit für Bürgerinnen und Bürger, Wirtschaft und Verwaltung EU-weit zu erhöhen.

**Themenbereich Bewusstseinsbildung (Awareness)**

Durch eine breite Sensibilisierung der Gesellschaft sollen die notwendige Wahrnehmung, das persönliche Interesse und die Aufmerksamkeit für Cybersicherheit weiter gestärkt werden. Dies ist eine Voraussetzung für ein selbstbestimmtes und verantwortungsbewusstes Handeln im Cyberraum und trägt zu einer höheren Widerstandsfähigkeit bei.

**Themenbereich freier Meinungsbildungsprozess**

Die Authentizität und Integrität von Informationen sind Voraussetzung für den freien Meinungsbildungsprozess. Je mehr sich die Informationsvielfalt in den digitalen Raum verlagert, desto wichtiger ist die Absicherung der Informationssysteme. Es kann mehrfach zur Streuung von falschen oder bewusst irreführenden Informationen durch verschiedene Akteure kommen. Derartige Bedrohungen im und aus dem Informationsraum haben oft die Manipulation der öffentlichen Debatte sowie eine generelle Destabilisierung des demokratischen Meinungsbildungsprozesses bis hin zur Beeinflussung von Wahlen zum Ziel. Daher muss die Meinungsfreiheit abgesichert werden.

**Themenbereich Ethik**

Damit Folgen und mögliche Risiken für Menschenrechte und Grundfreiheiten, die sich aus der Entwicklung und Einführung zukünftiger Technologien ergeben, beurteilt werden können, braucht es entsprechende Mechanismen und Gremien. Diese sollen damit in Zusammenhang stehende technische und ethische Fragestellungen behandeln.

## Wirtschaft

### Themenbereich Wirtschaftsstandort

Staat und Wirtschaft verfolgen als gemeinsames Ziel die Schaffung der Voraussetzungen für einen sicheren und attraktiven Wirtschaftsstandort. Die Steigerung der Cybersicherheit in Unternehmen trägt wesentlich zu deren Wachstum und Erfolg bei. Die digitale Souveränität Österreichs und der EU wird durch die Verringerung von Abhängigkeiten von IT-Produkten und -Diensten, deren Hersteller oder Dienstleister von außerhalb Österreichs beziehungsweise außerhalb der EU stammen, gestärkt.

Es müssen Lösungen/Produkte zur Identifikation und Abwehr von Cyberattacken verstärkt eingesetzt werden, welche die effiziente Einhaltung des nationalen und europäischen Rechts gewährleisten.

### Themenbereich kleine und mittlere Unternehmen (KMU)

Die Stärkung der KMU und die Verbesserung der Rahmenbedingungen für KMU hat im Bereich der Cybersicherheit große Bedeutung. Als Teil der Digitalisierungsoffensive, die eine Förderung von Digitalisierungsmaßnahmen im Bereich von heimischen KMU vorsieht, wird Cybersicherheit maßgeblich berücksichtigt. Ergänzend sollen die Rahmenbedingungen so gestaltet werden, dass auch Maßnahmen zur Stärkung der Cybersicherheit für KMU (z. B. durch Erhöhung der Digitalen Skills von Mitarbeiterinnen und Mitarbeitern, dem Erfüllen von technischen und organisatorischen Basis-Sicherheitsanforderungen, Unterstützung bei der Auswahl und Zusammenarbeit mit vertrauenswürdigen Partnerunternehmen und der Nutzung von vertrauenswürdigen Cloud-Diensten) ergriffen werden.

### Themenbereich Einrichtungen mit einer hohen Bedeutung für das Gemeinwesen

Einrichtungen mit einer hohen Bedeutung für das Gemeinwesen sind besonders schützenswert. Die Widerstandsfähigkeit Österreichs wird einerseits durch das Heben des Cybersicherheitsniveaus und andererseits durch eine verstärkte und enge Kooperation erhöht werden. Die nationalen Programme zum Schutz kritischer Infrastrukturen (APCIP) und der Cybersicherheit werden eng aufeinander abgestimmt.

## Bildung, Forschung und Entwicklung

### Themenbereich Bildung

Im Bereich der Cybersicherheit spielen der Ausbau von Kapazitäten und die Ausgestaltung zukünftiger Bildungsangebote eine wichtige Rolle. Damit wird ein Beitrag zur Abdeckung des Fachkräftebedarfes im Bereich der Cybersicherheit geleistet. In Österreich gibt es bereits eine Vielzahl an Einzelmaßnahmen und Initiativen, die zu einem Gesamtkonzept zusammengeführt werden müssen. Digitalisierung und Technologieentwicklung erfordern ein lebenslanges Lernen. Neben der Kinder-, Jugend- und Erwachsenenbildung kommt vor allem auch der Seniorinnen- und Seniorenbildung eine wichtige Rolle zu.

### Themenbereich Forschung und Entwicklung

Forschung und Entwicklung liefern einen wesentlichen Beitrag zu einer höheren Cybersicherheit und nehmen somit eine wichtige Rolle bei der Früherkennung von Trends und Technologien sowie der Entwicklung von IT-Sicherheitslösungen ein. Daher wird ein Rahmen geschaffen, der einen Lückenschluss zwischen anwendungsorientierten Forschungsprojekten und öffentlichem Beschaffungsprozess ermöglicht. Dieser deckt von der Grundlagenforschung bis hin zur Markteinführung den gesamten Prozess ab. Der Staat tritt als Bedarfsträger und Erstkunde bei der Entwicklung von österreichischen IT-Lösungen für Sicherheitsaufgaben auf, stärkt damit die Anwendungsorientierung der Forschung und schafft Markteintrittschancen.

## Öffentlicher Sektor

### Themenbereich Widerstandsfähigkeit

Um die Widerstandsfähigkeit Österreichs zu gewährleisten, ist es notwendig, eine effektive und verbindliche Zusammenarbeit zwischen Bund, Ländern und Gemeinden zu realisieren. Die Bereiche Umsetzung NISG und Schutz kritischer Einrichtungen haben hier eine besondere Bedeutung. Die existierenden Mechanismen zur effektiven Bewältigung von Cybervorfällen und -krisen sowie zur Aufrechterhaltung der Kommunikation werden kontinuierlich verbessert und weiterentwickelt. Österreichischen und europäischen Dienstleistern und Herstellern kommt bei der Steigerung der Widerstandsfähigkeit eine besondere Rolle zu. Die Weiterentwicklung der Rechtsgrundlagen zur Erhöhung der Cybersicherheit in einem gesamtstaatlichen Ansatz wird vorangetrieben.

### Themenbereich Cyberkriminalität und Strafverfolgung

Immer mehr Menschen, immer mehr Geräte und sich rasant entwickelnde Technologien führen zu einem immer stärkeren Vernetzungsgrad. Dies lässt das ohnehin schon hohe Bedrohungs- und Gefährdungspotential im Bereich der Cyberkriminalität weiter stark ansteigen. Daher ist es notwendig, in einem entwicklungsoffenen Strategiekonzept die laufende Anpassung der Ermittlungsmethoden und Präventionsansätze sicherzustellen. Durch die laufende Anpassung der rechtlichen Grundlagen, auch durch Erhöhung des Strafrahmens, wird die wirksame nationale und internationale Verfolgung von Internetkriminalität ermöglicht. Der Ausbau technischer Ermittlungsmaßnahmen wird gefördert. Fahndungs- und Ermittlungsunterstützung wird durch den Ausbau von Social Media und OSINT-Einheiten verbessert. Darüber hinaus werden spezialisiertes Know-how und Strukturen in den Strafverfolgungsbehörden ausgebaut. Eine effiziente Bekämpfung von Cyberkriminalität, verbunden mit einer effektiven Strafverfolgung, sind Grundvoraussetzung, um erfolgreich gegen Täterinnen und Täter im Cyberraum vorzugehen. Der Ausbau und die Weiterentwicklung von Cyberkriminalität-Dienststellen bei den Strafverfolgungsbehörden wird gefördert. Da Cyberkriminalität nicht vor nationalen Grenzen Halt macht, ist die Weiterführung und der weitere Ausbau der internationalen Zusammenarbeit in

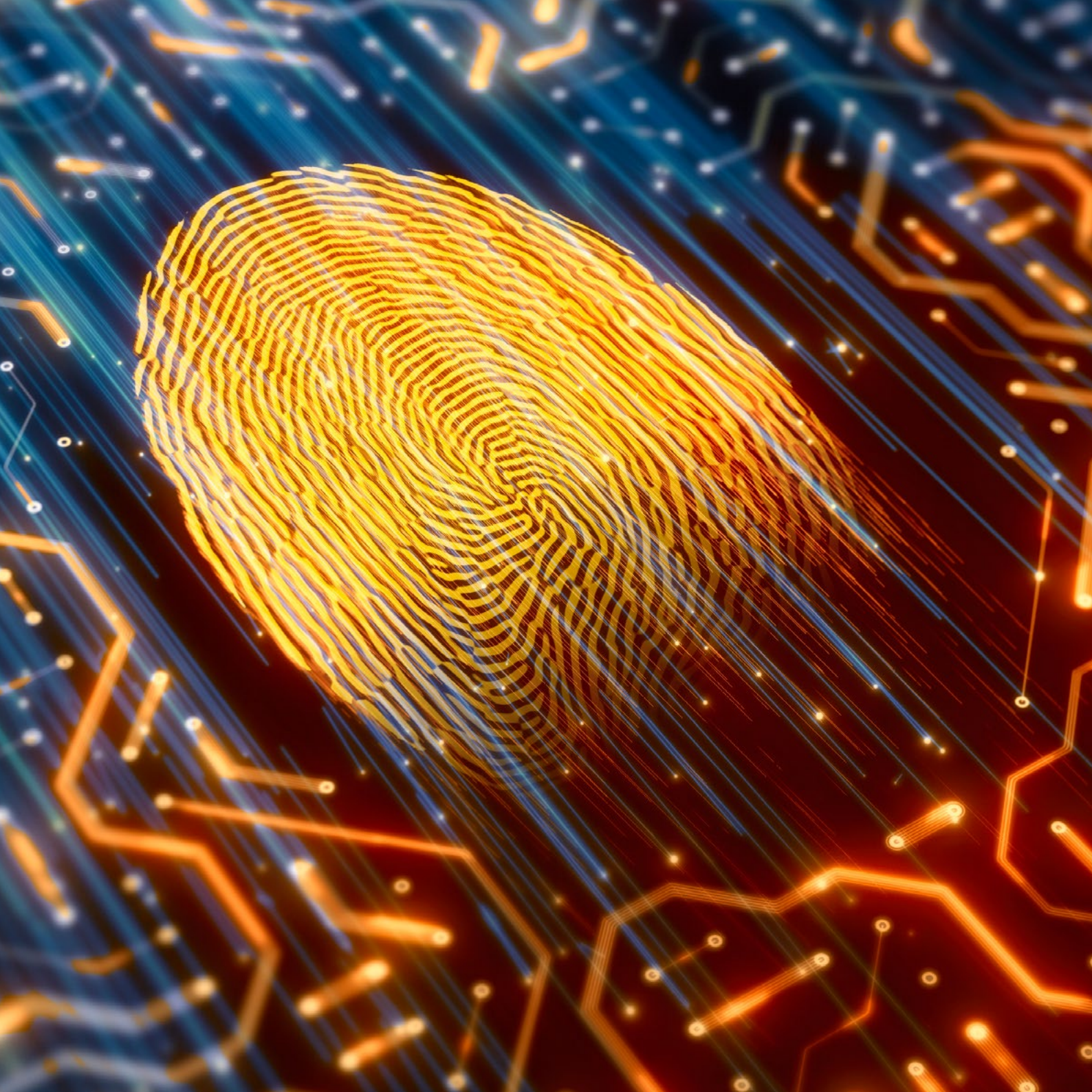
diesem Bereich notwendig. Die Kooperation im Rahmen des European Cybercrime Centre (EC3) bei Europol sowie mit Interpol ist unabdingbar. Besonderes Augenmerk gilt auch der neuen VN-Cybercrime Konvention, die in den nächsten Jahren in Wien und New York verhandelt wird. Aufgrund der Komplexität der Sachverhalte ist es notwendig, insbesondere auch auf regionaler Ebene Strukturen zu schaffen, die den Bürgerinnen und Bürgern sowie Unternehmen effizient, rasch und direkt erste Hilfestellungen geben.

**Themenbereich Cyberverteidigung**

Die militärische Landesverteidigung im Cyberraum ist als Teil der ULV und somit der gesamtstaatlichen Sicherheitsvorsorge Aufgabe des Österreichischen Bundesheeres (ÖBH). Angriffe auf die Souveränität Österreichs sollen durch die erforderlichen Cyberkapazitäten und -fähigkeiten im gesamten Spektrum abgehalten und abgewehrt werden. Dies ist ein unmittelbarer Beitrag zur Erhöhung der gesamtstaatlichen Resilienz und ermöglicht Assistenzleistungen bei der Bewältigung von Cyberkrisen als Beitrag zur österreichischen Cybersicherheitsarchitektur.

Das ÖBH und das BMLV leisten strategische Beiträge zum gesamtstaatlichen Lagebild sowie zur Attribuierung von Cyberangriffen, stärken die Cyberverteidigungsfähigkeiten in Zusammenarbeit mit nationalen und internationalen Partnern und tragen so auch zur Cyberverteidigung der EU bei.

Die Cyberverteidigung ist ein gesamtstaatlicher Prozess unter der Federführung des BMLV und umfasst daher alle Maßnahmen zur Vorbereitung, Aufrechterhaltung und Wiederherstellung der Handlungsfähigkeit im Rahmen einer souveränitätsgefährdenden bzw. -verletzenden Handlung.



**Themenbereich internationale Zusammenarbeit**
Cybersicherheit muss über nationale Grenzen hinweg gedacht werden.

Die ÖSCS 2021 verfolgt daher einen europäischen und internationalen Ansatz. Angesichts der transnationalen Vernetzung kann Cybersicherheit für Österreich nur durch Einbettung und Verstärkung der nationalen Maßnahmen in die europäischen, regionalen und internationalen Prozesse erreicht werden. Die aktive Positionierung Österreichs im Rahmen der EU, der Vereinten Nationen (VN), der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE), des Europarats, der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD), der NATO-Partnerschaft für den Frieden, sowie durch bilaterale Kontakte, wird vorangetrieben. Österreich wird sich als Standort für den offenen globalen Austausch zum Thema Cybersicherheit etablieren.

Bestehende Asymmetrien zum Nachteil der EU oder Österreichs (Gewährleistung der strategischen Autonomie und der digitalen Souveränität, z. B. im Hinblick auf Datenschutz, Hardware, Software, Cloud etc.) müssen durch effiziente europäische und internationale Kooperationen ausgeglichen werden.

Österreich setzt sich auf internationaler Ebene für einen sicheren, offenen und rechtlich gestalteten Cyberraum ein, in dem das Völkerrecht gilt und die Ausübung aller Menschenrechte gewährleistet ist und dieser höchste Priorität zukommt.

# 5

# Maßnahmen, Umsetzung und Monitoring

## Maßnahmen

Essentiell für die Umsetzung der Strategie sind die konkreten Maßnahmen, die im Maßnahmenkatalog aufgelistet werden. Dieser wird regelmäßig – soweit möglich – veröffentlicht. Jede Maßnahme ist zumindest einem der in Kapitel 3 genannten Ziele und einer oder mehrerer in Kapitel 4 erwähnten Zielgruppen zuzuordnen.

Der Maßnahmenkatalog wird im Hinblick auf die sich ständig erweiternde Bedrohungslage sowie auf aktuelle Herausforderungen durch die CSS aktualisiert. Die betreffenden Maßnahmen werden auf Vorschlag der CSS bzw. auf Basis der durch die CSS ausgearbeiteten Vorschläge durch die jeweiligen Generalsekretärinnen oder Generalsekretäre der von der Maßnahme in ihrem Wirkungsbereich betroffenen Ressorts beauftragt. Sofern die Vorschläge der CSS alle Ressorts betreffen, werden diese durch die Konferenz der Generalsekretäre beschlossen und deren Umsetzung bei den mit Cybersicherheit betrauten Ressortverantwortlichen beauftragt. Im Rahmen der Umsetzungsbeauftragung durch die Generalsektretärin bzw. den Generalsekretär erfolgt insbesondere auch die Sicherstellung organisatorischer, finanzieller und technischer Voraussetzungen.

Die für die Umsetzung der Maßnahmen unterstützenden Leitlinien finden sich im Anhang.

Maßnahmen für die Zielgruppen Gesellschaft, Wirtschaft sowie Bildung, Forschung und Entwicklung können von Akteuren aus dem Privatsektor im Rahmen der öffentlich-privaten Zusammenarbeit, beispielsweise über die Cyber Sicherheit Plattform (CSP) oder die Cybersecurity Competence Community (CCC), der CSS vorgeschlagen werden. Die CSS prüft die Aufnahme der vorgeschlagenen Maßnahmen in den Maßnahmenkatalog.

Die Maßnahmen sollen flexibel an die sich weiterentwickelnde Bedrohungslage und aktuelle Herausforderungen angepasst werden. Darüber hinaus können unter anderem politische, technologische, gesellschaftliche und wirtschaftliche Entwicklungen sowohl auf EU- und internationaler Ebene als auch auf nationaler Ebene Anpassungen notwendig machen.

”

Die für die Umsetzung verantwortlichen Akteure tragen mit ihrem Wissen maßgeblich zum Gelingen dieser Strategie und somit zur Erhöhung des Cybersicherheitsniveaus in Österreich bei.

## Umsetzungsplan

Die Ressorts erstellen für jede einzelne Maßnahme, die ihren Wirkungsbereich betrifft, einen detaillierten Umsetzungsplan. Dieser wird dem Sekretariat der CSS entweder aus einem bestimmten Anlass oder jedes halbe Jahr zur Verfügung gestellt. Der Umsetzungsplan hat für die jeweilige Maßnahme konkrete Aufgaben, Tätigkeiten und Zuständigkeiten sowie Qualitätssicherungsmaßnahmen, die jedenfalls einen Zeitplan und Meilensteine zu enthalten haben, festzulegen.

Als Hilfestellung für die Ressorts sind Leitlinien für die Umsetzung der Strategie im Anhang definiert.

## Monitoring

Die Überwachung der Umsetzung (Monitoring) der ÖSCS obliegt der CSS. Das Sekretariat der CSS verwahrt die Umsetzungspläne zentral. Auf deren Grundlage erstattet die CSS der Konferenz der Generalsekretäre halbjährlich einen Fortschrittsbericht. Die aktuellen Maßnahmen werden in Zwischenschritten, die in einem Zeitabstand von einem halben Jahr erfolgen, einer Evaluierung durch die CSS unterzogen.

# 6

# Chancen und Ausblick

”Eine gelebte Cybersicherheitspolitik bietet eine Vielzahl an Chancen und Möglichkeiten. Sie ist für den Wohlstand, die gesellschaftliche und politische Teilhabe und die Sicherheit der Bürgerinnen und Bürger von entscheidender Bedeutung.

## Chancen der Cybersicherheit

Neben den in Kapitel 2 erwähnten Herausforderungen und Bedrohungen eröffnet der Bereich der Cybersicherheit eine Vielzahl von Chancen und Möglichkeiten, die es zu nutzen gilt.

Für Österreich ergeben sich durch die fortschreitende Digitalisierung im Hinblick auf Cybersicherheit insbesondere folgende Chancen:

1. **Chancen für die Gesellschaft**
   Ein cybersicheres Umfeld erleichtert der Gesellschaft, vollumfänglich am öffentlichen Leben teilzunehmen und fördert die Nutzung des Cyberraums als Partizipationsraum. Eine sichere Kommunikation und Interaktion sowohl im privaten als auch im öffentlichen Bereich ist dafür unbedingt erforderlich.

2. **Chancen für die Wirtschaft**
   Cybersicherheit ist ein Wachstumsmarkt. Mit der zunehmenden Digitalisierung ergeben sich vermehrt Angriffsflächen oder Risiken, die es durch innovative Produkte und Dienstleistungen zu reduzieren gilt. Damit ergibt sich die Chance für neue Geschäftsfelder und Märkte. Dabei ist ein Fokus auf nachhaltige und ökologische Produktentwicklung zu legen. Durch ein sicheres und innovatives Umfeld sowie widerstandsfähige Infrastrukturen wird ein Fundament für alle wirtschaftlichen Aktivitäten geschaffen. Eine gut auf Cyberrisiken vorbereitete, resiliente Wirtschaft stärkt den Wirtschaftsstandort und bietet in einem immer komplexeren, digitalisierten Umfeld nachhaltige Wettbewerbsvorteile.

3. **Chancen für Bildung, Forschung und Entwicklung**

   Der stark zunehmende Bedarf an qualifizierten Kräften macht die Erweiterung des Bildungsangebots, die Stärkung der universitären Landschaft und die Förderung innovativer Projekte in diesem Bereich erforderlich. Der Bereich der Cybersicherheit birgt hohes Potential für eine effektive und zielgerichtete Erweiterung des primären, sekundären und tertiären Bildungsbereichs in sich, welches es zu nutzen gilt.

4. **Chancen für den öffentlichen Sektor**

   Die Entwicklung und Nutzung sicherer IT erlaubt dem öffentlichen Sektor die direkte und sichere Interaktion mit den Bürgerinnen und Bürgern und der Wirtschaft. Ein cybersicheres Umfeld und ein verlässliches Cyberkrisenmanagement stärken das Vertrauen in die staatlichen Institutionen und schützen dessen Handlungsfähigkeit. Das internationale Engagement stärkt zusätzlich den Amtssitz Wien.

# Ausblick

Die Lebensbereiche aller in Österreich lebenden Menschen sind mehr und mehr von Cybersicherheit betroffen. Der Cyberraum ist nicht statisch und entwickelt sich ständig weiter. Bestehende Rechtsgrundlagen, insbesondere Völkerrecht, Menschenrechte und humanitäres Völkerrecht gelten auch dort. Bedrohungen und Herausforderungen im Cyberraum, die nicht vor Landesgrenzen Halt machen, können nur durch eine umfassende Cybersicherheitspolitik und die Einbindung aller relevanten Akteure erreicht werden. Die ÖSCS zielt genau darauf ab und bietet durch einen konkreten Maßnahmenkatalog ein flexibles, wirksames und inklusives Instrument zur Erkennung, Vorbeugung und Bewältigung von Bedrohungen und Herausforderungen – immer vor dem Hintergrund, die höchstmögliche Stufe an Cybersicherheit zu verwirklichen, um die vielseitigen Chancen in allen Lebensbereichen nutzbar zu machen.

> Cybersicherheit geht uns alle an. Um langfristig einen sicheren Cyberraum zu schaffen und die Widerstandsfähigkeit Österreichs zu steigern, arbeiten alle Akteure zusammen. So werden die vielseitigen Chancen der Cybersicherheit verwirklicht.


152.68
123.05
279.82
977.65
73.79

## Abkürzungen

| | |
|---|---|
| AdD | Anbieter digitaler Dienste |
| APCIP | Österreichisches Programm zum Schutz kritischer Infrastrukturen |
| BKA | Bundeskanzleramt |
| BMG | Bundesministeriengesetz |
| BMEIA | Bundesministerium für europäische und internationale Angelegenheiten |
| BMI | Bundesministerium für Inneres |
| BMLV | Bundesministerium für Landesverteidigung |
| BwD | Betreiber wesentlicher Dienste |
| CCC | Cybersecurity Competence Community |
| CKM | Cyberkrisenmanagement |
| CKM-KA | Cyberkrisenmanagement Koordinationsausschuss |
| CSC | Cyber Security Center |
| CSP | Cyber Sicherheit Plattform |
| CSS | Cyber Sicherheit Steuerungsgruppe |
| EdöV | Einrichtungen der öffentlichen Verwaltung |
| EDT | Emergenten und Disruptiven Technologien |
| E-ID | elektronischer Identitätsnachweis |
| ENISA | Agentur der Europäischen Union für Cybersicherheit |
| EU | Europäische Union |
| EC3 | European Cybercrime Centre |
| IKDOK | Innerer Kreis der Operativen Koordinierungsstruktur |
| IKT | Informations- und Kommunikationstechnik |
| IT | Informationstechnik |
| IoT | Internet of Things |

| | |
|---|---|
| KI | Künstliche Intelligenz |
| KMU | Kleine und mittlere Unternehmen |
| NATO | Nordatlantikpakt-Organisation |
| NISG | Netz- und Informationssystemsicherheitsgesetz |
| NIS-RL | Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union |
| OECD | Organisation für wirtschaftliche Zusammenarbeit und Entwicklung |
| OpKoord | Operative Koordinierungsstruktur |
| OSINT | Open Source Intelligence |
| OSZE | Organisation für Sicherheit und Zusammenarbeit in Europa |
| ÖBH | Österreichisches Bundesheer |
| ÖSCS | Österreichische Strategie Cybersicherheit |
| ÖSS | Österreichische Sicherheitsstrategie |
| SKKM | Staatliches Krisen- und Katastrophenschutzmanagement |
| ULV | Umfassende Landesverteidigung |
| VN | Vereinte Nationen |

# 7

# Anhang zur ÖSCS 2021

## Leitlinien für die Umsetzung

Die folgenden Leitlinien sind den Ressorts eine Hilfestellung und Orientierung, um eine möglichst einfache und effiziente Umsetzung der Maßnahmen zu ermöglichen. Abhängig von der konkreten Maßnahme kommen alle oder einzelne Leitlinien zur Anwendung.

1. **Sicherheitsgedanke:** Der Betrieb und die Weiterentwicklung der IT hat auf einem umfassenden Sicherheitsgedanken zu basieren, der strategische, organisatorische und technische Elemente (z. B. Security by Design) berücksichtigt. Dabei ist ein gemeinsames Vorgehen der Ressorts herzustellen.

2. **Risikobasierter Ansatz:** Die ÖSCS 2021 geht von einem gesamtheitlichen und risikobasierten Ansatz aus. Dieser zielt darauf ab, die wahrscheinlichsten und folgenschwersten Risiken zu identifizieren, zu priorisieren und entsprechende Gegenmaßnahmen zu entwickeln.

3. **Transparenz:** Bei der Umsetzung von Maßnahmen wird der Ansatz der Transparenz verfolgt, indem der Maßnahmenkatalog und der Fortschrittsbericht – soweit möglich – veröffentlicht werden.

4. **Kooperativer Ansatz:** Die relevanten Akteure arbeiten gemeinsam an der Umsetzung von konkreten Maßnahmen.

5. **Multi-Stakeholder-Ansatz:** Im kooperativen Ansatz sollen die betroffenen Interessensgruppen, soweit möglich, eingebunden werden und aktiv mitgestalten können. Die Komplementarität staatlicher und nichtstaatlicher Maßnahmen ist dabei wesentlich.

6. **Eigenverantwortlichkeit:** Solange die IT-Systeme der Ressorts nicht konsolidiert sind, ist jedes Ressort für die Sicherheit der eigenen IT-Systeme verantwortlich.

7. **Wirtschaftlichkeit:** Bei der Umsetzung der Maßnahmen sollen vorhandene ökonomische Ressourcen sowie Synergien genutzt werden.

8. **Rechtsförmlichkeit:** Aus Gründen der Verständlichkeit, Übersichtlichkeit und Systematik sollen die rechtlichen Bestimmungen im Bereich der Cybersicherheit klar und verständlich und, soweit dies verfassungsrechtlich möglich ist, in einem Regelwerk enthalten sein.

9. **Unionskonformität:** Bei der Umsetzung sind die Vorgaben und Entwicklungen auf europäischer Ebene zu berücksichtigen.

10. **Ethik:** Es sollen ethische Fragestellungen im Zusammenhang mit neuen Technologien auf Basis bestehender europäischer und österreichischer Grundwerte berücksichtigt werden.

**Impressum**

Medieninhaber, Verleger und Herausgeber:
Bundeskanzleramt, Ballhausplatz 2, 1010 Wien
Autorinnen und Autoren: BKA, Abteilung I/8 – Cybersicherheit, GovCERT, NIS BÜRO und ZAS
Gesamtumsetzung: BKA
Fotonachweis: iStock, BKA/Andy Wenzel (Bundeskanzler Karl Nehammer)
Layout: BKA Design & Grafik
Druck: Druckwerkstatt Handels GmbH
Wien, 2021. Stand: 29. November 2021


Rückmeldungen: Ihre Überlegungen zu vorliegender Publikation übermitteln Sie bitte an cybersicherheit@bka.gv.at.